Universidade Vigo

I&C Lab

Avances en Comunicación y Computación Cuántica

Manuel Fernández Veiga
Ana Fernández Vilas
Rebeca P. Díaz Redondo

[24 de octubre de 2023]

XUNTA DE GALICIA

Unión Europea

Unha maneira de facer Europa.

Fondos Europeos

CESGA GALICIA SUPERCOMPUTING CENTER

Despregamento dunha infraestructura baseada en tecnoloxías cuánticas da información que permita impulsar a I+D+i en Galicia.

Apoiar a transición cara a una economía dixital.

Operación financiada pola Unión Europea, a través do FONDO EUROPEO DE DESENVOLVEMENTO REXIONAL (FEDER) como parte da resposta da Unión á pandemia da COVID-19

FECHA	AUTOR	CAMBIOS	VERSIÓN
22/09/2023	ARM	Informe para entrega	1.0

Índice de contenidos

Lista de figuras

Lista de tablas

1. Resumen ejecutivo

Las tareas básicas de procesamiento cuántico de la información son la *criptografía cuántica* (en especial la distribución cuántica de claves (QKD, *Quantum Key Distribution*)), la *computación cuántica* y las *comunicaciones cuánticas*. La criptografía cuántica materializa la transmisión de información de forma incondicionalmente segura [168, 54] ---o con seguridad perfecta, como también se denomina--- entre dos puntos. Las leyes de la mecánica cuántica (en particular el teorema de no clonación y el postulado de medida) impiden, al contrario de lo que sucede en un enlace de comunicaciones clásico, que un observador pueda copiar o modificar la información en tránsito. La computación cuántica [297, 344] es la manipulación local o remota de un estado cuántico para conseguir resolver determinados algoritmos computacionales de un modo que está fuera del alcance teórico y práctico de los ordenadores clásicos, hoy y en el futuro. Simplemente, las operaciones físicamente posibles sobre un estado cuántico no son realizables con los circuitos electrónicos clásicos, que manejan estados binarios. Las comunicaciones cuánticas consisten en la transmisión de información mediante la transferencia de estados cuánticos entre dos puntos, o bien en la manipulación local de un estado cuántico multipartito entrelazado que comparten dos o más participantes [230, 468]. El soporte físico para la transmisión de información cuántica es, y previsiblemente seguirá siendo, el estado cuántico de la luz, debido a que los fotones se pueden transmitir a largas distancias en fibra óptica o en espacio libre con poca decoherencia de estado, aunque sufren pérdidas por absorción (atenuación) y por dispersión.

Estas tareas y otras semejantes de procesamiento cuántico de la información podrán ser utilizadas de forma remota si operan sobre una infraestructura general de comunicación como la IC, que cabe definir como una red global de procesadores cuánticos interconectados. En este documento, se entiende por procesador cuántico o procesador de información cuántica (en adelante, QPU, *Quantum Processing Unit*) cualquier elemento capaz de llevar a cabo una o más de estas funciones: (a) generar estados cuánticos; (b) ejecutar puertas o circuitos de computación sobre estados cuánticos; (c) realizar medidas cuánticas sobre un estado [15, 470]. Cualquiera de estas operaciones podrá utilizarse asimismo para proporcionar comunicaciones clásicas seguras (sobre QKD u otras primitivas fundamentales de seguridad) o para incrementar la eficiencia de la comunicación, la computación y el almacenamiento (CCA) clásicos de la información. Como se sigue de esta definición, la IC servirá en particular para proporcionar acceso a un sustrato de computación cuántica distribuida, que se encuentra en la actualidad en estado embrionario. Los grandes conglomerados tecnológicos de Internet (Alphabet, IBM, Intel, Microsoft, Amazon, Alibaba, Baidu), además de los estados de naciones desarrolladas (EE.UU., Japón, Unión Europea, China) compiten por desarrollar procesadores cuánticos cada vez más capaces y sofisticados. Como estandarte de esta carrera, por ejemplo, IBM ha anunciado sus planes para fabricar en 2025 el procesador cuántico Kookaburra con 1386 qubits y una arquitectura diseñada con un bus de comunicaciones preparado para interconectar tres procesadores en un sistema de 4158 qubits capaz de paralelizar algoritmos cuánticos [154]. De modo experimental, empresas como IBM y Amazon han puesto ya a disposición de usuarios externos pequeños procesadores cuánticos [84, 7], en lo que no es sino un ensayo ancilar de computación cuántica distribuida.

No obstante las perspectivas, la IC, y en particular las comunicaciones cuánticas y las nuevas tecnologías de red, son importantes no solo para interconectar procesadores cuánticos remotos a escala global y conseguir que cooperen en una tarea computacional compleja o masiva, sino sobre todo en una primera fase de desarrollo tecnológico para interconectar procesadores cuánticos a corta distancia (por debajo de 10 m, por dar una referencia aproximada). Con la tec-

nología presente, las QPU tienen aún un tamaño y una complejidad muy limitados, de forma que para abordar la resolución de problemas complejos solo cabe conectar varias de ellas próximas entre sí por medio de canales cuánticos con los que transferir o compartir información cuántica. Un escenario de interés relacionado con este es el de la computación híbrida clásico-cuántica, en el que un conjunto de CPUs clásicas delegan en una o más QPUs la resolución, vía computación cuántica, de (una parte de) un algoritmo de optimización, de aprendizaje, de simulación, etc. Aunque la distinción entre comunicaciones a corta o a larga distancia es sustancial ---y se discute exhaustivamente en este informe--- es preciso señalar que varios de los retos técnicos son comunes a ambos escenarios de aplicación: la generación y uso de estados entrelazados, la decoherencia y el coste de la comunicación [62, 296] son ejemplos relevantes, tanto en sus aspectos teóricos como de realización técnica.

El propósito de este informe es revisar el estado del arte relativo a los fundamentos teóricos y la tecnología de la IC, con atención particular a la viabilidad, las dificultades y las posibilidades de aplicación relativas a la interconexión de QPUs cercanas. Como características destacadas de este trabajo, nos permitimos señalar las siguientes:

1. El informe ofrece una información detallada del estado del arte acerca de los fundamentos científicos, la arquitectura y la tecnología de la IC, por igual. A diferencia de otros documentos de parecido propósito, la aproximación que se ha seguido en este no prima ninguno de los tres aspectos sobre los demás y es, en cierto sentido, multidisciplinar. Este documento dedica espacio a los fundamentos físicos de la computación y la comunicación, a los elementos constitutivos de la IC, con su tecnología y aplicaciones, y también a la computación cuántica de manera homogénea y unificada.

2. Una parte sustancial del contenido está dedicada a exponer con cierta profundidad la noción de entrelazamiento, su caracterización formal, las realizaciones tecnológicas y experimentales disponibles y su significado como recurso nativo de comunicaciones en la IC.

3. Al final del informe se presenta un análisis prospectivo de las principales vías tecnológicas para la construcción de la IC, de nuevo con énfasis en la interconexión de QPUs como primer paso para el desarrollo de un sistema global más complejo y extenso. Se discuten asimismo los retos científicos de mayor orden que hay que superar para el desarrollo de la computación cuántica fiable y masiva, tanto de hardware como de software y de facilidad de programación.

En la elaboración de este informe se han consultado numerosas fuentes y referencias especializadas, entre ellas otros trabajos de naturaleza descriptiva o tutorial sobre aspectos parciales de la tecnología, la ingeniería, la ciencia de computación o la física subyacentes a la IC y sus elementos. Por completitud, pero sin intención exhaustiva, se da una lista de estos artículos extensos de revisión en la Tabla 1.

La estructura y organización del resto del documento es esta. En la sección 2 se ofrece una presentación del entrelazamiento cuántico, que es una de las propiedades distintivas de los sistemas cuánticos respecto de los estados clásicos. Pese a que el entrelazamiento es una forma de correlación de estados que no se comprende aún totalmente, este fenómeno resulta crucial para la existencia y funcionamiento de la computación y la comunicación cuántica ---por ejemplo, en la teleportación de qubits y en la codificación superdensa [230]---. El entrelazamiento es esencial en tanto que hace posibles formas de comunicación no clásicas que sacan partido de la

Tabla 1: Otros artículos de revisión sobre Internet cuántica.

Referencia	Año	Tema
[246]	2008	Introducción básica a la IC
[396]	2011	Repetidores cuánticos basados en conjuntos atómicos y óptica lineal
[378]	2015	Redes cuánticas basadas en cavidades resonantes con átomos aislados y fotones
[481]	2015	Criptografía cuántica MDI
[70]	2015	Criptografía cuántica QKD
[334]	2015	Primitivas de los repetidores cuánticos
[336]	2016	Generación de repetidores cuánticos
[205]	2016	Memoria cuánticas, aplicaciones
[160]	2017	Computación cuántica ciega
[191]	2018	Capacidad de los canales cuánticos
[13]	2018	Plataforma físicas para tecnologías cuánticas fotónicas basadas en espín
[470]	2018	Estadios de desarrollo de la IC
[15]	2020	Tecnologías cuánticas con sistemas de espín de estado sólido e interfaces ópticas
[392]	2021	Redes cuánticas basadas en centros de color en diamantes
[21]	2021	Herramientas para diseño de redes cuánticas
[255]	2021	Teoría de la información cuántica
[415]	2021	Quantum Networks
[22]	2022	Repetidores cuánticos
[80]	2022	Computación cuántica distribuida
[79]	2023	Quantum switches y quantum paths
[287]	2023	Quantum Networks

no localidad de los estados de un sistema físico cuántico distribuido entre varios puntos. Como tal, es preciso examinar los usos del entrelazamiento como nuevo recurso para la computación y las comunicaciones, y de esta cuestión nos ocupamos en el apartado 3, donde se revisan primitivas básicas como la teleportación y el intercambio de entrelazamiento, se presentan como elementos operacionales de conectividad los repetidores cuánticos [130, 477] y se introduce el problema de la comunicación sobre canales con ruido. A continuación, en el apartado 4 se examinan las realizaciones físicas de los repetidores y memorias cuánticas, con objeto de aclarar qué rango operativo poseen con la tecnología actual. El paso siguiente, en el apartado 5, es presentar las distintas propuestas de arquitectura que han ido apareciendo para la construcción de una IC global, analizando la división funcional y los conceptos que postulan, pues una red operable a gran escala exige estándares claros y bien definidos. Se tratan las cuestiones de diseño de la red (y con particular atención, el enrutamiento), la organización de las posibles pilas de protocolos, las normas emergentes en este campo y, por último, las aplicaciones más previsibles y los retos más notorios a los que se enfrenta la construcción de la IC. El apartado 6 abre la discusión específica sobre la computación cuántica, presentando el paradigma en que hoy se encuentra. Las métricas necesarias para cuantificar la capacidad de computación cuántica se introducen brevemente en el apartado 7, y los métodos para combatir los errores de cómputo

y aumentar la fiabilidad se repasan en el apartado 8. Después de estas bases, se hace una revisión exhaustiva de las soluciones de computación cuántica existente, primero las que integran hardware y software (apartado 9, seguidas de las soluciones solo hardware (apartado 10), las soluciones de servicios de computación en la nube (apartado 11), y as soluciones solo software (apartado 12). Para acabar, por lo que se refiere a las posibilidades técnicas, limitaciones y alternativas para la computación y la interconexión de procesadores cuánticos, las principales conclusiones y propuestas del informe se resumen en el apartado 13.

Con intención hacerlo en la medida de lo posible autocontenido, el informe se acompaña de varios apéndices donde se expone de forma condensada el formalismo de la mecánica y la información cuántica: el apéndice A presenta los postulados básicos de la mecánica cuántica, el apéndice B hace lo propio con los circuitos cuánticos, que son los bloques constitutivos de la computación cuántica; y el apéndice C es una introducción a las medidas y resultados de la teoría de la información cuántica, que ha pasado en los últimos 30 años de ser una curiosidad teórica a convertirse en una herramienta de trabajo para que físicos, matemáticos e ingenieros desarrollen las tecnologías de la información cuánticas.

2. Teoría de entrelazamiento cuántico

Este apartado presenta la definición formal del entrelazamiento, la caracterización de este fenómeno y varias clases importantes de estados entrelazados, que son fundamentales en distintas tareas de comunicación y computación cuántica, también por tanto en la interconexión de QPUs. El entrelazamiento es un fenómeno exclusivamente cuántico, sin parangón o analogía en el mundo clásico, y como tal es tenido por una de las propiedades definitorias de la teoría cuántica.

2.1. Definición y propiedades

En términos cualitativos, el entrelazamiento se refiere a la imposibilidad de describir estados cuánticos multipartitos mediante la especificación independiente de sus componentes o subestados. El entrelazamiento es una forma de correlación presente en los sistemas cuánticos que es incompatible con cualquier teoría de variables ocultas basada en el paradigma de la mecánica clásica. La existencia de entrelazamiento ha sido confirmada por multitud de experimentos que, junto con las consecuencias que implica desde la propia teoría cuántica, desafían la intuición física y filosófica corriente desde Einstein, Podolsky y Rosen (EPR) hasta nuestros días.

En la literatura existen varias formulaciones de la noción de medida del entrelazamiento cuántico [214, 230]. En todas ellas, no obstante, lo significativo es el hecho de que el entrelazamiento opera como un recurso para facilitar o mejorar o hacer posible las tareas de comunicación o computación cuántica, de modo singular en los casos de la teleportación cuántica, intercambio de entrelazamiento, purificación y destilación de entrelazamiento y corrección de errores cuánticos, todas las cuales desempeñan un papel fundamental en el diseño y construcción de dispositivos repetidores y conmutadores cuánticos. El entrelazamiento es además un recurso no trivial respecto del paradigma LOCC (operaciones locales y comunicaciones clásicas, *Local Operations and Classical Communications*; ver más adelante), lo que significa que no es posible incrementarlo solo con transformaciones locales como puertas cuánticas o medidas, con protocolos de comunicaciones clásicos (sean estos adaptativos o interactivos) ni con una

combinación arbitraria de los dos tipos de estrategias. Físicamente, el proceso de generación y distribución de estados entrelazados puede lograrse mediante sistemas con Hamiltonianos acoplados, enviando fotones entrelazados a múltiples destinos por una fibra óptica o espacio libre, y también llevando a cabo medidas colectivas de algún observable cuántico desde varios puntos diferentes. Las características del entrelazamiento varían dependiendo de la realización física concreta, como es natural suponer.

En términos formales, la noción de entrelazamiento es complementaria a la de *separabilidad*, que se puede aplicar tanto a estados como a canales como a medidas en sistemas bipartitos. A un sistema bipartito le corresponde por definición un espacio de Hilbert $\mathscr{H} = \mathscr{H}_A \otimes \mathscr{H}_B$ que es el producto tensor de dos subespacios componentes $\mathscr{H}_A$ y $\mathscr{H}_B$. El sistema bipartito tiene dimensión $d = \dim(\mathscr{H}_A)\dim(\mathscr{H}_B)$. Un estado bipartito ρ_{AB} en el espacio $\mathscr{H}$ se dice *separable* [468, 230] si existen un conjunto índice I, una distribución de probabilidades $\{p(i) : i \in I\}$ y dos familias de estados en los sistemas A y B, $\{|\varphi_i\rangle_A : i \in I\}$ y $\{|\phi_i\rangle_B : i \in B\}$ tales que

$$|\rho\rangle_{AB} = \sum_{i\in I} p(i)|\varphi_i\rangle_A \otimes |\phi_i\rangle_B. \tag{1}$$

Véase que, en esta definición, los estados $|\varphi_i\rangle_A$ y $|\phi_i\rangle_B$ pueden ser puros o mixtos: la noción de separabilidad se refiere a que los estados componentes son independientes, en el sentido de que

$$\rho_B = \mathrm{tr}_A\big(|\rho\rangle\langle\rho|_{AB}\big) = \sum_{i\in I} p(i)|\phi_i\rangle\langle\phi_i|_B, \quad \text{y } \rho_A = \mathrm{tr}_B\big(|\rho\rangle\langle\rho|_{AB}\big) = \sum_{i\in I} p(i)|\varphi_i\rangle\langle\varphi_i|_A$$

son los operadores de densidad reducidos en A y B. A la vista de (1), es claro que un estado separable representa una distribución de probabilidad clásica sobre los estados cuánticos independientes de dos subsistemas o registros los cuales, si se los considera por separado, solo pueden poseer correlación clásica. Visto de otro modo, supóngase que A (Alice) elige un valor $i \in I$ con probabilidad $p(i)$ y prepara su sistema local en el estado $|\varphi_i\rangle_A$. Alice transmite por un canal clásico el mensaje i a B (Bob) y este, con operaciones locales, crea o prepara el estado $|\phi_i\rangle_B$. A continuación, Alice y Bob descartan el valor de i, lo que deja al sistema conjunto en el estado separable (1). A este estado se ha llegado tan solo mediante operaciones cuánticas locales de Alice y Bob y mediante la transmisión clásica de información, es decir, dentro del paradigma LOCC. Por lo demás, usando en (1) la descomposición espectral, es posible probar que un estado separable siempre se puede expresar como una combinación convexa de productos de estados puros, es decir,

$$\rho_{AB} = \sum_{i\in J} p(i)|\psi_i\rangle_A \otimes |\xi_i\rangle_B \tag{2}$$

siendo los $\{\psi_i\rangle_A\}$ y $\{|\xi_i\rangle_B\}$ estados puros en A y B, respectivamente, y con $|J| \leq \mathrm{rango}(\rho_{AB})^2$. El conjunto de estados separables es además compacto.

Un estado ρ_{AB} es *entrelazado* si no es separable. Cuando, en todas las fórmulas de esta sección, se reemplazan los estados por operadores (completamente) positivos, obtenemos las definiciones y caracterización básica de las *medidas separables* y de los *canales separables*, análogamente.

2.2. Entrelazamiento bipartito. Caracterización

La propiedad de separabilidad guarda estrecha relación con el hecho de que una transformación sea positiva, tal como pone de manifiesto el *criterio de Horodecki*: un estado ρ_{AB}

es separable si y solo si para cualquier transformación positiva Φ del sistema A el operador $(\Phi \otimes \mathbb{1}_B)(\rho_{AB}) \in \mathscr{H}_{A'} \otimes \mathscr{H}_B$ es positivo. El uso principal de este enunciado consiste en aplicarlo con un Φ bien elegido para probar que ciertas familias de estados no son separables, es decir, están entrelazados. Otra forma sencilla de analizar si un estado es separable la da el *criterio PPT* (*Positive Partial Transpose*): si un estado bipartito ρ_{AB} es separable, entonces es PPT; o en forma contrarrecíproca: si un estado bipartito ρ_{AB} no es PPT, entonces es entrelazado. Aquí, se entiende por estado PPT aquel cuya traspuesta parcial (respecto de B en este caso)

$$T_B(\rho_{AB}) = \sum_{i,j=0}^{d-1} (\mathbb{1}_A \otimes |i\rangle\langle j|_B)\rho_{AB}(\mathbb{1}_A \otimes |i\rangle\langle j|_B)$$

es un operador positivo. Desde un punto de vista computacional, es claro que el criterio PPT es verdaderamente sencillo de aplicar, mientras que el criterio de Horodecki (más completo) no es constructivo.

Dentro del ámbito de este documento, los ejemplos de estados entrelazados que se utilizarán para analizar la comunicación y la computación cuántica distribuida son estos:

1. El *estado entrelazado maximal* $\Phi_{AB} = |\Phi\rangle\langle\Phi|_{AB}$ con

   $$|\Phi\rangle_{AB} := \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A \otimes |i\rangle_B,$$

   si los sistemas A y B tienen dimensión d. Φ_{AB} tiene *entrelazamiento máximo* porque $\mathrm{tr}_A(\Phi_{AB}) = \mathrm{tr}_B(\Phi_{AB}) = \mathbb{1}/d$, o lo que es igual, cada uno de los subsistemas A y B siguen una distribución de probabilidad uniforme en sus estados base. Cualquier transformación unitaria U sobre los sistemas A o B sigue resultando en un estado de entrelazamiento máximo $(U_A \otimes \mathbb{1}_B)\Phi_{AB}(U_A \otimes \mathbb{1}_B)^\dagger$. Se puede comprobar sin dificultad que $\Phi_{AB} = \frac{1}{d}\,\mathrm{vec}(\mathbb{1}_A)\,\mathrm{vec}(\mathbb{1}_B)^\dagger$.

2. Los *estados de Bell* de dos qubits. Sean X y Z los operadores de Pauli canónicos (ver el Apéndice A). Dados dos bits $z, x \in \{0,1\}$, se definen los estados de Bell de dos qubits por

   $$|\Phi_{z,x}\rangle := (Z^z X^x \otimes \mathbb{1})|\Phi\rangle,$$

   donde en este caso es $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. En concreto,

   $$|\Phi^\pm\rangle := \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$
   $$|\Psi^\pm\rangle := \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle),$$

   que se denominan también *pares EPR* y son equivalentes por acción de los operadores de Pauli: $|\Phi^+\rangle_{AB} = Z_B|\Phi^-\rangle_{AB} = -\imath Y_B|\Psi^-\rangle_{AB} = X_B|\Psi^+\rangle_{AB}$. Los estados de Bell se pueden generalizar a cualquier dimensión $d > 2$, aunque esta extensión no se usará en este documento [230]. Los estados de Bell constituyen una base ortonormal y, por consiguiente, una medida cuántica. Los estados de Bell son la clave de la teleportación cuántica (apartado 4).

3. *Estados isotrópicos*. Se definen los operadores de proyección

$$\Delta_0 := \frac{1}{d}\sum_{i=0}^{d-1} |ij\rangle|\otimes|ij\rangle, \quad \Delta_1 := \mathbb{1}_A\otimes\mathbb{1}_B - \Delta_0.$$

Para $\lambda\in[0,1]$, los estados de la forma

$$\zeta_{AB}(\lambda) := \lambda\Delta_0 + (1-\lambda)\frac{\Delta_1}{d^2-1}$$

son los estados isotrópicos.[1] Usando el criterio de Horodecki se puede probar que si $\lambda\in(1/d,1]$ los estados isotrópicos son entrelazados. Una de las propiedades de interés de los estados isotrópicos es que son invariantes frente a transformaciones $(U_A\otimes U_B^\dagger)$ con U_A, U_B unitarias: $(U_A\otimes U_B^\dagger)\zeta_{AB}(\lambda)(U_A\otimes U_B^\dagger)^\dagger = \zeta_{AB}(\lambda)$.

4. *Estados de Werner*. Se denota por $W(|\varphi\rangle\otimes|\phi\rangle) := |\phi\rangle\otimes|\varphi\rangle$ al *operador de intercambio* de dos vectores, que también se puede expresar por

$$W = \sum_{i,j=0}^{d-1} |ij\rangle\langle ji| = \sum_{i,j=0}^{d-1} |i\rangle\langle j|_A\otimes|j\rangle\langle i|_B.$$

Se definen los operadores de proyección

$$\Pi_0 := \frac{1}{2}\mathbb{1}_A\otimes\mathbb{1}_B + \frac{1}{2}W, \quad \Pi_1 := \mathbb{1}_A\otimes\mathbb{1}_B - \Pi_0 = \frac{1}{2}\mathbb{1}_A\otimes\mathbb{1}_B - \frac{1}{2}W.$$

Para $\lambda\in[0,1]$ los estados de la forma[2]

$$\omega_{AB}(\lambda) := \lambda\frac{\Pi_0}{\binom{d+1}{2}} + (1-\lambda)\frac{\Pi_1}{\binom{d}{2}}$$

son los estados de Werner, y no son separables cuando $\lambda\in[0,1/2)$, de nuevo en virtud del criterio de Horodecki [468]. Los estados de Werner son invariantes frente a la acción simultánea de operadores unitarios en ambos sistemas: $(U_A\otimes U_B)\omega_{AB}(\lambda)(U_A\otimes U_B)^\dagger = \omega_{AB}(\lambda)$.

5. *Estados GHZ* (Greenberger-Horne-Zeilinger [185]). Son estados multipartitos para $M>2$ componentes definidos por

$$|\mathrm{GHZ}_M\rangle := \frac{1}{\sqrt{2}}\left(\overbrace{|00\ldots0\rangle}^{M} + \overbrace{|11\ldots1\rangle}^{M}\right) = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes M} + |1\rangle^{\otimes M}\right).$$

Si tomamos $M=3$ y calculamos la traza parcial de $|\mathrm{GHZ}_3\rangle$ obtendremos

$$\mathrm{tr}_3\left(\frac{|000\rangle+|111\rangle}{\sqrt{2}}\frac{\langle 000|+\langle 111|}{\sqrt{2}}\right) = \frac{|00\rangle\langle 00|+|11\rangle\langle 11|}{2},$$

que es un estado mixto separable, $\sum_{i=0}^{1}|i\rangle\langle i|\otimes|i\rangle\langle i|$. Análogamente, una medida de uno cualquiera de los subsistemas capaz de distinguir entre los estados $|0\rangle$ y $|1\rangle$ dejaría el sistema en el estado $|00\rangle$ o $|11\rangle$, que es puro y separable. Los estados GHZ se demostraron experimentalmente por primera vez en [60].

[1] $\mathrm{tr}(\Delta_0)=1$, $\mathrm{tr}(\Delta_1)=d^2-1$.
[2] En este caso, $\mathrm{tr}(\Pi_0)=d^2/2+d/2=\binom{d+1}{2}$, $\mathrm{tr}(\Pi_1)=d^2-\mathrm{tr}(\Pi_0)=\binom{d}{2}$.

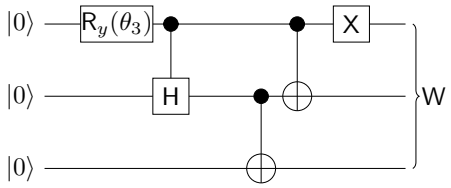


Figura 1: Circuito cuántico para generar el estado entrelazado W, formado por una puerta de rotación, una puerta Hadamard, una puerta Pauli X y dos puertas CNOT. El ángulo de rotación es $\theta_3 = 2\arccos(1/\sqrt{3})$.

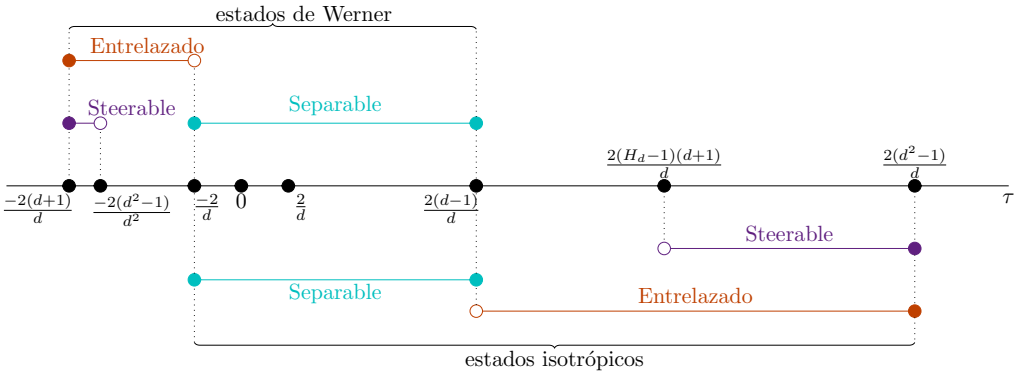


Figura 2: No-localidades en los estados isotrópicos y de Werner en función del parámetro $\tau = \frac{2(d(2\lambda-1)-1)}{2}$ (Werner) o $\tau = \lambda d/2$ (isotrópicos). El número H_d es el d-ésimo número armónico, y los círculos representan extremos abiertos o cerrados de los intervalos.

6. *Estado W*. Es también un estado M-partito para $M > 2$, en concreto el estado

$$|\mathrm{W}_M\rangle = \frac{1}{\sqrt{M}}\left(|100\ldots0\rangle + |010\ldots0\rangle + \cdots + |000\ldots1\rangle\right).$$

Si se realiza una medida de uno de los qubits, el estado resultante del sistema sigue siendo entrelazado, a diferencia de lo que sucede en el estado GHZ. Por lo tanto, los estados GHZ y W no se pueden transformar el uno en el otro por medio de operaciones LOCC, por lo que representan dos tipos de entrelazamiento fundamentalmente diferentes entre tres o más participantes. En cualquiera de los dos casos, vemos además que los estados son invariantes frente a cualquier permutación de los qubits. La Figura 1 representa el esquema de generación de W para tres qubits.

La Figura 2 muestra los fenómenos de entrelazamiento que aparecen en los estados isotrópicos y de Werner en función de un parámetro continuo τ.

La tarea de medir el grado de entrelazamiento de un sistema bi- o multipartito se puede formular como el problema de hallar una función cuyo valor cambie solo si varía el entrelazamiento entre los subsistemas ---y no las correlaciones clásicas entre ellos--- y que además sea no creciente tras operaciones LOCC arbitrarias. Se trata de una cuestión complicada para la que no hay una respuesta única [362]. En la literatura se han propuesto y utilizado para

medir el entrelazamiento el rango de Schmidt [468], la concurrencia [478], la negatividad logarítmica [502], o varias versiones de la entropía y la divergencia [44]. Para estados mixtos de dos qubits, se sabe que es posible calcular la medida de entrelazamiento con el concepto de concurrencia [478], pero hacer lo mismo en estados mixtos de dimensión arbitraria es todavía un problema abierto y activo de investigación [362]. La otra pregunta natural ---mucho más sencilla--- es qué unidad de medida se debe emplear para medir el entrelazamiento. Lo usual es tomar como unidad el *ebit*, la medida que da valor 1 al estado de Bell $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. De esta manera, un estado con entrelazamiento máximo y rango de Schmidt d tiene $\log_2 d$ ebits.

Puesto que, dependiendo de la tarea de cómputo o de comunicación, diferentes nociones de medida del entrelazamiento resultan útiles, presentaremos las más habituales en la literatura. Todas ellas responden a un principio axiomático muy general formulado en [45]: $E(A;B)_\rho$ es una medida de entrelazamiento del estado bipartito ρ_{AB} si para todo ρ_{AB} y todo canal LOCC $\mathscr{N}$ se cumple que $E(A;B)_\rho \geq E(A';B')_\omega$, donde $\omega_{A'B'} = \mathscr{N}(\rho_{AB})$; en otras palabras, solo se pide a la medida de entrelazamiento $E(\cdot;\cdot)$ que sea LOCC-monótona y no aumente de valor ni antes ni después del procesamiento local. No solo es una condición operativa razonable, sino que además resulta análoga a la desigualdad de procesamiento de la información que satisface la entropía relativa. El postulado de monotonía implica inmediatamente que una medida de entrelazamiento nunca es negativa y que $E(A;B)_\rho = 0$ para cualquier estado separable ρ_{AB}. Otras propiedades deseables para una medida de entrelazamiento son las que siguen:

P1 Fidelidad[3]. $E(A;B)_\rho = 0$ si y solo si ρ_{AB} es separable.

P2 Invariancia ante comunicaciones clásicas. Si tenemos un estado cq (clásico-cuántico) cuyo subestado cuántico q es bipartito y transmitimos el estado clásico de Alice a Bob (o viceversa), el entrelazamiento de q no varía.

P3 Convexidad. Significa, formulado de manera equivalente, que condicionar no disminuye el valor del entrelazamiento.

P4 Aditividad. El valor de la medida de entrelazamiento respeta el producto tensor.

P5 LOCC-monótona selectiva. Si el valor del entrelazamiento no aumenta en media bajo ninguna acción LOCC. Esta propiedad es más fuerte que el hecho de que $E(\cdot;\cdot)$ sea LOCC-monótona sin más, y la satisfacen muchas de las medidas comunes de entrelazamiento.

2.2.1. Rango de entrelazamiento

Supóngase que un estado bipartito es separable, por lo que se puede expresar como en (2)

$$\rho_{AB} = \sum_{i\in I} p(i)|\psi_i\rangle\langle\psi_i|_A \otimes |\xi_i\rangle\langle\xi|_B = \sum_{i\in I} p(i)\left(|\psi_i\rangle_A \otimes \langle\xi_i|_B\right)\left(|\psi_i\rangle_A \otimes \langle\xi_i|_B\right)^\dagger.$$

[3] En español, este término es confuso, pues es fácil confundirlo con una métrica entre estados $F(\rho,\sigma) = \mathrm{tr}\left(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)$. El término en inglés para la propiedad es *faithfulness*, mientras que para la medida $F(\cdot,\cdot)$ entre estados es *fidelity*. El cuadrado de la fidelidad se usa para definir una medida de distancia entre estados cuánticos denominada *distancia purificada*, $P(\sigma,\rho) := \sqrt{1-F^2(\sigma,\rho)}$. Entre las propiedades de la distancia purificada estñan $0 \leq P(\sigma,\rho) = P(\rho,\sigma) \leq 1$; $P(\rho,\sigma) = 0$ si y solo si $\rho = \sigma$; la desigualdad triangular $P(\rho,\omega) \leq P(\rho,\sigma) + P(\sigma,\omega)$; y la desigualdad de procesamiento de la informaciñon, $P\left(\mathscr{N}(\rho),\mathscr{N}(\sigma)\right) \leq P(\rho,\sigma)$ para cualquier canal ρ.

Tabla 2: Diversas medidas de entrelazamiento y sus propiedades.

Medida	Fiel	Invariante	Convexa	Aditiva	LOCC-selectiva
Rango de entrelazamiento	No				
Entropía de entrelazamiento	✓		✓	✓	
log-negatividad	✓		✓	✓	✓
Negatividad	✓		No	✓	✓
Divergencia generalizada	✓	entropía relativa	✓	✓	

Los operadores $|\psi_i\rangle_A \otimes \langle\xi_i|_B = \mathrm{vec}(A_i)$ tienen, por consiguiente, rango 1 a lo sumo, y el estado bipartito se puede expresar como una suma de operadores de rango menor o igual que 1. La generalización de esta fórmula es natural: si un estado bipartito se puede escribir como

$$\rho_{AB} = \sum_{i\in I} \mathrm{vec}(A_i)\,\mathrm{vec}(A_i)^\dagger$$

y los operadores A_i tienen rango menor o igual que r, se dice que ρ_{AB} tiene *rango de entrelazamiento* r. Los estados con rango de entrelazamiento $r = 1$ son separables.

2.2.2. Entrelazamiento de formación o entropía de entrelazamiento

Los dos estados reducidos $\rho_A = \mathrm{tr}_B(\rho_{AB})$ y $\rho_B = \mathrm{tr}_A(\rho_{AB})$ de un estado bipartito puro tienen los mismos autovalores y, en consecuencia, la misma entropía cuántica $H(\rho_A) = H(\rho_B)$. Además, se cumple que esta entropía es cero si y solo si ρ_{AB} es separable, o lo que es igual, $H(\rho_A) > 0$ si y solo si ρ_{AB} es un estado entrelazado. Esta observación motiva que se defina la *entropía de entrelazamiento* o *entrelazamiento de formación*

$$E_F(\rho_{AB}) := H\big(\mathrm{tr}_B(\rho_{AB})\big).$$

En el caso de que el estado ρ_{AB} sea mixto, la entropía de entrelazamiento se define como el mínimo del valor medio de la entropía de entrelazamiento en cualquier descomposición de ρ_{AB}. Omitimos la formulación matemática.

$E_F(\rho_{AB})$ es una medida fiel (propiedad P1), convexa (P3), y subaditiva (generaliza P4) [230].

2.2.3. (Log)-negatividad

Otra alternativa para medir el entrelazamiento consiste en partir del criterio PPT. Se define la *negatividad* del estado ρ_{AB} como

$$N(\rho_{AB}) := \frac{\|T_B(\rho_{AB}\|_1 - 1}{2},$$

donde T_B es el operador de trasposición parcial y $\|\cdot\|_1$ es la norma traza, la suma de los valores singulares de su argumento. La log-negatividad es simplemente $\log\|T_B(\rho_{AB})\|$. Esta cantidad es no negativa, fiel (P1) en el conjunto de estados PPT, LOCC-monótona selectiva para los estados PPT (generalizando P5), y aditiva (P4); la negatividad es convexa (P3), pero la log-negatividad, no.

2.2.4. Divergencia generalizada de entrelazamiento

Una clase de medidas geométricas de entrelazamiento surge al calcular la distancia entre un estado bipartito ρ_{AB} y el conjunto de todos los estados separables

$$E(A;B)_\rho := \inf_{\sigma_{AB}\ \text{separable}} D_f(\rho_{AB}||\sigma_{AB}),$$

donde la función D_f es una función de divergencia generalizada (ver el Apéndice C). Si bien la definición es intuitivamente simple y muchas de las propiedades de interés se derivan directamente de ella, el cálculo del valor del entrelazamiento por divergencia generalizada es, como se ve en la definición, un problema de optimización que rara vez tiene una solución en forma cerrada. Una posible idea para simplificar el cálculo es optimizar sobre un conjunto más pequeño, el de los estados PPT (la clase PPT contiene a los estados separables), es decir,

$$E_{\text{PPT}}(A;B)_\rho := \inf_{\sigma_{AB}\in\ \text{PPT}} D_f(\rho_{AB}||\sigma_{AB}).$$

Tomando en la definición de $E(A;B)_\rho$ distintas funciones de divergencia se obtienen variantes concretas de la divergencia de entrelazamiento. Para todas esas elecciones se cumple que la medida $E(A;B)_\rho$ es fiel (P1), convexa cuando D_f es convexa (P3), subaditiva (generaliza P4) y monótona no creciente en canales separables (como los canales LOCC). Cuando D_f es la entropía relativa cuántica, $E(A;B)_\rho$ es también invariante ante comunicaciones clásicas (P2).

2.3. Entrelazamiento multipartito. Estados grafo

Los estados GHZ y W son casos maximales de entrelazamiento multipartito. En su forma más general, la descripción de un entrelazamiento arbitrario en un sistema multiparte se lleva a cabo con los *estados grafo*. Un estado grafo es un estado entrelazado asociado con el grafo $G = (V,E)$ (vértices V y aristas E no dirigidas), definido como

$$|G\rangle := \prod_{\{i,j\}\in E} C_{ij}^{\mathsf{Z}} \left(\bigotimes_{v\in V} |+\rangle_v \right),$$

donde la puerta Z-controlada C_{ij}^{Z} está definida para los qubits de enbtrada i y j por

$$C_{ij}^{\mathsf{Z}} := |0\rangle\langle 0|_i \otimes \mathbb{1}_j + |1\rangle\langle 1|_i \otimes \mathsf{Z}_j = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

C_{ij}^{Z} es simétrica en i,j y cualesquiera C_{ij}^{Z}, $C_{k\ell}^{\mathsf{Z}}$ conmutan para i,j,k,ℓ arbitrarios.

Así pues, los estados grafo modelan relaciones de entrelazamiento arbitrarias entre los componentes del sistema multipartito, con las interacciones especificadas por medio de las puertas Z controladas. Por ejemplo, si el grafo es un triángulo, el correspondiente estado grafo es

$$\frac{1}{\sqrt{8}}\big(|000\rangle + |100\rangle + |010\rangle - |110\rangle + |001\rangle - |101\rangle - |011\rangle - |111\rangle\big).$$

Los estados grafo tienen especial interés en la construcción de códigos cuánticos de corrección de errores, esto es, en la computación cuántica [180]. La dinámica de los estados grafo se analiza en [201, 303] y se resume en estos principios:

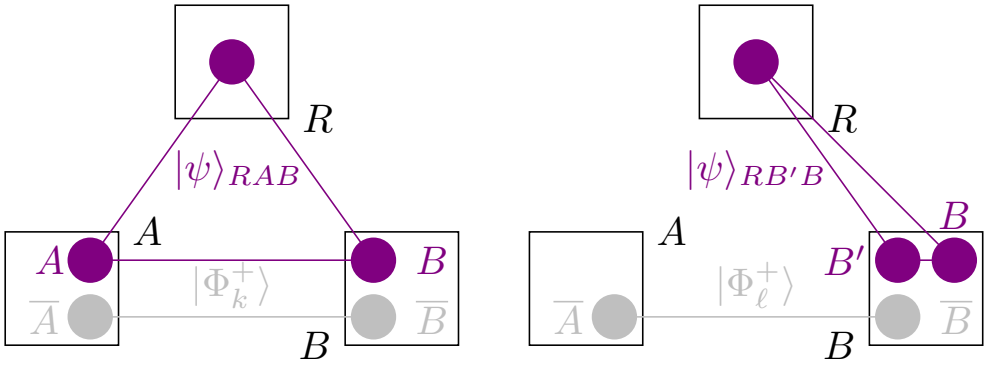


Figura 3: Fusión de estados exacta. A se apoya en el estado entrelazado $|\Phi_k\rangle_{\overline{AB}}$ para enviar la parte local reducida A de su estado $\psi\rangle_{RAB}$ a B. El proceso tiene un coste de $\log_2 k - \log_2 \ell$.

- Aplicar una puerta Clifford localmente a un grafo estado equivale a realizar una secuencia de complementos locales en el grafo. El complemento local de un grafo en un nodo a consiste en invertir el subgrafo inducido por la vecindad de a: si b y c son ambos vecinos de a, en el grafo invertido se elimina la arista $\{b,c\}$ si existe o bien se crea la arista $\{b,c\}$ si no existe.
- Una medida Pauli Z sobre un nodo desconecta ese nodo de todos sus vecinos (i.e., elimina todos los enlaces de ese nodo).
- Una medida Pauli Y sobre un nodo ejecuta el complemento en ese nodo y lo desconecta.
- Una medida Pauli X en dos qubits consecutivos dentro de un subgrafo lineal los desconecta pero conecta con una arista sus otros vecinos.
- El entrelazamiento en un grafo estado conectado es localizable. Esto significa que es posible proyectar dos qubits cualesquiera del grafo en un par de estados de Bell mediante la realización de una medida (Pauli X o Z) sonre los otros qubits.

El concepto de grafo estado se puede generalizar a sistemas bosónicos de variable continua [21].

2.4. Fusión y división de estados

La fusión (*merging*) (y su operación recíproca, la división (*splitting*)) de estados son formas de distribuir y concentrar un estado, respectivamente, en varios nodos a través de una red de comunicación cuántica. Puede entenderse la fusión como una forma generalizada de compresión y envío de información cuántica con menor coste que la teleportación pura, una tarea que se puede comparar a la compresión de información clásica con información lateral en el receptor [4]. Puesto que la fusión y la división de estados conllevan potencialmente un ahorro de recursos en una red cuántica, damos aquí algunas nociones y resultados principales sobre ellas.

En la fusión de estados intervienen tres participantes separados, un emisor A, un receptor B y un sistema de referencia R en el que considerar una purificación. A dispone de los sistemas

[4] El problema de Wyner-Ziv [168].

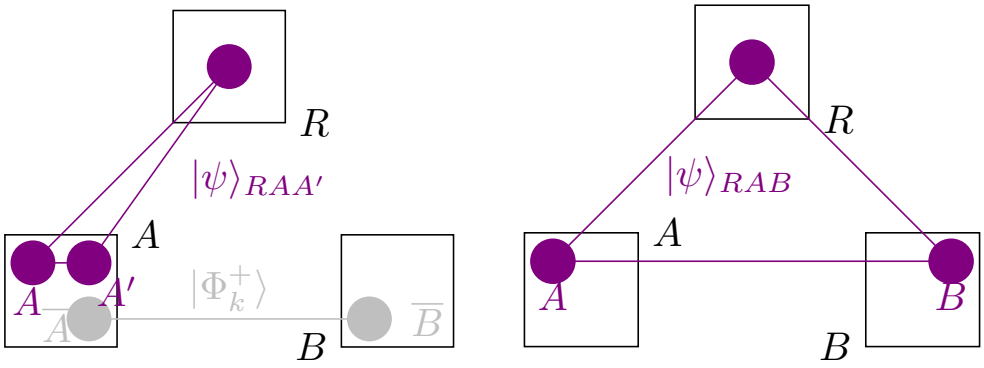


Figura 4: División de estados exacta. A se apoya en el estado entrelazado $|\Phi_k\rangle_{\overline{AB}}$ para enviar la parte local A' de su estado $|\psi\rangle_{RAA'}$ a B, $|\psi\rangle_{RAB}$. El coste del proceso es $\log_2 k$.

cuánticos A y $\overline{A}$; B tiene los sistemas locales B, B' y $\overline{B}$. Suponemos que A y B' tienen la misma dimensión. Dado un estado tripartito puro $|\psi\rangle_{RAB}$ compartido entre R, A y B, el objetivo de la *fusión de estados* es transferir el subsistema A de $|\psi\rangle_{RAB}$ a B manteniendo la coherencia de R y B, de modo que B obtenga $|\psi\rangle_{RB'B}$. Tanto A como B se atienen al paradigma LOCC, solo se les permiten operaciones locales y comunicación clásica asistida por un recurso de entrelazamiento máximo compartido de dimensión k, por ejemplo $|\Phi_k^+\rangle_{\overline{AB}} = \sum_{i=0}^{k-1} |i\rangle_{\overline{A}} \otimes |i\rangle_{\overline{B}}$. Ni A ni B pueden realizar transformación alguna sobre el sistema de referencia R, y tras la operación de fusión pueden seguir manteniendo un estado entrelazado $|\Phi_\ell^+\rangle_{\overline{AB}} = \sum_{i=0}^{k-1} |i\rangle_{\overline{A}} \otimes |i\rangle_{\overline{B}}$ de dimensión ℓ distinta del original. La variación en el entrelazamiento se mide como $\log_2 k - \log_2 \ell$ y puede ser positiva ---se consume una cierta cantidad del entrelazamiento inicial en el proceso de fusión---, o negativa ---y entonces $\log_2 \ell - \log_2 k$ mide la ganancia neta de entrelazamiento---. Si $k, \ell > 1$ se asume que una parte del entrelazamiento inicial se gasta en conseguir la fusión, y la situación se denomina catalítica. El caso especial en que $\log_2 \ell = 0$ se denomina no catalítico. Si bien la comunicación cuántica directa puede no ser posible, recordemos que se puede simular mediante un par de Bell y el envío de 2 bits clásicos de A a B por cada qubit, con teleportación. Así pues, la fusión de estados requeriría $2(\log_2 k - \log_2 \ell) \leq 2 \log_2 k$ bits de comunicación clásica, potencialmente menos que la teleportación directa.

El escenario descrito, una representación gráfica del cual se da en la Figura 3, se corresponde con la operación *one-shot* en la que el emisor desea transferir un estado exactamente, con probabilidad de error cero. Si un cierto margen de discrepancia es tolerable, digamos que una fidelidad $F(|\psi\rangle_{RAB}, |\psi\rangle_{RB'B}) \geq 1 - \varepsilon$, tenemos el escenario *one-shot* con fusión de estados aproximada; la versión asintótica ocurre cuando se quiere una fusión (aproximada) de muchas copias de $|\psi\rangle_{RAB}$, o sea cuando el estado en A es $(|\psi\rangle_{RAB})^{\otimes n}$ y $n \to \infty$.

En la *división de estados* exacta, A y B comaprten un estado $|\Phi_k^+\rangle_{\overline{AB}} = \frac{1}{\sqrt{k}} \sum_{i=0}^{k-1} |i\rangle_{\overline{A}} \otimes |i\rangle_{\overline{B}}$; A tiene también un estado $|\psi\rangle_{AA'}$ cuya purificación con R es $|\psi\rangle RAA'$. A y B pueden efectuar operaciones LOCC asistidas por $|\Phi_k^+\rangle_{\overline{AB}}$, pero no actuar sobre R. El objetivo es transferir la parte A' de $|\psi\rangle_{RAA'}$ desde A a B manteniendo la coherencia de R y AB, para obtener como resultado $|\psi\rangle_{RAB}$. El coste de entrelazamiento de la división de estados se define como $\log_2 k$. Como en el caso de la fusión, la división es aproximada si se relaja la transferencia exacta y se mide la discrepancia entre el estado inicial y el final con la fidelidad. La versión asintótica introduce la flexibilidad de usar

Tabla 3: Algunos resultados de coste de entrelazamiento para la fusión y división de estados bipartita. Los resultados aparecen en [483, 49].

	Asintótico	One-shot	
		one-way LOCC	two-way LOCC
Fusión	$H(A\|B)_\psi$ (exacto)	$\log_2 k = 1$ (aprox., no catalítico)	$\log_2 k = 0$ (aprox.)
División		$\log_2 k \geq \log_2 \text{rango}(\psi_{A'})$ (exacto)	

como estado inicial n copias de $|\psi\rangle_{RAB}$ y dejar que $n \to \infty$.

La Tabla 3 enumera algunos de los resultados conocidos para el coste de entrelazamiento de las tareas de fusión y división de estados en sistemas de dos nodos (más el de referencia).

2.5. Teoría Shannon cuántica

La teoría clásica de la información se ocupa de la transmisión fiable de información sobre un canal clásico que se modela como una transformación estocástica $W(y|x)$ entre una entrada X y una salida Y. Por transmisión fiable se debe entender el régimen en el que el canal se usa un número arbitrariamente grande de veces, ya que es esta condición la que permite acotar la probabilidad de error al decodificar y probar que, asintóticamente ($n \to \infty$), el error es 0 y por tanto el receptor puede recuperar el mensaje original perfectamente. Es bien conocido [168] que la capacidad clásica de un canal viene dada por el máximo de la información mutua

$$C = \max_{p(x)} I(X;Y) \tag{3}$$

sobre todas las posibles distribuciones de probabilidad de la entrada X. El funcionamiento en régimen asintótico es, aunque conveniente, una idealización y una simplificación matemática. En las últimas dos décadas, no obstante, ha habido avances significativos y profundos en la comprensión de la transmisión de información en bloques de longitud finita [363] y en los límites de capacidad que operan en este caso. Con todo, tanto en el enfoque asintótico como en el finito, la teoría de la información clásica tiene todavía un buen número de problemas abiertos, sobre todo en canales con múltiples transmisores o múltiples receptores.

La extensión de este marco a los canales cuánticos ha deparado varias sorpresas [344, 468, 230]. De entrada, en el caso cuántico existe un recurso que no está presente en el mundo clásico, el posible entrelazamiento de estado entre el emisor y el receptor. Además, sucede que la noción de capacidad no es única, sino que depende del contexto operativo: por ejemplo, si se utiliza un canal clásico o cuántico entre Alice y Bob, o si la comunicación ha de ser privada [191]; y, para cada una de estas definiciones de capacidad, es preciso diferenciar entre la capacidad *one-shot* y la capacidad regularizada. La primera se refiere al caso en que solo se permite al codificador emplear estados separables sobre cada uso del canal, mientras que en el segundo caso el codificador puede generar estados entrelazados sobre usos consecutivos del canal. Obviamente, este segundo supuesto es más general. La Figura 5 esquematiza el marco operativo de la noción de capacidad en canales cuánticos.

La *capacidad* de un canal cuántico como el de la Figura 5 se define de manera operativa, al

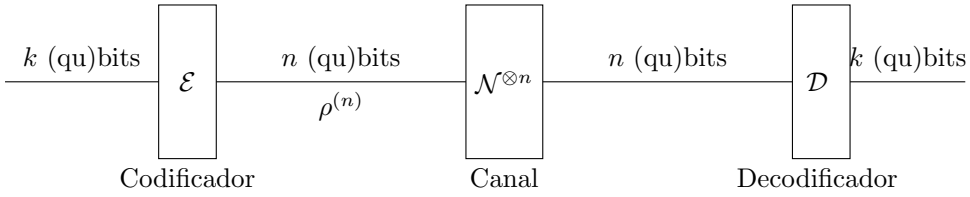


Figura 5: Sistema de comunicaciones cuántico con un emisor y un receptor. El canal $\mathcal{N}$ se usa n veces para transmitir los n (qu)bits codificados por $\mathcal{E}$ que representan los k (qu)bits de un mensaje. El decodificador $\mathcal{D}$ recupera con la mínima probabilidad de error $\varepsilon = 1 - F\big((\mathcal{D}\circ\mathcal{N}^{\otimes n}\circ\mathcal{E})(\rho),\rho\big)$, donde $F(\cdot,\cdot)$ es la medida de fidelidad entre dos estados cuánticos. En el caso *one-shot* los n qubits de $\rho^{(n)} = \rho_1\otimes\cdots\otimes\rho_n$ son separables; en el procedimiento de regularización pueden no serlo.

igual que en el caso clásico. En el régimen asintótico la definición es

$$\lim_{\varepsilon\to 0}\limsup_{n\to\infty}\left\{\frac{k}{n}:\ \text{existen } \mathcal{E},\mathcal{D}:\ \min_{m\in\mathcal{M}} F\Big(|m\rangle,\big(D\circ\mathcal{N}^{\otimes n}\circ\mathcal{E}\big)(|m\rangle)\Big) > 1-\varepsilon\right\},$$

donde la *fidelidad* $F(\rho,\sigma) := \mathrm{tr}(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})$ mide la distinguibilidad de los estados ρ y σ [468, 230]. En lenguaje más simple, la capacidad se define como la máxima tasa de transmisión k/n para la cual existe algún esquema de codificación-decodificación $(\mathcal{E},\mathcal{D})$ con el cual el receptor puede recuperar cualquier mensaje $|m\rangle$ de un conjunto $\mathcal{M}$ con una fidelidad tan grande como desee. Obsérvese que la fidelidad $1-\varepsilon$ se exige a *cualquier mensaje*. Al igual que en teoría de la información clásica, la información es la misma que si solo se impone este requisito en promedio.

Las referencias [230, 210, 475, 305, 301, 177] contienen teoremas de codificación avanzados para la obtención de la capacidad de canales cuánticos en distintos grados de generalidad (con y sin ayuda de entrelazamiento, en canales sin y con memoria, etc.). En todos los casos, la capacidad es una función a optimizar de alguna entropía cuántica, con o sin regularizar, como vamos a ver a continuación.

2.5.1. Capacidad clásica de canales cuánticos

La capacidad clásica de un canal cuántico es la medida de cuántos bits clásicos se pueden transmitir fielmente por un canal cuántico. Si bien a primera vista podría parecer que no hay ninguna ventaja en utilizar un canal cuántico para enviar información clásica ---puesto que no suponemos existencia de ningún estado entrelazado entre el emisor y el receptor---, ocurre que si se usa el canal múltiples veces el mensaje se puede codificar en un estado que sí es entrelazado sobre esos usos del canal, y el receptor puede decodificar con una medida colectiva sobre toda la secuencia. Para muchos ejemplos de canales, se sabe que esta estrategia puede mejorar la capacidad clásica de comunicación.

La expresión de la capacidad clásica de un canal cuántico la da el teorema de codificación de Holevo-Schumacher-Westmoreland (HSW) en términos de la maximización de una cantidad entrópica denominada *información de Holevo*

$$\chi(\mathcal{N}) := \max_{\{(p_x,\sigma_x):x\in\mathcal{X}} \chi\big((p_x,\sigma_x),\mathcal{N}\big),$$

donde

$$\chi\big((p_x,\sigma_x),\mathcal{N}\big) := H\Big(\sum_{x\in\mathcal{X}} p_x\sigma_x\Big) - \sum_{x\in\mathcal{X}} p_x H(\sigma_x)$$

y $H(\cdot)$ es la entropía de von Neumann. Este resultado se refiere al escenario *one-shot* y ha de interpretarse como sigue. Dados un estado clásico-cuántico arbitrario $\sum_{x\in\mathcal{X}} p_x\sigma_x$ definido sobre un alfabeto finito $\mathcal{X}$ que posee una distribución de probabilidad $\{p_x\}$, y un entero $M \leq 2^{n\chi((p_x,\sigma_x),\mathcal{N})}$, es posible elegir una colección $i = 1,\ldots,M$ de palabras de n-qubits separables $\sigma_i = \sigma_{i1}\otimes\cdots\otimes\sigma_{in}$ tales que el receptor puede discriminar perfectamente los M estados $\mathcal{N}^{\otimes n}(\sigma) = \mathcal{N}(\sigma_1)\otimes\cdots\otimes\mathcal{N}(\sigma_n)$. Obsérvese que el codificador está aquí limitado a generar palabras código que son estados separables.

Si se prescinde de esta limitación y se permite entonces que las palabras del código estén compuestas por n qubits en un estado cualquiera (posiblemente entrelazado), entonces cabe ver el codificador como un codificador de bloque sobre el canal extendido $\mathcal{N}^{\otimes n}$, cuya información de Holevo es $\chi(\mathcal{N}^{\otimes n})$. El teorema HSW establece entonces que la capacidad clásica del canal cuántico $\mathcal{N}$ es

$$C(\mathcal{N}) = \lim_{n\to\infty} \frac{\chi(\mathcal{N}^{\otimes n})}{n}. \tag{4}$$

El procedimiento de utilizar codificación en bloque y promediar la información de Holevo se denomina *regularización*. Es posible probar que el límite existe, aunque en general no es computable porque exige una maximización sobre un número de usos del canal no acotado [403]. Para algunos tipos simples de canales, como el depolarizador [8] o el canal con borrado [230] existe una fórmula explícita de $C(\mathcal{N})$.

2.5.2. Capacidad cuántica de canales cuánticos

La capacidad cuántica de un canal cuántico es la máxima tasa de transferencia de qubits entre el emisor y el receptor. De manera análoga al teorema HSW, la capacidad cuántica de un canal viene dada por la regularización de la capacidad *one-shot*, siendo esta la máxima tasa alcanzable cuando el codificador emplea solo estados separables. La capacidad *one-shot* $I_c(\mathcal{N})$ se expresa en términos de la *información coherente* del canal

$$I_c(\mathcal{N}) = \max_{\rho} I_c(\rho,\mathcal{N})$$

donde la maximización tiene lugar sobre todos los estados producto, y la información coherente es (ver Apéndice C)

$$I_c(\mathcal{N}) = \max_{\sigma} H\big(\mathcal{N}(\sigma)\big) - H\Big(\big(\mathcal{N}\otimes\mathbb{1}_{L(\mathcal{X})}\big)\big(\mathrm{vec}(\sqrt{\sigma})\,\mathrm{vec}(\sqrt{\sigma})^\dagger\big)\Big).$$

En general, la información coherente cuantifica la correlación existente tras aplicar el canal $\mathcal{N}$ a una purificación del estado σ. La definición anterior elige $\mathrm{vec}(\sqrt{\sigma})$ como purificación, pero cualquier otra da el mismo valor de información coherente. No es difícil probar que si X e Y son dos registros que corresponden al estado $\big(\mathcal{N}\otimes\mathbb{1}_{L(\mathcal{X})}\big)\big(\mathrm{vec}(\sqrt{\sigma})\,\mathrm{vec}(\sqrt{\sigma})^\dagger\big)$, entonces $I(\mathrm{X}:\mathrm{Y}) = I_c(\sigma;\mathcal{N}) + H(\sigma)$.

Con estos elementos, el teorema de capacidad cuántica de canales ---el teorema LSD--- establece que la capacidad $Q(\mathcal{N})$ es la regularización de la información coherente [295, 124, 411]

$$Q(\mathcal{N}) = \lim_{n\to\infty} \frac{I_c(\mathcal{N}^{\otimes n})}{n}. \tag{5}$$

Tabla 4: Resumen de capacidad de canales clásicos y cuánticos.

	Comunicación clásica	**Comunicación cuántica**
Canal clásico	Información mutua, capacidad Shannon (3)	—
Canal cuántico	Información de Holevo regularizada (4)	Información coherente regularizada (5)
	Propiedades de aditividad	
Canales de capacidad cero	Capacidad cero	*Superactivación*: pueden transmitir información en combinación *Activación causal*: pueden transmitir información combinando varios canales en una trayectoria cuántica
Canales de capacidad no cero	*Aditividad*: n usos de canal transmiten a lo sumo n veces la información que con un solo uso *Superaditividad*: n usos del canal pueden transmitir más información que n veces un solo uso	*Superactivación*: canales combinados en una trayectoria cuántica tienen mayor capacidad que cualquier combinación clásica

Como con la capacidad clásica, es posible probar que el límite existe.

2.5.3. Superaditividad

Un descubrimiento absolutamente sorprendente acerca de la información cuántica es que puede ser *superaditiva*: si un canal cuántico se usa n veces de forma independiente, su información coherente puede superar n veces la capacidad con un solo uso, $I_c(\mathcal{N}^{\otimes n}) > nI_c(\mathcal{N})$ [468, 230]. Vale la pena recordar que esto es imposible con canales clásicos, pues en canales sin memoria se tiene que la información mutua es subaditiva [363], $I(\mathbf{X}^n;\mathbf{Y}^n) \leq \sum_{i=1}^n I(X_i;Y_i)$ con independencia de la correlación que exista entre los símbolos de las palabras del código $\mathbf{X}^n$. Lo mismo ocurre con la capacidad Holevo,

$$\chi(\mathcal{N}^{\otimes n}) > n\chi(\mathcal{N})$$

es posible. Por consiguiente, esta propiedad muestra que la capacidad de los canales cuánticos es de naturaleza diferente a la capacidad Shannon. Por otro lado, mientras que se conocen ejemplos explícitos de superaditividad para la información coherente, la demostración de superaditividad para la información Holevo no es constructiva, y a día de hoy no hay ejemplos explícitos de canales en los que se cumpla. La *conjetura de aditividad* era la proposición $\chi(\mathcal{N}^{\otimes}) = n\chi(\mathcal{N})$, que se ha demostrado falsa. Se cumple para algunas clases de canales, como los de ruptura del

entrelazamiento [410] o el canal depolarizador [247], pero no en general. El primer contraejemplo apareció en [199]. Consiste en dos canales aleatorios conjugados

$$\mathcal{N}(\rho) = \sum_i p_i U_i^\dagger \rho U_i, \quad \overline{\mathcal{N}}(\rho) = \sum_i p_i \overline{U}_i^\dagger \rho \overline{U}_i$$

en los que cada operador de Kraus U_i se toma de una muestra de una distribución determinada y los coeficientes p_i se eligen igualmente al azar de otra distribución concreta, de tal manera que $H_{\min}(\mathcal{N} \otimes \overline{\mathcal{N}}) < 2H_{\min}(\mathcal{N})$ cuando se usa un estado entrelazado como entrada al canal compuesto $\mathcal{N} \otimes \overline{\mathcal{N}}$. Una consecuencia de este resultado es que no existe una fórmula cerrada (*single-letter*) general para la capacidad clásica de los canales cuánticos. También implica que codificar la información en un estado entrelazado incrementa la capacidad clásica del canal, aunque no sabemos en qué cantidad.

En cuanto a la información cuántica, se ha probado que es aditiva en canales degradables [124], de modo que para estos la fórmula de capacidad es single-letter

$$Q(\mathcal{N}_{\text{degradable}}) = \chi(\mathcal{N}_{\text{degradable}}).$$

Pero esto no se cumple en canales como el de depolarización. Para este caso, es posible calcular que el estado que maximiza la información Holevo es el de entrelazamiento máximo $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, y que con él $I_c(\mathcal{N}) = \max\{0, 1 - h(q) - q\log 3\}$, siendo q la probabilidad de error en el canal y $h(q) := -q\log q - (1-q)\log(1-q)$ la función de entropía binaria. Esta expresión se anula para $q \approx 0{,}1893$. Como por otro lado se sabe que $C(\mathcal{N}) = 0$ cuando $q \geq 1/4$, se concluye que si $q < 1/4$ la información coherente *one-shot* o sin regularizar no basta para caracterizar la capacidad del canal. Se sabe también que un simple código de repetición $(3,1)$ es suficiente para obtener la capacidad [255].

La discusión anterior se focaliza en la información coherente y la información Holevo, con lo que se circunscribe únicamente a las capacidades *one-shot*. Las capacidades clásica y cuántica regularizadas de un canal también son superaditivas, pero este hecho no es consecuencia directa de la regularización. Al contrario, puesto que se han definido como un límite, es claro que $C(\mathcal{N}^{\otimes n}) = nC(\mathcal{N})$ y $Q(\mathcal{N}^{\otimes n}) = nQ(\mathcal{N})$. En otras palabras, si se usan n canales idénticos de forma independiente o en paralelo, la capacidad clásica o cuántica es aditiva. Por lo tanto, la superaditividad tiene que provenir del uso de canales diferentes. Para el caso de la capacidad clásica, se sabe que $C(\mathcal{N} \otimes \mathcal{M}) \geq C(\mathcal{N}) + C(\mathcal{M})$, ya que basta con utilizar códigos óptimos en cada canal para conseguir la igualdad. Pero demostrar la desigualdad estricta es aún un problema abierto, nadie ha hallado aún un código mejor que el producto de dos códigos óptimos. Es conveniente enfatizar que la superaditividad de la información de Holevo no implica la superaditividad de la capacidad clásica. Para la capacidad cuántica, la situación se comprende mucho mejor. La condición de superaditividad $Q(\mathcal{N} \otimes \mathcal{M}) > Q(\mathcal{N}) + Q(\mathcal{M})$ es posible [260] incluso en casos en los que $Q(\mathcal{N}) = Q(\mathcal{M}) = 0$. Este fenómeno se conoce como *superactivación* y se discute a continuación.

2.5.4. Superactivación

Otro de los fenómenos profundamente anti-intuitivos que emanan del entrelazamiento cuántico es el de *superactivación*, la posibilidad de combinar dos canales de capacidad cuántica cero en una forma tal que la capacidad cuántica del canal resultante no es cero. Por razones que se

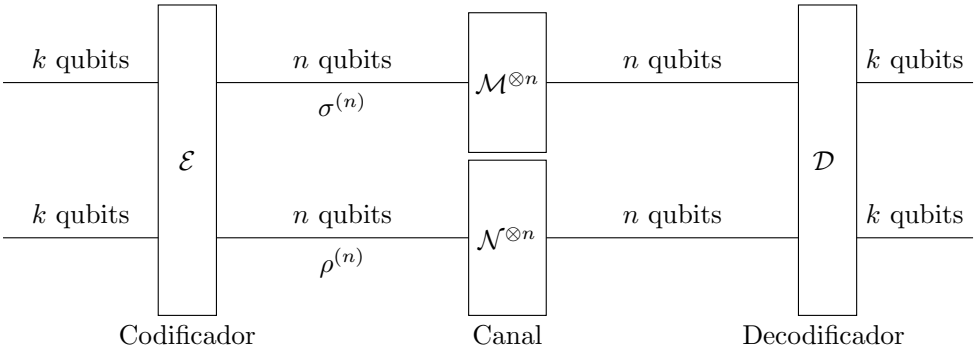


Figura 6: Esquema conceptual del fenómeno de la superactivación. El codificador conjunto $\mathscr{E}$ crea estados entrelazados que el decodificador $\mathscr{D}$ mide colectivamente.

explican más adelante, la superactivación no es posible para la capacidad clásica [422, 212] y, con canales cuánticos, solo es factible si ninguno de ellos puede simular al otro.

Al menos dos clases de canales cuánticos tienen capacidad cero (no se conoce todavía qué otras clases existen). Una es la de canales *antidegradables*. Estos son los canales cuyo entorno (su canal complementario) puede simular el canal original, es decir, $\mathscr{N} = \Psi \circ \mathscr{N}^c$. Esta propiedad permitiría copiar los qubits recibidos simplemente aplicándoles el canal Ψ, lo que constituye una violación del teorema de no clonación. Por consiguiente, la capacidad de los canales antidegradables es cero. Un ejemplo sencillo es el canal de dos qubits con borrado $\mathscr{N}(\rho) = \frac{1}{2}\rho + \frac{1}{2}|e\rangle\langle e|$, donde $|e\rangle$ es el estado de borrado. La segunda clase de canales con capacidad cero es la de canales PPT, aquellos cuya representación de Choi es PPT. Como se sabe, los estados (canales) separables son PPT, pero además los estados PPT no sirven para generar a partir de ellos ningún estado entrelazado. Por ese motivo, si un canal es PPT, lo serán también sus estados de salida, y a partir de ellos resulta imposible generar o recuperar ningún entrelazamiento entre el emisor y el receptor, incluso si se usa el canal un número ilimitado de veces. Un ejemplo particular de este tipo de canales es el canal de Horodecki de dimensión 4, con representación de Kraus

$$\sqrt{\frac{q}{2}}\mathbb{1}\otimes|0\rangle\langle 0|, \quad \sqrt{\frac{q}{2}}\mathsf{Z}\otimes|1\rangle\langle 1|, \quad \sqrt{\frac{q}{4}}\mathsf{Z}\otimes\mathsf{Y},$$
$$\sqrt{\frac{q}{4}}\mathbb{1}\otimes\mathsf{X}, \quad \sqrt{1-q}\mathsf{X}\otimes M_0, \quad \sqrt{1-q}\mathsf{Y}\otimes M_1,$$

donde

$$M_0 = \begin{pmatrix} \frac{1}{2}\sqrt{2+\sqrt{2}} & 0 \\ 0 & \frac{1}{2}\sqrt{2-\sqrt{2}} \end{pmatrix}, \quad M_1 = \begin{pmatrix} \frac{1}{2}\sqrt{2-\sqrt{2}} & 0 \\ 0 & \frac{1}{2}\sqrt{2+\sqrt{2}} \end{pmatrix}$$

con $\{\mathbb{1}, \mathsf{X}, \mathsf{Y}, \mathsf{Z}\}$ los operadores de Pauli.

Para que se dé el fenómeno de superactivación deben cumplirse varias condiciones. Si uno de los canales es clásico, la superactivación no es posible [44], la capacidad cuántica no aumenta. [422] muestra que la superactivación sí es posible cuando uno de los canales cuánticos es simétrico, y el mismo trabajo simplifica este resultado significativamente al probar que la combinación de un canal Horodecki de dimensión 4, $\mathscr{M}$, con un canal con borrado $1/2$, $\mathscr{N}$, cumple

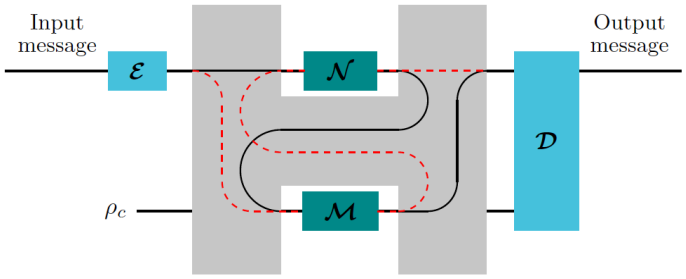


Figura 7: Activación causal con un switch cuántico. La figura aparece en [255] originalmente.

$Q(\mathcal{N}\otimes\mathcal{M}) \geq I_c(\rho,\mathcal{N}\otimes\mathcal{N}) > 0{,}1$ para un estado de entrada particular cuya expresión exacta puede consultarse en [422]. La desigualdad equivale a afirmar que la capacidad cuántica no es convexa. El canal compuesto $\mathcal{N}\times\mathcal{M}$ no es ni antidegradable ni PPT, pues su capacidad no es nula. Una forma de interpretar esta conclusión es afirmar que la simetría del canal con borrado se rompe de alguna forma como consecuencia de la información que se fuga por el canal de Horodecki.

Aún más sorprendente resulta el hecho de que esta no sea la única forma posible de superactivación. La combinación convexa

$$p\mathcal{M}\otimes|0\rangle\langle 0| + (1-p)\mathcal{N}\otimes|1\rangle\langle 1|,$$

esto es, el uso con probabilidad p de uno de los dos canales junto con el qubit auxiliar $|0\rangle$ o $|1\rangle$. Cabe entonces probar que, para determinados estados de entrada ρ y cierto rango de valores de p, la información coherente de esta canal compuesto no es nula, aun cuando la de sus canales constituyentes sí lo es. O lo que es igual, la capacidad de comunicación cuántica depende del contexto en que se usa un canal y de qué otros canales estén disponibles.

2.5.5. Activación causal

En la teoría de la información cuántica, aunque los elementos que portan la información obedecen las leyes de la mecánica cuántica, la manera en que estos objetos se propagan sigue siendo clásica, en tanto que sigue una trayectoria que o bien está fijada de antemano, o bien se decide a priori de forma probabilista. Algunos trabajos recientes han propuesto generalizar esta situación imaginando que no solo los canales o la información son cuánticos, sino que la propia posición de los canales es cuántica. Esto quiere decir que la trayectoria que sigue un qubit ---los canales que lo procesan--- se trata con el formalismo cuántico y está sujeta igualmente al principio de superposición [95, 260].

El ejemplo prominente de esta idea es el *switch cuántico*[5] representado en la Figura 7. Este dispositivo se comporta como la combinación $\mathcal{N}\circ\mathcal{M}$ si el qubit de control es $|0\rangle$ o bien como $\mathcal{M}\circ\mathcal{N}$ cuando el qubit de control es $|1\rangle$, de tal manera que el orden secuencial de los canales se decide en función del estado del qubit de control ρ_c. Este qubit de control está predeterminado de antemano (de modo que no transmite información alguna, no es un canal colateral) y es fundamental que pueda ser medido por el receptor, tal como indica la figura. Naturalmente, puede

[5] No confundir con los repetidores cuánticos ni con los switches cuánticos de los que se tratará más adelante.

estar en un estado superpuesto, lo que implica que los dos canales están en una configuración coherente superpuesta en cuanto al orden.

Este ingenioso dispositivo teórico ha demostrado tener mayor capacidad que el uso causal de los dos canales de que se compone, en cualquier orden. En concreto, cuando se usan dos canales depolarizadores para $\mathscr{M}$ y $\mathscr{N}$ (cuya información de Holevo es cero y no pueden transmitir información clásica), el switch cuántico tiene en cambio capacidad clásica no nula [142], si bien el valor numérico es pequeño. Es importante en este punto recordar que la información de Holevo es una cota inferior a la capacidad regularizada, que por lo tanto también será no nula.

En lo que concierne a la capacidad cuántica, existen asimismo canales cuánticos $\mathscr{M}$ y $\mathscr{N}$ de capacidad cero que, usados en el switch cuántico, dan lugar a una capacidad cuántica no nula. Un buen ejemplo ilustrativo de este hecho es el canal de ruptura de entrelazamiento

$$\mathscr{N}(\rho) = \frac{1}{2}(X\rho X + Y\rho Y)$$

con X e Y los operadores de Pauli, como de costumbre, el cual tiene capacidad cuántica $Q(\mathscr{N}) = 0$ porque es antidegradable. Ahora bien, un cálculo directo muestra que la salida del swicth cuántico es en este caso

$$\frac{1}{2}\rho \otimes |+\rangle\langle +|_c + \frac{1}{2} Z\rho Z |-\rangle\langle -|_c,$$

una combinación convexa de una canal ideal y un canal de inversión, ambos entonces de capacidad 1 qubit, por lo que la capacidad del sistema es 1.

La activación causal abre así una vía de exploración novedosa para formas de comunicación no conocidas hasta la fecha. En comparación con la teoría de la información clásica, es conveniente señalar que los resultados de activación causal significan que se violan en el ámbito cuántico las cotas *cut-set* (de corte, o de cuello de botella, como también se conocen) que rigen en el mundo clásico: allí, para una combinación causal de canales dispuestos en serie, la capacidad no puede ser mayor que cualquiera de las capacidades individuales. Una vez más, la teoría cuántica contradice lo que creemos saber.

2.5.6. Problemas abiertos

La superactivación todavía no se comprende bien científicamente, y muchas de las preguntas que suscita no tienen aún respuesta. Sobre todo, importa averiguar si existen otras clases de canales con capacidad cero además de los antidegradables y los PPT. En especial, no se sabe si la superactivación se cumple para otros canales Horodecki que no tengan capacidad privada positiva, o si existen otros pares de canales más allá del canal puro de borrado y el Horodecki de dimensión 4 que exhiban el efecto. Fuera del caso de canales discretos, hay un amplio terreno de investigación por explorar en sistemas continuos [469]. Se ha descubierto, por ejemplo, que la superactivación puede darse en un amplio conjunto de canales de atenuación térmica [389], aun si el ruido térmico es elevado [291]. Que la superactivación pueda ocurrir en condiciones útiles dentro de canales cuánticos gaussianos sería un avance crucial para futuros sistemas de comunicaciones basados en las propiedades cuánticas de la luz [421].

Por cuanto a la superaditividad se refiere, se ha probado para canales que podrían ser relevantes en aplicaciones realistas. Por ejemplo, en un cierto régimen de uso del canal depolarizador, o también para la información coherente en el canal *dephasure*, que es una concatenación de un canal con borrado y un canal de supresión de fase. El canal de borrado puede verse como

un canal bosónico sobre un sistema *dual-rail* de qubits, que resulta ser un modelo adecuado de las fibras ópticas. Asimismo, se ha descubierto un fenómeno de superaditividad fuerte en canales con capacidad casi-cero, en concreto en un canal *quantum rocket*. Este es un canal con $2\log d$ qubits de entrada y capacidad privada menor que 2, combinado con un canal puro con borrado en d dimensiones, que tienen capacidad privada cero. Esta combinación alcanza una capacidad de $\frac{1}{2}\log d$, sin embargo [420], notablemente mayor que la capacidad del primer canal. En abierto contraste con este estado del arte, se ignoran ejemplos concretos y prácticos de superaditividad con la capacidad Holevo, lo que deja margen de investigación sobre la posible utilidad de la superactivación para la transmisión de información clásica sobre un canal cuántico. Otras áreas en las que hay solo trabajo incipiente y muchas cuestiones abiertas son las diferencias de capacidad cuando se aplica codificación clásica más decodificación cuántica frente al caso de utilizar codificación cuántica más decodificación clásica. Las propias cuestiones de codificación-decodificación invitan a examinar esquemas de codificación de longitud finita [103] y a comparar las estrategias de decodificación basadas en medida colectiva y LOCC versus la discriminación de estados producto [242]. Pero tal vez el punto clave de esta área sea que la caracterización de la capacidad de modelos de canal realistas ---aquellos que modelan sistemas prácticos y realizables de comunicaciones cuánticas--- es por ahora muy incompleta y no bien comprendida. A modo de ejemplo, la capacidad del canal generalizado de atenuación de fase sigue sin estar bien explicada en la literatura científica [240]. La importancia de esta canal radica en que es una versión análoga para qubits del canal bosónico con ruido térmico, y en que modela algunas de las fuentes de error en computadores de circuitos cuánticos basados en superconductores. En el camino hacia ese objetivo, se han obtenido una serie de cotas superiores para la capacidad clásica de canales cuánticos [464, 157, 158, 40]. Cotas superiores similares para la capacidad cuántica se pueden encontrar en [476, 419, 434, 444], entre otros.

2.6. Sistemas físicos para entrelazamiento bipartito y multipartito

La información cuántica se representa por medio de qubits lógicos, que no son más que una superposición de dos estados puros, $a|0\rangle + b|1\rangle$. En las operaciones de comunicación o de computación cuántica, estos qubits lógicos se han de convertir en un estado físico que corresponda al estado del qubit lógico, en un proceso que llamamos *codificación*. En general, la forma más simple de manipular las propiedades cuánticas de un sistema físico para operar con qubits es hacerlo con luz (fotones).

Existen varios grados de libertad que se pueden aprovechar para codificar información cuántica en la luz. Cada uno tiene sus ventajas y retos particulares. En este apartado revisaremos algunos de los modos de *codificación fotónica* de la información, cuyo resumen se recoge en la Tabla 5.

Se dispone de varias formas de clasificar las codificaciones fotónicas. Una de ellas es simplemente la cardinalidad del espacio de Hilbert. El espacio de estados de la *codificación de variable discreta* (DV) está generado por un número finito de estados ortogonales (más en general, estados linealmente independientes), mientras que la *codificación de variable continua* (CV) o *codificación bosónica* tiene un espacio de estados generado por una colección de estados infinita, posiblemente numerable. Los estados pueden ser ortogonales o, en un caso general, solo linealmente independientes. Sin embargo, la línea divisoria entre ambos tipos de codificación no siempre es clara: los sistemas DV pueden ser interpretados como subespacios finitos de los espacios CV, y nuestro interés en los sistemas CV reside sobre todo en identificar en ellos los

Tabla 5: Descripción de varios sistemas de codificación fotónica con sus implementaciones asociadas de puertas cuánticas.

	Codificaciones single-rail			Codificaciones dual-rail		
	Estado de Fock	**Coherente/gato**	**GKP**	**Time-bin**	**Trayecto**	**Polarización**
Cardinalidad	DV	CV	CV	DV	DV	DV
Base física	Vacío, fotón único	Estados coherentes $\|\pm\alpha\rangle$	GKP-0 y GKP-1	Modos temporales ortogonales	Modos espaciales ortogonales	Polarizaciones ortogonales
Entrelazamiento	Determinista	Determinista	Determinista	Probabilista	Probabilista	Probabilista
Puertas Clifford single-mode	Probabilist	Probabilista	Determinista (*squeezing*)	Determinista	Determinista	Determinista
Puertas no-Clifford single-mode	Probabilista	Probabilista	Probabilista	Determinista	Determinista	Determinista
Uso	Espacio libre	Espacio libre	Espacio libre	Comunicaciones	Tx. fibra óptica	Espacio libre

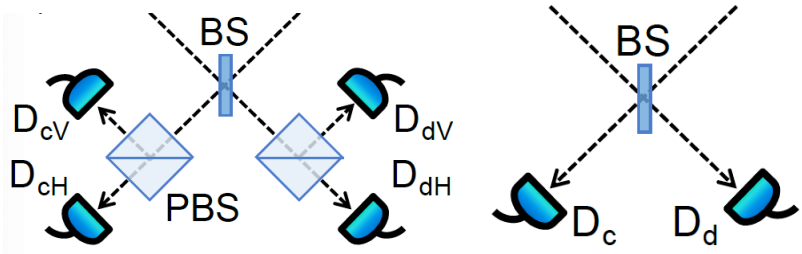


Figura 8: Ejemplos de implementación de una medida de Bell. Imagen original de [21].

subespacios de dos estados (qubits). Además, en la práctica, las imperfecciones e interacciones con el entorno tienen el efecto de aumentar la dimensión efectiva de los sistemas DV.

Otra caracterización posible de las codificaciones fotónicas es según el número de ``raíles'' (*rails*). En su acepción más restrictiva, un qubit *single-rail* se asocia con la presencia o ausencia de un único fotón en un modo óptico (temporal o espacial). De manera más laxa, cabe entender las codificaciones *single-rail* como aquellas en las que cada estado ---incluidos los de múltiples fotones--- ocupa un modo óptico. Por contra, un qubit con codificación *dual-rail* se define por la presencia de un fotón en uno de dos modos ortogonales. Para codificaciones *single-rail* es posible generar entrelazamiento de forma determinista con dispositivos ópticos lineales, en tanto que las operaciones ópticas lineales necesarias para generar entrelazamiento en sistemas *dual-rail* son probabilistas. En cambio, las rotaciones de un solo qubit en ciertos sistemas *single-rail* pueden necesitar no linealidad (porque la codificación podría estar basada en una superposición de estados con un número distinto de fotones, o sea, autoestados de energía), pero existen codificaciones *dual-rail* en las que son posibles rotaciones arbitrarias sobre un solo qubit utilizando tan solo elementos ópticos lineales [252].

