COMUNICACIÓN CUÁNTICA

Palabras clave: Comunicación cuántica, Distribución cuántica de claves, Metrología cuántica, Tecnologías cuánticas.
Keywords: *Quantum Communication, Quantum Key Distribution, Quantum Metrology, Quantum Technology.*

Resumen: Los fotones son los sistemas cuánticos fundamentales que describen el campo electromagnético (la luz) a nivel microscópico. Dicho de otra forma, la cuantificación del campo electromagnético implica que éste sea tratado como una colección de paquetes de energía discretos, que se denominan fotones. A lo largo de este artículo vamos a discutir las aplicaciones de estas "partículas de luz", fundamentalmente en el campo de las comunicaciones. Adicionalmente, las tecnologías actualmente en desarrollo basadas en el uso de fotones exceden a las aplicaciones en comunicaciones y se enfocan también en la metrología ultrasensible, la formación de imágenes y el sensado. Estos temas se repasan brevemente al final del artículo.

Laura T. Knoll[1,2*], Miguel A. Larotonda[1,2]**

1 División Óptica Cuántica - DEILAP (UNIDEF-CITEDEF), J.B. de Lasalle 4397, (B1603ALO) Villa Martelli, Buenos Aires, Argentina.
2 Departamento de Física, Facultad de Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, 1428, Buenos Aires, Argentina.

E-mail: *lknoll@citedef.gob.ar
**mlarotonda@citedef.gob.ar

Quantum Communication
Abstract: Photons are the fundamental quantum systems that describe the electromagnetic field (light) at the microscopic level. In other words, the quantization of the electromagnetic field implies that it is treated as a collection of discrete energy packets, called photons. Throughout this article, we will discuss the applications of these "particles of light", primarily in the field of communications. Additionally, state-of-the-art technologies that exploit the quantum nature of the photons exceed the applications in communications, and are also focused in ultra-sensitive metrology, imaging and sensing. These topics are briefly reviewed at the end of this article.

■EL ORIGEN DE LAS "COMUNICACIONES CUÁNTICAS". LA FOTÓNICA CUÁNTICA COMO TECNOLOGÍA DISRUPTIVA

Los principios y el formalismo de la mecánica cuántica fueron establecidos a principios del siglo XX, y surgieron para explicar el comportamiento de la materia y la energía a niveles atómico y subatómico. A este hito se lo denomina la **primera revolución cuántica**, y en general entendemos que se extiende desde 1900 hasta la década del '70. En este período aparecieron tecnologías como los láseres, los dispositivos semiconductores y, en general, la capacidad de manipular *ensambles* de sistemas cuánticos. Casi un siglo después, y gracias a los desarrollos anteriores, se pudo obtener la capacidad de manipular y controlar sistemas cuánticos individuales, como átomos, moléculas y fotones, para desarrollar nuevas tecnologías como computadoras cuánticas, sensores y sistemas de comunicaciones cuánticas. A este período actual de avances rápidos en aplicaciones prácticas de la mecánica cuántica se lo denomina **segunda revolución cuántica**.

Las comunicaciones cuánticas aparecen como concepto alrededor de 1970, en un trabajo de Stephen Wiesner llamado "*Conjugate Coding*" ("Codificación conjugada"), que se mantuvo inédito hasta 1983, en el que el autor explicaba cómo la física cuántica podría permitir que una entidad bancaria genere notas de pago que fueran imposibles de falsificar (Wiesner, 1983). Estas ideas se revisaron a principios de los '80, pero los incipientes posibles protocolos requerían tareas tecnológicamente imposibles, incluso para el estado del arte actual. Poco tiempo después Charles Bennett y Gilles Brassard realizaron una propuesta revolucionaria: al decir de los propios autores, el avance principal ocurrió cuando se percataron de que los fotones nunca estuvieron destinados a almacenar información, sino más bien a transmitirla (Bennett, 1989). En el año 1984, Bennett y Brassard publicaron el trabajo que da origen al famoso protocolo BB84 de **Distribución Cuántica de Claves** criptográficas (QKD por sus siglas en inglés, Quantum Key Distribution) (Bennett, 1984). A partir de ese momento QKD se transforma en algo realizable, y de hecho es una de las primeras tecnologías cuánticas que prepara y mide sistemas cuánticos a nivel individual llevadas a la práctica en el mundo real, es decir fuera del laboratorio.

En este artículo describimos con cierto grado de profundidad los aspectos teóricos de los protocolos de distribución cuántica de claves, así como algunas de sus posibles implementaciones y limitaciones. Finalmente, presentamos un repaso de otras aplicaciones tecnológicas que explotan las propiedades no clásicas y contraintuitivas de los fotones individuales. Estas aplicaciones se apoyan en desarrollos tec-

nológicos originalmente concebidos para la preparación y detección de fotones únicos, los cuales habilitaron a su vez nuevos esquemas de medición. En este marco, diversas tareas tradicionalmente realizadas con luz clásica resultan más eficientes cuando se implementan en un escenario cuántico (Barreto Lemos, 2022; Chen, 2022; Couteau, 2023; Defienne, 2024), entre ellas la determinación de fases interferométricas, la obtención de imágenes y la calibración de detectores de intensidad en regímenes de iluminación extremadamente baja.

■ EL PROBLEMA DE LA DISTRIBUCIÓN DE CLAVES CRIPTOGRÁFICAS.

Antes de enfocarnos en los detalles de la distribución cuántica de claves, conviene empezar mencionando qué problema resuelve. La distribución de claves criptográficas es el proceso de proveer claves en forma segura a dos o más partes de una red, con el fin de asegurar fundamentalmente tareas de autenticación (ser quien uno dice ser), integridad (conservar el mensaje inalterado) y privacidad, en una sesión de comunicación. Los protocolos criptográficos actuales de uso más difundido en comunicaciones seguras son los denominados asimétricos o de clave pública (por ejemplo el protocolo RSA), o los simétricos o de clave privada (por ejemplo el sistema AES). Ambas familias de protocolos se basan en la complejidad de algún problema matemático: factorización de números grandes en RSA y cifrado por bloques en AES (Katz, 2007). Estos problemas son, en principio, difíciles de resolver con una computadora clásica, pero fácilmente resolubles con una computadora cuántica (Ladd, 2010; Rieffel, 2000; ver también el artículo "Los principios básicos de una computadora cuántica", de Federico Holik y Augusto J Roncaglia, en este volumen). Por esta razón están actualmente amenazados por la inevitable aparición de computadoras cuánticas reales y la aplicación de algoritmos cuánticos de Shor (factorización de números grandes) y Grover (búsqueda no estructurada), respectivamente (Nielsen, 2010). Aún con el desarrollo de algoritmos post-cuánticos, que se basan en problemas matemáticos conocidos por su dificultad y son resistentes a ataques de computadoras clásicas y cuánticas, como por ejemplo AES-256, se requiere una instancia de distribución de la clave compartida. La mecánica cuántica, además del problema de la vulnerabilidad de protocolos clásicos, también aporta la solución a la distribución de la clave, a través de protocolos de

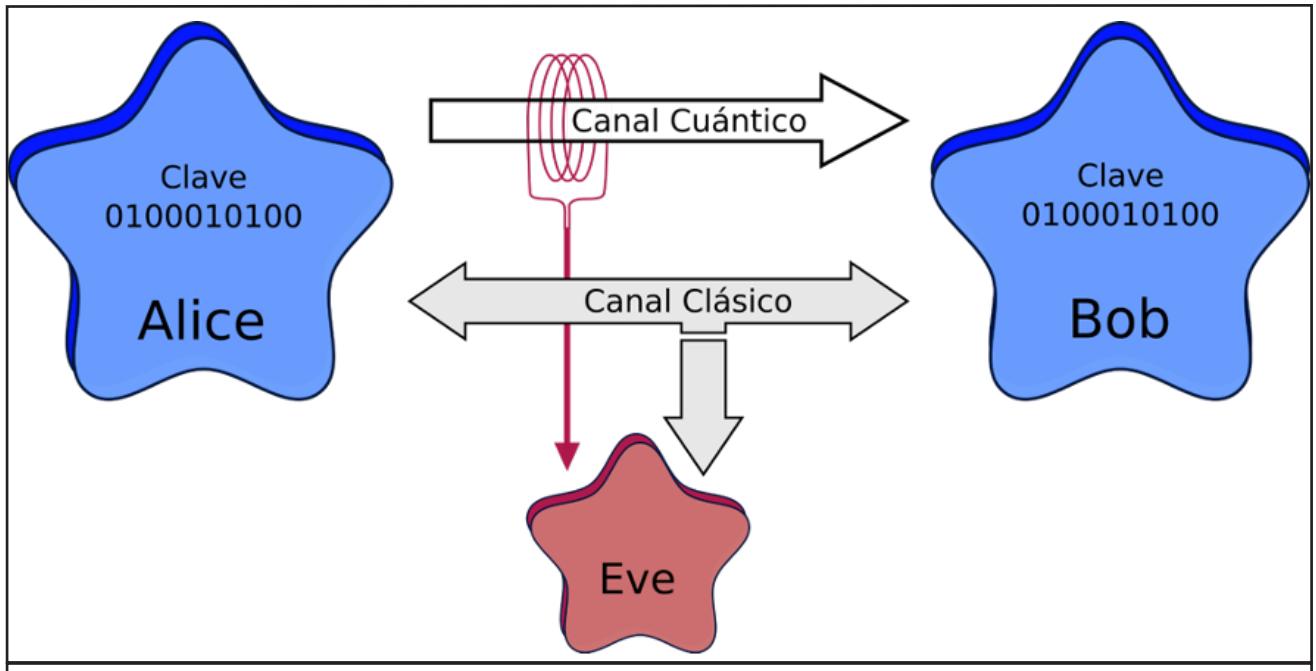

Figura 1. *La Distribución Cuántica de Claves es un método a partir del cual Alice y Bob, dos usuarios genuinos, buscan establecer una clave secreta compartida usando un canal de comunicación clásico y uno cuántico. El espía Eve intenta interceptar y obtener información que fluye entre Alice y Bob. La suposición es que Eve puede interferir de cualquier manera en el canal cuántico, mientras que el canal clásico debe ser autenticado (es decir, puede ser observado pero no modificado).*

QKD. En las siguientes secciones vamos a repasar algunos conceptos muy básicos de la mecánica cuántica relevantes para el procesamiento cuántico de la información y específicamente para la ejecución de un protocolo de QKD, y describiremos el protocolo de comunicación cuántica más famoso, BB84, usando una codificación particular de bits cuánticos (o 'qubits') mediante fotones.

