

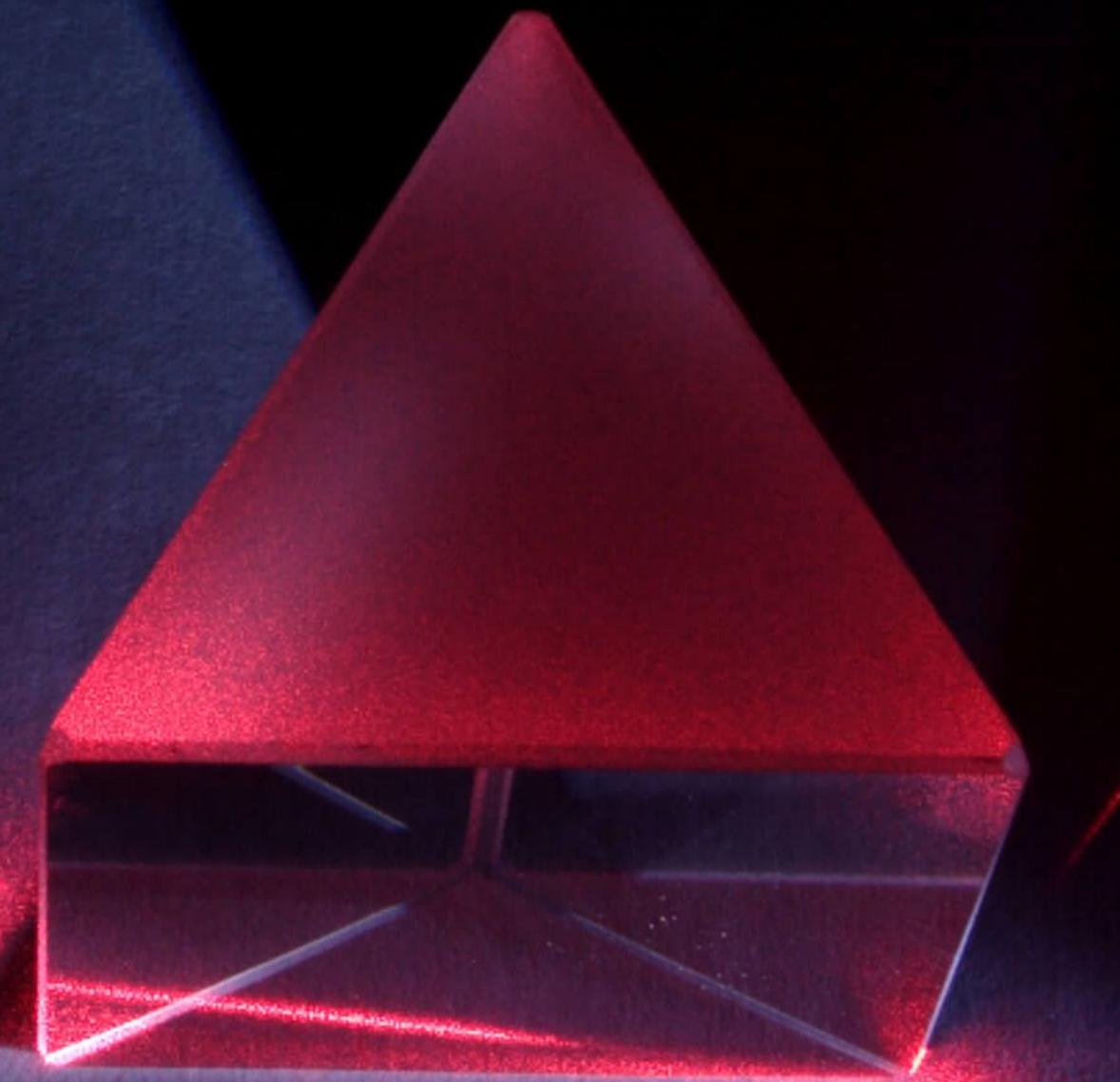
Criptografía Cuántica

2^a Escuela de Computación Cuántica

Dr. Esteban Sepúlveda Gómez
Profesor Asociado
Departamento de Física
Universidad de Concepción

Outline

- Introducción a la Criptografía
 - Problemas
- Mecánica Cuántica en la Criptografía
 - Conceptos fundamentales
- Protocolos de QKD
- Implementación: QKDS
- Arquitectura de un QKDS
- Rendimiento
- Ataques y vulnerabilidades
- Experimentos realizados en Chile
- Fin

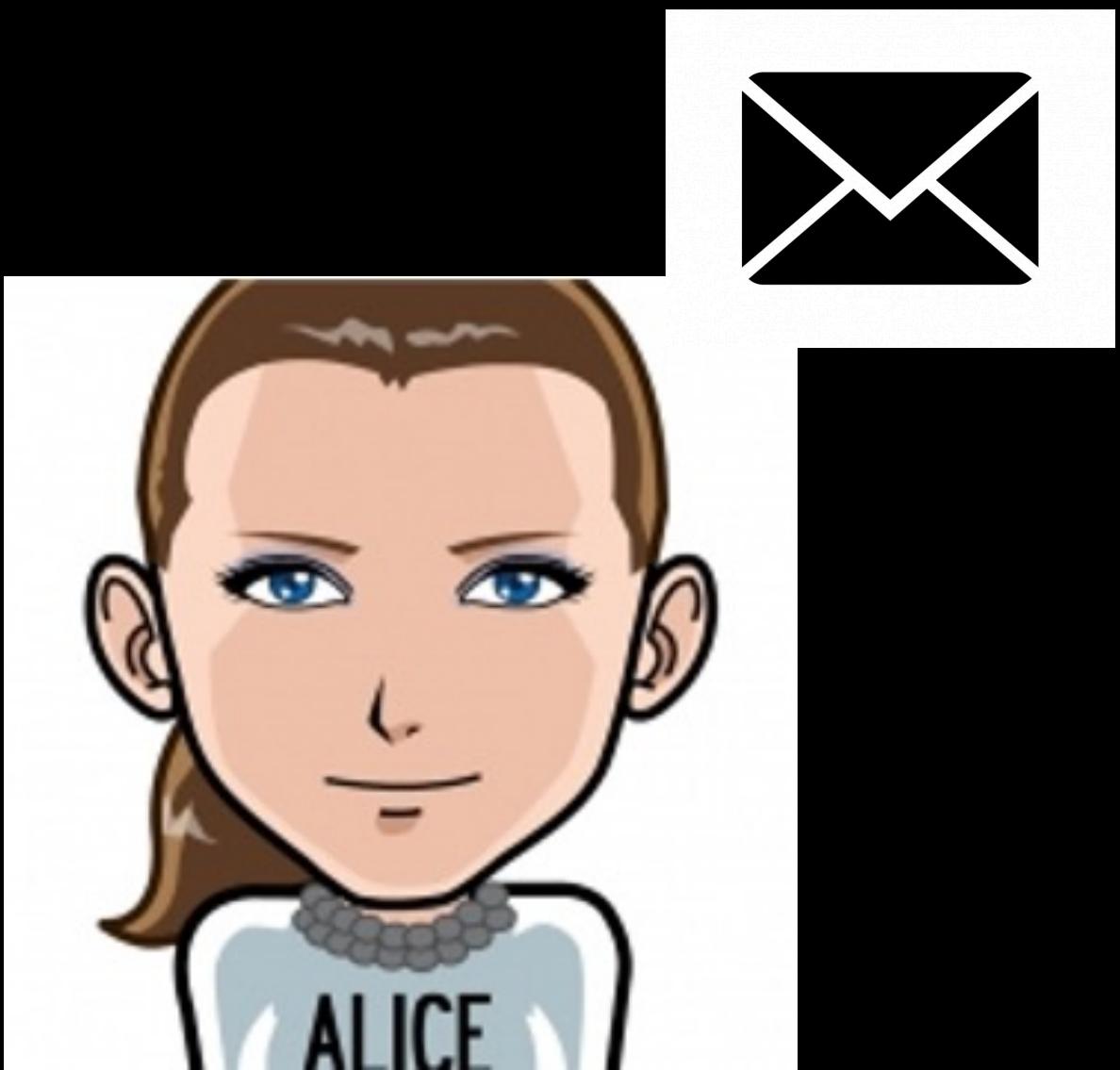


Introducción

- ¿Qué es la Criptografía? (del Griego: *krypto*, «oculto», y *graphos*, «escribir»; es decir, escritura oculta)
- “**Cryptography is the art of rendering a message unintelligible to any unauthorized party.**” RMP 74, 145 (2002).
- Es parte de la Criptología en conjunto con el Criptoanálisis: el arte de romper el código.
- Para poder ocultar un mensaje, se usa un **algoritmo** (llamado **criptosistema**) en conjunto con información adicional (llamado **clave**) para generar un **criptograma**. Este procedimiento se llama **encriptación**.
- Para que un criptosistema sea seguro, debe ser imposible de desbloquear el criptograma sin la clave correspondiente. En la práctica, este requisito se relaja exigiendo una gran dificultad para romper la clave.

Introducción

- Escenario de comunicación más sencillo



- Tipos de criptosistemas: **asimétricos (clave pública)** y **simétricos (clave privada)**.

Introducción

- Criptosistemas Asimétricos (clave pública)
- Diferentes claves para encriptar y desencriptar.
- Propuesto en 1976, primera implementación en 1978 por Ronald Rivest, Adi Shamir, and Leonard Adleman (RSA) (MIT).
- Bob, con una clave “*privada*”, genera una clave pública para que Alice encripte el mensaje. Sólo Bob puede desencriptar el mensaje.
- Sistema usado hasta la actualidad (variantes).
- Seguridad basada en complejidad matemática en resolver un problema.
- Criptosistemas Simétricos (clave privada)
- Misma clave para encriptar y desencriptar.
- Alice y Bob deben compartir la misma clave. Luego, por ejemplo, pueden usar el llamado One-time Pad (1926):
 - Para un mensaje en binario, Alice suma la clave para obtener un mensaje perturbado. Bob obtiene este mensaje y le resta la clave, para recuperar el mensaje.
- Shannon (1949) prueba su seguridad usando la teoría de la información.

Introducción

- Criptosistemas Asimétricos (clave pública)
- Vulnerabilidades:
 - Funciones “One-way”: dado x , es fácil obtener $f(x)$. El cálculo inverso no lo es.
 - Fácil: tiempo de cálculo polinomial.
 - Difícil: tiempo de cálculo exponencial.
Ejemplo: **Factorización**.
 - RSA está basado en la factorización de números enteros grandes. Sin embargo, no es posible probar que factorizar sea siempre “difícil”. Además, está el algoritmo de Shor.
 - Todos los criptosistemas asimétricos se basan en suposiciones no probadas. Por lo tanto, la seguridad de estos sistemas no está probada!
- Criptosistemas Simétricos (clave privada)
- Vulnerabilidades:
 - Alice y Bob deben compartir la misma clave, y debe ser tan larga como el mensaje a enviar. Además debe usarse sólo una vez. Si se ocupa más de una vez, un espía podría interceptar el mensaje y adivinarlo con una probabilidad no nula.
 - La clave debe ser transmitida por un medio seguro, confiable y privado, lo que implica un aumento del costo y de otras vulnerabilidades.
 - Por lo mismo, sólo se ocupa en casos críticos. Sin embargo, se ocupan claves más cortas junto con operaciones sobre la misma clave. La seguridad de estos sistemas también está basada en complejidad computacional.

Si estos criptosistemas son quebrados debido a avances matemáticos, o avances tecnológicos,

La Mecánica Cuántica es la única manera de resolver el problema de la distribución de claves.