Los siguientes esquemas de codificación fotónica se han considerado con frecuencia en la implementación o experimentación de protocolos de información cuántica. Son bien conocidos, en general:

1. Intervalos de tiempo (*time-bin*): un fotón sigue uno de dos caminos posibles de longitud

diferente en un interferómetro. El qubit $|0\rangle$ se asocia con uno de los caminos y $|1\rangle$ con el otro. Esta forma de codificación es idónea para la transmisión por fibra óptica, ya que no le afecta la birrefringencia de las fibras. Sin embargo, es difícil hacer que interactúen dos qubits *time-bin*, lo que implica que es un esquema más adecuado para comunicación que para computación cuántica.

2. Polarización: un tipo de codificación *dual-rail* en la que un qubit se convierte en los estados de polarización de un solo fotón. El convenio es que $|0\rangle$ se asocia con un fotón con polarización horizontal y $|1\rangle$ con la polarización vertical. Todas las puertas cuánticas de un único qubit se puede realizar en forma determinista con placas de onda (*waveplates*) y desplazadores de fase (PS, *Phase Shifters*), pero las puertas óptico-lineales para generar entrelazamiento tienen un funcionamiento probabilista, y requieren divisores de haz (BS, *beamsplitters*), placas de onda, medidas y post-selección. A modo de ejemplo de las operaciones con dos qubits, la Figura 8 representa el proceso de medida de Bell (BSM, *Bell State Mearuement*). El panel izquierdo representa la BSM para estados fotónicos polarizados horizontal y verticalmente $|H\rangle$ y $|V\rangle$. Esto se implementa aplicando un BS 50:50 a los modos ópticos, seguido de un BS de polarización (PS) en cada uno de los dos modos de salida y un contador de fotones a la salida de estos. Detección en los dispositivos D_{cH} y D_{cV} o en D_{dH} y D_{dV} proyectan el par de qubits recibido en el estado de Bell $|\Phi^+\rangle = (|H\rangle|V\rangle + |V\rangle|H\rangle)/\sqrt{2}$, y análogamente detección en los dispositivos D_{cH} y D_{dV} o en D_{cV} y D_{dH} proyectan los qubits del par recibido en el estado de Bell $|\Psi^-\rangle = (|H\rangle|V\rangle - |V\rangle|H\rangle)/\sqrt{2}$. Véase que esta medida de Bell solo funciona cuando los dos pulsos ópticos de entrada tienen 2 o más fotones en total. El panel de la derecha ilustra el proceso físico de BSM para fotones con codificación en estados de Fock, generados por el estado vacío $|0\rangle$ y el estado de un solo fotón $|1\rangle$. El proceso se implementa aplicando un BS 50:50 a los modos ópticos, seguido por un contador de fotones sobre los modos de salida. La activación del detector D_c (respectivamente, D_d) en el modo de interferencia constructiva (resp., destructiva) proyecta el par de qubits recibidos en el estado de Bell $|\Phi^+\rangle = (|0\rangle|1\rangle + |1\rangle|0\rangle)/\sqrt{2}$. Ambas implementaciones solo pueden distinguir $|\Psi^\pm\rangle$ de otros estados y las probabilidades de éxito son $1/2$ aun en el caso ideal.

   Este tipo de codificación es preferible en transmisión en espacio libre más que sobre fibra óptica, puesto que es vulnerable a la birrefringencia de la fibra.

3. Trayecto (*Path*): los estados base computacionales se asocian con modos espaciales ortogonales. Todas las puertas cuánticas de un qubit se pueden realizar de forma determinista con BS y PS. Como con la codificación por polarización, las puertas que generan entrelazamiento mediante elementos ópticos lineales son probabilistas, y deben utilizar BS, PS, medidas y post-selección. Y como en la codificación por intervalo de tiempo, la codificación por trayecto es más apta para la transmisión por fibra que por espacio libre.

4. Fock: el valor de un qubit se codifica en el subespacio de Hilbert generado por el estado vacío $|0\rangle$ y el estado de un solo fotón $|1\rangle$, correspondientes a un qubit *single-rail*. Por medio de un PS, es posible rotar su vector de Bloch alrededor del eje Z libremente, pero no sobre el eje X, pues los estados $|0\rangle$ y $|1\rangle$ tienen diferente energía. Por otro lado, un estado de Bell como $|\Psi^\pm\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$) se puede conseguir de modo determinista con un único fotón incidente en un BS 50:50. Sin embargo, solo se puede discriminar los estados de Bell $|\Psi^\pm\rangle$ de los otros con un BS 50:50 seguido de dos detectores-contadores de fotones (Figura 8).

Esta clase de codificación es sensible a las derivas de fase en un canal de transmisión, razón por la que es preferible usarla en espacio libre antes que en transmisión por fibra.

5. Coherente/gato: un qubit se codifica en el subespacio de Hilbert generado por los estados coherentes $|\alpha\rangle$ y $|-\alpha\rangle$ con $\alpha > 0$, lo que corresponde a un sistema qubit *single-rail*. Los estados base del qubit $|\pm\rangle$ se asocian con los estados gato (*cat*) $(|\alpha\rangle \pm |-\alpha\rangle)/(2\sqrt{p_\pm})$ donde $p_\pm := (1 \pm \langle -\alpha|\alpha\rangle)/\sqrt{2}$. Los estados $|\pm\rangle$ se pueden intercambiar con un cambiador de fase (PS) π, y se pueden distinguir mediante un detector-contador del número de fotones. Este tipo de codificación también se ve afectada por la deriva de fase en el canal de transmisión, luego es más indicada para transmisión por espacio libre que para transmisión por fibra.

6. GKP (Gottesman-Kitaev-Preskill): la base computacional son las superposiciones coherentes de infinitas auto-funciones equiespaciadas (o sea, infinitos estados *squeezed*)

$$|0_{\text{GKP}}\rangle = \sum_{n=-\infty}^{\infty} |q\rangle = 2n\sqrt{\pi}\rangle,$$
$$|1_{\text{GKP}}\rangle = \sum_{n=-\infty}^{\infty} |q\rangle = (2n+1)\sqrt{\pi}\rangle$$

donde $|q\rangle = n\sqrt{\pi}\rangle$ es el auto-estado correspondiente al autovalor $n\sqrt{\pi}$ del operador de posición q. En las implementaciones realistas, estos estados de infinita energía (no realizables) se sustituyen por sus versiones normalizadas. Todas las puertas Clifford de un qubit (respectivamente, de varios qubits), incluidas las puertas generadoras de entrelazamiento, se pueden realizar de forma determinista usando operaciones gaussianas de *single-mode* (resp., multimodo). Las puertas no-Clifford se implementan con ayuda de estados ancilares y teleportación, es decir, están condicionados únicamente en forma determinista por la disponibilidad de los estados ancilares.

3. Comunicación y redes cuánticas

Como punto de partida, la comunicación cuántica puede describirse bajo dos objetivos diferenciados, la mejora de la comunicación de información clásica mediante un canal cuántico, siendo su ejemplo más exitoso la distribución de claves cuánticas; o bien, la distribución extremo-a-extremo de estados cuánticos para su utilización en computación cuántica o metrología/medición cuántica. En cualquier caso, y al margen de sus objetivos, el elemento central es la transmisión de qubits que, en el caso de QKD son un elemento auxiliar, mientras que, en la transferencia de estados cuánticos, el recurso transferido es el estado cuántico en sí mismo. A pesar de ello, el diseño de canales de comunicación cuántica extremo a extremo es una problemática común a los dos propósitos descritos, utilizándose los términos Redes de comunicación cuántica, Redes de información cuántica y, como veremos en el apartado 4, la Internet Cuántica.

De acuerdo a [318] la comunicación cuántica se puede resumir como sigue: "nonlocality is the goal, teleportation is the heart, decoherence is the reality, and the speed of light is still the constraint", donde el entrelazamiento cuántico proporciona la no localidad y la teleportación es el método primario de transferencia de información cuántica; sin embargo, la realidad de los errores causados por el ruido, la imperfección de las operaciones, etc. conlleva algún grado de decoherencia que se mide con una estimación de fidelidad entre el estado cuántico deseado y

el real. Por último, a pesar de la no localidad del entrelazamiento, lo que permitiría una comunicación más rápida que la velocidad de la luz, el uso de la teleportación, y su vinculación a la comunicación tradicional, para el envío efectivo de información cuántica, limita la velocidad a la de la comunicación clásica. A este respecto, y hoy, el término comunicación cuántica no debe ser considerado un sustituto de la comunicación digital tradicional, sino que se sustenta en ella [123].

En esta sección se revisan las primitivas que dan soporte a las comunicaciones cuánticas, en lo que se refiere al intercambio de información cuántica, así como la fidelidad y la gestión de errores en dicho intercambio. En concreto tres son los fenómenos físicos en que se apoya la comunicación cuántica: (1) el entrelazamiento, ya revisado en el apartado anterior (bi-partito o multi-partido), como recurso elemental de comunicación (apartado 3.1); (2) la teleportación, como mecanismo de transmisión de información cuántica entre nodos vinculados por entrelazamiento (apartado 3.2); y (3) el intercambio de entrelazamiento, como mecanismo para extender la comunicación basada en entrelazamiento a una conexión extremo a extremo (apartado 3.3). El entrelazamiento y el intercambio de entrelazamiento tienen su materialización en el concepto de repetidor cuántico (apartado 3.4), definiendo la conectividad cuántica que persiste al margen de la conectividad física, tal y como se resume en el apartado 3.5. Tras estas bases de la mecánica cuántica para comunicación, en el apartado 4 se describen los elementos de la futura Internet Cuántica, para en 5 revisar las distintas propuesta arquitectónicas al respecto.

3.1. Entrelazamiento como recurso de comunicaciones

Como ya se ha mencionado, el entrelazamiento cuántico es una forma de correlación entre sistemas inexistente y *diferente* de cualquier tipo de correlación clásica. Esta naturaleza distintiva y única se concreta en las *desigualdades de Bell* [37], un conjunto de restricciones acerca de los resultados de las mediciones estadísticas realizables sobre el sistema completo que cualquier forma de correlación clásica ha de satisfacer necesariamente. La formulación más frecuente de estas condiciones se conoce como desigualdades CHSH (Clauser-Horne-Shimony-Holt). Pues bien, un sistema con entrelazamiento puede violar las desigualdades de Bell. Aunque inicialmente esta observación solo tuvo un valor teórico, hacia finales del s. xx las aplicaciones y posibilidades del fenómeno del entrelazamiento comenzaron a entenderse con claridad.

- Se han ideado protocolos de comunicaciones para la distribución cuántica de claves (QKD) basados en las propiedades de sistemas entrelazados [146, 360]. Los protocolos QKD proporcionan seguridad física perfecta (en el sentido de la teoría de la información), así que superan a cualquier esquema clásico de seguridad criptográfica, ya que estos se basan en hipótesis computacionales.
- El entrelazamiento puede usarse para incrementar la capacidad de un canal clásico de comunicaciones. La transmisión de dos bits clásicos de información sobre un canal clásico o sobre un canal cuántico (codificando el par de bits de alguna forma en un qubit) requiere por fuerza dos usos del canal. Pero si el emisor y el receptor comparten previamente un estado entrelazado, con la *codificación superdensa* [468, 42] dos bits de información pueden enviarse con un solo uso del canal. Más aún, esta forma de comunicación es intrínsecamente segura.
- Un qubit no puede transmitirse por un canal clásico, porque estos no preservan la coherencia cuántica. En cambio, un qubit en un estado no conocido de antemano ---incluso

para el emisor--- se puede transmitir a un receptor usando dos bits clásicos y un estado entrelazado previo compartido entre las partes. El protocolo de *teleportación cuántica* se describe en mayor detalle en el apartado 4. Es un resultado dual del de codificación superdensa, y ambos desafían las nociones clásicas de la comunicación de información. Una de sus implicaciones es que un estado de entrelazamiento máximo y un canal cuántico sin ruido son completamente equivalentes desde un punto de vista operacional, siempre que supongamos que la comunicación de los dos bits clásicos no tiene coste alguno.

- La transmisión de un qubit no requiere de la interacción directa de Alice y Bob. Si ambos comparten un qubit entrelazado con un intermediario, independientemente, y este realiza una medida de Bell sobre ellos, eventualmente los qubits de Alice y Bob alcanzan un estado de máximo entrelazamiento. Es evidente que esta forma de *intercambio de entrelazamiento* permite la propagación del entrelazamiento a lo largo de una ruta, y por ello resulta clave en el desarrollo de los repetidores cuánticos y de la Internet cuántica (véase también el apartado 4).
- Dada la dificultad de construir y mantener estables sistemas cuánticos de muchos qubits, el procesamiento distribuido de información cuántica emerge como solución prometedora. Una tarea de computación sobre un número elevado de qubits se puede resolver, en principio, usando múltiples QPUs de tamaño pequeño o medio interconectadas por una colección de canales cuánticos, i.e., una red de comunicaciones cuántica. En vez de acometer la solución a un problema computacional realizando una transformación (algoritmo) sobre los estados cuánticos de un sistema monolítico, en la versión distribuida cada una de los QPUs comparten un estado cuántico entrelazado global y llevan a cabo operaciones *locales* solo sobre su propio subsistema, más pequeño. Las transformaciones de estado no locales sobre el estado global tienen lugar combinando esas transformaciones locales en cada nodo por medio de comunicación cuántica y/o clásica. Es apropiado mencionar en este punto que la comunicación clásica no basta para generar o manipular un entrelazamiento arbitrario entre varias partes, pero que la comunicación cuántica ideal (sin ruido) se puede simular con el protocolo de *teleportación cuántica* si dos dispositivos comparten inicialmente un estado bipartito entralazado máximo.

En resumen, el entrelazamiento cuántico tiene variados usos como *recurso de comunicaciones* dentro del paradigma LOCC entre dispositivos QPU para la función de realizar transformaciones no locales de estados sobre sistemas cuánticos separados.

3.2. Teleportación cuántica

La teleportación cuántica es un procedimiento para transmitir información cuántica sin la transferencia física efectiva de la partícula que almacena el qubit, mediante la utilización de dos recursos en paralelo, un par entrelazado entre origen y destino y un par de bits clásicos. Por tanto, la teleportación requiere tanto un enlace clásico como un enlace cuántico. La teleportación implica la destrucción del qubit original a ser transmitido (el que codifica la información) y el elemento fuente del EPR (como consecuencia de la medición necesaria para el envío de los bits). La información puede ser reconstruida en el elemento destino del EPR gracias al par de bits, limitando la velocidad a la velocidad de la luz. Tal y como se recoge en las Figuras 9 y 10, la teleportación recae en la estricta vinculación de operaciones y comunicaciones cuánticas y clásicas.

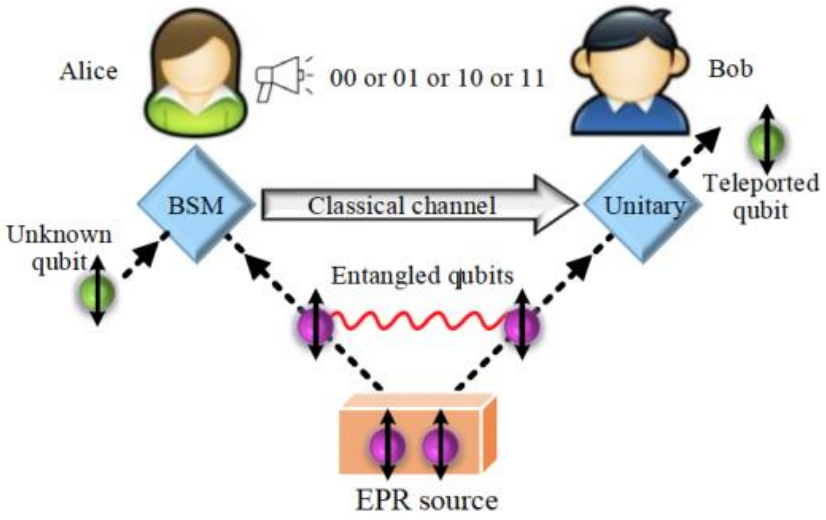


Figura 9: Concepto de teleportación. Figura extraída de [287].

Para la teleportación cuántica de Alice a Bob, los elementos del sistema se resumen a continuación. El elemento fuente de la información cuántica (Alice) utiliza un transmisor que procesa el mensaje cuántico $\Phi\rangle$ para producir una señal a transmitir por un canal clásico. El elemento destino (Bob) utiliza un receptor que realiza la operación inversa al transmisor. La conversión de la información cuántica en información clásica se basa en un subsistema de generación y distribución de entrelazamiento cuántico. Sobre este subsistema, el transmisor realiza un preprocesado cuántico, por ejemplo, BSM, para obtener un mensaje a ser trasmitido por el canal clásico. En sentido opuesto el receptor reconstruye la información cuántica a partir de la información clásica recibida; esto es, recuperar el qubit original a partir de su receptor EPR con las operaciones cuánticas que determinan los bits en el mensaje clásico.

En concreto, se trata de un protocolo gracias al cual Alice (A) transmite a Bob (B) dos bits clásicos que son suficientes para que Bob prepare localmente un estado cuántico idéntico a un estado cuántico $|\psi\rangle_A$ de Alice, que previamente desconoce. El protocolo no depende del estado $|\psi\rangle$. Para lograr este objetivo aparentemente imposible, Alice y Bob precisan un estado compartido con entrelazamiento máximo antes de iniciar las operaciones. El protocolo de teleportación tiene estos pasos:

1. Alice y Bob poseen inicialmente un estado de Bell compartido $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$ y sendos registros cuánticos, el de Alice en el estado $|\psi\rangle_A = \alpha|0\rangle_A + \beta|1\rangle_A$ (un qubit) y el de Bob vacío. El estado de Alice es totalmente arbitrario y no tiene por qué ser conocido ni por Alice ni por Bob.

2. Alice realiza una medida de Bell sobre sus dos qubits, $|\psi\rangle_A$ y la parte A' del qubit entrelazado que comparte con Bob. La medida no es más que una proyección sobre los estados

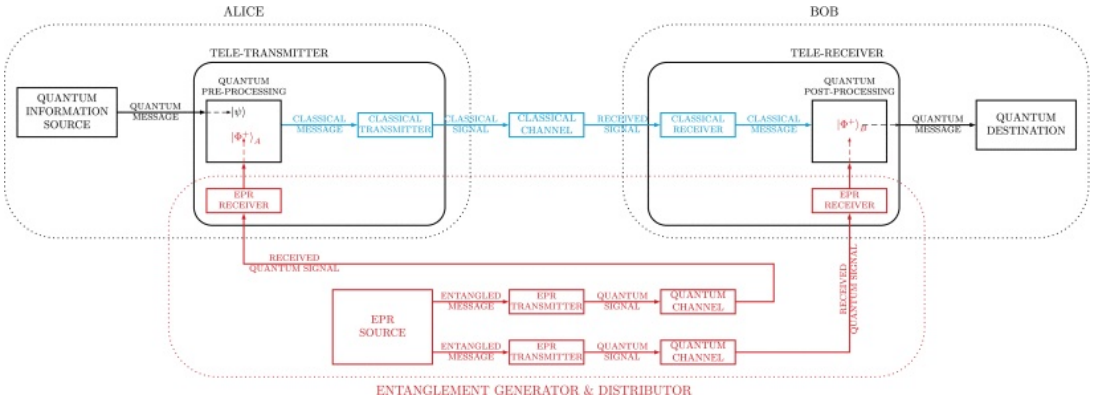


Figura 10: Modelo de sistema de comunicación para teleportación cuántica. Extraída de [75].

de Bell ---que son una base ortonormal--- por lo que el estado de los tres qubits es

$$|\psi\rangle_A \otimes |\Phi\rangle = \frac{1}{2}\left(|\Phi^+\rangle \otimes |\psi\rangle_B + |\Phi^-\rangle \otimes \mathsf{Z}|\psi\rangle_B + |\Psi^+\rangle \otimes \mathsf{X}|\psi\rangle_B + |\Psi^-\rangle \otimes \mathsf{XZ}|\psi\rangle_B\right).$$

El resultado de la medida es el par de bits clásicos (x,z) con probabilidad $1/4$ y el estado del qubit compartido de Bob tras la medida es $\mathsf{X}^x\mathsf{Z}^z|\psi\rangle_B$.

3. Alice transmite a Bob el par de bits (x,z) por un canal clásico.
4. Bob realiza la medida $\mathsf{Z}^z\mathsf{X}^x$ sobre su qubit y obtiene $|\psi\rangle_B$ en su registro local.

La Figura 11 resume estos pasos en forma de un circuito cuántico totalmente equivalente al protocolo descrito. Así por tanto, la medida local que efectúa Alice sobre el qubit entrelazado induce un cambio aleatorio en la parte de ese qubit que tiene Bob. Ese cambio deja el qubit de Bob en el mismo estado $|\psi\rangle$ que el de Alice, salvo por una rotación cuyo valor depende del resultado de la medida. Bob solo necesita, así, conocer el valor de dicha medida (dos bits) para recuperar $|\psi\rangle$. Obsérvese que, aunque Bob dispone ya del estado justo tras la medida de Bell que hace Alice, no sabe todavía cuál de las puertas de Pauli tiene que aplicar para extraer correctamente el estado, lo que quiere decir que la teleportación cuántica no consiste en transmitir información cuántica de forma instantánea. La comunicación clásica de los dos bits es esencial en el protocolo e implica que la teleportación cuántica no viola el absoluto de la velocidad de la luz. Esta imposibilidad de llevar a término un proceso de comunicación más rápido que la velocidad de la luz aun con ayuda de entrelazamiento cuántico se conoce como el *principio de no señalización* [141]. Para las versiones generales de la teleportación cuántica con qubits y en sistemas de variable continua, que también existen, véanse las referencias [468, 230, 472, 64].

En síntesis, la teleportación cuántica hace posible enviar cualquier cantidad de información cuántica empleando un ebit (preexistente entre las partes) y dos bits clásicos por cada qubit que se quiera transferir. Esto es lo mismo que afirmar que distribuir ebits de forma eficiente sobre una red de comunicaciones cuánticas es el problema tecnológico fundamental que hay que resolver.

Este modelo es válido bajo la suposición simplificadora de no decoherencia, pero en la práctica hay imperfecciones realistas que no pueden ser obviadas: la exposición del canal cuántico

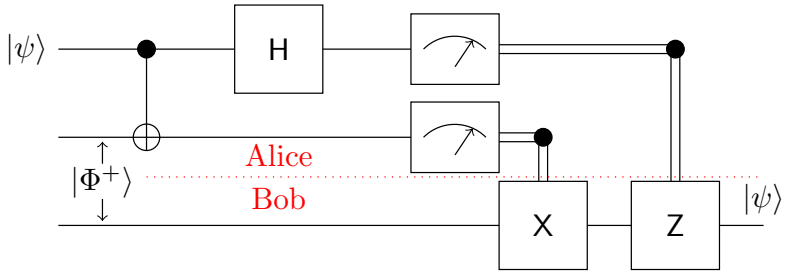


Figura 11: Circuito cuántico para la teleportación del qubit $|\psi\rangle$.

puede producir la decoherencia del qubit a ser teleportado y también del estado entrelazado que da soporte a dicha teleportación; asimismo se deben tener en cuenta las imperfecciones de las operaciones cuánticas en el sistema propuesto. Además, a las imperfecciones que afectan a la decoherencia cuántica, se une el ruido en el canal clásico necesario para la teleportación. Sin entrar en la formulación del problema y en los experimentos realizados, en [75] se revela la naturaleza multiplicativa de las imperfecciones cuánticas, así como su naturaleza asimétrica, esto es, la imperfección afecta de forma distinta a las distintas componentes de los estados cuánticos. Estas imperfecciones pueden ser corregidas con técnicas ya mencionadas como QEC (Quantum Error Correction), DFS (Decoherence-free subspace), DD (Dynamic coupling), purificación de entrelazamiento. Por último y aun aplicando cualquier de las técnicas de mejora de coherencia anteriores, la distribución del entrelazamiento decae exponencialmente con las distancias entre emisor y receptor, equivalente cuántico a la atenuación, pero aplicado al recurso básico de comunicación, lo que puede ser solventado con el uso de repetidores cuánticos que permitan extender el entrelazamiento cuántico a varios saltos aumentando su distancia operativa.

3.3. Intercambio de entrelazamiento

Para la ideación de una red de comunicaciones cuánticas, la teleportación, como mecanismo básico de comunicación, se debe complementar con, al menos, dos elementos adicionales que permiten aumentar la distancia a la que tal teleportación es factible, el intercambio de entrelazamiento (Figura 12), y las memorias cuánticas. El intercambio de entrelazamientos es una operación LOCC para extender efectivamente la distancia de entrelazamiento mediante un nodo intermedio que comparte estados entrelazados con los dos extremos de la comunicacíón (para el caso más simple de dos saltos)

Cabe entender el intercambio de entrelazamiento como una extensión de la teleportación en la que las partes Alice y Bob tienen cada una un estado entrelazado de dos qubits con un intermediario C (Charlie), los estados $|\Phi^+\rangle_{AC_1}$ y $|\Phi^+\rangle_{BC_2}$, respectivamente. Cuando Charlie realiza una medida de Bell sobre ellos, los qubits de Alice y Bob transitan ambos a uno de los estados de Bell dependiendo del resultado de la medida.

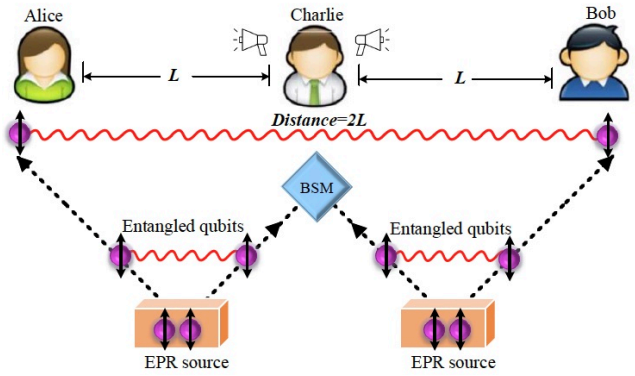


Figura 12: Esquema conceptual del intercambio de entrelazamiento.Figura extraída de [287].

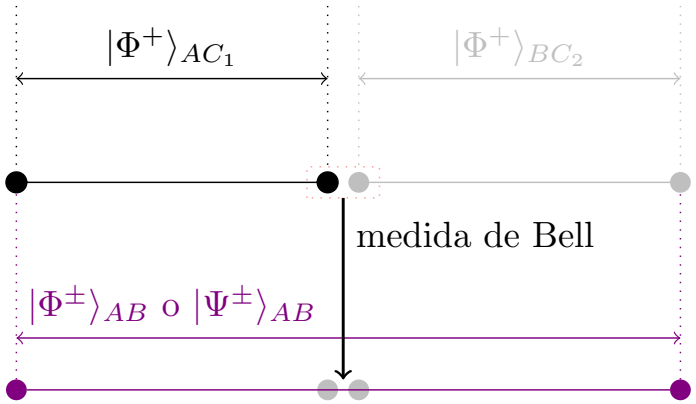


Figura 13: Esquema operativo del intercambio de entrelazamiento.

De modo específico

$$
\begin{aligned}
|\Phi^+\rangle_{C_1C_2} &\longrightarrow |\Phi^+\rangle_{AB} \\
|\Phi^-\rangle_{C_1C_2} &\longrightarrow |\Phi^-\rangle_{AB} = Z_B|\Phi^+\rangle_{AB} \\
|\Psi^+\rangle_{C_1C_2} &\longrightarrow |\Psi^+\rangle_{AB} = X_B|\Phi^+\rangle_{AB} \\
|\Psi^-\rangle_{C_1C_2} &\longrightarrow |\Psi^-\rangle_{AB} = Z_BX_B|\Phi^+\rangle_{AB}.
\end{aligned}
\tag{6}
$$

Por lo tanto, aunque Alice y Bob no interactúan directamente, han conseguido establecer un estado de entrelazamiento máximo entre ellos, como se representa gráficamente en la Figura 13. Otra manera equivalente de verlo es como la transformación de dos pares de qubits independientes $|\Phi^+\rangle_{AC_1}$ y $|\Phi^+\rangle_{BC_2}$ en un qubit entrelazado $|\Phi^\pm\rangle_{AB}$ o $|\Psi^\pm\rangle_{AB}$. La conclusión inmediata es que el entrelazamiento se puede propagar con ayuda de un tercero y, por lo tanto, puede ser distribuido a través de una red de comunicaciones. Vamos a ver a continuación las bases físicas y tecnológicas de estos dispositivos intermedios, los repetidores cuánticos.

Tabla 6: Probabilidad de éxito y fidelidad de varios protocolos de purificación de entrelazamiento.

Protocolo	Estados de entrada	Prob. éxito	Fidelidad
[122]	Estados de Bell	$(F_1+F_2)^2+(F_3+F_4)^2$	$\frac{F^2+F_2^2}{(F+F_2)^2+(F+F_4)^2}$
[122]	Binario	$F^2+(1-F)^2$	$\frac{F^2}{F^2+(1-F)^2}$
[65]	Werner	$\left(F+\frac{1-F}{3}\right)^2+\left(\frac{2(1-F)}{3}\right)^2$	$\frac{F^2+\frac{1}{9}(1-F)^2}{F^2+\frac{2}{3}F(1-F)+\frac{5}{9}(1-F)^2}$

Fidelidad del intercambio de entrelazamiento El protocolo de destilación o purificación de entrelazamiento propuesto en [46] (de IBM) parte de estados de Werner $\omega=\lambda|\Psi^-\rangle\langle\Psi^-|+\frac{1-\lambda}{4}\mathbb{1}$ cuya fidelidad inicial es de $F_0=\frac{3\lambda+1}{4}$ (el parámetro λ está en el intervalo $[-1/3,1]$). Suponiendo que $F_0\geq 1/2$ ($\lambda\geq 1/3$), tras una ronda de funcionamiento se obtienen nuevos estados con una fidelidad [89]

$$f(F_0,\eta,p_2)=\frac{\left(F_0^2+\left(\frac{1-F_0}{3}\right)^2\right)\left(\eta^2+(1-\eta)^2\right)+\left(F_0\frac{1-F_0}{3}+\left(\frac{1-F_0}{3}\right)^2\right)(2\eta(1-\eta))+\frac{1-p_2^2}{8p_2^2}}{\underbrace{\left(F_0^2+\frac{2}{3}F_0(1-F_0)+\frac{5}{9}(1-F_0)^2\right)\left(\eta^2+(1-\eta)^2\right)+\left(F_0\frac{1-F_0}{3}+\left(\frac{1-F_0}{3}\right)^2\right)(8\eta(1-\eta))+\frac{1-p_2^2}{2p_2^2}}_{g(F_0,\eta,p_2)}}, \tag{7}$$

donde p_2 denota la fidelidad de una puerta de dos qubits y η denota la fidelidad en la medida de la operación de intercambio de entrelazamiento. La fidelidad tras i rondas de destilación se puede calcular de forma recurrente con $F_i=f(F_{i-1},\eta,p_2)$. Pero este proceso de purificación no es determinista, y solo tiene éxito con probabilidad

$$p_s(F)=p_2^2 g(F_0,\eta,p_2).$$

Si en cada QR se ejecutan n_d rondas de purificación, la tasa de generación de entrelazamiento en un enlace será

$$R_L(R_0,n_d,L,F_0)=\frac{R_0 e^{-\frac{L}{L_{\text{att}}}}}{\prod_{i=1}^{n_d}\frac{2}{p_s(F_i)}}.$$

En esta expresión R_0 denota la tasa inicial de generación de estados entrelazados y L es la separación entre repetidores. El numerador contabiliza las pérdidas por atenuación, mientras que el denominador tiene en cuenta las rondas de purificación y su tasa de éxito. Tras las operaciones locales de destilación en cada enlace, se efectúan n intercambios de entrelazamiento que afectan a la fidelidad extremo a extremo, cuya expresión viene dada por

$$F_{e,0}(F,n)=\frac{1}{4}+\frac{3}{4}\left(\frac{p_2(4\eta^2-1)}{3}\right)^{n-1}\left(\frac{4F-1}{3}\right)^n.$$

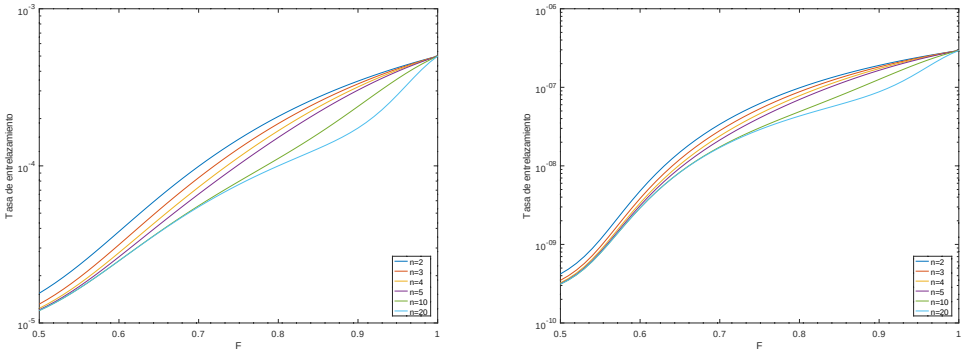


Figura 14: Ejemplos numéricos de la tasa de generación de entrelazamiento en una ruta de n repetidores cuánticos, en función de la fidelidad inicial F. Los parámetros son: $R_0 = 1$, $p = \eta = 0{,}95$, $L = L_{\mathtt{att}} = 21{,}7$ km, $n_d = n_e = 5$ (izquierda), $n_d = n_e = 10$ (derecha).

Este valor es la fidelidad inicial con la que comienza una última fase de destilación entre los extremos formada por n_e rondas. Tomando todos los factores en consideración, la tasa final de generación de entrelazamiento se calcularía como

$$R_E(R_0, n_e, n_d, L, F) = \frac{R_L(R_0, n_d, L, F_0)}{\prod_{j=1}^{n_e} \frac{2}{p_s(F_{e,j})}}.$$

La figura 14 presenta un par de casos numéricos para este modelo analítico, en donde se puede ver que la tasa de generación de entrelazamiento no es demasiado sensible a la longitud de la ruta pero sí al número de rondas de purificación en cada enlace. Es evidente que conviene partir de un estado inicial de entrelazamiento máximo.

3.4. Repetidores cuánticos

Al igual que los repetidores en la Internet clásica, que pueden ser considerados amplificadores de la señal de comunicación en una forma de restablecimiento de la energía/potencia, los repetidores cuánticos deberían asegurar la energía de las "señales cuánticas" para una transmisión estable, y garantizar que el qubit transportado no cambia [494]. El protocolo básico de teleportación hace posible transferir un estado cuántico arbitrario (y desconocido) entre dos puntos siempre y cuando estos compartan previamente un estado de Bell (un ebit). Adicionalmente, se han de enviar dos bits clásicos. Así pues, el problema fundamental para implementar este protocolo es el de generar y distribuir pares de Bell a Alice y Bob. Para este fin, el modo preferido en los laboratorios y en los ensayos consiste en utilizar fotones transmitidos por espacio libre o fibra óptica. Sin embargo, la transmisión por fibra óptica tiene una transmitancia η que decae exponencialmente con la longitud según $\eta = \mathrm{e}^{-L/L_{\mathtt{att}}}$, donde $L_{\mathtt{att}} \approx 21{,}7$ km para las fibras comerciales en uso en los sistemas de telecomunicación actuales. La transmitancia mide la ratio entre los fotones transmitidos y los recibidos, luego con el valor citado decae en un factor 10 cada 50 km aproximadamente. También en los sistemas continuos como el canal bosónico la transmitancia se comporta como $C(\eta) = -\log(1-\eta) \approx \eta$ si $\eta \ll 1$ [357]. Esa ate-

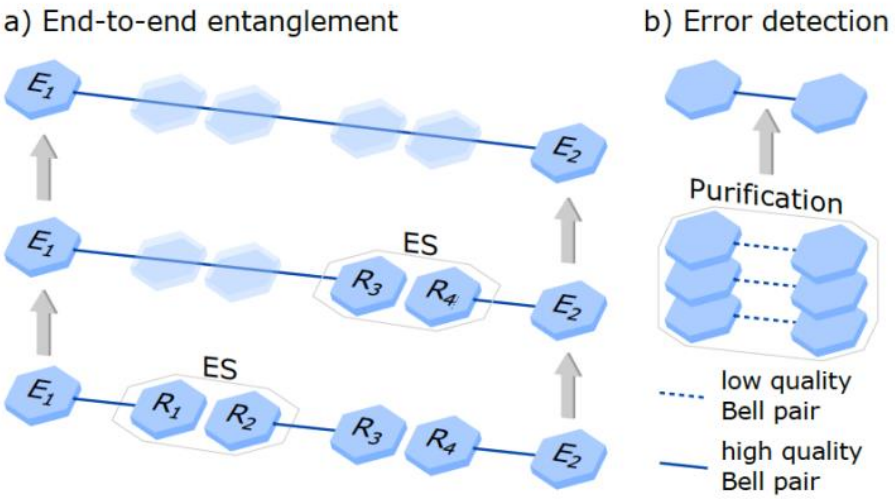


Figura 15: Distribución de entrelazamiento extremo a extremo: intercambio de entrelazamiento y purificación. Extraída de [318].

nuación exponencial significa, evidentemente, que la comunicación directa de pares de Bell por una fibra óptica no es eficiente a grandes distancias, ya que las pérdidas de fotones en la fibra enseguida son muy elevadas.

Una solución a este problema pasa por utilizar alguna forma de *repetidor cuántico* (QR, *quantum repeater*) basado, por ejemplo, en el intercambio de entrelazamiento. Recordemos que los qubits no se pueden clonar (regenerar) ni amplificar como en las comunicaciones clásicas, en virtud del teorema de no-clonación, de modo que un dispositivo como un repetidor es esencialmente cuántico, por fuerza. Con un QR se puede dividir el trayecto entre Alice y Bob en segmentos más cortos, con menos pérdidas, para que la generación de pares entrelazados en cada segmento sea más eficiente.

Los QRs habilitan la distribución de entrelazamiento extremo a extremo, lo que permite su uso por parte de las aplicaciones, tal y como se representa en la Figura 15, donde el intercambio de solapamiento extiende el entrelazamiento a múltiples saltos, y la corrección de errores se basa, por ejemplo, en la purificación, donde se reduce un conjunto de pares de baja calidad para producir pares de calidad superior (ver apartado 3.6). Estos repetidores cuánticos, de acuerdo a la definición en [318], incluyen la siguiente funcionalidad: (1) creación del entrelazamiento base, normalmente, produciendo pares de Bell; (2) extensión de entrelazamiento mediante el intercambio de entrelazamiento; (3) gestión de Errores (estados y puertas); y (4) otras operaciones relacionadas con la gestión de la red cuántica (recogidas en el apartado 5).

3.4.1. Repetidor ideal

En este apartado describiremos un protocolo sencillo que utiliza intercambio de entrelazamiento para propagar pares de Bell a lo largo de una concatenación de enlaces. Es, básicamente, una aplicación directa del mecanismo de intercambio descrito más arriba, sin más elaboración. Se supondrá además que el resto de los elementos del sistema funcionan sin error (circuitos,

medidas, canales sin errores), y que por tanto la única fuente de ineficiencia es la atenuación de la fibra con la distancia. Por esa razón, el tratamiento de esta sección se ciñe al caso de un QR ideal.

Imaginemos que se dispone de una memoria cuántica M en la que se puede almacenar un estado de Bell $|\Phi^+\rangle_{Xx} = \frac{1}{\sqrt{2}}\left(|0\rangle_X|H\rangle_x + |1\rangle_X|V\rangle_x\right)$ mediante un pulso óptico x ---un fotón con polarización horizontal o vertical---. En esta notación, $\{|0\rangle_X, |1\rangle_X\}$ es la base computacional del elemento de memoria cuántica. Supóngase además que un estado arbitrario $a|0\rangle + b|1\rangle$ de esa memoria se puede convertir en el estado de polarización $a|H\rangle + b|V\rangle$ de un qubit. Este tipo de memoria es una versión idealizada de un registro de memoria cuántico, y se puede implementar con dos conjuntos atómicos [396]. También se puede usar una BSM para qubits con codificación por polarización como la mostrada en la Figura 8 (izda.), y que opera como una medida de Bell probabilista. Con estos preliminares, es posible generar un estado de Bell entre Alice y Bob, separados por una distancia L_x, combinando la memoria cuántica M, la medida de Bell y fibra óptica para la transmisión. Para ello, Alice y Bob generan sendos estados de Bell $|\Phi^+\rangle_{Ax}$ e $|\Phi^+\rangle_{By}$ entre sus registros de memoria M_A, M_B y un pulso óptico x (y) localmente, y a continuación envían el fotón x (y) a un punto de medida situado en medio sobre una fibra óptica. El modelo de comportamiento de la fibra óptica es el de un canal bosónico puro en pérdidas. Cuando el elemento intermedio recibe los pulsos, lleva a cabo una medida BSM óptico-lineal sobre ellos. Esta medida tiene éxito solo si ambos fotones han llegado al nodo intermedio sin haber desaparecido por causa de las pérdidas en la fibra, y los fotones que alcanzan el detector se proyectan sobre un estado de Bell $|\Psi^+\rangle_{xy}$ o $|\Psi^-\rangle_{xy}$, lo que ocurre con probabilidad $p_g(L_x/2) = \frac{1}{2}\mathrm{e}^{-L_x/(2L_{\mathrm{att}})}$. Este evento, si ocurre, entrelaza las memorias cuánticas M_A y M_B en los estados $|\Psi^{\pm}\rangle_{AB}$ de acuerdo con las ecuaciones (6). Este es, por tanto, un protocolo de generación de entrelazamiento.

Si Alice y Bob no hubiesen utilizado el repetidor intermedio, estarían separados por una distancia L_x y el número medio de intentos que necesitarían para establecer el entrelazamiento sería de $p_g^{-1}(L_x) = 2\mathrm{e}^{L_x/L_{\mathrm{att}}}$, que aumenta exponencialmente con la distancia. En cambio, con el repetidor intermedio, el número medio de intentos decrece hasta $p_g^{-1}(L_x/2) = 2\mathrm{e}^{L_x/(2L_{\mathrm{att}})}$, porque gracias a los registros de memoria cada uno de los eventos (la creación de un par de Bell con Alice o con Bob) puede retenerse en su correspondiente memoria. Una vez que ambos ocurren, una señal clásica basta para indicar al repetidor que active el intercambio de entrelazamiento convirtiendo el contenido de las memorias en qubits polarizados y realizando una BSM con el procedimiento de la Figura 8, mediante dispositivos de óptica lineal. El resultado no es más que el intercambio de entrelazamiento tal como se describió, y brinda como salida un estado de Bell entre Alice y Bob con probabilidad $p_s = 1/2$ la de la medida de Bell, en el caso ideal. Así pues, el número medio de intentos necesarios para que el proceso completo de intercambio de entrelazamiento tenga éxito es p_s^{-1}. Si el protocolo falla, Alice y Bob comienzan una nueva ronda desde el principio a partir del proceso de generación de pares de Bell. Finalmente, el número medio de intentos para completar todo el protocolo con éxito es de $2p_s^{-1}\mathrm{e}^{L_x/(2L_{\mathrm{att}})}$ [21, 396]. Es obvio que la presencia del QR ofrece una mejora cuadrática de la probabilidad de éxito sobre la generación directa de entrelazamiento.

Por descontado, el proceso se puede iterar varias veces y ejecutar en paralelo, con ganancias de eficiencia aún mayores. En la Figura 16 se ilustra un ejemplo con tres repetidores equiespaciados. Como la longitud de cada segmento es $L_x/4$, la probabilidad global de éxito en la generación es de $p_s^{-2}\mathrm{e}^{L_x/(4L_{\mathrm{att}})}$. En general, con $2^k - 1$ repetidores intermedios se tendría una probabilidad de éxito de $p_s^{-k}\mathrm{e}^{L/(2^k L_{\mathrm{att}})}$, que también muestra claramente la mejora exponencial con el número de repetidores cuánticos empleados. Como además la probabilidad de éxito en una BSM, p_s, es

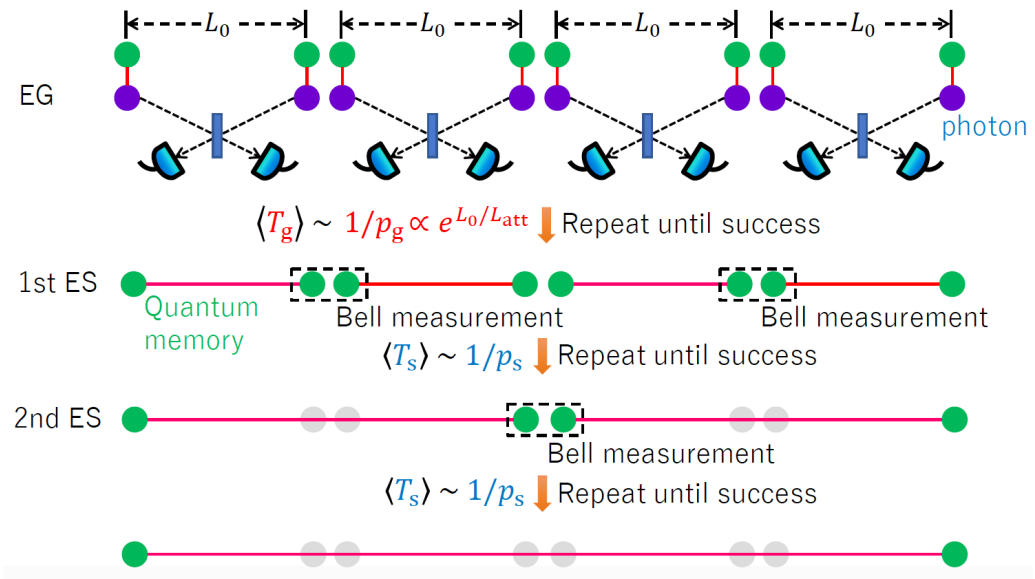


Figura 16: Ejemplo operacional de un protocolo de intercambio de entrelazamiento para la distribución de estados entrelazados con repetidores cuánticos. La figura es original de [21].

independiente de la distancia, el uso de QR sirve para compensar por completo la caída exponencial con la distancia de las pérdidas por atenuación en la fibra.

El protocolo que se acaba de presentar es uno de los primeros en aparecer y se propuso hace ya algún tiempo [134], se lo conoce como protocolo DLCZ. Forma parte de los llamados protocolos QR de primera generación [66, 21], que se examinan en detalle más adelante.

3.4.2. Intercambio vs. conmutación de entrelazamiento

Aunque en el estado del arte la mayor parte de las aproximaciones pasan por una red cuántica basada en intercambio de entrelazamiento y repetidores cuánticos, es preciso hacer una distinción operativa y terminológica entre un repetidor cuántico y un *conmutador cuántico* (QS, *quantum switch*). Los dos tipos de dispositivos se basan en el intercambio de entrelazamiento ---esto es, en la creación de estados entrelazados entre los nodos que están conectados mediante un enlace de comunicaciones al QR o al QS---, pero mientras que el QR es un dispositivo que une dos enlaces (lógicos) en una configuración lineal o en serie, un QS se supone equipado con una lógica interna de procesamiento que le permite crear entrelazamiento entre cualquiera de los k usuarios conectados a él, incluyendo entrelazamiento multi-partito entre $k \geq 2$ usuarios. Un QS, por consiguiente, tiene una topología lógica en estrella. Otra diferencia en la arquitectura entre un QR y un QS es que los switches necesitan en principio estar equipados con memorias cuánticas en número suficiente para atender a todos los enlaces, idealmente un número arbitrariamente grande de memorias cuánticas con un tiempo de persistencia infinito.

Para describir el funcionamiento de un QS podemos imaginar que cada uno de los usuarios establece continuamente pares de Bell con alguno de los registros de memoria del QS, quien los almacena una vez generados. Tan pronto como el QS reúna m de estos pares de Bell con

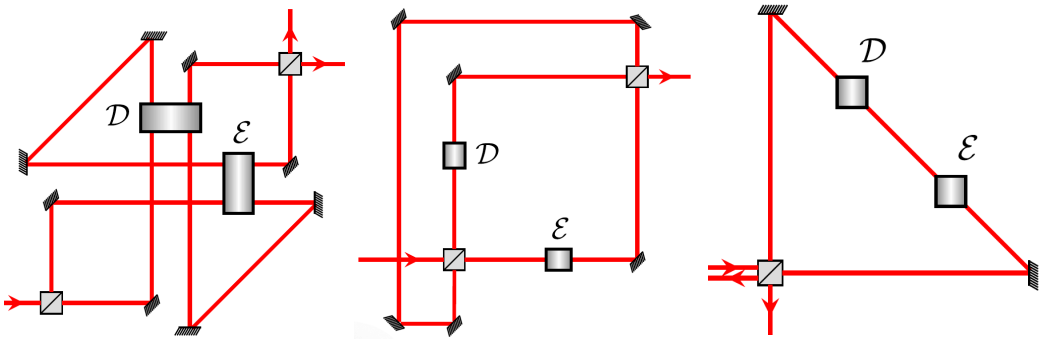


Figura 17: Ejemplos de posible *quantum SWITCH*. (izquierda) implementación con geometría Mach-Zender. El qubit de entrada se codifica en la polarización del fotón y el qubit de control decide entre los trayectos $\mathscr{E} \to \mathscr{D}$ y $\mathscr{D} \to \mathscr{E}$ tras el *beamsplitter*; (centro) una implementación con el qubit codificado en el grado de libertad del fotón. La función del qubit de control la lleva a cabo la polarización del qubit; (derecha) una implementación vía geometría Sagnac. El qubit de entrada se codifica en la polarización del fotón y un BS aplica la superposición de los órdenes causales de $\mathscr{E}$ y $\mathscr{D}$. Esta figura es de [79].

entrelazamiento máximo en m enlaces diferentes, genera mediante intercambio de entrelazamiento un estado GHZ m-partito entrelazado compartido por los m usuarios de esos enlaces. Cualquier conjunto de m usuarios podría estar interesado en compartir (distribuir) un estado entrelazado de esa forma, sin ninguna restricción. Es más, si existiesen combinaciones de usuarios para los que no interesase generar estados entrelazados por alguna razón, esta condición reduciría necesariamente la tasa a la que el QS puede generar entrelazamiento, es decir, reduce su capacidad. Por lo tanto, salvo por consideraciones de carácter tecnológico, no hay razón para limitar los subconjuntos de enlaces de entrada para los que un QS debe ser capaz de generar entrelazamiento.

El QS que se acaba de definir es, pues, un dispositivo para crear estados entrelazados entre cualesquiera de sus enlaces de entrada (dos o más), con una configuración arbitraria, apoyándose en un protocolo de señalización posiblemente y en un cierto número de unidades de memoria cuántica. Obviando por el momento las bases físicas del proceso, cabe ver un QS como un elemento que transfiere estados cuánticos entre cualquiera de sus enlaces entrantes y uno o más enlaces de salida, lo que resulta completamente análogo a un conmutador electrónico salvo porque en esos últimos los bits se pueden copiar hacia diferentes destinos, y en un conmutador cuántico no.

El término *quantum SWITCH* lo reservaremos para el dispositivo propuesto en [97]. Se trata de un dispositivo que implementa *trayectos cuánticos*, es decir, una combinación de canales cuánticos entre su entrada y su salida que no está predeterminada, sino que es el resultado de uno o más qubits de control. Un *quantum SWITCH*, así, establece un orden de procesamiento de los qubits que no se conoce previamente, aunque los pasos de procesamiento internos sí sean conocidos. De manera equivalente, un *quantum SWITCH* es un conmutador que opera sobre qubits y está internamente en un estado de superposición cuántica entre diferentes configuraciones. La Figura 17 da una idea esquemática de posibles realizaciones de un dispositivo de esta clase.

3.5. Conectividad cuántica

El uso del entrelazamiento como recurso de comunicación y el intercambio de entrelazamiento como mecanismo de distribución supone un cambio fundamental en la definición de conectividad en el mundo cuántico. A este respecto, se considera clarificadora la perspectiva de red proporcionada en [219], que se recoge a continuación. Mientras en las redes clásicas existe un único concepto de conectividad, que es la conectividad física ---existencia de un enlace de comunicación entre dos nodos que se dicen conectados; en el mundo cuántico además de un enlace cuántico, que implicaría la conexión física, la teleportación permite la transmisión de un qubit sin la necesidad de un enlace físico cuántico. De esta forma que, el entrelazamiento define enlaces cuánticos virtuales, dando lugar al concepto de conectividad virtual. De forma más detallada, si bien la conectividad física debe existir para la generación de entrelazamiento entre dos nodos, posteriormente, los dos nodos estarán virtualmente conectados sin la necesidad de conexión física, si bien esta conexión virtual se ve limitada por el proceso de decoherencia. Esta limitación temporal debe ser subsanada mediante la generación de nuevos entrelazamientos que permitan mantener la conectividad virtual. En otras palabras, la teleportación, esto es la transmisión de qubits, no requiere la existencia sincronizada de un enlace cuántico siempre y cuando el estado entrelazado haya sido creado previamente. La política de creación de los estados entrelazados esto es la creación proactiva o reactiva y al vuelo, en función de las necesidades específicas, es un aspecto que estará relacionado con la gestión de recursos en las redes cuánticas. Por otro lado, el intercambio de entrelazamiento permite la materialización de estados entrelazados a más de un salto, generalizando el concepto de conectividad virtual en un grafo de conectividad aumentada que elimina la necesidad de conectividad física cuántica entre dos nodos para la teleportación. Por último, y si no se limita la operativa de red al entrelazamiento bipartito, se puede conceptualizar una conectividad bajo demanda mediante el entrelazamiento multi-partito. Con el entrelazamiento bipartito y el intercambio de entrelazamiento tenemos una canal de comunicación unicast semidúplex. Por el contrario, la integración en el grafo virtual y aumentado del entrelazamiento multi-partito, permite un canal multicast y bajo demanda, en función de la selección de los nodos de la red entre los que se crean los pares EPR. Esta visión en [219] se representa la Figura 18.

3.6. Comunicación en canales cuánticos ruidosos

Desafortunadamente la comunicación cuántica tiene lugar en canales ruidosos y es necesario arbitrar técnicas que garanticen el intercambio de información cuántica sin errores aun en presencia de ruido. Dado la imposibilidad de clonación y/o amplificación de la información cuántica, su protección frente a ruido pasa por (1) la generación y mantenimiento de entrelazamiento de alta fidelidad vía purificación o (2) la corrección cuántica de errores vía codificación en un espacio de *Hilbert* de mayor dimensión, esto es, introduciendo una forma cuántica de redundancia.

En el caso de la comunicación cuántica basada en teleportación, es necesario garantizar un par entrelazado máximo entre los dos extremos; sin embargo, la presencia de ruido resulta en la pérdida de la maximalidad y la reducción de la fidelidad del qubit en la teleportación. La purificación del entrelazamiento permite solventar esta situación mediante el proceso de manipulación de estados entrelazados no máximos (el estado es conocido en teleportación) para obtener estados entrelazados con mayor fidelidad referida al entrelazamiento máximo. La teleportación unida a la purificación de entrelazamiento teóricamente habilita un esquema de

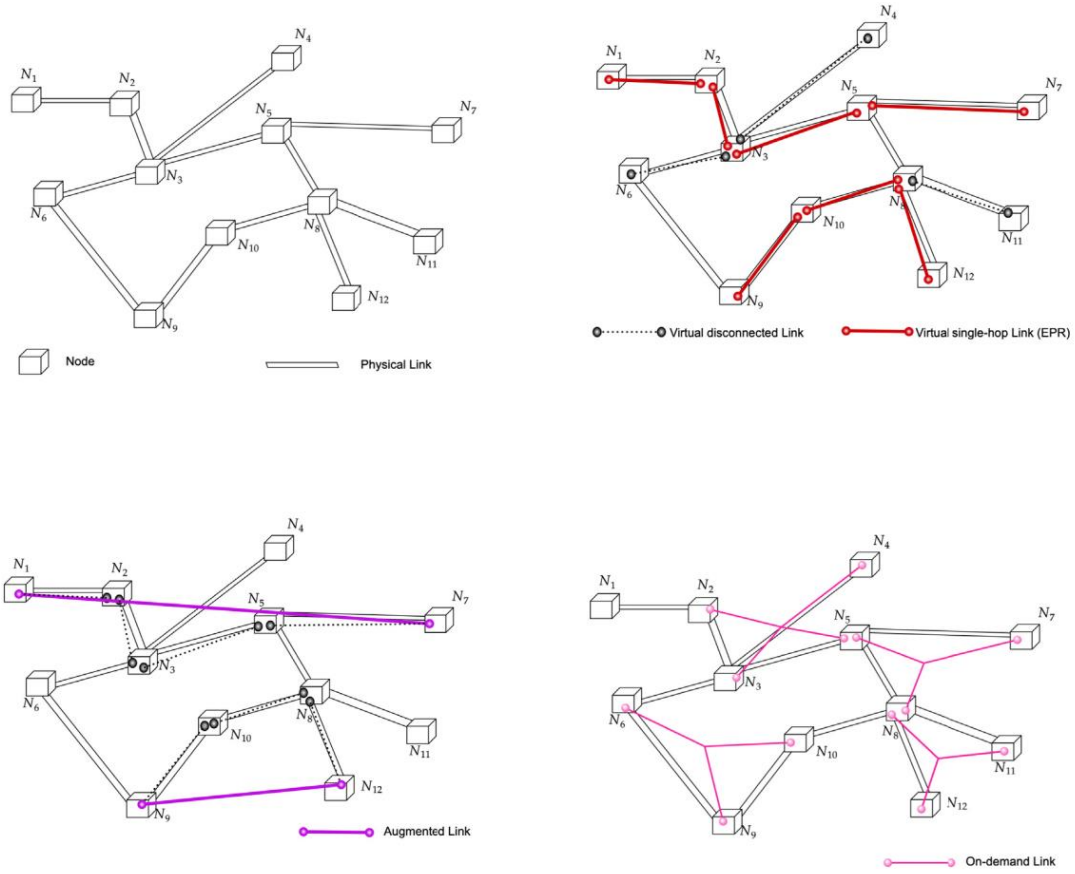


Figura 18: Representación de las distintas formas de conectividad resultantes de la combinación de canal cuántico, entrelazamiento bipartito, intercambio y entrelazamiento multi-partito. Extraída de [219].

comunicación cuántica sin errores sobre canales ruidosos. Los protocolos de purificación pueden ser o bien protocolos de destilación o esquemas *recurrence and pumping*. En la destilación, el protocolo manipula un conjunto de copias (idénticas) de estados entrelazados no máximos y se generan un número menor de pares con mayor cantidad de entrelazamiento y fidelidad mejorada. En los esquemas *recurrence and pumping*, un paso elemental de purificación se repite para obtener pares con fidelidad mejorada. Los dos mecanismos de purificación podrían ser aplicado a estados entrelazados bipartitos o multipartitos. En [138, 178] se encuentra una descripción exhaustiva de dichos mecanismos en el contexto de la comunicación cuántica.

Al igual que en la comunicación clásica, es necesario el diseño de QEC (*Quantum Error Correction*) que permita la protección de la información cuántica durante la trasmisión y/o su recuperación después de ella [145]. Aunque la idea que subyace bajo QEC es la misma que en su versión clásica, la redundancia, varias son las características cuánticas que hacen necesario la

reinvención de tales técnicas: la no clonación, el principio de superposición, y el colapso después de la medida. QEC es una disciplina que aúna la mecánica cuántica con la teoría clásica de los códigos de corrección de errores, de aplicación no solo a la comunicación cuántica en canales ruidosos, sino también al almacenamiento y la computación cuántica ante la inevitable de-coherencia en la información. Recientemente en [25], se estudian soluciones alternativas a la corrección de errores cuánticos mediante la generación de estados entrelazados multipartitos, que se basa en la observación de que incluso en canales ruidosos algunos estimadores de los qubits permanecen invariantes al ruido, lo que puede ser aprovechado para la codificación de información libre de errores.

4. Realizaciones físicas para IC

Los principios y procesos que dan soporte a la comunicación cuántica revisados en el apartado anterior son punto de partida para la definición de la futura Internet Cuántica. Aunque es mucho más que una infraestructura física, la Internet clásica se compone ante todo de enlace de comunicaciones y nodos de conmutación programables que mueven los bits de un origen a un destino arbitrarios. Una visión algo más contemporánea sería definir Internet no solo como la infraestructura de transporte, sino como el sistema de interconexión que hace posible la computación distribuida clásica. Para acabar, Internet es también en sí misma un sistema distribuido de almacenamiento de información.

Bajo esta perspectiva, en [219] se recoge la siguiente defínción para la IC: "The Quantum Internet is a heterogeneous network of quantum devices capable of exchanging quantum bits (qubits) and generating and distributing entangled quantum states". Los elementos físicos y lógicos de la futura Internet cuántica (IC) son, en una visión general, exactamente los mismos, con la diferencia fundamental de la producción, consumo y distribución del entrelazamiento para nuevas tareas de cómputo y comunicaciones. Entendido el entrelazamiento como recurso fundamental de comunicación, la Internet cuántica requiere el desarrollo del hardware de comunicaciones (dispositivos óptico/fotónicos) que implementen fuentes de información cuántica, repetidores cuánticos, memorias cuánticas, conmutadores cuánticos y detectores cuánticos. Sobre estos dispositivos, la comunicación se habilita con 4 mecanismos fundamentales: (1) la generación y manipulación de entrelazamiento; (2) la distribución del entrelazamiento; (3) la purificación del entrelazamiento y (4) la corrección cuántica de errores. Veremos en este apartado las tecnologías actuales para el soporte y desarrollo de los dispositivos de interconexión de una red cuántica (IQ) basada en repetidores y distribución del entrelazamiento, dado que es esta estructura de interconexión la que se encuentra más avanzada hasta el momento. Así, y tras revisar las realizaciones de un repetidos no ideal (apartado 4.1) y de los dispositivos de memoria (apartado 4.2), se analizan los distintos avances. En concreto, en el apartado 4.3 se recoge la clasificación habitual de los repetidores cuánticos, para en el apartado 4.4 describir los repetidores cuánticos enteramente óptimos y la problemática asociada a la generación de estados grafo. Finalmente, se describe la realidad de la generación y manipulación de entrelazamiento (apartado 4.5) y otros aspectos experimentales de la infraestructura de red cuántica 4.6.

4.1. Repetidores cuánticos no ideales

Un QR real está sometido a imperfecciones en el proceso de medida, en los elementos ópticos o en el propio canal de transmisión que hacen que el análisis presentado en la sección anterior sea demasiado simplista. Nos ocuparemos aquí de ver las soluciones que existen para equipar un repetidor cuántico con mecanismos de corrección de los errores físicos. En líneas generales, estos procedimientos de supresión o corrección de los errores se pueden clasificar en dos tipos: (a) los métodos deterministas, que engloban la corrección cuántica de errores [290] y la destilación del entrelazamiento [45]; (b) los métodos aleatorios de supresión de errores [290] y la purificación de entrelazamiento [45, 65, 122]. Los del primer tipo terminan de forma determinista, por lo que no es necesaria ninguna señal entre las partes que alerte del éxito o fallo de un intento de corrección; los del segundo tipo emplean intentos repetidos independientes de corrección hasta lograr uno con éxito, y deben avisar de cuando ese suceso ocurre. En redes con una extensión geográfica grande, esta comunicación final puede suponer un retardo de magnitud elevada, toda vez que un fotón necesita unos $0{,}5$ ms para recorrer 100 km en una fibra óptica. La ventaja de los métodos probabilistas es que funcionan incluso cuando los estados acumulan tanto ruido que es prácticamente imposible recuperarlos con un método determinista. Los primeros tienen, por consiguiente, mayor tolerancia a los errores o mayor capacidad de corrección.

A. Supresión de errores determinista

- Corrección cuántica de errores (QEC, *Quantum Error Correction*). Al igual que en la codificación de canal clásica, la idea con QEC es usar la redundancia presente en el entrelazamiento de un grupo de qubits para codificar un estado suficientemente diferenciado de otros y poder así corregir posibles errores. Para ser más concreto, un qubit se codifica en un subespacio bidimensional de un espacio de Hilbert de dimensión mayor compuesto por un cierto número de qubits, en lugar de convertirlo en un único sistema físico. Esta solución es reminiscente de los códigos lineales que se han empleado durante décadas en los sistemas de comunicaciones clásicos. La corrección cuántica de errores es claramente un proceso determinista, independiente de cualquier otra señal externa. En una red de comunicaciones cuántica grande este funcionamiento determinista es ventajoso y conveniente, y simplifica en gran medida el diseño de los protocolos básicos en la red, pero ocurre que el proceso de codificación y decodificación de códigos cuánticos es costoso y complejo, más que en el caso clásico. La QEC es un extenso campo de investigación en el presente, muy activo en razón de la importancia que los códigos de error tienen de cara a la consecución de ordenadores cuánticos lo bastante grandes y prácticos. Por ende, existen buenos códigos para QEC [78]. Para un tratamiento extenso y especializado de la QEC y las muchas familias de códigos existentes, remitimos al lector a [385, 250].

- Destilación de entrelazamiento. El procedimiento de *destilación de entrelazamiento* consiste en la obtención de un par de Bell con entrelazamiento máximo (o cercano al máximo) a partir de pares de qubits entrelazados más débiles usando tan solo operaciones LOCC de un único sentido. Esto último quiere decir que la comunicación clásica, si la hay, fluye siempre en un mismo sentido, no es interactiva. La destilación es, pues, un proceso de ``mejora'' o refuerzo del entrelazamiento de partida, y lo cierto es que se caracteriza por una estrecha relación con la QEC [214], que se puede explicar porque existe una forma de

convertir un protocolo de hashing de un solo sentido en un código cuántico de corrección de errores [45, 46]. Por ese motivo las dos técnicas devienen equivalentes desde el punto de vista del protocolo, pese a que en la práctica pueden aparecer diferencias entre las dos debidas a la acumulación de ruido.

B. Supresión de errores probabilista

- Detección cuántica de errores. Los códigos cuánticos de corrección se pueden utilizar solo para detectar errores, sin corregirlos; o sea, para señalar la presencia de errores si los hay, descartar el proceso y volver a empezarlo. La lógica que subyace a este método es que los códigos cuyo propósito es solo la detección pueden ser más simples y menos costosos en términos de cómputo que los correctores. La desventaja del método es que no termina en un tiempo predecible, determinista, y que puede conllevar un retardo elevado sobre todo en redes de gran tamaño.
- Protocolo de generación de entrelazamiento señalizado (HEGP, *Heralded Entanglement Generation Protocol*). Este es un protocolo capaz de generar entrelazamiento cuando se ejecuta con éxito y de detectar errores de pérdidas cuando falla. Como el entrelazamiento no es posible crearlo bajo condiciones LOCC, uno de los participantes tiene que generar un estado entrelazado entre un qubit local y un qubit móvil, por medios locales, y luego enviar el qubit móvil al otro participante. La elección típica para el qubit móvil es un sistema bosónico, por ejemplo un estado fotónico. El canal cuántico asociado (un canal bosónico) tiene como fuente principal de ruido las pérdidas. La finalidad de HEGP es, entonces, generar un estado entrelazado fuerte entre Alice y Bob, cualesquiera que sean las pérdidas en el canal. Dependiendo de cómo se codifique la información cuántica en los modos ópticos o de cómo se entrelazan los qubits locales estacionarios con esos modos ópticos, se eligen los esquemas más adecuados para detectar las pérdidas. Con codificaciones de variable discreta *dual-rail* (resp., *single-rail*), la generación del entrelazamiento se efectúa mediante la interferencia de dos fotones (un fotón) entre los modos ópticos procedentes de puntos vecinos, en tanto que la detección de errores se consigue según los patrones de activación de los detectores de fotones tras la interferencia [17, 20, 31, 94, 134, 396]. En los sistemas de variable continua (e.g., GKP [182]) es posible generar el entrelazamiento combinando los dos modos ópticos entrantes y pasándolo después por una medida homodina a los puertos de salida. Los salidas de la medición homodina dan información sobre la probabilidad de las pérdidas, y esta se puede usar para determinar si la generación de entrelazamiento ha tenido éxito o no [166]. En caso de que se detecten pérdidas, el procedimiento simplemente se repite hasta que los dos nodos adyacentes tengan la confirmación de que ciertos patrones de detección asociados al éxito del proceso se han producido. Esa confirmación no es más que un mensaje recibido por el canal clásico. Una alternativa a esta multiplexación temporal es sustituirla por multiplexación espacial o en frecuencia con el fin de ejecutar el protocolo de señalización en paralelo, de forma que uno de los ensayos multiplexados tenga éxito con una alta probabilidad dentro de un intervalo de tiempo prefijado [414].
- Destilación de entrelazamiento dúplex o a dos vías (2-EDP, *Two-way Entanglement Distillation Protocol*). La finalidad de 2-EDP es la de producir un par entrelazado máximo (o cercano al máximo) mediante el uso del paradigma LOCC a dos vías o dúplex, partiendo de pares entrelazados más débiles o ruidosos. En la estrategia LOCC dúplex se

Tabla 7: Comparación tecnológica de repetidores cuánticos. La escala de tiempos de generación de las claves y la complejidad evolucionan de forma diferente con la distancia total L, la distancia entre repetidores L_0 y el tiempo de las puertas cuánticas t_0.

Errores	**Supresión de errores**	**1G**	**2G**	**3G**
Pérdidas	Probabilista	✓	✓	
	Determinista			✓
Error operativo	Probabilista	✓		
	Determinista		✓	✓
Escala temporal		$\max\{\frac{L}{c}, t_0\}$	$\max\{\frac{L_0}{c}, t_0\}$	t_0
Complejidad		$\text{poly}(L)$	$\text{polylog}(L)$	$\text{polylog}(L)$

permite la comunicación clásica en ambos sentidos. Esta posibilidad abre la puerta a que uno de los participantes compare los resultados de sus medidas con las del otro, o bien a que ejecute operaciones locales que dependen de la información recibida del otro participante. Esto es, convierte al protocolo de destilación en un protocolo adaptativo o interactivo. Por ejemplo, si los estados de Bell tienen errores de inversión de bit, $\rho_{AB} = (1-\varepsilon)|\Phi^+\rangle\langle\Phi^+|_{AB} + \varepsilon|\Psi^+\rangle\langle\Psi^+|_{AB}$, los participantes pueden usar dos copias de los estados para obtener un par sin errores simplemente comparando los resultados de medidas de comprobación de paridad en cada una de sus mitades [45, 65, 122]. Esta técnica se puede extender de manera semejante para suprimir con cierta probabilidad errores de pérdida de fase. Para errores de depolarización generales, es posible emplear un método llamado *twirling* [46] o conmutar entre errores de fase y de bit para suprimir los errores [122].

Bajo hipótesis de funcionamiento ideales, estos métodos convergen rápidamente a pares de Bell máximos. En principio, resulta posible extraer entrelazamiento hasta una tasa que está limitada por la cantidad de entrelazamiento destilable en modo dúplex [45]. En la práctica, más bien, los errores de los dispositivos limitan la fidelidad de los pares de Bell destilados. Se han propuesto numerosos protocolos de destilación [46, 122, 165, 226, 258, 343, 383]. Por ejemplo, se pueden usar múltiples copias de pares imperfectos de Bell para purificar un solo par de Bell [165, 343]. También se ha propuesto utilizar un algoritmo genético para identificar el protocolo 2-EDP óptimo [258]. Un entrelazamiento auxiliar que ya exista puede mejorar el rendimiento de 2-EDP [383]. Y, al igual que con 1-EDP, dado que existe una conversión directa desde 2-EDP a un código cuántico de corrección de errores, ambos métodos se pueden enmarcar en una misma visión de protocolo.

Como regla general, los métodos deterministas funcionan adecuadamente solo si el umbral de transmitancia es $\eta > 1/2$ para las pérdidas de qubits o bosones y si $e < 1/4$ para la depolarización de qubits, aunque sí son aptos para el rango $e \lessapprox 0{,}18929$ con el protocolo de hashing y también es posible suprimir los errores cuando $e \lessapprox 0{,}19130$ con un esquema de codificación concatenado [155]. En cuanto a los métodos probabilistas, los umbrales correspondientes son $\eta > 0$ y $e < 1/2$, claramente mejores.

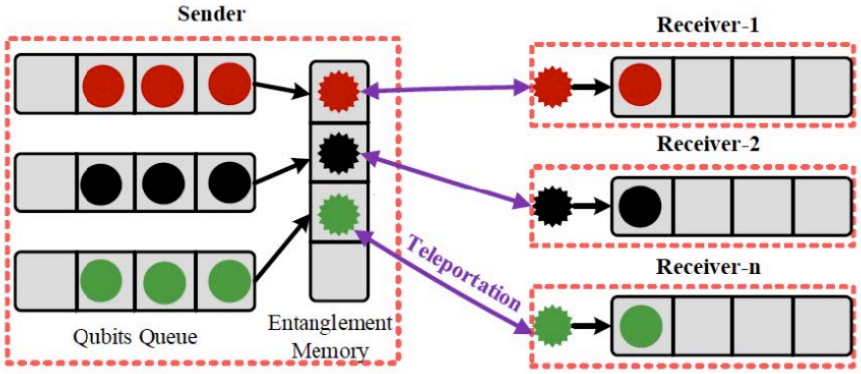


Figura 19: Nodo de comunicación cuántica. Extraído de [286].

4.2. Memorias cuánticas

Si el intercambio de entrelazamiento permite la extensión del entrelazamiento a más de un salto en la red, las memorias cuánticas son necesarias para la ideación de una red cuántica, tal y como se refleja en la Figura 19. Desde el punto de vista de un extremo de la red, cuyo objetivo es enviar/recibir qubits de información, se debe contar, de forma general con dos tipos de memorias cuánticas: la memoria de entrelazamiento y la cola de qubits. La memoria de entrelazamiento almacena pares entrelazados que pueden ser utilizados para el intercambio de entrelazamiento (como forma de repetidor cuántico) o para la teleportación como mecanismo básico de comunicación. Si existe un estado entrelazado entre el emisor y el receptor 1, será posible la teleportación de un qubit en la cola del emisor al receptor 1. Adicionalmente, si existe un estado entrelazado entre el emisor y el receptor 1, este estado se puede utilizar para la conexión del emisor con un tercero utilizando receptor 1 como nodo intermedio vía intercambio de entrelazamiento.

La viabilidad de un repetidor cuántico depende en gran medida de las características dinámicas de las memorias cuánticas. El parámetro más importante es el *tiempo de coherencia* T_2, el tiempo durante el cual la información guardada en el registro de memoria se mantiene sin ser degradada espontáneamente por su entorno físico. Por ilustrarlo mejor, si se quiere generar entrelazamiento entre dos nodos separados por una distancia L, los valores de fidelidad elevada solo se pueden lograr cuando $L \ll cT_2$, siendo c la velocidad de la luz. A mayores de este parámetro fundamental, una memoria cuántica debe poseer también una inicialización rápida, eficiente y con alta fidelidad, como rápidas y eficientes deben ser la aplicación de puertas y la lectura de los fotones. Las referencias [205, 302, 413] discuten en profundidad estas cuestiones.

Hay múltiples tecnologías en estudio y discusión para la construcción de memorias cuánticas: (i) conjuntos atómicos [135, 484] (clase I); (ii) trampas de iones [220] (clase II); (iii) defectos de color en diamantes y otros cristales [1, 28] (clases IV, V y VI); (iv) pozos cuánticos [186] (clase III); iones de tierras raras (clase VII). La Tabla 8 resume las características físicas de cada una de estas familias, y allí se puede apreciar la disparidad de valores de los parámetros que son factibles en cada caso. Todos estos sistemas son al mismo tiempo emisores cuánticos, lo que los convierte en candidatos idóneos para las interfaces átomos-fotones.

Tabla 8: Propiedades físicas de diversos sistemas para construir memorias de qubits. (1) conjuntos atómicos; (2) átomos individuales / trampas de iones; (3) pozos cuánticos; (4) defectos en diamantes; (5) defectos en carburo de silicio; (6) defectos en silicio; (7) iones de tierras raras. Se distinguen las propiedades como memorias (registros) acoplados a emisores de aquellas que tienen como emisores de fotones individuales: el tiempo de emisión T_1, la eficiencia η_{eff}, la indistiguibilidad ι del fotón, el factor Debye-Waller η_{DW}, la fidelidad F del entrelazamiento átomo-fotón y la longitud de onda de emisión λ_{QE}. Los valores marcados con asterisco se refieren a la fidelidad de entrelazamiento entre dos memorias cuánticas. Tabla adaptada de [21].

Emisor		Memoria cuántica			Registro q		Propiedades de emisión					
		T_2	T_2^*	F (puerta)	N	T_2	T_1	η_{eff}	ι	η_{DW}	F	λ_{QE} (nm)
I	^{87}Rb							87 %			$\geq$ 93,3 %	780
II	^{87}Rb	2-6 ms	400 μs	$\geq$ 97,5 %			300 ns	60 %			89 %	780
	^{171}Yb$^+$	$>$ 1 h										369
	^{128}Ba$^+$	4 ms			$\geq 4(^{171}\text{Yb}^+)$	$>$ 1 h	0,6-0,8 ns	57 %	99,5 %	90 %	$\geq$ 80 %	493
III		3 μs	39 ns	95 %	1	1 μs	0,6-0,8 ns	57 %	99,5 %	90 %	$\geq$ 80 %	900-1565
IV	NV	0,6 s	5-36 ns	$>$ 99 %	9	75 s	13 ns	37 %	98,6 %	4 %	96 %	637
	SiV	10 ms	115 ns		1	100 ms	1,6 ns	85 %	72 %	75 %	94 %	737
	GeV						5,5 ns	0,72 %		60 %		602
	SnV		540 ns				4,5 ns			57 %		620
V	V_{Si}	0,8-20 ms					37 ns		69 %	6-9 %		862-917
	$V_{Si}V_C$	64 ms	375 μs	99,98 %	$\geq$ 1		91 ns			7 %		1078-1132
	V^{4+}						45 ns			50 %		1278-1388
	NV		1 μs				13 ns					1180-1468
VI	G						34 ns			15 %		1269
	T						802 ns			23 %		1326
VII	Eu^{3+}	8,1 ms			$\geq$ 1	6 h	0,8-1,2 ms					579
	Er^{3+}				$\geq$ 1	1,2 s	1,5-8,7 ms					1532
	Pr^{3+}	880 μs			$\geq$ 1		140 μs				80 %	606
	Nd^{3+}				$\geq$ 1						80 %	883

Para poder aprovechar los tiempos de coherencia de estas memorias cuánticas se recurre a estrategias híbridas en las que la memoria cuántica se conecta indirectamente con fotones acoplándola con un emisor cuántico eficiente. Este fenómeno ocurre de forma natural en algunos sistemas, por ejemplo en los centros NV,[6] donde los electrones se acoplan con los núcleos de carbono próximos ($T_2 = 75$ s). El mismo fenómeno se da en los sistemas de trampa de iones, donde familias de iones con buenas propiedades de emisión interactúan en el mismo nodo con iones de otras familias con tiempos de coherencia mucho más prolongados (es el caso con $T_2 > 1$ h en la tabla). Otros resultados recientes dan cuenta de combinaciones entre pozos cuánticos y núcleos atómicos (del orden de 10^4 o 10^5 núcleos) que acaban por comportarse como memorias de duración en el rango de los μs aun cuando $T_2^* = 39$ ns para el espín de un electrón [171, 223]. El sistema formado por iones de elementos raros Eu^{3+} en cristales Y_2SiO_5 tiene el récord del mayor tiempo de coherencia observado experimentalmente hasta la fecha (6 horas [500]). Este mismo sistema tiene una memoria óptica capaz de almacenar un qubit con codificación fotónica *time-bin* durante 1 hora [304].

Otro criterio práctico importante de estas memorias cuánticas es la temperatura a la que

[6] Un centro nitrógeno-vacante (NV) es un defecto deliberado en la red cristalina del diamante, en donde dos posiciones adyacentes en lugar de contener dos átomos de carbono contienen uno de nitrógeno y una posición vacante. El espín electrónico de este punto de puede manipular a temperatura ambiente y da lugar a una marcada fotoluminiscencia que permite leer dicho estado.

operan, pues hará que se necesiten un tipo u otro de sistemas de enfriamiento, que pueden ir desde refrigeración por dilución, a criostatos de helio líquido o enfriamiento láser. Por eso algunas otras investigaciones optan por estudiar sistemas de memoria aptos para temperatura ambiente como los basados en sistemas electromecánicos con centros NV [225] o vapores atómicos [57, 129, 236, 279, 351, 406].

4.3. Generaciones de repetidores

En función de las técnicas que se adopten para suprimir los errores debidos a las pérdidas y las operaciones imperfectas de medida, se pueden clasificar los QR en tres categorías o generaciones [21, 334]. La combinación de supresión determinista de los errores de pérdida más supresión probabilista de los errores operativos no se contempla en la Tabla 7 porque es subóptima en comparación con las otras tres posibilidades. Cada una de estas categorías tiene unas prestaciones mejores que las demás para un determinado rango de los parámetros operativos como la velocidad de las puertas cuánticas, la fidelidad de esas puertas (p_2) y la eficiencia del acoplamiento. Revisaremos las opciones disponibles en cada caso y las implicaciones que conllevan el el diseño de redes cuánticas.

4.3.1. Repetidores 1G

La primera de las clases es la que se basa en supresión probabilista de los errores para corregir los fallos e imperfecciones de los elementos físicos, por ejemplo HEGP y algún protocolo de purificación del entrelazamiento como 2-EDP.

La solución básica es, como en el ejemplo de la Figura 16, dividir la distancia total L en segmentos (equiespaciados) de longitud L_0, con $n = L/L_0 - 1$ repetidores intermedios. La función de cada QR es establecer entrelazamiento con cada uno de sus QR adyacentes e intercambiarlo. Para ello, se puede emplear el protocolo HEGP como medio de crear un estado entrelazado de alta fidelidad entre un registro de memoria cuántico y el QR anterior, y otro para hacer lo mismo con el QR posterior. Se supone que cada intento de HEGP usa un tiempo igual a $T_1 = t_{\text{op}} + L_0/c$, siento t_{op} el tiempo total que consumen las operaciones locales y L_0/c el tiempo de tránsito de un fotón hasta alcanzar el QR intermedio, también el retardo para confirmar a los QR vecinos (por vía clásica) que el protocolo tuvo éxito. Se supone también que la probabilidad de éxito del protocolo HEGP es p_e, dependiente de los procesos de captura de fotones en el detector, la eficiencia de transmisión en la fibra y la eficiencia del detector fotónico. Para un sistema *dual-rail* la probabilidad es $p_e \leq 1/2$ en el caso ideal, y viene limitada por el uso de óptica lineal y por la probabilidad de pérdida de los fotones [81]. De todos modos, con codificaciones de los fotones más avanzadas es posible conseguir $p_e > 1/2$ [19, 310]. HEGP logra un entrelazamiento con alta fidelidad entre nodos adyacentes, aunque requiere ensayos repetidos ---p_e^{-1} en media--, dando lugar a un tiempo medio hasta el término del procedimiento de $T = p_e^{-1} T_1$. Nótese que es gracias a que los repetidores disponen de memorias cuánticas por lo que el primer paso de generar entrelazamiento con cada uno de los repetidores vecinos es eficiente, ya que se pueden ejecutar independientemente (y simplemente retener el par entrelazado en memoria hasta que se genera el del otro enlace). Esa es la razón de que este esquema sea superior a otras propuestas con nodos *relay* en las que los repetidores envían pares de Bell al siguiente QR y este debe medirlos tan pronto como llegan [224, 380, 459].