■ CODIFICACIÓN DE QUBITS CON FOTONES

Seguidamente veremos cómo es que usando un tipo de protocolo particular de preparación, transmisión y medición de estados de fotones únicos, al final del día dos interlocutores A y B (históricamente llamados Alice y Bob) pueden compartir una clave de unos y ceros aleatoria, segura y sólo conocida por ellos. La comunicación entre Alice y Bob requiere un canal cuántico (que transmite qubits) y un canal clásico autenticado (para realizar las tareas de tamizado, corrección de errores y amplificación de la privacidad). El, la o los potenciales espías se denominan Eve (por *eavesdropper*). Eve tiene acceso irrestricto al canal cuántico, y puede observar, pero no modificar, el canal clásico (Fig. 1).

Los bits cuánticos se codificarán en el llamado 'estado de polarización' de los fotones, que puede ser representado como un sistema cuántico de dos niveles. Otras codificaciones en distintos grados de libertad del fotón son posibles, pero eso lo discutiremos más adelante.

Antes de describir el protocolo, repasemos la notación que vamos a utilizar para describir los qubits: el estado de polarización de un fotón puede ser modelado por un vector que apunta en la dirección apropiada. Los posibles estados de qubits pueden representarse geométricamente mediante vectores en la llamada esfera de Bloch (Fig.2c). Cualquier estado de polarización arbitraria se puede expresar como una combinación lineal $|\psi\rangle = a\,|H\rangle + b\,|V\rangle$ de los dos vectores de la base *computacional*: $|H\rangle$ (polarización horizontal, también denotado $|0\rangle$) y $|V\rangle$ (polarización vertical, también denotado $|1\rangle$). En particular, los vectores de la base *diagonal* se pueden escribir como combinación lineal de los vectores de la base *computacional*: $|D\rangle = 1/\sqrt{2}\,(|H\rangle + |V\rangle)$, $|A\rangle = 1/\sqrt{2}\,(|H\rangle - |V\rangle)$ y viceversa: $|H\rangle = 1/\sqrt{2}\,(|D\rangle + |A\rangle)$, $|V\rangle = 1/\sqrt{2}\,(|D\rangle - |A\rangle)$. Estas dos bases de representación de estados de polarización son conjugadas, o "máximamente com-

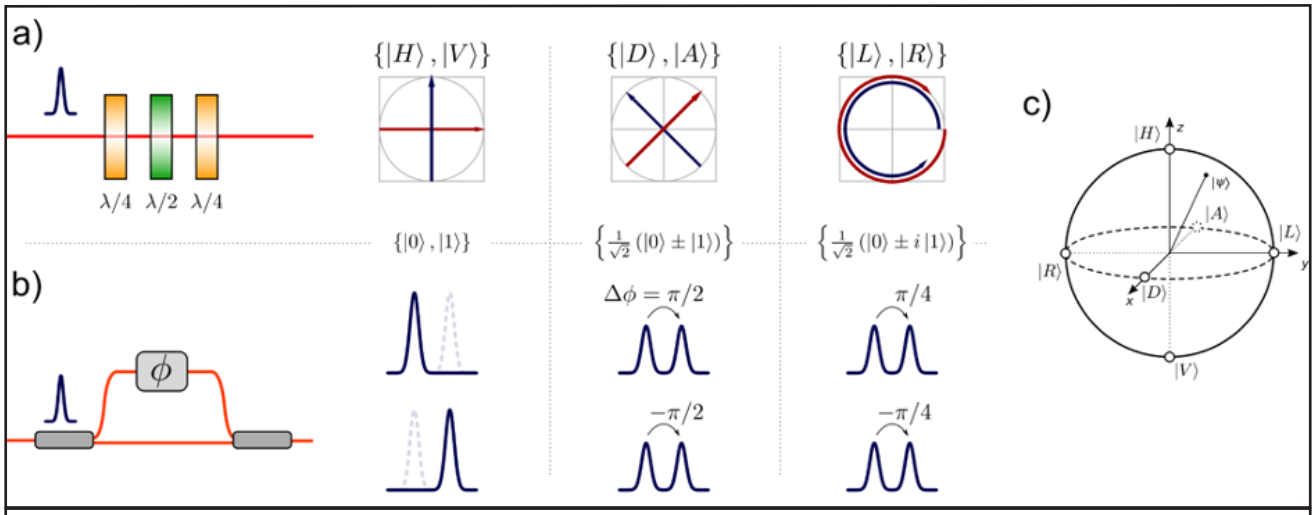

Figura 2. *Qubits codificados en grados de libertad del fotón: a) Codificación en polarización. Izquierda: la preparación del estado se puede realizar con un conjunto de láminas retardadoras cuyos ejes se puede rotar alrededor del eje de propagación; a la derecha, en tres columnas se representan los estados de tres bases mutuamente no sesgadas del qubit de polarización, usualmente llamadas computacional, diagonal y circular. b) Codificación en time-bin; se conforma con un par de pulsos que mantienen la coherencia. Izquierda: la preparación del estado se realiza apagando uno u otro pulso para la base computacional o modificando la fase relativa ΔΦ entre ambos pulsos en las otras dos bases; en las tres columnas de la derecha del panel se representa la amplitud de los símbolos para cada una de las bases, análogas a las de polarización. c) Representación geométrica de qubits en la llamada esfera de Bloch. La superficie de esta esfera representa a todos los posibles estados puros de dos niveles* $|\psi\rangle$ *. En particular, los estados de la base computacional se ubican en los polos de la esfera, y los de las otras dos bases sobre el ecuador.*

plementarias", en el sentido que conocer el estado de polarización en una de las bases aporta la mínima información posible sobre el estado del sistema en la otra base (la conjugada). Este concepto es crucial para entender el origen de la seguridad en protocolos de QKD. Los vectores de la base *circular* también pueden construirse como combinaciones lineales balanceadas de la base *computacional*, o de la base *diagonal*: $|R\rangle = 1/\sqrt{2}\ (|H\rangle + i\ |V\rangle)$, $|L\rangle = 1/\sqrt{2}\ (|H\rangle - i\ |V\rangle)$. Estas tres bases, conjugadas entre sí, forman lo que se denomina un conjunto de bases mutuamente no sesgadas en el espacio de Hilbert de dimensión d=2 de los qubits: si un sistema (estado de polarización de un fotón) es preparado en un autoestado de alguna de las bases, la probabilidad de obtener cualquier resultado en una medición respecto de las otras bases es igual a 1/2 para qubits (y es 1/d en general): si intento medir un estado $|D\rangle$ en la base computacional (medición cuyos resultados o proyecciones posibles son $|H\rangle$ o $|V\rangle$), aproximadamente la mitad de las veces obtendré $|H\rangle$ y las otras veces $|V\rangle$ (Fig. 2a).

En el párrafo anterior introdujimos disimuladamente (o no tanto) una notación específica: el concepto del espacio de Hilbert proyectado por los vectores de alguna de las bases. No es la idea transformar este texto en un curso acelerado de Física Cuántica, por lo que simplemente vamos a mencionar que el espacio de estados de un sistema cuántico, que consta de la posición, momento (o cantidad de movimiento), polarización, spin, etc. de las distintas partículas, se modela mediante un espacio de Hilbert de funciones de onda. Ignoraremos los detalles de estas funciones de onda. Los espacios de estados cuánticos y las transformaciones que actúan sobre ellos pueden describirse en términos de vectores y matrices o en la notación *bra/ket* más compacta inventada por Dirac (Dirac, 1981). Los *kets* como $|X\rangle$ denotan vectores columna y se utilizan normalmente para describir estados cuánticos. El *bra* complementario, $\langle X|$, denota el elemento transpuesto conjugado de $|X\rangle$. Para entender el funcionamiento de protocolos cuánticos simples sólo necesitamos tratar con sistemas cuánticos finitos y basta con considerar espacios vectoriales complejos de dimensión finita con un producto interno, que están abarcados por funciones de onda abstractas, como $|H\rangle$, o $|D\rangle$ en el caso de los estados de polarización de un fotón.

