Actividades en Comunicación Cuántica en Bariloche

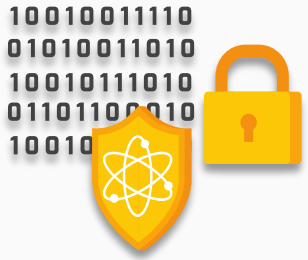
Juan Bonetti

22 de Junio de 2022

Comunicaciones Cuánticas

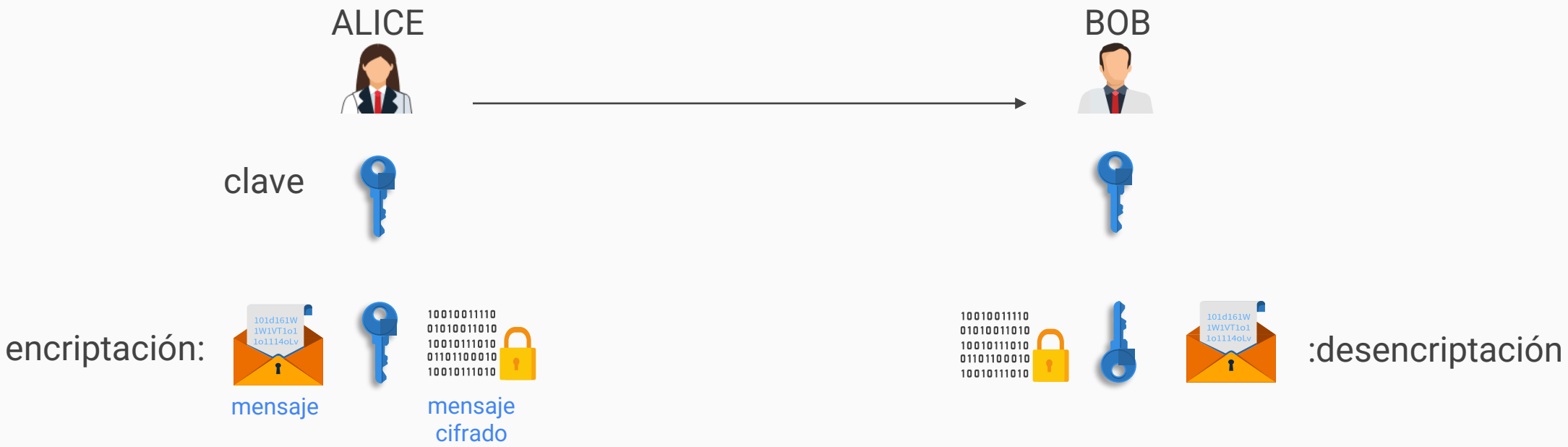
Son aquellas técnicas y sistemas que permiten utilizar los principios de la **física cuántica** para mejorar los sistemas de **comunicación clásica**.

Seguridad: comunicación secreta basada en las leyes fundamentales de la física.



Capacidad: la tasa de transmisión del canal puede superar los límites clásicos.

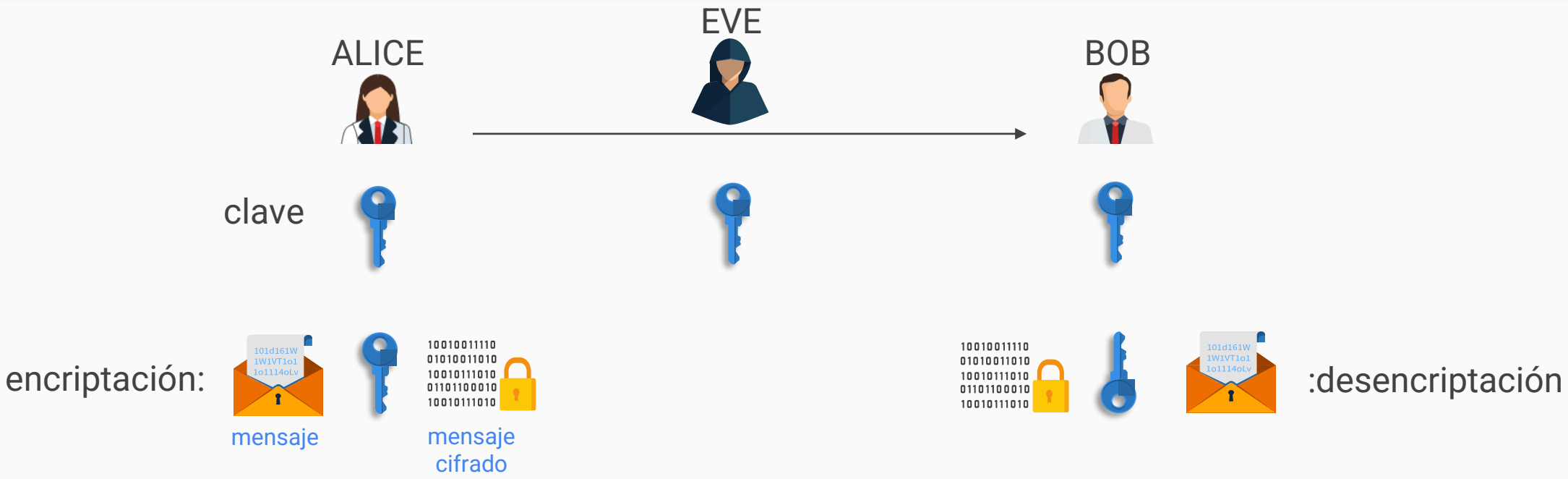
Comunicaciones Seguras



Protocolos de clave simétrica:

1. Alice genera la clave de encriptación y desencriptación.
2. Alice comparte la clave con Bob.
3. Alice encripta el mensaje.
4. Alice envía el mensaje cifrado a Bob, usando un canal de comunicación público.
5. Bob desencripta el mensaje cifrado.

Comunicaciones Seguras

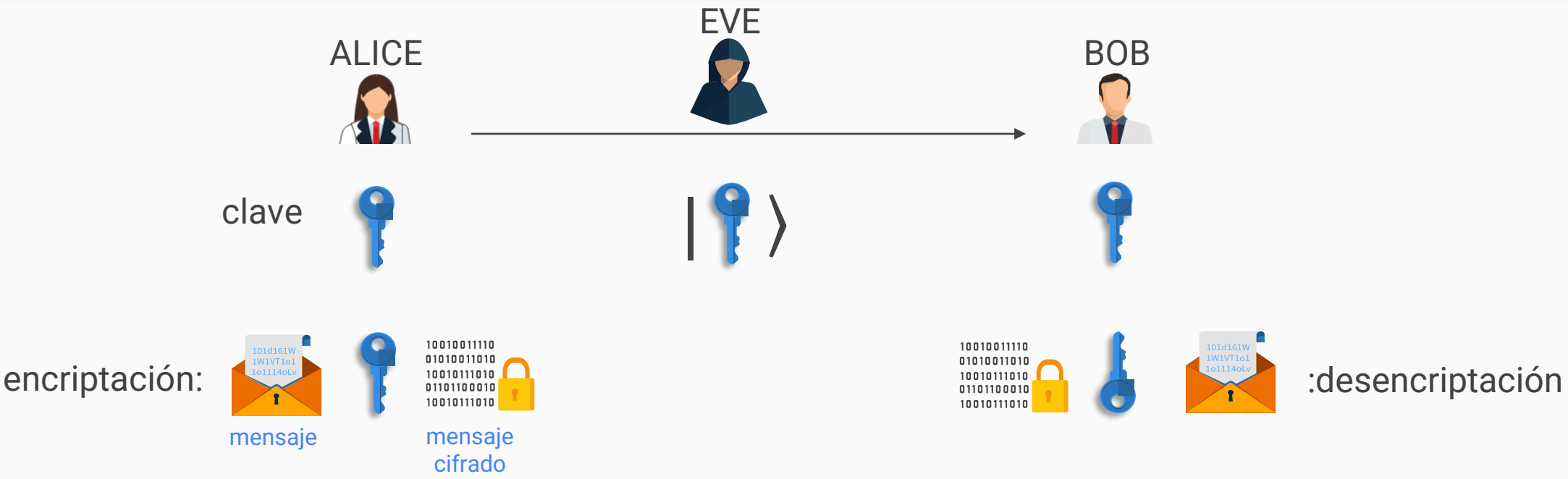


Protocolos de clave simétrica:

1. Alice genera la clave de encriptación y desencriptación.
2. **Alice comparte la clave con Bob.**
3. Alice encripta el mensaje.
4. Alice envía el mensaje cifrado a Bob, usando un canal de comunicación público.
5. Bob desencripta el mensaje cifrado.

Problema de la distribución de claves: ¿Cómo evitar que EVE obtenga la clave de desencriptación?