Una vez que el nodo ha creado pares entrelazados con cada uno de sus vecinos inmediatos, los intercambia entre sus registros de memoria y, si este proceso se realiza con éxito, habrá

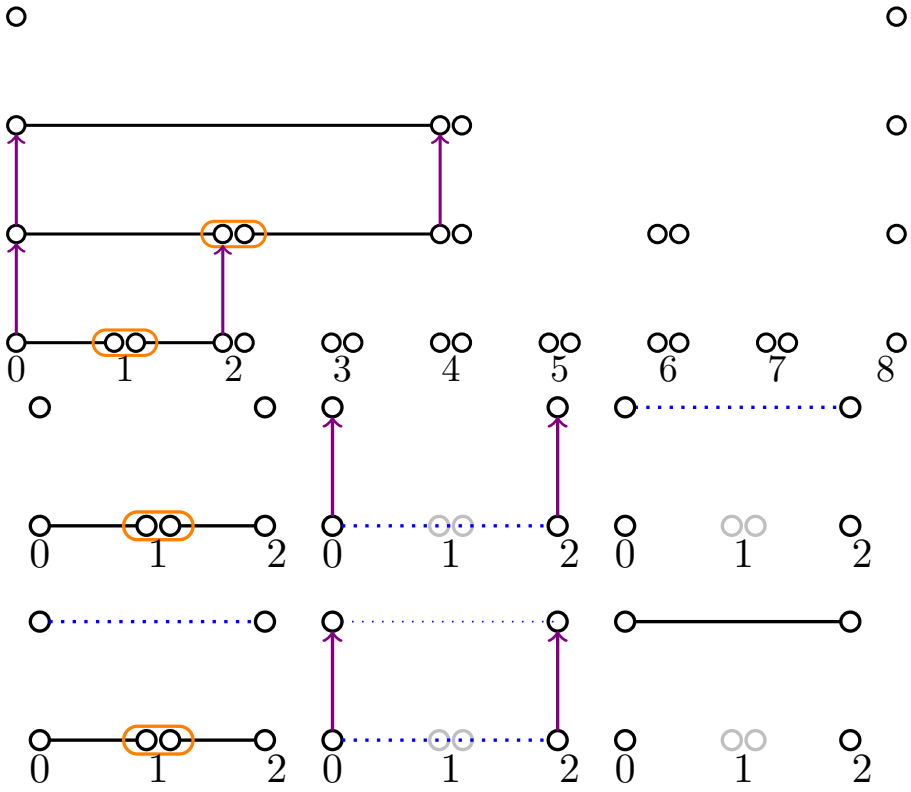


Figura 20: El protocolo BDCZ de repetidor cuántico. Dos pares entrelazados se intercambian en el nodo 1 y se almacenan (paneles intermedios); otro par entrelazado de distancia 2 se genera para purificar el primero (panel inferior); el esquema se repite de forma anidad para producir pares entrelazados de distancia 2^k, $k = 1, 2, \ldots$ hasta completar el proceso extremo e extremo.

creado un par de entrelazamiento máximo directo entre sus dos vecinos. Repitiendo este proceso en cada QR, finalmente Alice y Bob habrán conseguido tener un par entrelazado mutuo. Esta descripción, sin embargo, ha omitido el hecho de que el funcionamiento de las memorias y de las medidas es falible. Cualquiera de esas fuentes de error resta fidelidad a los qubits que se van generando en cada QR, y eventualmente a los que terminan compartiendo Alice y Bob. Para compensar estas imperfecciones se emplean, como se discutió previamente, técnicas de destilación o purificación del entrelazamiento. Uno de los primeros ejemplos en aprovechar esta idea es el protocolo BDCZ [65], o de destilación anidada, en realidad un método recursivo o en árbol para generar el entrelazamiento extremo a extremo. Vamos a describirlo con ayuda de las Figuras 16 y 20. Se parte de una situación inicial en la que todos los nodos intermedios tienen un par de qubits entrelazados con cada uno de sus vecinos inmediatos (llamemos a esto entrelazamiento a distancia 1). En la ronda o nivel de ejecución $k = 1, 2, \ldots$, el protocolo habrá sido capaz de generar entrelazamiento a distancia 2^k, o sea, entre nodos a 2^k saltos de distancia. El número total de rondas necesarias es por tanto $R = \log_2 L/L_0$, que podemos suponer entero por conveniencia ($L = 2^R L_0$). Como en cada operación de intercambio se produce una merma de

fidelidad [122], se incorpora un mecanismo como 2-EDP en cada nivel para evitar la acumulación de este efecto. El tiempo medio necesario para destilar (generar) un par entrelazado en la ronda k es, entonces, $T_k = \alpha_k T_{k-1} + \beta_k 2^k L_0/c$, donde α_k y β_k son coeficientes que subsumen el incremento de tiempo debido al propio intercambio de entrelazamiento, la purificación y la comunicación clásica. Puede suponerse sin mucho error que todas las rondas tienen aproximadamente el mismo valor para ambos, y así $\alpha_k \approx \alpha$, $\beta_k \approx \beta$ para todo k. El tiempo inicial para generar qubits entrelazados entre nodos adyacentes se modela por $T_0 = \beta_0 L_0/c$,, donde β_0 es un coeficiente que captura los mismos efectos que β. A partir de este sencillo análisis, el tiempo total de generación extremo a extremo sería

$$T_{\text{e2e}} = \max(\beta, \beta_0)\frac{L_0}{c}\left(\frac{L}{L_0}\right)^{\log_2 \max(\alpha,2)}$$

que aumenta en forma polinómica con L. Para el caso simple en que el canal solo induce pérdidas se tiene $\alpha \approx \frac{3}{2}\frac{1}{p_{\text{swap}}}$, siendo p_{swap} la probabilidad de éxito del intercambio de entrelazamiento. Por ejemplo, $p_{\text{swap}} \leq 1/2$ para el protocolo DLCZ basado en conjuntos atómicos y óptica lineal [134]. Si además existen errores operativos, es necesario un protocolo de purificación que use al menos dos copias de pares entrelazados, de modo que $\alpha \geq 2$ en todos estos esquemas, como sucede en los protocolos BDCZ o CTSL [94].

Esta primera generación de repetidores cuánticos es eficiente, ya que reduce el coste exponencial de la transferencia de estados a un coste polinómico limitado tan solo por la comunicación clásica dúplex que HEGP necesita entre nodos QR no adyacentes. La tasa de comunicación sigue decayendo en forma polinómica con la distancia, no obstante, y sigue siendo pobre para grandes distancias, aunque puede ser mejorada notablemente con multiplexación temporal, espacial o en frecuencia asociado a los grados de libertad internos de las memorias cuánticas [53, 396]. En cuanto al uso de recursos de entrelazamiento, los protocolos que se han descrito son también muy eficientes. El BDCZ tiene una estructura recursiva, como se ve en la Figura 20, con R niveles de anidamiento. El protocolo comienza con n pares de qubits entrelazados de distancia 1 y fidelidad F. En la ronda k se han obtenido $n/2^k$ pares de entrelazamiento de distancia 2^k y fidelidad $F_k \leq F$, y M pares de estos se utilizan para purificar hasta una fidelidad F otros $n/2^k$ pares entrelazados. Es decir, se utilizan $2M/2^k$ pares de qubits para crear cada pareja de qubits entrelazados de distancia $2^k L_0$. En total, entonces, se necesitan $(2M)^R = (L/L_0)^{1+\log_2 M}$ pares de qubits entrelazados. En términos de memoria, los esquemas presentados pueden igualmente ser eficientes si se supone que la purificación de un par entrelazado ruidoso de longitud $2^j L_0$ se puede llevar a cabo mediante la aplicación secuencial de un protocolo que ``insufla'' entrelazamiento al par ruidoso a partir de un par entrelazado auxiliar de la misma distancia 2^j que tiene un entrelazamiento inferior [65, 139]. El incremento de purificación depende tanto de la fidelidad inicial como de la del par auxiliar. Durante el proceso de destilación solo son necesarios dos pares de memoria, uno para almacenar el par entrelazado que se desea mejorar y el otro para almacenar el par auxiliar en cada ronda, y la purificación tiene lugar procesando dos pares no purificados de distancia 2^j. Uno de los pares (el auxiliar) tiene que ser preparado reiteradamente durante el proceso, y cabe imaginarlo como el resultado de conectar dos pares entrelazados purificados de distancia 2^{j-1} mediante intercambio. En resumen, un par purificado de distancia 2^j proviene con este método de un par no purificado (impulsado) de distancia 2^j y dos pares purificados de distancia 2^j. Iterando esta relación, y considerando que cada par entrelazado necesita dos registros de memoria cuántica, el número total de registros de memoria que requiere un QR de primera generación es de $N = 2\sum_{j=0}^{R} 2^j = 2(2^{R+1}-1) = 2(2L/L_0 - 1) = 4L/L_0 - 2$.

Por ejemplo, si $R = 5$ serían necesarios 126 registros de memoria.

Existen una serie de variaciones del protocolo BDCZ. Una implementación basada en medidas y usando estados grafo se da en [501]. El protocolo DLCZ la simplifica recurriendo a conjuntos atómicos y óptica lineal. [396] presenta una revisión en profundidad de QR de primera generación basados precisamente en esa combinación de conjuntos atómicos y elementos de óptica lineal, en donde además el HEGP se apoya en codificación de estados de Fock, codificación de polarización y codificación *time-bin*. Las propuestas de [17, 94, 298, 331], por el contrario, se basan en codificación con estados coherentes.

4.3.2. Repetidores 2G

La segunda clase de QR recurre a la supresión de errores probabilista para las pérdidas y a métodos deterministas para corregir los errores operacionales [227, 283, 312, 332]. A modo de ejemplo, se pueden preparar los estados $|0\rangle_L$ y $|+\rangle_L$ con el esquema de los códigos Calderbank-Shor-Steane (CSS) y almacenarlos en dos nodos consecutivos. Los códigos CSS son especialmente adecuados dada su implementación tolerante a fallos en la preparación, medida y funcionamiento de las puertas CNOT [227]. Después, se puede crear un par codificado de Bell $|\Phi^+\rangle_L = \frac{1}{\sqrt{2}}(|00\rangle_L + |11\rangle_L)$ entre nodos adyacentes vía teleportación con puertas CNOT [181] aplicadas sobre cada qubit físico en el bloque codificado usando los pares generados con el proceso HEGP. Para finalizar, se consigue corrección cuántica de errores cuando se realiza intercambio de entrelazamiento en el nivel codificado. Los repetidores cuánticos 2G usan así QEC en sustitución de la purificación 2-EDP y consiguen con ello evitar la lenta comunicación clásica entre nodos vecinos. Si la probabilidad de errores de operación acumulados a lo largo de toda la ruta de QR es suficientemente pequeña, incluso de pueden utilizar los repetidores 2G sin codificación alguna.

Los pares entrelazados se pueden generar con el proceso HEGP adaptado para esquemas de codificación fotónica diferentes. Con codificaciones *dual-rail* (*time-bin*, polarización o trayecto) basta con elementos de óptica lineal y detectores de fotones para anunciar las medidas de Bell exitosas y para detectar los errores de pérdida de fotones. La limitación potencial es que la probabilidad de éxito de la BSM está acotada por $1/2$ en los sistemas *dual-rail*. Alternativamente, podemos plantearnos el uso de codificaciones bosónicas como los estados GKP, para HEGP [166]. A diferencia de las codificaciones *dual-rail*, la GKP puede conseguir medidas de Bell deterministas con óptica lineal y detección homodina [182]. En presencia de errores por pérdidas habrá ruido de vacío añadido en el sistema, que la medida homodina podrá detectar. La codificación GKP puede corregir este ruido de vacío hasta un cierto nivel (pequeño), por encima del cual es más útil alertar de la presencia de error y recomenzar todo el proceso. Como en la primera generación, pueden deducirse cotas de la tasa de comunicación alcanzable con estos repetidores, que viene limitada por el HEGP y la purificación a dos vías entre nodos vecinos. Por citar un ejemplo, tenemos que la tasa C cumple $C \leq (2(L_0/c + t_{\text{op}}))^{-1}$, de donde se sigue que si ignoramos t_{op} y L_0 es pequeña, C puede ser muy elevada. Por supuesto, con un valor de L_0 pequeño harían falta muchos repetidores intermedios y, consecuentemente, una gran cantidad de memorias cuánticas.

Los recursos físicos que necesita esta segunda generación de QR dependen del tamaño del código CSS, n_{code}. En cada repetidor, son necesarios al menos $2n_{\text{code}}$ qubits para almacenar los estados codificados $|0\rangle_L$ y $|+\rangle_L$, y también qubits de memoria adicionales para almacenar y purificar el entrelazamiento entre los QR adyacentes [227]. Por lo tanto, el número de elemen-

tos de memoria es $\sim n_{\text{code}} L/L_0$. El tamaño del bloque de codificación n_{code} aumenta en forma poli-logarítmica con la distancia total L. Asintóticamente, existen códigos CSS con $n_{\text{code}} \leq 19t$ capaces de corregir hasta t errores de inversión de bit o de de-fase ---esta cota se obtiene a partir de la cota de Gilbert-Varshamov cuántica [78]---. Ello implica que solo son necesarios $n_{\text{code}} \propto t \sim \ln L/L_0$, una cantidad que aumenta de forma logarítmica con L. En la práctica, sin embargo, puede ser difícil inicializar un código CSS tan largo sin errores con operaciones locales que son imperfectas. Un medio de evitar esta complicación es inicializar el código CSS concatenando códigos más pequeños con r niveles de anidamiento, y entonces el tamaño del código escala polinómicamente con la distancia $n_{\text{code}} \propto t^r \sim (\ln L/l_0)^r$. Otra alternativa es el código Bacon-Shor [24] cuya longitud crece con el cuadrado de la distancia $n_{\text{code}} = (2t+1)^2 \sim (\ln L/L_0)^2$, y cuya inicialización se puede reducir a la preparación de estados GHZ de $2t+1$ qubits.

4.3.3. Repetidores 3G

Los repetidores de tercera generación emplean la supresión determinista de los errores, con QEC y funciones *hash*, para corregir ambos tipos de errores, los de pérdidas y los operativos [163, 333, 335]. En ellos la información cuántica va directamente codificada en un bloque de qubits físicos que se envían por un canal ruidoso. Si las pérdidas y errores de operación son suficientemente pequeñas, los qubits recibidos sirven para restaurar todos los qubits del bloque, y este se reenvía al siguiente repetidor. Como vemos, los QR de esta clase solo requieren comunicación clásica en un sentido, por lo que pueden lograr altas tasas de transmisión, semejante a como los repetidores clásicos solo están limitados por el retardo de propagación y el tiempo preciso para las operaciones locales.

Los códigos de corrección de errores disponibles para los QR de tercera generación son numerosos. Con QEC basada en qubits una opción son los códigos cuánticos de paridad [374] con longitudes de bloque moderadas (alrededor de 200 qubits), que bastan para combatir ambos tipos de errores [333, 335]. Códigos como los de superficie o el de *tree-cluster* [455] pueden corregir más errores (hasta el 50 %) con longitudes de bloque más largas. Para códigos cuánticos basados en sistemas de d niveles (por ejemplo, los basados en *time-bin*), se pueden implementar códigos cuánticos polinómicos [105] capaces de aproximarse a tolerancias cercanas al $50\,\%$ o códigos cuánticos Reed-Solomon [288] con los que mejorar más la tasa de generación [337]. Análogamente, si cada modo óptico se considera como un sistema de variable continua, eso abre la posibilidad de usar códigos cuánticos de corrección de error bosónicos, por ejemplo códigos gato [271, 324], códigos binomiales [319] y códigos GKP [5, 182, 345] para corregir las pérdidas. La ventaja destacada de los códigos bosónicos es que pueden explotar la elevada dimensión de los sistemas bosónicos para reducir el número de modos bosónicos, lo que supone posiblemente una ventaja a la hora de maximizar el uso del ancho de banda del canal cuántico [281]. Tal como se hace en los sistemas de comunicaciones clásicos, se consigue una reducción adicional de los errores residuales si se concatenan el código bosónico del primer nivel con un código de variable discreta en un segundo nivel, dando lugar a un esquema combinado CV-DV. Si se quiere reducir el coste respecto de una arquitectura en la que todos los repetidores tengan esa complejidad, es posible combinar repetidores de dos tipos, unos capaces de corregir los errores en los dos niveles y otros solo operando en la corrección de errores del primer nivel [390].

Es conveniente señalar que los repetidores 2G y 3G pueden lograr tasas de transmisión significativamente mayores que los 1G, pero lo hacen a costa de mayores requisitos tecnológicos, pues necesitan puertas cuánticas de alta fidelidad, ya que los QEC solo tienen buenas presta-

ciones cuando los errores operativos están por debajo del umbral de tolerancia a fallos de los circuitos. Además, la distancia entre repetidores debe ser más corta porque la corrección de errores solo puede corregir de manera determinista un número finito de errores [335, 426].

Paralelamente a lo que sucede con los QR 2G, los recursos físicos que necesitan los 3G dependen del tamaño del código de corrección de errores. Si el tamaño de dicho código es n_{code} (qubits o modos bosónicos), en cada repetidor hacen falta $O(n_{\text{code}})$ registros de memoria cuántica para corregir todos los tipos de error. El número total de elementos de memoria es entonces de $\sim n_{\text{code}} L/L_0$. En principio, podría usarse QEC sobre los modos ópticos para sustituir el requisito de tener memorias cuánticas de estado sólido o atómicas, lo que conduce a la idea de repetidores totalmente fotónicos (ver más adelante).

Una comparación rigurosa de los distintos tipos de QR sugiere un análisis de los recursos físicos necesarios y del tiempo de ejecución. Este tiempo depende de la tasa, que a su vez está limitada por la velocidad de las puertas (2G y 3G) y por el retardo en la comunicación clásica (1G y 2G). Por cuanto a los recursos físicos, dependen del número de qubits que necesitan HEGP (1G y 2G) y QEC (2G y 3G) [63]. Una medida cuantitativa homogénea y armonizada de ambos factores es la función de coste

$$C(L) := \frac{N_s}{C}\frac{L}{L_0},$$

donde C es la tasa de transmisión que se desea y N_s es el número de qubits necesarios por repetidor. Dado que esta función de coste escala linealmente con L, la normalización $C(L)/L$ ---especialmente para L grande--- nos da una idea mejor de cómo varía el coste unitario: qubits $\times$ tiempo para generar un bit sobre 1 km. Esta función normalizada depende también de la eficiencia del acoplamiento η_c, la probabilidad de error de las puertas ε_G y el tiempo de la puerta t_0. Atendiendo a la combinación de estos parámetros, se puede establecer una división como la que sigue.

- Para probabilidades de error en las puertas elevadas, $1\,\% \lessapprox \varepsilon_G$, los repetidores 1G resultan mejores.
- Con probabilidades de error en las puertas intermedias pero con baja eficiencia de acoplamiento o con operaciones locales lentas ---$0{,}1 L_{\text{att}}/L \lessapprox \varepsilon_G \lessapprox 1\,\%$ y $\eta_c \lessapprox 90\,\%$ o $1\,\mu\text{s} \lessapprox t_0$--- los repetidores 2G con codificación son superiores.
- Si la probabilidad de error en las puertas es baja ($0{,}1 L_{\text{att}}/L \lessapprox 0{,}1$ pero la eficiencia de acoplamiento es mala ($\eta_c \lessapprox 90\,\%$) o las operaciones locales son lentas ($t_0 > 1\ \mu$s), la elección más favorable son los repetidores 2G sin codificación.
- Para eficiencias de acoplamiento altas ($\eta_c > 90\,\%$), velocidad de puertas alta ($t_0 \lessapprox 1\ \mu$s) y probabilidad de error baja en las puertas ($\varepsilon_G \lessapprox 1\,\%$), los repetidores 3G son mejores en términos de la función de coste normalizada.

4.4. Repetidores enteramente ópticos (MBQC)

Aunque los protocolos habituales de los repetidores hacen uso de memorias (las memorias no son más que sistemas cuánticos estacionarios, es decir, con un tiempo de coherencia persistente) para mantener almacenados temporalmente los qubits entrelazados que van siendo

necesarios, en principio estos elementos de memoria podrían reemplazarse por dispositivos ópticos de memoria puros [273]. Ahora bien, materializar esta idea resulta ser singularmente difícil. También es cierto que los repetidores que aplican QEC podrían en teoría prescindir de las memorias convencionales, ya que los códigos de corrección son capaces de eliminar los errores en los qubits. En apoyo de esta idea, ocurre que los repetidores con QEC, que pertenecen tanto a la clase 2G como a la 3G, se pueden implementar de forma enteramente óptica. Tal transición desde repetidores basados en materia a repetidores basados en luz merece una discusión específica que proporcionamos en este apartado.

Para comprender el mecanismo de funcionamiento de los repetidores ópticos primero se verá en qué consiste la computación cuántica basada en medidas (MBQC, *Measurement Based Quantum Computation*) [38]. En un sistema de este tipo, se prepara inicialmente un estado entrelazado que se usa como recurso (normalmente un estado grafo o clúster) y la computación consiste en la realización de medidas locales adaptativas sobre el mismo [376]. En las plataformas físicas donde las puertas cuánticas pueden sufrir entrelazamiento probabilista, como pasa con los sistemas de variable discreta y codificación fotónica *dual-rail*, un computador de tipo MQBC tiene la ventaja de que ese tipo de puertas probabilistas solo están presentes en la preparación del estado inicial y no vuelven a ser necesarias durante la computación. En consecuencia, se evita la caída exponencial de la probabilidad de éxito en el cómputo con el número de operaciones de entrelazado y se reduce drásticamente el coste en comparación con un computador basado en puertas convencionales [71, 253]. Mejor aún, el enfoque MBQC permite circuitos de profundidad fija en los que un qubit pasa solo por un número finito y pequeño de operaciones antes de ser consumido por una medida de un solo qubit. Este proceso, además, encaja bien con qubits móviles y ayuda a reducir sustancialmente las pérdidas de fotones.

De forma diferente a como se hace con puertas convencionales, en MBQC la universalidad (que es la capacidad de realizar, de manera aproximada, cualquier transformación unitaria sobre un cierto número de qubits) se consigue con una elección apropiada del estado clúster inicial [66], más el acceso a operaciones no-Clifford. Análogamente, la tolerancia a fallos (que es la eliminación de errores en la preparación, medida y operación de las puertas con caída exponencial) se realiza mediante un código corrector de errores que se traduce en un estado clúster con una forma y estructura especiales donde se mapea la codificación, una regla para implementar las operaciones lógicas por medio de medidas adaptativas de un solo qubit, y un método para detectar y corregir el error, incluido un algoritmo para extraer los resultados de las medidas lógicas (la etapa de decodificación y recuperación del resultado). Una característica común en las arquitecturas de repetidores cuánticos completamente ópticos es que son realizables con implementaciones basadas en medidas de QEC. Un repetidor cuántico basado en medidas funciona a grandes rasgos de la misma manera que un computador MBQC. Sin embargo, existen algunas diferencias reseñables, emblemáticas de la diferencia entre computación y comunicación. En primer lugar, la universalidad no es necesaria para la comunicación, luego basta con operaciones Clifford. En segundo lugar, la causa dominante de errores para los estados fotónicos en los repetidores ópticos (las pérdidas) es si cabe más grave. Y tercero, a diferencia de la computación, que se puede ejecutar localmente, la comunicación es un proceso intrínsecamente no local. Por último, es importante tener en cuenta el tiempo necesario para la comunicación clásica, pues el ruido en los qubits físicos aumenta con el tiempo, en general.

El repetidor enteramente óptico de [18] está basado en un estado grafo de tres capas. La capa más interna o *core* es un grafo completo o clique, y es equivalente a un estado GHZ de n qubits. El hecho de que la conectividad en este grafo sea total sirve para facilitar el intercambio

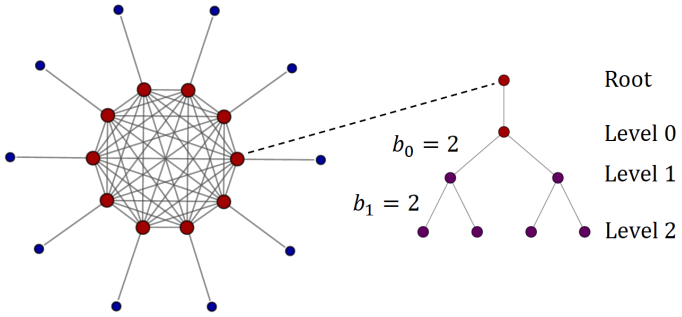


Figura 21: Estados grafo usados en [18]. Cada vértice del clique es un qubit lógico que puede ir codificado como indica el subgrafo en árbol de la derecha para corregir los errores de pérdidas. Los qubits lógicos de la capa interior (en rojo) están conectados a qubits físicos exteriores (en azul) que ayudan a realizar la generación de entrelazamiento.

de entrelazamiento. Esta función solo es posible si los qubits del *core* se aíslan de las pérdidas. Como los fotones de este nivel son muy sensibles a las pérdidas, cada uno de los qubits de la capa interna tiene que estar codificado en un grafo estado de mayor tamaño con suficiente redundancia. En [18] se emplea un código de corrección propuesto en [455]. La capa externa del grafo estado se conforma con qubits adicionales que se agregan a los vértices del *core*, y que son los que intervienen en la fase de generación de entrelazamiento del repetidor. El macroestado grafo resultante se ilustra en la Figura 21.

Las operaciones específicas para que Alice y Bob establezcan un par entrelazado en este repetidor óptico son, resumidas, como sigue sobre un trayecto de longitud total L, n repetidores intermedios, m pulsos ópticos paralelos y un estado grafo de tamaño $2m$. Si se supone que el estado grafo está disponible en ambas fuentes, cada uno de los dos nodos adyacentes a Alice y Bob, respectivamente, recibe m fotones, y acto seguido realiza medidas BSM simultáneas sobre esos m qubits. Esas medidas conectan los qubits del *core* con los recibidos. Aunque cada BSM fructifica con probabilidad $\leq 1/2$, con un número m suficientemente grande al menos una de las medidas de Bell tendrá éxito. A continuación, dependiendo de los resultados de las medidas de Bell, cada receptor aplica una medida en la base X sobre uno de los pares de los qubits de la capa interna cuya medida haya tenido éxito, y medidas en base Z en el resto de los qubits internos. Estas medidas realizadas sobre los qubits internos son quasi-deterministas por cómo está construido el estado grafo (siempre que las pérdidas sean inferiores al $50\,\%$). Como consecuencia, las medidas Z transforman el estado en un clúster lineal entre Alice y Bob, que se convierte a un par de Bell con las medidas X. Un aspecto importante es que la medida a aplicar sobre uno de los qubits codificados en la capa interna depende de los resultados de las medidas sobre los qubits externos. De aquí se sigue que es necesario comunicar información clásica desde esos qubits exteriores a los interiores. Ahora bien, esto se puede lograr de forma completamente local en cada repetidor, y así la cantidad de señales de control se reduce al mínimo. El esquema se completa con un algoritmo de voto por mayoría para compensar las otras fuentes de error distintas a las pérdidas. Con todos estos elementos, el protocolo del repetidor óptico con el código descrito es robusto frente a errores de tipo general bajo la única condición de que se realicen medidas Pauli en el qubit codificado. Hay otra codificación posible con códigos

de paridad [151], pero se ignora aún si existen mejores códigos que estos para obtener mejor rendimiento en los repetidores ópticos.

Existen otras formas o variantes de construcción de los repetidores ópticos:

1. Repetidores modificados. En [352] se proponen varios cambios sobre la arquitectura del repetidor [18]. Una es la introducción de las llamadas *medidas de Bell reforzadas*. La idea es incrementar la probabilidad de éxito de una BSM (que es de $1/2$ en el caso ideal) gracias al uso de recursos adicionales, como fotones ancila en estado separable [152] o entrelazado [188], pequeñas no linealidades [30] y predetección [244, 487]. Hay no obstante inconvenientes asociados a este enfoque: un aumento considerable de la complejidad experimental y un número de recursos muy elevado si se desea una probabilidad cercana a 1. En la propuesta de [352] el procedimiento específico consigue una probabilidad de éxito de $3/4$. Una segunda modificación es un procesamiento distinto de los qubits de la capa interior. Con la modificación son necesarias menos comunicaciones por fibra, pero a cambio las pérdidas son mayores. La tercera modificación atañe a la generación inicial de los estados grafo.

2. Repetidores basados en medidas de Bell codificadas. Los repetidores ópticos pueden estar basados en códigos de paridad para realizar las medidas de Bell [151, 270, 374, 153]. En este caso los estados grafo resultantes son bastante parecidos a los del protocolo original, tienen la forma de un biclique (un grafo bipartito completo) con múltiples hojas por nodo. Pero el protocolo es conceptualmente distinto del método original, ya que ahora se envía un qubit codificado desde un emisor a un receptor, lo que lo convierte en un protocolo más similar a aquellos basados en QEC. La eficiencia de las medidas de Bell y la tolerancia a las pérdidas mejora con la longitud del código de paridad; el nuevo protocolo tiene además menor tiempo de operaciones locales. El método de medida de Bell concatenado de [270] alcanza los límites fundamentales de eficiencia en las medidas de Bell bajo las hipótesis de óptica lineal y del teorema de no clonación.

3. Repetidores bosónicos. Se han considerado asimismo repetidores basados en estados de variable continua [166, 390]. Su principio de funcionamiento es el de aprovechar las propiedades inherentes de corrección de errores en las codificaciones bosónicas, combinadas con codificación de qubits en lo que puede interpretarse como un código concatenado CV-DV. En concreto, se dan varias ventajas con la codificación GKP. De entrada, puede tolerar pequeños errores de desplazamiento y, como cualquier error continuo se puede descomponer en una serie de desplazamientos, GKP puede igualmente tolerar los errores. De hecho, es sorprendente que los estados GKP son mejores corrigiendo errores que otros códigos diseñados a propósito para ese fin [5]. Además, para los estados GKP, las medidas de Bell y las puertas de generación de entrelazamiento dependen de manera determinista de la existencia de recursos gaussianos, siendo la generación de los estados la única componente probabilista. Finalmente, resulta posible utilizar información adicional (analógica) obtenida en el proceso de corrección de errores con GKP para mejorar las tasas lógicas de error en el nivel de codificación de qubits [167, 345]. La arquitectura de repetidor descrita en [390] exprime estas ventajas y plantea dos tipos de repetidores: los que consisten solamente de estados GKP y los que se componen de estados GKP concatenados con pequeños códigos a nivel de qubit.

4.4.1. Generación de estados grafo

En sí misma, la creación de los estados grafo que se precisan para los repetidores ópticos es compleja. Deben tener un elevado número de qubits ópticos de alta calidad (fidelidad). En los sistemas completamente ópticos, la variabilidad aleatoria en algunas formas de codificación (*dual-rail*) o de preparación de los estados (como en los estados GKP) puede tener como consecuencia un sobrecoste elevado. En los sistemas experimentales basados en materia, los efectos de decoherencia e inhomogeneidad entre emisores puede provocar una disminución significativa de la calidad del entrelazamiento con el tamaño final del estado buscado. En todo caso, ha habido progresos continuados recientes en esta dirección que hacen que la producción de estados grafo grandes sea técnicamente viable.

La generación de estados grafo ópticos puede entenderse como un proceso de sutura (*stitching*) iterativo, uniendo recursos cuánticos más pequeños en uno de mayor tamaño. Así, el proceso para generar este tipo de estados tiene estas fases:

- Producción de recursos unitarios. Para empezar, un circuito óptico produce pequeños estados unitarios, que pueden ser estados de un único qubit o estados entrelazados de pequeña dimensión, como pares de Bell, estados GHZ n-partitos ($n \geq 3$) o estados clúster lineales de unos pocos qubits.
- Crecimiento en meta-unidades. Este paso es opcional, pero consiste en combinar un cierto número de estados unitarios en meta-unidades de mayor tamaño. La utilidad de este paso intermedio reside en dejar abierta la posibilidad de generar, por ejemplo, estados GHZ n-partitos directamente a partir de fotones o a partir de pares de Bell fotónicos [175].
- Sutura. Las unidades o meta-unidades se entrelazan iterativamente hasta obtener el estado grafo deseado. Para codificaciones *dual-rail*, tal cosa es viable con las así llamadas fusiones de tipo II; para estados GKP, se hace mediante puertas CZ de variable continua.

Este plan general de creación de los estados admite también la generación de estados grafo ópticos con sistemas experimentales basados en materia, en cuyo caso el entrelazamiento en las fases de sutura es factible o bien directamente en el nivel óptico, o bien asistido por la interacción entre emisores. Un segundo aspecto a tener en cuenta es que cada una de las fases anteriores comporta una probabilidad y una fidelidad que dependen de la forma de codificación, del esquema para generar y entrelazar los recursos y del hardware específico que se disponga. Otras consideraciones que influyen en el diseño incluyen qué parte del estado se puede generar espacialmente (o sea, con las fuentes dispuestas espacialmente) o temporalmente (con entrelazamiento entre estados generados en etapas diferentes). Eso último guarda relación con qué parte del estado debe existir en un momento determinado.

Estados grafo *dual-rail* Existen dos maneras de generar un estado grafo con qubits codificados en modo *dual-rail*, uno probabilista pero completamente óptico y el otro determinista pero basado en materia.

- Generación probabilista óptica. En detalle, el estado grafo de [454] opera de este modo. Primero se preparan seis fotones con fuentes emisoras de fotones únicos. Estos fotones se envían luego a un circuito óptico compuesto por un divisor de haz (BS) y dos puertas de fusión especiales que producen un estado GHZ tripartito cn probabilidad $1/32$. Gracias

al diseño de este circuito, incluso cuando los detectores y las fuentes no tienen eficiencia uno, el estado tripartito GHZ solo se ve afectado por pérdidas individuales (incorreladas) [456]. Este estado GHZ se convierte así en el recurso unitario para producir el estado grafo. En particular, dos estados tripartitos GHZ se convierten en un estado 4-partito GHZ por la acción de una puerta cuántica (de fusión de tipo II), y este estado cuatripartito se corresponde gráficamente con un árbol de tres qubits con un qubit en la raíz del árbol que es redundante y se compone de dos qubits. Partiendo de esa estructura en árbol elemental se puede generar un árbol arbitrario en el que un nodo en el nivel i tiene b_i descendientes (los de la raíz son b_0), para $i = 0, \ldots, d-1$, con ayuda del mismo tipo de puertas de fusión II. De este procedimiento base se siguen varias posibles generalizaciones: [352] toma prestado de [284] un procedimiento más eficiente de generación con las puertas de fusión, mejora el modo de multiplexación y reorganiza las medidas locales para que sean incondicionales. Más aún, es factible crear un estado GHZ n-partito cn probabilidad 2^{1-2n}, y este número se puede mejorar empleando como entradas estados de Bell en vez de fotones aislados, teóricamente [175, 229, 456, 495].

- Generación determinista. En oposición a las propuestas previas, que eran probabilistas, el método propuesto por [73] usa qubits ancila para generar el estado grafo y es, al menos en principio, determinista. La generación de estados clúster lineales desde un único emisor se propuso en [400] para sistemas atómicos y en [292] para pozos cuánticos. Los estados grafo más complejos, como un *lattice* cuadrado en dos dimensiones, se pueden crear con una cadena de emisores y acoplamiento del vecino más próximo [143, 176]. De hecho, cualquier estado se puede crear con estos bloques [393]. En [73] el mecanismo fundamental para generar el estado grafo es entrelazar el emisor con un estado siervo y empujarlo para producir una de las ramas del estado grafo, que emerge así ya entrelazada con el emisor y el estado siervo. En ese momento, se hace una medida en el emisor para eliminarlo del grafo, y el proceso se repite hasta que todas las ramas fotónicas estén conectadas al estado ancila, el cual se supone que tiene un tiempo de coherencia mayor que el emisor. Una medida del estado ancila en la base Y lo desentrelaza del grafo y conecta todos los fotones interiores entre sí, completando la creación del estado grafo.

  Una característica interesante del protocolo en [73] es que resulta muy económico en términos de la cantidad de recursos que usa, medidos como el número de qubits de materia necesarios. Para generar la versión no codificada del estado, solo se precisan un emisor y un estado ancila, con independencia del tamaño del grafo. Además de la versión sin codificar, [73] presenta un método para la creación determinista de estados grafo arbitrariamente grandes pero codificados, en los que los qubits interiores se codifican por medio de árboles de profundidad 2 o 3. Estos protocolos tan solo requieren tres qubits de materia, incluidos dos emisores y uno ancila. El trabajo [207] da un método más general aún para crear estados grafo con codificaciones de los fotones *core* en forma de árboles de profundidad arbitraria, donde el número de qubits de materia requeridos aumenta linealmente con la profundidad d del árbol (son $d-1$ emisores y un qubit ancila). El número de puertas CZ que se usan en este caso es de $2m(2 + \sum_{k=0}^{d-2} \prod_{j=0}^{k} b_j)$, donde b_j denota el número de descendientes de un nodo de nivel j en el árbol y $2m$ es el número de ramas del estado. Estas ideas para la generación determinista de estados fotónicos entrelazados fueron generalizadas en [275], que desarrolla una técnica para la generación de un grafo con estructura arbitraria usando el mínimo número de emisores.

[73] también da cuenta de una técnica para producir estados con grafo en árbol de una profundidad arbitraria d y con k ramas en cada vértice usando solo $d-1$ emisores y un qubit siervo. El número de puertas CZ es, ahora, de $\frac{b^d+(-1)^{d+1}}{k+1}-1$. Este modo de crear qubits fotónicos entrelazados es muy potente por sí mismo y se puede aplicar a repetidores cuánticos de cualquier generación. Por ejemplo, [58] lo usa para implementar repetidores 3G basados en defectos SiV en diamantes como qubits de memoria.

El protocolo de generación de los estados grafo se puede aplicar a cualquiera de las formas de codificación *dual-rail*. Muchas de las propuestas para la generación, sobre todo las de pozos cuánticos, consideran el uso de codificación por polarización, pero la de *time-bin* también se ha contemplado [268]. En ese caso, un método alternativo de crear los estados grafo consiste en usar un único emisor y realimentación con retardo [356, 491]. Con el fin de implementar una puerta capaz de generar entrelazamiento máximo, estos sistemas deben hacer uso de una característica notoriamente complicada desde el punto de vista experimental, la capacidad de acoplamiento fuerte entre el emisor y la guiaonda fotónica por la que se propagan los fotones. De cara a la implementación física de los esquemas de generación de estados grafo, son necesarios registros de tamaño medio de emisores controlados con precisión y qubits ancila. Los emisores tienen que ser de alta calidad, sobre todo en brillo, para que el fotón sea emitido en el modo que se desea y se pueda capturar correctamente. Esto resulta crítico para poder catalogar el protocolo como determinista. El registro debe asimismo manejar qubits ancila con tiempos de coherencia largos, si bien no tanto como los que necesitan los repetidores 1G y 2G, además de poseer la capacidad de realizar puertas de alta fidelidad entre los emisores y los qubits ancila.

Los pozos cuánticos son la tecnología rival más destacada para la generación de los estados grafo. La primera demostración experimental de un protocolo de generación de estados clúster basado en emisores empleaba transiciones exciton-biexciton en estos sistemas [404]. Los pozos cuánticos constituyen excelentes emisores, con una transición óptica (resp., exciton) muy eficiente del orden de 1 ns (100 ps) sin (con) acoplamiento a una cavidad. Se han hecho rápidos avances en los últimos años hacia la mejora del brillo, indistinguibilidad y pureza de las fuentes fotónicas de pozos cuánticos [405]. En su contra, los pozos cuánticos tienen un tiempo de coherencia relativamente bajo en comparación con los qubits atómicos o los de defectos puntuales, y carecen de una memoria cuántica de larga duración que actúe como ancila. Con todo, algunos trabajos recientes apuntan a que el entorno denso de espín nuclear en el que operan (más de 104 núcleos) podría llegar a enfriarse y controlarse con precisión suficiente para suplir esa función. Otros candidatos para la generación determinista de estados grafo son los defectos puntuales ópticamente activos en materiales con una separación de bandas amplia, como los huecos de nitrógeno o los de silicio en los diamantes, o también los huecos dobles silicio-carbono o de silicio en el carburo de silicio. Estos sistemas tienen tiempos de coherencia más prolongados que los pozos cuánticos y se caracterizan por un número pequeño de espines nucleares (la abundancia natural es $\sim 1\,\%$ en el carbono y $\sim 4\,\%$ en el silicio), que son más fáciles de controlar y aislar y están siendo estudiados como registros de memoria para repetidores cuánticos [59, 341, 435]. Ahora bien, los defectos atómicos no son ni tan eficientes ni tan brillantes como los pozos cuánticos, y tienden a emitir luz en modos no deseados una fracción importante del tiempo. Los sistemas atómicos como las trampas de iones y los átomos en cavidades o *lattices* ópticos tienen tiempos de coherencia largos y se pueden

controlar con gran fidelidad. Aunque su emisión de fotones no es tan rápida, sus otras propiedades atractivas es posible que compensen esa menor tasa [441]. Algunas estrategias híbridas que combinan la generación determinista basada en emisores cuánticos con fusión óptico-lineal son especialmente interesantes en caso de que los emisores cuánticos no puedan interactuar entre sí [204, 207].

Estados grafo con codificación GKP Aunque las puertas entrelazadoras para codificaciones GKP son deterministas y asequibles desde un punto de vista experimental, la preparación de estados GKP presenta notorias dificultades. Se dispone en la literatura de distintas propuestas para solucionar este reto, con un predominio reciente por los dispositivos basados en el muestreo gaussiano de bosones (GBS, *Gaussian Boson Sampling*), que son los que usan óptica gaussiana conjuntamente con detectores basados en la cuenta de fotones [371, 394, 432, 447]. Una vez que los estados GKP han sido generados, se pueden pegar o suturar entre ellos de forma determinista con elementos ópticos pasivos y estáticos, como BS, PS y líneas de retardo [448].

Comparativa y prestaciones El coste de los diversos protocolos para repetidores ópticos es especialmente sensible al método de generación de estados en el que se basen. En el protocolo QR original [18] el número total de fotones que se consumen para producir un par entrelazado entre Alice y Bob aumenta de forma polinómica con la distancia, como vimos. La tasa media de producción de un par entrelazado con un sistema de un solo repetidor es del orden de la tasa de repetición del dispositivo más lento entre todas las fuentes de fotones, detectores de fotones y demás. El coste de los repetidores explicados en [151] y [153] aumenta linealmente o de forma sub-cuadrática con el número de fotones por cada qubit codificado.

El estudio [207] analiza el rendimiento de los repetidores basándose en la generación determinista de estados grafo de [73] calculando una cota a la tasa por cada qubit de materia y comparándola con la transmisión directa y con repetidores 1G y 2G. Para la comparación con estos últimos, la figura de mérito se define como la tasa de generación de un estado de Bell entre los extremos dividida por el número de qubits de materia por nodo. En el caso de repetidores 1G y 2G basados en memoria existe una cota superior a esta cantidad que surge de la necesidad de comunicar con mensajes clásicos los nodos, y que vale $c/(4L)$. La tasa de generación de estados grafo de [73] descansa sobre puertas CZ entre el emisor y los qubits ancila, que son las que hacen posible la síntesis de estados grafo fotónicos complejos. En sistemas realistas, la mayor escala de tiempos en la generación determinista es la duración de esas puertas T_{CZ}, en comparación con la cual los tiempos de generación del fotón y de las puertas de un único qubit son despreciables. Por consiguiente, es T_{CZ} el que fija la cota para estos repetidores. En [207] se fija la profundidad del árbol de codificación en 2 para los fotones de la capa interna y se hace una optimización sobre el tamaño del grafo estado, el vector de ramificación $\{b_0, b_1\}$ de la codificación en árbol y el número de nodos, con ánimo de maximizar la tasa para una distancia total de 1000 km. Con estos números, halla que cuando $T_{\mathrm{CZ}} \leq 60$ ns este sistema supera en rendimiento a los repetidores basados en memoria. La distancia entre repetidores en este caso resulta ser de $3{,}5$ km. Estas estimaciones numéricas son en cualquier caso bastante conservadoras, ya que los repetidores basados en memoria también requieren puertas entrelazadoras entre los qubits de materia, que reducen aún más la tasa. Más análisis de este tipo son necesarios para una comprensión más profunda de las ventajas de cada tecnología física, y en escenarios más complejos. Por ejemplo, aunque árboles de codificación de mayor profundidad que $d = 2$ ofrecen mejor protección frente a las pérdidas de fotones, también hacen uso de más puertas CZ-ancila,

lo que reduce a su vez la tasa.

Otras veces, la limitación no está en el número de fotones sino en el número de modos ópticos que están disponibles para comunicar dos QR vecinos. Es decir, por el ancho de banda del canal óptico de comunicaciones, como en las comunicaciones clásicas. Aquí es importante elegir formas de codificación eficientes en el uso de esos modos. En el régimen de bajas pérdidas, cabe usar códigos de variable continua que empaquetan varios qubits en cada modo bosónico. Por ejemplo, la codificación GKP puede acercarse mucho a la capacidad cuántica del canal puro en pérdidas [346]. Otros códigos de variable continua, como los códigos gato, también pueden mejorar la tasa de comunicación por modo en comparación con las codificaciones de variable discreta [281]. Para codificación concatenada CV-DV, puede reducirse aún más la cantidad de recursos necesarios optimizando la distribución de dos tipos de repetidores asociados con corrección de errores CV y DV, como se mencionó antes [390].

4.4.2. Repetidores cuánticos sin memoria

Evidentemente, los repetidores completamente ópticos no necesitan memorias cuánticas y tienen requisitos tecnológicos completamente diferentes a los otros. El problema principal que afrontan es la creación de estados fotónicos entrelazados grandes, lo que antes llamamos estados grafo.

Se han sugerido distintas aproximaciones para la generación de esos estados grafo. Hasta hace poco, los estados de fotones entrelazados de mayor tamaño se habían producido experimentalmente con fuentes de conversión paramétrica espontánea y puertas de fusión [71]. Pero la naturaleza aleatoria de las puertas de fusión supone la principal limitación sobre el número de fotones que es posible generar con este método, siendo 12 el máximo en la actualidad [499]. Se han llevado a cabo en laboratorio experimentos de prueba de concepto con repetidores cuánticos totalmente fotónicos [198, 285, 496] reemplazando el protocolo básico de [18] por una variante más sencilla de implementar. En este protocolo modificado, Alice y Bob preparan cada uno n pares de Bell y envían la mitad de cada par por una fibra a un nodo central C (Charlie). Antes de la llegada de los fotones, Charlie prepara un estado GHZ de $2n$ qubits y realiza una medida de Bell entre los fotones entrantes y el fotón correspondiente en el estado GHZ. El concepto clave en este procedimiento es, en primer lugar, el de medida de Bell adaptativa de tiempo invertido. Si el fotón a_i proveniente de Alice llega al nodo central y la medida conjunta con el fotón c_i de Charlie tiene éxito, entonces Charlie logra una proyección en un estado de Bell. Pero si a_i no llega al nodo central, o si la medida no es fructífera, el analizador de estados de Bell se adapta de forma pasiva para hacer una medida X sobre c_i, que desconecta c_i del estado GHZ. Este hecho conduce a una segunda idea ingeniosa, que los bits exteriores del estado grafo original se pueden eliminar, dejando un estado GHZ en su lugar.

En [285] se demuestra experimentalmente este esquema con un estado GHZ de 4 qubits y 2 canales de comunicación multiplexados. Aunque el experimento no sobrepasa la cota PLOB (por Pirandola-Laurenza-Ottaviani-Banchi [357], $C(\eta) \leq 1{,}44\eta$), el trabajo demuestra una mejora en las tasa de comunicación entre Alice y Bob en comparación con el caso donde Charlie usa un par de Bell para cada canal de comunicación (y, por tanto, no multiplexa los canales). Estos resultados atestiguan el interés y la viabilidad experimental de soluciones completamente fotónicas para las comunicaciones cuánticas.

Sobre el papel, el protocolo precedente simplifica el creado originalmente para los repetidores completamente ópticos, pero en realidad solo sirve si es usa un único QR, lo que implica una

ley de escalado de la forma $\eta^{1/2}$ como mucho, y limita la distancia de comunicación a un máximo de 800 km. Para ir más allá de este límite harían falta varios repetidores y estados fotónicos de muchos más fotones, como los que se postulaban en el protocolo original. Otro inconveniente es que el protocolo es particularmente sensible a las pérdidas locales en el nodo central [198]. Retrasar la preparación del estado GHZ solo solucionaría en parte este problema, la solución total pasa por una corrección de errores tolerante a las pérdidas. En esta línea, [496] acaba de demostrar un repetidor cuántico totalmente óptico con un código Shor de 9 qubits que se puede conectar en serie con otros de igual tipo, y que además es tolerante a pérdidas de fotones individuales. Con todo, faltan algunos pasos prácticos para hacerlo viable, como la generación de ese código Shor de manera señalizada en vez de pos-seleccionada. Para poder transmitir aún más fotones, la aproximación completamente óptica requiere puertas de fusión con las que fabricar grafos estado más grandes a partir de otros más pequeños. El uso de técnicas *feed-forward* es clave en estos esquemas, y estas solo son posibles con conmutadores y dispositivos optoelectrónicos ultrarrápidos.

Las dificultades técnicas de los repetidores bosónicos son algo diferentes a las del repetidor de variable discreta que hemos estado describiendo. Para el caso particular de codificar los qubits en estados GKP, se pueden combinar de manera determinista varios modos en estados grafo grandes mediante operaciones gaussianas (con óptica lineal). Ahora bien, la producción de estados GKP grandes es problemática, y está por demostrarse una implementación en una plataforma enteramente fotónica. En contraste, los estados gaussianos de luz son una tecnología que ya se domina [12].

Una alternativa más para producir estados grafo fotónicos consiste en usar interfaces luz-materia a la manera de [73, 356, 491], que se apoyan en el trabajo de [143, 292, 400]. El procedimiento es más complicado experimentalmente, aunque tiene la ventaja de ser determinista, en principio. En concreto, suponiendo eficiencia unidad en la captura de los fotones y un control perfecto de los emisores cuánticos, el proceso de generación es en efecto determinista y el entrelazamiento entre fotones se produce a través del control del emisor cuántico y no con las puertas de fusión probabilistas. En [404] se expone un experimento de prueba de concepto de esta idea que fue capaz de producir un estado clúster lineal manipulando e impulsando el espín de un pozo cuántico. Los resultados fueron la consecución de un clúster lineal de 3 qubits y la persistencia de entrelazamiento en uno de 5 fotones. Esta cifra ha aumentado recientemente hasta 10 fotones con una indistinguibilidad superior al $90\,\%$ [107]. Otros investigadores han probado a insertar fuentes de fotones entrelazados basadas en pozos cuánticos dentro de microcavidades para generar igualmente un clúster lineal de estados a tasas mucho mayores [109]. Con un sistema parecido a este se han llegado a generar un clúster lineal de 12 fotones y un estado GHZ de 14 fotones [441], que constituyen el récord hasta la fecha del mayor estado fotónico entrelazado medido. Para ir más allá de generar clústeres lineales de estados, se podrían usar múltiples qubits de estado sólido o la fuerte interacción no lineal que inducen los átomos en la luz para realizar las puertas entrelazadoras.

La Tabla 9 recoge un resumen de los parámetros físicos en que cada tipo de repetidor presenta las mejores prestaciones.

4.5. Generación y purificación de entrelazamiento

La producción física de sistemas con qubits entrelazados resistentes a una rápida decoherencia no es sencilla, en general, pero puede llevarse a cabo combinando variadas propiedades

Tabla 9: Rango operativo de los distintos tipos de repetidores cuánticos; ε_G es la probabilidad de error de las puertas cuánticas, η_c es la eficiencia de acoplamiento y t_0 es el tiempo de respuesta de una puerta cuántica.

Rango $(\varepsilon_G, \eta_c, t_0)$	**Tecnologías**
$(\gtrsim 1\,\%, -, -)$	1G
$([0{,}1L_{\text{att}}/L, 1\,\%], \lesssim 90\,\%, -)$	2G sin codificación
$[0{,}1L_{\text{att}}/L, 1\,\%], -, \gtrsim 1\mu\text{s})$	2G sin codificación
$(\lesssim 0{,}1L_{\text{att}}/L, \lesssim 90\,\%, -)$	2G con codificación
$(\lesssim 0{,}1L_{\text{att}}/L, -, \gtrsim 1\mu\text{s})$	2G con codificación
$(\lesssim 1\,\%, \gtrsim 90\,\%, \lesssim 1\mu\text{s})$	3G

cuánticas de la materia o la luz. Puesto que estos procesos afectan directamente a la construcción física de los repetidores y los conmutadores, y por tanto a su capacidad, este apartado revisa algunas de las posibilidades y avances que en esta área se han reportado recientemente.

4.5.1. Generación local de entrelazamiento fotón-memoria

Las memorias cuánticas por sí solas no son suficientes, además debe ser posible acoplarlas a emisores cuánticos cuyas transiciones ópticas permitan la emisión de fotones que estén entrelazados con los qubits contenidos en la memoria. Los qubits fotónicos que se emitan irán codificados en uno de los soportes *single-rail* o *dual-rail* que se discutieron en un apartado anterior. La emisión de qubis con espín entrelazado codificados en formatos de frecuencia fotónica, polarización, *time-bin* y modos espaciales se ha demostrado ya experimentalmente con la ayuda de trampas de iones, centros NV y pozos cuánticos. De entre los muchos esquemas existentes para la producción de fotones entrelazados con los grados de memoria cuántica, revisaremos a continuación los dos más comunes.

En el primero, los fotones entrelazados en polarización se producen con un sistema de los denominados de estructura en forma-Λ, o Λ-sistema. Los estados base $|0\rangle$, $|1\rangle$ del qubit se acoplan ambos ópticamente a un estado excitado $|e\rangle$ mediante fotones con polarización horizontal o vertical, respectivamente. Este tipo de estructura está presente en la mayoría de los emisores cuánticos, incluidas algunas clases de trampas de iones [51], en conjuntos atómicos [92], en centros NV [443] y en pozos cuánticos a los que se aplica un campo magnético transversal [187, 173, 398]. Una memoria cuántica preparada en el estado excitado emitirá espontáneamente un solo fotón con polarización horizontal o vertical, $|H\rangle$ o $|V\rangle$. Tras la emisión, el estado entrelazado del sistema memoria-fotón será $|0, H\rangle + |1, V\rangle$, pero para que este sistema conjunto pueda producir tal estado de entrelazamiento máximo la fuerza de las dos transiciones tiene que ser la misma. Si difieren en energía, como en los pozos cuánticos, entonces el estado resultante está descompensado, es $|0, (H, E_H)\rangle + |1, (V, E_V)\rangle$, donde E_H, E_V son los niveles de energía y (H, E_H), (V, E_V) denotan la codificación redundante del qubit fotónico. La constatación de entrelazamiento bipartito es, en consecuencia, complicada en este caso, porque requiere eliminar esa redundancia.

Aunque es relativamente simple, el esquema que se acaba de describir puede no ser posible en todos los tipos de memoria cuántica, dado que se apoya en un Λ-sistema. Hay no obstante una alternativa [203, 268, 439, 457] que solo necesita una transición óptica y resulta en un

fotón cuyo intervalo de emisión está entrelazado con el qubit de la memoria. El sistema consta en este caso, como mínimo, de tres niveles $|0\rangle$, $|1\rangle$, $|e\rangle$ en el cual solo uno de los estados está acoplado al estado excitado $|e\rangle$. La memoria se inicializa en el estado de superposición $|0\rangle+|1\rangle$ y la transición óptica $0 \leftrightarrow e$ se excita con un pulso, lo que deja al sistema en estado $|e\rangle+|1\rangle$. En el estado excitado, la memoria puede emitir un fotón (en el instante t_1) o no, y el estado final será $|0,t_1\rangle+|1,\text{vacío}\rangle$. En este estado final, se invierte el qubit de memoria para dejar $|1,t_1\rangle+|0,\text{vacío}\rangle$ y la transición $0 \leftrightarrow e$ se excita de nuevo, lo que lleva a la emisión de un fotón en t_0 si el estado excitado no estaba vacío: $|1,t_1\rangle+|0,t_0\rangle$. Es decir, un solo fotón se emite siempre, y es su intervalo de tiempo t_0 o t_1 el que está entrelazado con el qubit en memoria. El único problema de este método es que obliga a preparar la memoria en un estado superpuesto y requiere más pulsos de control, pero tiene en cambio la ventaja de operar con una sola transición óptica, lo cual se adapta particularmente bien a los sistemas de centros NV [48] en los que una de las transiciones ópticas tiene claras ventajas sobre la otra. Este mismo método ha sido ensayado con pozos cuánticos [269].

4.5.2. Generación de entrelazamiento memoria-memoria

Para la generación a distancia de entrelazamiento (con señalización) se usa la detección de fotones, normalmente con dispositivos ópticos lineales e interferencia de dos fotones. Para que esa interferencia pueda dar lugar a entrelazamiento máximo, los dos fotones emitidos por fuentes distantes tienen que ser perfectamente indistinguibles [4, 405]. Entre las demostraciones prácticas de este proceso de generación a distancia se encuentran [418] sobre trampas de iones, [121, 431] con pozos cuánticos, [216] con centros NV y [100] sobre conjuntos atómicos. El experimento de [431] trabaja con dos pozos cuánticos separados por unos pocos metros y ha dado como resultado una tasa de generación de entrelazamiento de $7{,}3$ kHz [431].

Por su interés especial en la aplicación de interconexión de QPUs, veamos con mayor detalle cómo funciona este experimento, que implementa el esquema de [74]. Dos pozos cuánticos A y B se preparan en una configuración denominada Voigt para tener la estructura de un Λ-sistema con niveles de energía en sus transiciones ópticas parecidos. Los dos pozos cuánticos se preparan inicialmente en el estado $|0_A,0_B\rangle = |\downarrow_A,\downarrow_B\rangle$ y son excitados por el mismo láser estabilizado en fase, de forma que se pueda producir un fotón en cada sistema A o B por dispersión Raman con una probabilidad $p \ll 1$. Los modos fotónicos se mezclan luego en un BS 50:50 en un punto central para eliminar la información del trayecto, esto es, para que sea imposible decir quién generó el fotón. El estado antes de la detección del fotón es

$$|\Psi\rangle = (1-p)|\downarrow_A,\downarrow_B\rangle|0_1,0_2\rangle + \sqrt{\frac{p(1-p)}{2}}\left(e^{\imath\Phi_A}|\uparrow_A,\downarrow_B\rangle + e^{\imath\Phi_B}|\downarrow_A,\uparrow_B\rangle\right)|1_1,0_2\rangle$$
$$+\sqrt{\frac{p(1-p)}{2}}\left(e^{\imath\Phi_A}|\uparrow_A,\downarrow_B\rangle - e^{\imath\Phi_B}|\downarrow_A,\uparrow_B\rangle\right)|0_1,1_2\rangle + \frac{p}{\sqrt{2}}e^{\imath(\Phi_A+\Phi_B)}|\uparrow_A,\uparrow_B\rangle\left(|0_1,2_2\rangle - |2_1,0_2\rangle\right),$$

donde $|i_1,j_2\rangle$ con i,j enteros denota el número de fotones en el primer y el segundo modos ópticos del divisor de haz BS y Φ_A, Φ_B son las fases ópticas de los dos caminos de los qubits A y B. Si se detecta un solo fotón, el pozo cuántico se proyecta con probabilidad $\approx p$ en el estado de entrelazamiento máximo $e^{\imath\Phi_A}|\uparrow_A,\downarrow_B\rangle \pm e^{\imath\Phi_B}|\downarrow_A,\uparrow_B\rangle$, con el signo dependiendo del modo de salida del BS en el que se detectó el fotón. En la práctica, p puede no ser tan grande como se desea porque el espín de un pozo cuántico puede sufrir dos inversiones de espín consecutivas con probabilidad p^2, lo que resulta en la emisión de dos fotones. En tal caso, si solo se detecta

uno de los fotones ---ya sea porque la captura es imperfecta, porque ha habido pérdidas o porque la detección no es eficiente--- el proceso lleva a un estado cuya fidelidad disminuye con p. Además de en [431], este método se ha probado en [485] para mostrar la mayor distancia hasta la fecha entre dos memorias cuánticas entrelazadas basadas en conjuntos atómicos. En un experimento posterior se obtuvo una distancia de $L_{\text{att}} \approx 22$ km entre dos memorias cuánticas usando memorias de largo tiempo de persistencia y reduciendo al máximo las pérdidas. Este experimento es extremadamente interesante, además, porque la reducción de las pérdidas se logra con detectores de mejor captura y eficiencia de detección, pero igualmente con la conversión de los fotones a las frecuencias comunes de las telecomunicaciones, que son las que tienen las ventanas de transmisión de mayor transmitancia en las fibras ópticas. Los resultados, en cualquier caso, deben tomarse con cautela, ya que aunque la distancia alcanzada fue de 22 km, se obtuvo con un carrete de fibra, la distancia real entre ambos sistemas era de 1 m.

Existen otros métodos para generar entrelazamiento a distancia con señalización, por ejemplo el método de Barrett y Kok [31] también basado en la detección de dos fotones. Este método se ha comprobado experimentalmente en sistemas de centros NV [48] y de trampas de iones [325], habiéndose alcanzado en el laboratorio distancias de $1{,}3$ km, al igual que en un experimento de prueba de Bell sin *loopholes* [203].

El primero de los esquemas que se han explicado debe operar en el régimen de emisión de fotones de baja probabilidad para poder generarlos con una fidelidad elevada. Por contra, en el esquema de Barrett y Kok el régimen de funcionamiento puede ser el de alta probabilidad de emisión con alta fidelidad. En principio, parecería más adecuado para emisores cuánticos eficientes a cortas distancias. No obstante, para distancias más largas las pérdidas de la fibra empiezan a ser el factor dominante y el primer método tiene un mejor comportamiento según aumenta la distancia comparado con el protocolo de Barrett y Kok.

4.5.3. Purificación del entrelazamiento

En la generación de estados entrelazados entre puntos distantes, la decoherencia o los errores de operación pueden hacer que las memorias cuánticas tengan pares entrelazados con un valor bajo de fidelidad entre ellas. En repetidores 1G la fidelidad se puede incrementar con purificación o destilación de entrelazamiento, a partir de dos copias imperfectas de un par de Bell. Con ellas se puede conseguir un par entrelazado de mayor fidelidad con una probabilidad $1/2$. La prueba experimental de purificación del entrelazamiento se puede explorar en [350, 482] con pares de Bell, en [377] con átomos y en [233] con centros NV. Las distintas realizaciones fotónicas difieren en la tasa de éxito porque es imposible ejecutar una puerta CNOT con óptica lineal. Por eso los protocolos de purificación de entrelazamiento se llevan a cabo con tasas de éxito del $25\,\%$, a lo sumo [349, 482].

[377] da la primera evidencia experimental de purificación de entrelazamiento con memorias cuánticas. En este trabajo se destilan dos pares de Bell de iones $^{9}\text{Be}^{+}$ confinados en la misma trampa de iones, con una probabilidad de éxito por encima del $35\,\%$. Mas como los pares de átomos entrelazados no están separados espacialmente, el método no resulta demasiado bueno para llevarlo a aplicaciones de comunicaciones cuánticas de larga distancia. Usando dos centros NV de espín nuclear con carbono 13 se ha conseguido una purificación de fidelidad $65 \pm 3\,\%$ de un estado de Bell en dos sistemas separados por 2 m. La tasa más elevada que se ha podido lograr experimentalmente es de 182 Hz [428] con trampas de iones separadas por dos metros de distancia, usando un método de interferencia con dos fotones.

Son necesarios múltiples qubits de memoria en cada QR, ya sea para aumentar la tasa de comunicaciones con multiplexación [108] o para permitir la corrección de errores en los repetidores que no son 1G. Un registro cuántico es una memoria cuántica de un número elevado de qubits con tiempo de coherencia grande combinada con un emisor de buenas propiedades y prestaciones. Semejante combinación física se da de manera natural en los diamantes, en los que el defecto se acopla con decenas de núcleos de carbono 13 [61] formando así el registro de qubits (ver de nuevo la Tabla 8). Ha habido una serie de avances en esta línea de investigación, con experimentos en los que el espín nuclear se controla individualmente usando el espín de un electrón [26, 61, 93, 164, 140, 435]. Análogamente, en los sistemas de trampas de iones se ha construido un registro de múltiples qubits usando un emisor acoplado a múltiples qubits de memoria en la misma trampa óptica. Por ejemplo, nodos cuánticos con dos especies de iones son la opción que se estudia en [220, 436]. En los pozos cuánticos, en cambio, el espín solo está acoplado con uno o dos tipos diferentes de iones magnéticos [223], haciendo que aparezca un límite al tamaño del registro. [429] estudia la alternativa de apilar verticalmente varios pozos cuánticos.

En los repetidores 2G y 3G un registro de memoria cuántica de un nodo se puede equiparar a un procesador cuántico que tiene como finalidad generar una codificación lógica de la información cuántica que se transfiere entre los nodos, así como corregir los errores. Un QEC ha sido implementado por [144] en trampas de iones con 9 qubits físicos y 4 más para medidas estabilizadoras, asociados todos ellos con un qubit adicional lógico del código Bacon-Shor en lo que emerge como un sistema tolerante a fallos. Hay también trabajo en desarrollo para construir repetidores con QEC basados en espín de estado sólido [110, 460]. En particular, con defectos en diamantes un experimento reciente ha conseguido demostrar [2] el funcionamiento con tolerancia fallos de un qubit lógico mediante el uso de un código de 5 qubits junto con un protocolo de señalización [87, 88]. El sistema completo emplea 7 qubits en total. Aun así, esta demostración experimental de prueba de concepto está todavía justo por encima del punto de equilibrio en el que las operaciones lógicas con qubits tiene mayor fidelidad que las operaciones físicas con qubits.

Es significativo que los qubits lógicos en los repetidores deben conectarse a interfaces ópticas. Para varias de las plataformas físicas bajo investigación para la realización de procesadores multi-qubit, como pueden ser los circuitos superconductores, uno de los problemas clave a resolver con vistas a las aplicaciones de comunicaciones cuánticas es la emisión de fotones ópticos, que precisa de la transducción cuántica entre energía de microondas y energía óptica [264, 323]. En estudio e investigación está también la materialización de qubits lógicos fotónicos como los que necesitan los repetidores 3G y los repetidores totalmente ópticos en cuanto a la corrección de los errores de pérdidas. La detección de errores se ha comprobado ya experimentalmente [36] y hace poco un código fotónico Shor de 9 qubits se ha implementado experimentalmente como parte de la propuesta de un nuevo repetidor cuántico totalmente fotónico [496].

4.6. Otros avances

Desafortunadamente, el teorema de no-clonación impone un límite estricto al impedir que se puedan corregir pérdidas de qubits físicos por encima del 50%. Se sigue de ello que la reducción de tales pérdidas físicas en una red cuántica es esencial para la implementación y despliegue de aquellos repetidores donde las pérdidas se compensan con QEC. Las pérdidas se

producen en cualquiera de los componentes ópticos, siendo las fuentes principales las pérdidas de propagación y las de acoplamiento causadas por las propiedades inherentes de las fibras y los chips fotónicos. Las pérdidas también se dan en los detectores durante la captura de los fotones que emiten las fuentes.

Las pérdidas en las fibras ópticas son causadas principalmente por absorción infrarroja y dispersión Rayleigh, así como por imperfecciones en la fabricación. Como es bien conocido, las menores pérdidas se producen en la longitud de onda de uso en telecomunicaciones (1550 nm), con un coeficiente de atenuación de $0{,}2$ dB/km, aunque existen fibras de pérdidas ultra-bajas con atenuación de $0{,}16$ dB/km ($0{,}12$ dB/km en laboratorio), que no obstante no tienen mucha difusión. Es claro que tienen que usarse, por tanto, emisores en esa longitud de onda, como algunos de los de pozos cuánticos o de iones de elementos raros o nodos de color en silicio. Como alternativa, cabría plantear el uso de conversores de frecuencia cuánticos, dispositivos que deberían modificar la frecuencia de los qubits fotónicos sin perturbar la información cuántica que portan [217, 314, 375]. Tales conversores de frecuencia están basados por lo general en un cristal no lineal $\chi^{(2)}$ alimentado por un pulso láser de frecuencia ω_ℓ que desplaza la frecuencia ω_i de los fotones de entrada según $\omega_f = \omega_i - \omega_\ell$. Esta técnica se ha utilizado para la conversión de frecuencia de fotones generados por centros NV [439], pozos cuánticos [14, 187, 373, 489], y conjuntos atómicos [136, 218, 438, 485].

La captura eficiente de la luz producida por los emisores cuánticos es otro de los retos tecnológicos a solventar. Puesto que la emisión espontánea no es direccional, la captura de los fotones emitidos tiende a tener una eficiencia baja. La obtención una alta eficiencia en fuentes de emisión de fotones individuales obliga a manipular el ambiente electromagnético en el entorno del dispositivo emisor con el objetivo de forzar la emisión en un modo determinado que se pueda acoplar a la fibra. Eso se puede hacer con guiaondas, que inhiben la emisión fuera de los modos permitidos por la geometría de la guiaonda [9], o bien con microcavidades que adaptan el acoplamiento entre el emisor cuántico y el modo electromagnético confinado en la cavidad. En ambos casos, la emisión de un fotón es mucho más probable dentro de uno de los modos particulares de la cavidad o de la guiaonda que en cualquier otro, y este modo fotónico se puede acoplar con facilidad a la fibra óptica. La solución con microcavidades tiene adicionalmente la importante ventaja de aumentar la probabilidad de emisión de fotones coherentes indistinguibles [379] en comparación con la emisión incoherente asistida por fotones. La eficiencia en la captura de fotones individuales ha aumentado enormemente a lo largo de los años para todos los tipos de emisores cuánticos, gracias a mejoras continuas en la tecnología y los materiales de los dispositivos de cavidad QED [32, 50, 306, 424, 445, 451, 461]. En dispositivos de emisión de pozos cuánticos, trampas de iones y defectos en diamantes, ha superado ya el $50\,\%$.

En relación con esto, conviene mencionar también que las fuentes de conversión paramétrica espontánea ---que no hacen uso de emisores cuánticos--- han visto cómo su eficiencia de captura sube hasta el $67\,\%$ gracias a la multiplexación y la conmutación activa. Pese a que no es posible utilizar estas fuentes en la construcción de una interfaz eficiente luz-materia en un QR basado en qubits de materia, estos dispositivos tienen gran potencial en los equipos totalmente fotónicos. La eficiencia de detección de fotones individuales ha aumentado hasta casi 1 con el desarrollo reciente de los detectores de nanocables superconductores (SNSPD, *Superconducting Nanowire Single-Photon Detectors*) [192]. Se encuentran disponiblescomercialmente dispositivos de este tipo con eficiencias del $95\,\%$. Los sensores de transición poseen igualmente alta eficiencia en la detección, con la ventaja añadida de que tienen resolución en el conteo del número de fotones [293], lo que viene bien para algunos métodos de generación de entrelaza-

miento con señalización clásica.

5. Arquitectura para IC

A la hora de vislumbrar o idear las redes de comunicación cuántica, como se ha mencionado en apartado anteriores, el principal hecho de diferenciador se sitúa en la imposibilidad de leer (postulado de medida) y copiar (teorema de no clonación) información cuántica sin su alteración, lo que, ineludiblemente, repercute en el diseño de la arquitectura de la futura Internet Cuántica. Aunque, en aras de la modularidad y escalabilidad, es de esperar que el diseño de protocolos da datos y control de la IC se adhiera al principio de separación de conceptos, tal diseño no puede sustentarse en lectura y copia de información propio de la pila de protocolos de la Internet clásica. La lectura y copia de la información es ahora reemplazada por el entrelazamiento cuántico, como recurso básico de comunicación, y que soporta lo que podemos denominar los dos mecanismos básicos de comunicación: el intercambio de entrelazamiento y la teleportación.

- Restricciones temporales: Mientras los bits pueden ser almacenados de forma indefinida, los qubits y los estados entrelazados se ven afectado por el proceso de decoherencia, lo que limita su tiempo de vida.
- Restricciones al duplicado: Mientras que los bits pueden ser copiados, el teorema de no clonación imposibilita la copia de qubits. Sin embargo, los estados entrelazados (de estado conocido) pueden ser re-preparados y, por tanto, su duplicación es posible.
- Naturaleza auto-contenida: Mientras bits y qubits son entidades auto-contenidas, en el caso de los estados entrelazados un solo qubit no es útil en sí mismo (es decir, sin el otro qubit en el entrelazamiento).
- Ámbito: Las operaciones sobre bits y qubits tienen ámbito local mientras las operaciones sobre estados entrelazados implican un ámbito no local que afecta al qubit local y al resto de qubits (bipartito o multipartito) en el estado entrelazado.
- Estado: Sin tener en cuenta aspectos relacionados con la combinación de bits en paquetes o el enrutado, los bits son entidades sin estado. Sin embargo, tanto los qubits como los entrelazamientos deben estar necesariamente vinculados a la información de estado que recoge el tiempo residual para la decoherencia. Además, los estados entrelazados necesitan para su operación información sobre las identidades de los nodos involucrados en el entrelazamiento.
- Información: La información codificada en los bits y en los qubits es local y predeterminada, y tiene valor sólo para el nodo destino. A diferencia de lo anterior, el valor de los estados entrelazados es global y dinámico, siendo un recurso de comunicación que tiene valor para los nodos que lo comparten.
- Orden y flujo de información: En el caso de información clásica, el orden de las operaciones es relevante, esto es, la información clásica debe ser recibida en un nodo intermedio antes de ser retransmitida, lo que intrínsecamente implica un flujo de información. En el caso cuántico el orden es flexible dado que el principal recurso de comunicación es el intercambio de entrelazamiento que puede suceder sin ningún orden específico o incluso de forma simultánea.

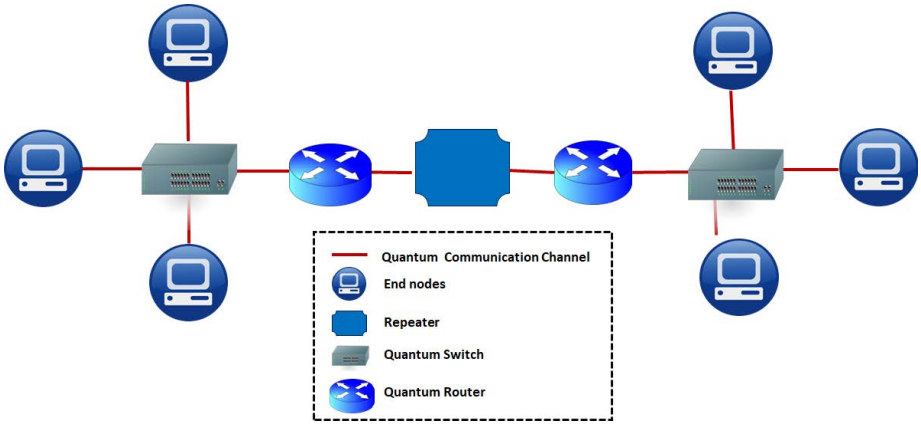


Figura 22: Diagrama de bloques de la IC. Extraída de [488]

5.1. Elementos lógicos de IC

Al igual que la Internet clásica, es previsible que la Internet cuántica (Figura 22 incluya, desde un punto de vista lógico, los siguientes componentes básicos: procesadores cuánticos, canales cuánticos, repetidores cuánticos, conmutadores cuánticos y enrutadores cuánticos. Como ya se ha mencionado, el canal cuántico que habilita la transmisión de qubit recae en la teleportación, lo que conlleva disponer de un enlace cuántico y un enlace clásico. Por un lado, las restricciones de la mecánica cuántica requieren un nuevo catálogo de hardware de comunicaciones; y, por otro lado, la necesaria infraestructura cuántico-clásica requiere mecanismos de sincronización y gestión inexistentes en la Internet clásica.

De acuerdo con el informe QNEXT de Argonne National Laboratory [16], en una futura Internet cuántica en la que los computadores cuánticos serán los extremos de la red, sus nodos se clasifican en 10 tipos de 3 categorías (nodos extremos; repetidores y nodos de soporte). Se describen a continuación en base al informe mencionado [7]. Además de los nodos considerados debemos contemplar los enlaces de comunicación cuánticos y clásicos; así como el plano de control y sus mensajes asociados, que describiremos más adelante.

- En cuanto a los nodos extremo, en una visión a largo plazo análoga a la Internet actual, serán nodos computacionales completos (COMP - *Full computacional nodes*), esto es computadoras cuánticas universales o de propósito general. En el camino hacia el desarrollo COMP, los nodos finales basados en memoria (MEM - *Memory based end-nodes*) son repetidores de interfaz única que se pueden utilizar para aplicaciones específicas. A diferencia de los anteriores, los nodos finales de sensado (SNSR - *Sensor End Nodes*), involucran hardware especializado, por ejemplo, relojes de alta precisión. Por último, los nodos finales de solo medición (MEAS - *Measurement-only end nodes*) seleccionan dinámicamente una base de medición en la recepción de fotones para su uso en QKD, computación ciega, etc.
- En cuanto a los nodos repetidores, el repetidor basado en memoria (REP1 - *Repeater 1G*) es el nodo repetidor estándar de dos interfaces para redes de transferencia bidireccional de

[7] Se recoge una categorización similar en RFC 9340

estado e información (clasificadas como redes 1G), admitiendo protocolos de mitigación de errores limitados, como la purificación de entrelazamientos. Por otro lado, los repetidores habilitados para QEC (REP2 - *Repeater 2G*) habilitan redes que emplean corrección cuántica de errores, clasificadas como 2G o 3G. Por último, la forma más avanzada de repetidor, son los enrutadores (RTR), siendo repetidores basados en memoria, capaz de interactuar con tres o más canales ópticos, incluida la sincronización. Los enrutadores se pueden utilizar en todas las generaciones de gestión de errores.

- Se contemplan también tres tipos de nodo de soporte en concreto los siguientes: (1) analizadores de estados de Bell (BSA - *Bell State Analyzers*), que constan de dos o más detectores y se utilizan para el intercambio de entrelazamiento; (2) fuentes de pares de fotones entrelazados (EPPS - *Entangled Photon Pair Sources*), basadas en procesos ópticos no lineales o emisión directa de fuentes cuánticas, incluidos puntos cuánticos o cascadas atómicas; y (3) nodos de conmutación óptica (OSW - *Optical Switch Nodes*), que permiten la conmutación de fotones individuales (así como señales eléctricas u ópticas clásicas) necesaria para el enrutado. En cualquier caso, la comunicación cuántica depende en la infraestructura clásica de comunicación para el control y coordinación, que operan al nivel de aplicación.

5.2. Hacia el diseño de IC

La tabla en la figura 23 representa la complejidad de los distintos componentes de red mencionados, así como la relación de su rendimiento (gradiente de color) con la madurez de la red. A un alto nivel de abstracción, en base a estos componentes, la arquitectura de IC debe definir el servicio de trasmisión de información cuántica, la interconexión entre redes heterogéneas y la gestión de la fidelidad. Para ello, es necesario la definición de los protocolos, la corrección de errores, el enrutado y multiplexación de información cuántica y la seguridad de las operaciones de red. En la definición de IC se persigue un sistema robusto, escalable, seguro, autónomo y manejable, entre otras características que permitan la interoperación de redes a largo plazo. No se trata de resolver sólo el problema de la comunicación cuántica, sino de la interconexión de distintas redes cuánticas, posiblemente heterogéneas. A este respecto, hoy existen distintas posibilidades abiertas entre las que se encuentra el uso de la teleportación frente a los grafos de estados multipartitos, el intercambio de entrelazamiento con purificación frente a conexiones puramente fotónicas si memorias cuánticas.

Previo a la descripción de las distintas aproximaciones propuestas para el diseño de IC, en la Figura 24 se recogen las fases en el desarrollo de las redes de comunicación cuántica, tal y como se enuncian en [470]. A pesar de que desde 2018 la literatura y los avances han sido numerosos, la figura permite entender el camino y el esfuerzo investigador por delante. Las distintas fases se conciben como un aumento de funcionalidad sobre las fases precedentes, y no un mero cambio de parámetros o de escala. En la primera fase de desarrollo, denominada redes con repetidores confiables, se concibe una red de transmisión de qubits extremo a extremo. Esta fase se alinea con los avances QKD, e.g. [395], y persigue una seguridad teórica de la transmisión de información extremo a extremo mediante el uso de enlaces cuánticos, siempre y cuando se disponga de nodos intermedios confiables ya que estos tienen acceso a la información transmitida. Los nodos intermedios confiables desempeñan así el papel de repetidores confiables clásicos (dado que el esquema QKD es de un solo salto) y no se incluyen repetidores

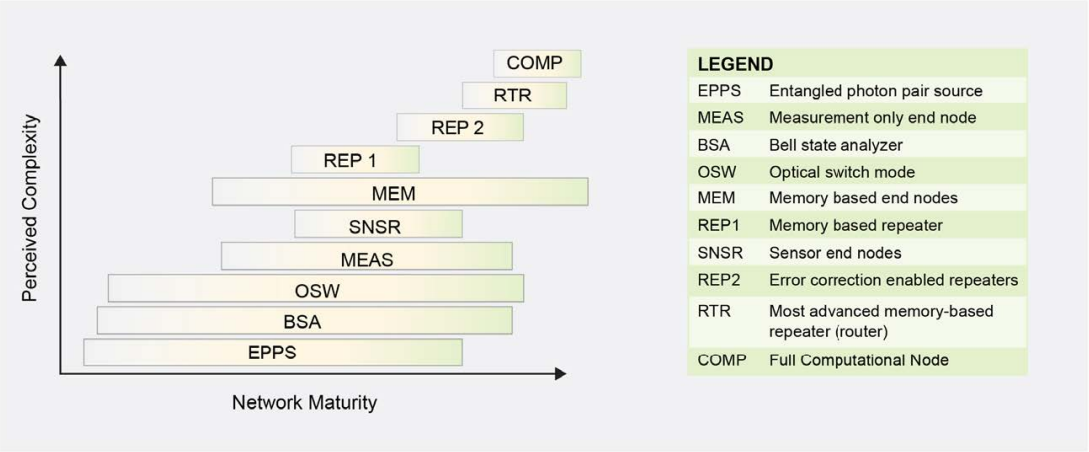


Figura 23: Complejidad de los componentes de red. Extraída del informe QNEXT de Julio del 2022 [16].

cuánticos. Aunque en esta primera fase no se aborda una funcionalidad de transmisión cuántica extremo a extremo, ha alcanzado éxito industrial en distintas infraestructuras QKD.