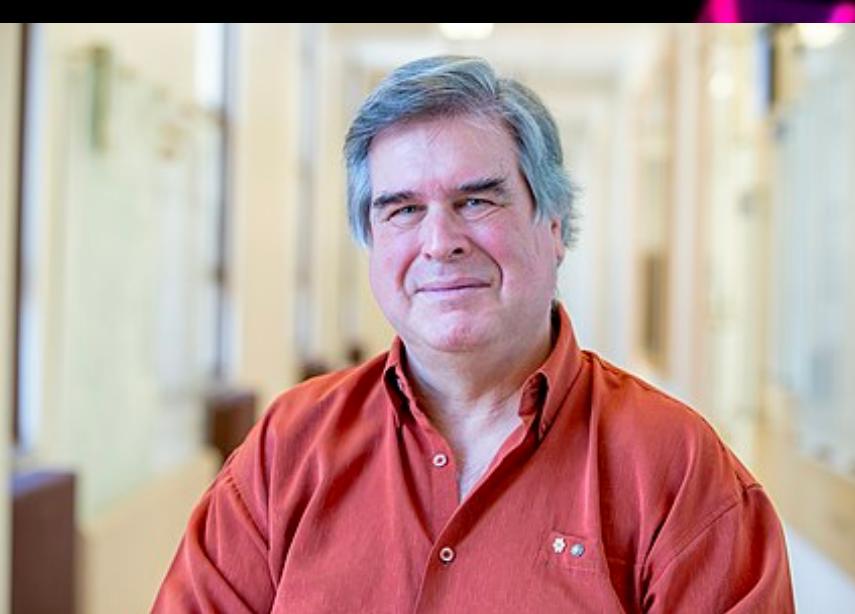
Introducción

- Un poco de historia:
 - **Quantum Money:** Stephen Wiesner propone un mecanismo para crear billetes imposibles de falsificar mediante la codificación de fotones polarizados en trampas de luz en los billetes de un dólar.
 - En 1984, Charles Bennett y Gilles Brassard toman la idea de Wiesner y proponen el primer diseño práctico de un sistema criptográfico cuántico de intercambio de clave (QKD):
 - Se establecen los dos primeros niveles de trabajo de un sistema de QKD, **el intercambio de la clave bruta y la reconciliación de bases.**
 - En un sistema ideal, estos niveles son necesarios y suficientes para intercambiar una clave para usar en el One-time Pad.
 - En la práctica, la implementación se ve afectada por imprecisiones, ruido, la acción del espía, etc.
 - **Luego se definen y desarrollan los siguientes niveles para una implementación práctica: corrección de errores y amplificación de privacidad.**

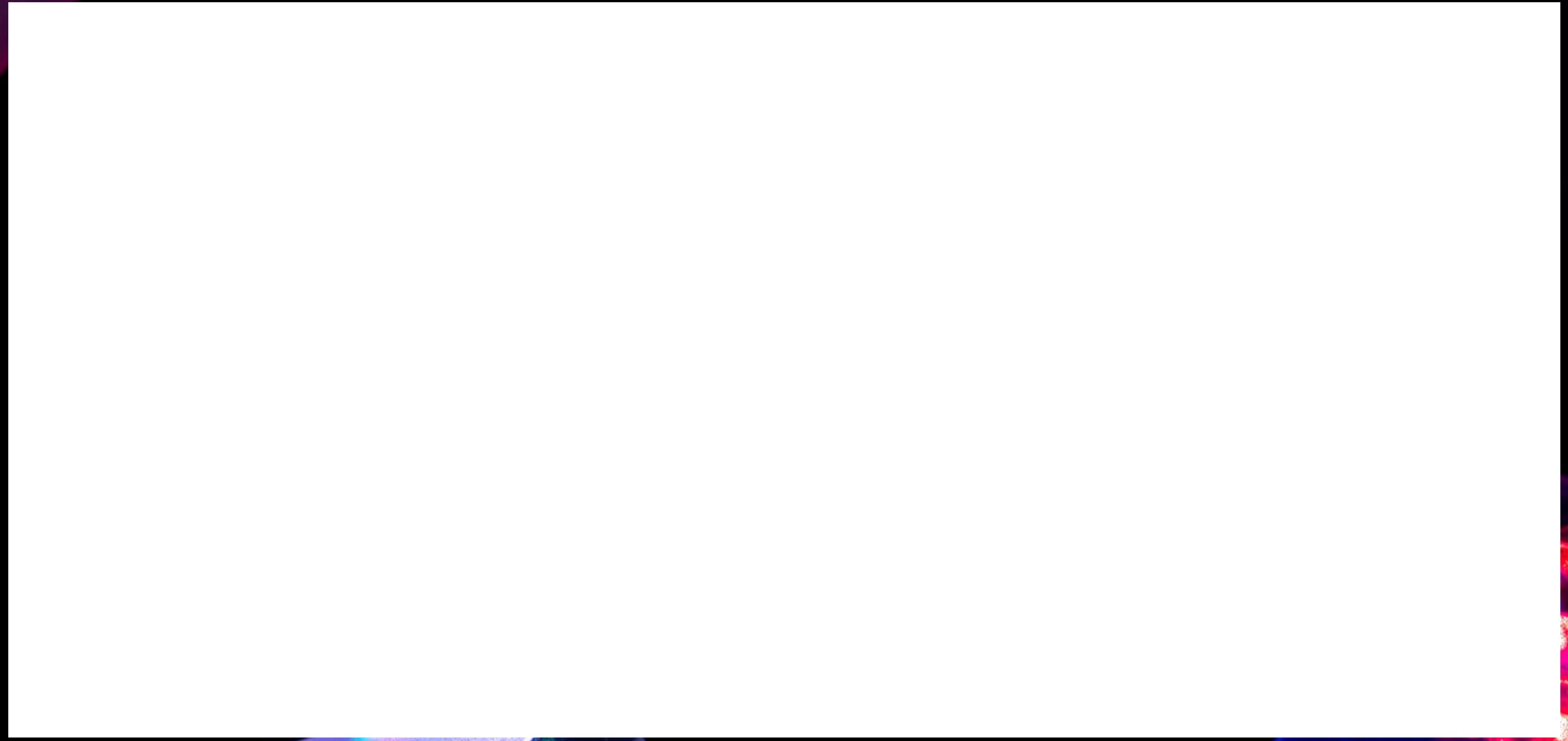


Introducción

- Cronología:
 - 1970: S. Wiesner propone el dinero cuántico.
 - 1982: R. Feynman inspira el concepto de computador cuántico.
 - 1983: S. Wiesner logra publicar su idea.
 - 1984: Bennett y Brassard proponen el primer protocolo QKD: BB84.
 - 1988: Bennett y Brassard utilizan la amplificación de privacidad para reducir la posible información que obtiene un espía.
 - 1989: Bennett y Smolin implementan el primer prototipo de QKD. Se dispara el interés en este sistema.
 - 1991: A. Ekert propone un nuevo protocolo QKD basado en el entrelazamiento.
 - 1992: Primera descripción del algoritmo de Shor. Se constituye un riesgo importante para los sistemas de cifrado asimétricos.



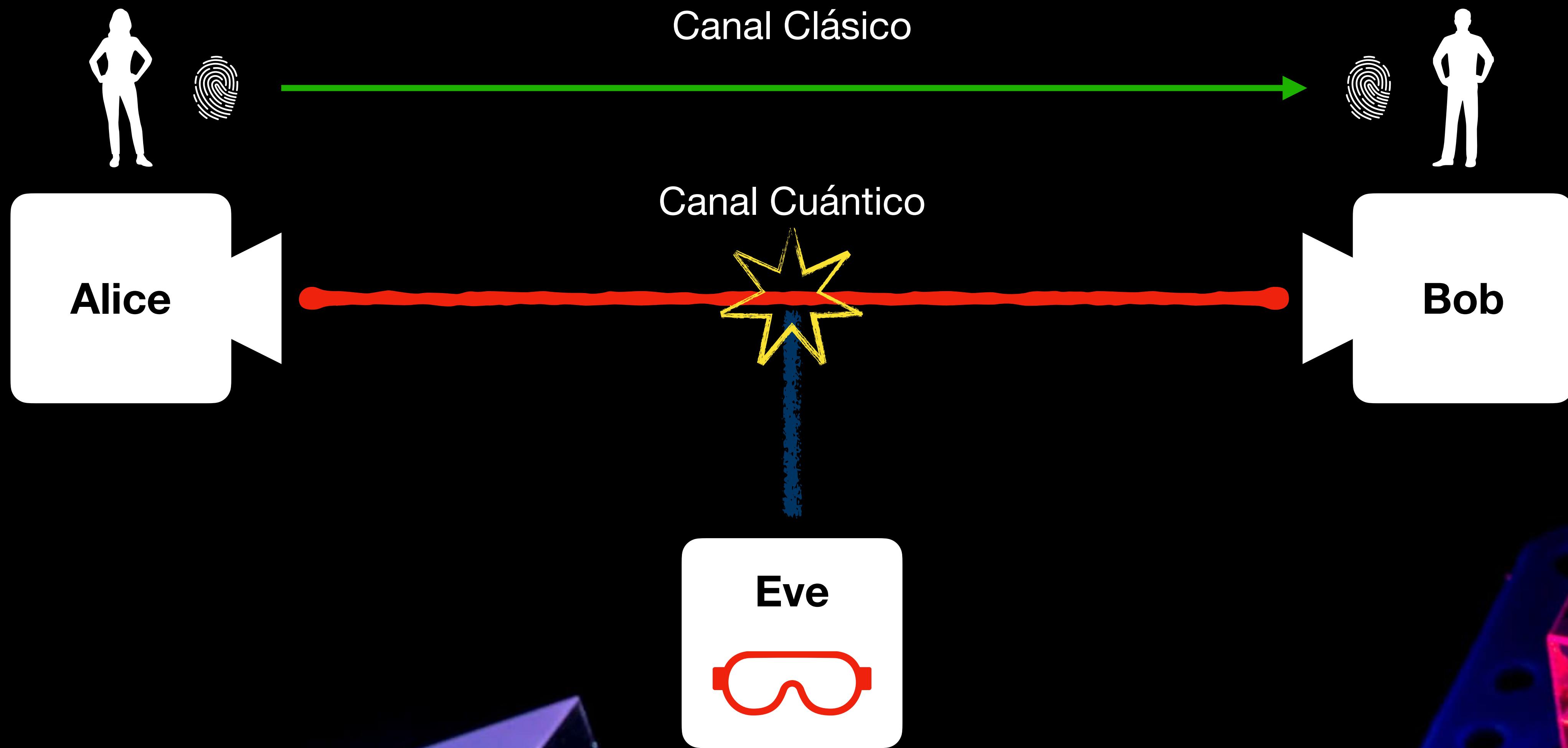
Conceptos Previos de Mecánica Cuántica



Protocolos QKD

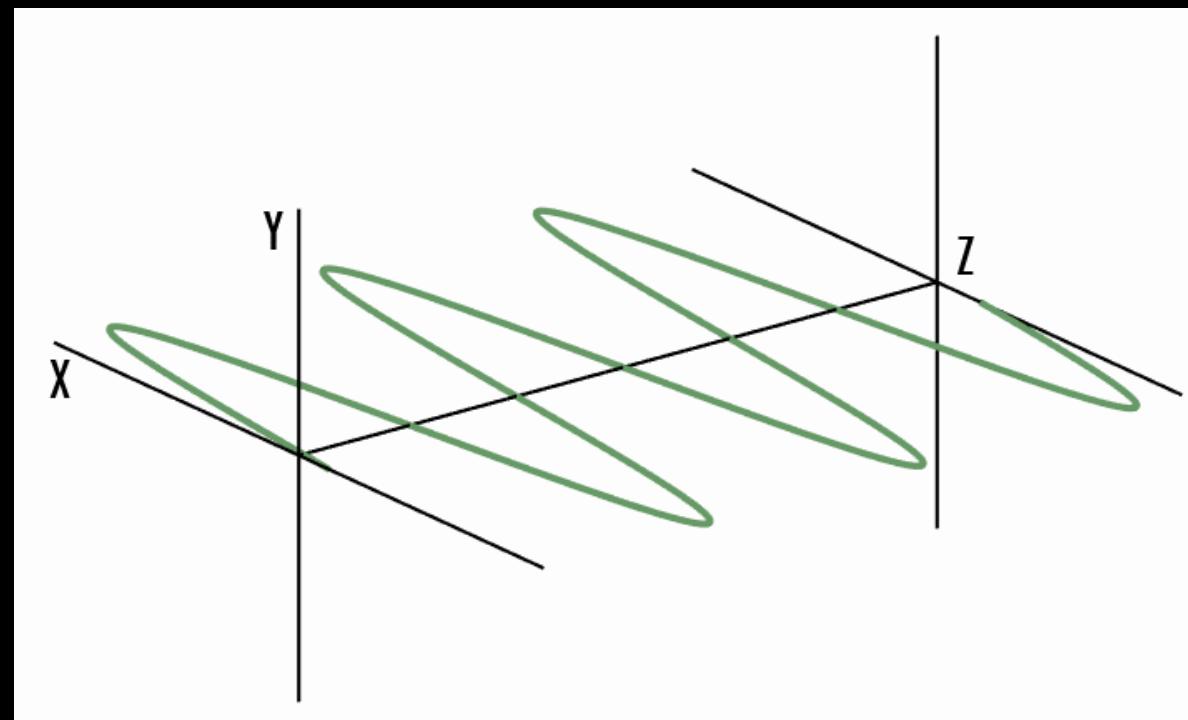
- Consideraciones previas:
 - Alice y Bob deberán estar conectados mediante **DOS** canales de comunicación, “clásico” y “cuántico”.
 - El canal clásico debe estar autenticado, es decir, nadie puede modificar la información que se intercambia en este canal.
 - Introduciremos la acción de un potencial espía, que llamaremos Eve. El objetivo del espía es obtener la máxima información sobre la clave a intercambiar.
 - El espía tendrá acceso a ambos canales, bajo las siguientes exigencias:
 - Acceso total al canal cuántico y a realizar todo lo que le sea posible bajo las reglas de la naturaleza (QM).
 - Podrá leer la información del canal clásico, pero no podrá modificarla.