■ OTROS GRADOS DE LIBERTAD

Además de la polarización, se pueden codificar bits cuánticos en distintos grados de libertad del fotón, como el camino o momento lineal, o los modos transversales del campo electromagnético. Dado que la aplicación de QKD requiere propagar estos estados a distancias de varios kilómetros, el grado de libertad elegido debe ser robusto frente a perturbaciones del medio. Para enlaces por aire, la polarización es bastante poco sensible a distorsiones de fase producidas en la atmósfera, por lo que es la codificación usada por excelencia. Para propagación en fibra, sin embargo, los efectos de birrefringencia residual del núcleo, y sobre todo la birrefringencia inducida térmica o mecánicamente, que es variable, alteran el estado de polarización a la salida de la fibra de forma errática, de manera que para codificar qubits en polarización, el canal de fibra debe contar con un control activo de la polarización. La alternativa es usar lo que se denomina modos de *time-bin*: los qubits se codifican en un par de pulsos desplazados temporalmente algunos nanosegundos o incluso menos. Ambos viajan juntos, por lo que las perturbaciones que modifican el índice de refracción y por ende la fase óptica de la fibra afectan a ambos pulsos simultáneamente, agregando una fase global irrelevante. Apagando el primero o el segundo pulso se obtienen los estados de la base computacional, y modificando la fase relativa entre ambos pulsos se generan los estados de las otras dos bases mutuamente no sesgadas de la codificación *time-bin* (Fig. 2b).

■ DISTRIBUCIÓN CUÁNTICA DE CLAVES. EL PROTOCOLO BB84.

Para comenzar el proceso de establecer una clave secreta entre Alice y Bob (personajes ficticios que participan de un sistema de comunicación), Alice envía una secuencia de bits (cada bit puede tomar el valor 0 o 1) a Bob, codificando cada bit en el estado cuántico de (la polarización de) un fotón de la siguiente manera. Alice utiliza aleatoriamente una de dos bases conjugadas para codificar cada bit: $0 \rightarrow |H\rangle$; $1 \rightarrow |V\rangle$, o $0 \rightarrow |D\rangle$; $1 \rightarrow |A\rangle$. En este caso Alice y Bob están usando las bases *computacional* y *diagonal*, pero el protocolo podría funcionar con cualquier par de bases mutuamente no sesgadas.

Bob, a su turno, mide el estado de polarización de los fotones que recibe, eligiendo cualquiera de las bases al azar. Una vez transmitidos los bits (y no antes), Alice y Bob usan el canal clásico autenticado para comunicar la base que utilizaron para preparar y medir, respectivamente, cada bit. Con esta información, ambos pueden determinar qué bits se han transmitido correctamente, identificando aquellos bits en los que están de acuerdo las bases emisora y receptora: en el caso de que las bases de preparación y de medición coinciden, el resultado es determinístico y sólo está alterado por eventuales errores de implementación. Utilizarán estos bits como clave y descartarán todos los demás. En

promedio, Alice y Bob estarán de acuerdo en el 50% de todos los bits transmitidos. Esta tarea es parte de las operaciones de post-procesado clásico de la clave cruda. Notemos que hay tres elecciones aleatorias durante el proceso: la de la base en la cual preparar el bit, la del bit a enviar y la de la base en la que se mide (Fig. 3).

Este procedimiento permite a Alice y Bob obtener una lista única de bits aleatorios (la clave cruda), pero ¿cómo es que este procedimiento da seguridad? Supongamos que un espía (Eve, en la jerga del criptólogo) mide el estado de los fotones transmitidos por Alice y reenvía nuevos fotones a Bob con el estado medido. Las bases de preparación y detección se intercambian al final del protocolo, por lo que Eve las desconoce durante el mismo, y debe "adivinar". En este proceso Eve utilizará la base incorrecta aproximadamente el 50% de las veces, en cuyo caso enviará a Bob un bit preparado en la base incorrecta. Entonces, cuando Bob mida (con la base correcta) un qubit reenviado, preparado en la base in-

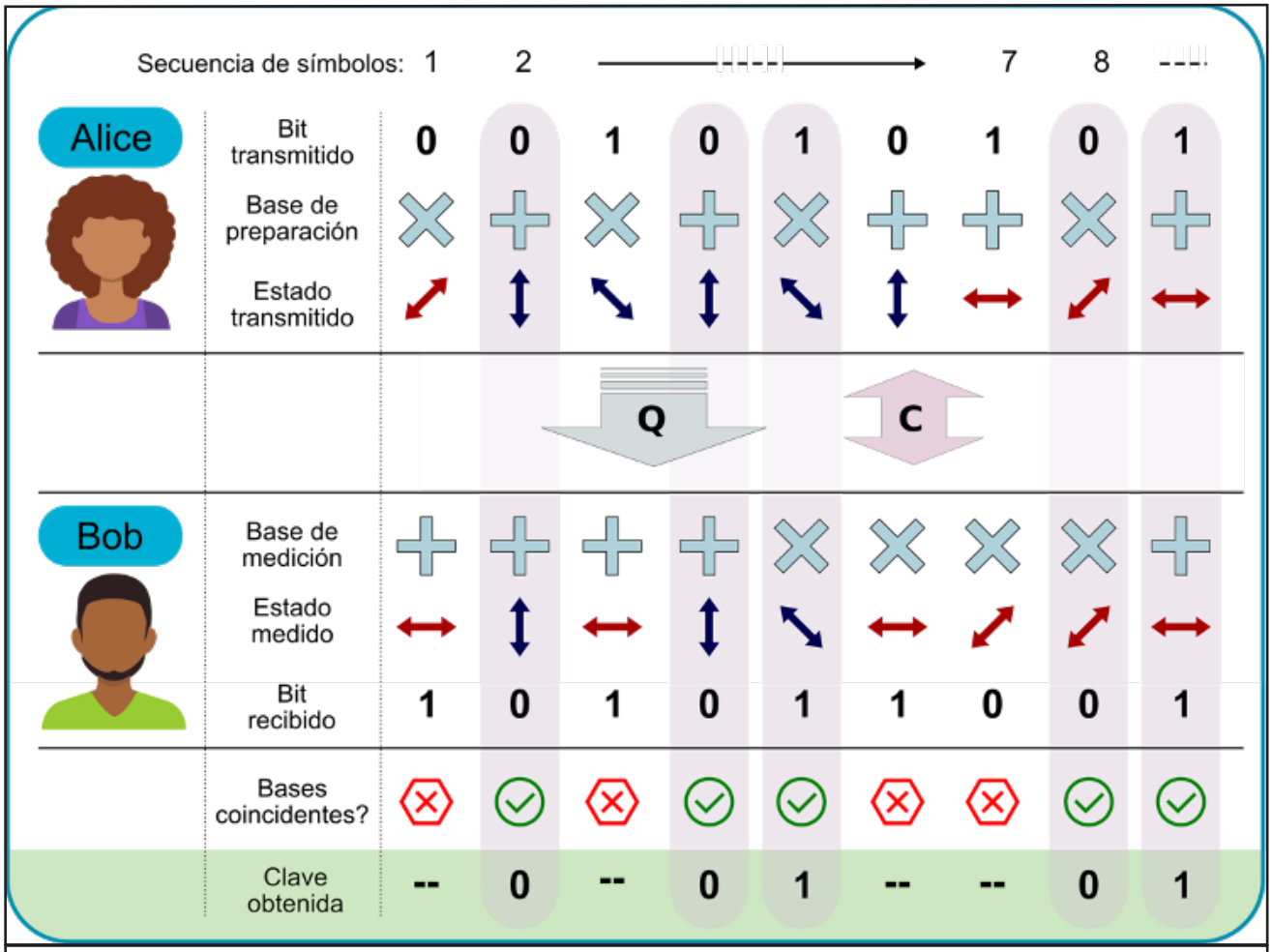

Figura 3. *En el protocolo BB84 los bits a preparar y medir se codifican en dos posibles bases; en la figura se usan la base computacional (+) y la diagonal (×). El intercambio comienza cuando Alice elige aleatoriamente un bit de la clave y una base en la cual prepararlo y lo envía a Bob a través del canal cuántico (Q); el estado transmitido puede ser uno entre cuatro posibles estados. Bob a su vez elige una base en la cual medir el estado recibido y obtiene como resultado un 0 o un 1. Posteriormente, a través de un canal clásico (C), público y autenticado, intercambian las bases usadas por el canal clásico y descartan los eventos en los cuales las bases no coincidieron. Con los bits conservados de las instancias de bases coincidentes se arma la clave cruda. Parte de esta clave se sacrifica para determinar la tasa de error (Quantum Bit Error Rate, QBER) intrínseca del sistema, y el resto se post-procesa para eliminar errores y amplificar la privacidad. La presencia de un espía Eve se manifiesta cuando éste interrumpe el canal, mide el estado preparado por Alice y lo reenvía a Bob. Como Eve desconoce la base de preparación, en promedio la mitad de las veces prepara un estado en la base incorrecta, incrementando el QBER.*

correcta, habrá un 25% de probabilidad de que mida el valor incorrecto. Por lo tanto, cualquier espía en el canal cuántico indefectiblemente introduce una alta tasa de error, que Alice y Bob pueden detectar comunicando un número suficiente de bits de paridad de sus claves a través del canal clásico abierto. Entonces, no sólo es probable que la versión de la clave de Eve sea 25% incorrecta, sino que el hecho de que alguien esté "pinchando" el canal a escondidas será evidente para Alice y Bob.

Una vez finalizada la sesión, y después de realizar otras tareas de post-procesamiento clásicas como corrección de errores, y amplificación de la privacidad, Alice y Bob cuentan con una clave aleatoria, sólo compartida entre ellos. Con esta clave podrán por ejemplo, encriptar un mensaje usando un protocolo de clave simétrica teóricamente seguro como One Time Pad.

Con algunas variaciones, lo expuesto anteriormente es la esencia de todos los protocolos de QKD: se basa en el uso de bases conjugadas para introducir aleatoriedad en los resultados de las mediciones, y en la emisión y detección de un único fotón (un sistema cuántico individual). Esta última condición es crítica, porque la seguridad está garantizada por la imposibilidad de clonar (copiar fielmente) un estado cuántico (Wooters, 1982). En la medida que el bit de la clave esté codificado en un ensamble de estados (muchas copias, como en el caso de un pulso de luz intenso), un espía podría tomar una muestra de ese ensamble, por ejemplo con un separador de haz, para separar algunos de estos fotones y obtener información sin alterar el estado de los fotones remanentes. Si la información está codificada en un único fotón, esta operación no es posible.