En ese mismo ámbito de aplicación, QKD, la segunda fase de desarrollo contempla las redes de preparación y medida, que eliminan la necesidad de contar con un repetidor confiable y permiten que un nodo extremo prepare un estado qubit y lo transmita al otro extremo para su medida. Más formalmente, para cualquiera dos extremos i y j; cualquier estado $|\Psi\rangle$; y cualquier medida M, i puede preparar $|\Psi\rangle$ y transferirlo a j de forma que o bien (1) j realiza la medida M o (2) j puede concluir que el qubit se ha perdido.

La tercera fase en el desarrollo de la IC pasa por el uso del entrelazamiento cuántico, en lo que se conoce como redes de distribución de entrelazamiento, donde o bien se asume la generación determinista de entrelazamiento o un modelo menos estricto basado en generación señalizada (*heralded entaglement*). Más formalmente, para cualquiera dos extremos i y j (1) la red permite la creación y anuncio de un estado de entrelazamiento máximo $|\Phi_{ij}\rangle$; y (2) los nodos i y j pueden realizar medidas de los qubits individuales (M_i, M_j) de forma determinista. Las redes de distribución de entrelazamiento incluyen, por generalización, la generación de estados entrelazados multipartitos sin memoria. La distribución de entrelazamiento soporta la creación de redes sin la restricción de nodos intermedios confiables dado que los dispositivos pueden registrar entradas y salidas, pero no pueden enviarlas a un adversario.

La concepción de memorias cuánticas habilita la cuarta fase de desarrollo, redes con memorias cuánticas, donde se admitiría una mayor complejidad de los protocolos al permitir el almacenamiento temporal de estados cuánticos. Más formalmente, para cualquiera dos extremos i y j (1) la red permite la generación de entrelazamiento y las siguientes tareas adicionales: (1) preparación de un estado auxiliar $|\Psi\rangle$ por parte de i o de j; (2) medidas de cualquier subconjunto de qubits en el nodo; y (3) aplicación de una operación unitaria U. Se considera que el almacenamiento de los qubits está limitado por un valor temporal dependiente del tiempo

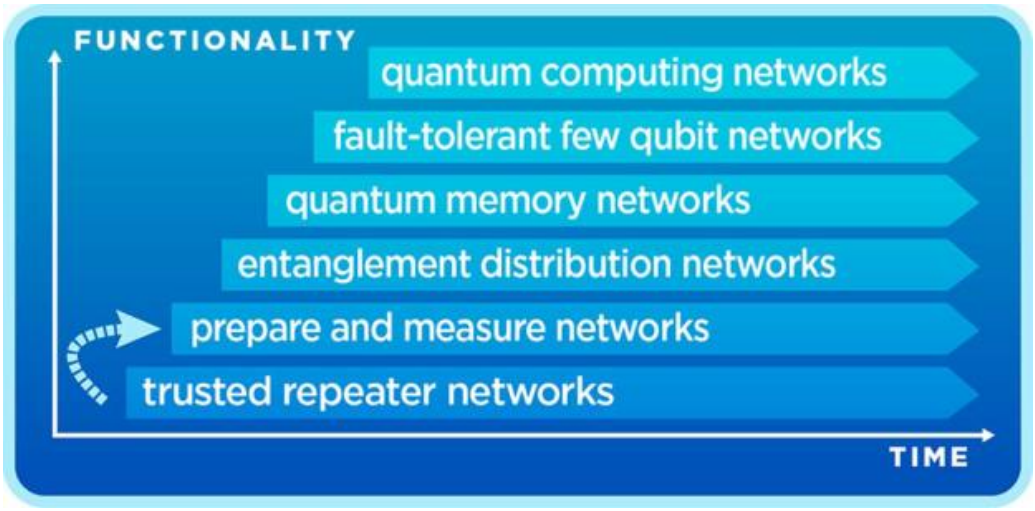


Figura 24: Estados en el desarrollo de la IC. Extraída de [470].

invertido en la generación EPR y la ejecución de circuitos cuánticos. La diferencia crucial frente a las fases anteriores es la capacidad de transmitir qubits no conocidos de un nodo a nodo, abriendo las puertas a protocolos de distribución de tareas, la purificación del entrelazamiento y la generación de estados entrelazados multipartitos. Las redes con memorias cuánticas amplían el ámbito de aplicación a tareas criptográficas, computación ciega, compartición de secretos, transmisión anónima, sincronización de relojes, mecanismo de elección, etc.

Se puede considerar que las fases descritas son estado de la práctica, o al menos estado del arte, de éxito; esto es, las redes de comunicación cuántica se encuentran hoy en este punto intermedio. Resta por tanto avanzar para las últimas dos fases en la figura. Las redes tolerantes a fallos de número reducido de qubits proporcionarían la funcionalidad adicional de una ejecución tolerante a fallos de un conjunto de puertas universales sobre q qubits donde q es lo suficientemente pequeño, aunque mayor que 1, para que el procesador cuántico puede pueda ser simulado de forma eficiente en un computador clásico. Esta tolerancia a fallos permite reducir los errores de las redes basada en memorias cuánticas y abre las puertas a protocolos de aplicación para computación cuántica distribuida.

El estado final de esta línea de tiempo son las redes de computación cuántica, donde los computadores cuánticos (COMP) se conectan arbitrariamente vía comunicaciones cuánticas. En dicha fase, la IC permitirá la resolución de problemas en sistemas distribuidos de forma incomparablemente eficiente dado que el entrelazamiento permitirá la coordinación de procesadores a grandes distancias, superando las restricciones clásicas. En [16] QNEXT identifican los avances experimentales necesarios en las comunicaciones cuánticas para alcanzar dicho estado final:

- Demostración de la comunicación cuántica basada en repetidores con probabilidades de éxito superiores a la comunicación cuántica directa. En [364] se recoge un experimento de una red cuántica con 3 nodos en la que se distribuyen con éxito en estado multipartitos y se consigue conectividad total entre los nodos vía intercambio de entrelazamiento.
- Además de la eficiencia de la distribución del entrelazamiento, es necesario demostrar su

ventaja práctica en términos de velocidad en el caso de larga distancia (interurbana), esto es, superando la velocidad sin la inclusión de repetidores.

- Desarrollar (optimizar y estandarizar) una arquitectura de IC con posiblemente múltiples arquitecturas de red que inter-opere en una arquitectura IC única, como sucede en la Internet Clásica. Una vez alcanzados estos hitos, restaría la realización de una red cuántica multi-nodo homogénea, y posteriormente heterogénea, a escala interurbana para finalmente llevar a la red de redes cuánticas a nivel global (heterogénea, tolerante a fallos, estandarizada, etc.), esto es, la Internet cuántica

5.3. La pila de protocolos IC

La primera propuesta de diseño de la pila de protocolos de la IC se localiza en el grupo de investigación en Teoría de la Información y de las Comunicaciones cuánticas de la Universidad de Keio [8] (Japón) [316] sobre un arquitectura de repetidores cuánticos basada en intercambio de entrelazamiento y purificación. Se conciben tres capas: (1) la capa de entrelazamiento físico (*PE- Physical Entanglement*); (2) la capa de generación de entrelazamiento; la capa de control de entrelazamiento (*EC - Entanglement Control*), responsable de medir/determinar si la generación de entrelazamiento fue exitosa o no; la capa de control de purificación (*PC - Purification Control*), que gestiona la purificación por entrelazamiento; y la capa de control de intercambio de entrelazamiento (*ESC - Entanglement Swapping Control*), encargada tanto del intercambio de entrelazamiento y de la teleportación. En resumen, el entrelazamiento y su control actúan recursivamente sobre enlaces de un solo salto, mientras que el control de purificación y el intercambio de entrelazamiento actúan recursivamente sobre múltiples saltos. Tras esta primera propuesta, diversos autores han propuesto versiones más avanzadas que se resumen a continuación. La depuración y el intercambio (PC y ESC) se repiten en cada nivel hasta que se alcanza el nivel superior, de extremo a extremo, como se muestra en la figura 25. Como se muestra en la figura la propuesta no respeta uno de los principios del diseño de la pila de protocolos de la IC, esto es, la clara separación entre capas. Esta forma de recursividad, que se observa también en otras propuestas, está relacionada con el hecho que el fenómeno de entrelazamiento (una forma de comunicación) es en sí un recurso de comunicación.

5.3.1. Modelo en capas basado en entrelazamiento bipartito

Una propuesta alternativa en capas se localiza en los trabajos de QuTech. La primera aproximación madura de este grupo [116], propone una serie de capas con correspondencia clara con la Internet clásica, tal y como se recoge en la Figura 26, para un esquema de comunicación basado en entrelazamiento bipartito. La capa física se encarga de la generación de entrelazamiento bipartito utilizando nodos autónomos que se coordinan mediante un protocolo de anuncio (MHP – *Midpoint Heralding Protocol*). Los nodos autónomos utilizan MHP para sondear la capa de enlace a intervalos de tiempo pre-definidos y determinar si es necesaria la generación de entrelazamiento. La capa de enlace es responsable de la generación de entrelazamiento robusto para lo que se define el protocolo QEGP (*Quantum Entanglement Generation Protocol*). El procolo QEGP recibe una solicitud de entrelazamiento hacia un nodo remoto así como los parámetros deseados (número de pares entrelazados, fidelidad mínima, base de medición, etc.).

[8] https://takeoka.elec.keio.ac.jp

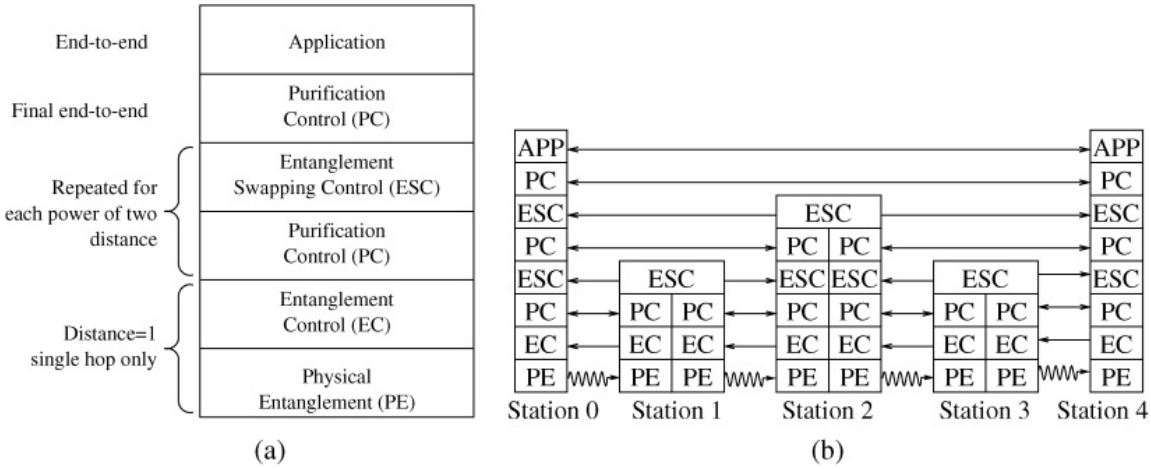


Figura 25: Estructura en capas para IC de Keio University, 2009 [316].

Encima de la capa de enlace, la capa de red es responsable de proveer entrelazamiento a más de un salto, por ejemplo, con intercambio de entrelazamiento y de monitorizar los recursos de entrelazamiento dentro de la red. Finalmente, la capa de transporte transmite los qubits, e.g. por teleportación, de acuerdo con las peticiones de la capa de aplicación. Este y otros trabajos del grupo de investigadores en QuTech se centran fundamentalmente en las capas físicas y de enlace, y se han respaldado con pruebas experimentales [365]. La evaluación experimental corrobora el equilibrio entre la latencia experimentada para generar el entrelazamiento y la fidelidad del estado entrelazado generado; y desvela la sobrecarga de latencia resultado de la interacción entre la capa física y de enlace. Cabe mencionar, que de acuerdo a los principios básicos de diseño, se define una pila de protocolos independiente del hardware, al igual que sucede en la Internet clásica, mediante una capa adicional HAL (*Hardware Abstraction Layer*) que permite abstraer los protocolos en la capa de red de los detalles físicos de implementación del hardware.

Los autores definen además en [257] una arquitectura de alto nivel para un nodo cuántico (Figura 27) en el que se representan las operaciones relacionadas con la generación de estados de entrelazados en base a primitivas del Sistema Operativo. Tras recibir una solicitud de entrelazamiento (de la capa de aplicación o de otro nodo), la operativa debe realizar dos tareas fundamentales: (1) coordinación con los nodos cuánticos vecinos; y (2) ejecución de instrucciones para la generación de estados entrelazados y el intercambio de entrelazamiento. En base a esta arquitectura de nodo, la capa de aplicación sobre el SO contempla dos categorías se aplicaciones: *Measure directly*, aplicaciones caracterizadas por el consumo de pares de Bell mediante su medida; y *Create and keep*, aplicaciones caracterizadas por la necesidad de almacenamiento de pares entrelazados para el envío de qubits de información vía teleportación. El plano de datos propuesto es soportado por un plano de control que incluye (1) un protocolo de enrutamiento que determina el camino óptimo para la generación del entrelazamiento extremo a extremo, donde el parámetro más relevante es la fidelidad del camino; Y (2) un protocolo de señalización que establece un circuito virtual entre los nodos extremos y que determina un protocolo orientado a conexión.

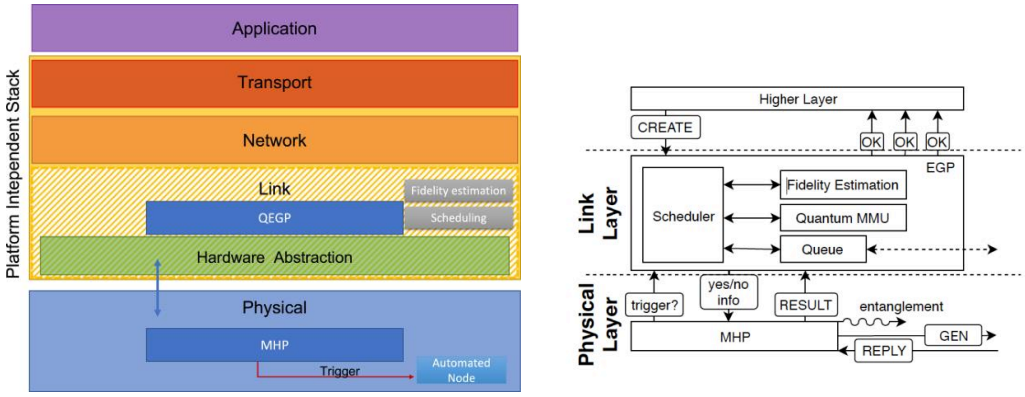


Figura 26: Estructura en capas de Internet Cuántica de QuTech. Figuras extraídas de [116] y de [219].

5.3.2. Modelo en capas basado en entrelazamiento multipartito

A diferencia de los dos modelos anteriores, las propuestas de pila de protocolos IC formuladas por el Instituto de Física Teórica de la Universidad de Innsbruck [359, 358] se basan en el entrelazamiento multipartito GHZ. En este caso se trata de un escenario a priori donde un recurso de entrelazamiento, al que se denomina estado de red, se distribuyen antes de cualquier solicitud; y es tal que cualquier estado grafo puede generarse a partir de él. Se trata de un enfoque más cercano a la Internet clásica, esto es, los dispositivos de red manipulan el recurso de entrelazamiento de forma colaborativa y distribuida para satisfacer las peticiones de los clientes, que son pasivos (solicitan estados grafo, no los construyen). Se puede considerar que, al igual que la propuesta anterior, se trata de una arquitectura dirigida por peticiones. Esto es, la capa de aplicación solicita un estado grafo a la red cuántica que realiza la generación de forma colaborativa y distribuida, suponiendo que el recurso de entrelazamiento está disponible y que, por tanto, no se requiere un tiempo adicional para su creación . De esta forma, el tiempo para generar el estado grafo multipartito depende exclusivamente de de la comunicación clásica entre dispositivos para la coordinación. Sin embargo, este enfoque requiere que los recursos de entrelazamiento distribuidos en los nodos de red sean tales que permitan generar cualquier estado grafo multipartito. Se trata de un enfoque top-down donde el entrelazamiento es un recurso universal siempre disponible a diferencia de otros enfoques bottom-up donde los recursos de entrelazamiento se generan bajo demanda, por ejemplo [149], lo que requiere alguna forma de coordinación a priori. Dado que un escenario de funcionalidad genérico puedo ser costoso, porque se debe habilitar la comunicación de cualesquiera conjunto arbitrario de nodos, en [320], lo investigadores proponen algoritmos de para la identificación óptima de clústeres de nodos conectados que permitan satisfacer una funcionalidad específica, aportando una importante reducción en el tiempo y recursos necesarios para el establecimiento de los recursos de entrelazamiento multipartito necesarios.

Al basarse en entrelazamiento multipartito, la propuesta define nuevos elementos de red, en concreto conmutadores de estados grafo y enrutadores de estados grafo. Los clientes se conectan a los dispositivos de infraestructura de red cuántica mediante entrelazamientos, e.g. pares de Bell, mientras que los dispositivos de red, enrutadores y conmutadores, utilizan un

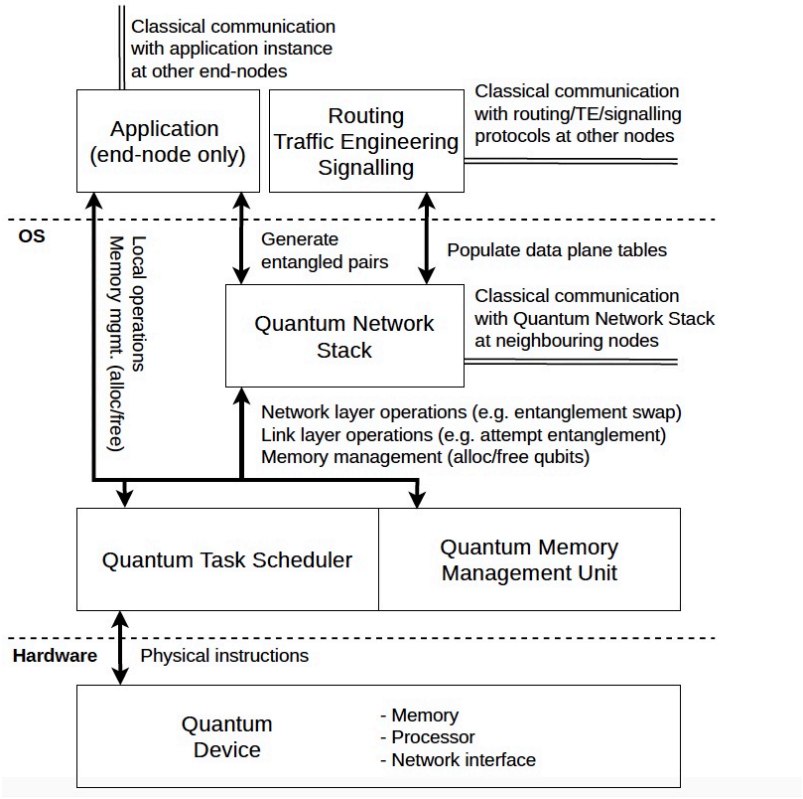


Figura 27: Componentes de un nodo cuántico. Extraída de [257].

estado cuántico multipartito interno y se conectan entre sí mediante entrelazamiento multipartito. A modo de ejemplo, en la Figura 28, se representa una red, donde los clientes se conectan a través de pares Bell a los dispositivos de red, y dispone de tres conmutadores (flechas horizontales) y un enrutador (flechas diagonales) conectados a través de estados GHZ (líneas negras indican entrelazamiento). Internamente cada dispositivo de interconexión utiliza también estados GHZ para la conexión de tres clientes. Tal y como se corresponde al concepto de conectividad virtual en una red cuántica, la estructura de entrelazamiento de la red es diferente de la configuración del canal físico (tubos de color naranja).

La red evoluciona según tres fases: dinámica, cuando el entrelazamiento se genera y distribuye por toda la red; estática, donde algunos dispositivos comparten pares entrelazados para satisfacer futuras demandas; y adaptativa, cuando se opera sobre los estados entrelazados para, principalmente, satisfacer las solicitudes cliente. Para este ciclo de vida, la operativa se organiza en cuatro capas 29: (1) la capa física consistente en los canales físicos cuánticos (estática); (2) la capa de conexión, que establece entrelazamientos a larga distancia a través de repetidores cuánticos y destilación de entrelazamiento (estática); (3) la capa de enlace, que se encarga de generar y distribuir los estados entrelazados multipartitos (dinámica) y de generar estados grafos en base a las solicitudes de clientes (adaptativa); y (4) la capa de red, respon-

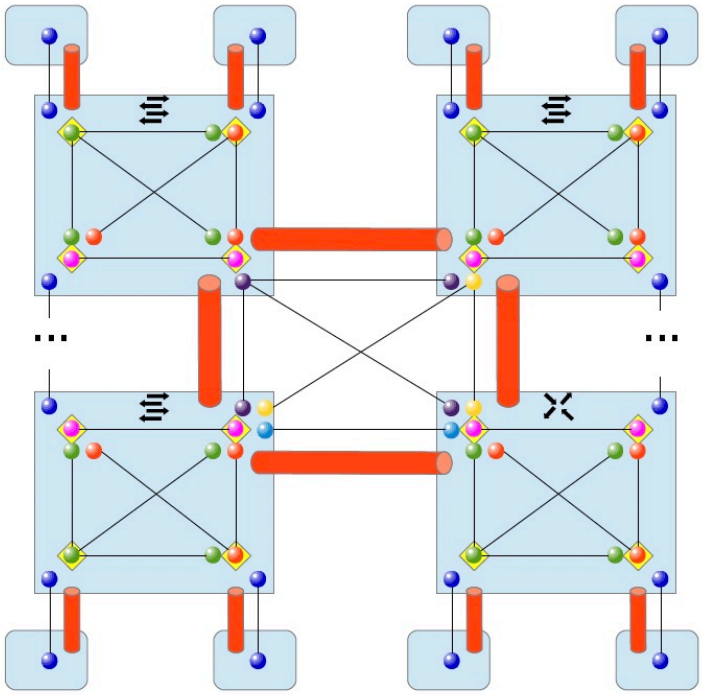


Figura 28: Ejemplo de red con entrelazamiento multipartiro. Extraída de [358].

sable de establecer el entrelazamiento entre redes a través de enrutadores de estados grafo. Además, las distintas capas pueden utilizar protocolos auxiliares para la destilación e intercambio de entrelazamiento, así como monitorizar el estado de la red. Para la configuración de la red se define un protocolo específico, similar a DHCP *Dynamic Host Configuration Protocol*, referido como QNCP (*Quantum Network Configuration Protocol*) [359] que permite la distribución del estado de red mediante un conjunto de servidores QNCP

5.3.3. Modelo en capas recursivas

A diferencia de los modelos anteriores, en capas, el modelo de Van Meter [318] se reformula como un modelo recursivo de generación y distribución de estados entrelazados, al que se denomina *Quantum Recursive Network Architecture* (QRNA). La idea bajo la arquitectura propuesta emana de la definición de conectividad virtual y aumentada que revisamos anteriormente. El intercambio de entrelazamiento cuántico subsume un conjunto de pares entrelazados a través de repetidores en un par entrelazado final, es decir un par EPR de alta fidelidad compartido entre fuente y destino. Por lo tanto, en la capa de aplicación, la cadena de repetidores colapsa en un solo nodo, el destino. Esta arquitectura recursiva abstrae las subredes a nodos individuales virtuales (Figura 30), y unifica las capas de software a través de llamadas recursivas a las dos primitivas principales, intercambio de entrelazamiento y purificación. El uso de recursividad también se ha utilizado en la Internet clásica para distintas formas de virtualización, por lo que

Network stack	Network device	Protocol	Goal/Responsibility	Auxiliary
Network layer	Router	Region Routing Hierarchical Regions Reliable Regions	Enable for inter-network graph state requests	Entanglement distillation protocols Reachability (Ping)
Link layer	Switch	State linking Reliable state linking Quantum network configuration	Generate arbitrary graph states on request in a network	
Connectivity layer	Repeater	Encoded direct communication Repeater protocols	Ensure point-to-point or point-to-multipoint connectivity	
Physical layer	Channel		Physically connect quantum networking devices	

Figura 29: Pila de protocolos con entrelazamaiento multipartiro. Extraída de [358].

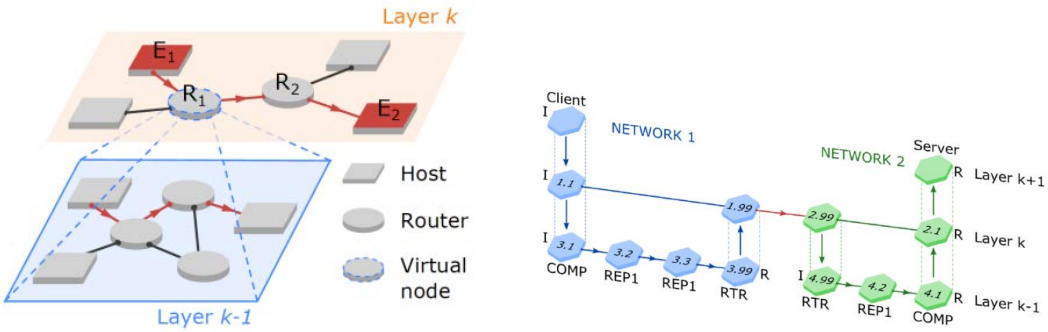


Figura 30: Aproximación QRNA que virtualiza una red como un nodo individual virtual y establecimiento de conexión multinivel. Extraída de [318].

su aplicación en la IC se considera acorde al concepto de conexión virtual. Se propone:

- Una jerarquía de redes lógicas superpuestas formadas por enlaces punto a punto (con pares de Bell entre ellos) en la que tienen cabida tanto redes cuánticas tipo overlay como conexión entre redes (internetworking), donde cada red es vista como un nodo virtual que pone en práctica los mismos principios.
- Un lenguaje de programación basado en reglas similar al de las redes definidas por software (SDN), extendiendo su semántica para para indicar a cada nodo (real o virtual) las operaciones a realizar sobre los recursos de entrelazamiento y los qubits: crearlos, medirlos, transferirlos, nombrarlos, etc. De acuerdo con el principio arquitectónico, el conjunto de reglas también es recursivo, esto es, una regla puede llamar a otra.

Entendida la IC como como un servicio para construir entrelazamientos extremo a extremo, se define un lenguaje de reglas (condición – acción) análogas a las utilizadas en redes SDN. Para cada nodo, un conjunto de reglas (*RuleSet*) determina las acciones locales del nodo ante la ocurrencia de los eventos vinculados a la recepción de mensajes (entrelazamiento con éxito, timeout, etc.); los estados entrelazados están vinculados a una etapa de procesamiento (*Stage*). Cuando se activa una regla para un estado entrelazado en una *Stage* específica, el estado pasa

a la siguiente etapa o bien se considera extinto (consumido por el protocolo o con error). Como se muestra en la Figura 30, el establecimiento de conexión en cualquiera de los niveles se define en un proceso en do pasos, un primer paso (`Initiator`) para recabar información de los enlaces y recursos disponibles para alcanzar el destino (`Responder`); el cual construye los `RuleSets` para cada uno de los nodos en el camino y los distribuye en el segundo paso.

El lenguaje de reglas, de forma a similar a lo que sucede en la Tnternet clásica, necesita una identificación única para los qubits físicos, que se define como el par `<QNICAddress, QubitIndex>`, identificando la interfaz de red cuántica y el índice del qubit en dicha interfaz. Adicionalmente, para la identificación de los estados entrelazados se propone como nombramiento `<NodeAddress, Timestamp>` cuya marca de tiempo tiene la precisión suficiente para identificar unívocamente un par de Bell. En la propuesta de referencia se recogen todos los detalles sobre esta operativa que se resume en la Tabla 10. Sobre el mecanismo de nombramiento y el lenguaje de reglas, se define una API de *sockets* cuánticos como analogía a la API de *sockets* clásica con las funciones estándar: creación de un externo de *socket*, lectura, escritura, opciones y destrucción del socket. La API opera sobre nodos de que devuelven información clásica (MEAS, SNSR), en cuyo caso es síncrona dado el resultado es clásico (lecturas, llamadas al sistema, etc.); y sombre nodos COMP cuánticos donde la necesidad de coordinación requiere un procesado asíncrono.

5.3.4. Circuitos vs paquetes

En [219] se recoge una comparativa de las anteriores propuestas académicas para la IC. Más allá de los detalles particulares, la comunidad académica parece decantarse por una arquitectura similar a la conmutación de circuitos en las redes clásicas, donde un camino de comunicación dedicado es establecido de forma previa a la transferencia de datos. Bajo un enfoque de conmutación de circuitos, e concibe una pila de protocolos donde la capa física es responsable de la generación de entrelazamiento con dispositivos clásicos y cuánticos; la capa de enlace se encarga del entrelazamiento robusto; la capa de red extiende, mediante intercambio de entrelazamiento. a entrelazamiento multi-salto; la capa de transporte implementa la transmisión confiable de qubits por teleportación; y la capa de aplicación da soporte a servicios y aplicaciones sobre las capacidades de red clásicas y cuánticas. Aunque se considera que el principio de no clonación ha llevado a aproximaciones basadas en la conmutación de circuitos, la comunidad científica también trabaja en aproximaciones cercanas a la conmutación de paquetes. De forma destacable, en [128] se propone una estructura de trama híbrida (clásico-cuántica) con una cabecera clásica, un *payload* cuántico y una cola que marca el final de la información cuántica. Como es habitual la cabecera contendría información de enrutado y de mitigación y corrección de errores. En la Figura 31 se representa el nodo fuente de la trama híbrida, así como la multiplexación: (1) en tiempo de la señal clásica y la señal cuántica, donde el encabezado se enviará antes que el *payload* cuántico; y (2) en el espacio, donde las dos señales se envían simultáneamente en diferentes longitudes de onda. En sí, el trabajo sólo se centra en la capa física con la definición del multiplexor, por lo que la conmutación de paquetes como posibilidad menos explorada para las redes cuántica necesita todavía contribuciones adicionales que atesoren su viabilidad.

5.4. RFC 9340

A pesar de que no existe un consenso en la arquitectura que regirá la IC, sus principios arquitectónicos se recogen en la siguiente RFC 9340 [256]) del IRTF (Internet Research Task Force)

Tabla 10: Quantum RuleSet

Mensajes del protocolo			
Nombre	**Nombre descriptivo**	**Argumentos**	**Comentarios**
Eventos remotos (transmisión de mensajes)			
free	Liberar un estado	Partner addr., resource ID	Release a state back to the free pool. Used after purification
update	Notificación de cambio de estado	Partner addr., resource IDs, Pauli frame correction	Used to indicate a Pauli frame correction to a state. Most commonly used with transfer to complete entanglement swapping
meas	Resultado de una medida	Partner addr., resource IDs, result	Exchange purification results. Each partner sends this message, and a separate rule will recognize whether purification results agree and proceed appropriately. Numerous types are possible
transfer	Notificación de transferencia de entrelazamiento	Partner addr., resource IDs	Distribute the result of a swapping circuit. Generalizes to a notice of entanglement transfer from one location or partner to another. Carries a new resource ID to use for the resulting state
Cláusulas de condición			
Nombre	**Nombre descriptivo**	**Argumentos**	**Comentarios**
Eventos remotos (transmisión de mensajes)			
cmp	Comprueba si una variable es igual, menor o mayor que un valor	variable ID, comparison operator, value	Used to track number of operations done (e.g., purification count, measurement count, or number of notification message received
timer	Expiración de un temporizador	Timer ID	Must be used with caution when dealing with distributed states; race conditions can occur
Eventos de estados cuánticos (hardware local, notificaciones, recepción de mensajes			
res	Suficientes recursos	Partner addr. (or wildcard) and fidelity	Matches Bell pairs. Used commonly for purification and entanglement swapping. Used to check fidelity of Bell pairs, this also serves as the primary "meets application requirements" clause for delivering to apps at EndNodes
Cláusulas de acción			
Nombre	**Nombre descriptivo**	**Argumentos**	**Comentarios**
acciones software locales (clásicas)			
settimer	Set timer	Timer ID	Use with caution; distributed race conditions can occur
promote	Promoción de qubits	Qubit IDs, Rule ID, Stage	Used to transfer the control/ownership of qubits from current Rule (Stage) to another Rule (Stage)
free	Liberar qubits	Qubit IDs	Release qubits to the pool of unallocated resources
set	Cambiar el valor de una variable de Rule/RuleSet	variable identifier	Can be used to track how many measurements have occurred for tomography
acciones hardware locales (cuánticas)			
meas	Medir qubits	Qubit IDs, measurement basis	Measure one or more qubits in specified basis or a randomly chosen one
qcirc	Aplicar un circuito cuántico	Qubit identifiers, Qcircuit	Apply a general unitary quantum operation on one or more qubits, without measuring. Bell state measurement, purification, and entanglement swapping execute qcirc first, then meas. Encoding into logical qubits also uses.

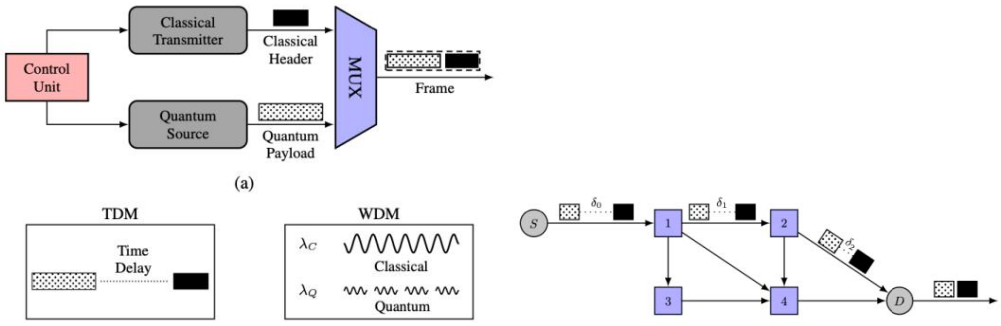


Figura 31: Esquema base para un modelo de redes cuánticas basado en conmutación de paquetes. Extraída de [128]

de IETF (Internet Engineering Task Force) que aloja el grupo Quantum Internet Research Group (QIRG) desde marzo de 2018. El ámbito de su trabajo se sitúa en los aspectos de diseño y construcción de redes cuánticas más ligados a la ingeniería de red clásica dado que es plausible que los principios bajo el enrutado, la reserva de recursos, el establecimiento de conexión, etc. sean trasladables a las redes cuánticas. Además, estas redes cuánticas estarán embebidas en redes clásicas en tanto en cuanto requieren comunicación tradicional para su gestión. El objetivo principal de QIRG es el desarrollo de un marco arquitectónico que delimite la definición y el rol de los nodos en la red de comunicación cuántica como primer paso hacía una arquitectura de red completamente basada en entrelazamiento. En el camino hacia ese objetivo final, QIRG también trata un escenario intermedio con repetidores confiables (esto es, si intercambio de entrelazamiento). QIRG define IC como una red de redes cuánticas que previsiblemente se integrará en la Internet clásica para la mejora de las aplicaciones tradicionales y para la ideación de nuevas aplicaciones cuánticas. Actualmente IRTF trabaja en dos documentos: (1) RFC 9340 "*Architectural Principles for a Quantum Internet*"; y (2) Internet Draft "*Application Scenarios for the Quantum Internet*".

La visión en la RFC 9340 no es exactamente una IC sino la mejora de Internet existente permitiendo la comunicación cuántica entre dos puntos cualesquiera, a pesar de que ello implique construir desde cero la pila de protocolos en base al principal recurso de comunicación, el entrelazamiento cuántico. Los principios de esta Internet cuántica se resumen según la RFC, como sigue:

- El servicio fundamental de la IC es el entrelazamiento y su distribución entre los nodos de la red cuántica;
- los pares de Bell son indistinguibles, lo que implica la coordinación de los nodos para garantizar la operación sobre qubits en el mismo estado de Bell;
- la fidelidad es parte del servicio, de forma que un servicio puede operar siempre y cuando la fidelidad supere un cierto umbral sin necesidad de corregirla;
- (4) el tiempo es un recurso caro debido a la baja tasa de generación de pares de Bell, el reducido tiempo de vida de las memorias, etc. y

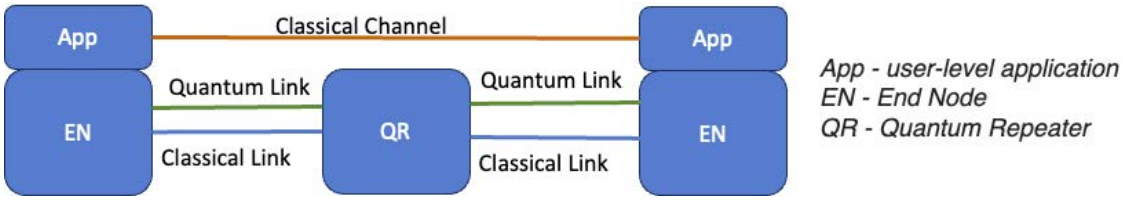


Figura 32: Comunicación en dos saltos

- (5) la IC debe ser flexible frente a las capacidades y limitaciones actuales dado que se espera sean superadas en el futuro.

Bajo esos principios, la RFC recoge también los retos principales:

- La necesidad de un canal clásico para el envío de la información de control, dado que a diferencia de los paquetes de la Internet clásica (con cabecera), los pares entrelazados son un mero recurso de comunicación sin información de control asociada. Tal información de control es necesario para la comunicación a más de un salto y para la corrección de errores;
- la gestión de estado es diferente a la Internet clásica donde la comunicación se materializa salto a salto de forma direccional; por el contrario el modelo "*Store and swap*" de la IC requiere la gestión de información de estado que garantice que los intercambios de entrelazamiento son los adecuados para la comunicación extremo a extremo;
- la necesidad de coordinación de los dos extremos en el entrelazamiento; mientras que en la Internet clásica la información en u n paquete existe un único punto y puede ser modificada, en la IC las operaciones en uno de lo qubits entrelazados modifican el estado mutuo por lo que se deben coordinar entre los dos nodos que contiene los estado entrelazados;
- y la generación de entrelazamiento requiere estados temporales que permitan almacenar los estados cuánticos hasta que la información de control sea recibida.

En consecuencia, los nodos cuánticos deben tener doble conectividad (Figura 32) clásico-cuántica y el modelo de red contempla un plano de control (gestión de recursos, topología de red, etc.) que puede operar mediante el intercambio de mensajes clásicos, y dos planos de datos: plano de datos cuántico (procesamiento e intercambio de pares entrelazados; así como anuncio) y plano de datos clásico en el que una aplicación en dos nodos extremos conectados por una canal clásico necesita la generación de pares entrelazados. La red utiliza enlaces clásicos para coordinar la generación de pares entrelazado extremo a extremo, y enlaces cuánticos para la generación y el intercambio de los pares entrelazados. Sobre este modelo sencillo de IC basada en repetidores cuánticos, la RFC enuncia también los objetivos de la Internet cuántica, en concreto: (1) soporte a la computación distribuida más allá de la simple trasmisión de información cuántica; (2) soporte a aplicaciones cuánticas distribuidas a largo plazo y a la heterogeneidad (de hardware, de gestión de errores, etc.); (3) seguridad a nivel de red que no menoscabe la seguridad cuántica aún a pesar de las operaciones e información clásica trasmitida; (4) facilidad de monitorización que convivas con el teorema de no clonación y el principio de medida ; y (5) por supuesto, garantías de alta disponibilidad y resiliencia.

5.5. Enrutado cuántico

De la descripción de las redes cuánticas y de la futura IC se sigue la necesidad de arbitrar distintos mecanismos y técnicas en el plano de control que emitan la transmisión cuántica extremo a extremo. Aunque existen diversos aspectos a ser resueltos (asignación y reserva de recurso, congestión, calidad de servicio, etc. [366, 221, 241]), el centro de los mismos es la distribución del entrelazamiento extremo a extremo en lo que podemos denominar un camino o ruta de entrelazamiento.

El problema de las *rutas de entrelazamiento* (*entanglement routing*) es el de construir y distribuir estados entrelazados en una red de topología arbitraria, entre dos o más de sus nodos, haciendo uso de repetidores o de switches intermedios, incluso en el caso de que esos nodos puedan ser no confiables o deshonestos [317, 353, 409, 280, 490].

La elección de rutas de entrelazamiento es pues el problema fundamental de una red cuántica entendida esta como un sistema distribuido y, desde un punto de vista de arquitectura del sistema, resulta análogo a la función de la capa de red de la Internet clásica, que se ocupa básicamente de la elección global descentralizada de las rutas y del reenvío de los paquetes. Sin embargo, existen notables diferencias de concepto y de operación entre el nivel de red clásico y la selección, gestión y uso de rutas de entrelazamiento en una red cuántica [409]:

- Dinamismo. En una red clásica, el cálculo de los caminos se basa en la elección de una métrica para cada enlace y en la ejecución distribuida de un algoritmo de estado de enlace o de vector de distancias para obtener los caminos más cortos. Esta aproximación presume que los enlaces permanecen en un estado estable, sin cambios, durante un tiempo suficiente como para que el algoritmo converja y puedan aplicarse los caminos que calcula. En una red cuántica esta premisa no se cumple: el estado de un enlace desde el punto de vista de la existencia o disponiblidad de entrelazamiento entre su extremos cambia en una escala de tiempos pequeña, inferior al tiempo de cómputo que necesitaría un algoritmo de selección de las rutas en una red grande.

- No determinismo. Un enlace cuántico es probabilista: los procesos de creación del entrelazamiento, purificación, medidas e intercambio son, como se ha visto, aleatorios, y las probabilidades de que estas tareas finalicen con éxito pueden ser bajas.

- No simultaneidad. Para el entrelazamiento, un enlace cuántico no se puede compartir más que entre un único emisor y un único emisor (o, de forma equivalente, entre dos registros cuánticos de memoria en el nodo emisor y en el nodo receptor). Si un mismo enlace es demandado por flujos distintos (s,d), cada uno de ellos necesita un par entrelazado diferente.

- Sincronismo. En una red clásica, los datos se pueden almacenar por un tiempo arbitrario en la memoria de los nodos intermedios hasta que el enlace está disponible. En una red cuántica, el entrelazamiento tiene que existir en el momento en que se necesita, o bien haberse creado de antemano y tener un tiempo de coherencia suficiente.

Los requisitos físicos para establecer el entrelazamiento multisalto en una red cuántica son, además, exigentes. Con la tecnología actual, una QPU puede tener alrededor de 128 qubits de memoria; el tiempo medio para el aparezca decoherencia en un estado entrelazado bipartito es de $1{,}46$ s, aproximadamente; el tiempo de establecimiento de un estado entrelazado es $\sim 165\ \mu$s

con intentos concurrentes; la comunicación clásica entre las partes ocupa ~ 1 ms; y el tiempo de lectura o medida del entrelazamiento es normalmente < 3 μs [116]. Las cifras mencionadas deben servir ante todo para enfatizar que: (a) el entrelazamiento es un recurso intrínsecamente cuántico, de naturaleza inherentemente distribuida pero aún costoso y con restricciones de tiempo; (b) como consecuencia, el principal factor de limitación en el desarrollo de rutas de entrelazamiento es (la memoria en) el propio switch y no los enlaces de comunicaciones, que tienen capacidad de transmisión suficiente. Se concluye, así, que a diferencia de lo que sucede en el nivel de red clásico, cuyo funcionamiento es enteramente lógico (rutas, métricas de enlaces, *forwarding* de los paquetes), el diseño de una capa de red equivalente en una red cuántica está necesariamente vinculado a los recursos de entrelazamiento cuánticos que se puedan generar y simular. Esto es, las capas tradicionales de red y de enlace no son completamente separables sino que requieren un diseño conjunto [409, 219]. La cuestión del diseño de una arquitectura de referencia para una futura Internet cuántica se discute en numerosos trabajos, véase [219] para una revisión reciente, por ejemplo.

En general, el establecimiento de una conexión multi-salto entre dos o más nodos de una red puede seguir dos modelos conceptuales y operativos en lo que se refiere a la generación de los recursos de entrelazamiento en los enlaces (la función LLE, *Link Layer Entanglement*). En forma abstracta, una demanda de conexión entre dos nodos puede modelarse con la tupla (s, d, F, ℓ, δ), donde s, d son los identificadores de los nodos origen y destino, F es la fidelidad mínima requerida, ℓ es el retardo máximo tolerable para establecer la petición y δ denota el tiempo de persistencia que se desea para la duración del entrelazamiento. En cualquiera de los dos posibles modelos, se supondrá que la topología completa de la red es conocida por todos los nodos.

5.5.1. Generación anticipada

Los recursos de entrelazamiento ---bipartitos, casi siempre--- se crean antes de conocer las demandas de rutas y de adoptar las decisiones de entrelazamiento. Puesto que están disponibles de antemano, esos recursos pueden ser concebidos como recursos estáticos, de manera que los mecanismos de decisión de la ruta y de asignación de los recursos (los pares o estados entrelazados) a la misma se pueden aislar por completo de los problemas de generación, purificación o intercambio. En ese caso, las funciones necesarias en las capas de enlace y de red son separables, y la arquitectura es más semejante a la de una red clásica de conmutación de paquetes, salvo por la existencia de un recurso adicional, el entrelazamiento mismo.

La mayoría de los trabajos publicados hasta la fecha sobre diversas variantes del problema de rutas de entrelazamiento asumen las hipótesis de generación anticipada de estados bipartitos, dando por resuelto el problema de la creación de los qubits de memoria en cada repetidor. Los algoritmos correspondientes pueden o bien generar entrelazamiento por intercambio antes de conocer las demandas, o bien anunciadas esas demandas, usando menos recursos. Por ejemplo, [353] estudia el problema de las rutas de entrelazamiento considerando repetidores e intercambio sobre pares de Bell, con memorias imperfectas y entrelazamiento probabilista, sobre redes regulares de dos dimensiones. El uso de múltiples procesos de establecimiento entre dos repetidores adyacentes mejora significativamente la tasa de generación frente al caso de una cadena lineal de QRs [18], pero a costa de usar un mayor número de registros de memoria. La idea de calcular y generar entrelazamiento bipartito entre todos los nodos se utiliza en [409] en el algoritmo denominado Q-PASS para acomodar múltiples demandas desconocidas maximi-

zando la tasa de generación. Los posibles fallos en el intercambio que se producen durante la creación de una ruta no se resuelven reiniciando el procedimiento, sino recurriendo a caminos de *backup* o de recuperación previamente identificados, para disminuir el tiempo de establecimiento total e incrementar la probabilidad de éxito. Aun así, el coste de ejecución de Q-PASS es considerable, y los autores dan una aproximación eficiente más ligera (Q-CAST) que aplica una variante sencilla del algoritmo de Dijkstra para la obtención de los caminos más cortos. En este trabajo, el establecimiento de las rutas utiliza una métrica que no tiene en cuenta la fidelidad resultante, y la estrategia de solución pasa por utilizar un algoritmo *greedy* que maximiza la tasa de generación de entrelazamiento localmente en cada repetidor, lo que conduce a asignar la mayoría de los recursos disponibles a solo unos pocos usuarios, mientras que los restantes deben esperar. El método, por otra parte, no tiene unas garantías de prestaciones deterministas. La idea de intentar el establecimiento de forma concurrente entre dos repetidores adyacentes se combina con la de enrutado por segmentos en [493]. Un segmento es un fragmento de un camino que, si se establece correctamente una ruta cuántica sobre él, su trata en adelante como un nodo simple. Este idea de segmentar en decisiones independientes la obtención de la ruta tiene una ventaja doble: reduce la complejidad computacional y se adecua de forma natural a una arquitectura de red jerárquica. Otras veces, en el problema de las rutas de entrelazamiento se introducen métricas o requisitos simultáneos, como en [490], donde se considera la maximización simultánea del número de pares entrelazados para los usuarios y de la tasa de generación. El modelo propuesto en este trabajo está formado por la combinación de dos problemas de programación entera secuenciales (NP-completos), cuya solución aproximada se obtiene con un heurístico eficiente.

[280] es uno de los escasos trabajos que incorpora en la formulación del problema la condición de un umbral mínimo de fidelidad para el entrelazamiento extremo a extremo. En el primero de los algoritmos propuestos (QPATH) se pre-construyen todos los posibles entrelazamientos entre cualesquiera dos nodos de la red para utilizarlos en cuanto sean solicitados, si bien es obvio que este enfoque tiene una elevada complejidad computacional y consume gran cantidad de recursos. Una variante del mismo algoritmo (Q-LEAP) prescinde de esa construcción completa y simplifica la carga de cómputo global. En [86, 85] se considera también la construcción de rutas con valores mínimos de fidelidad, pero la estrategia de solución es diferente. Primero se formula un problema de programación lineal para calcular las tasas de generación globales en la red, problema que admite una solución eficiente. Después, con esos valores se diseña y aplica algoritmos de extracción de caminos que son compatibles con esas tasas o región de capacidad.

Una revisión reciente de los avances en el área de los algoritmos de rutas de entrelazamiento, así como una clasificación de estos, puede consultarse en [137].

5.5.2. Generación bajo demanda

Los recursos de entrelazamiento se crean una vez se revelan las demandas de rutas entre nodos de la red, dinámicamente, activando todos los nodos intermedios que sean necesarios. Es obvio que en este caso todas las etapas del proceso de generación de los estados entrelazados a lo largo de la ruta deben ser tenidos en cuenta en el diseño y construcción de la ruta, incluyendo el funcionamiento probabilista de cada fase de intercambio o de medida o de destilación. Por consiguiente, las capas de enlace LLE y de red no son disociables sino conjuntas.

Los métodos de generación bajo demanda suelen estar asociados a estados de entrelazamiento multipartito que se especializan (se miden localmente) en el momento en que las de-

mandas de establecimiento de conexiones se dan a conocer. Por la dificultad tecnológica y porque el entrelazamiento multipartito está peor caracterizado teóricamente, los avances en esta línea son limitados y las propuestas concretas, reducidas. Una de las primeras es [359, 358], cuyo objetivo es construir estados grafo arbitrarios entre los nodos de la red especializando con operaciones locales estados GHZ n-partitos, no solo enlaces cuánticos punto a punto. Ello hace posible ejecutar protocolos y algoritmos cuánticos más complejos, y a la vez supone un ahorro de registros de memoria en comparación con una arquitectura basada únicamente en pares de Bell. Las hipótesis del modelo son:

1. Los nodos pueden aplicar sobre sus registros medidas cuánticas, medidas de Bell, operadores Pauli y puertas de rotación controladas.
2. Las operaciones cuánticas locales y las medidas son perfectas, sin error ni ruido.
3. Las medidas de Bell son deterministas, por ejemplo por hacer uso de algún QEC o de rondas de purificación.
4. La creación de estados cuánticos locales tiene coste cero, de modo que los nodos pueden crear los estados locales que necesiten.

La obtención de un estado grafo arbitrario requiere varias copias de estados GHZ. Para conseguirlo, se propone en primer lugar simetrizar los estados GHZ rotando circularmente la configuración inicial, de modo que cada nodo tenga una copia del estado raíz de una de las copias del estado GHZ. Si hay n nodos en la red y el estado es GHZ_m, cada nodo tendrá m/n copias del estado $\bigotimes_{i=2}^{n}|\text{GHZ}_i\rangle$. Este estado, a continuación, se extiende o ``decora'' con un qubit adicional para prevenir posibles fallos o caídas del nodo, que se sitúa en el nodo que alberga la raíz del estado GHZ. Para crear este qubit adicional, el nodo prepara un par de Bell con cada uno de sus vecinos y luego fusiona (con una medida local) ese qubit con el qubit raíz del estado GHZ. Si ese nodo se desconectase de la red, los demás pueden recuperar el estado haciendo una medida Z sobre sus bits de protección locales, garantizando una tolerancia a fallos simples. El número total de qubits que se precisan en la red con esta solución, incluidos los de protección, es de

$$M_S = \sum_{i=2}^{n} c_i \left(1 + \sum_{k=1}^{i-1} c_k\right) + \sum_{i=3}^{n} c_i (i-1),$$

donde c_i es el número de copias con las que el nodo i está conectado a los nodos $1, 2, \ldots, i-1$ mediante el estado $|\text{GHZ}_i\rangle$. Si la misma funcionalidad de interconexión arbitraria por entrelazamiento se hubiese realizado mediante pares de Bell entre los nodos, el número total de qubits necesarios habría sido de

$$M_B = 2 \sum_{i=1}^{n-1} c_i \sum_{j=i+1}^{n} c_j.$$

Si, por ejemplo, $c_i = c$ para todo i, se tiene $M_B = c^2 n(n-1)$ y $M_S = (n-2)c + c^2(n-1)n/2 + c(n-1)n/2$. El protocolo de creación de los estados grafo de [358] se complementa con una organización jerárquica para evitar que el número total de nodos n sea muy grande, ya que M_S es $O(n^2)$. La forma de acotar ese crecimiento es dividir los nodos de la red en niveles jerárquicos de forma que solo algunos de los nodos del nivel i, $\{a_{i,1}, a_{i,2}, \ldots, a_{i,\ell_i}\}$ estén conectados a un subconjunto

de nodos del nivel $i-1$ inmediatamente superior mediante un estado GHZ. Para otro tipo de operaciones gráficas sobre estados grafo multipartitos con las que obtener entrelazamientos múltiples de dos o más nodos puede verse también [193].

Un método similar pero evolucionado y con mejores prestaciones es el de [72] para la distribución de estados GHZ de m qubits sobre topologías arbitrarias. Aquí, se crea el estado n-partito entrelazado haciendo uso de una configuración en estrella en donde los nodos que se quieren entrelazar usan un nodo auxiliar central para formar el estado grafo correspondiente. A esta configuración se llega calculando un árbol de Steiner entre todos los nodos que quieren establecer el estado entrelazado. Si bien esta no es la única alternativa para la distribución de los estados, los autores muestran que esta solución es óptima para estados tripartitos, y más aún, que el algoritmo es independiente de la métrica que se quiera optimizar, como la tasa de generación. Además, a diferencia de [358], se tienen en cuenta los errores en los repetidores y en las memorias cuánticas, por lo que el protocolo es más realista.

Si los esquemas de establecimiento de rutas de estados entrelazados se apoyan en procesos de purificación o destilación para recuperar la fidelidad de los estados intermedios que se generan, entonces un problema adicional es el de la planificación de estas operaciones y, asociado a este, el de determinar la capacidad del switch: cuántas de estas operaciones puede completar por unidad de tiempo. Tanto la elección de una política de planificación como el cálculo de la región de capacidad se acometen con herramientas de análisis similares a las conocidas en nodos de conmutación clásicos. Así, [76] lo formula como un proceso de decisión de Markov para el que deduce la política óptima aplicando las técnicas de *optimal stopping*, mientras que [159] obtiene una política estable para los switches gracias a una formulación algebraica del problema. Esta política se puede implementar fácilmente como una disciplina de tipo MaxWeight en cada uno de los nodos.

5.6. Aplicaciones y retos

Si difícilmente podemos atisbar lo que será la Internet Cuántica, identificar sus aplicaciones es igualmente aventurado. En cualquier caso, en este apartado se recogen las áreas que se consideran, hoy, en el punto de mira de las aplicaciones que se desplegarán sobre esta Internet Cuántica, posiblemente una red con pocos extremos al inicio como lo fue ARPANET. En este apartado se recogen, de forma meramente ilustrativa, las relacionadas con los servicios criptográficos, los servicios de computación cuántica distribuida y la computación ciega, entre medias de los anteriores. Además, las redes cuánticas y la IC son también de interés para la mejora de la sensórica cuántica, en casos de uso, por ejemplo, de redes de sensores o sincronización de relojes de alta precisión.

5.6.1. Servicios criptográficos

La criptografía cuántica explota las propiedades cuánticas para la realización de tareas criptográficas. De lejos, la distribución cuántica de claves (QKD) es el servicio de criptografía cuántica más exitoso, en el que las características cuánticas dan soporte natural a la detección de interceptaciones en la comunicación (*eavesdropper*). Esta distribución de claves con seguridad incondicional puede ser utilizada en distintos protocolos criptográficos.

Al margen de QKD, las redes cuánticas habilitan otros servicios criptográficos como, por ejemplo. la compartición de secretos, en concreto, la compartición cuántica de secretos (QSS-

Quantum Secret Sharing [208]). Se trata de modificar la solución clásica a la compartición de secretos en grupo mediante el uso de información cuántica. QSS es el proceso de compartir un secreto entre partes garantizando que ninguna de ellas pueda revelar el secreto sin la colaboración con el resto de las partes. Sea Alice la parte que quiere compartir un secreto con Bob y Charlie; para lo que crea dos mensajes cifrados, de forma que cada uno de ello no desvela información sobre el mensaje original, pero juntos contienen el mensaje completo. Por lo tanto, ni Bob ni Charlie pueden individualmente reconstruir el mensaje de Alice, pero sí lo pueden hacer conjuntamente. Más formalmente, se trata de compartir un secreto entre n partes de forma que cualesquiera k de ellas pueden reconstruir el secreto, pero ninguna combinación de $k-1$ partes puede obtener información sobre el secreto. En un esquema de umbral (k,n), se debe garantizar la confiabilidad k (si más de k partes se combinan se puede recuperar la información original) y la confidencialidad, con menos de k partes no se podrá recuperar información. La ventaja cuántica reside en el teorema de no clonación, que permite garantizar que no existe ningún esquema de umbral cuántico (k,n) para $2k \leq n$. Podemos encontrar distintas aproximaciones, algunas recientes en [277, 465, 278]; QSS es de especial utilidad para la compartición de claves distribuidas por QKD y para computación segura en nodos cuánticos distribuidos.

5.6.2. Computación ciega

Blind Quantum Computing (BQC) es una forma computación cuántica delegada segura basada en la nube que permite realizar cálculos de forma privada. La investigación en este ámbito se centra en discernir el grado de computación cuántica que es necesario introducir, esto es, si es necesario un cliente cuántico o por contra es suficiente un cliente clásico; y, por otro lado, si es necesario uno o varios servidores cuánticos. Aunque existe diversos trabajos en la literatura desde sus inicios [69] hasta hora [160, 161, 408, 407], a modo ilustrativo describimos una de las soluciones recientemente difundidas en la comunidad científica. En cualquier caso, las carencias actuales de las memorias y los computadores cuánticas impiden hoy un escenario de BQC a gran escala. En [407] se propone un modelo de BQC multipartito en 3 fases: (1) registro, o fase de distribución cuántica de claves; (2) autenticación; y (3) computación ciega. La fase de distribución cuántica de claves es necesaria para garantizar la seguridad incondicional de la clave entre los clientes (legítimos) y el servidor previo a la realización de la computación ciega. A pesar de esta distribución segura de claves, es necesaria una autoridad de certificación para completar la autenticación (CA- *Certificate Authotity*). El despliegue de estas dos fases necesita tanto un canal cuántico como una canal clásico. Por último, La fase de computación ciega multipartita se basa en un protocolo de servidor único, que solo necesita tener capacidad de medición de estados, en el que el cliente delega la computación.

5.6.3. Computación cuántica distribuida

La computación cuántica distribuida requiere la trasmisión de información cuántica entre varios ordenadores cuánticos que cooperan para llevar a cabo tareas cuya complejidad es inasumible mediante computación clásica distribuida. Al igual que en su versión clásica, se refiere a la ejecución de tareas en dos o más ordenadores cuánticos, combinando el resultado para producir un resultado final, que es el mismo que si se hubiese ejecutad en un único computador cuántico. Se engloba, además, bajo este nombre las mejoras que las tecnologías cuánticas permite obtener en problemas clásicos de computación distribuida, en concreto los protocolos de

elección y de consenso distribuido tolerantes a fallos. En este caso se trata de un ejemplo de cómo las tecnologías cuánticas permiten la mejora de la comunicación y computación clásica.

A la hora de abordar protocolos de consenso y elección cuánticos, el punto de partida es su componente probabilístico como consecuencia de la naturaleza estocástica de las medidas cuánticas. De acuerdo con la categorización propuesta en [308], los protocolos de consenso cuántico pueden ser de 4 tipos: consenso de estado simétrico; consenso basado en entrelazamiento; consenso basado en media; y consenso basado en QKD. Más recientemente, en la literatura, existe un importante conjunto de trabajos que estudian el consenso cuántico en el ámbito de las tecnologías Blockchain y DLT [282, 463, 449] y del QKD [300]. Por otro lado, es necesario también resolver el problema de elección. En la computación tradicional, estos protocolos son ampliamente utilizados para garantizar la coordinación de operaciones y la coherencia de los datos para lo que se asumen, por ejemplo, el conocimiento a priori de los identificadores de los nodos. Sin esta asunción, sólo los protocolos cuánticos de elección permiten una solución eficiente y segura [172, 437]

5.6.4. Retos

En este apartado se recogen los retos que la comunicad investigadora ha identificado para el avance en las redes de comunicación cuánticas en la que se sustentan los caso de uso reseñados anteriormente. Aunque también se avecinan avances en los dispositivos físicos para solventar los problemas de decoherencia así como la mejora de repetidores y las memorias cuánticas, limitamos el resumen a aquellos aspectos del plano de control que difieren de la Internet clásica y que tienen que ver con la Ingeniería de red cuántica, esto es la arquitectura y el diseño de la red cuántica (Se puede encontrar una discusión más detallada en [287]).

- Planificación de la distribución del entrelazamiento. Dado que el tiempo para la preparación del entrelazamiento extremo a extremo no puede ser considerado despreciable (requiere varios intentos por enlace y está limitado por las restricciones de memoria en los nodos intermedios), la planificación se convierte en un elemento central para garantizar la calidad de servicio. Sin embargo, la planificación bajo demanda implica una alta latencia; mientras que la planificación continua (nodos adyacente intentan mantenerse entrelazados la mayor parte del tiempo) implica un mayor grado de decoherencia, reduciendo la fidelidad. A este respecto se trabaja en distintas formas de optimización del proceso de distribución de entrelazamiento para maximizar su ratio, esto es, *entanglement distribution rate* (EDR) [91, 492].

- Enrutado de entrelazamiento. Como se ha discutido anteriormente, los algoritmos de encaminamiento en las redes clásicas no pueden aplicarse directamente a las redes cuánticas asistidas por entrelazamiento. Aunque existen variadas aproximaciones al problema, el reto de investigación se sitúa en la búsqueda de esquemas de encaminamiento que consideren la decoherencia y la imperfección de las operaciones cuánticas con el objetivo de mantener un compromiso entre EDR y la fidelidad. Asimismo, es necesario establecer métricas y funciones de coste orientadas a la calidad del entrelazamiento, e.g. probabilidad de éxito de la preparación del entrelazamiento; probabilidad de éxito del intercambio; fidelidad del entrelazamiento; número de entrelazamientos disponibles (ancho de banda); etc. [490]. Aquí, los aspectos probabilísticos del entrelazamiento son claramente distintivos frente a los algoritmos de enrutado clásicos.

- Control eficiente del intercambio de entrelazamiento. El intercambio para garantizar el entrelazamiento extremo a extremo se enfrenta a dos problemas importantes. Por un lado, dado que la operación de intercambio es imperfecta, y su fallo puede pasar inadvertido, supone un desperdicio de recursos de entrelazamiento. Por otro lado, es posible que dos operaciones de intercambio intenten utilizar el mismo recurso de entrelazamiento impidiendo la distribución del mismo. Es necesario el diseño de soluciones de control de intercambio para detectar con precisión el fallo del intercambio y evitar en lo posible la competencia por un recurso de entrelazamiento [467].
- Gestión de la purificación. Si bien la purificación es necesaria en la distribución de entrelazamiento (para la corrección de errores vinculada a pérdidas del canal y a la decoherencia cuántica), no todos los escenarios tienen los mismos requisitos de fidelidad. Se deben definir estrategias de gestión de las operaciones de purificación en la ruta de intercambio para minimizar el consumo de entrelazamientos y, al mismo tiempo, cumplir los distintos requisitos de fidelidad extremo a extremo [498]. Con dichos requisitos y en aras de minimizar la sobrecarga, la estrategia de gestión debe determinar , al menos, el número de rondas necesarias y el criterio de selección de los pares entrelazados a utilizar en la purificación.
- Asignación eficiente y justa de recursos de entrelazamiento. Como se ha mencionado el entrelazamiento es un recurso caro y costoso (pérdidas del canal, decoherencia, imperfecciones de las operaciones), siendo necesario establecer estrategias de asignación que permitan distribuir estos recursos eficazmente para dar cabida a múltiples solicitudes de distribución de entrelazamiento bajo criterios de compromiso entre equidad y EDR [276].
- Control de la congestión para la mejora de la calidad del servicio. Como ya se ha mencionado, en una red cuántica, pueden producirse solicitudes de distribución de entrelazamiento simultáneas cuando, además, los recursos de entrelazamiento son limitados. Siendo así, es necesario establecer mecanismos de control de congestión que regulen la tasa de distribución de entrelazamiento de extremo a extremo. Previo al diseño de tales mecanismos es necesario definir claramente la noción de congestión en el entrelazamiento cuántico, que previsiblemente estará relacionado con la latencia en la distribución del entrelazamiento pero también con las imperfecciones en el intercambio [497].

6. Computación cuántica en la era NISQ (*Noisy intermediate-scale quantum*)

Actualmente, y debido al avance de la tecnología, se asume que nos encontramos en la denominada era Noisy Intermediate-Scale Quantum (*Noisy intermediate-scale quantum*), término acuñado por John Preskill en 2018 [367]. En su origen, el autor se refería a una era caracterizada por la disponibilidad de procesadores cuánticos que tienen entre 50 y 100 qubits, pero que aún no serían lo suficientemente avanzados para poder solventar el problema de la fiabilidad de las puertas cuánticas debido a la imposibilidad de contrarrestar el ruido y la influencia externa a la que se ven sometidas. De ahí el nombre: (i) *intermediate-scale* porque superar los 50 qubits se planteaba en el año 2018 como un hito que permitiría hacer frente al uso de la fuerza bruta de computación proporcionada por los sistemas HPC de la época y (ii) *noisy* porque, aun así, todavía

no se podía asumir que se tendría un control total sobre el comportamiento de dichos qubits, lo que implicaría serias limitaciones a la hora de la fiabilidad de los resultados de la computación.

Es decir, la era NISQ se caracteriza, en realidad, no tanto por un número de qubits utilizado en la computación (en la actualidad se habla de no más de $1{,}000$ qubits, en lugar de los 100 que mencionaba John Preskill en su trabajo), sino por disponer de procesadores cuánticos que no son lo suficientemente avanzados para la tolerancia a fallos, ni lo suficientemente potentes para superar a la computación clásica. De hecho, las dudas sobre si la computación cuántica podría superar a la computación clásica no son recientes. Diferentes investigadores a lo largo de estos últimos 30 años han planteado las serias dificultades que se presentan a la hora de gestionar adecuadamente las computadoras cuánticas [450, 195, 261, 174]. De forma subyacente a la mayoría de estos estudios, se encuentra la decoherencia (*decoherence*), fenómeno que ocurre cuando un sistema cuántico interactuando con su entorno a lo largo del tiempo pierden sus propiedades cuánticas. De hecho, investigaciones más recientes argumentan que no va a ser posible conseguir la supremacía cuántica [232] o, sin ser tan drásticos, afirman que la dificultades a solventar para conseguirla serán, sin duda, especialmente complejas [23]. La realidad es que los procesadores cuánticos, muy sensibles a su entorno (ruidoso) y propensos a la decoherencia cuántica, todavía no son capaces de corregir errores de forma continuada y estos condicionantes son lo que definen, en realidad, a la era NISQ en la que nos encontramos [263].

6.1. *Quantum Processing Unit* (QPU)

Una QPU utiliza el comportamiento de algunas partículas (electrones o fotones, por ejemplo) para realizar ciertos cálculos mucho más rápidamente que otros procesadores tradicionales, como CPUs (*Central Processing Unit*), GPUs (*Graphics Processing Unit*) o DPUs (*Data Processing Unit*). Una QPU puede acelerar ciertos cómputos utilizando propiedades de la mecánica cuántica como:

- la superposición, es decir, la habilidad de una partícula de estar en varios estados a la vez, por lo que es posible almacenar valores ortogonales entre sí de forma simultánea;
- el entrelazamiento, propiedad que permite que los estados cuánticos de dos o más elementos estén fuertemente correlacionados, aún habiendo una distancia espacial entre ellos, lo que implica que el estado de todos ellos debe describirse mediante un estado único que los involucre a todos;
- y la aleatoriedad intrínseca, que permitiría servir de base para la computación probabilística y obtener como resultado de algunos cómputos un conjunto de respuestas posibles con su probabilidad asociada, lo que es especialmente interesante para algunos problemas de optimización.

Esta última propiedad, al contrario de las dos anteriores, se veía dificultada por un aspecto relevante: la falta de control sobre las distribuciones de probabilidad asociadas a la aleatoriedad cuántica. Recientemente se ha producido un avance importante en esta línea, dado que un equipo de investigadores del MIT (*Massachusetts Institute of Technology*) ha publicado un artículo científico explicando una posible vía de control para la aleatoriedad cuántica [388]. En cualquier caso, y como vía intermedia mientras no se produzca este control sobre las distribuciones de probabilidad, ha habido otros intentos de emular el comportamiento de una unidad de

información cuántica utilizando los denominados *p-bits* o bits probabilísticos [231] obteniendo buenos resultados para algunos algoritmos clásicos, como el de factorización [56].

Para poder aprovechar estas propiedades es preciso que los algoritmos tengan, al menos, algún paso que se vea beneficiado por la superposición, el entrelazamiento o la aleatoriedad cuántica. Algunos de los más populares son el algoritmo de Shor [329], para la factorización de números enteros, o el algoritmo de Grover [183], para búsquedas en bases de datos no estructuradas o desordenadas. Es importante destacar que estas ventajas no permiten que algoritmos no resolubles aplicando algoritmia clásica puedan serlo aplicando algoritmia cuántica.

A la hora de evaluar la cantidad de información que se puede almacenar en un sistema de este tipo, se habla de *qudits* o *qdits* [466]: el estado cuántico en un espacio de Hilbert de dimensión d [466]. Cuando $d = 2$ se habla de qubit (*quantum bit*) y cuando $d = 3$ se habla de qutrit (*quantum trit*). En el primer caso el estado del qubit va más allá del tradicional 0 y/o 1 del bit y, en el caso del qutrit va más allá del tradicional 0, 1 y/o 2 del trit; si bien lo más habitual es hablar de qubits, un parámetro fundamental a la hora de poder comparar este tipo de unidades de cómputo (apartado 7).

6.2. Tecnologías para la implementación de QPUs

Un qubit puede ser creado o implementado utilizando diferentes fundamentos físicos o tecnologías, si bien destacan tres estrategias: los superconductores, las trampas de iones y la fotónica. Cada una de estas tres vías presenta, por supuesto, ventajas e inconvenientes que se resumen a continuación:

Qubits superconductores Están fabricados un materiales que, al ser enfriados, adoptan propiedades superconductoras [104, 126]. De esta forma que se produce un flujo de electrones (denominado también supercorriente), que fluye de forma continuada entre dos elementos sin que se llegue a aplicar ningún voltaje. El enlace (débil) que se produce entre ambos se denomina Josephson Junction (JJ) y se basa en el efecto Josephson [52]. Este enlace puede ser un material aislante (S-I-S, *Superconductor-insulator-superconductor*), un metal no superconductor (S-N-S, *superconductor-nosuperconductor-superconductor*) o bien una restricción física que hace más débil la superconductividad en el punto de contacto (S-c-S, *superconductor-constriction-superconductor*). Actualmente es posible crear más de 100 de estos enlaces débiles en una única QPU, por lo que se ha convertido en la tecnología más utilizada, destacando algunas empresas como IBM (apartado 9.1). En los últimos años, Google [11, 196] e IBM [101] han tratado de demostrar sus ventajas. En concreto, Google afirmó en 2019 que su procesador cuántico, denominado *Sycamore*, permitía resolver el problema objetivo en 200 segundos, cuando un supercomputador clásico ejecutando el mejor algoritmo posible necesitaría más de $10{,}000$ años [11]. Se considera que sus dos grandes ventajas son la rapidez a la que pueden ejecutar las operaciones (mayor que con otras tecnologías) y el hecho de que es posible utilizar el conocimiento y los procesos ya existentes para la elaboración de circuitos impresos. Sin embargo, presentan también importantes desventajas con las que están lidiando los equipos de investigación: (i) los qubits creados con esta tecnología experimentan decoherencia rápidamente, por lo tanto, es preciso disponer de técnicas de corrección de errores elaboradas para reducir los problemas que esto conlleva; (ii) su conectividad es 2D, entre elementos próximos, por lo que se limita el tamaño y la profundidad de los circuitos que se pueden ejecutar en ellos; y, finalmente, (iii) requieren de una temperatura muy baja para poder trabajar de forma adecuada (cerca del cero absoluto), lo

que implica una infraestructura más costosa.

Trampa de iones o trampa iónica Mediante la combinación de campos electromagnéticos se confinan iones (partículas cargadas) de forma suspendida en el vacío. Estos iones son considerados y tratados como qubits que pueden ser manipulados, utilizando láseres, para almacenar información cuántica [328]. La más habitual para la manipulación de estados cuánticos es la trampa de Paul [387] o trampa iónica cuadrupolar, denominada así por Wolfang Paul, inventor del dispositivo y que recibió el Premio Nobel de Física en 1981 por este trabajo. Aplicando esta vía de fabricación, se han conseguido éxitos razonables en ejecución [120, 399], destacando empresas como Quantinuum (apartado 9.3) o *Alpine Quantum Technologies* (AQT) (apartado 10.3). Presentan como gran ventaja el hecho de que sean más estables, entrando en decoherencia mucho más tarde que los qubits basados en superconductores, aunque, sin embargo, no está claro que, a pesar de disponer de períodos de operatividad mayores, tengan mayor rapidez a la hora de ejecutar la algoritmia (ver apartado 7). En 2019 se realizó un estudio detallado sobre un ordenador cuántico de trampa de iones de 11 qubits [479], donde se constatan estas dificultades. Como ventajas destacan también el hecho de poder trabajar a temperatura ambiente, ahorrando costes en infraestructura y la posibilidad de permitir interconexiones entre qubits más flexible, dado que se trabaja en un contexto 3D, frente al 2D de los superconductores. Por último, existe un inconveniente importante: el hecho de que la tecnología de fabricación no es tan madura como la que sí se tiene en el caso de trabajar con superconductores.

Qubit fotónico En este caso se utilizan partículas de luz, cada qubit se basa en un único fotón, para transportar y procesar información y realizar computaciones cuánticas [347]. Los fotones son mucho menos sensibles a su entorno, lo que implica que mantienen su estado cuántico mucho más tiempo y a distancias mucho mayores que otras alternativas. Además de poder trabajar en entornos a temperatura ambiente, es posible integrar estos qubits en infraestructuras ópticas ya existentes y, finalmente, es más sencillo la conexión de múltiples QPUs usando multiplexadores, por lo que, en teoría, su escalado es mucho mayor. En esta línea están trabajando algunas empresas, como Xanadu Quantum Technologies (apartado 9.5), que ha desarrollado un sistema completo hardware-software que se analiza en [10] con la intención de proporcionar una solución escalable. Sin embargo, es esta una tecnología emergente en el mercado en la que todavía se está investigando.

Otras tecnologías Adicionalmente a estas tres opciones, también se barajan otras vías como: (i) el uso de Nuclear Magnetic Resonance (NMR), (ii) el uso del espín electrónico o (iii) la utilización de átomos de Rydberg. Si bien estas tres vías son menos habituales y han tenido menos éxito a la hora de tratar de escalar las arquitecturas de cómputo.

6.3. Soluciones hardware y software para computación cuántica e híbrida

A la hora de diseñar e implementar software para ser ejecutado en entornos de computación cuántica es preciso, al igual que ocurre con la computación clásica, disponer de entornos de desarrollo adecuados que faciliten el trabajo a la hora de programar y ejecutar código.

En un contexto clásico, un compilador traduce código desarrollado en un lenguaje de programación legible para humanos a un código objeto ejecutable en un computador. Este proceso se divide habitualmente en tres fases o etapas: (i) una inicial o *front-end* que se ocupa del *parseado*,

análisis sintáctico y otras operaciones relacionadas con el lenguaje de programación original; (ii) una final o *back-end* que se ocupa de generar y almacenar el conjunto de instrucciones ejecutables en el lenguaje máquina objetivo para ser ejecutadas en la infraestructura hardware disponible; y (iii) una etapa intermedia que se ocupa de la gestión de los datos y el flujo de control, denominada Intermediate Representation. Esta etapa intermedia debe ser independiente tanto del lenguaje de codificación como del lenguaje máquina, por lo que se precisa de un estándar que desacople la fase inicial y la final.

En el ámbito de la computación cuántica se trata de emular este mismo esquema funcional, pero en la actualidad hay algunas características que condicionan esta fase de desarrollo y ejecución que deben ser tenidas en cuenta a la hora de trabajar y, por tanto, de diseñar entornos apropiados para ello.

- En primer lugar, la infraestructura hardware en el contexto de la computación cuántica no está estandarizada. De hecho, existen (como se ha visto en el apartado 6.2) diferentes tecnologías para la implementación de los entornos de ejecución. Además, es preciso disponer de soluciones hardware híbridas, donde sea posible combinar hardware de computación clásico con el hardware de computación cuántico para optimizar la ejecución de la algoritmia. En el apartado 6.3.1 se resumen las tendencias actuales a la hora de integrar ambos mundos (cuántico y clásico) y los bloques funcionales habituales, que después se materializan de formas diferentes en función de la empresa que los desarrolle.

- En segundo lugar, es preciso disponer de un entorno software (lenguajes, *Software Development Kit* (SDK), simuladores) que permita escribir código para computación cuántica, compilarlo y ejecutarlo. Adicionalmente, se requerirá que sea viable desarrollar soluciones híbridas, que combinen algoritmia específica para ser ejecutada en hardware cuántico y algoritmia clásica, para sistemas tradicionales. En el apartado 6.3.2 se muestran los bloques o módulos que se identifican como necesarios para poder trabajar tanto desde el punto de vista puramente cuántico como híbrido.

Si bien a continuación se resumen estos bloques principales, en este momento no existen soluciones completas y estandarizadas en el ámbito hardware y software de computación cuántica. Por lo tanto, hay empresas que ofertan soluciones verticales para toda la cadena de valor hardware y software (diseño de algoritmia, compilación, simulación y ejecución), que se describen en el apartado 9, mientras que otras han centrado su actividad únicamente en el ámbito hardware (apartado 10). Adicionalmente, y de forma transversal, las grandes empresas centradas en la oferta de plataformas de cómputo en la nube, también han entrado en el mundo de la computación cuántica y permiten acceder a soluciones propias y de empresas terceras actuando como *brokers*, tal y como se indica en el apartado 11. Finalmente, han surgido diferentes iniciativas para tratar de ofrecer entornos software adecuados para trabajar con esta infraestructura cuántica, las más relevantes se describen en el apartado 12.

6.3.1. Integración hardware de QPUs con sistemas de cómputo tradicionales

En teoría, las QPUs requerirán de menor energía y desprenderán menos calor que los procesadores clásicos pero, sin embargo, requerirán de una costosa infraestructura de soporte para que se puedan gestionar las partículas que se usan para el almacenamiento y procesado de información. De hecho, por ejemplo, los computadores cuánticos basados en el flujo de

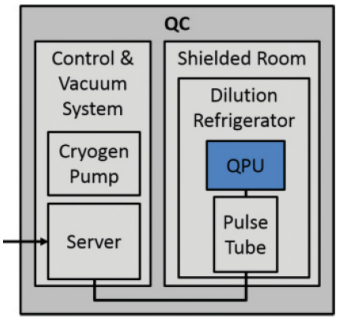


Figura 33: Estructura de un elemento de computación cuántica o computador cuántico [67].

electrones, que son los más habituales, deben tener sistemas de refrigeración potentes para garantizar temperaturas próximas al cero absoluto. El uso de fotones para crear QPUs permite obviar la refrigeración, pero requiere de sofisticados láseres y divisores de haz para gestionarlos adecuadamente. En cualquier caso, se requiere de sistemas que permitan aislar la unidad de computación cuántica para minimizar, en la medida de lo posible, el ruido y la interacción con el exterior y reducir el problema de decoherencia. Así, en la Fig. 33 se representa un esquema de la estructura habitual que sería necesaria alrededor de una QPU que, además de los muy habituales sistemas de refrigeración, requerirían de elementos para suprimir el ruido térmico y electromagnético o sistemas de vacío para garantizar la no contaminación de los dispositivos. Por lo tanto, actualmente se asume que este tipo de infraestructura se ubicará únicamente en centros de supercomputación y las QPUs tendrán que ser, necesariamente, integradas en sistemas de alta capacidad de cómputo o sistemas HPC (High-Performance Computing).

En realidad, el uso de QPUs se considera actualmente una estrategia alineada con el paradigma de aceleradores de cómputo (*accelerator paradigm*) [68]. El uso de aceleradores de cómputo, mecanismos hardware que permiten agilizar algunas actividades de computación, ha abierto una nueva era dorada para las arquitecturas de computación en la que se puede considerar ya el fin de la Ley de Moore [202]. En este nuevo contexto se puede afirmar que el diseño de unidades de cómputo ha virado desde la generalidad a la especialización [354], diseñándose soluciones específicas para las necesidades de cada ámbito de aplicación [118] como el procesamiento de gráficos, algoritmos de *deep learning*, simuladores, procesado de imagen, etc. Sin embargo, es necesario llegar a una solución de compromiso entre el uso de aceleradores más genéricos, como las FPGAs o GPUs, y el diseño de soluciones específicas ASICs (*Application-Specific Integrated Circuits* [453, 338]), dado que, si bien con estos últimos se consigue mayor eficiencia también es cierto que se incurre en un mayor coste de programabilidad y de NRE (*NonRecurring Engineering*).