Protocolos QKD

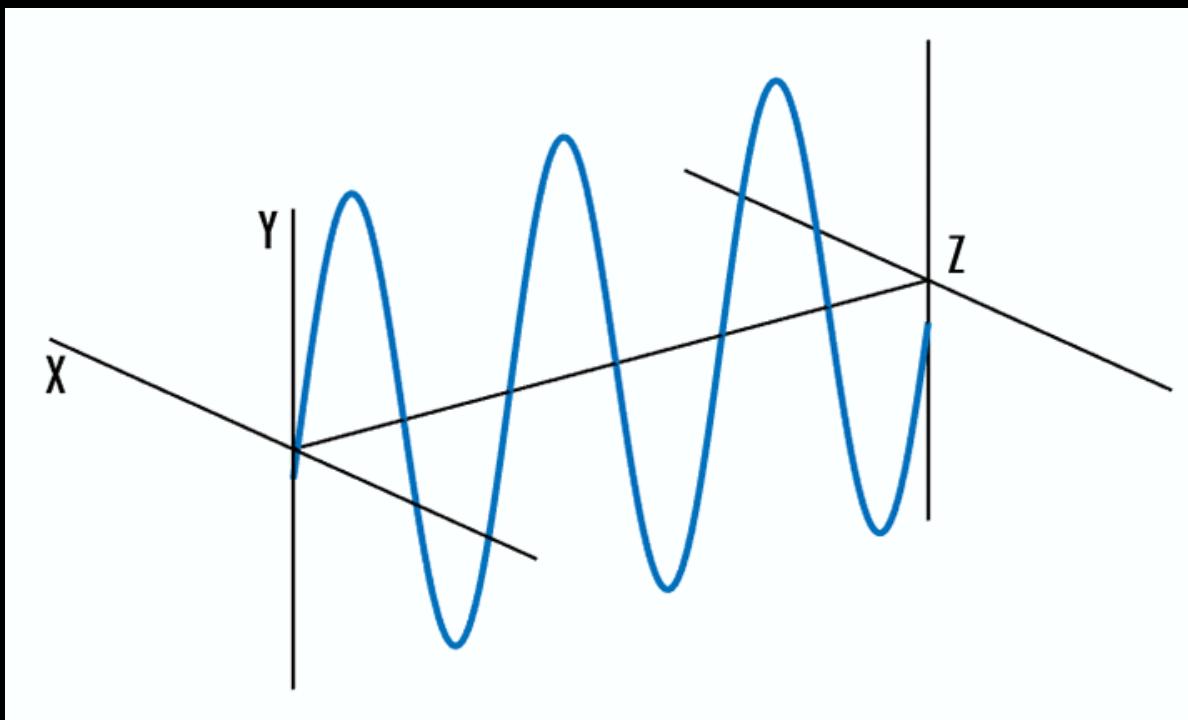


Protocolos QKD: BB84

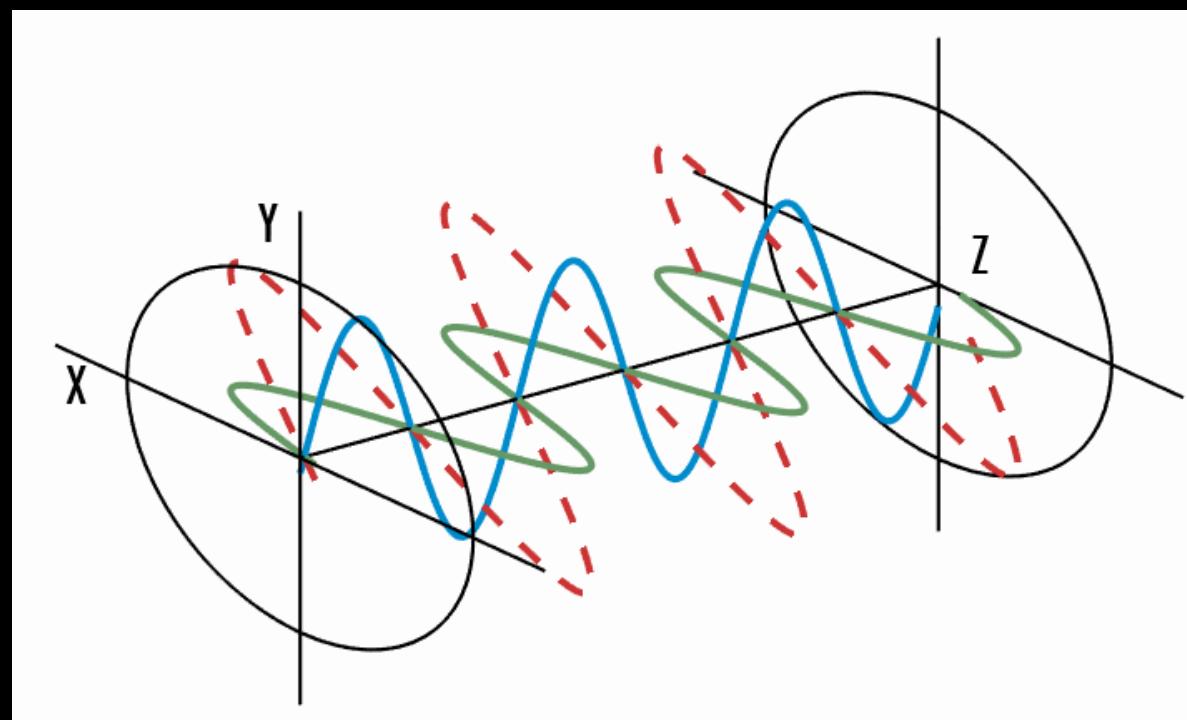
- Propuesto por Bennett y Brassard en la *International Conference on Computers, Systems and Signal*, Los Álamos, California (1984)
- Propuesta original: usando Fotones y la polarización.