El protocolo BB84 es conceptualmente bastante simple, y asume que el estado usado para codificar cada símbolo es el de un fotón único. Esto es, un estado de Fock, con número de fotones N bien definido (en este caso, N=1), sin dispersión. Esta condición es difícil de implementar experimentalmente, por lo que se recurre a aproximaciones físicamente realizables. La más simple (y la más usada) es utilizar los llamados estados coherentes atenuados. Las fluctuaciones de intensidad de un estado coherente con valor medio μ de fotones definen su estadística, que obedece a una distribución P(x=n) de Poisson. Por lo tanto la varianza del número de fotones de un estado coherente es igual al valor medio. Al usar estados coherentes atenuados se reduce la probabilidad de tener estados multifotónicos (que atentan contra la seguridad del protocolo), pero también aumenta la probabilidad de tener estados vacíos: por ejemplo para μ=0.1 la probabilidad de que se codifique un símbolo en un estado con n=0 es P(x=0)=0.905, al tiempo que la probabilidad de codificar un símbolo en un estado multifotónico es P(x>1)=0.005.

Pero eso no es todo; los estados coherentes tienen una fase global bien definida, que un espía podría explotar para realizar ataques coherentes y ganar información, por lo que además es necesario realizar una aleatorización de la fase, para transformar cada estado coherente en una mezcla estadística de estados de Fock (Lo, 2005). Todos los protocolos que usan estados coherentes atenuados como aproximación a fotones únicos deben implementar esta aleatorización de la fase. Estas son deficiencias no del protocolo en sí, sino de las particularidades de la implementación.

■ OTROS PROTOCOLOS

Desde que Bennett y Brassard presentaron su protocolo, se han propuesto varios otros protocolos, usando distintos tipos de fuentes de luz y/o de configuraciones del canal cuántico. La idea aquí no es hacer un listado completo de ellos sino mencionar los que proponen variaciones relevantes o implican alguna mejora sustancial.

En 1991 Arthur Ekert propuso un protocolo basado no en fotones individuales, sino en estados con una propiedad particular, el entrelazamiento: Alice y Bob deben compartir un par de estados entrelazados como recurso previo, por ejemplo usando un aparato que cada vez que se quiere generar un símbolo, prepara el estado $|\psi\rangle = 1/\sqrt{2}\ (|H\rangle_A |H\rangle_B + |V\rangle_A |V\rangle_B)$ (Ekert, 1991). Para generar la clave Alice y Bob eligen aleatoriamente las bases en las que medirán localmente la polarización. Para monitorear la seguridad, miden las correlaciones obtenidas, que deben ser compatibles con las prescritas por las desigualdades de Bell (Bell, 1966), ver "Test de Bell" en el glosario.

En el año 2003 se propuso una variación al protocolo BB84 que solucionaba el problema de ataques sobre el número de fotones, al que son susceptibles todos los protocolos que usan estados coherentes atenuados: el protocolo de estados señuelo (*Decoy State* QKD) agrega una variación en la intensidad de los estados emitidos, a partir de la cual se puede detectar a un espía sofisticado que esté explotando la vulnerabilidad de los estados multifotónicos. Es actualmente el protocolo de QKD más ampliamente implementado.

Device-Independent QKD (DI-QKD) es una estrategia de diseño e implementación de protocolos de QKD a partir de la cual la seguridad no se basa en la confianza que se tiene sobre los dispositivos (cuánticos), sino en la violación de una desigualdad de Bell, sin la necesi-

dad de conocer el funcionamiento interno de los dispositivos, ni los de preparación de estados ni los de medición. Sin embargo DI-QKD es poco práctico y difícil de implementar experimentalmente con la tecnología actual especialmente para distancias largas (Zapatero, 2019): requiere poder realizar mediciones de Bell *loophole-free*, separación entre estaciones sin conexión causal y detectores de alta eficiencia.

El enfoque de *Measurement Device-Independent* QKD (MDI-QKD) se basa en la misma filosofía pero relaja condiciones sobre la preparación de estados (que asume casi perfecta) y en esa situación elimina todas las vulnerabilidades generadas en la implementación de la detección de estados cuánticos (pero no las de preparación), para así simplificar el montaje y obtener tasas de generación de clave de uso práctico (Lo, 2012). A pesar de ser realizables en forma práctica, los protocolos de MDI-QKD requieren la interferencia entre dos fotones (indistinguibles) generados independientemente, uno por Alice y otro por Bob, y el proceso de interferencia (la medición) se realiza en un nodo intermedio que puede no ser confiable. Este sigue siendo un requerimiento un tanto demandante (Fig. 4).

En 2018 una variación ingeniosa de la arquitectura de sistemas MDI-QKD dio lugar a los llamados protocolos de *Twin-Field* QKD (TF-QKD), en los cuales la interferencia que ocurre en el nodo intermedio no es de dos fotones sino de uno. De ahí el nombre del protocolo: Alice y Bob no envían "fotones" indistinguibles, sino campos indistinguibles (gemelos). Existen distintas variantes

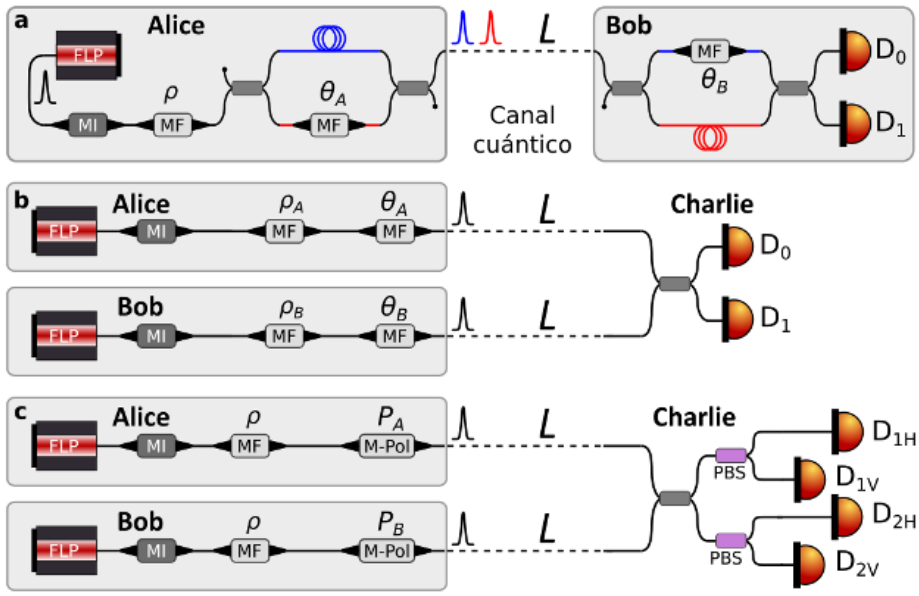

Figura 4. *Diagrama de algunos protocolos mencionados. a) Decoy state-QKD con codificación de fase: Una fuente de luz pulsada (FLP) genera pulsos con estados coherentes y un primer modulador de fase (MF) aplica una fase aleatoria* ρ *para randomizar la fase. Un segundo modulador dentro de un interferómetro desbalanceado codifica cada estado aplicando una fase* θ_A. *Los estados se transmiten una distancia L y Bob detecta usando un interferómetro desbalanceado equivalente, y una base de detección seleccionada definiendo* θ_B. *b) Twin-field QKD: Alice y Bob transmiten ambos, usando FLPs que emiten estados indistinguibles. Cada uno de ellos se constituye en el brazo de un interferómetro. Alice (Bob) prepara un pulso óptico con fase aleatoria discreta* $\rho_A(\rho_B)$ *y una fase de codificación de base y bit* $\theta_A(\theta_B)$ *y lo transmite. Charlie superpone ambos pulsos en un separador de haz y mide. Luego de anunciar cuál detector disparó, los usuarios revelan los valores de bases usadas en* $\theta_A(\theta_B)$ *(pero no la fase de codificación del bit), y las fases* $\rho_A(\rho_B)$. *La clave se construye con las ejecuciones en las que las fases* ρ_A *y* ρ_B *coinciden. c) MDI-QKD con codificación en polarización. Alice (Bob) prepara su estado de polarización* P_A (P_B) *usando moduladores de polarización (M-Pol). Charlie superpone ambos pulsos en un separador de haz por polarización (PBS) en cada salida. Se usan cuatro detectores para obtener en cada evento una medición de Bell (esto sucede cuando dos detectores en polarizaciones ortogonales se disparan). Todos los otros eventos se descartan. El modulador de intensidad (MI) genera estados señuelo en todos los casos. Figura inspirada en (Lucamarini, 2018).*