Es en este contexto donde se espera que las QPUs jueguen un rol fundamental como elementos aceleradores transversales que permitan un salto diferenciador en el rendimiento de sistemas HPC. Se espera que la computación cuántica reduzca la complejidad de algunos algoritmos ampliamente utilizados aprovechando las características diferenciadores de la mecánica cuántica (superposición, entrelazamiento y aleatoriedad intrínseca).

En [67] se analizaron diferentes posibilidades de integración, destacando dos: una integración fuerte y una más débil. La integración débil asume una interconexión basada en el modelo

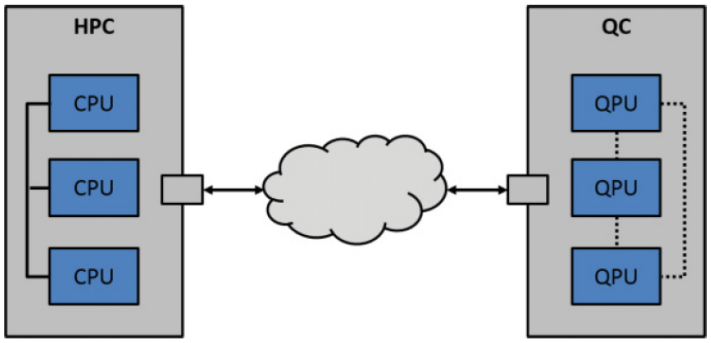


Figura 34: Conexión débil con un elemento de computación cuántico o QC (modelo cliente-servidor) [67].

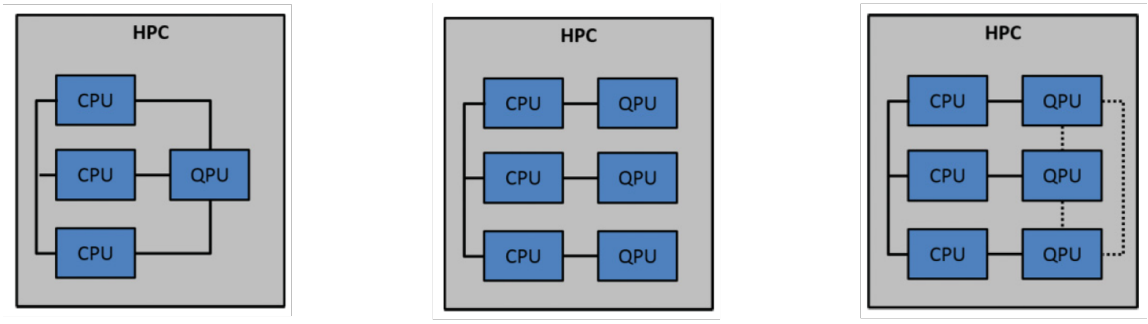


Figura 35: Conexión fuerte entre CPUs y QPUs, siguiendo diferentes esquemas de compartición [67]

cliente-servidor, donde el ordenador cuántico (QC, *Quantum Computer*), que puede estar compuesto por varias QPUs, funciona como un servidor que ofrece capacidad de computación al cliente o HPC (formado por una red de CPUs). La comunicación entre ambos elementos, tal y como se indica en la Fig. 34, es el principal cuello de botella y es preciso calcular adecuadamente el equilibrio entre la velocidad de cómputo adquirida al usar la unidad QC versus el coste en tiempo o latencia de la comunicación con ella. Por lo tanto, se asume que este modelo será rentable únicamente cuando la velocidad de computación alcanzada por el elemento QC es significativa.

La integración fuerte de elementos QC pasa por varios modelos de interconexión, como se indica en la Fig. 35, donde se han acercado las QPUs a las unidades de computación tradicional para reducir la latencia en las comunicaciones y maximizar, por tanto, el incremento de rendimiento en los cómputos. Los diferentes esquemas mostrados en la figura pasan por la compartición de una QPU por varias CPUs (Fig. 35.(a)), por la asignación de una QPU directamente a cada CPU ((Fig. 35.(b)) o el establecimiento de una modificación sobre esta última, donde las QPUs mantienen enlaces de comunicación entre sí para el reparto de tareas (Fig. 35.(c)).

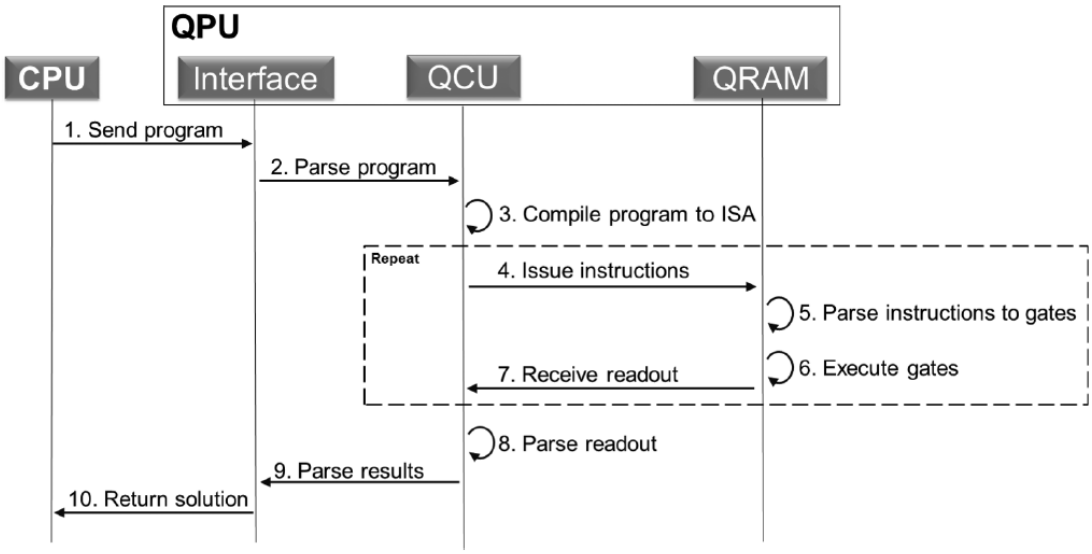


Figura 36: Modelo simplificado de QPU [67].

En cualquier caso, se estima que la computación cuántica pasa necesariamente por soluciones híbridas que combinen las unidades de cómputo disponibles actualmente: CPUs, GPUs, DPUs y QPUs. En los apartados 9 y 10 se resumen las iniciativas que están adoptando las empresas del sector para ofertar elementos hardware de computación cuántica e integrarlos con sistemas clásicos HPC. Además de ofertar sus propias plataformas de computación en la nube (mayoritariamente), también hacen uso de las plataformas de computación en la nube generalistas, como se indica en el apartado 11.

6.3.2. Integración software de QPUs con sistemas de cómputo tradicionales

En [67] se define la estructura lógica de una QPU, tal y como se indica en la Fig. 36, contando con (i) una interfaz que permita su interacción con una CPU tradicional para recibir el código que es preciso ejecutar; (ii) una unidad de control cuántica o Quantum Control Unit que se ocupará de transformar el programa en instrucciones, es decir, en *parsear* el código en una representación intermedia de instrucciones (IR, *Intermediate Representation*) que pueden ser ejecutadas utilizando una ISA (*Instruction Set Architecture*), que representa el conjunto de instrucciones de alto nivel que están disponibles para poder programar la unidad; y, finalmente, (iii) una QRAM (*Quatum Random Access Memory*) análoga a una RAM tradicional que se ocupará de ejecutar las instrucciones ISA en las puertas lógicas que maneja la QPU. Este modelo de bloques puede verse también en la Fig. 37, donde se detalla la composición de la QRAM: formada por el conjunto de puertas cuánticas y registros cuánticos (físicos y lógicos), que interactúan a través de las interfaces con los dispositivos de computación tradicionales.

Por lo tanto, lo ideal sería preciso disponer de una única ISA y estandarizar la interfaz de la QPU para poder utilizar una única IR y así disponer de un sistema que pueda integrarse adecua-

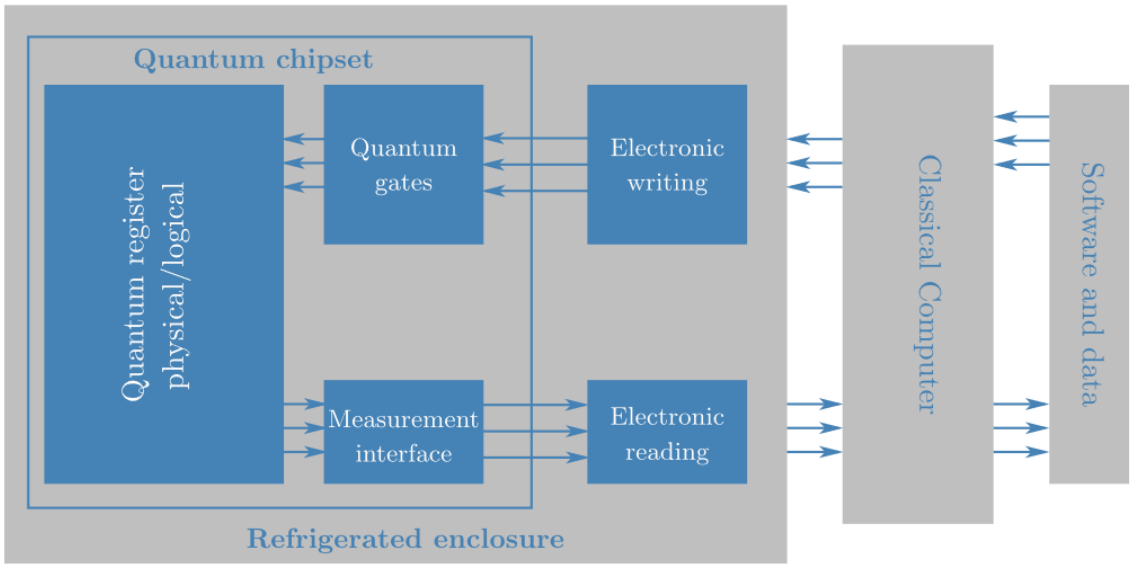


Figura 37: Modelo simplificado de QPU [239].

damente en diferentes soluciones arquitectónicas. Sin embargo, la situación actual dista mucho de aproximarse de forma general a soluciones estandarizadas. En cualquier caso, y si bien en los apartados 9 y 12 se resumen las principales líneas de trabajo de las empresas del sector para dotar de entornos de programación y desarrollo adecuados para la computación cuántica e híbrida.

7. Mecanismos para comparar computadores cuánticos

Tal y como se ha visto, existen diferentes tecnologías hardware para la implementación de qubits y, en consecuencia, QPUs. A la hora de comparar la eficiencia y eficacia de estas alternativas surgen también diferentes métricas o parámetros que, al igual que la tecnología que pretenden evaluar, están en continua evolución. En cualquier caso, y debido a la complejidad inherente a estas soluciones de cómputo, hay varios aspectos dentro del *QPU stack* que deben ser analizados: las propiedades y calidad de cada qubit de forma individual, los circuitos cuánticos que pueden ser construidos a partir de estos qubits, la interfaz entre el plano cuántico y clásico y, por supuesto, el rendimiento de los algoritmos que se implementen en estas soluciones hardware. En concreto, se suelen tener en cuenta los parámetros que se indican a continuación, centrados en (i) evaluar el sistema de cómputo cuántico a nivel de qubit (apartado 7.1); (ii) evaluar el sistema de cómputo cuántico a nivel de circuito o de forma agregada (apartado 7.2); y (iii) comparativa o benchmarking entre sistemas de cómputo cuántico en función del ámbito de aplicación (apartado 7.3).

7.1. Métricas para comparar QPUs a nivel de qubit

Número de qubits (qubits lógicos vs qubits físicos) Si bien suele mencionarse el número de qubits físicos como una medida de capacidad en computación cuántica, asumiendo que a mayor número de qubits físicos mayor capacidad, la realidad es un poco más compleja. Actualmente, la generación de qubits (y QPUs por consiguiente) no permite sistemas físicos libres de errores, es más, dado que el ruido inherente a los qubits que se pueden generar con la tecnología actual es mucho más elevado del deseado, es preciso utilizar alternativas para tratar de corregir estos errores. Una de ellas es usar los denominados qubits lógicos. Un qubit lógico aglutina un conjunto de qubits físicos, todos ellos idealmente en el mismo estado cuántico. Dado el elevado nivel de ruido en los qubits físicos, existe una probabilidad no despreciable de que no todos ellos se encuentren, en realidad, en el mismo estado cuántico. Disponer de un conjunto de qubits físicos aglutinados en un único qubit lógico permite utilizar técnicas de corrección de errores, como, por ejemplo, aplicar una decisión basada en la mayoría asumiendo que el estado correcto es aquel que comparten el mayor número de qubits físicos. Por lo tanto, sería más adecuado hablar de número de qubits físicos que es preciso tener para un qubit lógico, dado que esta medida permitiría evaluar la calidad de los qubits físicos.

Relación entre el tiempo de coherencia y el tiempo de operación de la puerta lógica Dado que los qubits son muy sensibles a la relación con su entorno, lo que produce el fenómeno de decoherencia en el que dejan de tener propiedades cuánticas, es preciso entonces que la ejecución de la algoritmia ocurra en períodos de coherencia, es decir, desde el momento de inicialización del qubit hasta el momento en el que se produce la decoherencia. La duración de este período de operatividad depende de las tecnologías utilizadas para la implementación del qubit: sus aspectos físicos o hardware. En sistemas basados en superconductores, estos tiempos son reducidos (del orden de microsegundos), mientras que en sistemas como los basados en trampas de iones consiguen períodos del orden de segundos. Sin embargo, este parámetro por sí solo no ofrece información adecuada de la operatividad de un qubit, dado que, en realidad, lo que interesa es el número de pulsos que se pueden aplicar a un qubit durante su tiempo de coherencia, es decir, el tiempo de operación de la puerta lógica. Si bien en los qubits basados en tecnologías de trampas de iones los tiempos de coherencia son más amplios, también lo son los pulsos que es necesario aplicar, por lo que el número de operaciones a realizar con la puerta lógica es lo que debería evaluarse, obteniendo resultados comparables a los de los sistemas de superconductores.

Fiabilidad de un qubit y una puerta lógica La fiabilidad, tanto de un qubit como de una puerta lógica, se define como la probabilidad de que se encuentre en un estado cuántico determinado después de una operación, es decir, evalúa hasta qué punto hay un resultado divergente entre el ideal y el real. Esta divergencia es consecuencia de la decoherencia y los errores acumulados durante la ejecución en un circuito cuántico. Esta medida permitiría evaluar cómo de ruidosa es una QPU y, en consecuencia, cuántos qubits físicos se precisarían para tener un qubit lógico. Para poder disponer de una medida, se utiliza la QST (*Quatum State Tomography*), un proceso que determinar el estado de los qubits tras un conjunto de operaciones previamente definidas, aunque tiene fuertes limitaciones. En primer lugar, no es posible aplicar esta técnica ni siquiera a circuitos de tamaño moderado. Aunque se han propuesto diferentes técnicas para mejorar su eficiencia, como esquemas de medida alternativos [111], aplicar técnicas de compresión a la me-

dida [189], aplicar técnicas de analítica de datos [102] y aplicar técnicas de aprendizaje máquina (ML, *Machine Learning*) para reconstruir estados a partir de mediciones parciales de volúmenes elevados de qubits [446], no es todavía una métrica que se pueda considerar escalable. En segundo lugar, el propio hecho de realizar esta medida implica que el sistema incurra en errores derivados de la preparación del estado y de la propia medida. En cualquier caso, existen trabajos en esta línea que tratan de ir un paso más y evaluar no sólo el estado sino la dinámica evolutiva a través de la denominada QPT (*Quantum Process Tomography*) [326], si bien, en este último caso, el número de parámetros que es necesario evaluar crece de forma excesiva como para ser considerado a día de hoy una solución viable y escalable. Otras vías de trabajo se centran en una exploración aleatoria, *Random Benchmarking* (RM) [251], donde se trata de medir la caída exponencial, en función de la longitud, de una secuencia aleatoria de puertas. Se asume que esta medida dará una estimación de la probabilidad de error por puerta y, por tanto, el nivel de coherencia en las operaciones lógicas o fiabilidad. Si bien es una técnica que no es nueva [251], sí sigue existiendo una línea de trabajo para mejorarla basada en la definición de modelos que aproximen mejor el efecto de decaimiento exponencial

7.2. Métricas para comparar QPUs usando redes de qubits

Topología y conectividad entre qubits Uno de los factores relevantes para cualquier sistema de computación cuántica es la posibilidad de conexión entre qubits y la topología que se puede establecer al hacerlo. En las soluciones basadas en superconductores, los qubits tienen como limitación la conectividad física en una capa de dos dimensiones, aspecto que no es limitante a la hora de trabajar con soluciones ópticas. Esto implica que, en el primer caso, es preciso utilizar elementos adicionales (como puertas SWAP) para poder compartir información entre qubits entrelazados.

Volumen cuántico El volumen cuántico o QV (*Quantum Volume*) es un parámetro que tiene en consideración diferentes propiedades de una QPU (número de qubits, tasas de error, conectividad...) y que permite comparar directamente dos soluciones de computación cuántica. Es preciso notar que el valor numérico no es consecuencia de un cálculo teórico, sino empírico. Originalmente definido en función del número de qubits y la profundidad del circuito (número de iteraciones que son ejecutadas) [327], se redefinió un año después por investigadores de IBM (apartado 9.1) [114] para tener en cuenta el tamaño del circuito y la complejidad de ser simulado en un ordenador clásico [27, 321]. Se definió entonces como el tamaño del mayor circuito cuadrado que puede ser ejecutado en el computador, entendiendo como circuito cuadrado aquel que tiene idéntica profundidad (la secuencia mayor de operaciones lógicas que se ejecutan en secuencia en el circuito) y ancho (número de qubits que definen el circuido). Actualmente se ha propuesto, tanto por IBM como por IonQ (apartado 10.1) utilizar una escala logarítmica para el valor QV, que represente mejor el rendimiento y permita realizar una mejor comparativa entre computadores. De esta forma, se obviarían aspectos menores y el valor obtenido sería consecuencia más directa del rendimiento de un circuito cuadrado compuesto únicamente por puertas lógicas con dos qubits entrelazados, la base de la mayor parte de los algoritmos cuánticos.

Esta medida no deja de ser controvertida, dado que algunos procesadores consiguen elevados valores de QV debido a sus características físicas, como es el caso de aquellos que se basan en trampas de iones. En este último caso, la conectividad entre qubits es total y presentan períodos de coherencia elevados, pero las operaciones que se ejecutan sobre ellos son más lentas

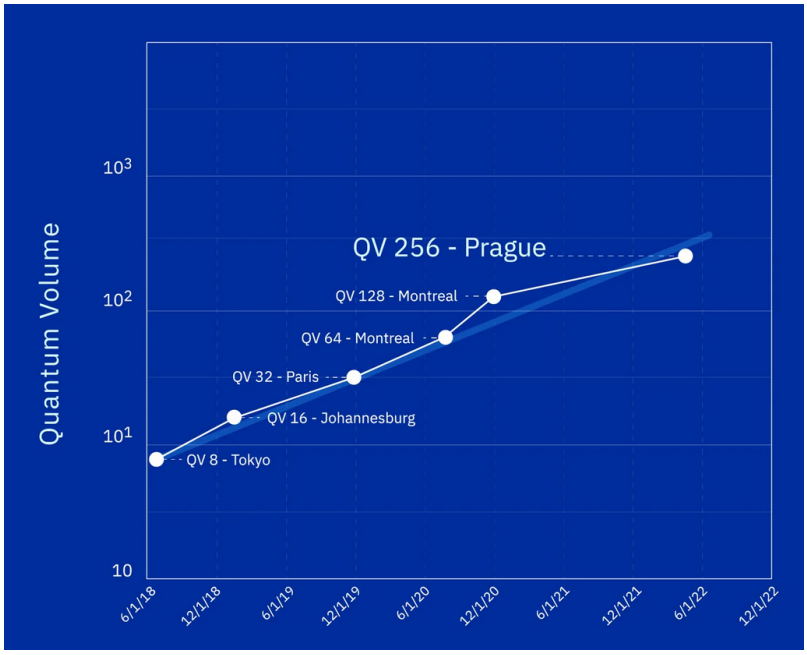


Figura 38: Evolución del QV en las soluciones implementadas por IBM [https://research.ibm.com/blog/quantum-volume-256].

que las que se obtendrían en computadores basados en otras tecnologías, como los superconductores. Puede verse a continuación las implicaciones que esto conlleva en el cálculo del QV. En la Fig. 38 se muestra la evolución de la tecnología que maneja IBM para sus computadores cuánticos, basados en tecnología de superconductores, en la que se observa que han conseguido un volumen cuántico de 256 en abril de 2022. Para evaluar el éxito, se ha seguido el siguiente criterio: exigir que el resultado más probable se encontrase al menos dos tercios de las veces que se ha ejecutado en un intervalo de confianza definido como dos veces la desviación típica. La empresa considera que este salto cuantitativo es debido a las mejoras conseguidas a la hora de tratar la coherencia y obtener así puertas más fiables. En la Fig. 39 se muestra también la evolución de las soluciones de Quantinuum (apartado 9.3), basadas en trampas de iones, llegando a un QV de $524,288$ en junio de 2023, usando el mismo criterio que en el caso de IBM y las mejoras para el cálculo del intervalo de confianza indicadas en [27], lo que supone una evolución fulgurante. En la Tabla 11 se muestra la trayectoria de los ordenadores cuánticos creados por las principales empresas del sector a lo largo de los últimos 3 años en función de su valor de QV.

CLOPS (*Circuit Layer Operations per Second***)** Tal y como se ha mencionado previamente, las características físicas de los qubits varían en función de la tecnología con la que fueron creados (diferentes tiempos de coherencia y tiempos de operatividad de las puertas) y, aunque se han mencionado varias métricas, ninguna de las anteriores por sí sola es realmente fiable a la hora de evaluar la velocidad de ejecución global de una QPU. Concretamente, el parámetro QV puede

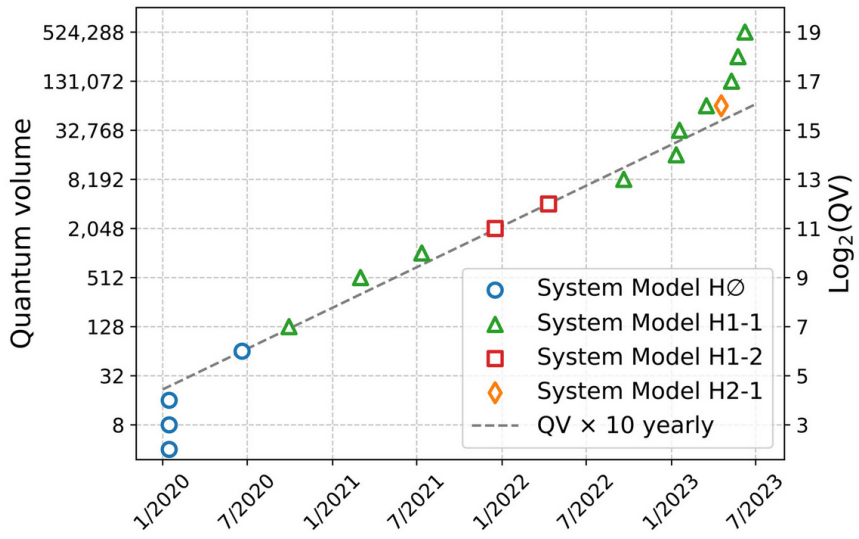


Figura 39: Evolución
del QV en las soluciones implementadas por Quantinuum [https://www.quantinuum.com/news/quantinuum-h-series-quantum-computer-accelerates-through-3-more-performance-records-for-quantum-vo

Tabla 11: Evolución de los ordenadores cuánticos en función de su parámetro de VQ.

Fecha	QV	Fabricante
2020 [enero]	32	IBM
2020 [junio]	64	Honeywell
2020 [agosto]	64	IBM
2020 [noviembre]	128	Honeywell
2020 [diciembre]	128	IBM
2021 [marzo]	512	Honeywell
2021 [julio]	1024	Honeywell
2021 [diciembre]	2048	Quantinuum (previamente Honeywell)
2022 [abril]	512	IBM
2022 [abril]	4096	Quantinuum
2022 [mayo]	512	IBM
2022 [septiembre]	8192	Quantinuum
2023 [febrero]	128	Alpine Quantum Technologies
2023 [febrero]	32768	Quantinuum
2023 [mayo]	65536	Quantinuum
2023 [junio]	524288	Quantinuum

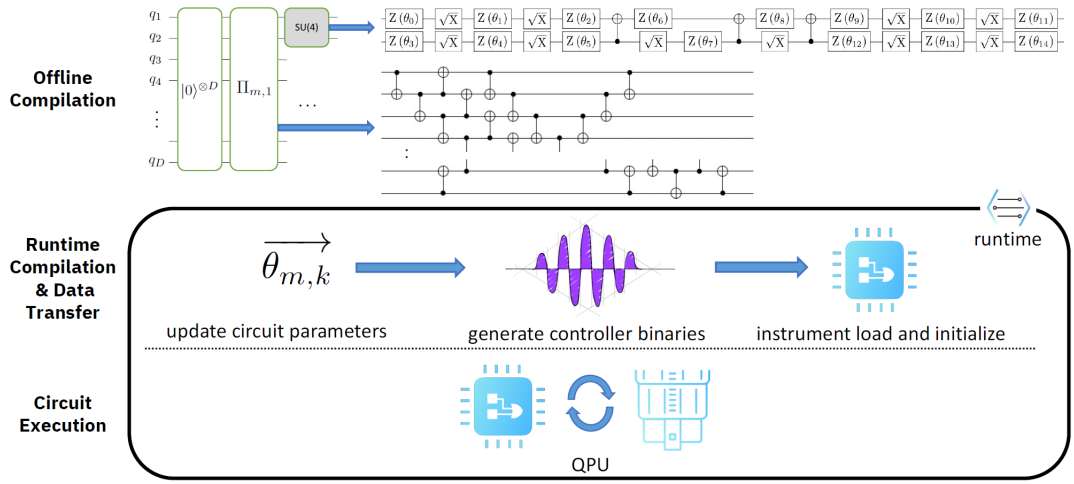


Figura 40: Compilación offline (optimizada para el cálculo del QV) y compilación online (propia de sistemas híbridos) [458].

ser optimizado cuando se analiza el cómputo únicamente de la ejecución que se realiza en una QPU, dado que se podría hacer una compilación *offline* adaptada a la estructura física disponible, como se indica en la parte superior de la Fig. 40. En realidad, y dado que la mayoría de las QPU serán integradas en sistemas híbridos como aceleradores de computación para partes concretas de la algoritmia, es preciso tener en cuenta la interacción entre las unidades de cómputo clásicas y las QPU, que son llamadas de forma reiterada en ejecución. Este tiempo de interacción se incorpora a una métrica definida recientemente por IBM [170]: CLOPS, que ofrece una medida de cuántos circuitos QV puede ejecutar una QPU por unidad de tiempo, incorporando, por tanto, los tiempos de interacción que se indican en la parte inferior de la Fig. 40.

#AQ (*Algorithmic Qubits*) Definida por la empresa IonQ (apartado 10.1) trata de solventar los problemas del QV y define este nuevo parámetro el número de qubits codificados útiles (lógicos) para un ordenador cuántico, por lo que representaría la capacidad de ejecutar algoritmos cuánticos reales para un tamaño de entrada determinado [90]. Por tanto, esta medida tiene en cuenta la corrección de errores dado que, en ausencia de codificación para la corrección de errores, la relación entre ambos parámetros sería la siguiente: $\#AQ = \log_2(QV)$. La propia empresa detalla una comparativa entre sus propios ordenadores en función de este parámetro $\#AQ$.

7.3. Benchmarking entre QPUs y ordenadores cuánticos

A pesar de las diferentes técnicas de comparación previamente indicadas (centradas en un único qubit o bien en redes de qubits), recientemente, y con el escalado de los sistemas NISQ de unas decenas a unos centenares de qubits, es preciso definir nuevos criterios más fiables que permitan la comparación o benchmarking entre sistemas de cómputo cuánticos. En los últimos tiempos se ha optado por centrar estas comparativas no en el análisis de las puertas lógicas sino en el rendimiento de los algoritmos cuando se ejecutan en dichos sistemas de cómputo.

Tabla 12: Resumen de diferentes propuestas de comparativa basadas en la algoritmia de aplicación [462].

[Ref]	Benchmark Name	Problems
[315]	Qpack	Max-Cut, dominating set, and travelling salesman problem (TSP)
[370]	Q-Score	TSP and Max-Cut
[340]	F-VQE (Variational Quantum Eigensolver)	Max-Cut
[117]	Variational quantum factoring (VQF) and fermionic simulation	VQF and fermionic simulation
[39]	Machine learning application	Approximating an unknown probability distribution from data
[322]	3 application-motivated quantum circuit	N/A
[299]	Application-oriented performance benchmarks	N/A
[133]	Quantum LINPACK	Dense random matrix in a quantum problem
[313]	Quantum chemistry benchmark	Electronic structure calculation instances
[274]	QASMBench	N/A

Es decir, centrar el análisis en los ámbitos de aplicación, que tienen también una influencia importante, además de la clara influencia de las características físicas de las QPUs.

En [462] se establece un análisis detallado de diferentes técnicas de comparativa o benchmarking que se resume en la Tabla 12. Estas seleccionan uno o varios algoritmos, bien conocidos en el ámbito de la computación cuántica y computación en la era NISQ, para poder evaluar el rendimiento de los computadores cuánticos.

8. Gestión de errores en computación cuántica: supresión, corrección y mitigación

La existencia de errores es inherente a la computación cuántica y se produce por diferentes causas que pueden aglutinarse bajo un único motivo genérico: cualquier operación o manipulación que se realice con un qubit supone una injerencia externa y, por tanto, puede provocar que se desestabilice (decoherencia), introduciendo errores en el proceso. Actualmente se estima que las computadoras cuánticas presentan una tasa de error en una de cada cien operaciones, aunque lo deseable para poder trabajar de forma eficaz sería disponer de, como mucho, un error en cada trillón de operaciones. Por lo tanto, se precisa de técnicas que permitan solventar esta situación mientras no se dispone de soluciones hardware más estables. Para gestionar adecuadamente estos errores se aplican diferentes técnicas que se suelen clasificar como sigue: (i) supresión de errores, (ii) corrección de errores o QEC (*Quantum Error Correction*) y (iii)

mitigación de errores o QEM (*Quantum Error Mitigation*).

Las técnicas de supresión de errores trabajan habitualmente al nivel más cercano al hardware y, por tanto, suelen ser muy dependientes del tipo de tecnología utilizada para la implementación de los qubits, por lo que suponen el nivel más básico de gestión de errores cuánticos. La idea subyacente, de forma general, es la de alterar o agregar señales de control al controlador, como secuencias de pulsos que puedan ayudar a *reenfocar* un qubit y mantener su estado cuántico por más tiempo o que puedan reiniciar su valor al estado original. Una de estas soluciones es la ofertada desde hace años por IBM (apartado 9.1) y su solución software de bajo nivel *Qiskit Pulse*.

La mitigación de errores o QEM [77] [148] trata de reducir o eliminar el efecto de los errores aprovechando las características aleatorias de las señales y ofertan una vía de solución para aplicar en la actualidad y a medio plazo: en la era NISQ en la que nos encontramos. Estas técnicas trabajan a nivel de algoritmia de bajo nivel y utilizan mecanismos como la cancelación de error o como la ejecución de varios circuitos físicos y la combinación de sus resultados para conseguir uno mejor [147]. Esta es, por ejemplo, la técnica *debiasing* que aplica la empresa IonQ (apartado 10.1) en su procesador *Aria*. Esta consiste en implementar o *mapear* un mismo circuito en varias variantes con permutaciones de qubits y usando diferentes descomposiciones de puertas, lo que permite reducir el efecto de errores sistemáticos en su tecnología (como la sobrerrotación). IBM (apartado 9.1) propuso recientemente otras dos técnicas, denominadas *Zero-noise extrapolation* (ZNE) [234] y *Probabilistic Error Cancellation* (PEC) [452], que fueron aplicadas exitosamente [245] en su procesador *Eagle*, de 127 qubits, consiguiendo resultados sin errores, mientras que un superordenador tradicional no pudo lograrlo. En cualquier caso, estas técnicas requieren de una cantidad importante de post-procesado, lo que supone un incremento del *overhead* que se estima exponencial.

Finalmente, desde casi el comienzo de la computación cuántica se está trabajando en técnicas que permitan la corrección de errores o QEC que permitan disponer de ordenadores cuánticos tolerantes a errores, es decir, capaces de, aplicando técnicas de corrección de errores, eliminar cualquier error lógico. Para que esto sea posible no sólo se depende de la algoritmia de las soluciones QEC, sino también se depende de la madurez de la tecnología hardware debido al *Quantum Fault-tolerance Theorem* [3], que indica que para que un ordenador cuántico sea tolerante a errores se tiene que satisfacer que la tasa de errores físicos se encuentre por debajo de un determinado umbral.

Este campo de trabajo presenta por sí solo una importante línea de investigación donde se trata de gestionar algunas peculiaridades de la mecánica cuántica que afectan a la hora de la aplicar soluciones tradicionales de corrección de errores: (i) no es posible copiar el estado de un qubit y (ii) no es posible medir un qubit sin alterar de alguna forma la información que almacena. La mayoría de estas técnicas utilizan qubits adicionales (o de síndrome) que se ocupan de evaluar de forma indirecta lo que está ocurriendo en los qubits de datos (que almacenan la información). Esta filosofía subyacente de aplicar redundancia es similar a la ya introducida para el ámbito de las comunicaciones. En la literatura especializada se resumen diferentes mecanismos para la corrección de errores de forma genérica (computación y/o comunicaciones) [125] [289] [386] y específica para el almacenamiento de información [440]. Todas ellas comparten terminología con los códigos de corrección de errores clásicos (distancia de código, redundancia, estimación, etc.). Actualmente, los algoritmos QEC con mejores resultados en el ámbito de la computación cuántica son los *surface code* [162], aunque requieren de una gran cantidad de qubits físicos para cada qubit lógico, por lo que es preciso seguir avanzando en soluciones hardware más estables.

En cualquier caso, es interesante destacar que recientemente (julio de 2023) se ha publicado una solución en la que está trabajando Google (apartado 11.3) basada en el uso de qubits lógicos (apartado 7.1), donde varios qubits físicos se usan simultáneamente como elementos de almacenaje de una unidad básica de información o qubit lógico. Sin embargo, es preciso tener en cuenta que a mayor número de qubits, mayor número de fuentes de error, por lo que la densidad de errores debería ser lo suficientemente baja (hablando en qubits lógicos) como para compensar la complejidad de la algoritmia a desarrollar para compensar los errores. La propuesta de Google consiste en utilizar 49 qubits físicos por cada qubit lógico para su solución basada en superconductores, con la que ha logrado resultados prometedores [433].

9. Soluciones integrales: hardware y software

En este apartado se detallan las principales soluciones verticales que ofertan las empresas del sector en este momento, proporcionando no sólo una infraestructura hardware donde ejecutar la algoritmia cuántica (usando diferentes tecnologías para implementar las QPUs), sino también proporcionando infraestructura software que permita disponer de entornos de desarrollo adecuados para el diseño, implementación, pruebas (simulación) y ejecución de soluciones cuánticas e híbridas. En concreto, se resume el trabajo de las siguientes empresas: IBM (apartado 9.1), Rigetti Computing (apartado 9.2), Quantinuum (apartado 9.3), Pasqal (apartado 9.4), Xanadu Quantum Technologies (apartado 9.5), Intel (apartado 9.6), QuEra (apartado 9.7), D-Wave (apartado 9.8) y QuTech (apartado 9.9).

9.1. IBM

IBM trabaja en el ámbito de la computación cuántica no sólo en la provisión de soluciones hardware, sino también para la provisión de soluciones de software.

En el ámbito hardware, IBM trabaja con tecnología de superconductores, con la que ha conseguido varios hitos. En el año 2020 anunció su procesador *Hummingbird* dotado con 65 qubits, que fue superado en 2021 por el procesador *Eagle* dotado con 127 qubits que, al año siguiente, 2022, fue de nuevo dejado atrás por su nuevo procesador *Osprey*, con 433 qubits. Según las previsiones de la empresa, expresadas en la línea temporal de la Fig. 41, se espera superar la barrera de los $1{,}000$ qubits en este año 2023 con su procesador *Condor*. Los avances que ha realizado IBM se centran en proporcionar mejores interconexiones entre qubits (*multi-level wiring*) y agregar elementos de filtrado que permitan reducir el ruido y mejorar la estabilidad. Adicionalmente, están trabajando en un mecanismo de control que esperan sea capaz de gestionar 400 qubits en un único rack. Al incrementar la calidad y la velocidad, han conseguido también mejorar el parámetro de QV hasta 512 y alcanzar una velocidad de $15K$ CLOPS.

IBM Quantum System One es el primer centro de datos cuántico integrado, incorporando los procesadores *Falcon*, *Hummingbird* y *Eagle*. Actualmente, IBM tiene un centro de datos en Nueva York (*NY Quantum Computing Data*) en el que hay 20 unidades IBM Quantum System One con el que soportan su propio sistema de acceso en la nube para poder ejecutar tareas o trabajos de computación cuántica en sus instalaciones. En la actualidad están trabajando en la segunda generación (*IBM Quantum System Two*) con el objetivo de que pueda llegar a tener hasta $4{,}148$ qubits. Adicionalmente, la filosofía con la que trabajan es que el *IBM Quantum System Two*) pueda concebirse como un módulo que permita construir centros de computación con el tamaño y capacidad demandados por sus clientes.

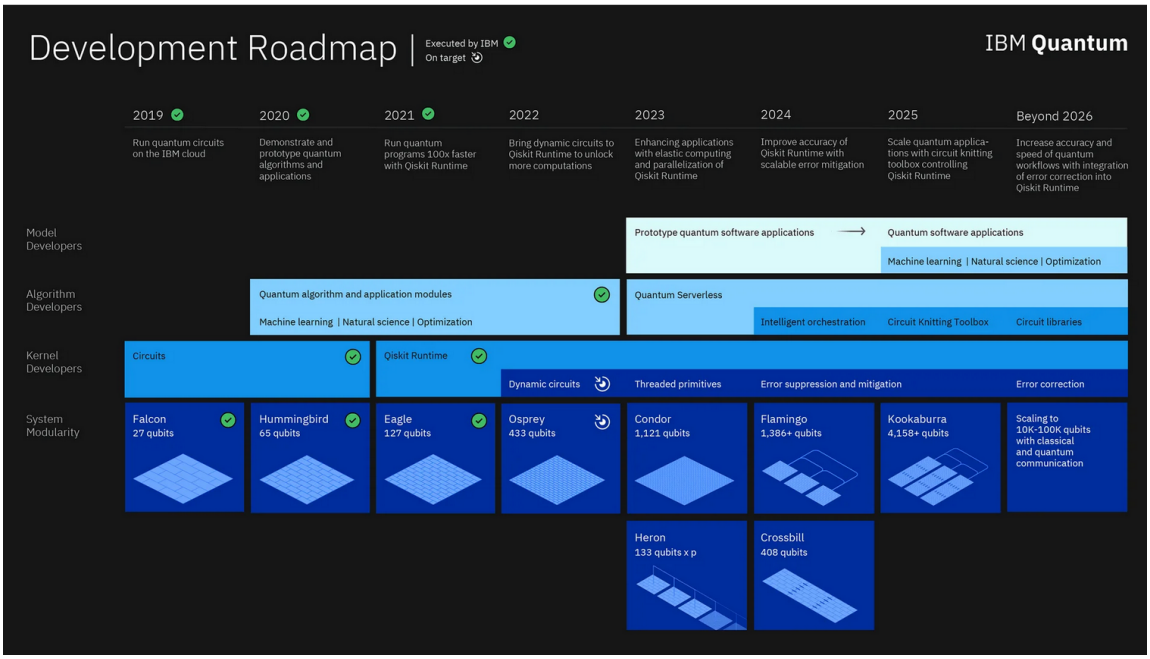


Figura 41: Previsiones de trabajo de IBM Quantum [https://research.ibm.com/blog/ibm-quantum-roadmap-2025].

En el ámbito software, IBM ofrece un entorno de desarrollo software completo denominado *Qiskit* [6] (Fig. 42) que proporciona todos los elementos necesarios para poder programar ordenadores cuánticos a partir de su unidad básica, el circuito cuántico. Este se construye o define en una primera fase (*build*) y después se ejecuta en una segunda (*execute*). La ejecución puede realizarse en ordenadores cuánticos o bien en simuladores que trabajan sobre infraestructura clásica. Su uso es amplio y tiene una comunidad activa que colabora y utiliza este entorno. De forma complementaria, IBM ofrece el módulo *Qiskit Runtime*, permite gestionar el conjunto de trabajos de ejecución (jobs) a gran escala, para ello proporciona un entorno de contenedores para la ejecución de los trabajos. Con esta funcionalidad la empresa indica que ha podido multiplicar la velocidad de ejecución para algunas aplicaciones hasta por un factor de 120, mejorando, además, la calidad de los resultados obtenidos [34, 471].

Qiskit y *Qiskit Runtime* trabajan de forma coordinada, como se puede ver en la Fig. 43, la API se ocupa de orquestar la ejecución entre el entorno clásico y el cuántico. En la figura se aprecian los dos elementos fundamentales de cualquier algoritmo cuántico: el muestreador (*sampler*) y el estimador (*estimator*), que se ocupan respectivamente de (i) calcular la distribución de probabilidades de la salida del circuito a partir de su muestreo y (ii) calcular los valores medios observados a la salida del circuito.

Finalmente, IBM también trabaja en la provisión de soluciones software específicas para determinados ámbitos, soluciones que pueden ejecutarse sobre la infraestructura previamente descrita. En concreto, destaca su producto *IBM Quantum Safe*, diseñado para proteger datos críticos (de empresas y gobiernos) de futuros potenciales ataques cuánticos. Fruto del trabajo

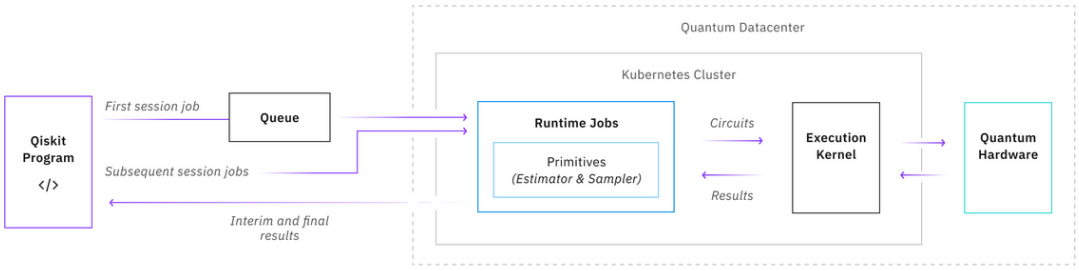


Figura 42: Arquitectura de Qiskit [https://docs.quantum-computing.ibm.com].

realizado, en el año 2022 el NIST (*Institute of Standards and Technology*) ha seleccionado cuatro algoritmos para ser estandarizados, siendo tres de ellos propuesta de IBM.

9.2. Rigetti Computing

Rigetti Computing crea computadores cuánticos y QPUs, basadas en tecnología de superconductores, que ponen a disposición de cualquier usuario a través de su plataforma de acceso en la nube QCS (*Quantum Cloud Services*). Según indica la propia compañía, proporcionan una solución global en la nube totalmente integrada con una infraestructura tradicional. Actualmente (desde diciembre de 2022), sus oferta de computación en la nube se basa en el *Aspen-M-3 Quantum Processor*, que consta de 79 qubits interconectados tal y como se indica en la Fig. 44, proporcionando una elevada fiabilidad del $99,7\,\%$ para una puerta de un qubit y de más del $93,7\,\%$ para puertas de dos qubits.

Para poder trabajar con esta infraestructura, la compañía oferta:

- Un lenguaje específico de programación denominado QUIL (*Quantum Instruction Language*) [423] y una extensión de dicho lenguaje, denominada QUIL-T que es soportada de forma nativa por las QPUs de la empresa, y

- un entorno de desarrollo y ejecución denominado *Forest SDK* que incorpora: (i) *pyQuil*, una librería escrita en Python para poder crear y ejecutar programas escritos en QUIL; (ii) *quilc*, un compilador optimizado de QUIL para la infraestructura física del QCS; y (iii) QVM, una máquina virtual que permite ejecutar código en simulador de un computador cuántico de la empresa.

Adicionalmente, y dado que esta empresa forma parte de la QIR Alliance y, por tanto, está interesada en la adopción generalizada de la representación intermedia QIR, oferta también una extensión denominada QCS QIR SDK para compilar y ejecutar QIR sobre su software de acceso a sus computadores en la nube. Por último, el servicio de computación en la nube, QCS, dispone de una API donde se especifica el acceso REST y HTTP.

El acceso a la plataforma QCS de Rigetti es también posible vía dos de las plataformas de computación en la nube más extendidas: (i) AWS (*Amazon Web Services*) vía su servicio Amazon Braket y (ii) Microsoft Azure a través de su servicio Azure Quantum.

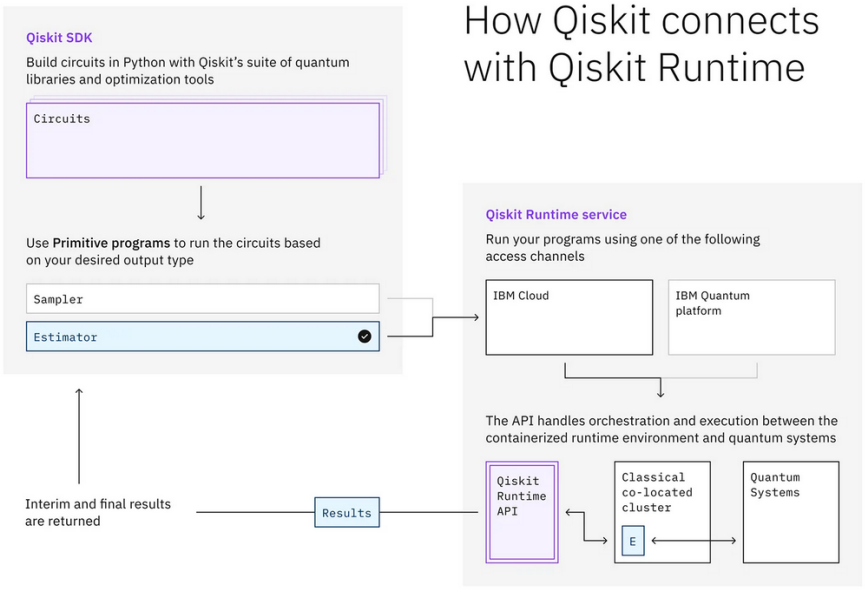


Figura 43: Flujo de trabajo entre *Qiskit* y *Qiskit Runtime* [https://research.ibm.com]

9.3. Quantinuum

Quantinuum, formada por la fusión de Cambridge Quantum y Honeywel Quantum Solutions en diciembre de 2021, desarrolla soluciones cuánticas basadas en trampas de iones y, si bien han publicado recientemente una tercera generación de computador batiendo el record al mayor QV ($524{,}288$), la solución más potente que tienen en producción es la correspondiente a su segunda generación, denominada *System Model H2*, que dispone de un total de 32 qubits totalmente interconectados, un QV de $65{,}536$ y una elevada fiabilidad tanto de puertas lógicas de un único qubit ($99{,}997\,\%$) como de puertas lógicas de dos qubits ($99{,}8\,\%$).

Además del diseño de soluciones hardware, Quantinuum ha desarrollado una plataforma de desarrollo software denominada TKET [416] para el diseño y ejecución de programas creados para computadores cuánticos independientemente de su arquitectura. Para facilitar la interacción con esta plataforma, la empresa ha desarrollado un módulo escrito en Python denominado *pytket*. Tal y como se introdujo en el apartado 6.3.2, en un contexto clásico un compilador traduce código desarrollado en un lenguaje de programación legible para humanos a un código objeto ejecutable en un computador. Este proceso se divide habitualmente en tres fases o etapas: (i) una inicial o *front-end* que se ocupa del *parseado*, análisis sintáctico y otras operaciones relacionadas con el lenguaje de programación original; (ii) una final o *back-end* que se ocupa de generar y almacenar el conjunto de instrucciones ejecutables en el lenguaje máquina objetivo; y (iii) una etapa intermedia que se ocupa de la gestión de los datos y el flujo de control, denominada *Intermediate Representation* (IR). Esta etapa intermedia es independiente tanto del lenguaje de codificación como del lenguaje máquina. Para ello, se utiliza un estándar que des-

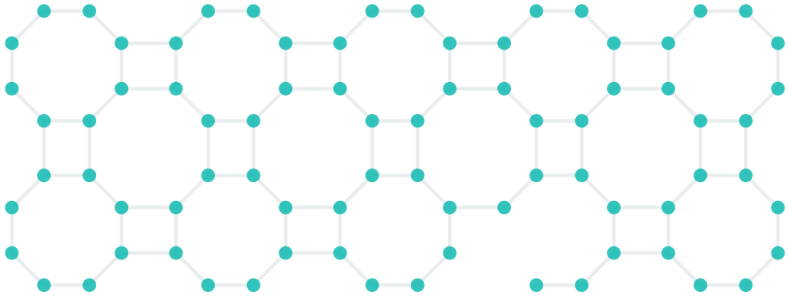


Figura 44: Interconexión entre los 79 qubits de la solución *Aspen-M-3 Quantum Processor* [https://www.rigetti.com/].

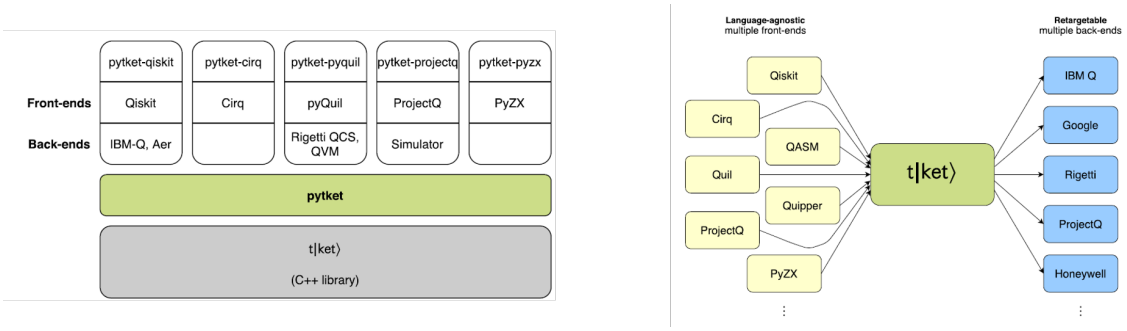


Figura 45: Componentes de TKET (izquierda) y modularidad con diferentes *front-ends* y *back-ends* (derecha) [416].

acople la fase inicial y la final. Esta es la filosofía que subyace en la solución TKET, tal y como se puede ver en las Fig. 45 y Fig. 46. Es decir, TKET sería capaz de trabajar con diferentes lenguajes de programación y obtener una traducción a código ejecutable para diferentes plataformas, no sólo la que proporciona la propia compañía. Dado que, además, Quantinuum pertenece a la QIR Alliance, trabaja en la línea de estandarización de esta representación interna para el ámbito cuántico, que se materializa en la solución QIR (apartado 12.2.2) y, por tanto, ofrecen también la librería *pytket.qir* que, siendo una extensión de la librería *pytket*, permite convertir estos circuitos en la representación intermedia QIR. Este es un paso directo, dado que TKET y QIR están ambas basadas en LLVM (*Low Level Virtual Machine*). Esta plataforma permite a equipos de investigación de diferentes ámbitos trabajar con soluciones de computación cuántica para el avance de sus propuestas[9].

Sobre la plataforma TKET, Quantinuum ha diseñado una librería denominada *LAMBEQ* especialmente orientada para trabajar en el ámbito del procesado de lenguaje natural que, a alto nivel, permite convertir cualquier frase en un circuito cuántico, lo que permitiría realizar el en-

[9]En el siguiente enlace se recogen las investigaciones publicadas que se han llevado a cabo utilizando esta plataforma: https://www.quantinuum.com/developers/publications

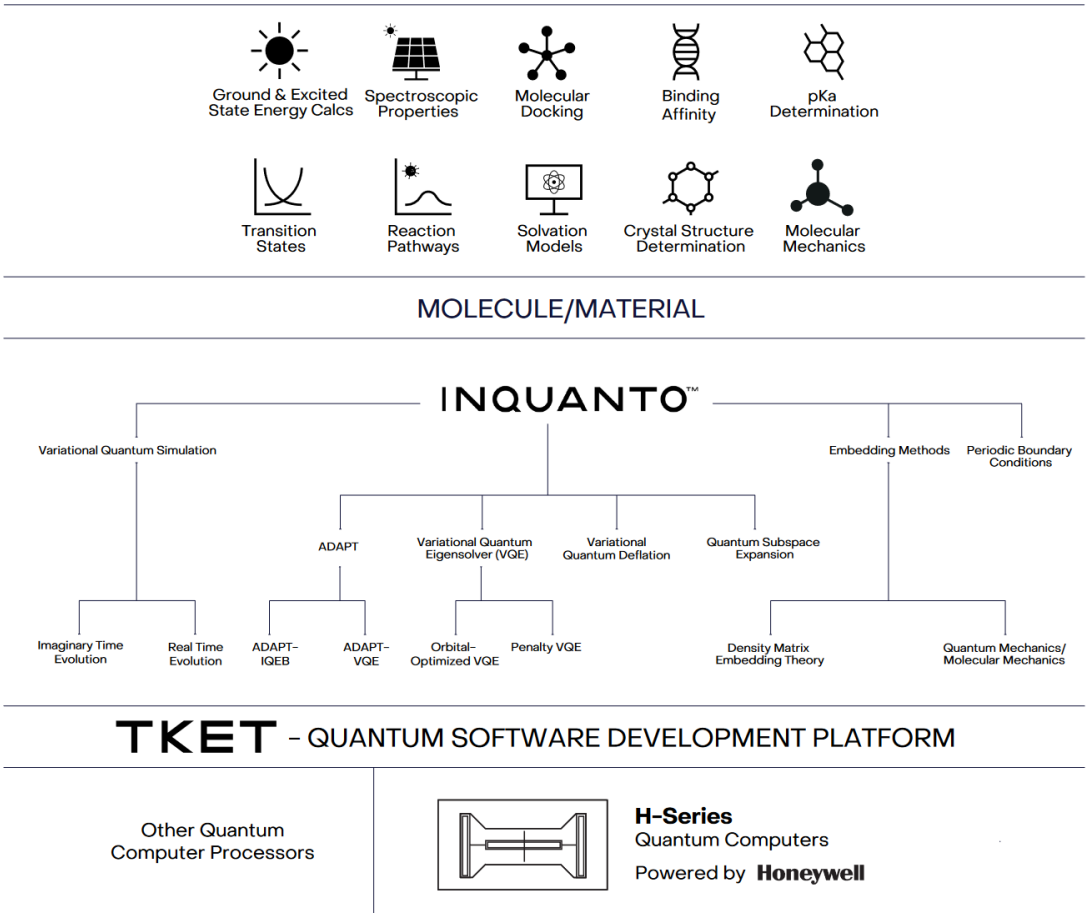


Figura 46: Estructura y servicios de la plataforma de computación cuántica orientada al ámbito químico InQuanto [https://www.quantinuum.com].

trenamiento de experimientos clásicos, cuánticos e híbridos en este ámbito[10].

Sobre esta capa orientada al desarrollo software de soluciones que precisen computación cuántica, la empresa ofrece también servicios específicos e integrales a empresas relacionados con las áreas de ciberseguridad y química. En el ámbito químico, oferta una plataforma de computación cuántica denominada *InQuanto*, cuyos detalles se ilustran en la Fig. 46, donde se puede acceder a varios algoritmos que sirvan de base para las líneas de investigación en este campo[11]. En el ámbito de la ciberseguridad, la empresa oferta una plataforma denominada *Quantum Origin* cuyo elemento central es la provisión de claves generadas utilizando computación cuántica a partir de la generación de una semilla y la verificación de su fortaleza. Esta

[10] En el siguiente enlace se recogen las investigaciones publicadas que se han llevado a cabo utilizando esta plataforma: https://www.quantinuum.com/qai/publications

[11] En el siguiente enlace se recogen las investigaciones publicadas que se han llevado a cabo utilizando esta plataforma: https://www.quantinuum.com/computationalchemistry/publications

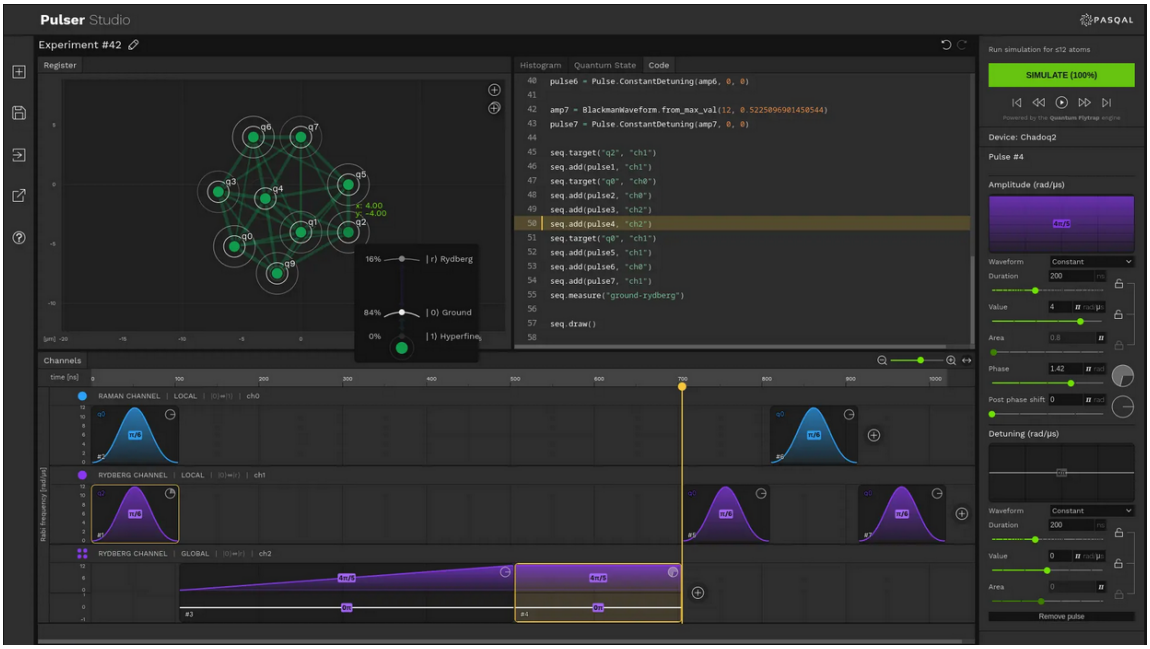


Figura 47: Interfaz de Pulser Studio, proporcionada por Pasqal para la programación y control de sus QPUs [https://pulserstudio.pasqal.cloud/]

plataforma se articula en dos vías: (i) una orientada para la computación en la nube (*Quantum Origin Cloud*) que permite trabajar en el ámbito de las estructuras de clave pública, usar tecnologías de cadenas de bloques y securizar comunicaciones y almacenamiento; y (ii) una orientada al uso local (*Quantum Origin OnBoard*) orientada a aplicaciones de securización de redes IoT y comunicaciones inalámbricas. En ambos casos se oferta un conjunto de librerías con software que permite agilizar el desarrollo de soluciones de ciberseguridad en ambos contextos[12].

Para el acceso a estas instalaciones hardware, Quantinuum oferta varias posibilidades. De forma general, es viable acceder a través de la plataforma de computación en la nube proporcionada por Microsoft Azure (apartado 11.2) ofertando varias QPUs, todas ellas entre 20 y 32 qubits usando la tecnología de su solución *System Model H2* o bien *System Model H1*. Para equipos de investigación con convenios para trabajar en EEUU, es posible acceder a través de las instalaciones del centro de investigación Oak Ridge National Laboratory (ORNL), gestionado por el Departamento de Energía de EE.UU. Finalmente, es posible también el acceso a través de la propia empresa Quantinuum de forma genérica o bien con una licencia de uso de la plataforma InQuanto.

9.4. Pasqal

Pascal desarrolla procesadores cuánticos basados en átomos neutros que son manipulados

[12] En el siguiente enlace se recogen las investigaciones publicadas que se han llevado a cabo utilizando esta plataforma:https://www.quantinuum.com/cybersecurity/cybersecurity-news

usando tecnología láser. Actualmente tiene en producción una solución hardware de primera generación con 100 qubits (que esperan que pueda pasar a 200 qubits en breve) y otras dos generaciones posteriores que se encuentran en fase de investigación y desarrollo. De estas dos últimas, sólo se ha publicado el tamaño en qubits del computador cuántico de segunda generación de la compañía: 1000 qubits. Todas sus soluciones hardware trabajan con una perspectiva híbrida analógica/digital, usando el modo analógico para el control de parámetros físicos con mayor precisión.

Pasqal permite acceder a sus equipos hardware usando dos vías. Se ofrece a aquellas empresas o entidades que requieran de elevadas necesidades de computación la instalación de la solución hardware en sus propios centros de datos, desarrollando así una solución de computación de nube privada. Adicionalmente, y para aquellas empresas y/o personas interesadas en utilizar los recursos hardware de Pasqal se les puede habilitar acceso a la plataforma de computacion cuántica en la nube que la empresa tiene desplegada y alojada en el proveedor externo OVH-cloud. Finalmente, la empresa tiene un convenio firmado con Microsoft Azure (apartado 11.2) para habilitar un acceso a sus equipos de computación a través de esta entidad; se espera que se pueda facilitar este acceso a principios de 2024.

Para poder facilitar las labores de diseño e implementación de los algoritmos, Pasqal ofrece la posibilidad de emular el comportamiento de sus procesadores cuánticos (hasta 100 qubits en *arrays* de dos y tres dimensiones). Para ello hacen uso de hardware de la empresa NVIDIA, en concreto de nodos DGX equipados con GPUs de elevada capacidad. En función de las necesidades de emulación, se podría utilizar un equipo personal (para hasta 15 qubits), un clúster de GPUs (hasta 40 qubits) o bien una combinación de arquitectura de clúster GPU y redes de tensores (para hasta 100 qubits).

Pasqal ofrece una plataforma de trabajo para programar sus QPUs con una orientación diferente a la habitual, dado que se basa en una plataforma, denominada Pulser Studio, totalmente gráfica que permite la creación de prototipos y algoritmia sin código escrito. En este momento, la plataforma Pulser Studio se encuentra en una fase de desarrollo beta y no permite la interconexión directa con los equipos hardware, sino con los emuladores de su comportamiento que tiene disponibles la empresa. En la Fig. 47 se muestra la apariencia gráfica de la herramienta.

Por último, Pasqal oferta una plataforma de computación cuántica especialmente orientada para el área de química industrial y ciencia de materiales, denominada Qubec, que aglutina los algoritmos más habituales que se precisan en este ámbito y los combina con sus emuladores, ofreciendo una solución integrada. Los avances en investigación que realizan los equipos de Pasqal y publican en diferentes foros internacionales pueden ser accedidos desde el siguiente enlace: https://www.pasqal.com/learn/science.

9.5. Xanadu Quantum Technologies

Xanadu Quantum Technologies oferta soluciones hardware, denominadas denominadas *X-Series*, que han sido desarrolladas por los equipos de investigación de la propia empresa, que ha publicado las bases de estos ordenadores cuánticos basados en qubits fotónicos en [10]. Sus equipos están disponibles a través de una plataforma propia de computación en la nube, lo que permite acceder al hardware desarrollado por Xanadu y, también, a soluciones de simulación de ordenadores cuánticos basados en qubits fotónicos que proporciona la propia empresa.

Con el objetivo de mejorar la usabilidad de los computadores cuánticos y ofrecer una solución vertical, Xanadu ha desarrollado también varios complementos software de interés para

desarrolladores: dos librerías de software y dos simuladores.

PennyLane [47] Es una librería de programación desarrollada en Python para ordenadores cuánticos genéricos, independientemente de las tecnologías con las que hayan sido creados. Uno de los distintivos de PennyLane es que utiliza el paradigma de programación cuántica diferenciable, por lo que es especialmente interesante a la hora de ser integrado con herramientas de aprendizaje automático o ML (*Machine Learning*). La idea subyacente sería la de entrenar un ordenador cuántico de forma análoga a como se haría con una red neuronal. Los convenios adquiridos entre Xanadu y otras empresas desarrolladoras de hardware para computación cuántica (como IBM, Rigetti, IonQ, AQT) y otros actores relevantes en el ecosistema cuántico (como AWS, Google, Microsoft Azure) permiten que el código desarrollado con PennyLane pueda ejecutarse en diferentes QPUs (distintas tecnologías) a través de proveedores de computación en la nube. PennyLane puede descargarse y usarse también de forma local en sistemas de cómputo clásico y un software de simulación de hardware cuántico.

Strawberry Fields [243] Es una librería desarrollada en Python para construir, simular y ejecutar programas en ordenadores cuánticos fotónicos, por lo que está especialmente diseñada para las soluciones hardware de Xanadu. De hecho, está integrada en la plataforma de computación en la nube de la empresa y permite la ejecución en sus equipos *X-Series*. Al igual que ocurre con PennyLane, Strawberry Fields se puede instalar también localmente.

Lightning Es una plataforma de simulación de computación cuántica, escrita en C++ y que es accesible vía una API desarrollada en Python, que ha sido diseñada para operar con los sistemas hardware de Xanadu y para trabajar con su orientación al aprendizaje máquina. Consta de dos simuladores: *lightning.qubit* y *lightning.gpu*. El primero está integrado en la librería *PennyLane* y puede ejecutarse en cualquier arquitectura de computación habitual, incluso localmente. El segundo está diseñado para trabajar con GPUs, especialmente en el entorno *cuQuantum SDK* proporacionado por NVIDIA (apartado 12.3.2). Se puede acceder a ambos simuladores también a través de la plataforma de computación en la nube proporcionada por la empresa.

Jet Es una librería escrita en C++ y Python que permite simular circuitos cuánticos usando redes de tensores y permite el uso de *qudits*, pudiendo así variar la base de información sin que tenga que ser necesariamente binaria.

9.6. Intel

Intel está trabajando en el ámbito de la computación cuántica en dos vías principales y complementarias, como se puede ver en la parte izquierda de la Fig. 48 que proporciona la propia compañía.

En primer lugar, en el desarrollo de hardware se encuentra investigando en el diseño y desarrollo de chips de computación cuántica que permitan, en un futuro, obtener una solución completa o computador cuántico. Intel ha trabajado con una solución basada en superconductores desarrollando dos propuestas de chips, denominadas *Intel Horse Ridge* e *Intel Horse Ridge II* [355], presentadas ambas en el año 2020. Recientemente, en junio de 2023, Intel ha presentado una nueva solución denominada *Tunnel Falls*: un chip de 12 qubits que utiliza tecnología basada

Figura 48: Soluciones HW/SW (izquierda) y estructura del Intel Intel Quantum Software Development Kit (derecha) [`https://www.intel.la`].

en espines. El objetivo último de Intel, tal y como ha publicado, es poder utilizar esta tecnología para construir un sistema de computación cuántica completo que pueda comercializarse. En paralelo, Intel cede esta solución hardware (chip) a los laboratorios y equipos de investigación de EE.UU. que se encuentran trabajando en tecnologías cuánticas para que puedan centrarse en el desarrollo de sus experimentos y algoritmos sobre esta solución.

En segundo lugar, Intel trabaja en el ámbito software proporcionando un entorno de desarrollo, denominado *Intel Quantum Software Development Kit*, cuya estructura se esquematiza en la parte derecha de la Fig. 48. Esta solución software, lanzada en su versión beta en septiembre de 2022 y en su versión 1.0 en febrero de 2023, realmente ofrece un ordenador cuántico simulado que puede interactuar con el chip *Intel Horse Ridge II* y, en breve, con el chip *Tunnel Falls*. Se proporciona una interfaz escrita en C++ y que usa el compilador LLVM para el desarrollo de algoritmos en C/C++ y Python, permitiendo a los desarrolladores acostumbrados a entornos clásicos un contexto más familiar. Este SDK permite elegir dos modos de trabajo: (i) uno centrado en un módulo de simulación cuántico genérico, en el que Intel lleva años trabajando (*Intel Quantum Simulator* o IQS [190]) o bien (ii) simular hardware de Intel. Es interesante destacar que este SDK permite, usando sus extensiones, integrar resultados de algoritmos cuánticos en proyectos C++, habilitando así la integración de algoritmia cuántica-clásica.

9.7. QuEra

QuEra desarrolla procesadores cuánticos basados en átomos de Rubidio neutros controlados con tecnología láser. Su producto más avanzado en el momento de redactar este documento se denomina *Aquila*, un ordenador cuántico de 256 qubits cuyas especificaciones y detalles de fiabilidad se encuentran detallados en [480].

Para acceder a este equipamiento se puede optar por hacer uso de los servicios de Amazon Braket (apartado 11.1), o bien a través de una conexión segura habilitada por la propia empresa para sus clientes. Adicionalmente, ofrecen un servicio a centros HPC y de investigación que permite instalar su solución de computación cuántica en los centros de datos locales de forma particularizada en cada caso.

Finalmente, QuEra proporciona un entorno de desarrollo propio denominado *Bloqade* que

	2000Q	Advantage	Advantage *performance update*
Performance			
Better Solutions (Satisfiability problems)	--	3x more often than 2000Q	23x more often than 2000Q
Time-To-Solution (3D lattice problems)	--	10x faster than 2000Q	2x faster than Advantage
Annealing Quantum Processor Design			
Qubits	2000+	5000+	5000+
Couplers	6000+	35000+	35000+
Couplers Per Qubit	6	15	15
Topology			
Graph	Chimera	Pegasus	Pegasus
Graph Size	C16	P16	P16
Connectivity	Degree 6	Degree 15	Degree 15
Lattice	8x8x8	15x15x12	15x15x12
Chain Length (for problem size n=64)	17	7	6

Figura 49: Evolución de las características de las soluciones hardware de D-Wave [https://www.dwavesys.com].

proporciona un emulador de un vector programable de qubits basados en átomos neutros para facilitar el diseño y pruebas de la algoritmia. Se puede trabajar con *Bloqade* en la nube, vía Amazon Braket, o bien descargarlo y ejecutarlo localmente en un ordenador clásico con suficiente capacidad de cómputo. En el caso de querer hacerlo vía AWS, se ofertan dos servicios: uno básico y otro mejorado vía la tecnología de NVIDIA CUDA Quantum (apartado 12.3.2).

9.8. D-Wave

D-Wave utiliza tecnología de superconductores para desarrollar sus soluciones hardware. Su producto estrella, denominado *Advantage^{TM} quantum computing*, tiene una arquitectura donde se combinan más de $5{,}000$ qubits, con elevada conectividad. En la Fig. 49 se resumen las características de las diferentes soluciones hardware de la empresa, donde destaca la topología de conexión entre qubits, denominada *Pegasus* [55], que mejora las caracerísticas topológicas de los ordenadores basados en superconductores.

Sus QPUs se implementan utilizando una red de dispositivos superconductores de interferencia cuántica o rf-SQUID (*rf Superconducting Quantum–interference Device*) [265, 197], utilizados para medir campos magnéticos extremadamente reducidos. Incorporan para el su control el proceso de optimización denominado *Quantum Annealing* (QA) [330, 425], que básicamente trata de localizar el mínimo global para una función objetivo dada cuando se dispone de un conjunto de potenciales soluciones haciendo uso de la propiedad de fluctuación cuántica (cambio temporal en la cantidad de energía como resultado del principio de indeterminación de Heisenberg)[13].

Leap^{TM} Quantum Cloud Service es la plataforma de computación en la nube que oferta D-Wave desde el año 2018 y que da acceso a su hardware *Advantage^{TM} quantum computing*. Adi-

[13] El trabajo de investigación llevado a cabo en la empresa se encuentra accesible de forma conjunta en https://www.dwavesys.com/learn/publications/

cionalmente, incluye el acceso al SDK diseñado por la empresa, denominado Ocean™ SDK, basado en Python. Esto permite a los equipos de desarrollo poder trabajar de forma sencilla en el entorno sin un conocimiento profundo de lenguajes de computación cuántica.

9.9. QuTech

Qtech es un centro tecnológico fundado en 2015 por la Delft University of Technology y la Netherlands Organisation for Applied Scientific Research (TNO) con el objetivo de investigar y desarrollar soluciones en el ámbito de la computación cuántica. En la actualidad Qtech oferta *Quantum Inspire* (QI), una plataforma de computación cuántica que proporciona acceso a un entorno de programación, diseño y ejecución para algoritmia cuántica cuya estructura en capas se indica en la parte izquierda de la Fig. 50.

A través de una interfaz gráfica, los desarrolladores pueden utilizar el entorno de desarrollo y programar sus soluciones software. Para ello QI proporciona un lenguaje de programación propio denominado *cQASM* [238], en el que se integra una intefaz programada en Python para acceder a la API REST de la plataforma QI. La estructura de bloques para trabajar con este lenguaje se esquematiza en la parte derecha de la Fig. 50. La fase de compilación utiliza los bloques de OpenQL y ProjectQ [427]. *cQASM* utiliza como base el lenguaje de representación intermedia QASM (apartado 12.2.1) y permite definir circuitos sencillos, si bien se infiere que será preciso un nivel de abstracción más elevado para poder gestionar el gran número de qubits que se utilizarán en el futuro.

La estructura hardware a la que se puede acceder está diseñada utilizando tecnología de espines. En concreto, disponen de una QPU (denominada *Spin-2*) que utiliza dos qubits y que proporciona un elevado período de coherencia y una QPU (denominada *Starmon-5*) que tiene cinco qubits con una topología en forma de X.

Para poder trabajar sin necesidad de este *back-end*, disponen también de varios simuladores (denominados *QX Quantum computer simulator*) con los que se podría trabajar con hasta 34 qubits.

10. Soluciones hardware

En este apartado se detallan las principales propuestas para computación cuántica de empresas centradas únicamente en el desarrollo del hardware. En el momento actual, lo más frecuente (dada la carencia de estándares) es ofertar soluciones integrales, pero aún así hay algunas empresas que prefieren llegar a acuerdos con otras que oferten soluciones software y enfocar su actividad exclusivamente en la tecnología hardware. En concreto, se resume el trabajo de las siguientes empresas: IonQ (apartado 10.1), Oxford quantum Circuits (apartado 10.2) y Alpine Quantum Technologies (apartado 10.3).

10.1. IonQ

IonQ, fundada en 2015 por investigadores de la University of Maryland, proporciona soluciones hardware basadas en tecnología de trampas de iones y, en el momento de escribir este documento, ofrece varios equipos de computación cuántica:

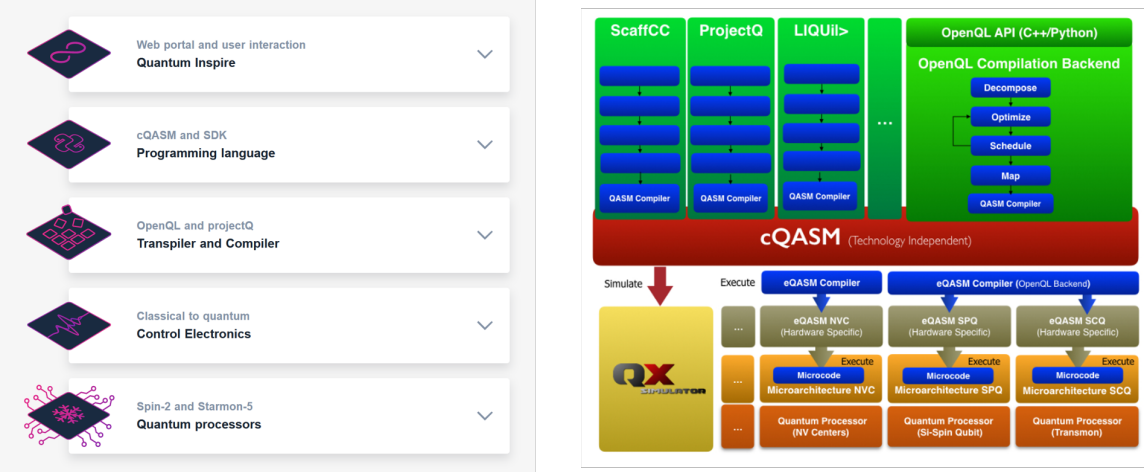


Figura 50: Estructura de la solución integral de Qtech (QI) (izquierda) y arquitectura de bloques para trabajar con el lenguaje cQASM (derecha) [https://www.quantum-inspire.com/].

- *IonQ Harmony*, dotado de 11 qubits, un valor de $\#AQ$ de 9 y una fiabilidad de 99,6 % para una puerta de un qubit y de 97,3 % para una puerta de dos qubits;
- *IonQ Aria*, dotado de 25 qubits, un valor de $\#AQ$ de 25 y una fiabilidad de 99,94 % para una puerta de un qubit y de 99,4 % para una puerta de dos qubits; e
- *IonQ Forte*, dotado de 32 qubits, un valor de $\#AQ$ de 29 y una fiabilidad de 99,98 % para una puerta de un qubit y de 99,6 % para una puerta de dos qubits.

Todos ellos disponen de una topología de interconexión total entre todos los qubits. Actualmente la empresa dispone de un nuevo ordenador cuántico, que no se encuentra en producción, denominado *IonQ Inquire*, que supera todos los parámetros actuales de la solución más potente (*IonQ Forte*), si bien la empresa no concreta detalles de eficiencia ni características de diseño (Fig. 51).

Para acceder a estas soluciones hardware, IonQ tiene convenio con las plataformas de computación en la nube más conocidas (Google Cloud, AWS y Microsoft Azure) y ofrece también acceso desde la plataforma de computación en la nube que ofrece la propia empresa, *IonQ Quantum Cloud*. En la Fig. 51 se detalla qué ordenadores cuánticos están accesibles para cada plataforma, así como los servicios a los que se podría acceder de forma adicional (como los simuladores tanto de modelado de ruido como el simulador para los sistemas IonQ) y la compatibilidad con las plataformas de desarrollo más habituales. Es preciso notar que para acceder al computador más avanzado (*IonQ Forte*) es preciso realizar una solicitud específica que ha de ser evaluada por la compañía, que sólo permite su acceso a un número reducido de investigadores y clientes[14].

[14] En el siguiente enlace se recogen las investigaciones publicadas que se han llevado a cabo utilizando esta plataforma por equipos de investigación de IonQ: https://ionq.com/resources/publications

	IonQ Quantum Cloud	Amazon Braket	Microsoft Azure	Google Cloud
	Get Started	Get Started	Get Started	Get Started
System Availibility				
Harmony	✓	✓	✓	✓
Aria	✓	✓	✓	—
Forte	Coming Soon Request Early Access →	—	—	—
IonQ Simulator	✓	—	✓	✓
Noise Model Simulation	✓	—	—	✓
Pricing	Volume Based Pricing Request Custom Pricing →	Pricing Details →	Pricing Details →	Pricing Details →
Features				
On demand access	✓	✓	✓	✓
Reservations	✓	—	—	✓
Application/ Dev Support	✓	✓	✓	✓
IonQ Quantum Cloud Console	✓	—	—	✓
Fully Managed Hybrid Environment	—	✓	✓	—
Native Gate Access	✓	✓	—	✓
SDK Compatibility				
Qiskit	✓	✓	✓	✓
Cirq	✓	—	✓	✓
Q#	—	—	✓	—
PennyLane	✓	✓	—	✓
See Additional SDK Support				
CQ tket	✓	—	—	✓
QCW Forge	✓	—	—	✓
ProjectQ	✓	—	—	✓
Braket	—	✓	—	—

Figura 51: Vías de acceso a los computadores cuánticos de IonQ a través de plataformas de computación en la nube [https://ionq.com/]

10.2. Oxford Quantum Circuits (OQC)

Oxford Quantum Circuits (OQC) basa sus desarrollos hardware en la tecnología de superconductores y en un desarrollo propio, denominado *Coaxmon* [372], que permite escalar el número de qubits manteniendo su calidad. Esta innovación proporciona una arquitectura tridimensional que reduce los problemas habituales de los circuitos tradicionales 2D.

Para acceder a sus equipos de computación, OQC establece cuatro vías posibles. La principal es directamente a través de su propia plataforma de computación en la nube que ofertan bajo un acceso QCaaS (*Quantum Computing-as-a-Service*). Adicionalmente, ofrecen acceso vía Amazon Braket (apartado 11.1), Cyxtera y Equinix.

Si bien, a diferencia de otras empresas previamente mencionadas, OQC no se centra en la provisión de plataformas de desarrollo software, sí tiene convenios con empresas para que el software que estas proporcionan sea ofertado en la infraestructura hardware de OQC. Adicionalmente, OQC también colabora en un proyecto dirigido por Riverlane para obtener un sistemas operativo, denominado *Deltaflow.OS*, que permita operar cualquier algoritmia cuántica (software) en cualquier hardware de computación cuántica (apartado 12.4).

10.3. Alpine Quantum Technologies (AQT)

Alpine Quantum Technologies (AQT) desarrolla sus soluciones de computación cuántica utilizando tecnologías basadas en trampas de iones. Ofertan una solución para ser integrada localmente en centros de datos que habilita 20 qubits totalmente interconectados y que se puede instalar en un *rack* estándar de 19 pulgadas, siendo la empresa pionera en comercializar este tipo de integración de hardware. Su base diferencial, atendiendo a los resultados que hacen públicos, es el trabajo realizado en la corrección de errores, lo que les permite tener tasas muy bajas y así mejorar el rendimiento de los equipos y qubits disponibles.

Adicionalmente, AQT comercializa cuatro módulos que permiten trabajar con tecnologías cuánticas: (i) un módulo, denominado *Beech* que permite la estabilización de la frecuencia de láseres; (ii) *Pine Grap*, un módulo que permite almacenar y manipular de forma coherente partículas cargadas; (iii) *Pine Set-up*, el elemento clave de su solución hardware, una trampa de iones de alta precisión almacenada en una cámara de vacío con la que la empresa indica que ha creado el mayor estado cuántico entrelazado utilizando 24 iones de calcio; y (iv) *Rowan*, un modulador que permite gestionar de forma eficaz los pulsos de láser.