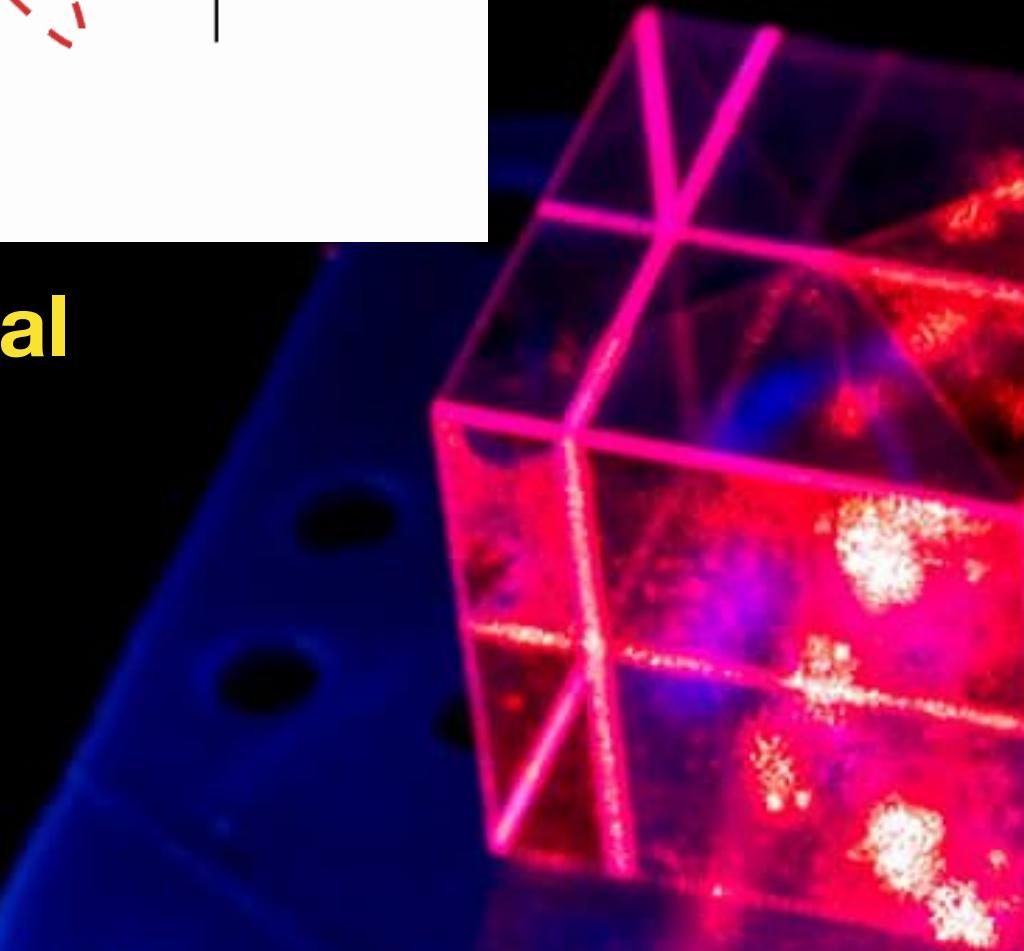
Horizontal



Vertical



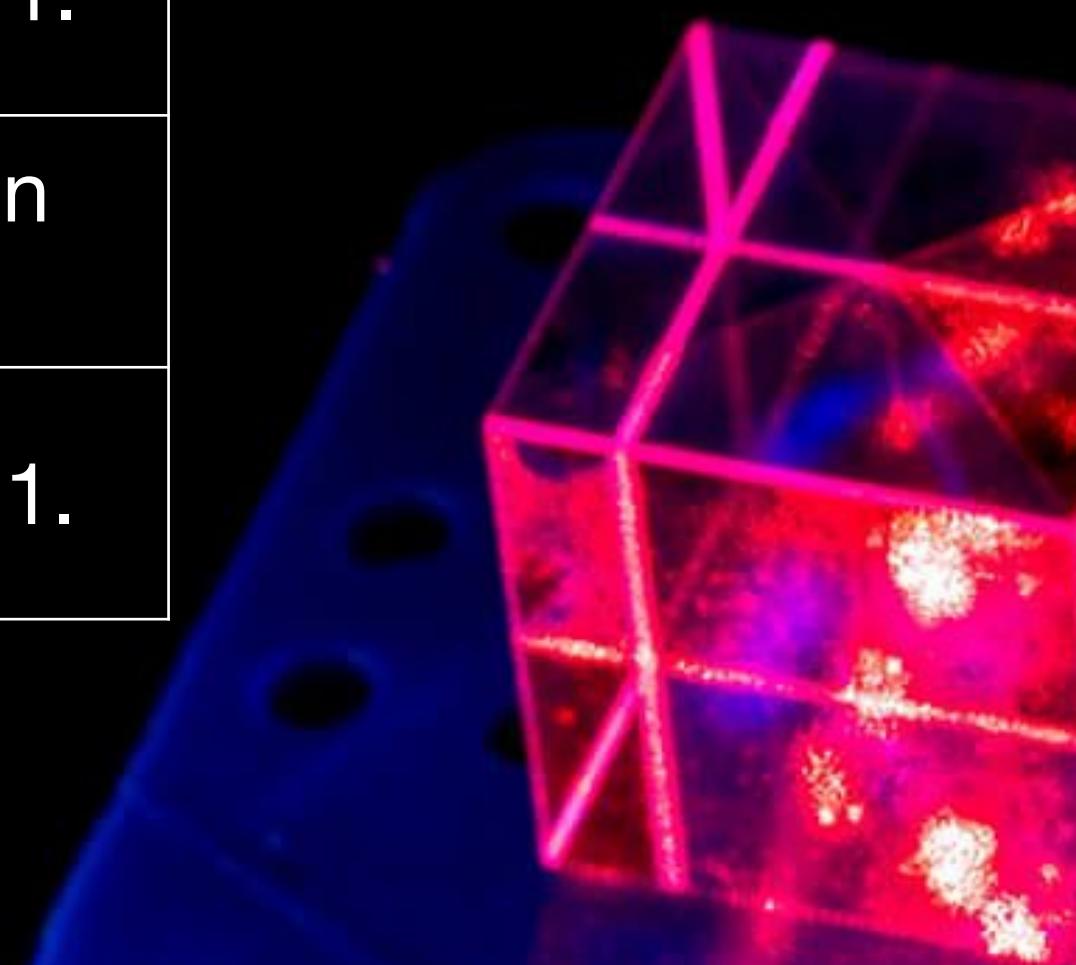
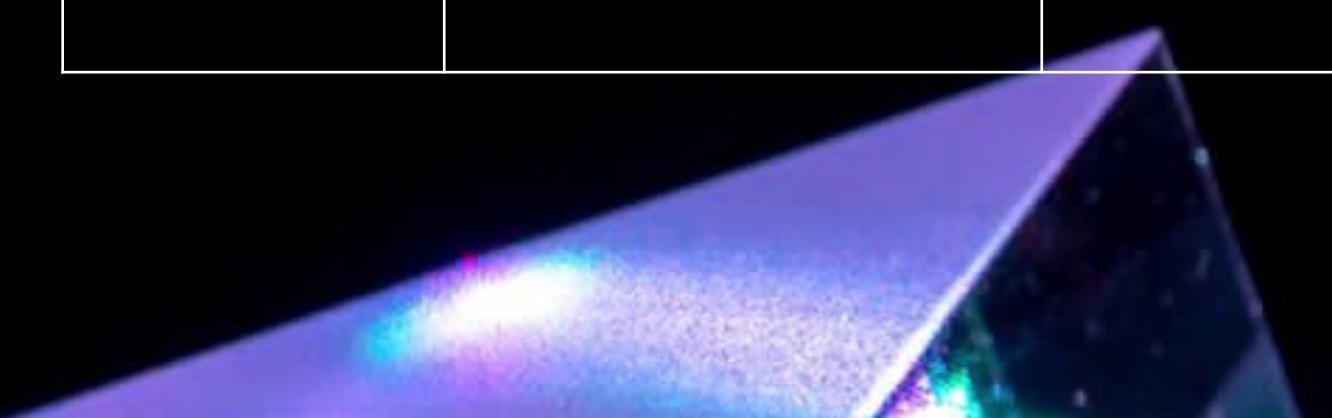
Diagonal



Protocolos QKD: BB84

- Una idea brillante: Alice y Bob intercambian qubits: estados de fotones individuales codificados en polarización. Estos estados forman dos bases ortogonales y mutuamente excluyentes. Por ejemplo:

Base	Polarización	Estado	Tarea
B_+	H	$ 0\rangle$	Preparar el qubit en la base B_+ (polarización horizontal-vertical) con el valor 0.
B_+	V	$ 1\rangle$	Preparar el qubit en la base B_+ con el valor 1.
B_x	D	$ +\rangle$	Preparar el qubit en la base B_x (polarización diagonal) con el valor 0.
B_x	A	$ -\rangle$	Preparar el qubit en la base B_x con el valor 1.

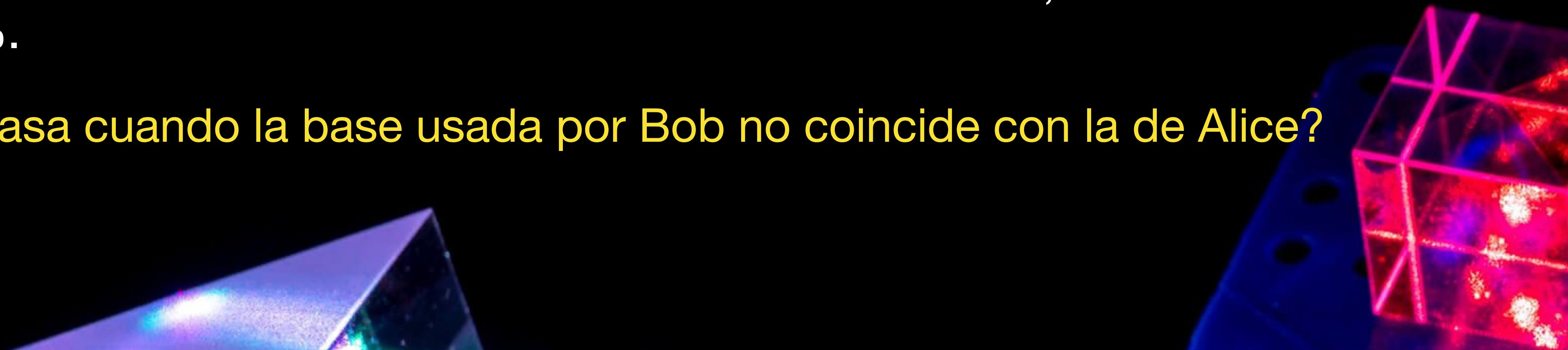


Protocolos QKD: BB84



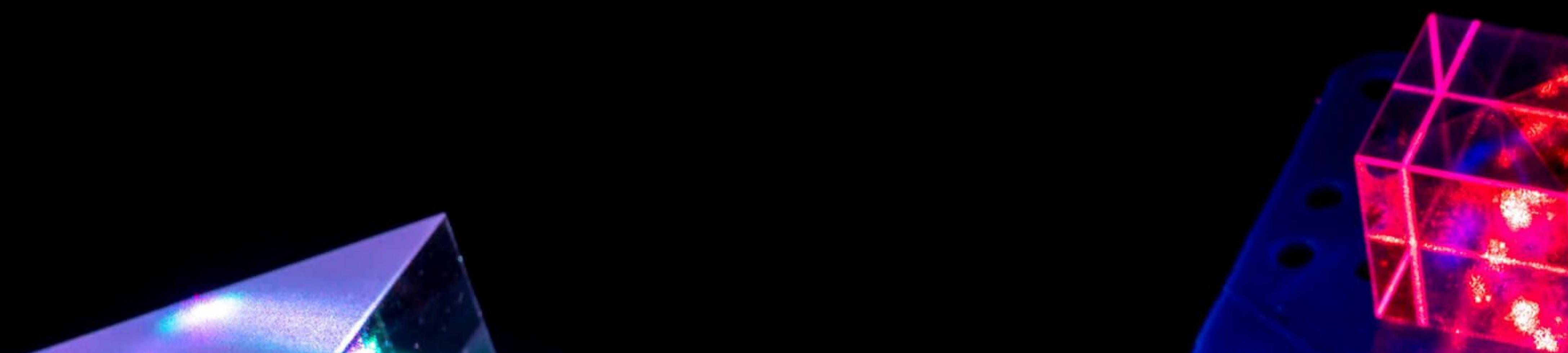
Protocolos QKD: BB84

- **Intercambio de clave bruta:** Alice prepara una secuencia de n estados, obtenidos a partir de dos secuencias aleatorias, una de bases y otra de valores para la clave (estados).
- Alice envía cada estado a Bob.
- Bob analiza los estados enviados por Alice, eligiendo aleatoriamente que base utilizar.
- Como ambas secuencias de bases usadas son aleatorias, sólo coinciden en un 50%.
- ¿Qué pasa cuando la base usada por Bob no coincide con la de Alice?



Protocolos QKD: BB84

- **Reconciliación de bases:** ahora Alice y Bob se comunican por el canal clásico, para mostrar las bases usadas en cada repetición.
- Aquellos casos en que las bases no coinciden son descartados por ambos.
- En el caso ideal (sin espías ni ruido), ambos compartirían una clave idéntica!
- Si hubiese espía, la clave no sería idéntica, por lo que sigue un proceso de reducción de errores a través de un proceso de Amplificación de Privacidad.



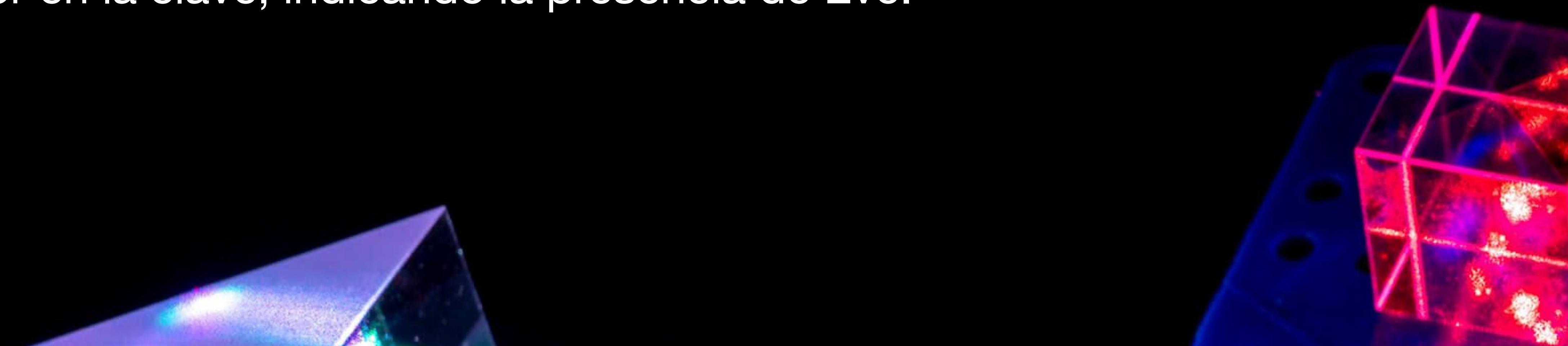
Protocolos QKD: BB84

- **Algoritmo:**

1. Alice genera una secuencia de valores aleatorios que corresponderá con la clave que desea intercambiar con Bob.
2. Alice genera otra secuencia aleatoria, ahora con las bases que utilizará para la codificación de la clave generada en el paso anterior.
3. Alice codifica cada valor de la clave con la base correspondiente y envía la secuencia de qubits a Bob.
4. Bob genera una secuencia aleatoria con las bases que utilizará para decodificar la secuencia de estados recibidos de Alice.
5. Bob mide cada estado recibido en la base correspondiente a la secuencia generada.
6. Bob envía a Alice la secuencia de bases utilizada a través de un canal público autenticado.
7. Alice compara la secuencia de bases que ha utilizado, quedándose sólo con aquellas mediciones para las que han coincidido ambas bases.
8. Alice y Bob comparten ahora una secuencia de valores formada por aquellos en los que las posiciones donde las bases de preparación y medición han coincidido.