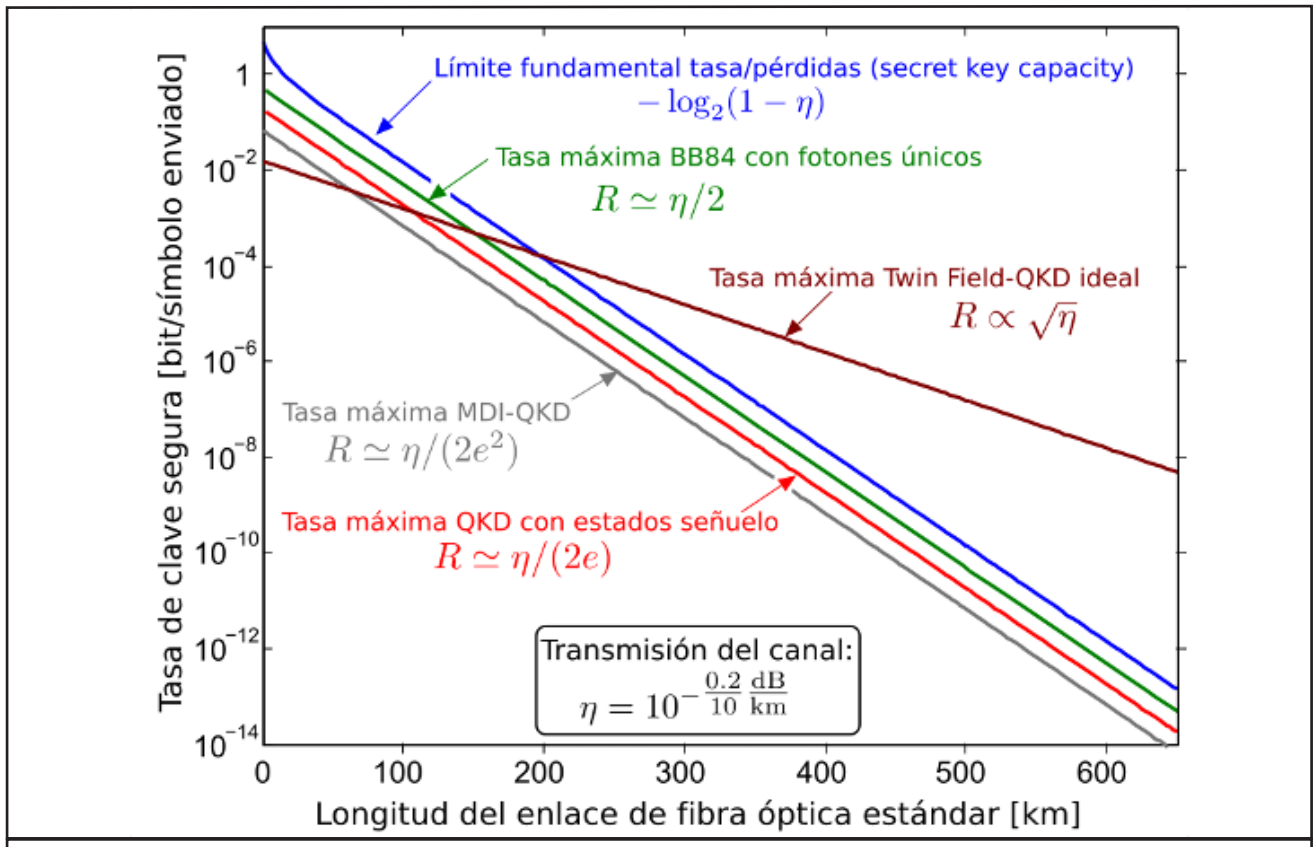

Figura 5. *Cotas teóricas del límite tasa-distancia para sistemas QKD basados en fibra óptica. El límite fundamental o Secret Key Capacity corresponde al de un canal cuántico de pérdidas (erasure channel). Para altas pérdidas (η≃0) este límite escala como 1.44η. La transmisión del canal está dada por la atenuación del largo del enlace de fibra óptica. Los protocolos Twin-Field, al ubicar el nodo de medición en el medio de las dos estaciones, escalan como √η. El protocolo MDI también ubica el nodo en un punto intermedio pero requiere interferencia de dos fotones, con lo que logra una ley de escala similar a los protocolos convencionales. Gráfico adaptado de (Lucamarini, 2018; Pirandola, 2017).*

de estos protocolos, y debido a que la medición se realiza en el punto intermedio entre Alice y Bob, y que es un proceso de interferencia de un único fotón, estos protocolos permiten duplicar el límite de distancia entre estaciones para una tasa de clave segura fija, respecto de los protocolos tradicionales (Lucamarini, 2018; Rusca, 2024). Técnicamente es un protocolo más complejo de implementar que MDI, debido a que es necesario mantener un control preciso de la fase óptica entre Alice y Bob sobre toda la longitud del enlace, pero la tasa de clave segura extraíble escala mucho mejor con la atenuación (longitud) del enlace (Fig. 5).

Por último, hay que mencionar que los protocolos descritos se basan en estados cuánticos de variable discreta. También existen protocolos de QKD basados en estados de variable continua (típicamente las cuadraturas del campo electromagnético): *Continuous-variable* QKD (CV-QKD) aparecen actualmente como una alternativa floreciente, debido a su compatibilidad con la industria de las telecomunicaciones, por ejemplo usando láseres continuos y receptores coherentes para preparación y medición respectivamente. Un compendio de protocolos, avances actuales y perspectivas de CV-QKD se puede leer en (Zhang, 2024).

■ ESTADO DEL ARTE INTERNACIONAL Y LOCAL

En la actualidad existen dos escenarios principales en los cuales se implementan protocolos de QKD: entre estaciones vinculadas por línea de visión en enlaces Tierra-satélite (y con el mismo esquema de trabajo se planean comunicaciones entre satélites) donde el canal cuántico se constituye principalmente en el espacio exterior, y en enlaces de telecomunicaciones por fibra óptica.

Las implementaciones de QKD en fibra óptica son las que han tenido mayor desarrollo durante los últimos 15 años. La codificación

elegida mayoritariamente es la de time-bin, debido a que es robusta frente a perturbaciones térmicas y mecánicas de la fibra óptica. Con protocolos tradicionales como BB84 o de estados señuelo se han logrado tasas de intercambio de clave segura de hasta 1 Mbit/s sobre un enlace de 20 km de fibra óptica (Dixon, 2008). Para una longitud de fibra de 310 km la mejor tasa de distribución es de 12.7 kbit/s (Korzh, 2015). Y el récord de longitud para esta clase de protocolos es de 405 km, pero con una tasa de generación de clave de sólo 6.5 bit/s (Boaron, 2018). Al no admitir amplificación de la señal (que destruye la coherencia de los estados preparados), existe un compromiso insalvable entre longitud del enlace (atenuación) y tasa máxima extraíble de clave segura. La aparición de la propuesta de TF-QKD significó la realización de varias implementaciones de este protocolo, que al disponer de la etapa de medición en un punto intermedio entre ambos extremos, permite duplicar la distancia del enlace. Entre los experimentos más destacables de este enfoque a la distribución de claves están el realizado en el *Key Laboratory of Quantum Information* dependiente de la Academia China de Ciencias, en el que se pudo distribuir clave segura a una tasa de 44 bit/s sobre un canal de 610 km, y tolerar pérdidas en distancias de hasta 830 km (140 dB de pérdidas) (Wang, 2022) y el de un grupo liderado por investigadores del Istituto Nazionale di Ricerca Metrologica (INRIM, Torino, Italia) en el que usando técnicas interferométricas derivadas de la metrología de frecuencias pudieron simultáneamente distribuir clave y controlar la fase global del canal completo a lo largo de una fibra desplegada en campo de 206 km de longitud y 65 dB de pérdidas (Clivati, 2022).

Por otro lado, en el año 2017, como parte del programa *Quantum Experiments at Space Scale* un grupo de investigadores liderados por Jian-Wei Pan de la Universidad de Ciencia y Tecnología de China pudo implementar en forma exitosa un protocolo BB84 con estados de polarización entre el satélite de investigación de baja órbita Micius y estaciones terrenas en China y en Austria (Liao, 2017). A la fecha es el único satélite operativo declarado dedicado a demostrar tecnologías cuánticas. El 28 de junio de 2025 la empresa Seal SQ lanzó el satélite WiSeSat 3, con el objetivo de habilitar comunicaciones satelitales con seguridad post-cuántica.

En Argentina, el laboratorio de Óptica Cuántica de CITEDEF (ubicado en Villa Martelli, provincia de Buenos Aires) trabaja desde el año 2011 en la implementación de protocolos de QKD, primero en enlaces horizontales por aire, y a partir de 2013 en enlaces por fibra óptica (Magnoni, 2017; López Grande, 2018; Morales, 2023). (Fig. 6)

■ OTRAS APLICACIONES DE FOTONES COMO SISTEMAS CUÁNTICOS. INTERFEROMETRÍA, FORMACIÓN DE IMÁGENES, RADIOMETRÍA

La fotónica cuántica no sólo tiene aplicaciones tecnológicas en el campo de las comunicaciones. En los últimos años, la metrología cuántica emergió como un enfoque poderoso para obtener mediciones con precisión que supera a la de estrategias clásicas. El manejo y detección de fotones a nivel individual ha alcanzado un estadío de desarrollo sin precedentes. Estos logros tecnológicos, junto con el diseño de protocolos que explotan en forma efectiva el recurso cuántico, permiten la estimación mejorada de parámetros ópticos como fase e intensidad, empujando la sensibilidad de las mediciones por encima de los límites