11. Computación cuántica como servicio: oferta en la nube

La mayoría de las empresas que proporcionan soluciones integradas hardware-software (apartado 9) y soluciones hardware (apartado 10), permiten acceder de forma remota a sus ordenadores cuánticos, ofertando su propia plataforma de computación cuántica en la nube. Sin embargo, las grandes provisoras de computación en la nube no podían quedar al margen de este cambio tecnológico, y las tres más destacadas (Amazon AWS, Azure y Google) ofertan también sus servicios de computación en la nube. Google ha trabajado también en la provisión de nuevas soluciones tecnológicas para el hardware, pero Amazon AWS y Azure se centran fundamentalmete en proporcionar acuerdos con empresas terceras y ofertar soluciones software para el desarrollo de algoritmia híbrida cuántica-clásica.

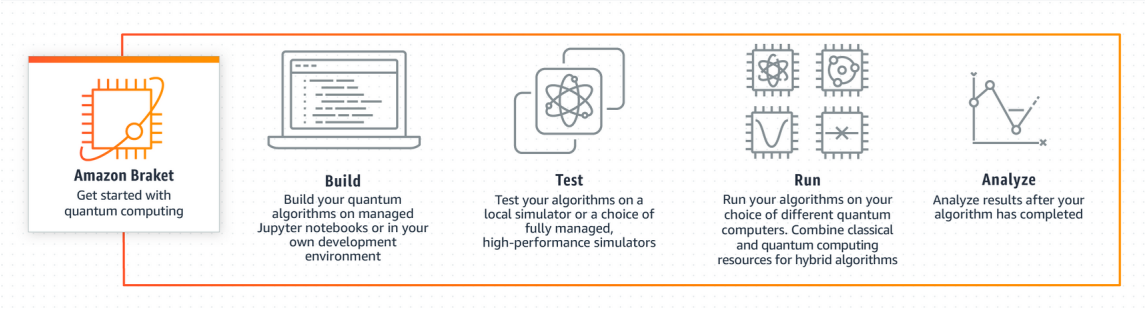


Figura 52: Esquema de trabajo para Amazon Braket [https://aws.amazon.com/es/braket/].

Use case	Local simulator	SV1	TN1	DM1
Debugging & prototyping	✓			
Large scale experiments		✓	✓	✓
Simulate many circuits in parallel		✓	✓	✓
Study the effects of noise	✓			✓
Simulate circuits with special structure			✓	

Figura 53: Servicios de simulación disponibles en Amazon Braket [https://aws.amazon.com/es/braket/].

11.1. AWS: Amazon Braket

Amazon, a través de su plataforma de computación en la nube AWS (*Amazon Web Services*) oferta una vía de acceso, denominada Amazon Braket, con computadores cuánticos, facilitando también un entorno que permita el desarrollo del software. En la Fig. 52 se muestra la funcionalidad disponible en esta plataforma.

El proceso comenzaría con el diseño e implementación del código para computación cuántica, para lo que Amazon Braket ofrece varias opciones. Se puede utilizar directamente su propio entorno de desarrollo, denominado Amazon Braket Python SDK, bien vía la consola AWS o bien localmente instalando el Amazon Braket SDK en el entorno de desarrollo local o cuaderno Jupyter. Otras vías posibles serían la utilización del entorno de desarrollo PennyLane (apartado 9.5) o bien Qiskit (apartado 9.1), ambas opciones implicarían utilizar los *plugins* que proporciona el propio Amazon Braket.

Antes de realizar ninguna ejecución en las computadoras cuánticas que oferta AWS, se sugiere comenzar con los entornos de simulación, para los que se ofertan las opciones resumidas

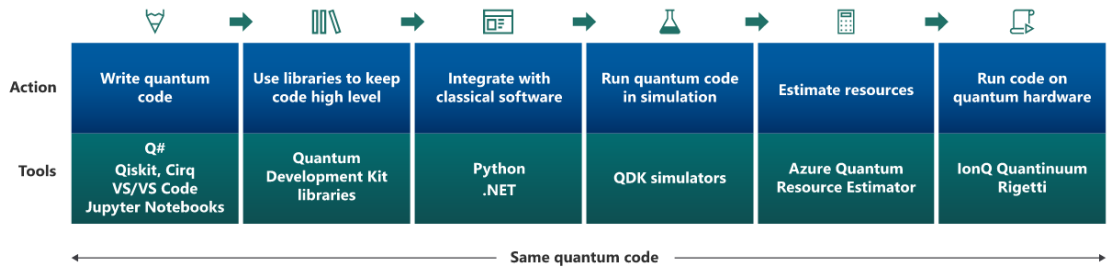


Figura 54: Flujo de trabajo para programación y ejecución en Azure [https://azure.microsoft.com/es-es/products/quantum/].

en la Fig. 53. Tras la instalación del AWS Braket SDK, es posible hacer simulaciones locales, aunque estas estarán fuertemente condicionadas por las características de hardware disponible localmente, por lo que para ejecuciones más pesadas se puede usar algunas de las opciones que oferta AWS: SV1 para simulaciones de hasta 34 qubits, DM1 para simular el efecto del ruido en hasta 16 qubits o TN1 para simular circuitos cuánticos de hasta 50 qubits. Igualmente estas tres opciones permitirían simular circuitos en paralelo.

Finalmente, la ejecución del software diseñado se realizaría utilizando el hardware disponible en AWS, que abarca tecnologías y empresas diferentes. En el momento de redactar este documento, Amazon Braket tiene convenio con cuatro empresas proveedoras de hardware para computación cuántica[15] (i) Rigetti (apartado 9.2) y OQC (apartado 10.2), utilizando tecnologías de superconductores; (ii) IonQ (apartado 10.1), que se basa en tecnología de trampas de iones; y (iii) QuEra (apartado 9.7), que utiliza procesadores basados en átomos neutros.

11.2. Azure Quantum

Microsoft, a través de su plataforma de computación en la nube Azure, oferta el servicio de computación denominado Azure Quantum, para el que propone un flujo de trabajo similar al de otras proveedoras de este servicio en la nube, detallado en la Fig. 54, donde se mencionan algunas de las plataformas y soluciones software y hardware que se podrían adoptar en cada paso.

Para el diseño de la algoritmia, Azure integra su propio entorno de desarrollo (*Quantum Development Kit*) y un lenguaje de alto nivel desarrollado por Microsoft (de código abierto) denominado *Q#*. Está diseñado para ser independiente del hardware, ofrece un elevado nivel de abstracción y no incorpora ninguna noción de estado cuántico o circuito. En su lugar *Q#* trabaja con instrucciones y expresiones muy similares a las habituales en los lenguajes de programación clásicos, lo que permite una integración de la computación híbrida (cuántica-clásica) muy natural, dado que los qubits son entendidos como recursos que se solicitan en el entorno de ejecución cuando son necesarios (de forma análoga al uso de memoria en la computación tradicional) y son modelados como tipo de datos opacos dentro del lenguaje.

En cualquier caso, y como se puede apreciar en la Fig. 54, Azure tiene integrados varios entornos de desarrollo populares para la programación cuántica además de *Q#*, como son *Qiskit*

[15] El listado de empresas colaboradoras se actualiza en el enlace siguiente: https://aws.amazon.com/es/braket/quantum-computers/

(apartado 9.1) y *Cirq* (apartado 11.3). Permite programar directamente en cuadernos Jupyter integrados en el espacio de trabajo de Azure o bien que se haga de forma local usando los entornos de desarrollo que se desee, si bien Azure ofrece extensiones para programar en *Q#* con las extensiones desarrolladas para el Visual Studio 2022 y el Visual Studio Code. Se recomienda el uso de librerías que ya implementan algunos de los algoritmos más habituales en aplicaciones de aprendizaje máquina o ML (*Machine Learning*) para el lenguaje *Q#*, dado que así el trabajo se puede centrar en la parte lógica de alto nivel.

Azure ofrece la posibilidad de combinar software escrito en *Q#* con Python y .NET para poder disponer de soluciones integradas que combinen computación cuántica y clásica. Para facilitar esta computación híbrida, Azure ofrece cuatro arquitecturas, cuyas características se resumen en la Fig. 55:

- *Batch quantum computing*. En esta solución, el cliente se ejecuta localmente y define y envía los trabajos que han de ser ejecutados en una QPU a la nube, que devuelve el resultado una vez han concluido. Al agrupar las diferentes taras en un único trabajo se reducen los tiempos de trasiego y de espera. Algunos algoritmos que son adecuados para este tipo de arquitectura serían el algoritmo de Shor o el *simple quantum phase estimation*

- *Interactive quantum computing*. En esta solución, el cliente se ejecuta en la nube, lo que reduce la latencia en las comunicaciones y permite repetir la ejecución del mismo circuito cuántico (variando los parámetros) de forma sencilla y directa. Es posible agrupar los trabajos en una única sesión y así establecer un sistema de prioridades entre sesiones. Si bien la ejecución en una única sesión permite reducir los tiempos de espera, es necesario notar que los estados de los qubits no permanecen entre una iteración y la siguiente. Este tipo de arquitectura es interesante para algoritmos como el VQE o el QAOA (*Quantum Approximate Optimization Algorithms*).

- *Integrated quantum computing*. En esta solución la arquitectura cuántica y clásica están muy imbricadas, lo que permitiría que se realicen cálculos clásicos durante los períodos de coherencia de los qubits. Esto permite que, a la hora del diseño, se utilicen construcciones programáticas habituales para optimizar y reutilizar qubits. Este tipo de arquitectura es adecuada para algoritmias de ML, por ejemplo.

- *Distributed quantum computing*. En esta solución la computación clásica trabaja con qubits lógicos. Estos permiten disponer de amplios tiempos de coherencia y así se pueden ejecutar computaciones más complejas y distribuidas usando infraestructura hardware heterogénea. Si a esto se le une un número elevado de qubits, se dispondría de una plataforma con capacidad de ejecución que permitiría abordar algoritmos más complejos y computacionalmente más costosos.

Antes de realizar la ejecución del software en las soluciones hardware disponibles, Azure ofrece la posibilidad de utilizar simuladores cuánticos para realizar tareas de validación y pruebas. Actualmente, Azure ofrece dos opciones para la simulación:

- Simuladores genéricos embebidos en el QDK, lo que permite la ejecución local y, por tanto, más rápida. Se ofrecen cinco opciones diferentes, cuyas características están resumidas en la Fig. 56. En función de las necesidades de la algoritmia, se seleccionará una u otra opción para simular la ejecución del código.

Figura 55: Arquitecturas de computación híbrida en Azure [https://azure.microsoft.com/es-es/products/quantum/].

Simulator	Class	Namespace	Description
Full state simulator	`QuantumSimulator`	`Microsoft.Quantum.Simulation.Simulators`	Runs and debugs quantum algorithms, and is limited to about 30 qubits.
Sparse simulator	`SparseSimulator`	`Microsoft.Quantum.Simulation.Simulators`	Simulates quantum algorithms with sparse states, small number of states in superposition.
Trace-based resource estimator	`QCTraceSimulator`	`Microsoft.Quantum.Simulation.Simulators`	Runs advanced analysis of resources consumptions for the algorithm's entire call-graph, and supports thousands of qubits.
Toffoli simulator	`ToffoliSimulator`	`Microsoft.Quantum.Simulation.Simulators`	Simulates quantum algorithms that are limited to `X`, `CNOT`, and multi-controlled `X` quantum operations, and supports million of qubits.
Noise simulator	`OpenSystemsSimulator`	`Microsoft.Quantum.Simulation.Simulators`	Simulates quantum algorithms under the presence of noise, and also the *stabilizer representation* (also known as CHP simulation) of quantum algorithms.

Figura 56: Simuladores ofertados por Azure y sus especificaciones [https://azure.microsoft.com/es-es/products/quantum/].

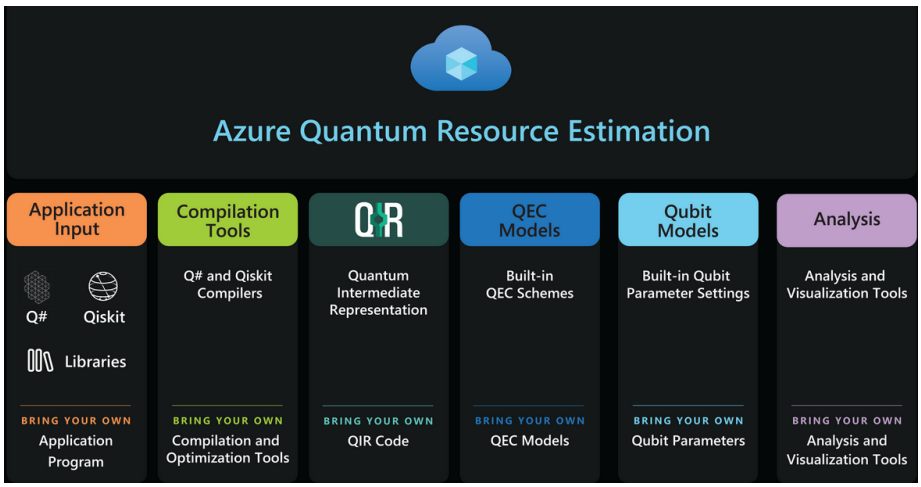


Figura 57: Servicios de estimación de recursos en Azure [https://learn.microsoft.com/es-MX/azure/quantum/intro-to-resource-estimation].

- Simuladores específicos que son ofertados por entidades terceras a Microsoft y que permiten una simulación más precisa porque tienen en cuenta las arquitecturas hardware de cada empresa. En el momento de redactar este documento Azure oferta la posibilidad de ejecutar simuladores externos proporcionados por tres empresas: IonQ (apartado 10.1), Quantinuum (apartado 9.3) y Rigetti (apartado 9.2), cada uno de ellos adaptado al hardware que proporciona.

En cualquier caso, Azure ofrece un servicio denominado *Azure Quantum Resource Estimation*, cuyos pasos se esquematizan en la Fig. 57, que permite analizar el impacto de las distintas opciones de diseño algorítmico utilizado en cuanto a los recursos necesarios para que pueda ser ejecutado de forma eficiente (número de qubits necesario, tiempo de ejecución, tecnologías de qubits más adecuadas, etc.). Como se indica en la misma figura, este estimador está basado en la representación QIR (apartado 12.2.2), facilitando así la operativa con cualquier lenguaje de programación compatible con esta representación interna.

Finalmente, la ejecución de los algoritmos diseñados se realiza en el hardware disponible por Azure Quantum, que abarca diferentes tecnologías proporcionadas por varias empresas. En el momento de realizar este documento, Azure Quantum tiene convenio con seis empresas: (i) Rigetti (apartado 9.2) y Quantum Circuits, Inc. (QCI), utilizando tecnologías de superconductores; (ii) IonQ (apartado 10.1) y Quantinuum (apartado 9.3), basadas ambas en tecnología de trampas de iones; (iii) Pasqal (apartado 9.4), que utiliza procesadores basados en átomos neutros y (iv) Toshiba, que oferta una solución de optimización de inspiración cuántica.

Sin embargo, no todos los convenios se encuentran operando en igual medida. El convenio con Quantum Circuits, Inc. (QCI) se encuentra en suspenso en el momento de redactarse este documento y no parece que vaya a activarse en los próximos meses. El convenio con Toshiba, si bien permite acceder a su solución algorítmica de optimización, no parece tener continuación temporal, dado que Microsoft Azure informa que será eliminado en los próximos meses de la plataforma. Finalmente, el convenio con Pasqal, que no está operativo en el momento de redactar este texto, sí que se espera que pueda estarlo al principio de 2024.

11.3. Google

Google ofrece servicios de computación cuántica a través de su plataforma Quantum AI, embebida en su plataforma de computación en la nube *Google Cloud*. El hardware, desarrollado internamente en la empresa, trabaja con tecnología de superconductores, obteniendo tres procesadores cuánticos en los últimos años: *Foxtail* en 2016, *Bristlecone* en 2017 y *Sycamore* en 2019. Este último es la base para el servicio de computación cuántica que ofrece Google y agrupa 54 qubits organizados en una topología cuadrangular, cuyas características técnicas están disponibles en la web de la empresa.

Google oferta el conjunto de servicios detallado en la Fig. 58, centrados en la parte software en el entorno de programación *Cirq*, una librería escrita en Python que permite escribir, manipular y optimizar circuitos cuánticos, para poder ser ejecutados en simuladores y computadores cuánticos. Para poder probar el software desarrollado, se ofertan dos opciones de simulación. Un simulador integrado en *Cirq*, desarrollado también en Python, para poder ejecutar circuitos sencillos de hasta 20 qubits. Un simulador desarrollado en C++ denominado *Qsim* que también está integrado en *Cirq* y que permite ejecutar simulaciones de hasta 40 qubits usando una estación de trabajo Xeon de 90 núcleos. Con el objetivo de conseguir mayor eficiencia en la simulación, Google colabora con NVIDIA para utilizar su entorno cuQuantum SDK (apartado 12.3.2)

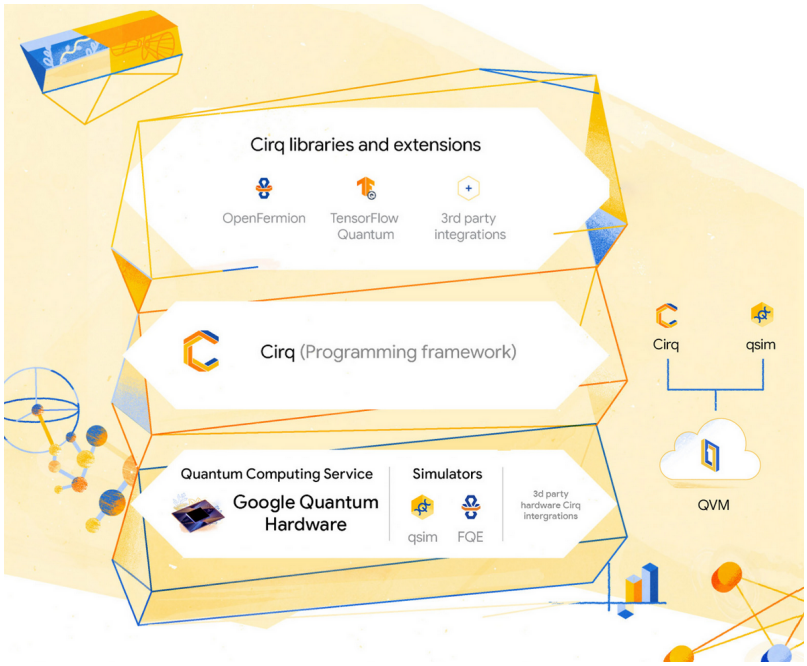


Figura 58: Estructura de servicios de computación ofertados por Google [https://quantumai.google/software].

y así acelerar la simulación en las GPUs que proporciona.

Para la ejecución de algoritmia Google proporciona una QVM (*Quantum Virtual Machine*) que permite realizar pruebas emulando el comportamiento del hardware cuántico de Google, entorno que se usará también cuando el hardware no esté disponible. Para facilitar el acceso, se ha implementado una vía de trabajo a través de Google Colab.

En la documentación pública proporcionada por Google, no está realmente claro si es posible acceder al hardware desarrollado por la empresa para ejecutar algoritmia cuántica. En su lugar, parece que el modelo de trabajo por el que apuesta Google es la provisión de un entorno completo para la simulación de computación cuántica y el entorno de programación *Cirq*, que permite trabajar con soluciones hardware de varias empresas destacadas del sector, como Alpine Quantum Technologies (apartado 10.3), IonQ (apartado 10.1), Pasqal (apartado 9.4) o Rigetti (apartado 9.2). Para reforzar esta línea, se puede observar que, de hecho, sus trabajos en el diseño e implementación de soluciones hardware no han avanzado sustancialmente desde la creación de *Sycamore* en 2019 y que, dentro de la documentación de *Cirq* se ofrece la opción de trabajar con las soluciones en la nube proporcionadas por Microsoft Azure, en concreto para acceder a las soluciones hardware de Quantinuum y de IonQ.

12. Soluciones software

La falta de unificación tecnológica a la hora de implementar soluciones hardware para la computación cuántica ha traído consigo la necesidad de ofrecer soluciones específicas para el desarrollo de software. Esta línea de trabajo es la que han seguido la mayoría de las empresas, con las aportaciones resumidas en los apartados previos, creando así soluciones integradas y verticales hardware-software. En cualquier caso, y de forma paralela, algunos equipos de investigación, empresas y asociaciones de empresas han venido trabajando en la provisión de soluciones más genéricas (lenguajes de programación, entornos de desarrollo software o SDKs, compiladores), que puedan ser utilizadas con diferentes soportes hardware y que permitan el diseño de algoritmia híbrida cuántica-clásica de adopción estándar.

12.1. Lenguajes de programación

En la revisión de las soluciones integrales ofertadas por las principales empresas del sector (apartado 9) se mencionaron ya algunos lenguajes de programación. Algunos son específicos para la infraestructura de la empresa, (i) como es el caso de QUIL, diseñado por Rigetti (apartado 9.2), que permite la descripción textual de secuencias de instrucciones y que consta de su propio compilador *quilc*; y de (ii) Pulser Studio, diseñado por Pasqal (apartado 9.4), que con una orientación totalmente diferente ofrece una interfaz gráfica sin código escrito.

De las opciones revisadas, destaca por su versatilidad el caso de $Q\#$, lenguaje de programación diseñado por Microsoft e integrado dentro de su solución cuántica en la nube (*Quantum Development Kit*, apartado 11.2). $Q\#$ fue diseñado para ser independiente del hardware y ofrece un elevado nivel de abstracción (no trata el concepto de circuito y/o estado cuántico) muy similar a los lenguajes de programación clásicos, lo que facilita el desarrollo de algoritmia híbrida cuántica-clásica y permite su uso en plataformas diferentes a la proporcionada por la propia empresa, como es el caso de la plataforma TKET de Quantinuum (apartado 9.3).

Con la intención compartida con $Q\#$ de ofertar lenguajes transversales, se pueden encontrar en la literatura especializada otras opciones como las que se describen a continuación. Dentro de las opciones de programación gráficas y transversales destaca *ZX-calculus* (apartado 12.1.1) y en las opciones más tradicionales de código escrito se debe mencionar Quipper (apartado 12.1.2).

12.1.1. ZX-calculus y PyZX

ZX-calculus [473, 106] es un lenguaje de programación gráfico que permite trabajar con diagramas ZX, para representar mapas lineales arbitrarios entre qubits, lo que facilita la representación convencional en diagramas de circuitos cuánticos (Fig. 59).

PyZX [249] es una extensión del lenguaje de programación gráfico *ZX-calculus*, una librería codificada en Python, que permite optimizar circuitos cuánticos, conjugarlos, validarlos y visualizarlos y que se puede utilizar conjuntamente con otro software para tener un conjunto completo de herramientas que permitan trabajar con soluciones cuánticas. En la Fig. 60 se resume la funcionalidad que se ofrece y las herramientas que la complementan. Se sugiere trabajar con cuadernos Jupyter, dado que al facilitar la ejecución de código Python se pueden visualizar la representaciones de los circuitos de forma sencilla y utilizar TikZit, una interfaz gráfica para diseñar diagramas ZX. Asimismo, PyZX se puede utilizar con otro tipo de lenguajes de representación de circuitos cuánticos, como OpenQASM (apartado 12.2.1), que permita bajar de nivel

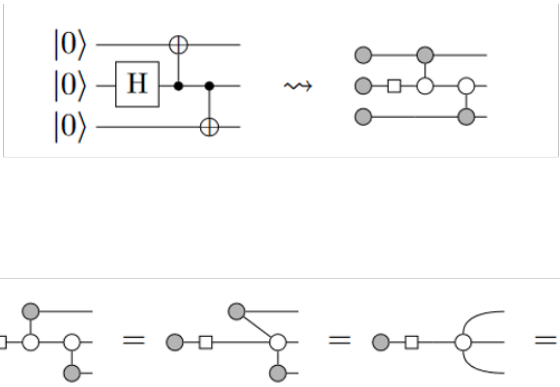


Figura 59: Representación de un circuito cuántico usando un diagrama ZX (parte superior) y diferentes tipos de diagramas en *ZX-calculus* (parte inferior) [473].

de abstracción y aproximarse a la infraestructura de ejecución hardware.

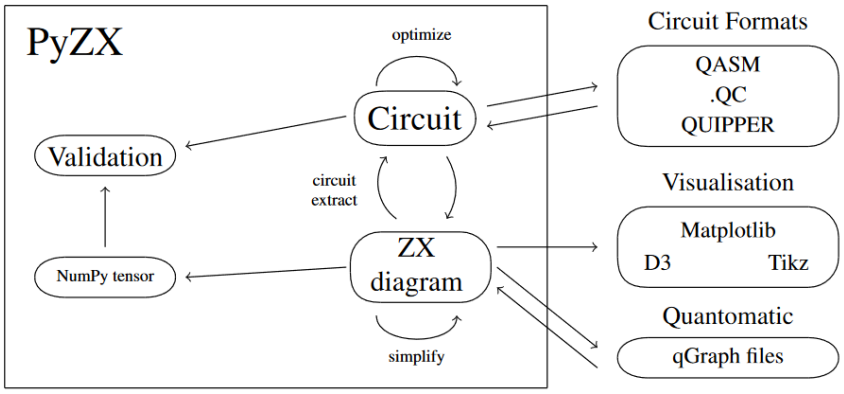


Figura 60: Funcionalidad de PyZx y su integración en un ecosistema software para soluciones cuánticas [249].

12.1.2. Quipper

Quipper [184] es un lenguaje embebido en Haskell [215], un lenguaje de propósito general. Por tanto, se puede entender que Quipper ofrece un conjunto de tipos de datos, combinadores y una biblioteca funcional dentro de Haskell que, al igual que el lenguaje que lo acoge, es fuertemente tipado. Trabaja con el concepto de circuito cuántico, por lo que, a diferencia de lo que ocurre con *C#*, es próximo al concepto hardware para el que se ha diseñado.

El código escrito en este lenguaje ha de compilarse en dos fases o etapas: una genérica, que puede hacerse en un compilador Haskell en una plataforma de computación clásica, y una posterior, para la generación de los circuitos. En su momento planteaba una alternativa interesante

a otros lenguajes más antiguos, como QCL [348], pero en la actualidad no es una opción que parezca que haya evolucionado como para suponer una alternativa de interés.

12.2. Representación intermedia o IR

En esta línea de trabajo surgen las iniciativas para tratar de tener un estándar de representación intermedia (IR), cuya necesidad se adelantó en el apartado 6.3.2. Así, se podrían transformar programas escritos en cualquier lenguaje utilizado para la programación cuántica en esta representación intermedia que, sin ser un lenguaje de alto nivel sí sería de mayor nivel que el lenguaje necesario para poder operar con el hardware disponible (qubits) y sus características físicas, para lo que habría que hacer un siguiente paso de compilación o transformación. En este ámbito destacan los intentos de estandarización realizados por los principales actores del ámbito cuántico (empresas, universidades y centros tecnológicos) que se materializaron fundamentalmente en dos opciones: (i) OpenQASM: *Open Quantum Assembly Language* (apartado 12.2.1) y (ii) QIR: *Quantum Intermediate Representation* (apartado 12.2.2).

12.2.1. OpenQASM: *Open Quantum Assembly Language*

Una de las iniciativas destacadas para la provisión de una representación intermedia para algoritmia cuántica es la solución OpenQASM que, propuesta en el año 2017 [113], llegó a ser un estándar *de facto* para describir e intercambiar modelos de circuitos cuánticos al ser promovido por entidades de peso de este ámbito (Zurich Instruments, IBM Quantum, Zapata Computing, AWS Center for Quantum Computing y la Universidad de Oxford)

Su diseño surge al tratar de unificar intentos previos de representar este tipo de circuitos, todos ellos denominados QASMs (*Quantum Assembly Languages*), como una forma de ofrecer una única representación interna (IR) legible para los desarrolladores y que sirviese como nexo a la hora de permitir la interoperabilidad entre diferentes soluciones hardware-software.

OpenQASM combina elementos del lenguaje de programación C y de soluciones previas QASM para permitir especificar algoritmos híbridos bajo la siguiente filosofía: la visión de un algoritmo híbrido clásico-cuántico como una secuencia de circuitos cuánticos intercalados con elementos de computación clásica. Así, y tal y como se muestra en la fase 3 de la Fig. 61, se tendría un conjunto de circuitos cuánticos controlados (alto nivel) por instrucciones clásicas. Sería en la fase 2 (generación de circuitos) donde se obtendría esta representación interna que, haciendo uso de las APIs propias del entorno hardware disponible, podrían ser llevadas en una fase posterior para su ejecución. Es decir, aunque OpenQASM es un lenguaje de programación de bajo nivel, no puede ser ejecutado directamente por el hardware cuántico, sino que deberá ser adaptado en función de las características del hardware disponible.

Recientemente, en el año 2022, se publicó una actualización o nueva versión de esta representación intermedia: OpenQASM 3 [112]. Esta nueva representación se basa en la definición de una extensión de un circuito cuántico incorporando a la visión tradicional (secuencia de operaciones cuánticas sobre datos cuánticos) elementos de control de flujo clásico. De esta forma, sería posible describir circuitos más versátiles donde hay elementos que definen secuencias y flujos de datos entre las operaciones cuánticas tradicionales, integrando parte de las secuencias de control que en la versión anterior quedaban relegadas a elementos externos (tal y como se puede ver en el diagrama de la Fig. 61). Adicionalmente, OpenQASM 3 tiene en cuenta los condiciones físicos del entorno de ejecución hardware y, por ello, centra el modelo en la circuitería que debe ser ejecutada en tiempo real, es decir, en el tiempo de coherencia de los qubits,

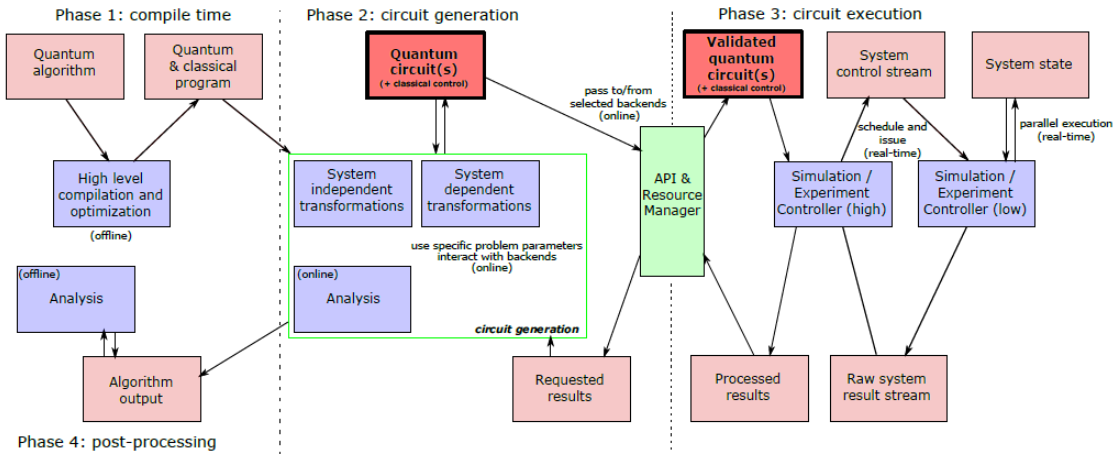


Figura 61: Diagrama modular del proceso de transformación y ejecución de un algoritmo cuántico desde la perspectiva de la representación interna de OpenQASM [113].

condicionada por la estructura física. Debido a ello, se incorpora en OpenQASM 3 la posibilidad de definir la calibración de las puertas (a nivel de pulso), además de la especificación de parámetros temporales. Con el objetivo de mantener la interoperabilidad lograda con OpenQASM, los circuitos expresados con la versión anterior son perfectamente interpretados en la posterior sin necesidad de realizar adaptaciones al software.

El modelo de compilación y ejecución que se detalla en el estándar OpenQASM 3 asume lo siguiente (tal y como se representa en la Fig. 62). Cualquier aplicación estará compuesta por programas cuánticos e híbridos que podrán ser ejecutados en el soporte hardware a través de circuitos cuánticos representados en OpenQASM 3 y funciones externas para la ejecución en tiempo real (dentro de los períodos de coherencia). En la figura se representa la secuencia de compilación que, básicamente, se organiza en una representación lógica (*logical OpenQASM*), que definiría los circuitos cuánticos extendidos definidos en OpenQASM 3, y una física (*physical OpenQASM*), que permite *mapear* y organizar la ejecución de estos circuitos en qubits.

Tal y como está definida esta representación, sería posible utilizar un lenguaje de más alto nivel para la especificación de la algoritmia, para después ser transformada en la representación interna OpenQASM 3.

12.2.2. **QIR:** *Quantum Intermediate Representation*

El estándar QIR (*Quantum Intermediate Representation*) ha sido propuesto por la QIR Alliance, como uno de los elementos clave para tratar de ofertar un especificación completa e interoperable para programación cuántica. La QIR Alliance forma parte de The Linux Foundation, una organización sin ánimo de lucro que pretende promover el código abierto, y pertenecen a ella entidades como Microsoft, NVIDIA, OAK Ridge National LAboratory, Quantinuum, Quantum Circuits Inc. o Rigetti Computing.

El estándar QIR (*Quantum Intermediate Representation*) se basa en la solución de código abierto LLVM (*Low Level Virtual Machine* [262]), una representación interna utilizada para la creación de compiladores que ha sido desarrollada en lenguaje C++. La filosofía que subyace

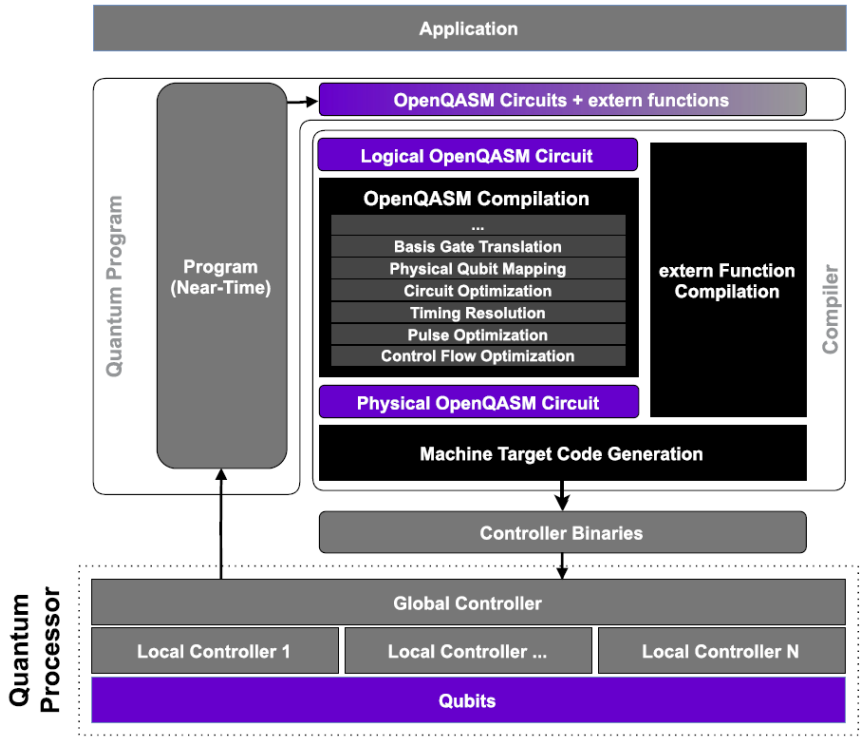


Figura 62: Flujo de compilación y ejecución para OpenQASM 3 [112].

tras QIR es la de disponer de una única representación intermedia que pueda expresar programas escritos en cualquier lenguaje utilizado para la programación cuántica y que pueda convertirse en código para cualquier ordenador cuántico, permitiendo disponer de un puente para que cualquier lenguaje pueda operar en cualquier ordenador. Por lo tanto, QIR trabajaría sobre cualquier lenguaje que pueda expresar la programación de puertas cuánticas, como es el caso de *Q#* (apartado 11.3) o *Qiskit* (apartado 9.1), y también opera sobre cualquier hardware dado que no especifica un conjunto de instrucciones para la operativa con puertas lógicas cuánticas. La fig. 63 muestra un ejemplo de representación QIR de un código sencillo escrito en *Q#*.

Para poder trabajar con QIR, la QIR Alliance ofrece algunas herramientas como

- El kit PyQIR, que permite generar, parsear y evaluar documentos QIR utilizando una API escrita en Python o bien una librería desarrollada en Rust.
- Una herramienta denominada QAT (*QIR Adaptor Tool*) que permite transformar una representación QIR en otra que cumpla ciertos requisitos.
- El compilador QCOR [342] que es una extensión del compilador de C++ para la programación híbrida cuántica-clásica.
- El simulador NWQSim (*NorthWest Quantum circuit Simulation Environment*), que permite

```
// Assumes that qb1 and qb2 are already in the |0> state
operation BellPair(qb1 : Qubit, qb2 : Qubit) : Unit
{
    H(qb1);
    CNOT(qb1, qb2);
}
```

(a)

```
define void @BellPair__body(%Qubit* %qb1, %Qubit* %qb2) {
entry:
  call void @__quantum__qis__h(%Qubit* %qb1)
  call void @__quantum__qis__cnot(%Qubit* %qb1, %Qubit* %
  ret void
}
```

(b)

Figura 63: Aspecto de la representación intermedia QIR (b) tras compilar un código sencillo en *Q#* (a)

simular el entorno cuántico sobre una infraestructura clásica multinodo y multi CPU/GPU típica de sistemas HPC.

12.3. Entornos de desarrollo o SDKs

En la revisión de las soluciones integrales ofertadas por las principales empresas del sector (apartado 9) se mencionaron algunos entornos de desarrollo destacados como Qiskit de IBM (apartado 9.1), TKET de Quantinuum (apartado 9.3) y PennyLane de Xanadu (apartado 9.5). Todos ellos son lo suficientemente versátiles y potentes como para que se hayan integrado como opciones de trabajo dentro de dos de las tres grandes plataformas de computación en la nube (Azure y AWS). Estas plataformas, también ofertan sus propios SDK para desarrollo de software cuántico: Azure Quantum de Microsoft (apartado 11.2), AWS Amazon Braket de Amazon (apartado 11.1) y Cirq de Google (apartado 11.3). Sin embargo, y analizando la documentación disponible, parece que son Azure y AWS las dos empresas que han optado por no hacer desarrollo hardware propio y centrar su modelo de negocio en la provisión de una solución transversal propia y también acoger con un rol de *broker* los SDKs de las empresas más destacadas del sector. Google, por el contrario, parece que apostaba por una solución integral (incluyendo hardware y software propio). Si bien, ahora la evolución seguida parece indicar que opta por la integración de soluciones hardware cuánticas de terceros trabajando con su propio SKD (Cirq).

Adicionalmente, en la literatura y en la oferta comercial se ofrecen dos soluciones SDK transversales que se detallan a continuación: projectQ (apartado 12.3.1) y la solución de NVIDIA (apartado 12.3.2).

12.3.1. projectQ

Adicionalmente, surge en el año 2018 una propuesta de entorno de desarrollo completo transversal y que pude operar con diferentes soluciones hardware: projectQ [427]. Se planteó como un entorno completo de desarrollo de software para computación cuántica basado en una filosofía modular, como se aprecia en la Fig. 64. Se parte de la definición de la algoritmia usando un lenguaje de alto nivel embebido en Python e integrando un conjunto de funciones especialmente definidas para el contexto cuántico. Este código será compilado a un lenguaje de menor nivel de abstracción, donde se traduzca la codificación a una representación basada en circuitos cuánticos y, finalmente, una compilación a lenguaje máquina ya altamente dependiente de la solución hardware disponible. En el entorno de trabajo de projectQ se facilita un simulador [194], si bien se puede ejecutar en plataformas disponibles en la nube.

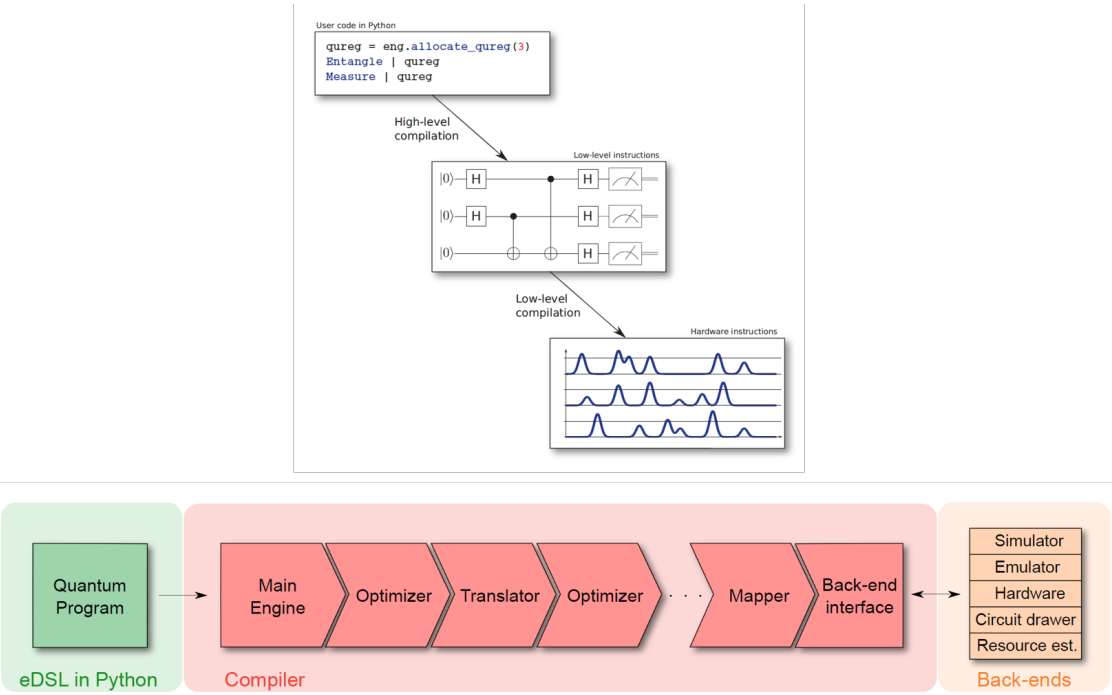


Figura 64: Resultados obtenidos en las diferentes etapas de compilación en projectQ [427].

Aunque en su momento se planteó como una solución transversal, de hecho se indica que se podría integrar en los SDKs de IBM, AWS, Azure e IonQ, la evolución de las propuestas hardware-sofware con el soporte del sector industrial han absorbido este tipo de iniciativas de origen universitario (ETH Zurich) cuyo progreso depende de financiación externa.

12.3.2. NVIDIA CUDA Quantum

NVIDIA oferta la plataforma NVIDIA CUDA Quantum orientada a la programación de sistemas cuánticos híbridos. La estructura en módulos es esquematiza en la Fig. 65 donde se puede apreciar que esta plataforma utiliza un compilador propio $NVQ++$ cuyo código resultante puede ejecutarse en entornos de computación híbridos QPUs (reales o emuladas), GPUs y CPUs. La representación intermedia utilizada por este compilador es QIR, dado que NVIDIA pertenece también a la QIR Alliance (apartado 12.2.2).

Para la ejecución en hardware de computación cuántica, NVIDIA trabaja con varios socios comerciales, como OQC, Pasqal, Quantinuum, o Rigetti, entre otros. Entre los recursos cuánticos, NVIDIA oferta el entorno NVIDIA cuQuantum disponible en GitHub, que acelera simulaciones de computadores cuánticos, lo que permite ir más allá de la oferta hardware actual. Para la emulación utiliza recursos propios, como la ejecución en una única GPU o bien utilizando nodos NVIDIA DGX equipados con GPUs de elevada capacidad.

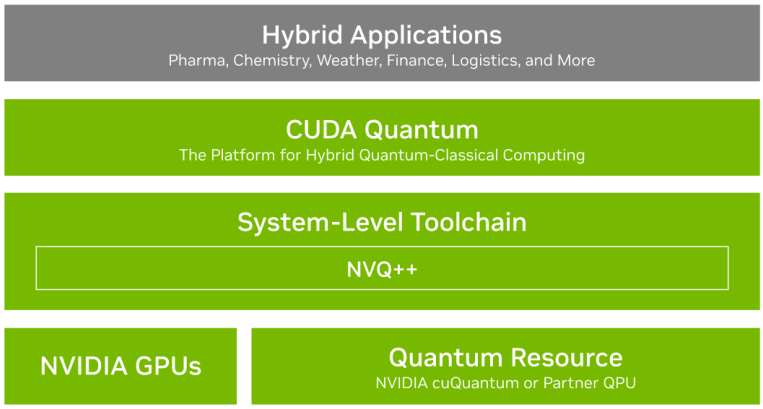


Figura 65: Estructura de la plataforma NVIDIA CUDA Quantum [https://developer.nvidia.com/cuda-quantum].

12.4. Sistemas Operativos

Si bien en este documento se han tratado diferentes líneas de trabajo en el ámbito software, el diseño de un sistema operativo que sea capaz de gestionar tareas (*jobs*) de naturaleza cuántica, clásica e híbrida no era uno de los objetivos. Cerca ya de las propuestas hardware, las grandes empresas que ofrecen soluciones en este campo disponen de sus propias soluciones que, en su mayoría, se asume que son ampliaciones o modificaciones de los sistemas de gestión de computación clásica.

Sin embargo, es un campo interesante si se plantea la posibilidad de crear un sistema operativo específicamente pensado para la computación cuántica que sea transversal, es decir, capaz de trabajar con diferentes lenguajes de programación y diferentes infraestructuras hardware. Esa es la idea que subyace en el diseño de *Deltaflow.OS*, el producto en desarrollo estrella de la empresa Riverlane.

Riverlane es una empresa de software que nace en 2016 a partir de investigadores de la Universidad de Cambridge con el objetivo de trabajar en el ámbito de la computación cuántica. Su principal producto es un sistema operativo, *Deltaflow.OS*, pensado para operar en un entorno de computación cuántica ruidoso. Para este desarrollo se han aliado con otras empresas del sector, de Reino Unido fundamentalmente, como Oxford Quantum Circuits (apartado 10.2). Si bien sus resultados de investigación se publican en foros internacionales de reconocido prestigio, pueden encontrarse agrupados en este enlace: https://www.riverlane.com/research.

El sistema operativo *Deltaflow.OS* [127] permite operar a cualquier conjunto de aplicaciones que requieran de computadores cuánticos y trabaja con cualquier tipo de hardware de computación cuántica. Tal y como se puede apreciar en la Fig. 66 consta de tres grandes bloques: (i) un sistema de control (*Deltaflow.Control*); (ii) un módulo de ejecución y (iii) un módulo de decodificación (*Deltaflow.Decode*).

- *Deltaflow.Control* se ocupará, idealmente, de trabajar con cualquier tipo de tecnologías cuánticas, si bien en la actualidad está operativo para qubits de trampas de iones y están desarrollándolo para que pueda operar con qubits basados en superconductores. Este

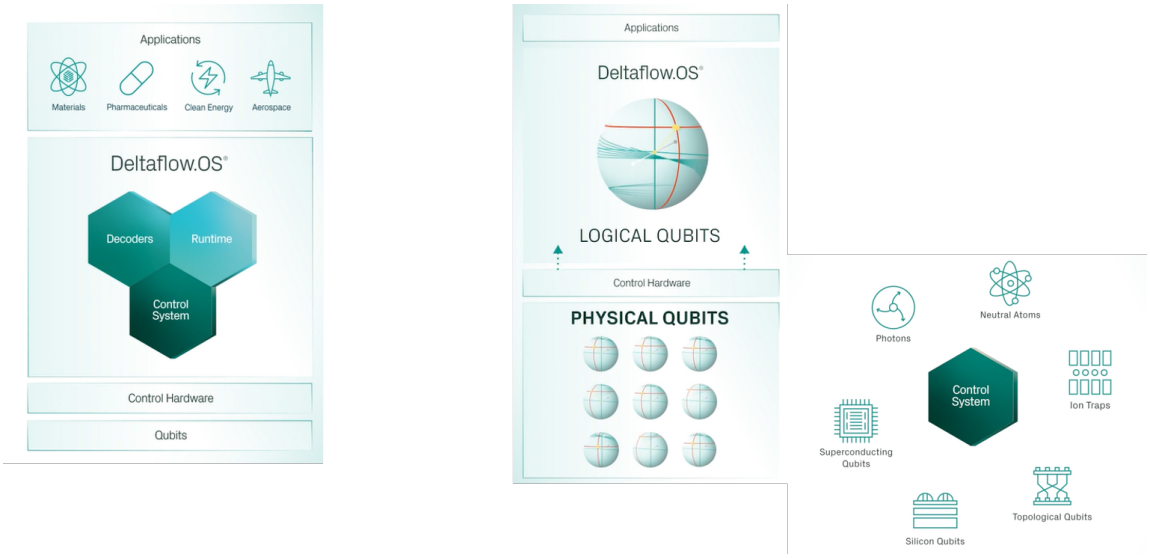


Figura 66: Esquema de bloques del sistema operativo *Deltaflow.OS* (izquierda) y operativa del módulo de control de errores (derecha) [`https://www.riverlane.com`].

módulo es totalmente programable en Python para poder definir los pulsos con los que manipular los estados cuánticos de los qubits para almacenar información, realizar cálculos y corregir errores. Para ello opera con qubits lógicos a partir de los qubits físicos que estén en el sistema subyacente.

- *Deltaflow.Decode* se ocupa de detectar errores que afectan a los qubits físicos cuando estos ocurren. Actualmente los equipos de investigacion de la empresa están trabajando en el desarrollo de técnicas que permitan decodificar y en cómo implementarlas en el hardware dedicado para poder abarcar la ingente cantidad de datos que es preciso procesar. Sus resultados de investigación en este ámbito han sido ya publicados en [417] y en [33].

Además de *Deltaflow.OS*, en la literatura se puede encontrar otra propuesta del año 2021 [254], que también aboga por un sistema transversal capaz de gestionar los recursos para ejecutar eficazmente código cuántico. En la Fig. 67 se puede ver la estructura de bloques donde se desglosa la gestión de la computación cuántica y la computación clásica. Sin embargo, y sin el apoyo de actores destacados del ámbito industrial, esta alternativa parece una propuesta teórica que difícilmente pueda transitar a una implementación real.

13. Conclusiones

Para finalizar, este apartado recoge las principales conclusiones técnicas acerca de la viabilidad de la computación cuántica distribuida, en dos partes, una primera sobre los retos de la computación cuántica en general, y una segunda más específica sobre las posibilidades tecnológicas de interconexión local de QPUs.

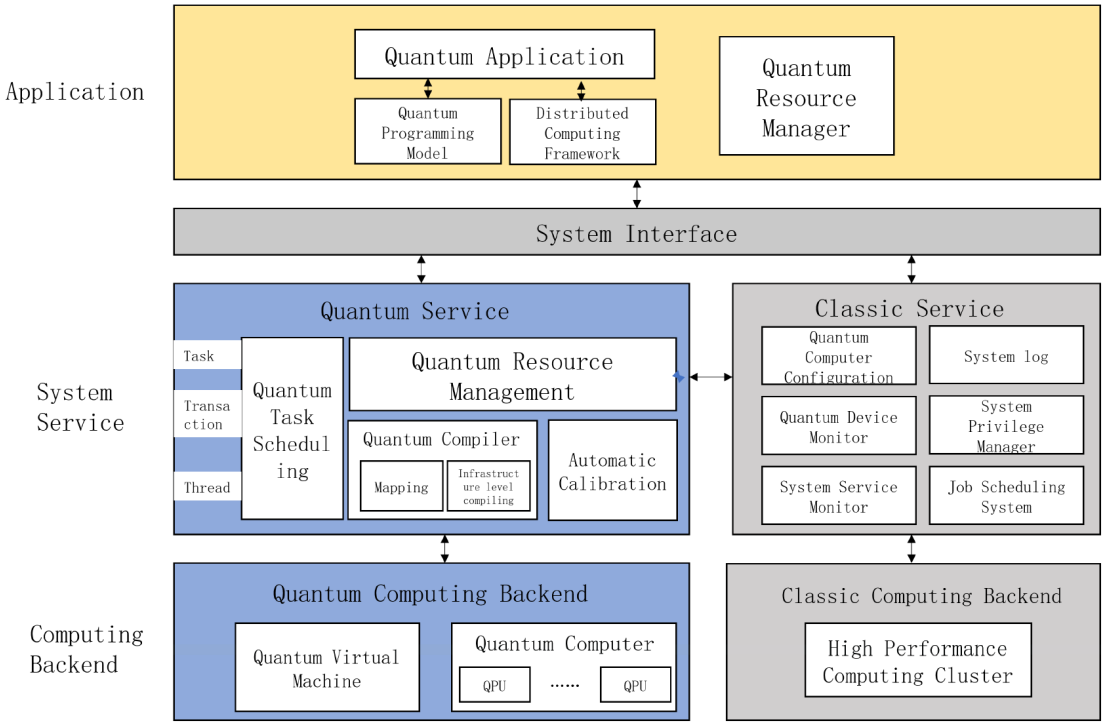


Figura 67: Arquitectura del sistema operativo Origin Pilot [254].

13.1. Retos en computación cuántica

El principal reto al que se enfrenta la computación cuántica es el de la estandarización, que es común a todos los niveles. Este problema comienza ya en el nivel físico, dado que no parece haber en la actualidad una tecnología que se pueda considerar más avanzada o con un conjunto de ventajas que la hagan ganadora frente al resto. De hecho, y como se puede ver en el apartado 7, a la hora de comparar este tipo de tecnologías hardware entre sí surgen diferentes medidas o criterios de benchmarking que, en muchos casos, están definidas o propiciadas por las propias empresas que comercializan sus soluciones hardware. Esto hace que, en consecuencia, las medidas se creen o redefinan *ad hoc* y ofrezcan resultados sesgados si se usan de forma individual. En cualquier caso, y a tenor de la situación actual, todo parece indicar que a medio plazo se tenderá hacia dos vías: una que permita el uso de pequeños computadores cuánticos para entidades o usuarios que no puedan disponer de infraestructuras complejas de frío y aislamiento y otra orientada a super-computación para centros especializados.

Este documento se ha centrado en las soluciones para este último ámbito (grandes centros de computación), pero ya hay algunas alternativas para usuarios o entidades con requisitos menos ambiciosos. Este es el caso, por ejemplo, de la empresa SpinQ que ha comenzado recientemente la comercialización de varios ordenadores cuánticos basados en la tecnología NMR (*Nuclear Magnetic Resonance*) de 2 y 3 qubits (denominados *Gemini* y *Triangulum* respectivamente) que traen un software incorporado capaz de simular 8 qubits. Dado que no requieren de

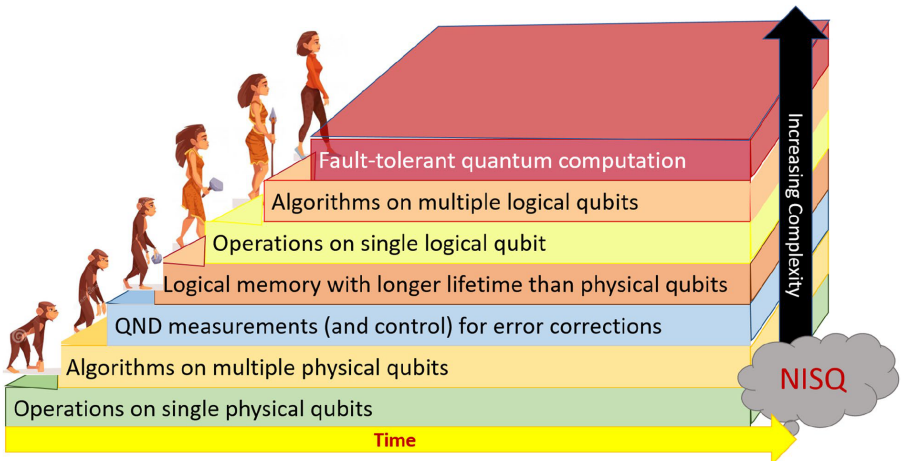


Figura 68: Evolución de los sistemas de computación cuántica [263].

complicada infraestructura adicional y por su peso (entre 14 y 40 kg), son portátiles y su uso, en la actualidad, se restringe a experimentos limitados y al ámbito educativo.

Si bien no existe consenso en el sector sobre cómo evaluar o comparar soluciones hardware, sí hay un conjunto de requisitos, definidos en el año 2000 por DiVicenzo [131], que se consideran vigentes hoy día y esenciales para disponer de un hardware adecuado:

1. Disponer de un sistema físico escalable que contiene qubits bien definidos.
2. Capacidad de poder iniciar el sistema de forma determinista en un estado perfectamente definido.
3. Constar de un conjunto de puertas cuánticas, tales como puertas de un único qubit o puertas con dos qubits entrelazados.
4. El período de coherencia del qubit ha de ser mayor que el de operatividad de las puertas.
5. Capacidad de medir con precisión el estado del qubit.

La satisfacción gradual de estos aspectos permite marcar la evolución en el soporte físico y, por tanto, en la calidad de la computación hardware. Sin embargo, todavía no es factible satisfacerlos de forma escalable (aumentando el número de qubits) de forma que se mantengan ratios de error lo suficientemente reducidos como para poder implementar códigos de corrección de errores operativos.

En la Fig. 68 se muestra un esquema de evolución de las tecnologías cuánticas desde la más básica, en la que se pueden realizar operaciones en qubits de forma individual, a la más avanzada, donde se podría disponer de un sistema masivo de computación cuántica tolerante a errores. En el momento actual de la tecnología, tanto para la parte de implementación hardware como la de soporte software para mitigar los problemas de decoherencia y ruido, los estudios indican que nos encontramos entre la fase 3, medidas QND *Quantum Non-Demolition* para el control y corrección de errores, y la fase 4, creación de qubits lógicos a partir de qubits físicos.

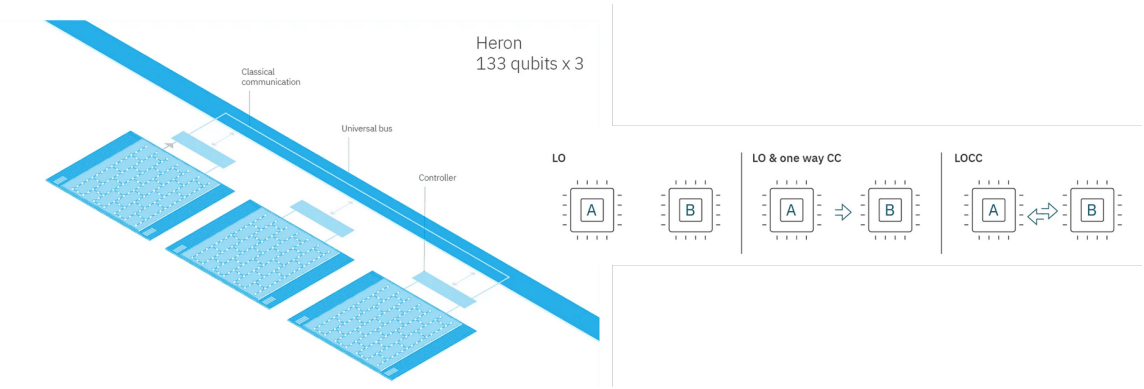


Figura 69: Escenarios de intercambio de información en técnicas de *Circuit knitting* [https://research.ibm.com].

Mientras no se dispone de soluciones hardware masivas y accesibles, surge con fuerza una línea de trabajo: tratar de resolver el problema de simular circuitos cuánticos cada vez mayores en computadoras cuánticas que no tienen esta infraestructura física. Para solventarlo se plantean técnicas denominadas de *circuit knitting*, en las que está trabajando activamente IBM (apartado 9.1) [361]. La filosofía subyacente es la de dividir los grandes circuitos cuánticos en subcircuitos que sí puedan ser ejecutados en el hardware disponible y entrelazar o tejer los resultados (usando postprocesado clásico) para conseguir el resultado que se habría obtenido de haber tenido la infraestructura adecuada. Esta estrategia llevada al ámbito hardware implica conectar procesadores más modestos usando conexiones clásicas y enlaces cuánticos y se espera que esta estrategia permita, en un futuro, ejecutar algoritmia en procesadores cuánticos paralelizados al uso clásico, permitiendo, así, incrementar el número de qubits disponibles. Por supuesto, esta solución presenta un inconveniente no desdeñable: el incremento de los costes de computación u *overhead*. En el apartado siguiente se desarrollan con más detalle las alternativas existentes o viables para la interconexión de los procesadores cuánticos.

Las soluciones que está tratando de llevar a cabo IBM implican la comunicación entre elementos de computación cuántica (en concreto están usando el procesador de 133 qubits *Heron*) usando elementos de comunicación clásica, tal y como se indica en la Fig. 69. En la misma figura (derecha) se esquematizan las tres opciones de comunicación: (i) sin comunicación ninguna, (ii) comunicación unidireccional y (iii) comunicación bidireccional. Los estudios llevados a cabo [361] permiten afirmar que la comunicación bidireccional reduce el *overhead* de $O(9^n)$ al $O(4^n)$, lo que permitiría en la práctica reducir el número de puertas CNOT (usadas para entrelazar los qubits).

Esto supone un ejemplo claro de las ventajas que se pueden obtener cuando se utilizan elementos de comunicación clásica entre dispositivos de computación cuántica.

Esta estrategia de *circuit knitting* encaja dentro de las soluciones para la planificación de recursos hardware. No existe mucha información disponible sobre cómo se está abordando este problema, que en la mayoría de los casos parece realizarse desde la perspectiva clásica, asumiendo las QPUs como aceleradores o módulos de computación similares (para la unidad que gestiona lo recursos) a otras como las GPUs o las DPUs. En este contexto surge una nueva iniciativa: crear un sistema operativo adecuado para computadores cuánticos. La única iniciativa destacable, producto de la financiación pública a una agrupación de empresas y centros tec-

nológicos británicos, es la que lidera Riverlane con su solución *Deltaflow.OS*, que está todavía en vías de desarrollo. El reto que se plantea con este sistema operativo es la gestión unificada de diferentes recursos cuánticos creados con tecnologías diferentes, asumiendo que no habrá convergencia en un futuro próximo.

En lo que respecta al software para programar, probar, simular y ejecutar algoritmia cuántica, la situación es semejante y es consecuencia de la diversidad de tecnologías para el soporte físico. Tal y como se ha visto en los apartados 9 y 12, lo habitual es que las mismas empresas que proporcionan las unidades de computación cuántica proporcionen también su correspondiente solución software adaptada. Esta falta de estandarización, de la que es consciente el sector, es un freno a la hora de desarrollar algoritmia transversal y disponer de una comunidad científica que pueda compartir de forma sencilla sus avances. Por ello, han surgido como líneas fuertes de trabajo dos grandes vías.

En primer lugar, disponer de representaciones intermedias que permitan independizar el software para programación cuántica y la tecnología hardware subyacente. En la actualidad, y tal y como se indicó en el apartado 12.2 hay dos grandes alternativas, cada una de ellas apoyada por un colectivo diferente de empresas y centros tecnológicos del sector: (i) OpenQASM: *Open Quantum Assembly Language* (apartado 12.2.1) y (ii) QIR: *Quantum Intermediate Representation* (apartado 12.2.2). El devenir de los próximos años nos permitirá saber si finalmente es posible disponer de esta capa intermedia e independizadora.

En segundo lugar, tratar de ofertar un lenguaje de muy alto nivel de abstracción y más próximo a los tradicionales lenguajes de programación clásica. Así se dispondría de una capa superior con la que científicos y programadores podrían diseñar su algoritmia sin tener que particularizarla o condicionarla a la infraestructura de ejecución. Es más, en un diseño en capas, este tipo de lenguajes podrían tener, a su vez, un compilador intermedio que permitiese obtener código en lenguajes de programación cuánticos más cercanos a la circuitería disponible. En esta línea destaca la iniciativa de Microsoft Azure (apartado 11.2) con su lenguaje *Q#*, que está integrado ya en los SDKs habituales de esta empresa.

En cualquier caso, la diversidad de lenguajes de programación cuántica no tiene que ser, en sí misma, un problema. De hecho, en el ámbito de la computación clásica existen multitud de lenguajes con diferentes niveles de abstracción y ofreciendo alternativas más adecuadas para un tipo de desarrollos o aplicaciones que otras. Quizá lo que se percibe en el contexto cuántico es que todavía no está clara esta diversidad en la orientación de los lenguajes existentes.

De forma transversal a estas líneas de trabajo se encuentran las investigaciones que tratan de (i) minimizar los errores físicos en los ordenadores cuánticos y (ii) mitigar y o corregir dichos errores con el objetivo de disponer de soluciones de computación cuántica estables y escalables. En el apartado 8 se describió brevemente la situación actual y los avances en ambas líneas. Estas técnicas de mitigación y/o corrección de errores proporcionan un conjunto de herramientas que permiten tratar de solventar los problemas causados por el ruido en la computación cuántica, pero todavía se está lejos de disponer soluciones que permitan construir un ordenador cuántico que se ocupe de corregir errores a gran escala, a lo largo de miles de qubits interconectados y varios millones de veces por segundo. La complejidad de aspectos técnicos y teóricos que abarca permiten considerar este reto (conseguir un ordenador cuántico tolerante a fallos) como el mayor en el ámbito de la computación cuántica.

Finalmente, y en cualquier caso, la competición entre computación cuántica y clásica es latente y no toda la comunidad científica está de acuerdo en considerar la supremacía de la primera. Recientemente (junio de 2023) se publicaba un estudio en el que personal investigador de

IBM había conseguido, con un procesador cuántico de 127 qubits y aplicando medidas adicionales para reducir el impacto del ruido inherente, resultados de computación que no podrían ser realizados en computadores clásicos [245]. Unas semanas después, y en respuesta, se publicaban sendos trabajos del Flatiron Institute Center [442] y de Caltech [35] en los que se evidenciaba que sí era posible obtener resultados comparables con computación clásica, pero con una algoritmia optimizada en memoria y tiempo. En cualquier caso, esta pugna incentiva la mejor de los mecanismos que puedan mitigar el ruido al que se ven sometidos los computadores cuánticos, que es en sí mismo un avance tecnológico considerable.

13.2. Interconexión de QPUs distribuidas y QPUs multi-núcleo

En el presente estadio de desarrollo NISQ, la computación cuántica a gran escala solo es posible si se unen las capacidades síncronas de varias QPU con algunos cientos de qubits robustos cada una, ya sea QPUs que están físicamente próximas (porque son parte de un mismo computador cuántico modular, como los que anticipan IBM y otros fabricantes [169]; o porque, siendo de computadores distintos, estos están instalados en proximidad, por ejemplo en un centro de datos, una planta o un campus), ya sean QPUs distribuidas que se comunican por medio de una Internet cuántica. Las QPUs monolíticas con un número elevado de qubits, capaces de resolver problemas de escala realista, están aún lejos de existir, e imponen además complicaciones técnicas severas debidas al efecto de las perturbaciones de estados y las dificultades de los sistemas necesarios para controlar los qubits. Por otro lado, la interconexión hardware entre una QPU masiva en qubits y el sistema de procesamiento clásico que la alberga (cuyos tamaños son muy dispares y operan a temperaturas muy diferentes) se convierte pronto en un cuello de botella de todo el sistema [307]. Con la tecnología actual, la lectura de qubits de una QPU desde un procesador externo requiere de unas 10 operaciones que ocupan alrededor de 1 Mb/s de ancho de banda, así que la gestión de QPUs con miles o decenas de miles de qubits llevaría a tasas de Gb/s o Tb/s y forzaría un consumo de energía ultra-bajo, de solo algunos fJ/bit.

Por consiguiente, la alternativa es la de una arquitectura de computación cuántica modular compuesta por cierto número de unidades QPU de tamaño moderado, interconectadas mediante un sistema de comunicaciones dual clásico y cuántico para el intercambio de bits y qubits [228, 150]. En el análisis de un posible sistema denso de interconexión de QPUs, tanto en una arquitectura multi-núcleo como en una interconexión de QPUs embebidas en ordenadores diferentes, hemos de tener en cuenta una serie de aspectos de arquitectura, limitaciones físicas e hipótesis de funcionamiento:

1. Latencia. La separación física entre cualesquiera dos QPUs en un sistema denso puede estar en el rango de $0{,}01$ a 100 m (si incluimos como posibilidades tanto un multi-núcleo como un conjunto de servidores independientes de computación cuántica). En consecuencia, el tiempo de señalización entre ellas tanto por un canal clásico como por uno fotónico será del orden de los ns a los μs. En ese rango de distancias es razonable suponer que la atenuación es tan pequeña que las pérdidas de fotones serán despreciables, si es que la orquestación y transferencia de los qubits se hace con fotones.

2. Determinismo.El tiempo de comunicación o sincronismo o entrelazamiento entre las QPUs debe ser determinista. El modelo funcional debería asemejarse al de una arquitectura NUMA (*Non-uniform Memory Access*) convencional, en la que el acceso a los qubits comunes se obtenga tras un tiempo que puede ser diferente según la ubicación de las QPUs, pero

que es determinista. Esta asunción descarta los repetidores 1G y, parcialmente, los 2G como elementos de interconexión cuántica, puesto que estos están basados en mecanismos probabilistas para compensar los errores operativos.

3. Fiabilidad. Las QPUs dispondrán de puertas cuánticas de alta fiabilidad para las operaciones de medida y generación de entrelazamiento. Esto implica que no serán necesarios métodos sofisticados de corrección de errores en ellas, e incluso que podría prescindirse de ellos.

En cuanto al medio físico de comunicación entre las QPUs sobre el que han de llevarse a cabo las transferencias de qubis de estado, se investigan en la actualidad distintas tecnologías:

- Lanzaderas de iones [237]. Es una tecnología específica de las plataformas hardware construidas con trampas de iones. Usa campos electromagnéticos para transportar físicamente iones a través de un espacio en el que deliberadamente se han dejado qubits vacantes, para así aproximarlos y habilitar su interacción. Requiere una interacción física fuerte entre las QPUs y no parece demasiado escalable.
- Teleportación. El uso de teleportación para comunicación inter-QPUs es perfectamente natural, pero depende significativamente de la generación eficiente de entrelazamiento y de su pureza, y se encuentra todavía en sus primeras etapas de desarrollo [294, 384].
- Interconexión chip-con-chip Consiste en el acoplamiento entre qubits por vía de algún medio físico, como un cable coaxial [272], una línea de transmisión superconductora [119] o resonadores con acoplamiento capacitivo [179].
- Redes fotónicas. Transmisión de fotones sobre guías ópticas o fibras ópticas, tal como se ha descrito en otros apartados de este informe (por ejemplo, en 2.6).

La interconexión con sistemas fotónicos también resulta especialmente interesante en el caso de la comunicación vertical con el host clásico que contiene las QPUs, dado el elevado ancho de banda que precisa, ancho de banda en el que fibras ópticas y guiaondas ópticas son abundantes. En cambio, cualquiera de las tecnologías alternativas (salvo la teleportación quizá) está sujeta a restricciones en la tasa de intercambio de los qubits. La ventaja crucial de la tecnología fotónica reside, entonces, en que la capacidad del canal cuántico de interconexión es siempre suficiente, y la tasa de transferencia quedaría limitada únicamente por la tasa de generación e intercambio del entrelazamiento.

13.2.1. Interconexión directa

La primera de las posibilidades de interconexión entre QPUs es la conexión directa dos a dos, como esquematiza la Figura 70. El sistema estaría compuesto por enlaces cuánticos directos entre las QPU vecinas, punto a punto, más un sistema de interconexión clásico con bits entre todas ellas, que se puede implementar con un bus digital convencional o con un elemento de interconexión como un hub/switch digital si se desea reducir el cableado. La ventaja de una arquitectura en bus para las comunicaciones clásicas es el elevado ancho de banda que proporciona.

Los canales cuánticos directos entre las QPU se pueden construir combinando el entrelazamiento memoria-memoria que se describió en el apartado 4.5.2 con una fibra óptica o una

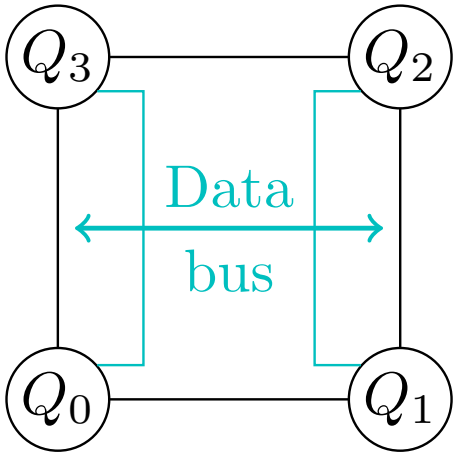


Figura 70: Esquemas de interconexión de QPUs: interconexión óptica directa más bus clásico de control.

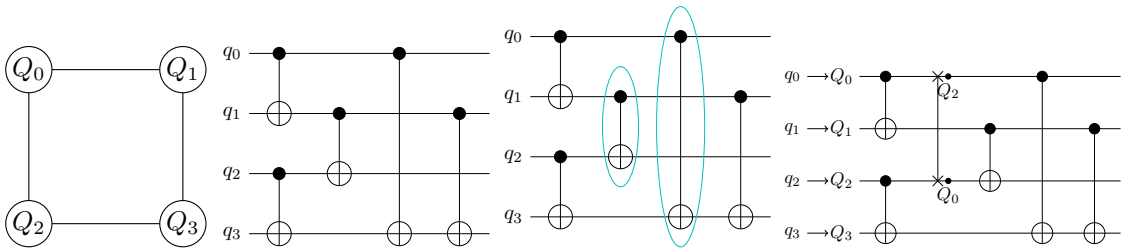


Figura 71: Conversión de un circuito cuántico para ejecución en varias QPU. Los qubits físicos q_0, q_1, q_2, q_3 son convertidos en qubits virtuales Q_0, Q_1, Q_2, Q_3 y se introducen dos puertas de intercambio para ajustar el circuito a la topología física del panel de la izquierda: las QPU Q_1-Q_2 y Q_0-Q_3 no tienen conexión directa.

guía-onda adecuada. Las guía-ondas solo precisan de un acoplamiento adecuado con los dispositivos de memoria, en tanto que las fibras ópticas tendrían que hacer uso de algún sistema de conversión de frecuencia óptica para adaptarla salida de las fuentes a las longitudes de onda comerciales en banda C (1530 nm - 1565 nm) (ver Tabla 8). La generación de los qubits entrelazados es posible llevarla a cabo en este escenario con pozos cuánticos (ver de nuevo el apartado 4.4.1), tanto si son pares de Bell como estados grafo más complejos, que como se vio admiten acoplamiento con los conversores de frecuencia.

13.2.2. Interconexión directa, QBUS

El principal inconveniente de la solución anterior es el hecho de que la topología de interconexión entre las QPU es fija y dedicada, no es posible cambiarla sin modificar la estructura física del sistema y, para poder explotar eficazmente todas sus posibilidades, tiene que ser conocida por los compiladores y los generadores de representación intermedia. Por ejemplo, puesto que

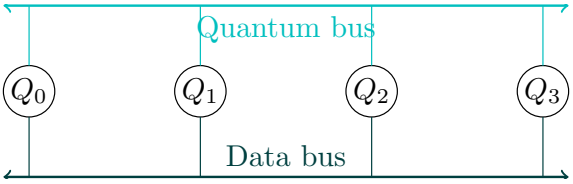


Figura 72: Esquemas de interconexión de QPUs: interconexión directa con bus cuántico y bus clásico.

no es posible ejecutar una puerta lógica de dos qubits a menos que esos qubits sean físicamente contiguos, será necesario en ocasiones transformar la estructura de un determinado circuito cuántico en función de la topología de conexión subyacente de las QPU (la Figura 71 muestra un ejemplo sencillo de esta idea).

La segunda opción de interconexión de QPUs consiste en extender la idea de un bus digital clásico al caso cuántico: un bus cuántico o QBUS conecta todos los dispositivos próximos. Funcionalmente, el QBUS permite la transmisión de fotones en ambas direcciones, de tal manera que pueda ser leído y capturado por cualquiera de las demás QPU. La configuración se muestra en la Figura 72. Tecnológicamente, esta idea de un bus cuántico se ha descrito e implementado recientemente en un trabajo [235] que dibuja una arquitectura novedosa capaz de lograr la emisión direccional de fotones en uno u otro sentido del QBUS mediante la generación de pares de qubits y el uso del fenómeno de interferencia cuántica, junto con una guiaonda común a todas las QPU[16]. Esta tecnología vuelve a basarse de forma crucial en componentes ópticos y fotónicos, que representan hoy día la vía más prometedora para casi cualquier forma de interconexión física de los procesadores cuánticos.

13.2.3. Interconexión directa con repetidores ópticos

La solución de interconexión con un bus cuántico es conceptualmente simple pero plantea algunas dificultades, en concreto, necesita de un elemento de control para arbitrar el uso del bus común y gestionar las operaciones de transferencia de los qubits y la generación de entrelazamiento. Este dispositivo de arbitrio del acceso al QBUS tendría que ir embebido en la propia QPU o diseñarse ad hoc, tal como hoy sucede con los controladores de acceso a buses digitales en los ordenadores convencionales. Estos elementos de control son, esencialmente, dispositivos que serializan el acceso al recurso compartido (el QBUS) por un tiempo limitado. No está todavía claro, sin embargo, cuáles habrían de ser las condiciones de diseño y funcionamiento en el caso de un QBUS genérico compartido por un número variable de QPUs, ni tampoco las dependencias entre las operaciones sobre el QBUS y el bus de datos clásico. Una ventaja potencial de la solución con un QBUS sería claramente que la combinación QBUS más bus clásico puede utilizarse conjuntamente como un canal clásico asistido por entrelazamiento (ver el desarrollo en el apartado 2.5). Un inconveniente, por contra, es que la contienda por el bus comporta que el tiempo de acceso no sea determinista.

La lógica de control para la interconexión de las QPUs puede centralizarse en el propio ele-

[16] En palabras de los propios autores: Ït can be used as a fully programmable quantum node that can emit/absorb/pass/store quantum information on a quantum network and as an interface for a bus connecting multiple quantum computer chips".

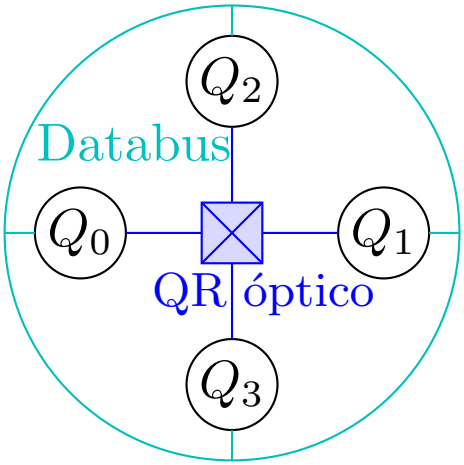


Figura 73: Esquemas de interconexión de QPUs: interconexión directa con un repetidor óptico.

mento de interconexión, formando una arquitectura compuesta por un repetidor central al que se conectan todas las QPU en una topología en estrella (Figura 73). Por las ventajas que se presentaron en los apartados 4.4, 4.4.1 y 4.4.2, la tecnología de repetidores enteramente ópticos parece la más conveniente para una arquitectura de este tipo, por varias razones. Primera, un repetidor totalmente óptico puede manipular estados grafos complejos, en principio; si esos estados se han creado con qubits físicos redundantes, entonces las medidas locales que hiciesen las QPUs son quasi-deterministas. Segunda, salvo por la complejidad de generación de estados grafo o estados clúster muy grandes, el repetidor óptico permite la creación de estados entrelazados entre cualquier subconjunto de las QPUs conectadas, sin más limitación que el propio diseño del estado grafo y del código QEC en que se sustente. Y tercera, como ya vimos, los repetidores ópticos hacen uso de un número de recursos bastante moderado (básicamente, la dimensión del estado grafo) en comparación con los qubits materiales de memoria que requiere un repetidor cuántico más convencional de las generaciones precedentes.

13.2.4. Interconexión indirecta con repetidores/switches

Si bien una arquitectura con repetidor/conmutador completamente óptico es la más flexible y de mayor capacidad, en el sentido de poder satisfacer una región de demandas de conexión más amplia y de mayor tasa que con las otras soluciones, la tecnología de los repetidores ópticos no está aún lo bastante desarrollada como para poder implementar un dispositivo general con estas características capaz de dar servicio a un número razonable de QPUs. En tal caso, la última de las soluciones de arquitectura que examinaremos es similar, pero reemplazando el repetidor óptico por un repetidor 2G/3G como los discutidos en el apartado 4.3. Estos repetidores están basados en memoria y, al menos en el caso de la tecnología 3G, operan de forma determinista por cuanto concierne a la corrección de errores operativos, aunque como vimos necesitan, en general, de un número de registros de memoria bastante elevados. Por ello, cabe observar que su principal limitación técnica a corto plazo radica en el desarrollo de memoria cuánticas eficaces, estables en tiempo de coherencia y en fiabilidad, y baratas.

El repetidor central estaría equipado con un multiplexor/demultiplexor de E/S para estable-

cer estados entrelazados entre cualquier par de QPUs conectadas a él, según demanda, siendo la diferencia fundamental respecto de la solución basada en repetidores ópticos que aquí el multiplexor conecta únicamente dos de las QPU. De esta manera, el repetidor opera como un switch cuántico elemental entre sus clientes. Ahora bien, la lógica de conmutación habría de implementarse con un dispositivo de control integrado en el repetidor, que tendría que ejecutar en tiempo real un planificador de los recursos para activar y desactivar las conexiones lógicas entre las entradas y las salidas. Y aunque la operación conceptual del planificador no es en sí muy diferente a la de un conmutador convencional, un aspecto importante en el caso de la conmutación cuántica (y por tanto un inconveniente potencial) es que el planificador tiene como restricción operar dentro del los tiempos de coherencia de las memorias y de los estados entrelazados.

13.3. Interfaz HPC-QPUs

La aplicación de la computación cuántica a problemas realistas de la ciencia y la industria, como la resolución de sistemas lineales, la fijación de condiciones iniciales para sistemas de ecuaciones diferenciales, los métodos de *machine learning* y muchos otros tiene como condición previa que los datos clásicos se pueden convertir fácil y eficientemente en un estado cuántico que sirva como entrada a las QPU. Desafortunadamente, esta tarea de representar un conjunto de datos en forma de un conjunto de qubits es, en general, muy poco eficiente y requiere un número exponencial de operaciones unitarias y puertas para la preparación de la entrada que consume el algoritmo cuántico en cuestión.