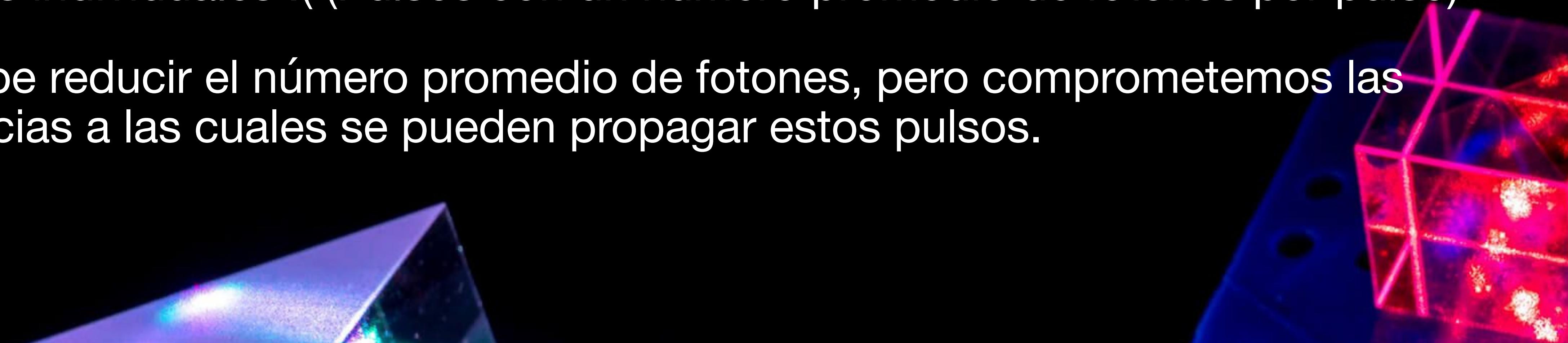
Protocolos QKD: BB84

- Después de los puntos anteriores existe un postproceso cuyo objetivo es estimar la presencia de un espía, corregir los errores, y amplificar la privacidad. Estos pasos siempre se ejecutan en un proceso de QKD, aunque formalmente no se consideren parte del protocolo BB84.
- La seguridad del protocolo radica en que el espía tiene un 25% de error al intentar leer los qubits de Alice, ya que no tiene información de que base usó.
- El espía tendría que reenviar los estados a Bob, por lo que él tendría un 25% de error en la clave, indicando la presencia de Eve.



Protocolos QKD: Decoy States

- Decoy states, o estados señuelos, no es un protocolo QKD en si mismo, sino que una herramienta usada en conjunto con otro protocolo para incrementar la seguridad.
- Esto sucede cuando la etapa de implementación del protocolo tiene imperfecciones, permitiendo ataques al sistema, en particular, el llamado PNS (Photon Number Splitting).
- ¿Por qué sucede esto? Por la imperfección de las fuentes emisoras de fotones individuales :((Pulsos con un número promedio de fotones por pulso)
- Se debe reducir el número promedio de fotones, pero comprometemos las distancias a las cuales se pueden propagar estos pulsos.

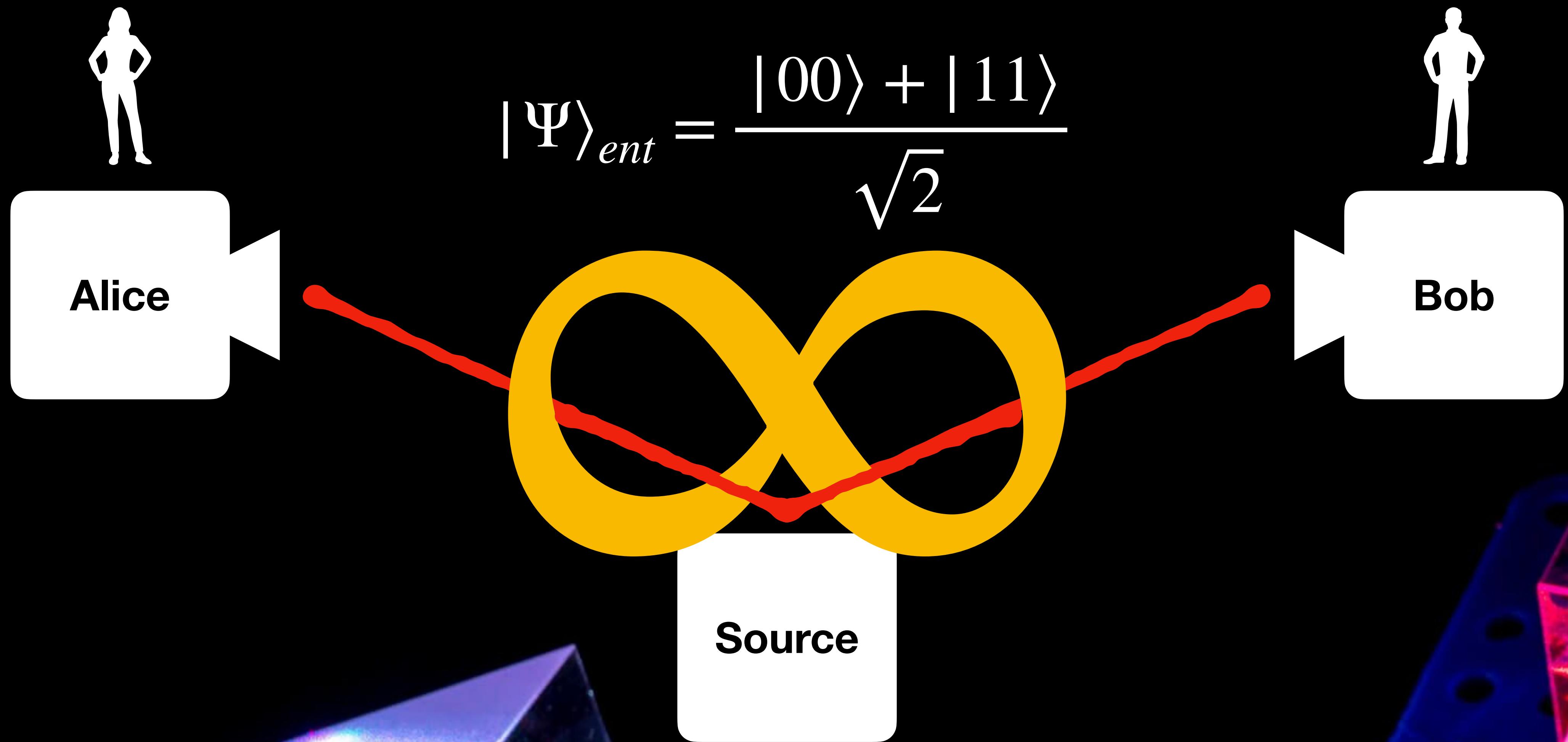


Protocolos QKD: Decoy States

- **Algoritmo:**
 1. Alice selecciona las intensidades $\mu < 1$ y $\mu' > 1$ (señuelos) usadas en su fuente.
 2. Alice envía a Bob pulsos con intensidades escogidas aleatoriamente.
 3. Cuando Bob comunica que ha completado la recepción de los pulsos, Alice publica los índices de los pulsos donde se ha enviado un estado señuelo.
 4. Con la información de μ y μ' , Alice y Bob pueden estimar el rendimiento de la clave para cada caso.
 5. Dependiendo del resultado del análisis, siguen con el proceso de reconciliación de base (BB84).

Protocolos QKD: E91

- A. Ekert propone un nuevo protocolo de QKD basado en el entrelazamiento.



Protocolos QKD: E91

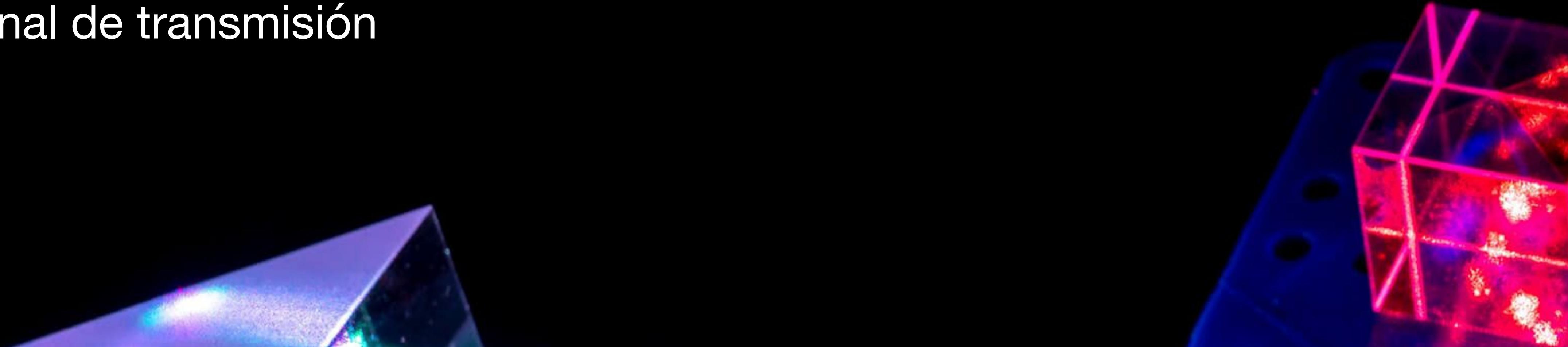


Protocolos QKD: E91

- **Algoritmo:**
 1. Alice genera una secuencia de bases perfectamente aleatoria.
 2. Bob genera otra secuencia de bases perfectamente aleatoria.
 3. La fuente comienza la emisión de pares entrelazados hacia ambos extremos de la comunicación.
 4. Alice mide en las bases del paso 1.
 5. Bob mide en las bases del paso 2.
 6. Ambos interlocutores intercambian la secuencia de bases utilizadas en cada medida, desechando los eventos que no coinciden.