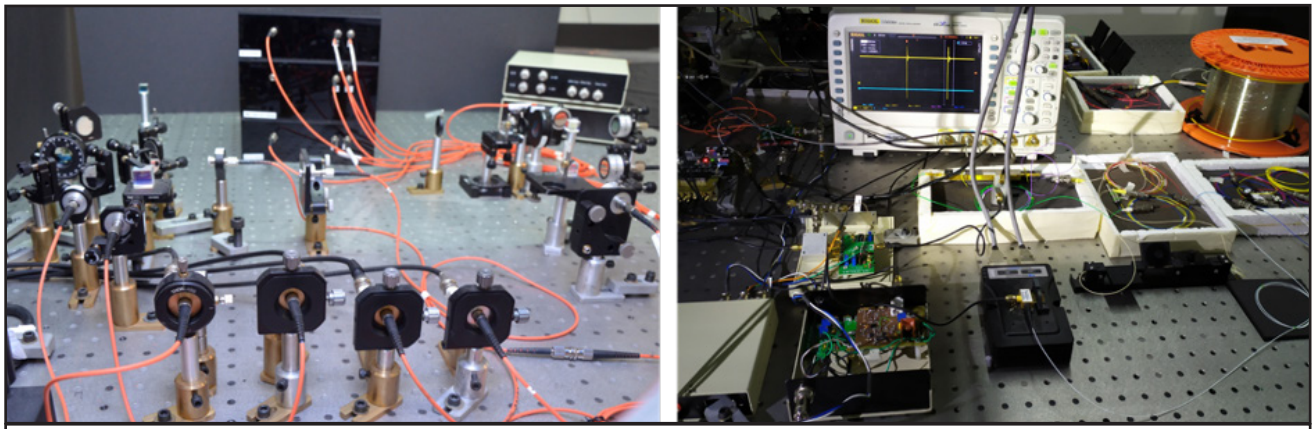

Figura 6. *Realizaciones de protocolos de QKD en el laboratorio de Óptica Cuántica del DEILAP (CITEDEF-CONICET). Izquierda: detalle del arreglo de detección (Bob) de un experimento con propagación por aire. Derecha: implementación en canal de fibra óptica con codificación en time-bin.*

clásicos. Las aplicaciones de la metrología cuántica con fotones es diversa, abarcando desde la detección de ondas gravitatorias (LIGO, 2011) a la formación de imágenes de muestras biológicas; ver por ejemplo (Couteau, 2023). La metrología cuántica fotónica manipula estados cuánticos de la luz para sensar sistemas físicos (Polino, 2020).

■ ESTIMACIÓN DE LA FASE ÓPTICA

Los fotones son portadores ideales de información cuántica: son robustos, se los puede manipular fácilmente, y se los puede generar y detectar con alta precisión usando las tecnologías actuales. Una de las tareas más relevantes del sensado cuántico con fotones es la de la estimación de una fase óptica. Para detectar un corrimiento de fase se requiere el uso de un interferómetro: el parámetro de interés se codifica durante la evolución del estado *sonda*, y la información se extrae mediante alguna medición adecuada a la salida del interferómetro. El interferómetro óptico más básico es un dispositivo de dos modos, cuya diferencia relativa de fase es desconocida (Fig. 7). Esta fase desconocida puede diseñarse para codificar información sobre diferentes cantidades de interés en diferentes contextos. Por ejemplo, puede estar relacionada con la distancia, birrefringencia, ángulos, o concentración de alguna muestra (KAGRA, 2013; Rozema, 2014).

Sin correlaciones cuánticas, la mínima incerteza de fase $\Delta\phi$ alcanzable usando N fotones está dada por el **Límite de *Shot-Noise*** (SNL): $\Delta\phi \sim 1/\sqrt{N}$. La metrología cuántica, sin embargo, permite mejorar la sensibilidad: haciendo uso de fenómenos como el entrelazamiento, es posible alcanzar el **Límite de Heisenberg**: $\Delta\phi \sim 1/N$ (Giovannetti, 2004). De esta manera, utilizando fotones entrelazados se puede alcanzar súper-sensibilidad en la estimación de fase, es decir, mediciones de fase con una incerteza por debajo del SNL. Los estados entrelazados multifotónicos, como los estados *N00N*, pueden alcanzar esta súper-sensibilidad y, en principio, pueden saturar el límite de Heisenberg.

■ MEDICIONES DE INTENSIDAD

Otra de las aplicaciones intensamente estudiada es la mejora en la precisión para la estimación de la absorción óptica de una muestra, comparada con una medición usando luz clásica. La incerteza de esta medición está dada por una combinación de las fluctuaciones aleatorias inherentes al haz de prueba (que en un haz de luz clásico están caracterizadas por una distribución de Poisson), y por la naturaleza estocástica de la interacción entre la luz y la materia en el objeto de estudio. Esquemas para estimar la transmisión de una muestra generalmente consisten en medir la atenuación de la intensidad de un haz de luz que se propaga a través de la misma. Con una fuente de pares de fotones correlacionados, se puede usar uno de los fotones para incidir sobre la muestra, y su par correlacionado para registrar (y eliminar) las fluctuaciones de intensidad del haz, para obtener medidas con ruido por debajo del denominado *shot-noise*. La aplicación de esta técnica y otras equivalentes en el área de las ciencias biológicas permite sobrepasar

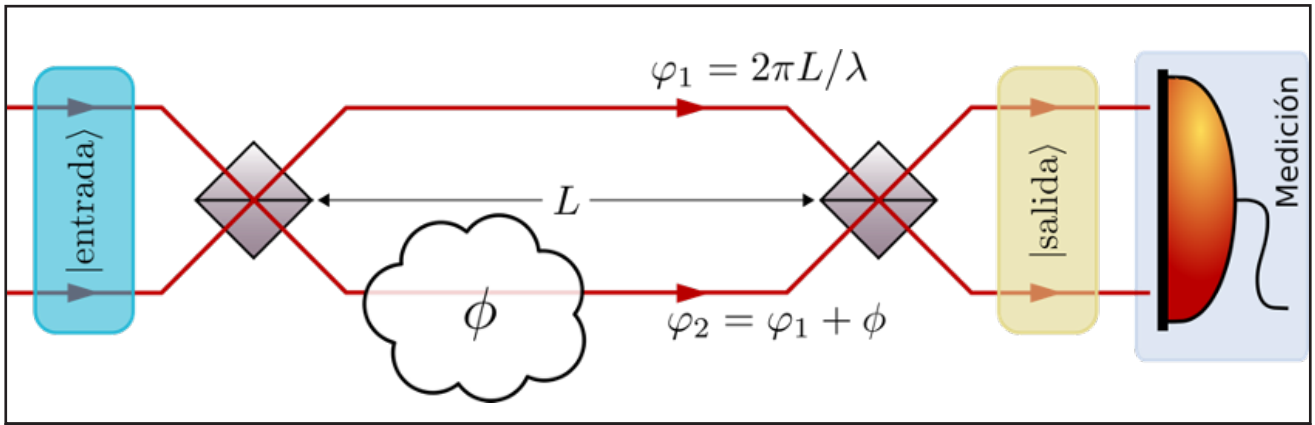

Figura 7. *Representación esquemática de un interferómetro de Mach–Zehnder para la estimación de una fase interferométrica. Un estado sonda es enviado al dispositivo a través de las entradas de un separador de haz, donde se crea un estado de superposición de dos modos. Ambos modos acumulan una fase proporcional al largo L del camino recorrido. Además, el estado interactúa con un mecanismo donde se codifica una diferencia de fase relativa ϕ entre ambos modos. Esta fase puede estimarse a partir de mediciones de un observable específico a la salida, después de la recombinación coherente de los dos modos en el divisor de haz de salida.*

los límites clásicos de precisión por unidad de intensidad (Taylor, 2016; Berchera, 2019; Moreau, 2019).

■ FUENTES DE LUZ NO CLÁSICA

Finalmente, comentamos que una tecnología asociada a las aplicaciones fotónicas en comunicaciones y metrología, y necesaria para alguna de estas aplicaciones es la ingeniería de fuentes de fotones únicos. Las fuentes de fotones únicos a demanda pasan a ser un activo valioso para dispositivos basados en óptica cuántica, ya que de por sí exhiben una estadística de emisión sub-Poissoniana, una característica clave en aplicaciones de metrología cuántica (Berchera, 2019). Además, estos estados son de importancia crítica para la seguridad de protocolos de QKD, a menos que se apliquen técnicas de estados señuelo. Por estos motivos, hay un gran esfuerzo global destinado a desarrollar y caracterizar fuentes cuasi-óptimas de fotones únicos. Los dos enfoques más relevantes para estas realizaciones se clasifican en fuentes determinísticas (emisores de fotones individuales, como átomos, iones o moléculas, *quantum dots* o centros de nitrógeno-vacancia (Tomm, 2021)) y fuentes probabilísticas (generación de pares de fotones mediante procesos no lineales como conversión paramétrica espontánea o *four-wave mixing*) (Adam, 2014; Meyer-Scott. 2020).

El Laboratorio de Óptica y Fotónica junto con el Laboratorio de Detectores de Bajo Umbral y sus Aplicaciones, ambos del Departamento de Física, de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires, usando detectores de imagen de tecnología skipper-CCD, con resolución de número de fotones y ruido de lectura por debajo de los 0.2e–, realizaron experimentos sobre obtención de imágenes y reconstrucción de frentes de onda con resolución por encima del shot-noise en condiciones de baja iluminación (Pears Stefano, 2023; Pears Stefano, 2024). El laboratorio de Óptica Cuántica de CITEDEF, además de su trabajo en comunicaciones cuánticas, viene desarrollando desde 2019 investigaciones en metrología cuántica, abordando tanto cuestiones fundamentales como posibles aplicaciones. Se han realizado estudios teóricos y experimentales sobre el rol de la indistinguibilidad en la estimación de una fase interferométrica (Knoll, 2019; Knoll, 2023); se trabajó en el desarrollo y caracterización de una fuente de pares de fotones múltiples para aplicaciones de interferometría (Ma, 2025); y en el análisis y desarrollo de una fuente de fotones multiplexada para medidas de absorción con sensibilidad mejorada (Magnoni, 2021; Magnoni, 2024).