Hay básicamente dos maneras de codificar datos clásicos digitales en estados cuánticos. En la primera, cada bit se traduce en un elemento de la base computacional $0 \mapsto |0\rangle$ y $1 \mapsto |1\rangle$. El método es elemental, pero requiere tantos qubits como bits clásicos se usen para la información clásica, lo que es claramente poco eficiente en términos de representación de los estados (o de compresión de la información). En el segundo método, una función de densidad arbitraria f se discretiza primero en un cierto número de niveles que luego se codifican en un estado cuántico. Con el algoritmo de Grover-Rudolph, la codificación toma la forma[17]

$$|\Psi(f)\rangle_n = \sum_{i=0}^{2^n-1} \sqrt{f_i}|i\rangle$$

sobre n qubits. El algoritmo es constructivo, y da una secuencia específica de rotaciones que, aplicadas sobre el n qubit $|0\rangle^{\otimes n}$ produce el estado deseado. Los coeficientes f_i tienen obviamente la interpretación de probabilidades correspondientes a la función f. Sin embargo, este protocolo de preparación clásico-cuántica necesita un número exponencial de puertas CNOT, exactamente $2^{n+2} - 4n - 4$, y cada una de las rotaciones precisa a su vez 2^{k-1} puertas CNOT y 2^{k-1} puertas de un qubit. Así pues, aunque es un método muy general, es claro que el coste de aplicarlo a un problema de escala realista es prohibitivo e impide de facto la computación cuántica. Hay no obstante algunas mejoras posibles sobre este orden de complejidad. En [309] se presenta un método que codifica la función de densidad f discretizándola en amplitud y llevando esos valores de amplitud a la amplitud de los estados de los qubits, con una representación

[17] En esta ecuación $|i\rangle$ debe entenderse no como uno de los vectores de la base computacional sino como el qubit $|i_1 i_2 \dots i_n\rangle$, donde $i_1 i_2 \dots i_n$ es la representación binaria del entero i.

normalizada de la forma

$$|f\rangle_n = \sum_{i=0}^{2^n-1} f(j/(2^n-1))|j\rangle.$$

Esta representación discreta se puede después convertir a un estado cuántico $|\Psi(f)\rangle_n$ de n qubits para el que solo son necesarias $2^{k_0(\varepsilon)}-1$ puertas de dos qubits, donde ε es la fidelidad entre los estados $|f\rangle_n$ y $|\Psi(f)\rangle_n$ y $k_0(\varepsilon)$ es una cantidad menor que 2 que, asintóticamente, no depende de n, el tamaño de la entrada. Aunque la complejidad sigue siendo exponencial, de la expresión explícita del exponente $k_0(\varepsilon)$

$$k_0(\varepsilon) = \text{máx}\left\{\left\lceil -\frac{1}{2}\log_2\left(4^{-n} - \frac{96}{\eta^2}\log(1-\varepsilon)\right)\right\rceil, 2\right\},$$

donde η es un parámetro relacionado con la curvatura de f, se sigue que para valores de fidelidad relativamente grandes se tiene $k_0(\varepsilon) \ll 2$, lo que representa una ventaja muy significativa sobre el método anterior. A pesar de este resultado positivo, que puede hacer práctica la computación cuántica en QPUs de unas pocas decenas o cientos de qubits, son necesarias más reducciones de esta complejidad si se aspira a tener un sistema de computación cuántico eficiente para datos masivos. Están por explorar en la literatura otras alternativas de compresión clásico-cuántica eficientes que pueden funcionar igual de bien que en el procesado digital clásico, por ejemplo, el muestreo compresivo o las representaciones de datos *sparse*. Este campo del preprocesado clásico para la preparación de qubits de entrada a una QPU ha recibido no demasiada atención hasta la fecha, pese a su importancia, y es un área técnica con potencial, en nuestra opinión.

Referencias

[1] M. H. Abobeih et al. "One-second coherence for a single electron spin coupled to a multi-qubit nuclear-spin environment". En: *Nature Communications* 9.1 (jun. de 2018). doi: 10.1038/s41467-018-04916-z.

[2] M. H. Abobeih et al. "Fault-tolerant operation of a logical qubit in a diamond quantum processor". En: *Nature* 606.7916 (mayo de 2022), págs. 884-889. doi: 10.1038/s41586-022-04819-6.

[3] Dorit Aharonov y Michael Ben-Or. "Fault-tolerant quantum computation with constant error". En: *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*. 1997, págs. 176-188.

[4] Igor Aharonovich, Dirk Englund y Milos Toth. "Solid-state single-photon emitters". En: *Nature Photonics* 10.10 (sep. de 2016), págs. 631-641. doi: 10.1038/nphoton.2016.186.

[5] Victor V. Albert et al. "Performance and structure of single-mode bosonic codes". En: *Physical Review A* 97.3 (mar. de 2018), pág. 032346. doi: 10.1103/physreva.97.032346.

[6] Thomas Alexander et al. "Qiskit pulse: programming quantum computers through the cloud with pulses". En: *Quantum Science and Technology* 5.4 (2020), pág. 044006.

[7] *Amazon Braket launches Lucy, a new quantum processor from Oxford Quantum Circuits and expands to the Europe (London) Region10.1023/A:1026009100467*. 2022. url: https://aws.amazon.com/es/blogs/quantum-computing/amazon-braket-launch-oqc-oxford-quantum-circuits-expands-to-the-europe-region/.

[8] Grigori G. Amosov. "Strong superadditivity conjecture holds for the quantum depolarizing channel in any dimension". En: *Physical Review A* 75.6 (jun. de 2007), pág. 060304. doi: 10.1103/physreva.75.060304.

[9] M. Arcari et al. "Near-Unity Coupling Efficiency of a Quantum Emitter to a Photonic Crystal Waveguide". En: *Physical Review Letters* 113.9 (ago. de 2014), pág. 093603. doi: 10.1103/physrevlett.113.093603.

[10] Juan M Arrazola et al. "Quantum circuits with many photons on a programmable nanophotonic chip". En: *Nature* 591.7848 (2021), págs. 54-60.

[11] Frank Arute et al. "Quantum supremacy using a programmable superconducting processor". En: *Nature* 574.7779 (2019), págs. 505-510.

[12] Warit Asavanant et al. "Generation of time-domain-multiplexed two-dimensional cluster state". En: *Science* 366.6463 (oct. de 2019), págs. 373-376. doi: 10.1126/science.aay2645.

[13] Mete Atatüre et al. "Material platforms for spin-based photonic quantum technologies". En: *Nature Reviews Materials* 3.5 (abr. de 2018), págs. 38-51. doi: 10.1038/s41578-018-0008-9.

[14] Serkan Ates et al. "Two-Photon Interference Using Background-Free Quantum Frequency Conversion of Single Photons Emitted by an InAs Quantum Dot". En: *Physical Review Letters* 109.14 (oct. de 2012), pág. 147405. doi: 10.1103/physrevlett.109.147405.

[15] David Awschalom. "From Long-distance Entanglement to Building a Nationwide Quantum Internet: Report of the DOE Quantum Internet Blueprint Workshop". En: (feb. de 2020). doi: 10.2172/1638794. url: https://www.osti.gov/biblio/1638794.

[16] David D. Awschalom et al. "A Roadmap for Quantum Interconnects". En: (jul. de 2022). doi: 10.2172/1900586. url: https://www.osti.gov/biblio/1900586.

[17] Koji Azuma y Go Kato. "Optimal entanglement manipulation via coherent-state transmission". En: *Physical Review A* 85.6 (jun. de 2012), pág. 060303. doi: 10.1103/physreva.85.060303.

[18] Koji Azuma, Kiyoshi Tamaki y Hoi-Kwong Lo. "All-photonic quantum repeaters". En: *Nature Communications* 6.1 (abr. de 2015). doi: 10.1038/ncomms7787.

[19] Koji Azuma et al. "Optimal entanglement generation for efficient hybrid quantum repeaters". En: *Physical Review A* 80.6 (dic. de 2009), pág. 060303. doi: 10.1103/physreva.80.060303.

[20] Koji Azuma et al. "Quantum repeaters and computation by a single module: Remote nondestructive parity measurement". En: *Physical Review A* 85.6 (jun. de 2012), pág. 062309. doi: 10.1103/physreva.85.062309.

[21] Koji Azuma et al. "Tools for quantum network design". En: *AVS Quantum Science* 3.1 (feb. de 2021). doi: 10.1116/5.0024062.

[22] Koji Azuma et al. "Quantum repeaters: From quantum networks to the quantum internet". En: (dic. de 2022). doi: 10.48550/ARXIV.2212.10820. arXiv: 2212.10820 [quant-ph].

[23] Ryan Babbush et al. "Focus beyond quadratic speedups for error-corrected quantum advantage". En: *PRX Quantum* 2.1 (2021), pág. 010103.

[24] Dave Bacon. "Operator quantum error-correcting subsystems for self-correcting quantum memories". En: *Physical Review A* 73.1 (ene. de 2006), pág. 012340. doi: 10.1103/physreva.73.012340.

[25] Rajni Bala, Sooryansh Asthana y V. Ravishankar. "Combating errors in quantum communication: an integrated approach". En: *Scientific Reports* 13.1 (feb. de 2023). doi: 10.1038/s41598-023-30178-x. url: https://doi.org/10.1038%2Fs41598-023-30178-x.

[26] Gopalakrishnan Balasubramanian et al. "Ultralong spin coherence time in isotopically engineered diamond". En: *Nature Materials* 8.5 (abr. de 2009), págs. 383-387. doi: 10.1038/nmat2420.

[27] Charles H Baldwin et al. "Re-examining the quantum volume test: Ideal distributions, compiler optimizations, confidence intervals, and scalable resource estimations". En: *Quantum* 6 (2022), pág. 707.

[28] N. Bar-Gill et al. "Solid-state electronic spin coherence time approaching one second". En: *Nature Communications* 4.1 (abr. de 2013). doi: 10.1038/ncomms2771.

[29] Howard Barnum, M. A. Nielsen y Benjamin Schumacher. "Information transmission through a noisy quantum channel". En: *Physical Review A* 57.6 (jun. de 1998), págs. 4153-4175. doi: 10.1103/physreva.57.4153.

[30] S. D. Barrett et al. "Symmetry analyzer for nondestructive Bell-state detection using weak nonlinearities". En: *Physical Review A* 71.6 (jun. de 2005), pág. 060302. doi: 10.1103/physreva.71.060302.

[31] Sean D. Barrett y Pieter Kok. "Efficient high-fidelity quantum computation using matter qubits and linear optics". En: *Physical Review A* 71.6 (jun. de 2005), pág. 060310. doi: 10.1103/physreva.71.060310.

[32] H G Barros et al. "Deterministic single-photon source from a single ion". En: *New Journal of Physics* 11.10 (oct. de 2009), pág. 103004. doi: 10.1088/1367-2630/11/10/103004.

[33] Francesco Battistel et al. "Real-Time Decoding for Fault-Tolerant Quantum Computing: Progress, Challenges and Outlook". En: *arXiv preprint arXiv:2303.00054* (2023).

[34] Daniel Beaulieu y Anh Pham. "Evaluating performance of hybrid quantum optimization algorithms for MAXCUT Clustering using IBM runtime environment". En: *arXiv preprint arXiv:2112.03199* (2021).

[35] Tomislav Begušić y Garnet Kin Chan. "Fast classical simulation of evidence for the utility of quantum computing before fault tolerance". En: *arXiv preprint arXiv:2306.16372* (2023).

[36] B. A. Bell et al. "Experimental demonstration of a graph state quantum error-correction code". En: *Nature Communications* 5.1 (abr. de 2014). doi: 10.1038/ncomms4658.

[37] J. S. Bell. "On the Einstein Podolsky Rosen paradox". En: *Physics Physique Fizika10.1103/PhysRevA.69.062311* 1.3 (nov. de 1964), págs. 195-200. doi: 10.1103/physicsphysiquefizika.1.195.

[38] Naphan Benchasattabuse, Michal Hajdušek y Rodney Van Meter. "Architecture and protocols for all-photonic quantum repeaters". En: (jun. de 2023). doi: 10.48550/ARXIV.2306.03748. arXiv: 2306.03748 [quant-ph].

[39] Marcello Benedetti et al. "A generative modeling approach for benchmarking and training shallow quantum circuits". En: *npj Quantum Information* 5.1 (2019), pág. 45.

[40] C.H. Bennett et al. "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem". En: *IEEE Transactions on Information Theory* 48.10 (oct. de 2002), págs. 2637-2655. doi: 10.1109/tit.2002.802612.

[41] Charles H. Bennett, David P. DiVincenzo y John A. Smolin. "Capacities of Quantum Erasure Channels". En: *Physical Review Letters* 78.16 (abr. de 1997), págs. 3217-3220. doi: 10.1103/physrevlett.78.3217.

[42] Charles H. Bennett y Stephen J. Wiesner. "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states". En: *Physical Review Letters* 69.20 (nov. de 1992), págs. 2881-2884. doi: 10.1103/physrevlett.69.2881.

[43] Charles H. Bennett et al. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels". En: *Physical Review Letters* 70.13 (mar. de 1993), págs. 1895-1899. doi: 10.1103/physrevlett.70.1895.

[44] Charles H. Bennett et al. "Concentrating partial entanglement by local operations". En: *Physical Review A* 53.4 (abr. de 1996), págs. 2046-2052. doi: 10.1103/physreva.53.2046.

[45] Charles H. Bennett et al. "Mixed-state entanglement and quantum error correction". En: *Physical Review A* 54.5 (nov. de 1996), págs. 3824-3851. doi: 10.1103/physreva.54.3824.

[46] Charles H. Bennett et al. "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels". En: *Physical Review Letters* 76.5 (ene. de 1996), págs. 722-725. doi: 10.1103/physrevlett.76.722.

[47] Ville Bergholm et al. "Pennylane: Automatic differentiation of hybrid quantum-classical computations". En: *arXiv preprint arXiv:1811.04968* (2018).

[48] H. Bernien et al. "Heralded entanglement between solid-state qubits separated by three metres". En: *Nature* 497.7447 (abr. de 2013), págs. 86-90. doi: 10.1038/nature12016.

[49] Mario Berta. *Single-shot Quantum State Merging*. 2009. doi: 10.48550/ARXIV.0912.4495.

[50] M. K. Bhaskar et al. "Experimental demonstration of memory-enhanced quantum communication". En: *Nature* 580.7801 (mar. de 2020), págs. 60-64. doi: 10.1038/s41586-020-2103-5.

[51] B. B. Blinov et al. "Observation of entanglement between a single trapped atom and a single photon". En: *Nature* 428.6979 (mar. de 2004), págs. 153-157. doi: 10.1038/nature02377.

[52] F Bloch. "Simple interpretation of the Josephson effect". En: *Physical Review Letters* 21.17 (1968), pág. 1241.

[53] M Bonarota, J-L Le Gouët y T Chanelière. "Highly multimode storage in a crystal". En: *New Journal of Physics* 13.1 (ene. de 2011), pág. 013013. doi: 10.1088/1367-2630/13/1/013013.

[54] D. Boneh y V. Shoup. *A Graduate Course in Applied Cryptography*. Online. 2023. url: https://toc.cryptobook.us.

[55] Kelly Boothby et al. "Next-generation topology of d-wave quantum processors". En: *arXiv preprint arXiv:2003.00133* (2020).

[56] William A Borders et al. "Integer factorization using stochastic magnetic tunnel junctions". En: *Nature* 573.7774 (2019), págs. 390-393.

[57] J. Borregaard et al. "Scalable photonic network architecture based on motional averaging in room temperature gas". En: *Nature Communications* 7.1 (abr. de 2016). doi: 10.1038/ncomms11356.

[58] Johannes Borregaard et al. "One-Way Quantum Repeater Based on Near-Deterministic Photon-Emitter Interfaces". En: *Physical Review X* 10.2 (jun. de 2020), pág. 021071. doi: 10.1103/physrevx.10.021071.

[59] Alexandre Bourassa et al. "Entanglement and control of single nuclear spins in isotopically engineered silicon carbide". En: *Nature Materials* 19.12 (sep. de 2020), págs. 1319-1325. doi: 10.1038/s41563-020-00802-6.

[60] Dik Bouwmeester et al. "Observation of Three-Photon Greenberger-Horne-Zeilinger Entanglement". En: *Physical Review Letters* 82.7 (feb. de 1999), págs. 1345-1349. doi: 10.1103/physrevlett.82.1345.

[61] C. E. Bradley et al. "A Ten-Qubit Solid-State Spin Register with Quantum Memory up to One Minute". En: *Physical Review X* 9.3 (sep. de 2019), pág. 031045. doi: 10.1103/physrevx.9.031045.

[62] Gilles Brassard. "Quantum Communications Complexity". En: *Foundations of Physics* 33.11 (2003), págs. 1593-1616. doi: 10.1023/a:1026009100467.

[63] Sylvia Bratzik, Hermann Kampermann y Dagmar Bruß. "Secret key rates for an encoded quantum repeater". En: *Physical Review A* 89.3 (mar. de 2014), pág. 032335. doi: 10.1103/physreva.89.032335.

[64] Samuel L. Braunstein y H. J. Kimble. "Teleportation of Continuous Quantum Variables". En: *Physical Review Letters* 80.4 (ene. de 1998), págs. 869-872. doi: 10.1103/physrevlett.80.869.

[65] H.-J. Briegel et al. "Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication". En: *Physical Review Letters* 81.26 (dic. de 1998), págs. 5932-5935. doi: 10.1103/physrevlett.81.5932.

[66] Hans J. Briegel y Robert Raussendorf. "Persistent Entanglement in Arrays of Interacting Particles". En: *Physical Review Letters* 86.5 (ene. de 2001), págs. 910-913. doi: 10.1103/physrevlett.86.910.

[67] Keith A Britt y Travis S Humble. "High-performance computing with quantum processing units". En: *ACM Journal on Emerging Technologies in Computing Systems (JETC)* 13.3 (2017), págs. 1-13.

[68] Keith A Britt, Fahd A Mohiyaddin y Travis S Humble. "Quantum accelerators for high-performance computing systems". En: *2017 IEEE International Conference on Rebooting Computing (ICRC)*. IEEE. 2017, págs. 1-7.

[69] Anne Broadbent, Joseph Fitzsimons y Elham Kashefi. "Universal Blind Quantum Computation". En: *2009 50th Annual IEEE Symposium on Foundations of Computer Science*. IEEE, oct. de 2009. doi: 10.1109/focs.2009.36.

[70] Anne Broadbent y Christian Schaffner. "Quantum cryptography beyond quantum key distribution". En: *Designs, Codes and Cryptography* 78.1 (dic. de 2015), págs. 351-382. doi: 10.1007/s10623-015-0157-4.

[71] Daniel E. Browne y Terry Rudolph. "Resource-Efficient Linear Optical Quantum Computation". En: *Physical Review Letters* 95.1 (jun. de 2005), pág. 010501. doi: 10.1103/physrevlett.95.010501.

[72] Luís Bugalho et al. "Distributing Multipartite Entanglement over Noisy Quantum Networks". En: *Quantum 7, 920 (2023)* 7 (26 de mar. de 2021), pág. 920. doi: 10.22331/q-2023-02-09-920. arXiv: 2103.14759 [quant-ph].

[73] Donovan Buterakos, Edwin Barnes y Sophia E. Economou. "Deterministic Generation of All-Photonic Quantum Repeaters from Solid-State Emitters". En: *Physical Review X* 7.4 (oct. de 2017), pág. 041023. doi: 10.1103/physrevx.7.041023.

[74] C. Cabrillo et al. "Creation of entangled states of distant atoms by interference". En: *Physical Review A* 59.2 (feb. de 1999), págs. 1025-1033. doi: 10.1103/physreva.59.1025.

[75] Angela Sara Cacciapuoti et al. "When Entanglement Meets Classical Communications: Quantum Teleportation for the Quantum Internet". En: *IEEE Transactions on Communications* 68.6 (jun. de 2020), págs. 3808-3833. doi: 10.1109/tcomm.2020.2978071.

[76] Angela Sara Cacciapuoti et al. "Entanglement Distribution in the Quantum Internet: Knowing when to Stop!" En: (jul. de 2023). doi: 10.48550/ARXIV.2307.05123. arXiv: 2307.05123 [quant-ph].

[77] Zhenyu Cai et al. "Quantum error mitigation". En: *arXiv preprint arXiv:2210.00921* (2022).

[78] A. R. Calderbank y Peter W. Shor. "Good quantum error-correcting codes exist". En: *Physical Review A* 54.2 (ago. de 1996), págs. 1098-1105. doi: 10.1103/physreva.54.1098.

[79] Marcello Caleffi, Kyrylo Simonov y Angela Sara Cacciapuoti. "Beyond Shannon Limits: Quantum Communications Through Quantum Paths". En: *IEEE Journal on Selected Areas in Communications* 41.8 (ago. de 2023), págs. 2707-2724. doi: 10.1109/jsac.2023.3288263.

[80] Marcello Caleffi et al. "Distributed Quantum Computing: a Survey". En: (dic. de 2022). doi: 10.48550/ARXIV.2212.10609. arXiv: 2212.10609 [quant-ph].

[81] J. Calsamiglia y N. Lütkenhaus. "Maximum efficiency of a linear-optical Bell-state analyzer". En: *Applied Physics B* 72.1 (ene. de 2001), págs. 67-71. doi: 10.1007/s003400000484.

[82] F Caruso, V Giovannetti y A S Holevo. "One-mode bosonic Gaussian channels: a full weak-degradability classification". En: *New Journal of Physics* 8.12 (dic. de 2006), págs. 310-310. doi: 10.1088/1367-2630/8/12/310.

[83] Filippo Caruso y Vittorio Giovannetti. "Degradability of Bosonic Gaussian channels". En: *Physical Review A* 74.6 (dic. de 2006), pág. 062307. doi: 10.1103/physreva.74.062307.

[84] Davide Castelvecchi. "IBM's quantum cloud computer goes commercial". En: *Nature* 543.7644 (mar. de 2017), págs. 159-159. doi: 10.1038/nature.2017.21585.

[85] Kaushik Chakraborty et al. "Distributed Routing in a Quantum Internet". En: (jul. de 2019). doi: 10.48550/ARXIV.1907.11630. arXiv: 1907.11630 [quant-ph].

[86] Kaushik Chakraborty et al. "Entanglement Distribution in a Quantum Network: A Multi-commodity Flow-Based Approach". En: *IEEE Transactions on Quantum Engineering* 1 (2020), págs. 1-21. doi: 10.1109/tqe.2020.3028172.

[87] Christopher Chamberland y Michael E. Beverland. "Flag fault-tolerant error correction with arbitrary distance codes". En: *Quantum* 2 (feb. de 2018), pág. 53. doi: 10.22331/q-2018-02-08-53.

[88] Rui Chao y Ben W. Reichardt. "Flag Fault-Tolerant Error Correction for any Stabilizer Code". En: *PRX Quantum* 1.1 (sep. de 2020), pág. 010302. doi: 10.1103/prxquantum.1.010302.

[89] Mahdi Chehimi et al. "Scaling Limits of Quantum Repeater Networks". En: (mayo de 2023). doi: 10.48550/ARXIV.2305.08696. arXiv: 2305.08696 [cs.NI].

[90] Jwo-Sy Chen et al. "Benchmarking a trapped-ion quantum computer with 29 algorithmic qubits". En: *arXiv preprint arXiv:2308.05071* (2023).

[91] Lutong Chen et al. "A Heuristic Remote Entanglement Distribution Algorithm on Memory-Limited Quantum Paths". En: *IEEE Transactions on Communications* 70.11 (2022), págs. 7491-7504. doi: 10.1109/TCOMM.2022.3205683.

[92] Shuai Chen et al. "Demonstration of a Stable Atom-Photon Entanglement Source for Quantum Repeaters". En: *Physical Review Letters* 99.18 (nov. de 2007), pág. 180505. doi: 10.1103/physrevlett.99.180505.

[93] L. Childress et al. "Coherent Dynamics of Coupled Electron and Nuclear Spin Qubits in Diamond". En: *Science* 314.5797 (oct. de 2006), págs. 281-285. doi: 10.1126/science.1131871.

[94] L. Childress et al. "Fault-Tolerant Quantum Communication Based on Solid-State Photon Emitters". En: *Physical Review Letters* 96.7 (feb. de 2006), pág. 070504. doi: 10.1103/physrevlett.96.070504.

[95] Giulio Chiribella, Giacomo Mauro D'Ariano y Paolo Perinotti. "Theoretical framework for quantum networks". En: *Physical Review A* 80.2 (ago. de 2009), pág. 022339. doi: 10.1103/physreva.80.022339.

[96] Giulio Chiribella, Matt Wilson y H. F. Chau. "Quantum and Classical Data Transmission through Completely Depolarizing Channels in a Superposition of Cyclic Orders". En: *Physical Review Letters* 127.19 (nov. de 2021), pág. 190502. doi: 10.1103/physrevlett.127.190502.

[97] Giulio Chiribella et al. "Quantum computations without definite causal structure". En: *Physical Review A* 88.2 (ago. de 2013), pág. 022318. doi: 10.1103/physreva.88.022318.

[98] Giulio Chiribella et al. "Indefinite causal order enables perfect quantum communication with zero capacity channels". En: *New Journal of Physics* 23.3 (mar. de 2021), pág. 033039. doi: 10.1088/1367-2630/abe7a0.

[99] Man-Duen Choi. "Completely positive linear maps on complex matrices". En: *Linear Algebra and its Applications* 10.3 (jun. de 1975), págs. 285-290. doi: 10.1016/0024-3795(75)90075-0.

[100] Chin-Wen Chou et al. "Functional Quantum Nodes for Entanglement Distribution over Scalable Quantum Networks". En: *Science* 316.5829 (jun. de 2007), págs. 1316-1320. doi: 10.1126/science.1140300.

[101] Jerry Chow, Oliver Dial y Jay Gambetta. "IBM Quantum breaks the 100-qubit processor barrier". En: *IBM Research Blog* 2 (2021).

[102] Matthias Christandl y Renato Renner. "Reliable quantum state tomography". En: *Physical Review Letters* 109.12 (2012), pág. 120403.

[103] Hye Won Chung, Saikat Guha y Lizhong Zheng. "Superadditivity of quantum channel coding rate with finite blocklength quantum measurements". En: *2014 IEEE International Symposium on Information Theory*. IEEE, jun. de 2014. doi: 10.1109/isit.2014.6874963.

[104] John Clarke y Frank K Wilhelm. "Superconducting quantum bits". En: *Nature* 453.7198 (2008), págs. 1031-1042.

[105] Richard Cleve, Daniel Gottesman y Hoi-Kwong Lo. "How to Share a Quantum Secret". En: *Physical Review Letters* 83.3 (jul. de 1999), págs. 648-651. doi: 10.1103/physrevlett.83.648.

[106] Bob Coecke. *Basic ZX-calculus for students and professionals*. 2023. arXiv: 2303.03163 [quant-ph].

[107] Dan Cogan et al. "Deterministic generation of indistinguishable photons in a cluster state". En: *Nature Photonics* 17.4 (feb. de 2023), págs. 324-329. doi: 10.1038/s41566-022-01152-2.

[108] O. A. Collins et al. "Multiplexed Memory-Insensitive Quantum Repeaters". En: *Physical Review Letters* 98.6 (feb. de 2007), pág. 060502. doi: 10.1103/physrevlett.98.060502.

[109] N. Coste et al. "High-rate entanglement between a semiconductor spin and indistinguishable photons". En: *Nature Photonics* 17.7 (abr. de 2023), págs. 582-587. doi: 10.1038/s41566-023-01186-0.

[110] J. Cramer et al. "Repeated quantum error correction on a continuously encoded qubit by real-time feedback". En: *Nature Communications* 7.1 (mayo de 2016). doi: 10.1038/ncomms11526.

[111] Marcus Cramer et al. "Efficient quantum state tomography". En: *Nature communications* 1.1 (2010), pág. 149.

[112] Andrew Cross et al. "OpenQASM 3: A broader and deeper quantum assembly language". En: *ACM Transactions on Quantum Computing* 3.3 (2022), págs. 1-50.

[113] Andrew W Cross et al. "Open quantum assembly language". En: *arXiv preprint arXiv:1707.03429* (2017).

[114] Andrew W Cross et al. "Validating quantum computers using randomized model circuits". En: *Physical Review A* 100.3 (2019), pág. 032328.

[115] Toby Cubitt et al. "Unbounded number of channel uses may be required to detect quantum capacity". En: *Nature Communications* 6.1 (mar. de 2015). doi: 10.1038/ncomms7739.

[116] Axel Dahlberg et al. "A link layer protocol for quantum networks". En: *Proceedings of the ACM Special Interest Group on Data Communication*. ACM, ago. de 2019. doi: 10.1145/3341302.3342070.

[117] Pierre-Luc Dallaire-Demers et al. "An application benchmark for fermionic quantum simulations". En: *arXiv preprint arXiv:2003.01862* (2020).

[118] William J Dally, Yatish Turakhia y Song Han. "Domain-specific hardware accelerators". En: *Communications of the ACM* 63.7 (2020), págs. 48-57.

[119] Rabindra N. Das et al. "Large Scale Cryogenic Integration Approach for Superconducting High-Performance Computing". En: *2017 IEEE 67th Electronic Components and Technology Conference (ECTC)*. IEEE, mayo de 2017. doi: 10.1109/ectc.2017.54.

[120] Shantanu Debnath et al. "Demonstration of a small programmable quantum computer with atomic qubits". En: *Nature* 536.7614 (2016), págs. 63-66.

[121] Aymeric Delteil et al. "Generation of heralded entanglement between distant hole spins". En: *Nature Physics* 12.3 (dic. de 2015), págs. 218-223. doi: 10.1038/nphys3605.

[122] David Deutsch et al. "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels". En: *Physical Review Letters* 77.13 (sep. de 1996), págs. 2818-2821. doi: 10.1103/physrevlett.77.2818.

[123] Oskar van Deventer et al. "Towards European standards for quantum technologies". En: *EPJ Quantum Technology* 9.1 (nov. de 2022). doi: 10.1140/epjqt/s40507-022-00150-1.

[124] I. Devetak y P. W. Shor. "The Capacity of a Quantum Channel for Simultaneous Transmission of Classical and Quantum Information". En: *Communications in Mathematical Physics* 256.2 (mar. de 2005), págs. 287-303. doi: 10.1007/s00220-005-1317-6.

[125] Simon J Devitt, William J Munro y Kae Nemoto. "Quantum error correction for beginners". En: *Reports on Progress in Physics* 76.7 (2013), pág. 076001.

[126] Michel H Devoret y Robert J Schoelkopf. "Superconducting circuits for quantum information: an outlook". En: *Science* 339.6124 (2013), págs. 1169-1174.

[127] Stephen DiAdamo, Marco Ghibaudi y James Cruise. "Distributed quantum computing and network control for accelerated vqe". En: *IEEE Transactions on Quantum Engineering* 2 (2021), págs. 1-21.

[128] Stephen DiAdamo et al. "Packet Switching in Quantum Networks: A Path to Quantum Internet". En: (mayo de 2022). doi: 10.48550/ARXIV.2205.07507. arXiv: 2205.07507 [quant-ph].

[129] Karsten B. Dideriksen et al. "Room-temperature single-photon source with near-millisecond built-in memory". En: *Nature Communications* 12.1 (jun. de 2021). doi: 10.1038/s41467-021-24033-8.

[130] D. Dieks. "Communication by EPR devices". En: *Physics Letters A* 92.6 (nov. de 1982), págs. 271-272. doi: 10.1016/0375-9601(82)90084-6.

[131] David P DiVincenzo. "The physical implementation of quantum computation". En: *Fortschritte der Physik: Progress of Physics* 48.9-11 (2000), págs. 771-783.

[132] David P. DiVincenzo, Peter W. Shor y John A. Smolin. "Quantum-channel capacity of very noisy channels". En: *Physical Review A* 57.2 (feb. de 1998), págs. 830-839. doi: 10.1103/physreva.57.830.

[133] Yulong Dong y Lin Lin. "Random circuit block-encoded matrix and a proposal of quantum LINPACK benchmark". En: *Physical Review A* 103.6 (2021), pág. 062412.

[134] L.-M. Duan et al. "Long-distance quantum communication with atomic ensembles and linear optics". En: *Nature* 414.6862 (nov. de 2001), págs. 413-418. doi: 10.1038/35106500.

[135] Y. O. Dudin, L. Li y A. Kuzmich. "Light storage on the time scale of a minute". En: *Physical Review A* 87.3 (mar. de 2013), pág. 031801. doi: 10.1103/physreva.87.031801.

[136] Y. O. Dudin et al. "Entanglement of Light-Shift Compensated Atomic Spin Waves with Telecom Light". En: *Physical Review Letters* 105.26 (dic. de 2010), pág. 260502. doi: 10.1103/physrevlett.105.260502.

[137] Fabrice Dupuy, Claire Goursaud y Fabrice Guillemin. "A Survey of Quantum Entanglement Routing Protocols—Challenges for Wide-Area Networks". En: *Advanced Quantum Technologies* 6.5 (mar. de 2023). doi: 10.1002/qute.202200180.

[138] W Dür y H J Briegel. "Entanglement purification and quantum error correction". En: *Reports on Progress in Physics* 70.8 (jul. de 2007), págs. 1381-1424. doi: 10.1088/0034-4885/70/8/r03. url: https://doi.org/10.1088%2F0034-4885%2F70%2F8%2Fr03.

[139] W. Dür et al. "Quantum repeaters based on entanglement purification". En: *Physical Review A* 59.1 (ene. de 1999), págs. 169-181. doi: 10.1103/physreva.59.169.

[140] M. V. Gurudev Dutt et al. "Ultrafast optical control of electron spin coherence in charged quantum dots". En: *Physical Review B* 74.12 (sep. de 2006), pág. 125306. doi: 10.1103/physrevb.74.125306.

[141] Phillippe H. Eberhard y Ronald R. Ross. "Quantum field theory cannot provide faster-than-light communication". En: *Foundations of Physics Letters* 2.2 (mar. de 1989), págs. 127-149. doi: 10.1007/bf00696109.

[142] Daniel Ebler, Sina Salek y Giulio Chiribella. "Enhanced Communication with the Assistance of Indefinite Causal Order". En: *Physical Review Letters* 120.12 (mar. de 2018), pág. 120502. doi: 10.1103/physrevlett.120.120502.

[143] Sophia E. Economou, Netanel Lindner y Terry Rudolph. "Optically Generated 2-Dimensional Photonic Cluster State from Coupled Quantum Dots". En: *Physical Review Letters* 105.9 (ago. de 2010), pág. 093601. doi: 10.1103/physrevlett.105.093601.

[144] Laird Egan et al. *Fault-Tolerant Operation of a Quantum Error-Correction Code*. 2020. doi: 10.48550/ARXIV.2009.11482.

[145] Artur Ekert y Chiara Macchiavello. "Quantum Error Correction for Communication". En: *Phys. Rev. Lett.* 77 (12 sep. de 1996), págs. 2585-2588. doi: 10.1103/PhysRevLett.77.2585. url: https://link.aps.org/doi/10.1103/PhysRevLett.77.2585.

[146] Artur K. Ekert. "Quantum cryptography based on Bell's theorem". En: *Physical Review Letters* 67.6 (ago. de 1991), págs. 661-663. doi: 10.1103/physrevlett.67.661.

[147] Suguru Endo, Simon C Benjamin y Ying Li. "Practical quantum error mitigation for near-future applications". En: *Physical Review X* 8.3 (2018), pág. 031027.

[148] Suguru Endo et al. "Hybrid quantum-classical algorithms and quantum error mitigation". En: *Journal of the Physical Society of Japan* 90.3 (2021), pág. 032001.

[149] Michael Epping, Hermann Kampermann y Dagmar Bruß. "Large-scale quantum networks based on graphs". En: *New Journal of Physics* 18.5 (mayo de 2016), pág. 053036. doi: 10.1088/1367-2630/18/5/053036.

[150] Pau Escofet et al. "Interconnect Fabrics for Multi-Core Quantum Processors: A Context Analysis". En: (sep. de 2023). doi: 10.1145/3610396.3623267. arXiv: 2309.07313 [quant-ph].

[151] Fabian Ewert, Marcel Bergmann y Peter van Loock. "Ultrafast Long-Distance Quantum Communication with Static Linear Optics". En: *Physical Review Letters* 117.21 (nov. de 2016), pág. 210501. doi: 10.1103/physrevlett.117.210501.

[152] Fabian Ewert y Peter van Loock. "3/4-Efficient Bell Measurement with Passive Linear Optics and Unentangled Ancillae". En: *Physical Review Letters* 113.14 (sep. de 2014), pág. 140403. doi: 10.1103/physrevlett.113.140403.

[153] Fabian Ewert y Peter van Loock. "Ultrafast fault-tolerant long-distance quantum communication with static linear optics". En: *Physical Review A* 95.1 (ene. de 2017), pág. 012327. doi: 10.1103/physreva.95.012327.

[154] *Expanding the IBM Quantum roadmap to anticipate the future of quantum-centric supercomputing*. url: https://research.ibm.com/blog/ibm-quantum-roadmap-2025.

[155] Jesse Fern y K. Birgitta Whaley. "Lower bounds on the nonzero capacity of Pauli channels". En: *Physical Review A* 78.6 (dic. de 2008), pág. 062335. doi: 10.1103/physreva.78.062335.

[156] Davide Ferrari et al. "Compiler Design for Distributed Quantum Computing". En: *IEEE Transactions on Quantum Engineering* 2 (2021), págs. 1-20. doi: 10.1109/tqe.2021.3053921.

[157] Sergey N. Filippov. "Lower and Upper Bounds on Nonunital Qubit Channel Capacities". En: *Reports on Mathematical Physics* 82.2 (oct. de 2018), págs. 149-159. doi: 10.1016/s0034-4877(18)30083-1.

[158] Sergey N. Filippov, Vladimir V. Frizen y Daria V. Kolobova. "Ultimate entanglement robustness of two-qubit states against general local noises". En: *Physical Review A* 97.1 (ene. de 2018), pág. 012322. doi: 10.1103/physreva.97.012322.

[159] Paolo Fittipaldi, Anastasios Giovanidis y Frédéric Grosshans. "A Linear Algebraic Framework for Dynamic Scheduling Over Memory-Equipped Quantum Networks". En: (jul. de 2023). doi: 10.48550/ARXIV.2307.06009. arXiv: 2307.06009 [quant-ph].

[160] Joseph F. Fitzsimons. "Private quantum computation: an introduction to blind quantum computing and related protocols". En: *npj Quantum Information* 3.1 (jun. de 2017). doi: 10.1038/s41534-017-0025-3.

[161] Joseph F. Fitzsimons y Elham Kashefi. "Unconditionally verifiable blind quantum computation". En: *Physical Review A* 96.1 (jul. de 2017), pág. 012303. doi: 10.1103/physreva.96.012303.

[162] Austin G Fowler et al. "Surface codes: Towards practical large-scale quantum computation". En: *Physical Review A* 86.3 (2012), pág. 032324.

[163] Austin G. Fowler et al. "Surface Code Quantum Communication". En: *Physical Review Letters* 104.18 (mayo de 2010), pág. 180503. doi: 10.1103/physrevlett.104.180503.

[164] G. D. Fuchs et al. "A quantum memory intrinsic to single nitrogen–vacancy centres in diamond". En: *Nature Physics* 7.10 (jun. de 2011), págs. 789-793. doi: 10.1038/nphys2026.

[165] Keisuke Fujii y Katsuji Yamamoto. "Entanglement purification with double selection". En: *Physical Review A* 80.4 (oct. de 2009), pág. 042308. doi: 10.1103/physreva.80.042308.

[166] Kosuke Fukui, Rafael N. Alexander y Peter van Loock. "All-optical long-distance quantum communication with Gottesman-Kitaev-Preskill qubits". En: *Physical Review Research* 3.3 (ago. de 2021), pág. 033118. doi: 10.1103/physrevresearch.3.033118.

[167] Kosuke Fukui, Akihisa Tomita y Atsushi Okamoto. "Analog Quantum Error Correction with Encoding a Qubit into an Oscillator". En: *Physical Review Letters* 119.18 (nov. de 2017), pág. 180507. doi: 10.1103/physrevlett.119.180507.

[168] Abbas El Gamal y Young-Han Kim. *Network Information Theory*. Cambridge University Press, 2012. isbn: 9781139030687.

[169] Jay Gambetta. *Expanding the IBM Quantum roadmap to anticipate the future of quantum-centric supercomputing*. IBM Research Blog [Online]. url: https://research.ibm.com/blog/ibm-quantum-roadmap-2025.

[170] Jay Gambetta et al. "Driving quantum performance: More qubits higher quantum volume and now a proper measure for speed". En: *IBM Res.* (2021).

[171] D. A. Gangloff et al. "Quantum interface of an electron and a nuclear ensemble". En: *Science* 364.6435 (abr. de 2019), págs. 62-66. doi: 10.1126/science.aaw2906.

[172] Maor Ganz. "Quantum Leader Election". En: *Quantum Information Processing* 16 (feb. de 2017). doi: 10.1007/s11128-017-1528-8.

[173] W. B. Gao et al. "Observation of entanglement between a quantum dot spin and a single photon". En: *Nature* 491.7424 (nov. de 2012), págs. 426-430. doi: 10.1038/nature11573.

[174] Bertrand Georgeot y Dima L Shepelyansky. "Quantum chaos border for quantum computing". En: *Physical Review E* 62.3 (2000), pág. 3504.

[175] Mercedes Gimeno-Segovia. "Towards practical linear optical quantum computing". En: (2015). doi: 10.25560/43936.

[176] Mercedes Gimeno-Segovia, Terry Rudolph y Sophia E. Economou. "Deterministic Generation of Large-Scale Entangled Photonic Cluster State from Interacting Solid State Emitters". En: *Physical Review Letters* 123.7 (ago. de 2019), pág. 070501. doi: 10.1103/physrevlett.123.070501.

[177] Vittorio Giovannetti y Stefano Mancini. "Bosonic memory channels". En: *Physical Review A* 71.6 (jun. de 2005), pág. 062304. doi: 10.1103/physreva.71.062304.

[178] N. Gisin et al. "Error filtration and entanglement purification for quantum communication". En: *Physical Review A* 72.1 (jul. de 2005), pág. 012338. doi: 10.1103/physreva.72.012338.

[179] Alysson Gold et al. "Entanglement Across Separate Silicon Dies in a Modular Superconducting Qubit Device". En: (feb. de 2021). doi: 10.48550/ARXIV.2102.13293. arXiv: 2102.13293 [quant-ph].

[180] Daniel Gottesman. *Stabilizer Codes and Quantum Error Correction*. 1997. doi: 10.48550/ARXIV.QUANT-PH/9705052.

[181] Daniel Gottesman. "Theory of fault-tolerant quantum computation". En: *Physical Review A* 57.1 (ene. de 1998), págs. 127-137. doi: 10.1103/physreva.57.127.

[182] Daniel Gottesman, Alexei Kitaev y John Preskill. "Encoding a qubit in an oscillator". En: *Physical Review A* 64.1 (jun. de 2001), pág. 012310. doi: 10.1103/physreva.64.012310.

[183] Markus Grassl et al. "Applying Grover's algorithm to AES: quantum resource estimates". En: *International Workshop on Post-Quantum Cryptography*. Springer. 2016, págs. 29-43.

[184] Alexander S Green et al. "Quipper: a scalable quantum programming language". En: *Proceedings of the 34th ACM SIGPLAN conference on Programming language design and implementation*. 2013, págs. 333-342.

[185] Daniel M. Greenberger, Michael A. Horne y Anton Zeilinger. "Going Beyond Bell's Theorem". En: (2007). doi: 10.48550/ARXIV.0712.0921.

[186] A. Greilich et al. "Nuclei-Induced Frequency Focusing of Electron Spin Coherence". En: *Science* 317.5846 (sep. de 2007), págs. 1896-1899. doi: 10.1126/science.1146850.

[187] Kristiaan De Greve et al. "Quantum-dot spin–photon entanglement via frequency down-conversion to telecom wavelength". En: *Nature* 491.7424 (nov. de 2012), págs. 421-425. doi: 10.1038/nature11577.

[188] W. P. Grice. "Arbitrarily complete Bell-state measurement using only linear optical elements". En: *Physical Review A* 84.4 (oct. de 2011), pág. 042331. doi: 10.1103/physreva.84.042331.

[189] David Gross et al. "Quantum state tomography via compressed sensing". En: *Physical review letters* 105.15 (2010), pág. 150401.

[190] Gian Giacomo Guerreschi et al. "Intel Quantum Simulator: A cloud-ready high-performance simulator of quantum circuits". En: *Quantum Science and Technology* 5.3 (2020), pág. 034007.

[191] Laszlo Gyongyosi, Sandor Imre y Hung Viet Nguyen. "A Survey on Quantum Channel Capacities". En: *IEEE Communications Surveys & Tutorials* 20.2 (2018), págs. 1149-1205. doi: 10.1109/comst.2017.2786748.

[192] Robert H. Hadfield. "Single-photon detectors for optical quantum information applications". En: *Nature Photonics* 3.12 (dic. de 2009), págs. 696-705. doi: 10.1038/nphoton.2009.230.

[193] F. Hahn, A. Pappa y J. Eisert. "Quantum network routing and local complementation". En: *npj Quantum Information* 5.1 (sep. de 2019). doi: 10.1038/s41534-019-0191-6.

[194] Thomas Häner et al. "High performance emulation of quantum circuits". En: *SC'16: Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*. IEEE. 2016, págs. 866-874.

[195] Serge Haroche y Jean-Michel Raimond. "Quantum computing: dream or nightmare?" En: *Physics Today* 49.8 (1996), págs. 51-52.

[196] Matthew P Harrigan et al. "Quantum approximate optimization of non-planar graph problems on a planar superconducting processor". En: *Nature Physics* 17.3 (2021), págs. 332-336.

[197] Richard Harris et al. "Experimental investigation of an eight-qubit unit cell in a superconducting optimization processor". En: *Physical Review B* 82.2 (2010), pág. 024511.

[198] Yasushi Hasegawa et al. "Experimental time-reversed adaptive Bell measurement towards all-photonic quantum repeaters". En: *Nature Communications* 10.1 (ene. de 2019). doi: 10.1038/s41467-018-08099-5.

[199] M. B. Hastings. "Superadditivity of communication capacity using entangled inputs". En: *Nature Physics* 5.4 (mar. de 2009), págs. 255-257. doi: 10.1038/nphys1224.

[200] Paul Hausladen et al. "Classical information capacity of a quantum channel". En: *Physical Review A* 54.3 (sep. de 1996), págs. 1869-1876. doi: 10.1103/physreva.54.1869.

[201] M. Hein, J. Eisert y H. J. Briegel. "Multiparty entanglement in graph states". En: *Physical Review A* 69.6 (jun. de 2004), pág. 062311. doi: 10.1103/physreva.69.062311.

[202] John L Hennessy y David A Patterson. "A new golden age for computer architecture". En: *Communications of the ACM* 62.2 (2019), págs. 48-60.

[203] B. Hensen et al. "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres". En: *Nature* 526.7575 (oct. de 2015), págs. 682-686. doi: 10.1038/nature15759.

[204] David A. Herrera-Martí et al. "Photonic implementation for the topological cluster-state quantum computer". En: *Physical Review A* 82.3 (sep. de 2010), pág. 032332. doi: 10.1103/physreva.82.032332.

[205] Khabat Heshami et al. "Quantum memories: emerging applications and recent advances". En: *Journal of Modern Optics* 63.20 (mar. de 2016), págs. 2005-2028. doi: 10.1080/09500340.2016.1148212.

[206] Fumio Hiai y Milán Mosonyi. "Different quantum f-divergences and the reversibility of quantum operations". En: *Reviews in Mathematical Physics* 29.07 (ago. de 2017), pág. 1750023. doi: 10.1142/s0129055x17500234.

[207] Paul Hilaire, Edwin Barnes y Sophia E. Economou. "Resource requirements for efficient quantum communication using all-photonic graph states generated from a few matter qubits". En: *Quantum* 5 (feb. de 2021), pág. 397. doi: 10.22331/q-2021-02-15-397.

[208] Mark Hillery, Vladimír Bu žek y André Berthiaume. "Quantum secret sharing". En: *Phys. Rev. A* 59 (3 mar. de 1999), págs. 1829-1834. doi: 10.1103/PhysRevA.59.1829. url: https://link.aps.org/doi/10.1103/PhysRevA.59.1829.

[209] A S Holevo y V Giovannetti. "Quantum channels and their entropic characteristics". En: *Reports on Progress in Physics* 75.4 (mar. de 2012), pág. 046001. doi: 10.1088/0034-4885/75/4/046001.

[210] A.S. Holevo. "Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel". En: *Probl. Peredachi Inf.* 9.3 (1973), págs. 177-183.

[211] A.S. Holevo. "The capacity of the quantum channel with general signal states". En: *IEEE Transactions on Information Theory* 44.1 (1998), págs. 269-273. doi: 10.1109/18.651037.

[212] Michael Horodecki, Peter W. Shor y Mary Beth Ruskai. "Entanglement Breaking Channels". En: *Reviews in Mathematical Physics* 15.06 (ago. de 2003), págs. 629-641. doi: 10.1142/s0129055x03001709.

[213] Michał Horodecki, Jonathan Oppenheim y Andreas Winter. "Quantum State Merging and Negative Information". En: *Communications in Mathematical Physics* 269.1 (oct. de 2006), págs. 107-136. doi: 10.1007/s00220-006-0118-x.

[214] Ryszard Horodecki et al. "Quantum entanglement". En: *Reviews of Modern Physics* 81.2 (jun. de 2009), págs. 865-942. doi: 10.1103/revmodphys.81.865.

[215] Paul Hudak y Joseph H Fasel. "A gentle introduction to Haskell". En: *ACM Sigplan Notices* 27.5 (1992), págs. 1-52.

[216] Peter C. Humphreys et al. "Deterministic delivery of remote entanglement on a quantum network". En: *Nature* 558.7709 (jun. de 2018), págs. 268-273. doi: 10.1038/s41586-018-0200-5.

[217] Rikizo Ikuta et al. "Wide-band quantum interface for visible-to-telecommunication wavelength conversion". En: *Nature Communications* 2.1 (nov. de 2011). doi: 10.1038/ncomms1544.

[218] Rikizo Ikuta et al. "Polarization insensitive frequency conversion for an atom-photon entanglement distribution via a telecom network". En: *Nature Communications* 9.1 (mayo de 2018). doi: 10.1038/s41467-018-04338-x.

[219] Jessica Illiano et al. "Quantum Internet protocol stack: A comprehensive survey". En: *Computer Networks* 213 (ago. de 2022), pág. 109092. doi: 10.1016/j.comnet.2022.109092.

[220] I. V. Inlek et al. "Multispecies Trapped-Ion Node for Quantum Networking". En: *Physical Review Letters* 118.25 (jun. de 2017), pág. 250502. doi: 10.1103/physrevlett.118.250502.

[221] Álvaro G. Iñesta y Stephanie Wehner. "Performance metrics for the continuous distribution of entanglement in multi-user quantum networks". En: (jul. de 2023). doi: 10.48550/ARXIV.2307.01406. arXiv: 2307.01406 [quant-ph].

[222] Abhijith J. et al. "Quantum Algorithm Implementations for Beginners". En: *ACM Transactions on Quantum Computing* 3.4 (jul. de 2022), págs. 1-92. doi: 10.1145/3517340.

[223] D. M. Jackson et al. "Quantum sensing of a coherent single spin excitation in a nuclear ensemble". En: *Nature Physics* 17.5 (feb. de 2021), págs. 585-590. doi: 10.1038/s41567-020-01161-4.

[224] B. C. Jacobs, T. B. Pittman y J. D. Franson. "Quantum relays and noise suppression using linear optics". En: *Physical Review A* 66.5 (nov. de 2002), pág. 052307. doi: 10.1103/physreva.66.052307.

[225] Jia-Wei Ji et al. "Proposal for room-temperature quantum repeaters with nitrogen-vacancy centers and optomechanics". En: *Quantum* 6 (mar. de 2022), pág. 669. doi: 10.22331/q-2022-03-17-669.

[226] Liang Jiang et al. "Distributed quantum computation based on small quantum registers". En: *Physical Review A* 76.6 (dic. de 2007), pág. 062323. doi: 10.1103/physreva.76.062323.

[227] Liang Jiang et al. "Quantum repeater with encoding". En: *Physical Review A* 79.3 (mar. de 2009), pág. 032325. doi: 10.1103/physreva.79.032325.

[228] Hamza Jnane et al. "Multicore Quantum Computing". En: *Physical Review Applied* 18.4 (oct. de 2022), pág. 044064. doi: 10.1103/physrevapplied.18.044064.

[229] Jaewoo Joo et al. "One-way quantum computation with four-dimensional photonic qudits". En: *Physical Review A* 76.5 (nov. de 2007), pág. 052326. doi: 10.1103/physreva.76.052326.

[230] S. Kahtri y M. M. Wilde. *Principles of Quantum Communication Thoery: A Modern Approach*. 2021. url: https://www.markwilde.com/PQCT-khatri-wilde.pdf.

[231] Jan Kaiser y Supriyo Datta. "Probabilistic computing with p-bits". En: *Applied Physics Letters* 119.15 (2021).

[232] Gil Kalai. "The argument against quantum computers". En: *Quantum, probability, logic: The work and influence of Itamar Pitowsky* (2020), págs. 399-422.

[233] N. Kalb et al. "Entanglement distillation between solid-state quantum network nodes". En: *Science* 356.6341 (jun. de 2017), págs. 928-932. doi: 10.1126/science.aan0070.

[234] Abhinav Kandala et al. "Error mitigation extends the computational reach of a noisy quantum processor". En: *Nature* 567.7749 (2019), págs. 491-495.

[235] Bharath Kannan et al. "On-demand directional microwave photon emission using waveguide quantum electrodynamics". En: *Nature Physics* 19.3 (ene. de 2023), págs. 394-400. doi: 10.1038/s41567-022-01869-5.

[236] Or Katz y Ofer Firstenberg. "Light storage for one second in room-temperature alkali vapor". En: *Nature Communications* 9.1 (mayo de 2018). doi: 10.1038/s41467-018-04458-4.

[237] V. Kaushal et al. "Shuttling-Based Trapped-Ion Quantum Information Processing". En: (dic. de 2019). doi: 10.48550/ARXIV.1912.04712. arXiv: 1912.04712 [quant-ph].

[238] Nader Khammassi et al. "cqasm v1. 0: Towards a common quantum assembly language". En: *arXiv preprint arXiv:1805.09607* (2018).

[239] Tariq M Khan y Antonio Robles-Kelly. "Machine learning: Quantum vs classical". En: *IEEE Access* 8 (2020), págs. 219275-219294.

[240] Sumeet Khatri, Kunal Sharma y Mark M. Wilde. "Information-theoretic aspects of the generalized amplitude-damping channel". En: *Physical Review A* 102.1 (jul. de 2020), pág. 012401. doi: 10.1103/physreva.102.012401.

[241] Sumeet Khatri et al. "Practical figures of merit and thresholds for entanglement distribution in quantum networks". En: *Physical Review Research* 1.2 (sep. de 2019), pág. 023032. doi: 10.1103/physrevresearch.1.023032.

[242] Andrey Boris Khesin y Peter Shor. *Simultaneous Measurement and Entanglement*. 2022. doi: 10.48550/ARXIV.2201.10667.

[243] Nathan Killoran et al. "Strawberry fields: A software platform for photonic quantum computing". En: *Quantum* 3 (2019), pág. 129.

[244] Thomas Kilmer y Saikat Guha. "Boosting linear-optical Bell measurement success probability with predetection squeezing and imperfect photon-number-resolving detectors". En: *Physical Review A* 99.3 (mar. de 2019), pág. 032302. doi: 10.1103/physreva.99.032302.

[245] Youngseok Kim et al. "Evidence for the utility of quantum computing before fault tolerance". En: *Nature* 618.7965 (2023), págs. 500-505.

[246] H. J. Kimble. "The quantum internet". En: *Nature* 453.7198 (jun. de 2008), págs. 1023-1030. doi: 10.1038/nature07127.

[247] C. King. "The capacity of the quantum depolarizing channel". En: *IEEE Transactions on Information Theory* 49.1 (ene. de 2003), págs. 221-229. doi: 10.1109/tit.2002.806153.

[248] Christopher King et al. "Properties of Conjugate Channels with Applications to Additivity and Multiplicativity". En: (2005). doi: 10.48550/ARXIV.QUANT-PH/0509126.

[249] Aleks Kissinger y John van de Wetering. "Pyzx: Large scale automated diagrammatic reasoning". En: *arXiv preprint arXiv:1904.04735* (2019).

[250] Emanuel Knill y Raymond Laflamme. "Theory of quantum error-correcting codes". En: *Physical Review A* 55.2 (feb. de 1997), págs. 900-911. doi: 10.1103/physreva.55.900.

[251] Emanuel Knill et al. "Randomized benchmarking of quantum gates". En: *Physical Review A* 77.1 (2008), pág. 012307.

[252] Pieter Kok, Colin P. Williams y Jonathan P. Dowling. "Construction of a quantum repeater with linear optics". En: *Physical Review A* 68.2 (ago. de 2003), pág. 022301. doi: 10.1103/physreva.68.022301.

[253] Pieter Kok et al. "Linear optical quantum computing with photonic qubits". En: *Reviews of Modern Physics* 79.1 (ene. de 2007), págs. 135-174. doi: 10.1103/revmodphys.79.135.

[254] Weicheng Kong et al. "Origin pilot: a quantum operating system for effecient usage of quantum resources". En: *arXiv preprint arXiv:2105.10730* (2021).

[255] Seid Koudia et al. "How Deep the Theory of Quantum Communications Goes: Superadditivity, Superactivation and Causal Activation". En: *IEEE Commun. Surv. Tutor. 24 (4), 1926-1956 (2022)* 24.4 (ago. de 2021), págs. 1926-1956. doi: 10.1109/comst.2022.3196449. arXiv: 2108.07108 [quant-ph].

[256] W. Kozlowski et al. *Architectural Principles for a Quantum Internet*. Inf. téc. Mar. de 2023. doi: 10.17487/rfc9340.

[257] Wojciech Kozlowski, Axel Dahlberg y Stephanie Wehner. "Designing a quantum network protocol". En: *Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies*. ACM, nov. de 2020. doi: 10.1145/3386367.3431293.

[258] Stefan Krastanov, Victor V. Albert y Liang Jiang. "Optimized Entanglement Purification". En: *Quantum* 3 (feb. de 2019), pág. 123. doi: 10.22331/q-2019-02-18-123.

[259] K Kraus. "General state changes in quantum theory". En: *Annals of Physics* 64.2 (jun. de 1971), págs. 311-335. doi: 10.1016/0003-4916(71)90108-4.

[260] Hlér Kristjánsson et al. "Resource theories of communication". En: *New Journal of Physics* 22.7 (jul. de 2020), pág. 073014. doi: 10.1088/1367-2630/ab8ef7.

[261] Rolf Landauer. "The physical nature of information". En: *Physics letters A* 217.4-5 (1996), págs. 188-193.

[262] Chris Lattner y Vikram Adve. "LLVM: A compilation framework for lifelong program analysis & transformation". En: *International symposium on code generation and optimization, 2004. CGO 2004.* IEEE. 2004, págs. 75-86.

[263] Jonathan Wei Zhong Lau et al. "NISQ computing: where are we and where do we go?" En: *AAPPS Bulletin* 32.1 (2022), pág. 27.

[264] Nikolai Lauk et al. "Perspectives on quantum transduction". En: *Quantum Science and Technology* 5.2 (mar. de 2020), pág. 020501. doi: 10.1088/2058-9565/ab788a.

[265] N Lazarides y GP Tsironis. "RF superconducting quantum interference device metamaterials". En: *Applied Physics Letters* 90.16 (2007).

[266] Felix Leditzky, Debbie Leung y Graeme Smith. "Dephrasure Channel and Superadditivity of Coherent Information". En: *Physical Review Letters* 121.16 (oct. de 2018), pág. 160501. doi: 10.1103/physrevlett.121.160501.

[267] Felix Leditzky et al. "Generic Nonadditivity of Quantum Capacity in Simple Channels". En: *Physical Review Letters* 130.20 (mayo de 2023), pág. 200801. doi: 10.1103/physrevlett.130.200801.

[268] J P Lee et al. "A quantum dot as a source of time-bin entangled multi-photon states". En: *Quantum Science and Technology* 4.2 (mar. de 2019), pág. 025011. doi: 10.1088/2058-9565/ab0a9b.

[269] J. P. Lee et al. "Controllable Photonic Time-Bin Qubits from a Quantum Dot". En: *Physical Review X* 8.2 (jun. de 2018), pág. 021078. doi: 10.1103/physrevx.8.021078.

[270] Seung-Woo Lee, Timothy C. Ralph y Hyunseok Jeong. "Fundamental building block for all-optical scalable quantum networks". En: *Physical Review A* 100.5 (nov. de 2019), pág. 052303. doi: 10.1103/physreva.100.052303.

[271] Zaki Leghtas et al. "Hardware-Efficient Autonomous Quantum Memory Protection". En: *Physical Review Letters* 111.12 (sep. de 2013), pág. 120501. doi: 10.1103/physrevlett.111.120501.

[272] N. Leung et al. "Deterministic Bidirectional Communication and Remote Entanglement Generation Between Superconducting Quantum Processors". En: (abr. de 2018). doi: 10.48550/ARXIV.1804.02028. arXiv: 1804.02028 [quant-ph].

[273] Patrick M. Leung y Timothy C. Ralph. "Quantum memory scheme based on optical fibers and cavities". En: *Physical Review A* 74.2 (ago. de 2006), pág. 022311. doi: 10.1103/physreva.74.022311.

[274] Ang Li et al. "Qasmbench: A low-level quantum benchmark suite for nisq evaluation and simulation". En: *ACM Transactions on Quantum Computing* 4.2 (2023), págs. 1-26.

[275] Bikun Li, Sophia E. Economou y Edwin Barnes. "Photonic resource state generation from a minimal number of quantum emitters". En: *npj Quantum Information* 8.1 (feb. de 2022). doi: 10.1038/s41534-022-00522-6.

[276] Changhao Li et al. "Effective routing design for remote entanglement generation on quantum networks". En: *npj Quantum Information* 7 (2020). url: https://api.semanticscholar.org/CorpusID:210023698.

[277] Chen-Long Li et al. "Breaking the rate-distance limitation of measurement-device-independent quantum secret sharing". En: *Phys. Rev. Res.* 5 (3 ago. de 2023), pág. 033077. doi: 10.1103/PhysRevResearch.5.033077. url: https://link.aps.org/doi/10.1103/PhysRevResearch.5.033077.

[278] Fulin Li et al. "A verifiable (k, n)-threshold dynamic quantum secret sharing scheme". En: *Quantum Information Processing* 21 (2022). url: https://api.semanticscholar.org/CorpusID:251169605.

[279] Hang Li et al. "Heralding quantum entanglement between two room-temperature atomic ensembles". En: *Optica* 8.6 (jun. de 2021), pág. 925. doi: 10.1364/optica.424599.

[280] Jian Li et al. "Fidelity-Guarantee Entanglement Routing in Quantum Networks". En: (nov. de 2021). doi: 10.48550/ARXIV.2111.07764. arXiv: 2111.07764 [quant-ph].

[281] Linshu Li et al. "Cat Codes with Optimal Decoherence Suppression for a Lossy Bosonic Channel". En: *Physical Review Letters* 119.3 (jul. de 2017), pág. 030502. doi: 10.1103/physrevlett.119.030502.

[282] Qin Li et al. "Efficient Quantum Blockchain With a Consensus Mechanism QDPoS". En: *IEEE Transactions on Information Forensics and Security* 17 (2022), págs. 3264-3276. doi: 10.1109/tifs.2022.3203316.

[283] Ying Li et al. "Long range failure-tolerant entanglement distribution". En: *New Journal of Physics* 15.2 (feb. de 2013), pág. 023012. doi: 10.1088/1367-2630/15/2/023012.

[284] Ying Li et al. "Resource Costs for Fault-Tolerant Linear Optical Quantum Computing". En: *Physical Review X* 5.4 (oct. de 2015), pág. 041007. doi: 10.1103/physrevx.5.041007.

[285] Zheng-Da Li et al. "Experimental quantum repeater without quantum memory". En: *Nature Photonics* 13.9 (jun. de 2019), págs. 644-648. doi: 10.1038/s41566-019-0468-5.

[286] Zhonghui Li et al. "Building a large-scale and wide-area quantum Internet based on an OSI-alike model". En: *China Communications* 18.10 (oct. de 2021), págs. 1-14. doi: 10.23919/jcc.2021.10.001.

[287] Zhonghui Li et al. "Entanglement-Assisted Quantum Networks: Mechanics, Enabling Technologies, Challenges, and Research Directions". En: *IEEE Communications Surveys & Tutorials* (2023), págs. 1-1. doi: 10.1109/comst.2023.3294240.

[288] Zhuo Li, Li-Juan Xing y Xin-Mei Wang. "Quantum generalized Reed-Solomon codes: Unified framework for quantum maximum-distance-separable codes". En: *Physical Review A* 77.1 (ene. de 2008), pág. 012308. doi: 10.1103/physreva.77.012308.

[289] Daniel A Lidar y Todd A Brun. *Quantum error correction*. Cambridge university press, 2013.

[290] Daniel A. Lidar y Todd A. Brun. *Quantum Error Correction*. Cambridge University Press, 2013. isbn: 9781139034807.

[291] Youngrong Lim et al. "Activation and superactivation of single-mode Gaussian quantum channels". En: *Physical Review A* 99.3 (mar. de 2019), pág. 032337. doi: 10.1103/physreva.99.032337.

[292] Netanel H. Lindner y Terry Rudolph. "Proposal for Pulsed On-Demand Sources of Photonic Cluster State Strings". En: *Physical Review Letters* 103.11 (sep. de 2009), pág. 113602. doi: 10.1103/physrevlett.103.113602.

[293] Adriana E. Lita, Aaron J. Miller y Sae Woo Nam. "Counting near-infrared single-photons with 95% efficiency". En: *Optics Express* 16.5 (2008), pág. 3032. doi: 10.1364/oe.16.003032.

[294] Daniel Llewellyn et al. "Chip-to-chip quantum teleportation and multi-photon entanglement in silicon". En: *Nature Physics* 16.2 (dic. de 2019), págs. 148-153. doi: 10.1038/s41567-019-0727-x.

[295] Seth Lloyd. "Capacity of the noisy quantum channel". En: *Physical Review A* 55.3 (mar. de 1997), págs. 1613-1622. doi: 10.1103/physreva.55.1613.

[296] Hoi-Kwong Lo. "Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity". En: *Physical Review A* 62.1 (jun. de 2000), pág. 012313. doi: 10.1103/physreva.62.012313.

[297] Hoi-Kwong Lo, Sandu Popescu y Tim Spiller. *Introduction to Quantum Computation and Information*. World Scientific Publishing Company, pág. 348. isbn: 9789810233990.

[298] P. van Loock et al. "Hybrid Quantum Repeater Using Bright Coherent Light". En: *Physical Review Letters* 96.24 (jun. de 2006), pág. 240501. doi: 10.1103/physrevlett.96.240501.

[299] Thomas Lubinski et al. "Application-oriented performance benchmarks for quantum computing". En: *IEEE Transactions on Quantum Engineering* (2023).

[300] Yi Luo, Hao-Kun Mao y Qiong Li. *An Information-theoretical Secured Byzantine-fault Tolerance Consensus in Quantum Key Distribution Network*. 2022. arXiv: 2204.09832 [quant-ph].

[301] Cosmo Lupo, Vittorio Giovannetti y Stefano Mancini. "Capacities of Lossy Bosonic Memory Channels". En: *Physical Review Letters* 104.3 (ene. de 2010), pág. 030501. doi: 10.1103/physrevlett.104.030501.

[302] Alexander I. Lvovsky, Barry C. Sanders y Wolfgang Tittel. "Optical quantum memory". En: *Nature Photonics* 3.12 (dic. de 2009), págs. 706-714. doi: 10.1038/nphoton.2009.231.

[303] Hein M. et al. "Entanglement in graph states and its applications". En: *Proceedings of the International School of Physics Enrico Fermi* 162 (2006), págs. 115-218. issn: 0074-784X. doi: 10.3254/978-1-61499-018-5-115.

[304] Yu Ma et al. "One-hour coherent optical storage in an atomic frequency comb memory". En: *Nature Communications* 12.1 (abr. de 2021). doi: 10.1038/s41467-021-22706-y.

[305] Chiara Macchiavello y G. Massimo Palma. "Entanglement-enhanced information transmission over a quantum channel with correlated noise". En: *Physical Review A* 65.5 (abr. de 2002), pág. 050301. doi: 10.1103/physreva.65.050301.

[306] Robert Maiwald et al. "Collecting more than half the fluorescence photons from a single ion". En: *Physical Review A* 86.4 (oct. de 2012), pág. 043431. doi: 10.1103/physreva.86.043431.

[307] M. Malinowski, D. T. C. Allcock y C. J. Ballance. "How to wire a 1000-qubit trapped ion quantum computer". En: (mayo de 2023). doi: 10.48550/ARXIV.2305.12773. arXiv: 2305.12773 [quant-ph].

[308] Marco Marcozzi y Leonardo Mostarda. *Quantum Consensus: an overview*. 2021. doi: 10.48550/ARXIV.2101.04192.

[309] Gabriel Marin-Sanchez, Javier Gonzalez-Conde y Mikel Sanz. "Quantum algorithms for approximate function loading". En: *Phys. Rev. Research 5, 033114 (2023)* 5.3 (15 de nov. de 2021), pág. 033114. doi: 10.1103/physrevresearch.5.033114. arXiv: 2111.07933 [quant-ph].

[310] Leigh S. Martin y K. Birgitta Whaley. *Single-shot deterministic entanglement between non-interacting systems with linear optics*. 2019. doi: 10.48550/ARXIV.1912.00067.

[311] Josu Etxezarreta Martinez, Antonio deMarti iOlius y Pedro M. Crespo. "Superadditivity effects of quantum capacity decrease with the dimension for qudit depolarizing channels". En: *Physical Review A* 108.3 (sep. de 2023), pág. 032602. doi: 10.1103/physreva.108.032602.

[312] Paweł Mazurek et al. "Long-distance quantum communication over noisy networks without long-time quantum memory". En: *Physical Review A* 90.6 (dic. de 2014), pág. 062311. doi: 10.1103/physreva.90.062311.

[313] Alexander J McCaskey et al. "Quantum chemistry as a benchmark for near-term quantum computers". En: *npj Quantum Information* 5.1 (2019), pág. 99.

[314] H. J. McGuinness et al. "Quantum Frequency Translation of Single-Photon States in a Photonic Crystal Fiber". En: *Physical Review Letters* 105.9 (ago. de 2010), pág. 093604. doi: 10.1103/physrevlett.105.093604.

[315] Koen Mesman, Zaid Al-Ars y Matthias Möller. "Qpack: Quantum approximate optimization algorithms as universal benchmark for quantum computers". En: *arXiv preprint arXiv:2103.17193* (2021).

[316] R. Van Meter et al. "System Design for a Long-Line Quantum Repeater". En: *IEEE/ACM Transactions on Networking* 17.3 (jun. de 2009), págs. 1002-1013. doi: 10.1109/tnet.2008.927260.

[317] Rodney Van Meter et al. "Path selection for quantum repeater networks". En: *Networking Science* 3.1-4 (dic. de 2013), págs. 82-95. doi: 10.1007/s13119-013-0026-2.

[318] Rodney Van Meter et al. "A Quantum Internet Architecture". En: *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*. IEEE, sep. de 2022. doi: 10.1109/qce53715.2022.00055.

[319] Marios H. Michael et al. "New Class of Quantum Error-Correcting Codes for a Bosonic Mode". En: *Physical Review X* 6.3 (jul. de 2016), pág. 031006. doi: 10.1103/physrevx.6.031006.

[320] Jorge Miguel-Ramiro, Alexander Pirker y Wolfgang Dür. "Optimized Quantum Networks". En: *Quantum 7, 919 (2023)* 7 (21 de jul. de 2021), pág. 919. doi: 10.22331/q-2023-02-09-919. arXiv: 2107.10275 [quant-ph].

[321] Keith Miller et al. "An improved volumetric metric for quantum computers via more representative quantum circuit shapes". En: *arXiv preprint arXiv:2207.02315* (2022).

[322] Daniel Mills et al. "Application-motivated, holistic benchmarking of a full quantum computing stack". En: *Quantum* 5 (2021), pág. 415.

[323] Mohammad Mirhosseini et al. "Superconducting qubit to optical photon transduction". En: *Nature* 588.7839 (dic. de 2020), págs. 599-603. doi: 10.1038/s41586-020-3038-6.

[324] Mazyar Mirrahimi et al. "Dynamically protected cat-qubits: a new paradigm for universal quantum computation". En: *New Journal of Physics* 16.4 (abr. de 2014), pág. 045014. doi: 10.1088/1367-2630/16/4/045014.

[325] D. L. Moehring et al. "Entanglement of single-atom quantum bits at a distance". En: *Nature* 449.7158 (sep. de 2007), págs. 68-71. doi: 10.1038/nature06118.

[326] Masoud Mohseni, Ali T Rezakhani y Daniel A Lidar. "Quantum-process tomography: Resource analysis of different strategies". En: *Physical Review A* 77.3 (2008), pág. 032322.

[327] Nikolaj Moll et al. "Quantum optimization using variational algorithms on near-term quantum devices". En: *Quantum Science and Technology* 3.3 (2018), pág. 030503.

[328] Christopher Monroe y Jungsang Kim. "Scaling the ion trap quantum processor". En: *Science* 339.6124 (2013), págs. 1164-1169.

[329] Thomas Monz et al. "Realization of a scalable Shor algorithm". En: *Science* 351.6277 (2016), págs. 1068-1070.

[330] Satoshi Morita e Hidetoshi Nishimori. "Mathematical foundation of quantum annealing". En: *Journal of Mathematical Physics* 49.12 (2008).

[331] W. J. Munro et al. "High-Bandwidth Hybrid Quantum Repeater". En: *Physical Review Letters* 101.4 (jul. de 2008), pág. 040502. doi: 10.1103/physrevlett.101.040502.

[332] W. J. Munro et al. "From quantum multiplexing to high-performance quantum networking". En: *Nature Photonics* 4.11 (ago. de 2010), págs. 792-796. doi: 10.1038/nphoton.2010.213.

[333] W. J. Munro et al. "Quantum communication without the necessity of quantum memories". En: *Nature Photonics* 6.11 (oct. de 2012), págs. 777-781. doi: 10.1038/nphoton.2012.243.

[334] William J. Munro et al. "Inside Quantum Repeaters". En: *IEEE Journal of Selected Topics in Quantum Electronics* 21.3 (mayo de 2015), págs. 78-90. doi: 10.1109/jstqe.2015.2392076.

[335] Sreraman Muralidharan et al. "Ultrafast and Fault-Tolerant Quantum Communication across Long Distances". En: *Physical Review Letters* 112.25 (jun. de 2014), pág. 250501. doi: 10.1103/physrevlett.112.250501.

[336] Sreraman Muralidharan et al. "Optimal architectures for long distance quantum communication". En: *Scientific Reports* 6.1 (feb. de 2016). doi: 10.1038/srep20463.

[337] Sreraman Muralidharan et al. "One-way quantum repeaters with quantum Reed-Solomon codes". En: *Physical Review A* 97.5 (mayo de 2018), pág. 052316. doi: 10.1103/physreva.97.052316.

[338] Peshal Nayak. "A study of technology roadmap for application-specific integrated circuit". Tesis doct. Rice University, 2021.

[339] M. A. Neumark. "On a representation of additive operator set functions". English. En: *C. R. (Dokl.) Acad. Sci. URSS, n. Ser.* 41 (1943), págs. 359-361. issn: 1819-0723.

[340] *New Cambridge Quantum Algorithm Sets a Benchmark in Performance and Effectively Outperforms Existing Methods*. Available online: https://quantumzeitgeist.com/new-cambridge-quantum-algorithm-sets-a-benchmark-in-performance-and-effectively-outperforms-existing-methods/.

[341] C. T. Nguyen et al. "An integrated nanophotonic quantum register based on silicon-vacancy spins in diamond". En: *Physical Review B* 100.16 (oct. de 2019), pág. 165428. doi: 10.1103/physrevb.100.165428.

[342] Thien Nguyen et al. "Extending C++ for Heterogeneous Quantum-Classical Computing". En: *arXiv e-prints*, arXiv:2010.03935 (oct. de 2020), arXiv:2010.03935. arXiv: 2010.03935 [quant-ph].

[343] Naomi H. Nickerson, Ying Li y Simon C. Benjamin. "Topological quantum computing with a very noisy network and local error rates approaching one percent". En: *Nature Communications* 4.1 (abr. de 2013). doi: 10.1038/ncomms2773.

[344] Michael A. Nielsen et al. *Quantum computation and quantum information - 10. ed.* Cambridge University Press, 2010. isbn: 9781107002173.

[345] Kyungjoo Noh, Victor V. Albert y Liang Jiang. "Quantum Capacity Bounds of Gaussian Thermal Loss Channels and Achievable Rates With Gottesman-Kitaev-Preskill Codes". En: *IEEE Transactions on Information Theory* 65.4 (abr. de 2019), págs. 2563-2582. doi: 10.1109/tit.2018.2873764.

[346] Kyungjoo Noh y Christopher Chamberland. "Fault-tolerant bosonic quantum error correction with the surface–Gottesman-Kitaev-Preskill code". En: *Physical Review A* 101.1 (ene. de 2020), pág. 012316. doi: 10.1103/physreva.101.012316.

[347] Jeremy L O'brien. "Optical quantum computing". En: *Science* 318.5856 (2007), págs. 1567-1570.

[348] Bernhard Ömer. "Quantum programming in QCL". Tesis doct. 2000.

[349] Jian-Wei Pan et al. "Entanglement purification for quantum communication". En: *Nature* 410.6832 (abr. de 2001), págs. 1067-1070. doi: 10.1038/35074041.

[350] Jian-Wei Pan et al. "Experimental entanglement purification of arbitrary unknown states". En: *Nature* 423.6938 (mayo de 2003), págs. 417-422. doi: 10.1038/nature01623.

[351] Xiao-Ling Pang et al. "A hybrid quantum memory–enabled network at room temperature". En: *Science Advances* 6.6 (feb. de 2020). doi: 10.1126/sciadv.aax1425.

[352] Mihir Pant et al. "Rate-distance tradeoff and resource costs for all-optical quantum repeaters". En: *Physical Review A* 95.1 (ene. de 2017), pág. 012304. doi: 10.1103/physreva.95.012304.

[353] Mihir Pant et al. "Routing entanglement in the quantum internet". En: *npj Quantum Information* 5.1 (mar. de 2019). doi: 10.1038/s41534-019-0139-x.

[354] Biagio Peccerillo et al. "A survey on hardware accelerators: Taxonomy, trends, challenges, and perspectives". En: *Journal of Systems Architecture* 129 (2022), pág. 102561.

[355] Stefano Pellerano et al. "Cryogenic CMOS for Qubit Control and Readout". En: *2022 IEEE Custom Integrated Circuits Conference (CICC)*. IEEE. 2022, págs. 01-08.

[356] Hannes Pichler et al. "Universal photonic quantum computation via time-delayed feedback". En: *Proceedings of the National Academy of Sciences* 114.43 (oct. de 2017), págs. 11362-11367. doi: 10.1073/pnas.1711003114.

[357] Stefano Pirandola et al. "Fundamental limits of repeaterless quantum communications". En: *Nature Communications* 8.1 (abr. de 2017). doi: 10.1038/ncomms15043.

[358] A Pirker y W Dür. "A quantum network stack and protocols for reliable entanglement-based networks". En: *New Journal of Physics* 21.3 (mar. de 2019), pág. 033003. doi: 10.1088/1367-2630/ab05f7.

[359] A Pirker, J Wallnöfer y W Dür. "Modular architectures for quantum networks". En: *New Journal of Physics* 20.5 (mayo de 2018), pág. 053054. doi: 10.1088/1367-2630/aac2aa.

[360] Stefano Pironio et al. "Device-independent quantum key distribution secure against collective attacks". En: *New Journal of Physics* 11.4 (abr. de 2009), pág. 045021. doi: 10.1088/1367-2630/11/4/045021.

[361] Christophe Piveteau y David Sutter. "Circuit knitting with classical communication". En: *IEEE Transactions on Information Theory* (2023).

[362] M B Plenio, S Virmani y P Papadopoulos. "Operator monotones, the reduction criterion and the relative entropy". En: *Journal of Physics A: Mathematical and General* 33.22 (mayo de 2000), págs. L193-L197. doi: 10.1088/0305-4470/33/22/101.

[363] Y. Polyanski e Y. Wu. *Information Theory: From Coding to Learning*. 1.ª ed. Cambridge University Press, 2023.

[364] M. Pompili et al. "Realization of a multinode quantum network of remote solid-state qubits". En: *Science* 372.6539 (abr. de 2021), págs. 259-264. doi: 10.1126/science.abg1919. url: https://doi.org/10.1126%2Fscience.abg1919.

[365] M. Pompili et al. "Experimental demonstration of entanglement delivery using a quantum network stack". En: *npj Quantum Information* 8.1 (oct. de 2022). doi: 10.1038/s41534-022-00631-2.

[366] Shahrooz Pouryousef et al. "Resource Management in Quantum Virtual Private Networks". En: (mayo de 2023). doi: 10.48550/ARXIV.2305.03231. arXiv: 2305.03231 [quant-ph].

[367] John Preskill. "Quantum computing in the NISQ era and beyond". En: *Quantum* 2 (2018), pág. 79.

[368] Lorenzo M. Procopio et al. "Experimental superposition of orders of quantum gates". En: *Nature Communications* 6.1 (ago. de 2015). doi: 10.1038/ncomms8913.

[369] E. Prugovečki. "Information-theoretical aspects of quantum measurement". En: *International Journal of Theoretical Physics* 16.5 (mayo de 1977), págs. 321-331. doi: 10.1007/bf01807146.

[370] *qscore*. Available online: https://github.com/myQLM/qscore.

[371] N. Quesada et al. "Simulating realistic non-Gaussian state preparation". En: *Physical Review A* 100.2 (ago. de 2019), pág. 022341. doi: 10.1103/physreva.100.022341.

[372] J Rahamim et al. "Double-sided coaxial circuit QED with out-of-plane wiring". En: *Applied Physics Letters* 110.22 (2017).

[373] Matthew T. Rakher et al. "Quantum transduction of telecommunications-band single photons from a quantum dot by frequency upconversion". En: *Nature Photonics* 4.11 (oct. de 2010), págs. 786-791. doi: 10.1038/nphoton.2010.221.

[374] T. C. Ralph, A. J. F. Hayes y Alexei Gilchrist. "Loss-Tolerant Optical Qubits". En: *Physical Review Letters* 95.10 (ago. de 2005), pág. 100501. doi: 10.1103/physrevlett.95.100501.