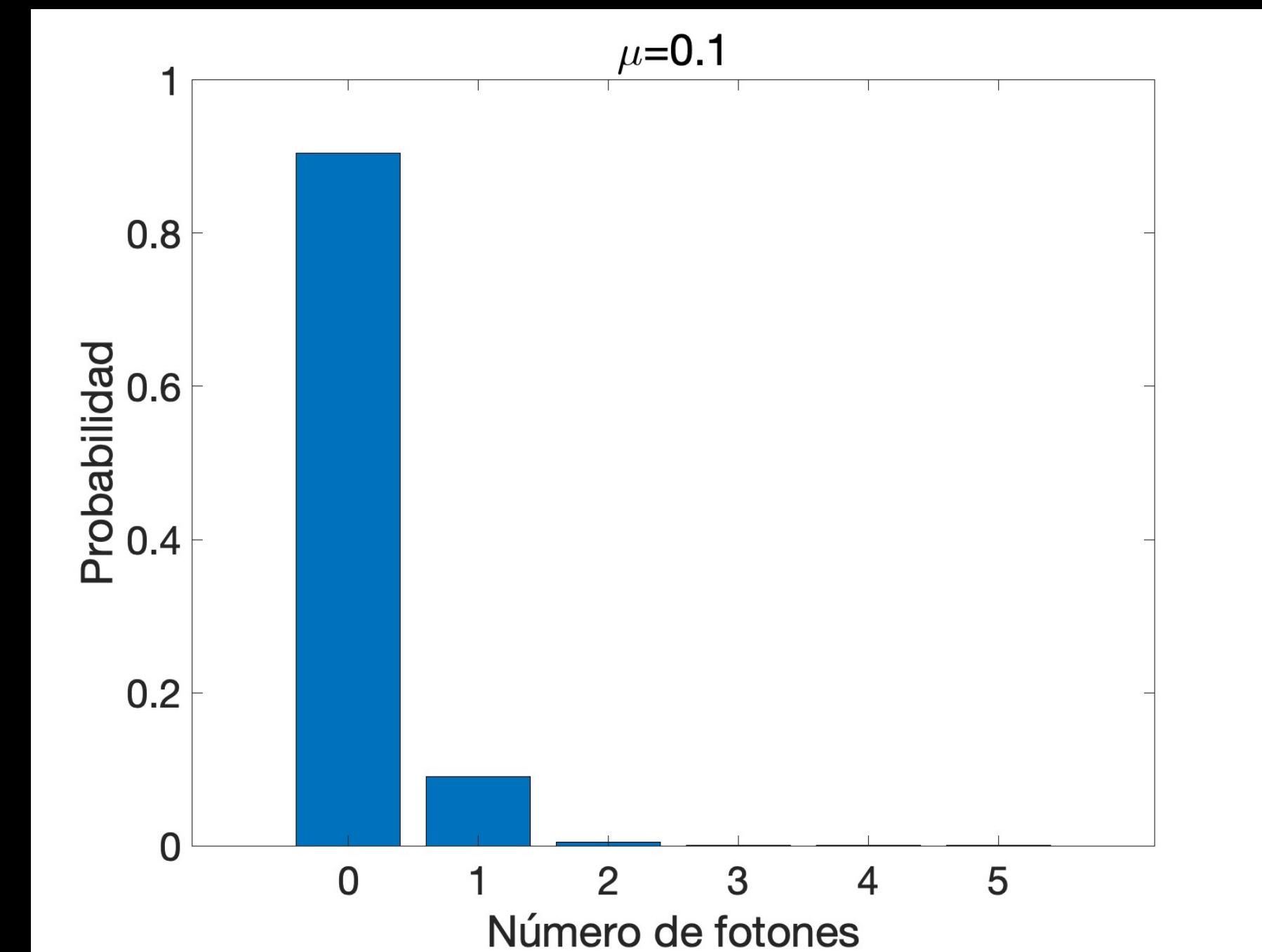
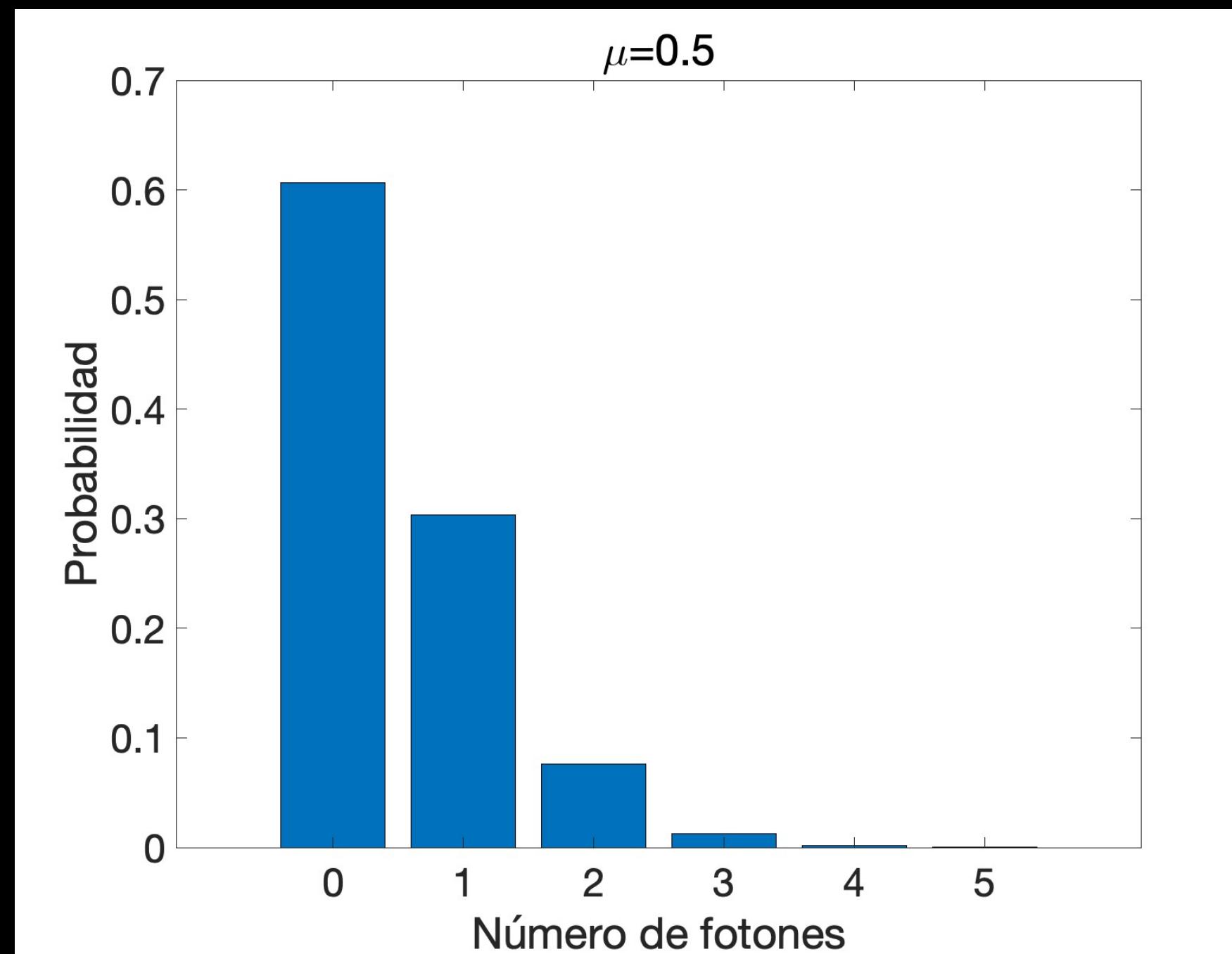
Implementación

- Aquí aparecen los problemas (algunos los mencionamos anteriormente). Pero veamos los componentes:
 - **El fotón:** fácilmente manipulable y con distintos grados de libertad para realizar la codificación. Se requiere:
 - Fuente de fotones individuales
 - Detectores eficientes
 - Canal de transmisión



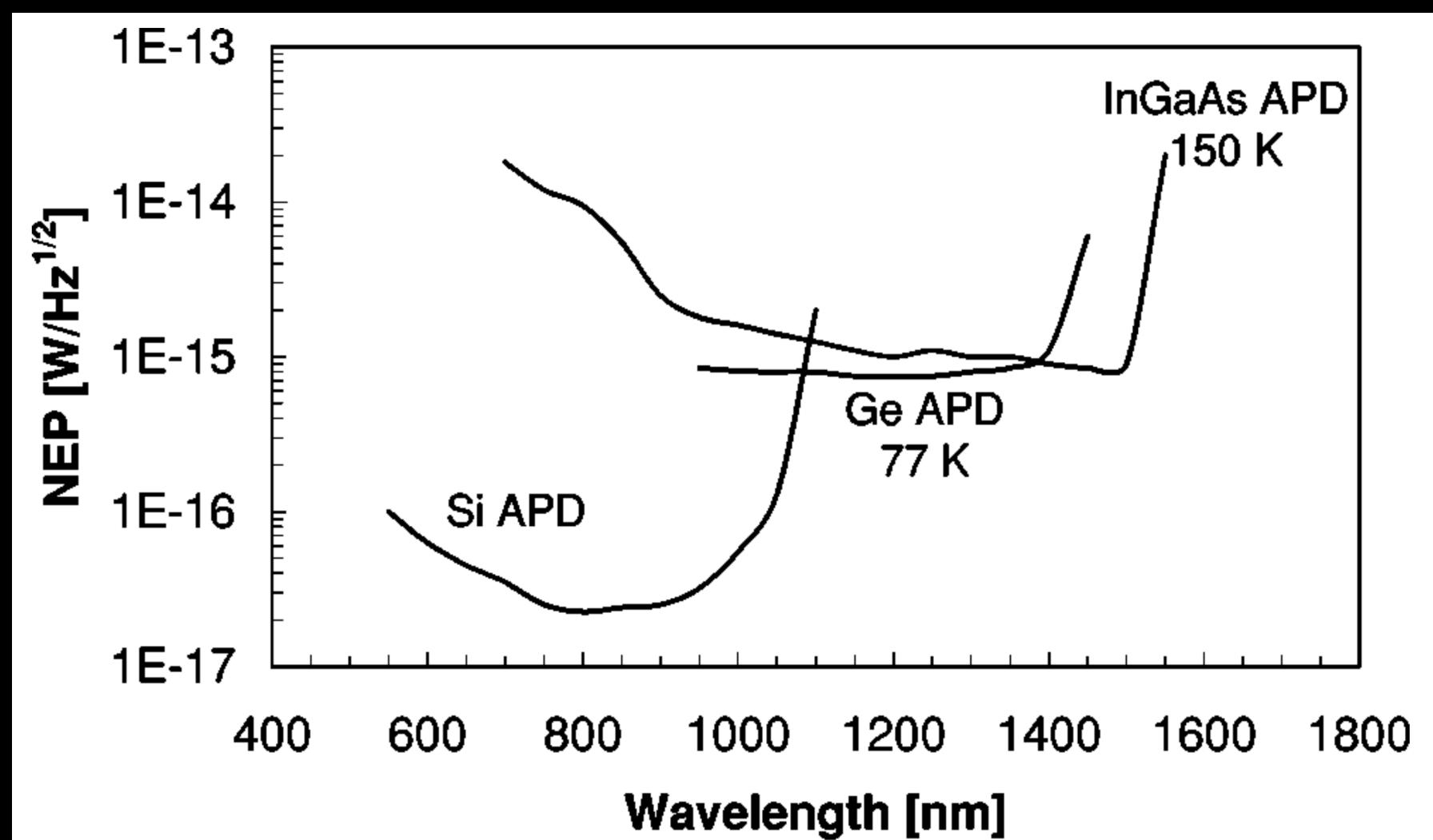
Implementación

- Desde el punto de vista práctico, se usan pulsos de láser atenuados para alcanzar el nivel de fotones individuales (no hay on-demand :()
- El atenuador es imperfecto, lo que genera una estadística para el número de fotones por pulso: $P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu}$.



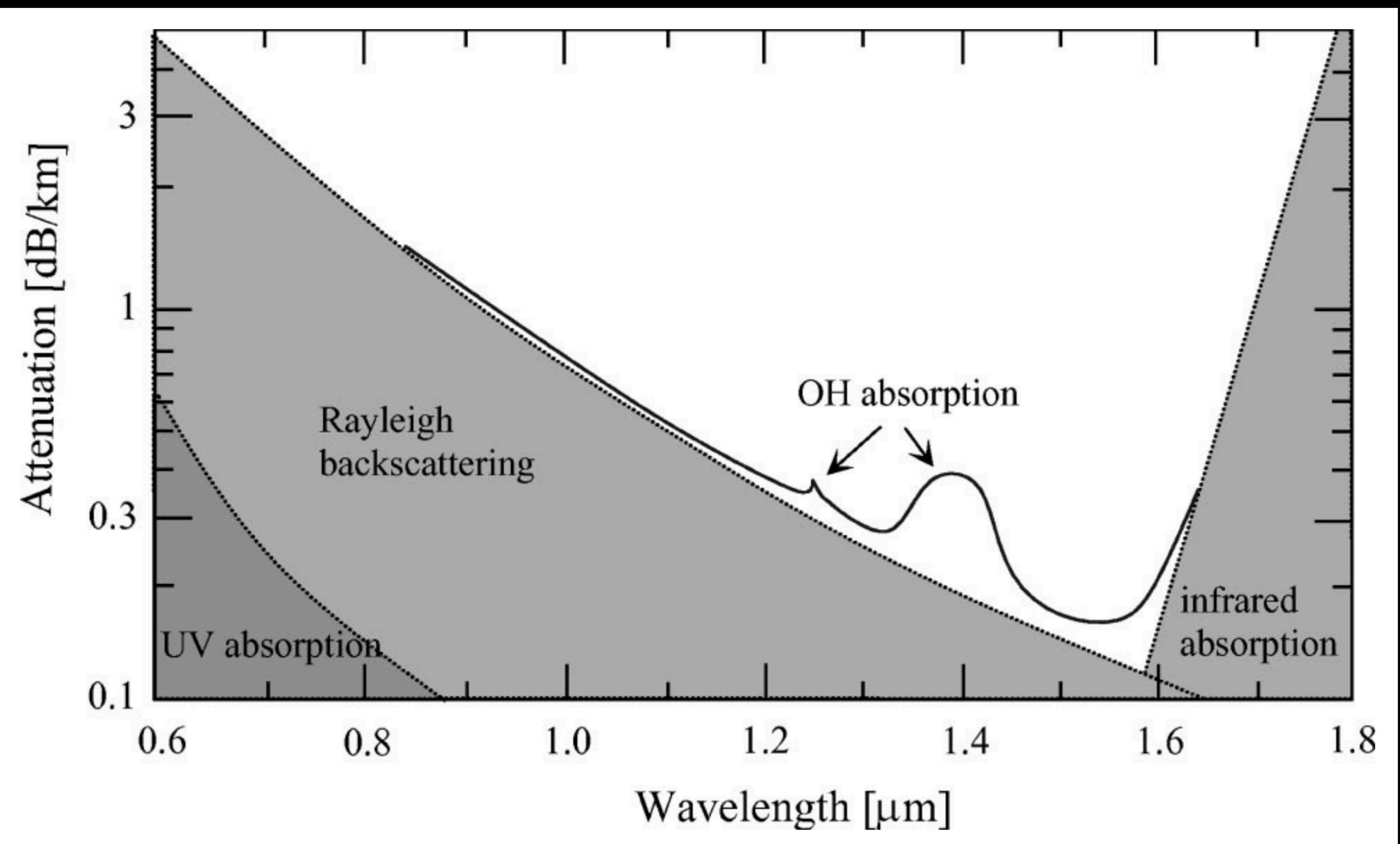
Implementación

- La probabilidad de obtener 0 fotones es grande siempre! Hay un compromiso entre reducir los eventos de multifotones y la cantidad de pulsos vacíos.
- Detectores:
 - Por ventana de detección, no son capaces de resolver fotones individuales.
 - Presencia de tiempo muerto.
 - Eficiencia en función de la longitud de onda.