■ CONSIDERACIONES FINALES

La fotónica cuántica, que se basa en el uso de fotones individuales como sistemas cuánticos, desempeña un papel fundamental en el avance de las tecnologías cuánticas. Aun cuando los fotones no son los sistemas más adecuados para tareas de computación cuántica, resultan ser especialmente idóneos para aplicaciones en comunicaciones seguras, y también para metrología de precisión.

Como hemos visto, las comunicaciones cuánticas seguras aprovechan las leyes de la mecánica cuántica para generar claves criptográficas y transmitir información de manera teóricamente inviolable. En estas aplicaciones, los fotones, debido a su interacción débil con el entorno, su facilidad de preparación y su carácter de sistemas en movimiento, dominan el escenario. La posible llegada del "Q-Day", cuando las computadoras cuánticas puedan romper los protocolos de encriptación actuales (clásicos) y las infraestructuras digitales críticas, representa un cambio de paradigma en la seguridad de la información. Estados y empresas deberán reinventar sus estrategias de protección, posiblemente adoptando enfoques orientados a la comunicación cuántica. Los protocolos de QKD evolucionaron en forma muy dinámica desde sus primeras implementaciones prácticas a principios del milenio, hasta llegar a cubrir distancias superiores a los 500 km en fibra óptica y a cuadruplicar esta distancia para enlaces satelitales.

Por otro lado, el sensado óptico es una herramienta fundamental en muchas disciplinas, debido a su capacidad para detectar y medir luz sin contacto directo, su inmunidad a interferencias electromagnéticas y la facilidad para preparar y leer los estados de las sondas. Estas ventajas, combinadas con las propiedades únicas de los fotones —como la coherencia, la interferencia cuántica y el entrelazamiento— abren nuevas posibilidades para realizar mediciones ultrasensibles de parámetros físicos, superando los límites impuestos por la física clásica.

Una tecnología emergente que acompaña esta tendencia es la de los chips ópticos cuánticos, que integran componentes como guías de onda, divisores de haz y detectores para manipular fotones individuales. Su desarrollo resulta crucial para impulsar tanto las comunicaciones seguras como las aplicaciones de sensado de alta precisión (Katiyi, 2025).

En los últimos años, a nivel mundial, se puede observar una transición del desarrollo a la implementación de tecnologías cuánticas en general, y en particular en las que usan fotones como recurso cuántico. Innovaciones recientes apuntan

hacia la construcción de sistemas cuánticos más seguros y confiables. Aunque las instituciones académicas siguen siendo las principales incubadoras de avances, en estos años varias de las transformaciones más decisivas han sido impulsadas por empresas tecnológicas, más que por acciones gubernamentales. Según la consultora McKinsey & Company, se estima que para 2035 el mercado global de comunicaciones cuánticas podría alcanzar entre 11.000 y 15.000 millones de dólares, mientras que el de sensado cuántico, que abarca distintas plataformas más allá de los fotones, oscilaría entre 7.000 y 10.000 millones (Soller, 2025).

A modo de conclusión, podríamos decir que "esto recién empieza". Efectivamente, estamos en un momento crucial donde la evolución de las tecnologías cuánticas, impulsada por sectores tanto académicos como industriales, promete transformar radicalmente nuestra forma de comunicarnos, medir y proteger (¡y procesar!) la información. La frontera cuántica nos invita a seguir explorando y preparando a la sociedad para un futuro cada vez más dependiente de estas innovaciones. En este contexto, para un país como Argentina con una economía en desarrollo, pero aún con una valiosa base de conocimiento científico y tecnológico, resulta estratégico promover desarrollos de escala contenida pero de alto impacto. Estos esfuerzos permiten -al menos- sostener capacidades críticas, ofrecer valor agregado en la cadena tecnológica global y preservar una mínima soberanía tecnológica, y autonomía en la gestión de datos sensibles y los sistemas que los procesan.

■ GLOSARIO

AES: *Advanced Encryption System*; sistema de encriptación usado habitualmente para proteger redes inalámbricas, encriptar archivos y dispositivos de almacenamiento, proteger aplicaciones de mensajería como Whatsapp, y asegurar transacciones bancarias entre varias otras aplicaciones.

Amplificación de privacidad: Proceso que transforma una clave criptográfica inicial, que podría ser parcialmente conocida por un espía, en una clave final que es segura y completamente desconocida para cualquier adversario.

Autenticación: Proceso de verificar la identidad de un usuario, dispositivo, o fuente de datos para asegurar que es lo que pretende ser. Es una parte crucial de la seguridad de la información, que construye confianza en el proceso específico de comunicación. Éste confirma no sólo el origen de los datos sino además si han sido alterados o no durante la transmisión o el almacenamiento.

Base vectorial: Conjunto de vectores linealmente independientes que puede generar cualquier otro vector del espacio vectorial.

Clave criptográfica: Lista de caracteres o símbolos, usualmente generados en forma aleatoria, usada junto con un algoritmo apropiado para encriptar o desencriptar datos.

Coherencia óptica: Medida de la correlación de fase de distintas ondas de luz, que permite que ocurra el fenómeno de interferencia.

Conversión paramétrica espontánea: SPDC por sus siglas en inglés (*Spontaneous Parametric Down-Conversion*) es un proceso no lineal instantáneo que convierte un fotón de energía mayor (llamado bombeo) en un par de fotones (llamados *signal* e *idler*) de menor energía, respetando las leyes de conservación de energía y momento. Es un proceso importante en óptica cuántica, que permite generar pares de fotones correlacionados en uno o más grados de libertad (energía, polarización, momento lineal), o incluso pares de fotones en estados entrelazados.

Ensamble: Número grande de copias de un sistema, consideradas en conjunto, que usualmente se usa para representar el desconocimiento completo del sistema, asignando probabilidades a los distintos posibles estados en que éste se pueda encontrar.

Espacio de Hilbert: En el marco de la mecánica cuántica, un espacio de Hilbert es una estructura matemática usada para representar todos los posibles estados de un sistema cuántico, y las manipulaciones (operaciones) que pueden ser realizadas sobre esos estados.

Estados coherentes: Estados cuánticos específicos, o soluciones, del oscilador armónico cuántico, que replican el comportamiento oscilatorio de un oscilador armónico clásico. A menudo se describen como los estados cuánticos "más parecidos" a un estado clásico, porque su comportamiento es similar al de las ondas electromagnéticas clásicas. Se caracterizan por tener una mínima incerteza en posición y momento. En un estado coherente fotónico, el número (cantidad) de fotones del estado tiene una distribución de Poisson $P(x=n)=e^{-n}/n!$, por lo que la dispersión o incerteza en el número de fotones es igual a la raíz cuadrada del valor medio m de fotones del estado.

Estados de Fock: Un estado fotónico de Fock representa un estado cuántico de la luz con un número definido de fotones. Estos estados son fundamentales en óptica cuántica y tienen funciones críticas en tareas de procesamiento cuántico de la información, metrología cuántica y otras tecnologías cuánticas.

Estado entrelazado: Estado cuántico específico en el que dos o más partículas están correlacionadas entre sí de forma tal que el estado cuántico de cada partícula constituyente no puede ser descrito en forma independiente del resto de las partículas del sistema, aún cuando las mismas estén arbitrariamente distanciadas. Matemáticamente, los estados entrelazados no pueden ser expresados como un producto simple de estados de partículas individuales.

Factorización: El proceso de reducir un número o una expresión al producto de sus factores.

Fase óptica: Propiedad de la luz o en general de una onda electromagnética que describe la posición de una onda respecto de su ciclo ondulatorio a un determinado tiempo.

Four-wave mixing: Fenómeno de intermodulación no lineal entre cuatro ondas que permite obtener suma de frecuencias, resta de frecuencias o dos ondas de frecuencias distintas al excitar al sistema no lineal con dos ondas de la misma frecuencia. En óptica cuántica es de interés al permitir obtener pares de fotones en sistemas en los que la conversión paramétrica no es posible debido a la simetría del material.

Función de onda: Descripción matemática del estado cuántico de un sistema. Es una función a valores complejos que da información sobre la probabilidad de encontrar un sistema cuántico en alguna posición particular o con un momento particular.

Indistinguibilidad: En el marco de la mecánica cuántica, partículas indistinguibles son las que no pueden ser distinguidas entre sí, aún en principio. Las partículas pueden ser distinguibles debido a diferencias inherentes como masa, frecuencia, carga eléctrica, spin, etc, pero aún cuando las partículas tuvieran las mismas propiedades físicas, existe posibilidad de incluir distinguibilidad a partir de sus trayectorias, o cualquier otra "etiqueta" que permita saber de qué camino proviene cada una, o con qué retardo llegan a un cierto punto.

Láser: Dispositivo que emite luz mediante el proceso de amplificación óptica basada en la emisión estimulada de radiación electromagnética; generalmente emite en una región muy estrecha del espectro electromagnético, y con un haz colimado y de baja divergencia.

Modos transversales (de la radiación electromagnética): También conocidos como Modos Electromagnéticos Transversos (TEM), describen los patrones del campo eléctrico en una onda perpendiculares a la dirección de propagación de la onda. Son relevantes para entender el comportamiento de las ondas con condiciones de contorno definidas, como guías de onda, fibras ópticas o cavidades resonantes como la de un láser.

Polarización: Propiedad de las ondas electromagnéticas (en particular de la luz) de oscilar en un plano específico, transversal a la dirección de propagación. La polarización es una propiedad cuántica de la luz, que se manifiesta en los 'cuantos' o partículas indivisibles de la misma, es decir en los fotones.