[375] S. Ramelow et al. "Polarization-entanglement-conserving frequency conversion of photons". En: *Physical Review A* 85.1 (ene. de 2012), pág. 013845. doi: 10.1103/physreva.85.013845.

[376] Robert Raussendorf y Hans J. Briegel. "A One-Way Quantum Computer". En: *Physical Review Letters* 86.22 (mayo de 2001), págs. 5188-5191. doi: 10.1103/physrevlett.86.5188.

[377] R. Reichle et al. "Experimental purification of two-atom entanglement". En: *Nature* 443.7113 (oct. de 2006), págs. 838-841. doi: 10.1038/nature05146.

[378] Andreas Reiserer y Gerhard Rempe. "Cavity-based quantum networks with single atoms and optical photons". En: *Reviews of Modern Physics* 87.4 (dic. de 2015), págs. 1379-1418. doi: 10.1103/revmodphys.87.1379.

[379] Daniel Riedel et al. "Deterministic Enhancement of Coherent Photon Generation from a Nitrogen-Vacancy Center in Ultrapure Diamond". En: *Physical Review X* 7.3 (sep. de 2017), pág. 031040. doi: 10.1103/physrevx.7.031040.

[380] H. de Riedmatten et al. "Long Distance Quantum Teleportation in a Quantum Relay Configuration". En: *Physical Review Letters* 92.4 (ene. de 2004), pág. 047904. doi: 10.1103/physrevlett.92.047904.

[381] Eleanor Rieffel y Wolfgang Polak. "An introduction to quantum computing for non-physicists". En: *ACM Computing Surveys* 32.3 (sep. de 2000), págs. 300-335. doi: 10.1145/367701.367709.

[382] Eleanor G. Rieffel y Wolfgang H. Polak. *Quantum Computing A Gentle Introduction. A Gentle Introduction*. The MIT Press, pág. 388. isbn: 9780262526678.

[383] F. Riera-Sàbat et al. "Entanglement-Assisted Entanglement Purification". En: *Physical Review Letters* 127.4 (jul. de 2021), pág. 040502. doi: 10.1103/physrevlett.127.040502.

[384] Santiago Rodrigo et al. "Modelling Short-range Quantum Teleportation for Scalable Multi-Core Quantum Computing Architectures". En: *Proceedings of the Eight Annual ACM International Conference on Nanoscale Computing and Communication*. ACM, sep. de 2021. doi: 10.1145/3477206.3477461.

[385] Joschka Roffe. "Quantum error correction: an introductory guide". En: *Contemporary Physics* 60.3 (jul. de 2019), págs. 226-245. doi: 10.1080/00107514.2019.1667078.

[386] Joschka Roffe. "Quantum error correction: an introductory guide". En: *Contemporary Physics* 60.3 (2019), págs. 226-245.

[387] Ch Roos et al. "Quantum state engineering on an optical transition and decoherence in a Paul trap". En: *Physical Review Letters* 83.23 (1999), pág. 4713.

[388] Charles Roques-Carmes et al. "Biasing the quantum vacuum to control macroscopic probability distributions". En: *Science* 381.6654 (2023), págs. 205-209.

[389] Matteo Rosati, Andrea Mari y Vittorio Giovannetti. "Narrow bounds for the quantum capacity of thermal attenuators". En: *Nature Communications* 9.1 (oct. de 2018). doi: 10.1038/s41467-018-06848-0.

[390] Filip Rozpędek et al. "Quantum repeaters based on concatenated bosonic and discrete-variable quantum codes". En: *npj Quantum Information* 7.1 (jun. de 2021). doi: 10.1038/s41534-021-00438-7.

[391] Giulia Rubino et al. "Experimental quantum communication enhancement by superposing trajectories". En: *Physical Review Research* 3.1 (ene. de 2021), pág. 013093. doi: 10.1103/physrevresearch.3.013093.

[392] Maximilian Ruf et al. "Quantum networks based on color centers in diamond". En: *Journal of Applied Physics* 130.7 (ago. de 2021), pág. 070901. doi: 10.1063/5.0056534.

[393] Antonio Russo, Edwin Barnes y Sophia E Economou. "Generation of arbitrary all-photonic graph states from quantum emitters". En: *New Journal of Physics* 21.5 (mayo de 2019), pág. 055002. doi: 10.1088/1367-2630/ab193d.

[394] Krishna Kumar Sabapathy et al. "Production of photonic universal quantum gates enhanced by machine learning". En: *Physical Review A* 100.1 (jul. de 2019), pág. 012326. doi: 10.1103/physreva.100.012326.

[395] Louis Salvail et al. "Security of trusted repeater quantum key distribution networks". En: *Journal of Computer Security* 18.1 (ene. de 2010). Ed. por Jan Camenisch et al., págs. 61-87. doi: 10.3233/jcs-2010-0373.

[396] Nicolas Sangouard et al. "Quantum repeaters based on atomic ensembles and linear optics". En: *Reviews of Modern Physics* 83.1 (mar. de 2011), págs. 33-80. doi: 10.1103/revmodphys.83.33.

[397] Sk Sazim et al. "Classical communication with indefinite causal order for completely depolarizing channels". En: *Physical Review A* 103.6 (jun. de 2021), pág. 062610. doi: 10.1103/physreva.103.062610.

[398] J. R. Schaibley et al. "Demonstration of Quantum Entanglement between a Single Electron Spin Confined to an InAs Quantum Dot and a Photon". En: *Physical Review Letters* 110.16 (abr. de 2013), pág. 167401. doi: 10.1103/physrevlett.110.167401.

[399] Philipp Schindler et al. "A quantum information processor with trapped ions". En: *New Journal of Physics* 15.12 (2013), pág. 123012.

[400] C. Schön et al. "Sequential Generation of Entangled Multiqubit States". En: *Physical Review Letters* 95.11 (sep. de 2005), pág. 110503. doi: 10.1103/physrevlett.95.110503.

[401] Benjamin Schumacher. "Sending entanglement through noisy quantum channels". En: *Physical Review A* 54.4 (oct. de 1996), págs. 2614-2628. doi: 10.1103/physreva.54.2614.

[402] Benjamin Schumacher y M. A. Nielsen. "Quantum data processing and error correction". En: *Physical Review A* 54.4 (oct. de 1996), págs. 2629-2635. doi: 10.1103/physreva.54.2629.

[403] Benjamin Schumacher y Michael D. Westmoreland. "Sending classical information via noisy quantum channels". En: *Physical Review A* 56.1 (jul. de 1997), págs. 131-138. doi: 10.1103/physreva.56.131.

[404] I. Schwartz et al. "Deterministic generation of a cluster state of entangled photons". En: *Science* 354.6311 (sep. de 2016), págs. 434-437. doi: 10.1126/science.aah4758.

[405] Pascale Senellart, Glenn Solomon y Andrew White. "High-performance semiconductor quantum-dot single-photon sources". En: *Nature Nanotechnology* 12.11 (nov. de 2017), págs. 1026-1039. doi: 10.1038/nnano.2017.218.

[406] R. Shaham, O. Katz y O. Firstenberg. "Strong coupling of alkali-metal spins to noble-gas spins with an hour-long coherence time". En: *Nature Physics* 18.5 (abr. de 2022), págs. 506-510. doi: 10.1038/s41567-022-01535-w.

[407] Rui-Ting Shan, Xiubo Chen y Kai-Guo Yuan. "Multi-party blind quantum computation protocol with mutual authentication in network". En: *Science China Information Sciences* 64.6 (abr. de 2021). doi: 10.1007/s11432-020-2977-x.

[408] Yu-Bo Sheng y Lan Zhou. "Blind quantum computation with a noise channel". En: *Physical Review A* 98.5 (nov. de 2018), pág. 052343. doi: 10.1103/physreva.98.052343.

[409] Shouqian Shi y Chen Qian. "Concurrent Entanglement Routing for Quantum Networks". En: *Proceedings of the Annual conference of the ACM Special Interest Group on Data Communication on the applications, technologies, architectures, and protocols for computer communication*. ACM, jul. de 2020. doi: 10.1145/3387514.3405853.

[410] Peter W. Shor. "Additivity of the classical capacity of entanglement-breaking quantum channels". En: *Journal of Mathematical Physics* 43.9 (ago. de 2002), págs. 4334-4340. doi: 10.1063/1.1498000.

[411] Peter W. Shor. "Capacities of quantum channels and how to find them". En: *Mathematical Programming* 97.1 (jul. de 2003), págs. 311-335. doi: 10.1007/s10107-003-0446-y.

[412] Peter W. Shor. "Equivalence of Additivity Questions in Quantum Information Theory". En: *Communications in Mathematical Physics* 246.3 (abr. de 2004), págs. 453-472. doi: 10.1007/s00220-003-0981-7.

[413] C. Simon et al. "Quantum memories". En: *The European Physical Journal D* 58.1 (abr. de 2010), págs. 1-22. doi: 10.1140/epjd/e2010-00103-y.

[414] Neil Sinclair et al. "Spectral Multiplexing for Scalable Quantum Photonics using an Atomic Frequency Comb Quantum Memory and Feed-Forward Control". En: *Physical Review Letters* 113.5 (jul. de 2014), pág. 053603. doi: 10.1103/physrevlett.113.053603.

[415] Amoldeep Singh et al. "Quantum Internet—Applications, Functionalities, Enabling Technologies, Challenges, and Research Directions". En: *IEEE Communications Surveys & Tutorials* 23.4 (2021), págs. 2218-2247. doi: 10.1109/COMST.2021.3109944.

[416] Seyon Sivarajah et al. "t| ket>: a retargetable compiler for NISQ devices". En: *Quantum Science and Technology* 6.1 (2020), pág. 014003.

[417] Luka Skoric et al. "Parallel window decoding enables scalable fault tolerant quantum computation". En: *arXiv preprint arXiv:2209.08552* (2022).

[418] L. Slodička et al. "Atom-Atom Entanglement by Single-Photon Detection". En: *Physical Review Letters* 110.8 (feb. de 2013), pág. 083603. doi: 10.1103/physrevlett.110.083603.

[419] Graeme Smith y John A. Smolin. "Additive extensions of a quantum channel". En: *2008 IEEE Information Theory Workshop*. IEEE, mayo de 2008. doi: 10.1109/itw.2008.4578688.

[420] Graeme Smith y John A. Smolin. "Extensive Nonadditivity of Privacy". En: *Physical Review Letters* 103.12 (sep. de 2009), pág. 120503. doi: 10.1103/physrevlett.103.120503.

[421] Graeme Smith, John A. Smolin y Jon Yard. "Quantum communication with Gaussian channels of zero quantum capacity". En: *Nature Photonics* 5.10 (ago. de 2011), págs. 624-627. doi: 10.1038/nphoton.2011.203.

[422] Graeme Smith y Jon Yard. "Quantum Communication with Zero-Capacity Channels". En: *Science* 321.5897 (sep. de 2008), págs. 1812-1815. doi: 10.1126/science.1162242.

[423] Robert S Smith, Michael J Curtis y William J Zeng. "A practical quantum instruction set architecture". En: *arXiv preprint arXiv:1608.03355* (2016).

[424] N. Somaschi et al. "Near-optimal single-photon sources in the solid state". En: *Nature Photonics* 10.5 (mar. de 2016), págs. 340-345. doi: 10.1038/nphoton.2016.23.

[425] Rolando D Somma, Daniel Nagaj y Mária Kieferová. "Quantum speedup by quantum annealing". En: *Physical review letters* 109.5 (2012), pág. 050501.

[426] Thomas M. Stace, Sean D. Barrett y Andrew C. Doherty. "Thresholds for Topological Codes in the Presence of Loss". En: *Physical Review Letters* 102.20 (mayo de 2009), pág. 200501. doi: 10.1103/physrevlett.102.200501.

[427] Damian S Steiger, Thomas Häner y Matthias Troyer. "ProjectQ: an open source software framework for quantum computing". En: *Quantum* 2 (2018), pág. 49.

[428] L. J. Stephenson et al. "High-Rate, High-Fidelity Entanglement of Qubits Across an Elementary Quantum Network". En: *Physical Review Letters* 124.11 (mar. de 2020), pág. 110501. doi: 10.1103/physrevlett.124.110501.

[429] E. A. Stinaff et al. "Optical Signatures of Coupled Quantum Dots". En: *Science* 311.5761 (feb. de 2006), págs. 636-639. doi: 10.1126/science.1121189.

[430] W. Forrest Stinespring. "Positive Functions on C $*$ -Algebras". En: *Proceedings of the American Mathematical Society* 6.2 (abr. de 1955), pág. 211. doi: 10.2307/2032342.

[431] R. Stockill et al. "Phase-Tuned Entangled State Generation between Distant Spin Qubits". En: *Physical Review Letters* 119.1 (jul. de 2017), pág. 010503. doi: 10.1103/physrevlett.119.010503.

[432] Daiqin Su, Casey R. Myers y Krishna Kumar Sabapathy. "Conversion of Gaussian states to non-Gaussian states using photon-number-resolving detectors". En: *Physical Review A* 100.5 (nov. de 2019), pág. 052301. doi: 10.1103/physreva.100.052301.

[433] "Suppressing quantum errors by scaling a surface code logical qubit". En: *Nature* 614.7949 (2023), págs. 676-681.

[434] David Sutter et al. "Approximate Degradable Quantum Channels". En: *IEEE Transactions on Information Theory* 63.12 (dic. de 2017), págs. 7832-7844. doi: 10.1109/tit.2017.2754268.

[435] T. H. Taminiau et al. "Detection and Control of Individual Nuclear Spins Using a Weakly Coupled Electron Spin". En: *Physical Review Letters* 109.13 (sep. de 2012), pág. 137602. doi: 10.1103/physrevlett.109.137602.

[436] T. R. Tan et al. "Multi-element logic gates for trapped-ion qubits". En: *Nature* 528.7582 (dic. de 2015), págs. 380-383. doi: 10.1038/nature16186.

[437] Seiichiro Tani, Hirotada Kobayashi y Keiji Matsumoto. "Exact Quantum Algorithms for the Leader Election Problem". En: *Lecture Notes in Computer Science* 3404 (ene. de 2008). doi: 10.1145/2141938.2141939.

[438] S. Tanzilli et al. "A photonic quantum information interface". En: *Nature* 437.7055 (sep. de 2005), págs. 116-120. doi: 10.1038/nature04009.

[439] Anna Tchebotareva et al. "Entanglement between a Diamond Spin Qubit and a Photonic Time-Bin Qubit at Telecom Wavelength". En: *Physical Review Letters* 123.6 (ago. de 2019), pág. 063601. doi: 10.1103/physrevlett.123.063601.

[440] Barbara M Terhal. "Quantum error correction for quantum memories". En: *Reviews of Modern Physics* 87.2 (2015), pág. 307.

[441] Philip Thomas et al. "Efficient generation of entangled multiphoton graph states from a single atom". En: *Nature* 608.7924 (ago. de 2022), págs. 677-681. doi: 10.1038/s41586-022-04987-5.

[442] Joseph Tindall et al. "Efficient tensor network simulation of IBM's kicked Ising experiment". En: *arXiv preprint arXiv:2306.14887* (2023).

[443] E. Togan et al. "Quantum entanglement between an optical photon and a solid-state spin qubit". En: *Nature* 466.7307 (ago. de 2010), págs. 730-734. doi: 10.1038/nature09256.

[444] Marco Tomamichel, Mark M. Wilde y Andreas Winter. "Strong Converse Rates for Quantum Communication". En: *IEEE Transactions on Information Theory* 63.1 (ene. de 2017), págs. 715-727. doi: 10.1109/tit.2016.2615847.

[445] Natasha Tomm et al. "A bright and fast source of coherent single photons". En: *Nature Nanotechnology* 16.4 (ene. de 2021), págs. 399-403. doi: 10.1038/s41565-020-00831-x.

[446] Giacomo Torlai et al. "Neural-network quantum state tomography". En: *Nature Physics* 14.5 (2018), págs. 447-450.

[447] Ilan Tzitrin et al. "Progress towards practical qubit computation using approximate Gottesman-Kitaev-Preskill codes". En: *Physical Review A* 101.3 (mar. de 2020), pág. 032315. doi: 10.1103/physreva.101.032315.

[448] Ilan Tzitrin et al. "Fault-Tolerant Quantum Computation with Static Linear Optics". En: *PRX Quantum* 2.4 (dic. de 2021), pág. 040353. doi: 10.1103/prxquantum.2.040353.

[449] Muhammad Asad Ullah et al. "On the Robustness of Quantum Algorithms for Blockchain Consensus". En: *Sensors* 22.7 (abr. de 2022), pág. 2716. doi: 10.3390/s22072716.

[450] William G Unruh. "Maintaining coherence in quantum computers". En: *Physical Review A* 51.2 (1995), pág. 992.

[451] Ravitej Uppu et al. "Scalable integrated single-photon source". En: *Science Advances* 6.50 (dic. de 2020). doi: 10.1126/sciadv.abc8268.

[452] Ewout Van Den Berg et al. "Probabilistic error cancellation with sparse Pauli–Lindblad models on noisy quantum processors". En: *Nature Physics* (2023), págs. 1-6.

[453] Wim Vanhaverbeke, Geert Duysters y Niels Noorderhaven. "External technology sourcing through alliances or acquisitions: An analysis of the application-specific integrated circuits industry". En: *Organization Science* 13.6 (2002), págs. 714-733.

[454] Michael Varnava, Daniel E Browne y Terry Rudolph. "Loss tolerant linear optical quantum memory by measurement-based quantum computing". En: *New Journal of Physics* 9.6 (jun. de 2007), págs. 203-203. doi: 10.1088/1367-2630/9/6/203.

[455] Michael Varnava, Daniel E. Browne y Terry Rudolph. "Loss Tolerance in One-Way Quantum Computation via Counterfactual Error Correction". En: *Physical Review Letters* 97.12 (sep. de 2006), pág. 120501. doi: 10.1103/physrevlett.97.120501.

[456] Michael Varnava, Daniel E. Browne y Terry Rudolph. "How Good Must Single Photon Sources and Detectors Be for Efficient Linear Optical Quantum Computation?" En: *Physical Review Letters* 100.6 (feb. de 2008), pág. 060502. doi: 10.1103/physrevlett.100.060502.

[457] Rui Vasconcelos et al. "Scalable spin–photon entanglement by time-to-polarization conversion". En: *npj Quantum Information* 6.1 (ene. de 2020). doi: 10.1038/s41534-019-0236-x.

[458] Andrew Wack et al. "Quality, speed, and scale: three key attributes to measure the performance of near-term quantum computers". En: *arXiv preprint arXiv:2110.14108* (2021).

[459] Edo Waks, Assaf Zeevi y Yoshihisa Yamamoto. "Security of quantum key distribution with entangled photons against individual attacks". En: *Physical Review A* 65.5 (abr. de 2002), pág. 052310. doi: 10.1103/physreva.65.052310.

[460] G. Waldherr et al. "Quantum error correction in a solid-state hybrid spin register". En: *Nature* 506.7487 (feb. de 2014), págs. 204-207. doi: 10.1038/nature12919.

[461] Hui Wang et al. "Towards optimal single-photon sources from polarized microcavities". En: *Nature Photonics* 13.11 (ago. de 2019), págs. 770-775. doi: 10.1038/s41566-019-0494-3.

[462] Junchao Wang, Guoping Guo y Zheng Shan. "Sok: Benchmarking the performance of a quantum computer". En: *Entropy* 24.10 (2022), pág. 1467.

[463] Ping Wang et al. "Consensus algorithm based on verifiable quantum random numbers". En: *International Journal of Intelligent Systems* 37.10 (mar. de 2022), págs. 6857-6876. doi: 10.1002/int.22865.

[464] Xin Wang, Wei Xie y Runyao Duan. "Semidefinite programming converse bounds for classical communication over quantum channels". En: *2017 IEEE International Symposium on Information Theory (ISIT)*. IEEE, jun. de 2017. doi: 10.1109/isit.2017.8006825.

[465] Yu Wang et al. "Verifiable Multi-Dimensional (t,n) Threshold Quantum Secret Sharing Based on Quantum Walk". En: *International Journal of Theoretical Physics* 61 (feb. de 2022). doi: 10.1007/s10773-022-05009-w.

[466] Yuchen Wang et al. "Qudits and high-dimensional quantum computing". En: *Frontiers in Physics* 8 (2020), pág. 589504.

[467] Zhaoying Wang et al. "An Asynchronous Entanglement Distribution Protocol for Quantum Networks". En: *IEEE Network* 36.5 (2022), págs. 40-47. doi: 10.1109/MNET.001.2200177.

[468] John Watrous. *Theory of Quantum Information*. Cambridge University Press, 2018. isbn: 9781316848142.

[469] Christian Weedbrook et al. "Gaussian quantum information". En: *Reviews of Modern Physics* 84.2 (mayo de 2012), págs. 621-669. doi: 10.1103/revmodphys.84.621.

[470] Stephanie Wehner, David Elkouss y Ronald Hanson. "Quantum internet: A vision for the road ahead". En: *Science* 362.6412 (oct. de 2018). doi: 10.1126/science.aam9288.

[471] Johannes Weidenfeller et al. "Scaling of the quantum approximate optimization algorithm on superconducting qubit based hardware". En: *Quantum* 6 (2022), pág. 870.

[472] R F Werner. "All teleportation and dense coding schemes". En: *Journal of Physics A: Mathematical and General* 34.35 (ago. de 2001), págs. 7081-7094. doi: 10.1088/0305-4470/34/35/332.

[473] John van de Wetering. *ZX-calculus for the working quantum computer scientist*. 2020. arXiv: 2012.13966 [quant-ph].

[474] Mark M. Wilde. *Quantum Information Theory*. University of Cambridge ESOL Examinations, 2017, pág. 776. isbn: 9781107176164.

[475] A. Winter. "Coding theorem and strong converse for quantum channels". En: *IEEE Transactions on Information Theory* 45.7 (1999), págs. 2481-2485. doi: 10.1109/18.796385.

[476] Michael M. Wolf y David Pérez-García. "Quantum capacities of channels with small environment". En: *Physical Review A* 75.1 (ene. de 2007), pág. 012303. doi: 10.1103/physreva.75.012303.

[477] W. K. Wootters y W. H. Zurek. "A single quantum cannot be cloned". En: *Nature* 299.5886 (oct. de 1982), págs. 802-803. doi: 10.1038/299802a0.

[478] William K. Wootters. "Entanglement of Formation of an Arbitrary State of Two Qubits". En: *Physical Review Letters* 80.10 (mar. de 1998), págs. 2245-2248. doi: 10.1103/physrevlett.80.2245.

[479] Kenneth Wright et al. "Benchmarking an 11-qubit quantum computer". En: *Nature communications* 10.1 (2019), pág. 5464.

[480] Jonathan Wurtz et al. "Aquila: QuEra's 256-qubit neutral-atom quantum computer". En: *arXiv preprint arXiv:2306.11727* (2023).

[481] Feihu Xu et al. "Measurement-Device-Independent Quantum Cryptography". En: *IEEE Journal of Selected Topics in Quantum Electronics* 21.3 (mayo de 2015), págs. 148-158. doi: 10.1109/jstqe.2014.2381460.

[482] Takashi Yamamoto, Masato Koashi y Nobuyuki Imoto. "Concentration and purification scheme for two partially entangled photon pairs". En: *Physical Review A* 64.1 (jun. de 2001), pág. 012304. doi: 10.1103/physreva.64.012304.

[483] Hayata Yamasaki et al. "Multipartite entanglement outperforming bipartite entanglement under limited quantum system sizes". En: *Physical Review A* 98.5 (nov. de 2018), pág. 052313. doi: 10.1103/physreva.98.052313.

[484] Sheng-Jun Yang et al. "An efficient quantum light–matter interface with sub-second lifetime". En: *Nature Photonics* 10.6 (abr. de 2016), págs. 381-384. doi: 10.1038/nphoton.2016.51.

[485] Yong Yu et al. "Entanglement of two quantum memories via fibres over dozens of kilometres". En: *Nature* 578.7794 (feb. de 2020), págs. 240-245. doi: 10.1038/s41586-020-1976-7.

[486] Ziang Yu y Yingzhou Li. "Analysis of Error Propagation in Quantum Computers". En: (sep. de 2022). doi: 10.48550/ARXIV.2209.01699. arXiv: 2209.01699 [quant-ph].

[487] Hussain A. Zaidi et al. "Near-deterministic creation of universal cluster states with probabilistic Bell measurements and three-qubit resource states". En: *Physical Review A* 91.4 (abr. de 2015), pág. 042301. doi: 10.1103/physreva.91.042301.

[488] Syed Mohammad Hassan Zaidi et al. "Quantum Internet: A Revolutionary Disruption". En: *2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*. IEEE, dic. de 2022. doi: 10.1109/honet56683.2022.10018973.

[489] Sebastian Zaske et al. "Visible-to-Telecom Quantum Frequency Conversion of Light from a Single Quantum Emitter". En: *Physical Review Letters* 109.14 (oct. de 2012), pág. 147404. doi: 10.1103/physrevlett.109.147404.

[490] Yiming Zeng et al. "Entanglement Routing Design Over Quantum Networks". En: *IEEE/ACM Transactions on Networking* (2023), págs. 1-16. doi: 10.1109/tnet.2023.3282560.

[491] Yuan Zhan y Shuo Sun. "Deterministic Generation of Loss-Tolerant Photonic Cluster States with a Single Quantum Emitter". En: *Physical Review Letters* 125.22 (nov. de 2020), pág. 223601. doi: 10.1103/physrevlett.125.223601.

[492] Bingzhi Zhang et al. "Hybrid Entanglement Distribution between Remote Microwave Quantum Computers Empowered by Machine Learning". En: *Phys. Rev. Appl.* 18 (6 dic. de 2022), pág. 064016. doi: 10.1103/PhysRevApplied.18.064016. url: https://link.aps.org/doi/10.1103/PhysRevApplied.18.064016.

[493] Ling Zhang y Qin Liu. "Concurrent multipath quantum entanglement routing based on segment routing in quantum hybrid networks". En: *Quantum Information Processing* 22.3 (mar. de 2023). doi: 10.1007/s11128-023-03891-9.

[494] Peiying Zhang et al. "Future Quantum Communications and Networking: A Review and Vision". En: *IEEE Wireless Communications* (2022), págs. 1-8. doi: 10.1109/mwc.012.2200295.

[495] Qiang Zhang et al. "Demonstration of a scheme for the generation of "event-ready" entangled photon pairs from a single-photon source". En: *Physical Review A* 77.6 (jun. de 2008), pág. 062316. doi: 10.1103/physreva.77.062316.

[496] Rui Zhang et al. "Loss-tolerant all-photonic quantum repeater with generalized Shor code". En: *Optica* 9.2 (feb. de 2022), pág. 152. doi: 10.1364/optica.439170.

[497] Yangming Zhao y Chunming Qiao. "Distributed Transport Protocols for Quantum Data Networks". En: *IEEE/ACM Transactions on Networking* (2023), págs. 1-16. doi: 10.1109/TNET.2023.3262547.

[498] Yangming Zhao, Gongming Zhao y Chunming Qiao. "E2E Fidelity Aware Routing and Purification for Throughput Maximization in Quantum Networks". En: *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*. 2022, págs. 480-489. doi: 10.1109/INFOCOM48880.2022.9796814.

[499] Han-Sen Zhong et al. "12-Photon Entanglement and Scalable Scattershot Boson Sampling with Optimal Entangled-Photon Pairs from Parametric Down-Conversion". En: *Physical Review Letters* 121.25 (dic. de 2018), pág. 250505. doi: 10.1103/physrevlett.121.250505.

[500] Manjin Zhong et al. "Optically addressable nuclear spins in a solid with a six-hour coherence time". En: *Nature* 517.7533 (ene. de 2015), págs. 177-180. doi: 10.1038/nature14025.

[501] M. Zwerger et al. "Long-Range Big Quantum-Data Transmission". En: *Physical Review Letters* 120.3 (ene. de 2018), pág. 030503. doi: 10.1103/physrevlett.120.030503.

[502] Karol Życzkowski et al. "Volume of the set of separable states". En: *Physical Review A* 58.2 (ago. de 1998), págs. 883-892. doi: 10.1103/physreva.58.883.

A. Estados cuánticos, qubits, medidas y canales

En este apéndice se resumen los conceptos básicos y necesarios de la información cuántica, y se introduce la notación habitual de la disciplina. Los textos [344, 474, 468, 230] son excelentes como referencia o complemento de este breve repaso. Un *qubit* ---la versión en la mecánica cuántica de un bit clásico y la unidad de medida de la información cuántica--- es un espacio de Hilbert de dos dimensiones. Los vectores en este espacio se representan convencionalmente con la *notación bra-ket*, o notación de Dirac, en la que $|\psi\rangle$ representa un vector columna y $\langle\psi| := |\psi\rangle^\dagger$ es el vector traspuesto conjugado (†) de $|\psi\rangle$.[18] Un qubit, por tanto, es un objeto matemático que representa el estado de un sistema cuántico. Se materializa experimentalmente asociándolo a un espacio bidimensional de algún sistema físico de dos niveles, por ejemplo el espín de un electrón, la polarización de un fotón, o un átomo con un estado de energía base y un estado excitado.

El estado de un qubit se puede expresar en general como una combinación lineal (una *superposición*) de dos estados base computacionales $|0\rangle$ y $|1\rangle$, en la forma $a|0\rangle + b|1\rangle$, con $a, b \in \mathbb{C}$ y $|a|^2 + |b|^2 = 1$. Un *estado puro* es aquel que se puede escribir como $|u\rangle$, con $u \in \mathbb{C}^2$ un vector unitario. Una combinación de estados puros es un estado mixto, y su descripción general (que incluye a la de los estados puros) es mediante un *operador de densidad* $\rho = |\psi\rangle\langle\psi|$ para el estado $|\psi\rangle$. El operador ρ es positivo y tiene traza 1; el estado es puro cuando el rango de ρ es uno o, de manera equivalente, cuando $\mathrm{tr}(\rho^2) = 1$; y es mixto si $\mathrm{tr}(\rho^2) < 1$.[19] Evidentemente, $\mathbb{C}^2$ tiene

[18] Una de las ventajas formales de la notación bra-ket es que el producto interno de dos vectores se escribe directamente como $\langle\rho|\phi\rangle$ y el producto externo como $|\rho\rangle\langle\phi|$.

[19] La condición $\mathrm{tr}(\rho^2) = 1$ equivale a $\rho^2 = \rho$, que es lo mismo que afirmar que ρ es una proyección.

Tabla 13: Lista de algunas de las puertas cuánticas más frecuentes. La doble línea horizontal separa la puertas Clifford (antes) y las no-Clifford (después).

Puerta cuántica	Operador	Operación
Identidad	I	No modifica el estadio cuántico
Pauli X	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	Bit-flip
Pauli Y	$Y = \begin{pmatrix} 0 & -\imath \\ \imath & 0 \end{pmatrix}$	bit-flip + cambio de fase
Pauli Z	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	Cambio de fase
Raíz cuadrada	$\mathsf{SX} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1+\imath & 1-\imath \\ 1-\imath & 1+\imath \end{pmatrix}$	$X = \mathsf{SX} \circ \mathsf{SX}$
Hadamard	$\mathsf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}$	Convierte un elemento de la base computacional en una superposición de los dos elementos
S	$\mathsf{S} = \begin{pmatrix} 1 & 0 \\ 0 & \imath \end{pmatrix}$	Cambio de fase en $\pi/2$
Cambio de fase	$\mathsf{P}_\theta = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\imath\theta} \end{pmatrix}$	Cambio de fase en θ
Rotación-x	$\mathsf{R}_x(\theta) = \mathrm{e}^{-\imath\theta/2X} = \cos\frac{\theta}{2} I - \imath \sin\frac{\theta}{2} X$	Rotación en θ sobre el eje x de la esfera de Bloch
Rotación-y	$\mathsf{R}_y(\theta) = \mathrm{e}^{-\imath\theta/2Y} = \cos\frac{\theta}{2} I - \imath \sin\frac{\theta}{2} Y$	Rotación en θ sobre el eje y de la esfera de Bloch
Rotación-z	$\mathsf{R}_z(\theta) = \mathrm{e}^{-\imath\theta/2Z} = \cos\frac{\theta}{2} I - \imath \sin\frac{\theta}{2} Z$	Rotación en θ sobre el eje z de la esfera de Bloch
CNOT	$\mathsf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	Invierte el segundo qubit de entrada cuando el primero es $\lvert 1\rangle$
Toffoli	$\mathsf{CCNOT} = \begin{pmatrix} I_6 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & 0 & 1 \\ \mathbf{0} & 1 & 0 \end{pmatrix}$	Controlled CNOT

múltiples bases además de la base computacional $\{|0\rangle, |1\rangle\}$, por ejemplo la base conjugada

$$|\pm\rangle := \frac{1}{\sqrt{2}}\big(|0\rangle \pm |1\rangle\big).$$

Una *transformación unitaria* U ---operadores U que cumplen $U^\dagger U = \mathbb{1}$--- describe operaciones reversibles sobre qubits que preservan las probabilidades: se la denomina *puerta cuántica*.[20] Un ejemplo importante son las puertas u *operadores de Pauli*, que se definen por

$$X = |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$Y = -\imath|0\rangle\langle 1| + \imath|1\rangle\langle 0| = \begin{pmatrix} 0 & -\imath \\ \imath & 0 \end{pmatrix},$$
$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

y se corresponden con una inversión de fase (Z), una inversión de bit (X) y una combinación de ambas sobre un qubit (Y). Una transformación unitaria U es *Clifford* si convierte cualquier operador de Pauli en otro bajo conjugación, es decir, si $UPU^\dagger$ es un operador de Pauli, donde $P = \{\mathbb{1}, X, Y, Z\}$. Un ejemplo de una puerta cuántica que es Clifford pero no Pauli es la *puerta de*

[20] No todas las puertas cuánticas son transformaciones unitarias, sin embargo. Véase más adelante en este apartado.

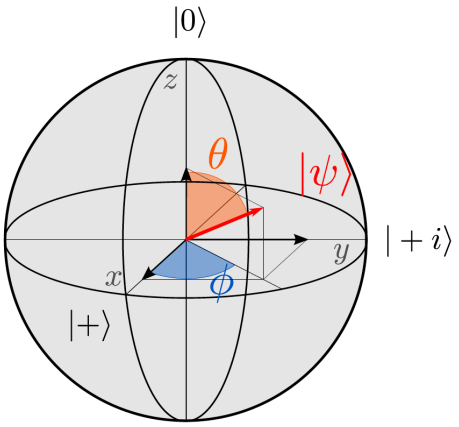


Figura 74: La representación de un qubit en la esfera de Bloch. Un vector de estado $|\psi\rangle$ se puede escribir como $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{\iota\phi}\sin\frac{\theta}{2}|1\rangle$. Imagen tomada de [22].

Hadamard

$$\mathsf{H} = \frac{1}{\sqrt{2}}\big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\big).$$

La puerta T de cambio de fase

$$\mathsf{T} = \mathsf{P}_{\pi/4} = |0\rangle\langle 0| + e^{\iota\frac{\pi}{4}}|1\rangle\langle 1| \tag{8}$$

no es Clifford. La Tabla 13 enumera una lista de las puertas cuánticas más comunes empleadas para construir circuitos cuánticos (Apéndice B).

Puesto que los operadores de Pauli son ortogonales entre sí, cualquier qubit ρ se puede representar como

$$\rho = \frac{1}{2}\big(\mathbb{1} + aX + bY + cZ\big) \tag{9}$$

donde a, b, c son números reales no negativos tales que $a^2 + b^2 + c^2 \leq 1$. Es inmediato comprobar que los coeficientes a, b, c son las proyecciones de ρ sobre cada uno de los operadores de Pauli (e.g., $\mathrm{tr}(X^\dagger\rho) = a$) y que un estado es puro si y solo si $a^2 + b^2 + c^2 = 1$, y es mixto en otro caso. La expresión (9) sugiere la representación gráfica denominada *esfera de Bloch*, en la que el estado de un qubit se representa mediante las coordenadas (a, b, c): son estados puros todos los de la superficie de la esfera y mixtos los del interior, véase la Figura 74.

En la descripción formal de un estado cuántico no hay nada especial en suponer que la dimensión del espacio es 2, de modo que todo el desarrollo se puede generalizar para cualquier dimensión d y para cualquier número de qubits. Así, un operador ρ positivo con traza unidad definido sobre un espacio de Hilbert de dimensión d se denomina *qudit* ---algunos textos utilizan el término *qutrit* específicamente cuando $d = 3$---. Y un conjunto de n qudits (qubits cuando $d = 2$) se puede describir mediante un operador ρ positivo definido en el espacio $\mathbb{C}^{nd} = \mathbb{C}^d \otimes \cdots \otimes \mathbb{C}^d$ (n veces), en donde $\otimes$ denota el producto tensor de dos espacios. Un *estado producto* es aquel que se puede expresar como producto de subestados independientes $\rho = \rho_1 \otimes \cdots \otimes \rho_n$, con $\rho_i \in L(\mathbb{C}^{d_i})$ para $i = 1, \ldots, n$.

Un ejemplo frecuente de estado producto es un *estado clásico-cuántico* (cq)

$$\sum_{i\in I} p(i)|i\rangle\langle i| \otimes \rho_i,$$

en el cual $\{\rho_i : i \in I\}$ es una colección de estados cuánticos en el espacio $\mathscr{X}$, $\{p(i) : i \in I\}$ es una distribución de probabilidades, I es un conjunto índice y los estados $\{|i\rangle : i \in I\}$ son una base computacional en $\mathbb{C}^{|I|}$. Esta expresión debe entenderse como sigue: el sistema se compone de dos registros, uno clásico con el conjunto de estados I y otro cuántico con el conjunto de estados $\{\rho_i\}$. Una observación del sistema da como resultado el estado clásico i con probabilidad $p(i)$. En otras palabras, el estado cq codifica un conjunto de estados cuánticos en los valores clásicos $\{i \in I\}$. La representación de un estado cq en forma de un operador es, claramente,

$$\rho = \mathrm{diag}(p(1)\rho_1, \ldots, p(|I|)\rho_{|I|}),$$

o sea, un operador diagonal por bloques.

Una *purificación* de un estado cuántico ρ es cualquier estado puro $|u\rangle$ definido en el espacio $\mathscr{X} \otimes \mathscr{Z} := \mathbb{C}^d \otimes \mathbb{C}^{d'}$ tal que $\rho = \mathrm{tr}_{\mathscr{Z}}(|u\rangle\langle u|)$, en donde $\mathrm{tr}_{\mathscr{Z}}(\cdot)$ es la traza parcial $\mathrm{tr}_{\mathscr{Z}}(A \otimes B) = (\mathrm{tr}B)A$. La operación de traza parcial puede interpretarse (aunque realmente es una generalización no trivial) como la marginalización de una distribución de probabilidad conjunta. Para que exista una purificación de un estado cuántico es condición suficiente y necesaria que $d' \geq \mathrm{rango}(\rho)$ y, de hecho, la purificación de un estado no es única. Es posible probar que todas ellas son equivalentes, en el sentido de que siempre hay una isometría que convierte una purificación en otra. La purificación de estados es una herramienta de trabajo muy habitual y conveniente en la teoría cuántica de la información.

Una *medida* en un sistema cuántico ρ es en general una operación descrita por una colección $M = \{M_i : i \in I\}$ de operadores lineales positivos que satisfacen la condición $\sum_{i\in I} M_i^\dagger M_i = \mathbb{1}$. El resultado de realizar la medida M sobre un estado ρ es: (i) una observación $i \in I$ con probabilidad $p_i = \mathrm{tr}(M_i^\dagger M_i \rho)$; (ii) un sistema cuántico que queda en el estado $M_i \rho M_i^\dagger / p_i$. Esta regla es una generalización y una formalización abstracta de la *regla de Born*. De forma equivalente, una medida cuántica se puede definir como una colección de operadores positivos $\{\mu(i) : i \in I\}$ tales que $\sum_{i\in I} \mu(i) = \mathbb{1}$, que producen como resultado una observación $i \in I$ con probabilidad $p_i = \mathrm{tr}(\mu(i)\rho)$ y destruyen el estado ρ, el cual colapsa o cesa de existir. Nótese que, aunque ρ puede estar en cualquier superposición, el resultado de una medida es uno de entre un conjunto I de resultados posibles, que están definidos por el propio sistema de medida M. También es crucial entender la diferencia entre las probabilidades ``cuánticas'' p_i ---que aparecen solo después de realizar una medida--- y las probabilidades clásicas $p(i)$ como las que aparecen en un estado cq, que están definidas a priori. Una medida es una *medida proyectiva* si cada uno de los operadores (M_i, $\mu(i)$) es una proyección, esto es, $M_i^2 = M_i$ o $\mu(i)^2 = \mu(i)$. Un resultado importante de la teoría de la información cuántica, el *teorema de Naimark* [339], establece que toda medida se puede formular como una medida proyectiva en un espacio que incluye al espacio original $\mathscr{X} = \mathbb{C}^d$ como subespacio. Otro notable resultado, el lema de Winter [475], muestra que si una medida destructiva arroja un resultado cuya probabilidad es elevada, entonces la correspondiente medida no destructiva deja el estado resultante en un estado muy similar al original (en términos de una métrica llamada *fidelidad*) en caso de que se produzca el mismo resultado con ella. En el caso particular de una medida (destructiva) de Pauli de un qubit, es posible tomar $M = \{\langle v_0|, \langle v_1|\}$, donde $|v_0\rangle$ y $|v_1\rangle$ son los autovectores (auto-estados) del operador correspondiente P. Así, las medidas en base Z (las correspondientes al operador de Pauli Z) son $\{\langle 0|, \langle 1|\}$;

las medidas en base X (correspondientes al operador de Pauli X) son $\{\langle+|, \langle-|\}$; y las medidas en base Y (correspondientes al operador de Pauli Y) son $\{\langle \pm \imath| := \frac{1}{\sqrt{2}}(\langle 0| \pm \imath \langle 1|\}$. Naturalmente, como se aprecia en las definiciones, un estado cuántico puede medirse en una base arbitraria, distinta a aquella en la que fue preparado o generado [381, 382, 344, 230].

El último elemento fundamental de la teoría de la información cuántica son los *canales cuánticos*. Un canal cuántico es formalmente cualquier operador lineal $\mathscr{N}$ completamente positivo que preserva la traza. Mientras que la segunda condición es obvia, la primera significa que, para cualquier espacio de Hilbert $\mathscr{Z}$ y estado bipartito ρ definido en el espacio $\mathscr{X} \otimes \mathscr{Z}$, se cumple que $(\mathscr{N} \otimes \mathbb{1})(\rho)$ es positivo, o lo que es igual, que la acción de $\mathscr{N}$ sobre una parte de un estado (aquí $\mathscr{Z}$ representa el entorno o un estado de referencia arbitrario auxiliar al que quizá no tengamos acceso) deja como resultado otro estado cuántico. Obsérvese que un canal cuántico es una transformación determinista, y que incluye como caso particular las medidas, es decir, toda medida puede verse como un canal cuántico si así conviene. En realidad, cualquier operación sobre un estado cuántico puede formularse como la acción de un canal sobre el mismo. Por otro lado, a partir de la definición abstracta, los canales cuánticos admiten múltiples representaciones matemáticas, todas ellas equivalentes, claro está:

- La *representación de Choi* [99] de un canal $\mathscr{N}$ es el operador bipartito

  $$J(\mathscr{N}) = \big(\mathbb{1} \otimes \mathscr{N}\big)(\mathrm{vec}(\mathbb{1})\,\mathrm{vec}(\mathbb{1})^\dagger).$$

  $J(\mathscr{N})$ es positivo y $\mathrm{tr}_{\mathscr{Y}}\big(J(\mathscr{N}) = \mathbb{1}$.

- La *representación de Kraus* [259] de $\mathscr{N}$ es

  $$\mathscr{N}(\rho) = \sum_{i \in I} M_i \rho M_i^\dagger$$

  para una cierta colección de operadores de Kraus $\{M_i : i \in I\}$ que además satisfacen $\sum_{i\in I} M_i^\dagger M_i = \mathbb{1}$. La representación de Kraus de un canal no es única.

- La *representación de Stinesrping* [430] de $\mathscr{N}$ es

  $$\mathscr{N}(\rho) = \mathrm{tr}_E\big(V \rho V^\dagger\big),$$

  donde E es un sistema de referencia, V es una isometría que actúa en el espacio bipartito $\mathscr{H}_A \otimes \mathscr{H}_E$. El *canal complementario* $\mathscr{N}^c$ de $\mathscr{N}$ es

  $$\mathscr{N}^c(\rho) = \mathrm{tr}_A\big(V \rho V^\dagger\big),$$

  describe la dinámica de la información transferida al entorno o sistema de referencia E (E puede ser un observador externo interesado en averiguar cuál es el estado ρ, por ejemplo).

La noción de canal complementario motiva, a su vez, la definición de *canal degradable* y canal antidegradable [474, 124, 82]. $\mathscr{N}$ es degradable si existe otro canal $\mathscr{M}$ tal que $\mathscr{N}^c = \mathscr{M} \circ \mathscr{N}$, es decir, si es posible simular el canal complementario ---el efecto de $\mathscr{N}$ sobre el entorno--- pos-procesando la salida del canal $\mathscr{N}$; y es anti-degradable cuando $\mathscr{N} = \mathscr{M}' \circ \mathscr{N}^c$, o sea, si procesando la observación del canal complementario se puede simular $\mathscr{N}$.

Como se señaló al comienzo de esta sección, prácticamente cualquier operación matemática sobre un estado cuántico se puede concebir como un canal, pero con algunas notables excepciones. Así por ejemplo, el operador de traza $\mathrm{tr}(\cdot)$ y el de traza parcial son canales cuánticos, pero

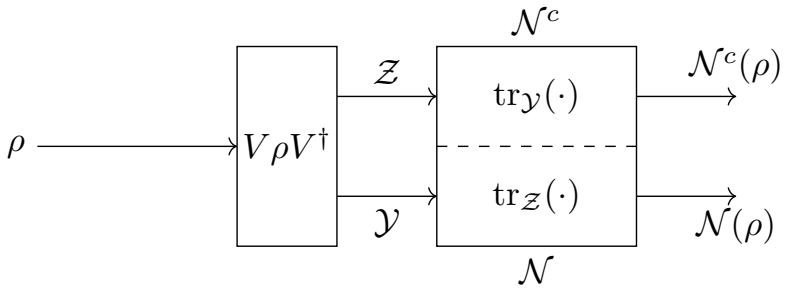


Figura 75: Ilustración del canal complementario de un canal cuántico. Una interpretación posible es verlo como la versión cuántica del canal clásico *wiretap* [168].

el operador de trasposición $T(\rho) = \rho^\top$ no es un canal cuántico: aunque evidentemente preserva la traza y es positivo, no es difícil ver que no es completamente positivo [255].

Pese a ser transformaciones deterministas, los canales cuánticos modelan errores de transmisión y ruido. Sea $p \in [0,1]$ una probabilidad de error, algunos ejemplos útiles y sencillos de canales cuánticos con errores son:

- El canal inversor de fase $\mathcal{N}(\rho) = (1-p)\rho + pZ\rho Z$.
- El canal inversor de bit $\mathcal{N}(\rho) = (1-p)\rho + pX\rho X$.
- El *canal depolarizador*

$$\mathcal{N}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z).$$

  El efecto del canal depolarizador, como se puede comprobar haciendo directamente el cálculo, es poner a cero todos los elementos de ρ fuera de la diagonal principal. Como caso extremo, el canal $\mathcal{N}(\rho) = \frac{1}{2}\mathbb{1} = \frac{1}{4}(\mathbb{1} + X + Y + Z)$ se llama *completamente depolarizador*.

- El canal con borrado $\mathcal{N}(\rho) = (1-p)\rho + p|e\rangle\langle e|$, donde $|e\rangle$ es un estado ortogonal a cualquiera de los estados del sistema $\mathscr{X}$.

Otro caso de interés es el *canal bosónico puro en pérdidas*, que se define por su representación de Stinespring

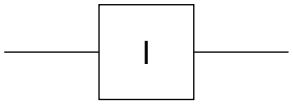
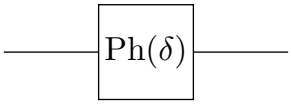
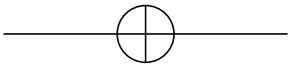
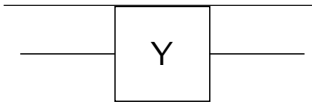
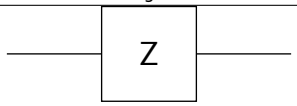
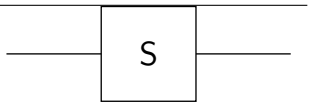
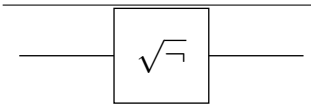
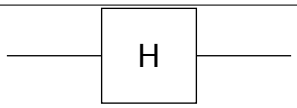
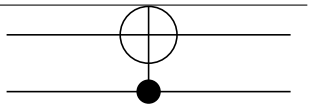
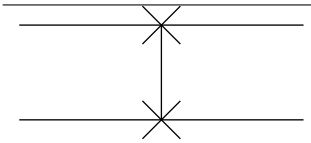
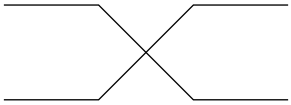
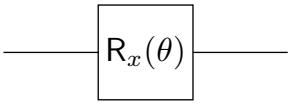
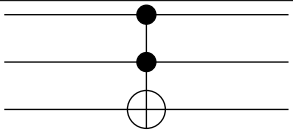
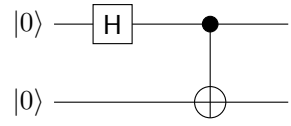
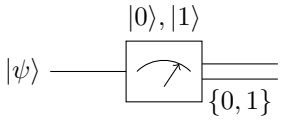
$$Va_{\mathscr{X}}V^\dagger = \sqrt{\eta}a_{\mathscr{Y}} + \sqrt{1-\eta}a_{E'},$$

en donde $a_{\mathscr{X}}$ (respectivamente, $a_{\mathscr{Y}}$) es el operador de anihilación del sistema bosónico $\mathscr{X}$ (resp., $\mathscr{Y}$), $0 \leq \eta \leq 1$ es la transmitancia del canal y $|0\rangle_E$ es el estado vacío del sistema bosónico E. Este modelo de canal es importante porque se emplea habitualmente como modelo de una fibra óptica, siendo $\eta = \mathrm{e}^{-L/L_{\mathrm{att}}}$ con L la longitud de la fibra y L_{att} la distancia de atenuación. $L_{\mathrm{att}} \approx 21{,}7$ km para una atenuación de $0{,}2$ dB/km como la que exhiben las fibras ópticas en uso hoy día.

B. Circuitos cuánticos

Un *circuito cuántico* es una combinación en serie de puertas cuánticas lógicas [344] que especifica las operaciones elementales que se han de llevar a cabo sobre uno o más qubits de

Tabla 14: Símbolos normalizados para algunas de las puertas cuánticas habituales.

Puerta cuántica	Puerta cuántica	Puerta cuántica
 Identidad	 Fase global	 Pauli X
 Pauli Y	 Pauli Z	 Fase S
 SX	 Hadamard H	 NOT controlada – CNOT
 Swap (I)	 Swap (II)	 Rotación
 Toffoli	 Estado de Bell (EPR) $\lvert\Phi^+\rangle = \frac{\lvert 00\rangle + \lvert 11\rangle}{\sqrt{2}}$	 Medida cuántica

entrada. Así pues, un circuito cuántico es una estructura de cómputo que modela los pasos de procesamiento un determinado algoritmo cuántico [156]. Al igual que con los circuitos digitales clásicos, para implementar una misma secuencia de cómputo se pueden utilizar circuitos cuánticos diferentes formados por una combinación de puertas distinta o una organización entre ellas diferente. La Tabla 14 recoge ls definiciones y los símbolos que se emplean por consenso para representar las operaciones de las puertas cuánticas básicas.

Muchas de las puertas cuánticas que se han propuesto en la literatura son operadores unitarios sobre un solo qubit, por lo que pueden englobarse en la expresión general

$$U = \mathrm{e}^{\imath\theta_1}\mathrm{R}_x(\theta_2)\mathrm{R}_y(\theta_3)\mathrm{R}_z(\theta_4), \quad \theta_i \in \mathbb{R},$$

es decir, como una concatenación de rotaciones alrededor los los ejes x, y, z más un cambio de fase global θ_1. Un ejemplo de un circuito cuántico elemental ---que se puede utilizar para crear estados entrelazados--- aparece en la última fila de la Tabla 14, donde se combinan una puerta de Hadamard H y una puerta CNOT sobre dos qubits $|0\rangle$ independientes. El resultado es uno de los *estados de Bell*.

Las puertas H, S y CNOT forman un *grupo de Clifford* [181], y se pueden simular de forma eficiente con un computador clásico haciendo uso del teorema de Gottesman-Knill [344]. El grupo de Clifford no es universal, no se puede emplear para describir cualquier circuito cuántico. Sin embargo, basta con añadir al grupo la puerta cuántica T ---que se definió en (8)--- para

obtener un conjunto universal, si bien ese conjunto no es único. Cada familia de ordenadores cuánticos, por ejemplo el IBM Q one [222], implementa su propio conjunto universal de puertas, dependiendo del hardware sobre el que opera.

Desde el punto de vista de la ingeniería, las características que cuentan en un circuito cuántico son sus medidas de complejidad (de implementación física), esto es, su *amplitud* o número de qubits de entrada, su *número de puertas* y su *profundidad* o longitud máxima entre una de sus entradas y una de sus salidas. Todas ellas tienen relación con la calidad o fiabilidad de los valores de salida computados, en el sentido de que la propagación de errores de cálculo se puede acotar por[21] $2(1-(1-r)^m)$, donde r es una constante independiente del número de qubits del circuito y m es su número de puertas [486]. Vemos, por tanto, que los errores se propagan exponencialmente con el número de puertas básicas. Estos errores en la ejecución de una puerta o de un circuito, que se deben a las imperfecciones de los sistemas físicos que las realizan, se pueden caracterizar de acuerdo con dos modelos básicos [486]: el modelo de error probabilístico y el modelo de error de Kraus. En el primer caso, después de que una puerta cuántica G se haya ejecutado, en el resultado aparece con cierta probabilidad un error, lo que se modela como un *operador de error* P

$$P(\rho) = \begin{cases} \rho, & \text{con probabilidad } 1-p \\ \text{otro estado}, & \text{con probabilidad } 1-p. \end{cases}$$

Este modelo se suele usar con los errores representados por los operadores de Pauli (X, Y, Z) y con el error de depolarización. En cambio, bajo el modelo de errores de Kraus se supone que tras la aplicación de la puerta G el resultado ρ se somete a la acción de un operador de Kraus

$$K(\rho) = V_1 \rho V^\dagger + \cdots + V_K \rho V_K^\dagger$$

para ciertos $\{V_k : k = 1, \ldots, K\}$ que cumplen $\sum_{k=1}^{K} V_k^\dagger V_k = \mathbb{1}$. Dos ejemplos comunes de errores de Kraus son la atenuación de amplitud

$$V_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \quad V_2 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix},$$

y la atenuación de fase

$$V_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}, \quad V_2 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{pmatrix},$$

donde γ y λ son los parámetros de atenuación en cada caso. Ambos modelos de error son equivalentes, extensibles a varios qubits y se utilizan ampliamente en los simuladores de computación cuántica, pero se prefiere uno de los dos en determinados casos (Tabla 15).

Las figuras 76 y 77 son esquemas que representan las operaciones de *teleportación* cuántica y de cálculo de la *transformada de Fourier cuántica* (QFT), respectivamente. La QFT se corresponde con la acción del operador

$$F = \frac{1}{\sqrt{n}} \sum_{i,j=0}^{n-1} \mathrm{e}^{\imath \frac{2\pi i j}{n}} |i\rangle\langle j|$$

sobre los n qubits de entrada. F es unitario, $F^\dagger F = \mathbb{1}$.

[21] Para ser precisos, esta es una cota para la norma Frobenius entre ρ y el estado resultante del error.

Tabla 15: Tipos de errores que puede describir cada modelo. Los errores combinados se pueden describir con el modelo de Kraus si las probabilidades de error X e Y son iguales.

Tipo de error	Modelo de error probabilista	Modelo de error de Kraus
X	✓	No
Y	✓	No
Z	✓	✓
Reset a $\|0\rangle\langle 0\|$	✓	✓
Depolarización	✓	✓
Atenuación de amplitud	No	✓
Atenuación de fase	No	✓
Relajación térmica	No	✓
Combinación	No	Condicionado

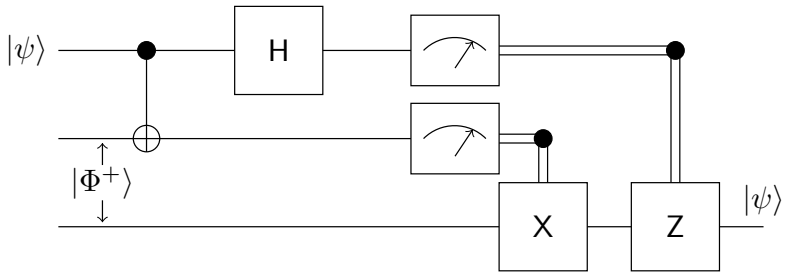


Figura 76: Circuito cuántico para la teleportación del qubit $|\psi\rangle$.

C. Información cuántica

La medida fundamental de la información cuántica es la *entropía cuántica* o entropía de von Neumann [344, 474, 468, 230]. Se define para un operador ρ como[22]

$$H(\rho) := -\operatorname{tr}(\rho \log \rho),$$

y generaliza la entropía clásica de Shannon $H_c(X) := -\sum_{i\in I} p_i \log p_i$ para un vector de probabilidades $\{p_i : i \in I\}$. La relación más inmediata entre ambas es que $H(\rho) = H_c(\{\lambda_i\})$, donde $\{\lambda_i\}$ son los autovalores de ρ. Por ejemplo, para un estado puro $\rho = |\psi\rangle\langle\psi|$, la entropía cuántica es nula $H(\rho) = 0$, dado que un estado puro solo tiene un autovalor no nulo, 1. En cambio, si consideramos el estado probabilista

$$\psi = \begin{pmatrix} |a|^2 & 0 \\ 0 & |b|^2 \end{pmatrix}, \quad |a|^2 + |b|^2 = 1,$$

entonces $|a|^2$ y $|b|^2$ son obviamente los autovalores y la entropía de von Neumann coincide con la entropía de Shannon, $H(\psi) = H_c(|a|^2, |b|^2)$. Estrechamente relacionada con la entropía cuántica está la cantidad denominada *entropía relativa cuántica* entre dos operadores ρ, σ

$$D(\rho||\sigma) := \operatorname{tr}(\rho \log \rho) - \operatorname{tr}(\rho \log \sigma),$$

[22] La notación que se usa para simbolizar las medidas de información cuántica varía según los autores, por ejemplo otros documentos denotan la entropía cuántica por $S(\cdot)$, $S(\cdot|\cdot)$, o como $H_\rho(A)$ o $H(A)_\rho$ para hacer explícito el sistema cuántico A de un estado ρ. Variantes parecidas se utilizan en ocasiones para la información mutua y la información coherente. En este Apéndice se ha seguido el criterio de mantener la notación más ligera posible sin perder ambigüedad.

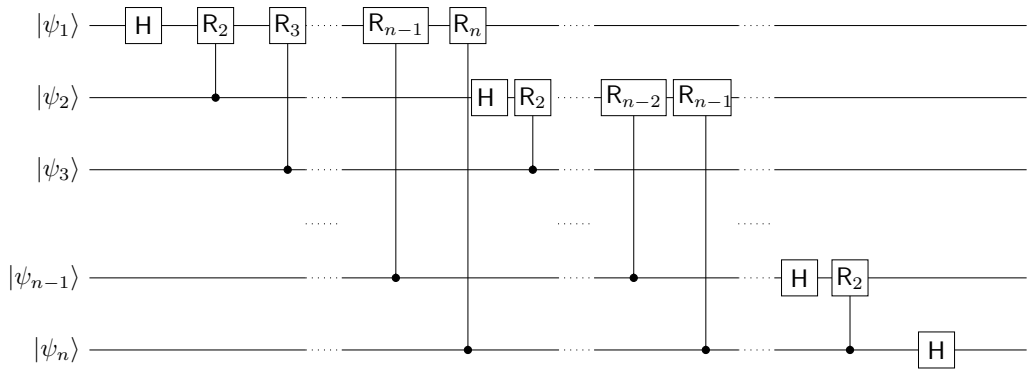


Figura 77: Circuito cuántico para la transformada cuántica de Fourier (QFT). El qubit i-ésimo se obtiene mediante una puerta Hadamard seguida de $n-i$ operaciones R_n controladas, donde $R_i = P_{2\pi/i}$ es una puerta de cambio de fase. Los $n-i$ qubits de mayor orden actúan como qubits de control.

que está bien definida siempre que $\mathrm{Im}(\rho) \subseteq \mathrm{Im}(\sigma)$; $D(\rho||\sigma) = +\infty$ en otro caso. La entropía relativa puede entenderse como una medida de la diferencia entre ρ y σ, si bien hay que advertir que $D(\rho||\sigma)$ no es simétrica. Las propiedades fundamentales de estas cantidades se enumeran a continuación.

1. $H(\rho) = -D(\rho||\mathbb{1})$.
2. Invariancia isométrica: para cualquier isometría V, $D(V\rho V^\dagger||V\sigma V^\dagger) = D(\rho||\sigma)$.
3. Desigualdad de Klein: $D(\rho||\sigma) \geq 0$ si $\mathrm{tr}(\rho) \geq \mathrm{tr}(\sigma)$; $D(\rho||\sigma) = 0$ si $\rho = \sigma$. Nótese que cuando ρ y σ son operadores de densidad la entropía relativa nunca es negativa.
4. Aditividad: para cualesquiera operadores $\rho_1, \rho_2, \sigma_1, \sigma_2$ se tiene $D(\rho_1 \otimes \rho_2||\sigma_1 \otimes \sigma_2) = \mathrm{tr}(\rho_2)D(\rho_1||\sigma_1) + \mathrm{tr}(\rho_1)D(\rho_2||\sigma_2)$. Por tanto, con operadores de densidad, $D(\rho_1 \otimes \rho_2||\sigma_1 \otimes \sigma_2) = D(\rho_1||\sigma_1) + D(\rho_2||\sigma_2)$. La entropía cuántica relativa de sistemas independientes se suma. Lo mismo ocurre con la entropía cuántica.
5. Suma directa: para dos estados cq $\rho = \sum_{i\in I} p(i)|i\rangle\langle i| \otimes \rho_i$, $\sigma = \sum_{i\in I} q(i)|i\rangle\langle i| \otimes \sigma_i$, se cumple
$$D(\rho||\sigma) = D(\mathbf{p}||\mathbf{q}) + \sum_{i\in I} p(i)D(\rho_i||\sigma_i),$$
donde $D(\mathbf{p}||\mathbf{q})$ es la entropía relativa (clásica) entre los vectores de probabilidad $\mathbf{p}$ y $\mathbf{q}$ [168].
6. Convexidad conjunta: la entropía relativa es conjuntamente convexa en sus argumentos. Para $0 < \lambda < 1$ siempre se cumple que
$$D\big(\lambda\rho_1 + (1-\lambda)\rho_2||\lambda\sigma_1 + (1-\lambda)\sigma_2\big) \leq \lambda D(\rho_1||\sigma_1) + (1-\lambda)D(\rho_2||\sigma_2).$$
En otras palabras, condicionar incrementa la entropía relativa. La convexidad conjunta implica a su vez la concavidad de la entropía
$$H\big(\lambda\rho_1 + (1-\lambda)\rho 2\big) \geq \lambda H(\rho_1) + (1-\lambda)H(\rho_2),$$

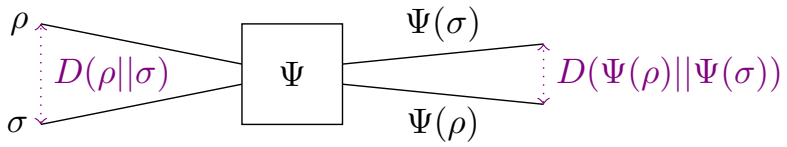


Figura 78: Desigualdad de procesamiento de la información para la entropía relativa.

y también el hecho de que sea subaditiva: si ρ es un sistema bipartito y $\rho[X] = \mathrm{tr}_Y(\rho)$, $\rho[Y] = \mathrm{tr}_X(\rho)$ son sus componentes, entonces $H(\rho) \leq H(\rho[X]) + H(\rho[Y])$.

7. Desigualdad de procesamiento de la información (DPI). Para cualquier canal $\mathscr{N}$ se tiene que
$$D(\rho||\sigma) \geq D\big(\mathscr{N}(\rho)||\mathscr{N}(\sigma)\big).$$
Así pues, ninguna forma de procesamiento cuántico de la información puede incrementar la entropía relativa. La desigualdad confirma la intuición de que ninguna forma de procesamiento de la información ayuda a distinguir entre sí mejor que antes dos estados que hayan sufrido ruido o distorsión. La Figura 78 ilustra esa característica.

A partir de estas definiciones y propiedades básicas, se definen otras medidas de información que aparecen y juegan un papel relevante en muchos problemas de la teoría de información cuántica. La *información mutua cuántica* para un sistema bipartito (X,Y) es la cantidad

$$I(\mathsf{X}:\mathsf{Y}) := D\big(\rho||\rho[\mathsf{X}]\otimes\rho[\mathsf{Y}]\big) = \inf_{\tau,\sigma} D(\rho||\tau\otimes\sigma) = H(\rho[\mathsf{X}]) + H(\rho[\mathsf{Y}]) - H(\rho).$$

En general, $I(\mathsf{X}:\mathsf{Y})$ cuantifica la correlación existente entre la entrada X y la salida $\mathsf{Y} = \mathscr{N}(\mathsf{X})$ de un canal cuántico. La *entropía condicional cuántica* es la cantidad

$$H(\mathsf{X}|\mathsf{Y}) := H(\rho) - H(\rho[Y]) = -D(\rho||\mathbb{1}\otimes\rho[\mathsf{Y}]) = -\inf_{\sigma} D(\rho||\mathbb{1}\otimes\sigma).$$

A diferencia de lo que sucede con la entropía condicional clásica, $H(\mathsf{X}|\mathsf{Y})$ puede ser negativa.[23] Una interpretación física del significado de este valor negativo de la entropía cuántica condicional se presenta en [213] en el contexto de la fusión de estados cuánticos, donde se explica que está relacionado con el hecho de que el emisor y el receptor obtienen un potencial para comunicaciones futuras (ver también [209]). Utilizando la entropía cuántica condicional se define la *información mutua cuántica condicional*

$$I(\mathsf{X}:\mathsf{Y}|\mathsf{Z}) := H(\mathsf{X}|\mathsf{Z}) + H(\mathsf{Y}|\mathsf{Z}) - H(\mathsf{X},\mathsf{Y}|\mathsf{Z}).$$

Otra cantidad importante en el estudio de las comunicaciones cuánticas es la *información de Holevo* [369], que se da en un contexto como el que sigue. Supóngase que Alice dispone de

[23] Obsérvese que la entropía condicional Shannon se define como un promedio de entropías, mientras que la entropía condicional von Neumann es una diferencia de entropías. Y, en segundo lugar, recuerde que la entropía von Neumann mide correlaciones clásicas y cuánticas. Un ejemplo sencillo puede ser cualquier purificación ψ de un estado ρ definido en el espacio $\mathscr{X}$: $H(\mathsf{Y}|\mathsf{X}) = H(\psi) - H(\rho) = 0 - H(\rho) = -H(\rho)$. De hecho, es fácil probar que los dos subestados de ψ tienen la misma entropía, $H(\rho[\mathsf{X}]) = H(\rho[\mathsf{Y}])$ y que, en general, para cualquier sistema bipartito (X,Y) se verifica $H(\mathsf{X}) \leq H(\mathsf{Y}) + H(\mathsf{X},\mathsf{Y})$.

una colección de estados cuánticos $\{\rho_i : i \in I\}$ con probabilidades $\{p(i) : i \in I\}$, de modo que su estado esperado es $\rho = \sum_{i\in I} p(i)\rho_i$. Alice transmite a Bob su estado a través de un canal $\mathcal{N}$. La información de Holevo en esta situación se define por

$$\chi(\mathcal{N})_\rho := H\big(\mathcal{N}(\rho)\big) - \sum_{i\in I} p(i) H\big(\mathcal{N}(\rho_i)\big).$$

Se puede probar [210] que la información de Holevo es una cota superior de la información mutua cuántica

$$I(\mathrm{X} : \mathrm{Y}) \leq \chi(\mathcal{N})_\rho$$

siendo X la variable aleatoria que registra el mensaje i que Alice quiere transmitir e Y el resultado de la estimación hecha a la salida del canal por el receptor Bob.

La última de las medidas de información que encierra importancia para ciertos problemas de teoría de información cuántica es la *información coherente* [402] de un canal $\mathcal{N}$ con respecto a un estado arbitrario ρ, la cual se define por

$$I_c(\rho, \mathcal{N}) := H\big(\mathcal{N}(\rho)\big) - H\big(\mathcal{N}^c(\rho)\big) = H\big(\mathcal{N}(\rho)\big) - H\big((\mathcal{N}\otimes \mathbb{1})(\mathrm{vec}(\sqrt{X})\,\mathrm{vec}(\sqrt{X})^\dagger)\big).$$

La información coherente se puede entender de forma equivalente como $I_c(\rho, \mathcal{N}) = H(\mathrm{Y}) - H(\mathrm{X},\mathrm{Y}) = -H(\mathrm{X}|\mathrm{Y})$, y mide la cantidad de información que se puede transferir por el canal cuando se tiene en cuenta el sistema de referencia. La importancia de la información coherente proviene del hecho de que induce una condición necesaria y suficiente para la existencia de un código de corrección de errores cuántico sobre un canal ruidoso.

Para finalizar, es una propiedad notable tanto de la información de Holevo como de la información coherente que ambas satisfagan una forma de desigualdad de procesamiento de la información: dados dos canales $\mathcal{M}$ y $\mathcal{N}$ en secuencia, se cumple que

$$\chi(\mathcal{M}\circ\mathcal{N})_\rho \leq \min\{\chi(\mathcal{M})_{\mathcal{N}(\rho)}, \chi(\mathcal{N})_\rho\}, \quad I_c(\rho, \mathcal{M}\circ\mathcal{N}) \leq I_c(\rho,\mathcal{N}) + I_c(\mathcal{N}(\rho),\mathcal{M}).$$

Como se ha visto, las propiedades esenciales de las medidas de información son en último término consecuencia de la convexidad conjunta y la DPI de la entropía relativa. Pues bien, si se toman como condiciones para una definición estas propiedades, entonces es posible generalizar el concepto de entropía relativa y encontrar otras funciones similares que satisfacen también esas condiciones. Existen en la literatura muchas variantes que generalizan la entropía cuántica relativa, y cuyas propiedades son muy semejantes a las dadas. Damos un resumen de estas nociones de entropía generalizada en la Tabla 16. El lector interesado puede consultar [230], por ejemplo, para una exposición rigurosa y en detalle de todas ellas.

D. Cronología y progreso

A título informativo, la Tabla 17 enumera varios de los hitos científico-técnicos acaecidos en los últimos 30 años en el campo de la información cuántica. Naturalmente, la tabla no es más que una antología.

Glosario

amplitud número de qubits de entrada a uncircuito cuántico, 191

Tabla 16: Entropías generalizadas: definición. Para una revisión exhaustiva de las llamadas f-divergencias, véase [206].

Entropía	Definición	Dominio
Petz-Rényi	$D_\alpha(\rho\|\|\sigma) = \frac{1}{\alpha-1}\log_2 \mathrm{tr}(\rho^\alpha \sigma^{1-\alpha})$	$\alpha \in (0,1)\cup(1,\infty)$
Sandwiched Rényi	$\tilde{D}_\alpha(\rho\|\|\sigma) = \frac{1}{\alpha-1}\log_2 \mathrm{tr}\left(\left(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right)$	$\alpha \in (0,1)\cup(1,\infty)$
Geometric Rényi	$\hat{D}_\alpha(\rho\|\|\sigma) = \frac{1}{\alpha-1}\log_2 \lim_{\varepsilon\to 0^+} \mathrm{tr}\left(\sigma_\varepsilon\left(\sigma_\varepsilon^{-1/2}\rho\sigma_\varepsilon^{-1/2}\right)^\alpha\right)$	$\sigma_\varepsilon = \sigma + \varepsilon\mathbb{1}$
Belavkin-Staszweski	$\hat{D}(\rho\|\|\sigma) = \mathrm{tr}\left(\rho\log\left(\rho^{1/2}\sigma^{-1}\rho^{1/2}\right)\right)$	$\mathrm{Im}(\rho)\subseteq\mathrm{Im}(\sigma)$
Max-relative	$D_{\max}(\rho\|\|\sigma) = \log_2 \left\|\sigma^{1/2}\rho\sigma^{1/2}\right\|_\infty$	$\mathrm{Im}(\rho)\subseteq\mathrm{Im}(\sigma)$
ε-hipótesis	$D_H^\varepsilon(\rho\|\|\sigma) = -\log_2 \inf_\Lambda\{\mathrm{tr}(\Lambda\rho) : 0\le\Lambda\le\mathbb{1}, \mathrm{tr}(\Lambda\sigma) = 1-\varepsilon\}$	–

bra-ket Notación vectortial para los estados cuánticos, 184

canal bosónico puro en pérdidas modelo de canal cuántico de una fibra óptica, 189

canal complementario traza parcial del sistema de referencia tras la acción de un canal, 188

canal cuántico operador lineal completamente positivo y de traza unidad, 188

canal degradable canal cuyo canal complementario es simulable mediante otro canal cuántico, 188

canal depolarizador canal cuántico que suprime todas las correlaciones entre sus componentes, 189

capacidad máxima tasa de transferencia de información (clásica o cuántica) a través de un canal, 22

circuito cuántico combinación básica de puertas cuánticas, 189

codificación bosónica codificación de variable continua, 30

codificación de variable continua codificación fotónica con un espacio de estados infinito, 30

codificación de variable discreta codificación fotónica con un número de estados discreto, 30

codificación fotónica correspondencia entre el estado físico de un fotón (espín, polarización, etc.) y un qubit lógico, 30

conmutador cuántico dispoisitivo físico de intercambio de entrelazamiento entre cualquier grupo de enlaces conectados al mismo, 44

criterio de Horodecki condición matemática que liga la separabilidad al hecho de que una transformación sea positiva, 13

criterio PPT condición necesaria para que un estado sea separable, 14

desigualdades de Bell desigualdades sobre correlación que debe cumplir todo sistema físico clásico, 34

Tabla 17: Hitos y resultados en el desarrollo de la teoría de la información cuántica, 1990–. Adaptado de [255].

Año	Resultado
1992	Codificación superdensa [42]
1993	Teleportación cuántica [43]
1995	Información de Holevo como tasa alcanzable para la capacidad clásica *one-shot* sobre canales clásico-cuánticos [200]
1996	Información coherente como cota superior de la capacidad *one-shot* cuántica [401, 402]
1997	Teorema HSW de capacidad: capacidad clásica *one-shot* y regularizada [211, 403] Teorema LSD: capacidad cuántica *one-shot* y regularizada [295]
1998	Existencia del límite en la regularización de la capacidad clásica [29] Superaditividad de la información coherente [132]
1999	Aditividad de la información Holevo para canales cuánticos con borrado [41]
2002	Aditividad de la información Holevo para canales destructivos de entrelazamiento [410]
2003	Conceptos de canal complementario y canal degradable [124] Aditividad de la información de Holevo para el canal depolarizador [247]
2005	Aditividad de la información de Holevo para canales Hadamard [248] Conjetura de aditividad [412] Trayectorias controladas cuánticas para filtrado de errores y purificación de entrelazamiento [178]
2006	Concepto de canal anti-degradable [83]
2007	Contraejemplo de Hasting para establecer la superaditividad de la información de Holevo [199]
2008	Superactivación de la capacidad cuántica [422]
2009	Superaditividad de la capacidad cuántica para los canales Rocket y cuántico con borrado [420]
2013	Switch cuántico: formulación teórica [97]
2015	Superaditividad de la información coherente [115] Realización experimental de un switch cuántico [368]
2018	Switch cuántico: violación de la DPI para la información de Holevo del canal completamente depolarizador [142] Superaditividad del canal *dephrasure* [266]
2020	Switch cuántico: violación de la desigualdad DPI para la información coherente del canal completamente depolarizador [96, 397]
2021	Switch cuántico: violación de la desigualdad DPI para la información coherente de los canales destructivos de entrelazamiento [98] Switch cuántico: verificación experimental de la violación de la desigualdad DPI para la información de Holevo y la información coherente [391]
2023	Disminución de la superaditividad con la dimensión del canal depolarizador [311] No-aditividad general de la capacidad en canales simples [267]

destilación de entrelazamiento proceso de obtención de un estado entrelazado más a partir de uno o más estados entrelazados precursores con entrelazamiento más débil, 49

dual-rail codificación fotónica en la que cada fotón ocupa uno de dos modos ópticos, 31

ebit unidad de medida del entrelazamiento, correspondiente a un estado de Bell, 17

entrelazado entrelazamiento, propiedad o condición de no ser separable, 13

entrelazamiento de formación entropía de entrelazamiento, 18

entrelazamiento máximo estado bipartito entrelazado cuyos estados componentes son $\mathbb{1}$, 14

entropía cuántica función de entropía de un estado (operador) cuántico, 192

entropía de entrelazamiento medida cuantitativa del entrelazamiento de un operador, 18

esfera de Bloch Representación del estado de un qubit en coordenadas esféricas, 186

estado clásico-cuántico estado de un sistema bipartiuto formado por un registro clásico probabilista y una colección de estados cuánticos, 187

estado producto producto tensor de varios estados cuánticos, 186

estado puro Un estado cuántico de rango 1, 184

estados de Bell estados de entrelazamiento máximo (qubits), 14, 190

Estados de Werner familia paramétrica de estados con una grado variable de entrelazamiento, 15

Estados GHZ estados multipartitos entrelazados para $M > 2$ sistemas, 15

estados grafo estados cuánticos multipartitos cuyas correlaciones se modelan con un grafo, 19

Estados isotrópicos familia paramétrica de estados con un grado variable de entrelazamiento, 15

fidelidad métrica de distancia entre dos operadores (estados) cuánticos, 23, 187

información coherente medida de informacióncuántica que caracteriza la capacidad cuántica de un canal, 24

información de Holevo medida de información cuántica que caracteriza la capacidad clásica de un canal cuántico, 23

Intermediate Representation representaci´pon intermedia entre la descripción algorítmica y la ejecución hardware de una determnminada computación cuántica 100

LOCC Local Operations and Classical Communications, paradigma operacional en el que solo dse permiten transformaciones cuánticas locales y comunicación clásica (uni o bidireccional) enytre las partes, 12

medida operadores positivos $\{M_i\}$ con $\sum_i M_i^\dagger M_i = \mathbb{1}$. POVM, positive operator-valued measure, 187

medida proyectiva cualquier medida cuántica POVM cuyios operadores son proyecciones, 187

medidas de Bell reforzadas uso de recursos cuánticos adicionales para incrementar la probabilidad de éxito en una medida de Bell, 62

merging fusión de estados, transferencia de un estado cuántico local a otro punto sin romper la coherencia del estado global, asistida por entrelazamiento, 20

negatividad medida cuantitativa del entrelazamiento de un operador, 18

Noisy Intermediate-Scale Quantum característica actual de las QPU, con un número moderado de qubits (cientos) y computacuión con ruido 96

operador de densidad Un operador lineal positivo de traza unidad. Es la representación matemática de un estado cuántico, 184

operador de intercambio operador lineal que permuta el orden del producto tensor de dos vectores, 15

operadores de Pauli Un tipo específico de operadores unitarios sobre qubits, 185

pares EPR estados de Bell, 14

principio de no señalización imposibilidad de llevar a término un proceso de comunicación más rápido que la velocidad de la luz aun con ayuda de entrelazamiento cuántico, 37

profundidad longitud máxima (puertas) de un camino en un circuito cuántico, 191

puerta cuántica Csualquier transformación reversible sobre un qubit, 185

purificación extensión de un estado cuántico a un espacio de mayor dimensión en el cual admite una representación como subestado de un estado puro, 187

QPU Procesador cuántico, Quantum Processing Unit. Cualquier ente físico capaz de procesar información cuántica, 9, 97

Quantum Control Unit unidad de control cuántica, el equivalente cuántico de una CPU 103

quantum SWITCH conmutador cuya ruta interna está en un estado cuántico cuperpuesto controlado por uno o varios qubits de control, 5, 45

qubit Quantum bit. Unidad de medida de la información cuántica. Un estado en un espacio de Hilbert de dimensión 2, 184

qudit Un estado cuántico en d dimensiones, 186

rango de entrelazamiento medida cuantitativa del entrelazamiento de un operador, 18

regla de Born postulado de la mecánica cuántica, la medida de un sistema cuántico es i con probabilidad $\mathrm{tr}(M_i^\dagger \rho)$, 187

regularización en teoría de información cuántica, proceso de paso al límite de una medida de informacióin (promedio), 24

repetidor cuántico sistema físico para porpagar un estado cuántico entre un punto de entrada y uno de salida, 42

representación de Choi representación matemática de un canal cuántico como un operador bipartito sobre un estado entrelazado máximo, 188

representación de Kraus representación de un canal cuántico como una combinación lineal de operadores de Kraus o de conjugación, 188

representación de Stinesrping representación matemática de una canal cuántico como una acción sobre una purificación del sistema de entrada, 188

separabilidad propiedad de un estado, operador, canal o medida que permite expresarlo como un producto tensor de estados (etc.) de menor dimensión, 13

single-rail codificación fotónica en la que cada fotón ocupa un solo modo óptico, 31

superactivación propiedad superaditiva de la combinación en paralelo de algunos canales cuánticos, 26

superposición Una combinación probabilista de estados cuánticos puros, 184

teleportación transmisión de un estado cuántico sobre un canal clásico, 191

teorema de Naimark resultado de la teoría de información cuántica, en un espacio extendido, toda media es proyectiva, 187

tiempo de coherencia tiempo durante el cual la información guardada en un registro de memoria cuántico se mantiene sin ser degradada espontáneamente por su entorno físico, 52

time-bin codificación fotónica en la que se envían fotones por trayectos de longitud diferente, 31

transformación unitaria Un operador lineal U que cumple $U^\dagger U = \mathbb{1}$, 185

transformada de Fourier cuántica versión cuántica de la transformada de Fourier, 191

trayectos cuánticos concatenación no causal de canales cuánticos, 45