Implementación

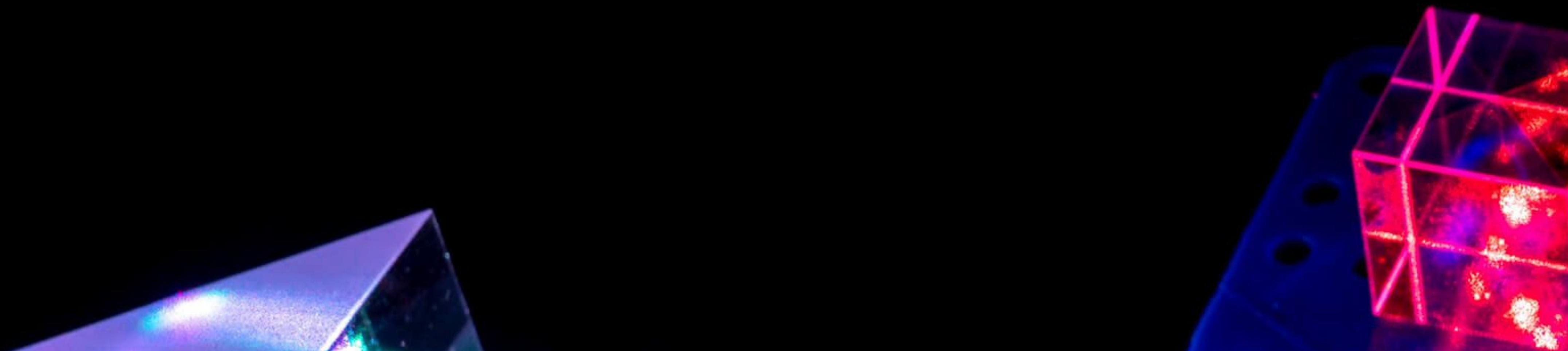
- **Canales: Fibra Óptica**, compatible con la red de telecomunicaciones actual. Sin embargo, efectos de despolarización, atenuación y birrefringencia afecta a los estados transmitidos.



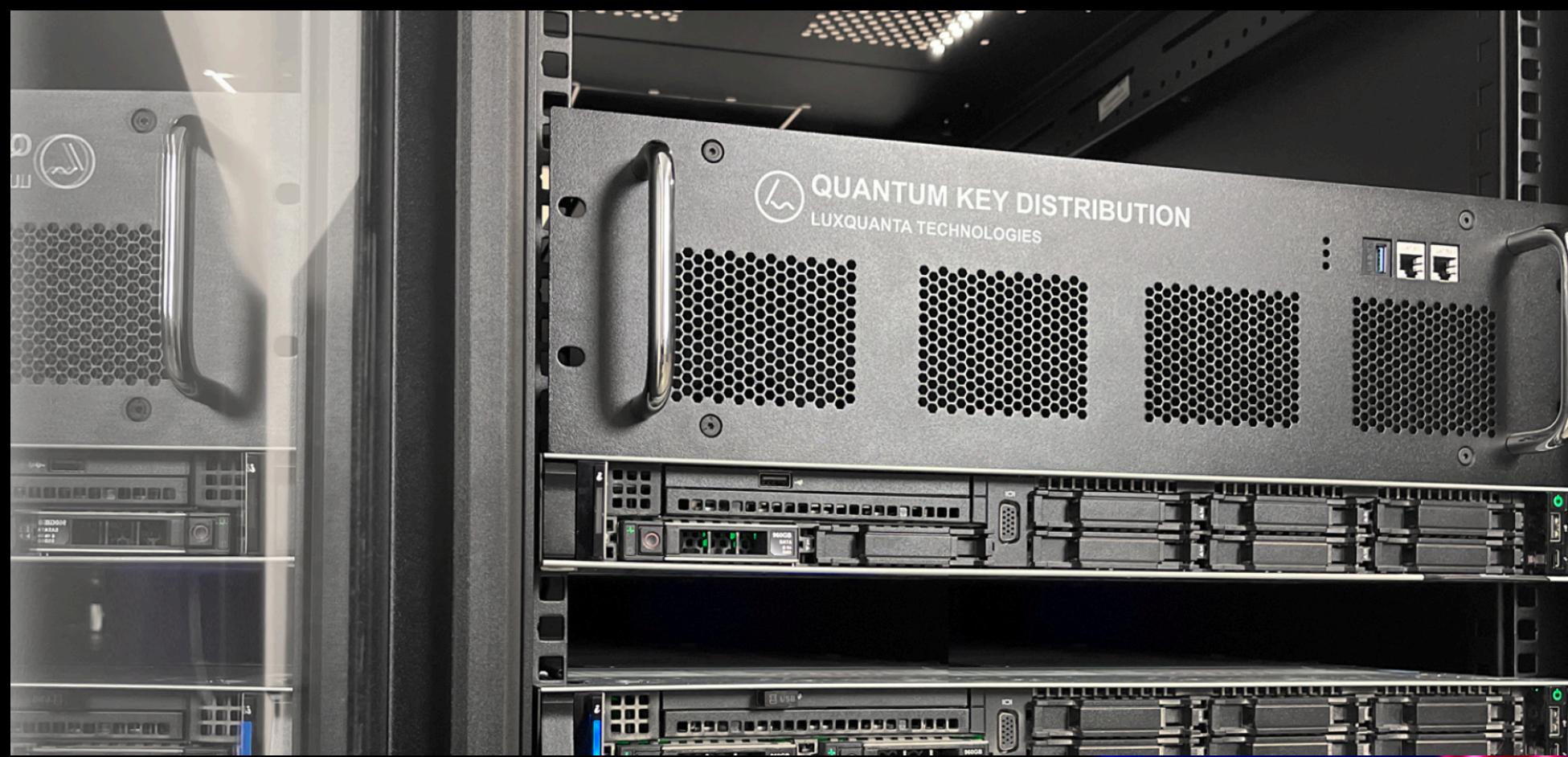
RMP 74, 145 (2002)

Implementación

- **Canales: Fibra Óptica**, compatible con la red de telecomunicaciones actual. Sin embargo, efectos de despolarización, atenuación y birrefringencia afecta a los estados transmitidos.
- Esto afecta a la codificación de los estados cuánticos a utilizar en una sesión criptográfica (polarización, fase, tiempo).



Implementación



Arquitectura

- Basada en dos pilares: el **pilar teórico**, basado en las leyes de la QM, y el **pilar práctico**, que permite obtener finalmente una clave segura.
1. Intercambio de una clave:
 - Intercambio de la clave en bruto, sin conocimiento de las bases.
 - Reconciliación de bases, obteniendo una clave “real”.
 2. Destilación de la clave intercambiada, debido a las imperfecciones:
 - Mecanismo de corrección de errores.
 - Soporte de amplificación de privacidad.
 3. Autenticación del canal público o clásico.

Arquitectura

- Basada en dos pilares: el **pilar teórico**, basado en las leyes de la QM, y el **pilar práctico**, que permite obtener finalmente una clave segura.

1. Intercambio de una clave:

- Alice y Bob tienen que sincronizarse.
- Desde el punto de vista práctico, se debe caracterizar y calibrar el sistema antes de realizar el protocolo.
- Cuando el sistema funciona correctamente, se debe cumplir lo siguiente:
 - Los valores de los bits de la clave deben ser distribuidos de forma aleatoria y uniforme,
 - El tamaño de la clave bruta debe ser el esperado,
 - El tamaño de la clave reconciliada debe ser el esperado.

¿Qué tan buena es la clave?

- **Quantum Bit Error Rate (QBER):** $\frac{Nbits_{err}}{Nbits_{corr} + Nbits_{err}}$ (en la reconciliación de bases).
- Se establece un límite para el QBER: 11% (caso de qubits).

Arquitectura

- Basada en dos pilares: el **pilar teórico**, basado en las leyes de la QM, y el **pilar práctico**, que permite obtener finalmente una clave segura.
2. Destilación de la clave:
- Corrección de errores: a pesar de que un 11% de tolerancia pareciera razonable, en la práctica el QBER es de dicho orden. El proceso de corrección debe proporcionar la menor cantidad de información sobre la clave que queremos corregir. Además, debe ser eficiente.
 - Amplificación de privacidad: el error puede haber sido producido por un espía, lo que se debe buscar minimizar la cantidad de información que el espía pudo obtener incluso en la etapa de corrección de errores.
 - La implementación también es un factor de riesgo (p.ej, eventos multifotones).
 - **La única forma de aumentar la seguridad es reduciendo el tamaño de la clave.**

Consideraciones Finales

- Ataques y Vulnerabilidades
 - PNS, Interceptar y Reenviar
 - Ataques experimentales (al hardware que implementa el QKDS, ejemplo Vadim Makarov)
 - Aleatoriedad (QRNG)

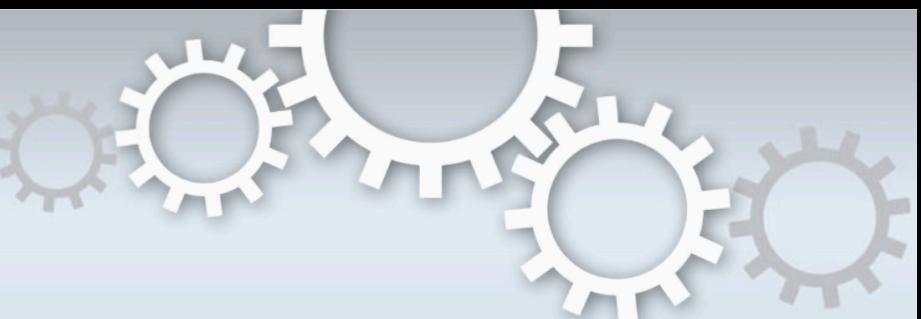


Consideraciones Finales



Experimentos realizados en Chile

SCIENTIFIC REPORTS



OPEN

SUBJECT AREAS:

- QUANTUM INFORMATION
- FIBRE OPTICS AND OPTICAL COMMUNICATIONS
- QUANTUM MECHANICS
- QUANTUM OPTICS

Received
10 April 2013

Accepted
15 July 2013

Published
30 July 2013

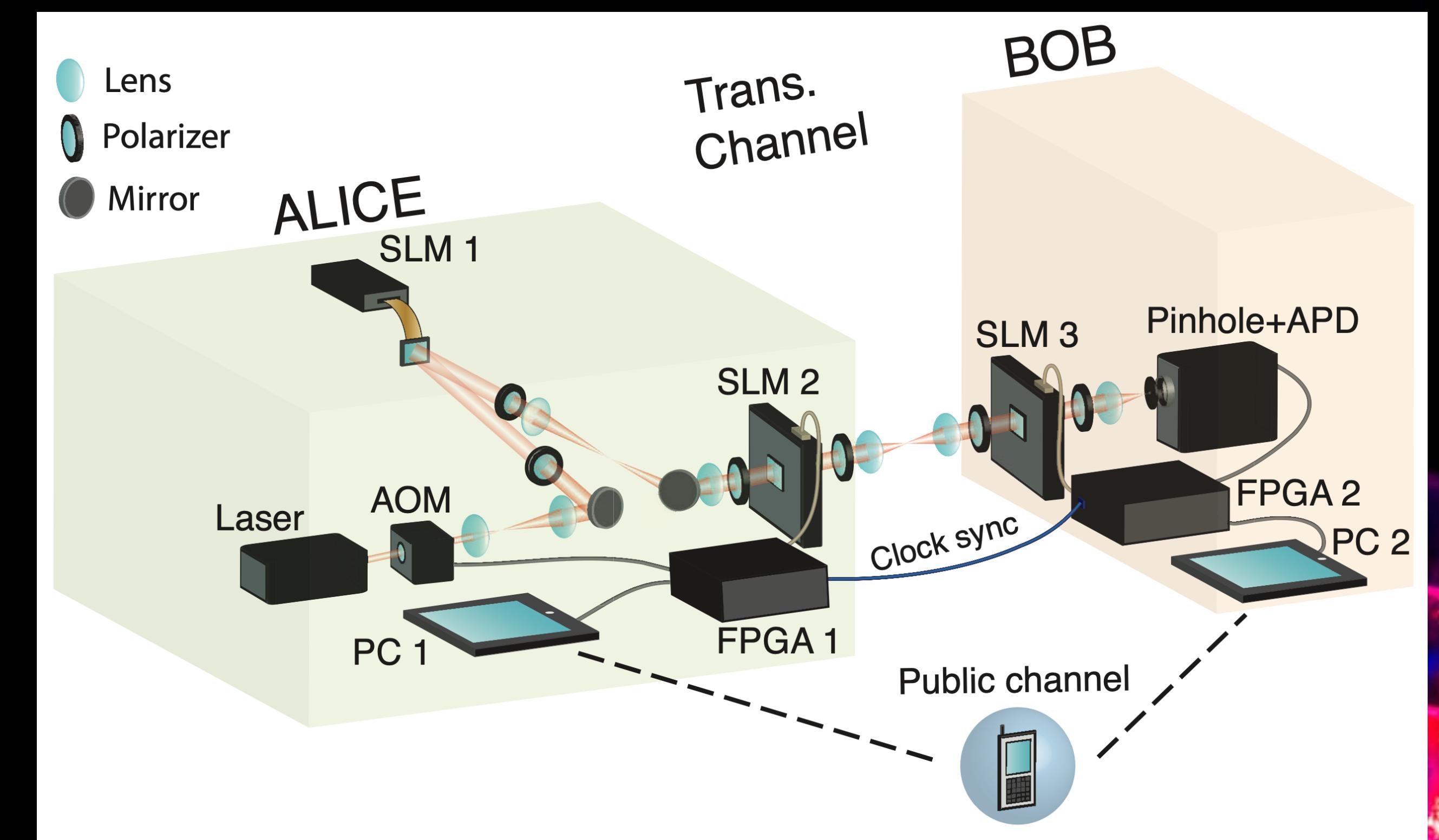
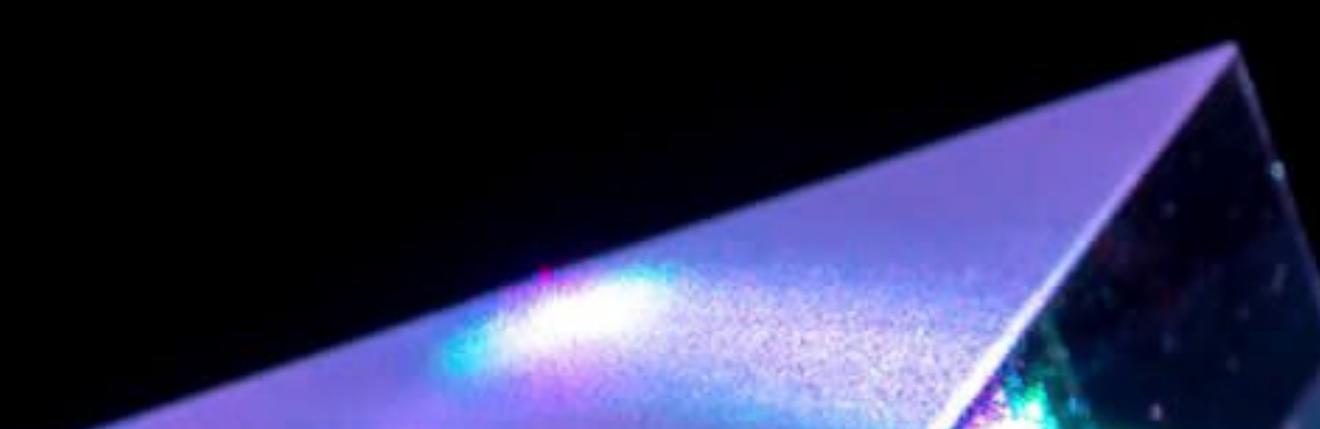
Correspondence and

Quantum key distribution session with 16-dimensional photonic states

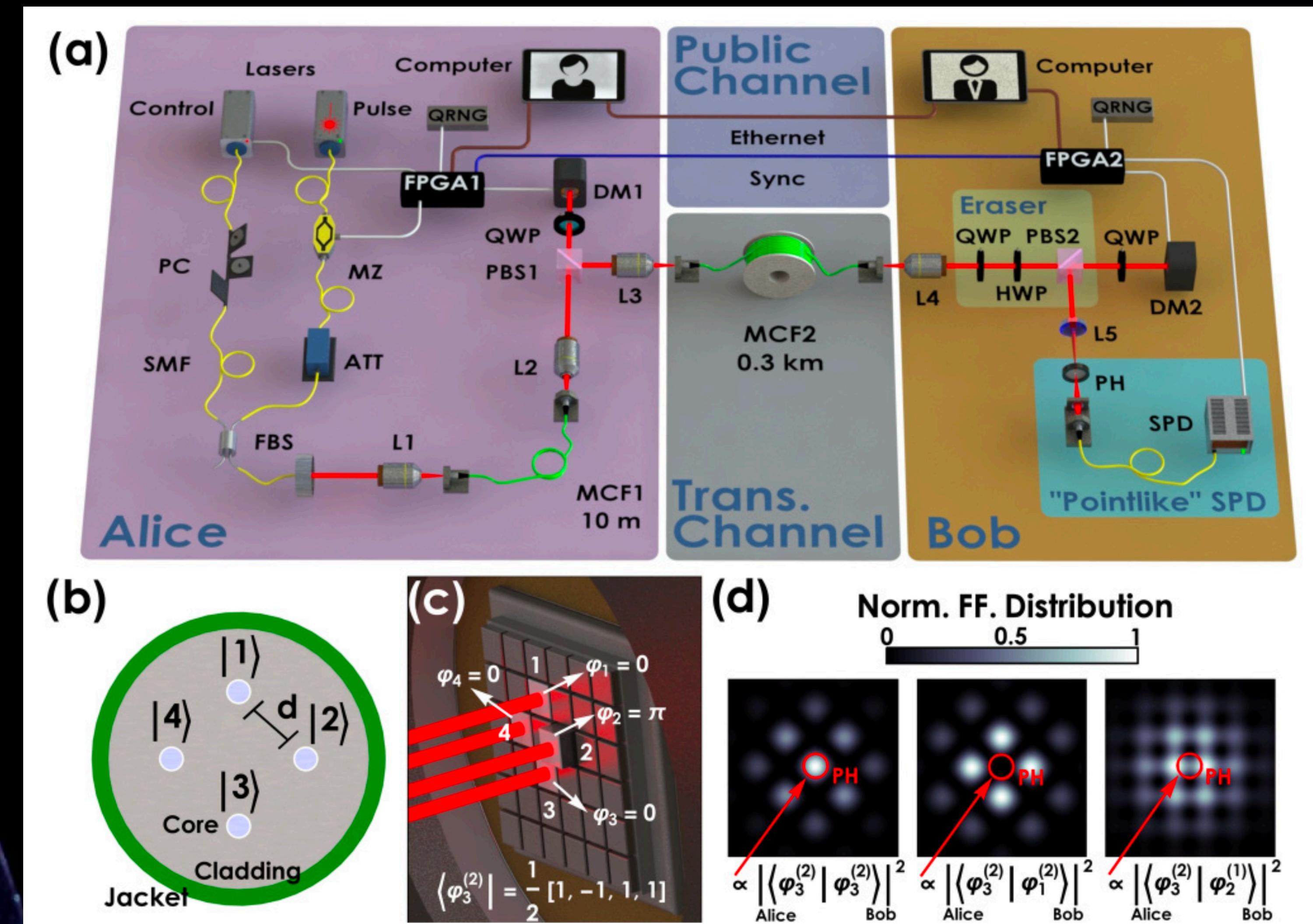
S. Etcheverry^{1,2}, G. Cañas^{1,2,3}, E. S. Gómez^{1,2,3}, W. A. T. Nogueira^{1,2,3}, C. Saavedra^{1,2}, G. B. Xavier^{2,3,4} & G. Lima^{1,2,3}

¹Departamento de Física, Universidad de Concepción, 160-C Concepción, Chile, ²Center for Optics and Photonics, Universidad de Concepción, Concepción, Chile, ³MSI-Nucleus for Advanced Optics, Universidad de Concepción, Concepción, Chile,
⁴Departamento de Ingeniería Eléctrica, Universidad de Concepción, 160-C Concepción, Chile.

The secure transfer of information is an important problem in modern telecommunications. Quantum key distribution (QKD) provides a solution to this problem by using individual quantum systems to generate correlated bits between remote parties, that can be used to extract a secret key. QKD with D -dimensional quantum channels provides security advantages that grow with increasing D . However, the vast majority of QKD implementations has been restricted to two dimensions. Here we demonstrate the feasibility of using higher dimensions for real-world quantum cryptography by performing, for the first time, a fully automated QKD session based on the BB84 protocol with 16-dimensional quantum states. Information is encoded in the single-photon transverse momentum and the required states are dynamically generated with programmable spatial light modulators. Our setup paves the way for future developments in the field of experimental high-dimensional QKD.

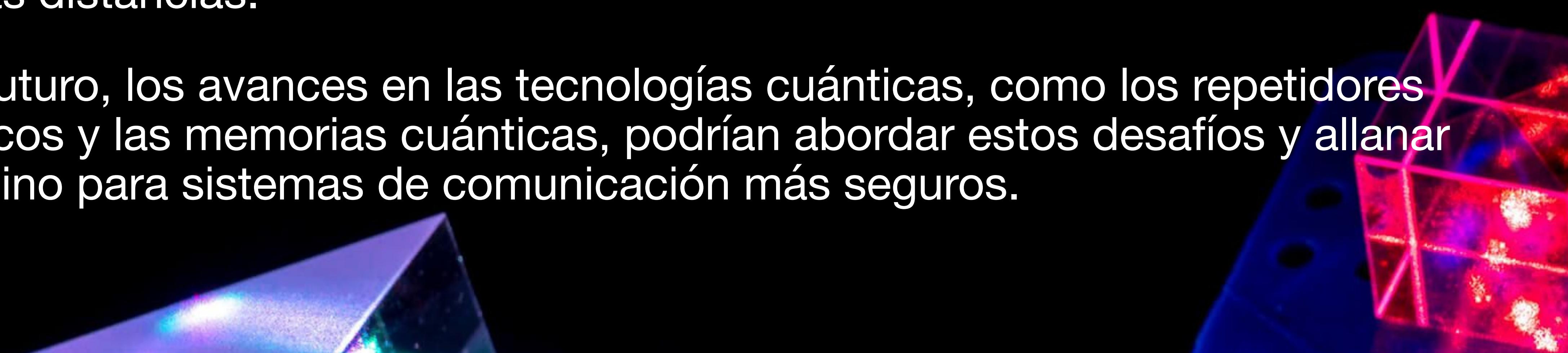


Experimentos realizados en Chile



Desafíos y perspectivas de futuro

- Un desafío de la criptografía cuántica es la vulnerabilidad de los sistemas de distribución de claves cuánticas a ataques debido a limitaciones tecnológicas.
- Otro desafío es la dificultad de ampliar los sistemas criptográficos cuánticos para soportar redes de comunicaciones a gran escala.
- Además, la criptografía cuántica enfrenta el desafío de lograr comunicaciones seguras a larga distancia, ya que las señales cuánticas tienden a degradarse a largas distancias.
- En el futuro, los avances en las tecnologías cuánticas, como los repetidores cuánticos y las memorias cuánticas, podrían abordar estos desafíos y allanar el camino para sistemas de comunicación más seguros.



Muchas gracias