QBER (*Quantum Bit Error Rate*): Magnitud que cuantifica la tasa de error presente en un sistema de distribución cuántica de claves. Específicamente, mide la 'descorrelación' entre estados cuánticos transmitidos y recibidos, es decir, cuán a menudo Bob recibe un bit diferente del que Alice envió. El QBER es una medida crucial para evaluar la seguridad de un protocolo de QKD.

QKD (*Quantum Key Distribution*): Método de comunicación segura que emplea propiedades de los sistemas cuánticos para crear y distribuir claves criptográficas.

Qubit: bit cuántico, es la unidad básica de información en la computación cuántica, equivalente a un bit binario en el marco de la computación clásica. A diferencia de un bit clásico que sólo puede valer 0 o 1, un qubit puede existir en una superposición de estados cuánticos.

RSA: Protocolo de encriptación de clave pública desarrollado en 1973 por Rivest, Shamir y Adleman, que se usa actualmente -entre otras aplicaciones- para garantizar la seguridad en el protocolo de navegación segura por internet HTTPS, y en firmas digitales.

Shot noise: aleatoriedad inherente en la emisión y detección de luz debido a su naturaleza cuántica. Proviene del comportamiento discreto de los fotones y la subsecuente aleatoriedad de la llegada de esos fotones al detector. El *shot noise* aparece cuando las detecciones son independientes y aleatorias, con varianza igual a la media, lo que usualmente se asocia a un proceso de Poisson. Fuentes de luz con distinta estadística tendrán ruidos asociados menores o mayores, según su varianza.

Test de Bell (o test de desigualdad de Bell, o experimento de Bell): Es una clase de experimentos de física diseñados para poner a prueba los principios de la mecánica cuántica contra teorías de realismo local. Esencialmente, buscan mostrar si el universo está mejor descrito por la mecánica cuántica o por alguna teoría basada en variables ocultas locales. Un test de Bell *loophole-free* trata de eliminar la mayor cantidad de suposiciones que podrían ser

explotadas por teorías de variables locales. Entre estas suposiciones o "*loopholes*" se destacan el de detección, el de localidad, el de memoria y el de impredictibilidad. Hasta ahora, todos los tests de Bell realizados, incluso los más sofisticados (es decir, los que se aproximan a un experimento completamente *loophole-free*), han mostrado que la naturaleza se comporta como predice la mecánica cuántica, descartando en forma efectiva la posibilidad de que variables ocultas locales puedan explicar en forma completa los fenómenos cuánticos.

Transpuesto conjugado: El transpuesto conjugado de un vector escrito en forma matricial es el resultado de intercambiar filas por columnas y de reemplazar cada elemento por su complejo conjugado.

■ REFERENCIAS

Adam, P., et al. (2014) Optimization of periodic single-photon sources. Physical Review A **90**, 053834.

Barreto Lemos, G., et al. (2022) Quantum imaging and metrology with undetected photons: tutorial. Journal of the Optical Society of America B **39**, 2200.

Bell, J.S. (1966) On the problem of hidden variables in quantum mechanics. Reviews of Modern Physics **38**, 447.

Bennett, C.H., Brassard G. (1984) Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, December 1984, 175.

Bennett, C.H., Brassard G. (1989) Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working. ACM Sigact News **20**, 78.

Berchera, I.R., Degiovanni, I.P. (2019) Quantum imaging with sub-Poissonian light: challenges and perspectives in optical metrology. Metrologia **56**, 024001.

Boaron, A., et al. (2018) Secure quantum key distribution over 421 km of optical fiber. Physical Review Letters **121**, 190502.

Chen, Y., et al. (2022) Quantum interferometric metrology with entangled photons. Frontiers in Physics **10**, 892519.

Clivati, C., et al. (2022) Coherent phase transfer for real-world twin-field quantum key distribution. Nature Communications **13**, 157.

Couteau, C., et al. (2023) Applications of single photons in quantum metrology, biology and the foundations of quantum physics. Nature Reviews Physics **5**, 354.

Defienne, H., et al. (2024) Advances in quantum imaging. Nature Photonics **18**, 1024.

Dirac, P.A.M. (1981) "The Principles of Quantum Mechanics" . Oxford University Press.

Dixon, A.R., et al. (2008) Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. Optics Express 16, 18790.

Ekert A.K. (1991) Quantum cryptography based on Bell's theorem. Physical Review Letters **67**, 661.

Giovannetti, V., et al. (2004) Quantum-enhanced measurements: beating the standard quantum limit. Science **306**, 1330.

KAGRA Collaboration (2013) Interferometer design of the KAGRA gravitational wave detector. Physical Review D—Particles, Fields, Gravitation, and Cosmology **88**, 043007.

Katiyi, A., Karabchevsky, A. (2025) Quantum photonics on a chip. APL Quantum **2**, 020901.

Katz, J., Lindell, Y. (2007) "Introduction to modern cryptography: principles and protocols". Chapman and Hall/CRC .

Knoll, L.T., Bosyk, G.M. (2023) Simultaneous quantum estimation of phase and indistinguishability in a two-photon interferometer. Journal of the Optical Society of America B **40**, C67.

L. T. Knoll, G. M. Bosyk, I. H. López Grande, and M. A. Larotonda (2019) Role of indistinguishability in interferometric phase estimation. Physical Review A **100**, 062125.

Korzh, B., et al. (2015) Provably secure and practical quantum key distribution over 307 km of optical fibre. Nature Photonics **9**, 163.

Ladd, T.D., et al. (2010) Quantum computers. Nature **464**, 45.

Liao, S., et al. (2017) Satellite-to-ground quantum key distribution. Nature **549**, 43.

LIGO Scientific Collaboration (2011) A gravitational wave observatory operating beyond the quantum shot-noise limit. Nature Physics 7, 962.

Lo, H.K., Preskill, J (2005) Phase randomization improves the security of quantum key distribution. arXiv preprint quant-ph/0504209.

Lo, H.K. et al. (2012) Measurement-device-independent quantum key distribution. Physical Review Letters **108**, 130503.

López Grande, I.H., Larotonda, M.A. (2018) Implementation of a hybrid scheme for coherent plug-and-play quantum key distribution. Quantum Information Processing **17**, 176.

Lucamarini, M., et al. (2018) Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature **557**, 400.

Ma, A., et al. (2025) Unraveling quantum phase estimation: exploring the impact of multi-photon interference on the quantum Fisher information. Quantum Science and Technology **10**, 035021.

Magnoni, A.G., Lopez Grande, I.H., and Larotonda, M.A. (2017) Free Space Decoy-state Quantum Key Distribution Implementation. Óptica Pura y Aplicada **50**, 187.

Magnoni, A.G., Knoll, L.T., and Larotonda, M.A. (2021) Scheme for sub-shot-noise transmission measurement using a time-multiplexed single-photon source. Journal of the Optical Society of America B **38**, 2502.

A.G. Magnoni, L.T. Knoll, L. Wölcken, J. Defant, J. Morales, and M.A. Larotonda. (2024) Toward an optical-fiber-based temporally multiplexed single-photon source. Physical Review A **110**, 033712.

Meyer-Scott, E., et al. (2020) Single-photon sources: Approaching the ideal through multiplexing. Review of Scientific Instruments **91**, 041101.

J. Morales, M.G. Aparicio, C.F. Longo, C.L. Arrieta, and M.A. Larotonda (2023) Optical transmitter for time-bin encoding quantum key distribution. Journal of the Optical Society of America B **40**, C15.

Moreau P.A., et al. (2019) Imaging with quantum states of light. Nature Reviews Physics **1**, 367.

Nielsen, M.A., Chuang, I.L. (2010) "Quantum computation and quantum information". Cambridge University Press.

Q. Pears Stefano, A.G. Magnoni, J. Estrada, C. Iemmi, D. Rodrigues, and J. Tiffenberg (2023) Infrared Photon-Number-Resolving Imager Using a Skipper Charge-Coupled Device. Physical Review Applied **19**, 064044.

Q. Pears Stefano, A.G. Magnoni, D. Rodrigues, J. Tiffenberg, and C. Iemmi (2024) Interferometry with few photons. Physical Review Applied **21**, 064050.

Pirandola, S., et al. (2017) Fundamental limits of repeaterless quantum communications. Nature Communications **8**, 15043.

Polino, E., et al. (2020) Photonic quantum metrology. AVS Quantum Science **2**, 024703.

Rieffel, E., Polak, W. (2000) An introduction to quantum computing for non-physicists. ACM Computing Surveys (CSUR) **32**, 300.

Rozema, L.A., et al. (2014) Scalable spatial superresolution using entangled photons. Physical Review Letters **112**, 223602.

Rusca, D., Gisin, N. (2024) Quantum cryptography: An overview of quantum key distribution. arXiv preprint arXiv:2411.04044.

Soller, H., et al. (2025) "The Year of Quantum: From concept to reality in 2025". McKinsey annual quantum technology report.

Taylor, M.A, Bowen, W.P. (2016) Quantum metrology and its application in biology. Physics Reports 615, 1.

Tomm, N., et al. (2021) A bright and fast source of coherent single photons. Nature Nanotechnology **16**, 399.

Wang, S. et al. (2022) Twin-field quantum key distribution over 830-km fibre. Nature Photonics **16**, 154.

Wiesner, S. (1983) Conjugate Coding. ACM Sigact News **15**, 78.

Wootters, W.K., Zurek, W.H. (1982) A single quantum cannot be cloned. Nature **299**, 802.

Zapatero, V., Curty, M. (2019) Long-distance device-independent quantum key distribution. Scientific Reports **9**, 17749.

Zhang, Y., et al. (2024) Continuous-variable quantum key distribution system: Past, present, and future. Applied Physics Reviews **11**, 011318.