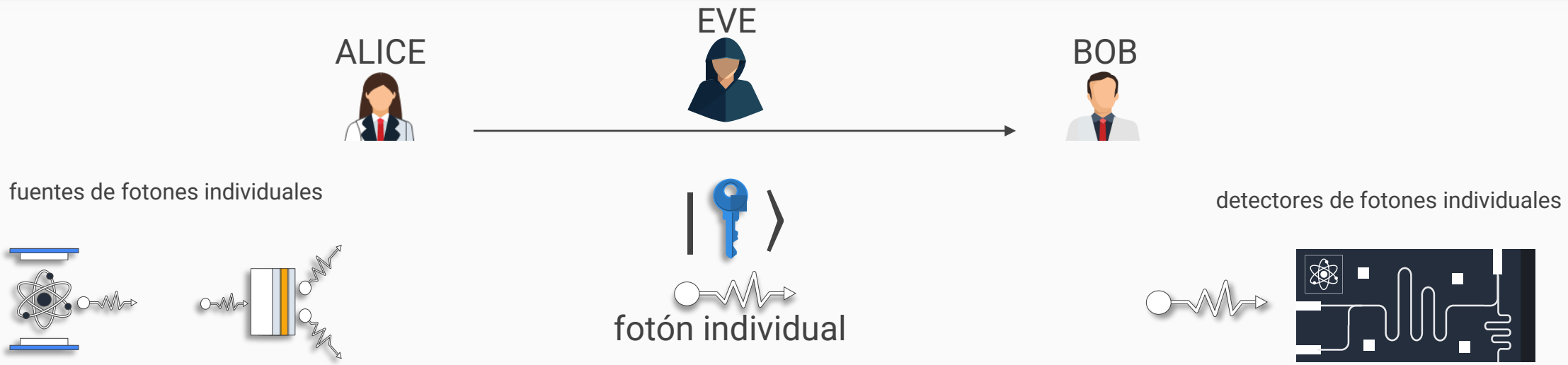
Comunicaciones Seguras



Protocolos de distribución cuántica de claves (QKD):

- Alice comparte la clave utilizando estados cuánticos.
- Los estados cuánticos no pueden copiarse (teorema de no clonación).
- Las mediciones del estado cuántico lo alteran irreversiblemente (colapso del estado cuántico).
- Cualquier interacción de Eve con el estado cuántico produce ruido en el canal.
- Los protocolos de QKD permiten detectar este ruido e interrumpir la comunicación en presencia de EVE.

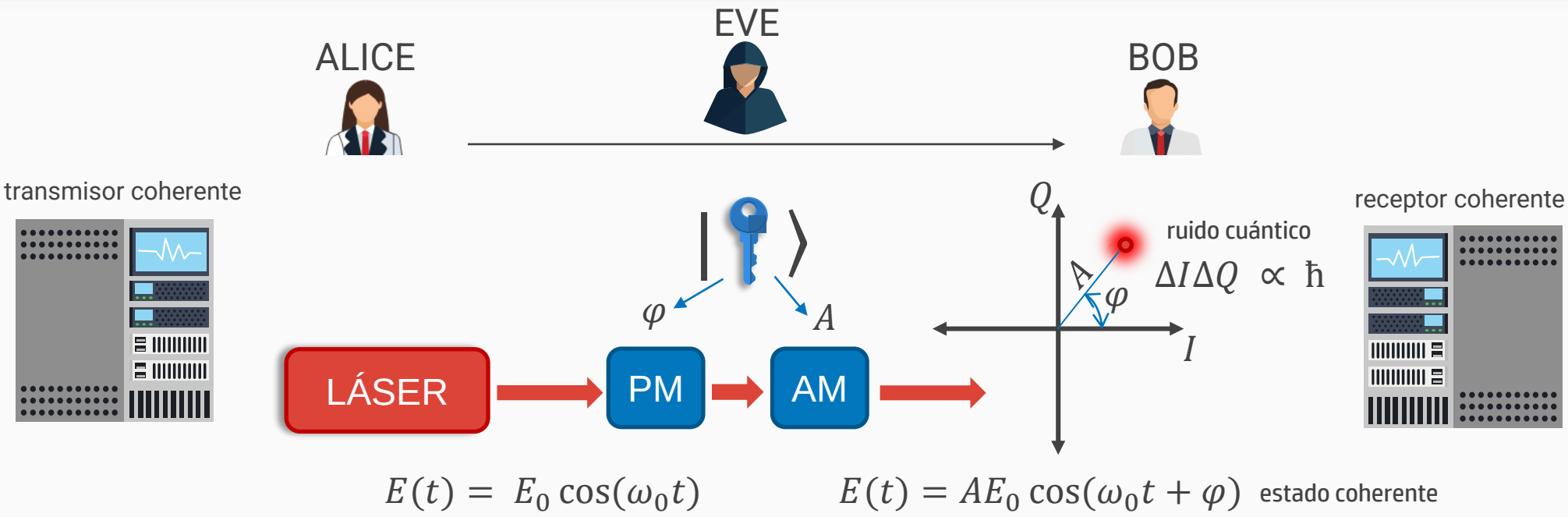
Implementación de protocolos de QKD



QKD de variable discreta (DV-QKD):

- Los estados cuánticos son fotones (partículas de luz) individuales.
- Normalmente, los bits de la clave se codifican en una variable discreta del fotón, como su polarización: $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$.
- En fibras ópticas, el estado de polarización del fotón puede variar fácilmente; nuevos formatos de modulación (*e.g.*, codificación por color) podrían ser más robustos.
- Alice y Bob deben estar equipados con fuentes y receptores de fotones individuales, respectivamente.
- Son equipos costosos, muy sensibles al ruido y, en general, operan a bajas temperaturas.

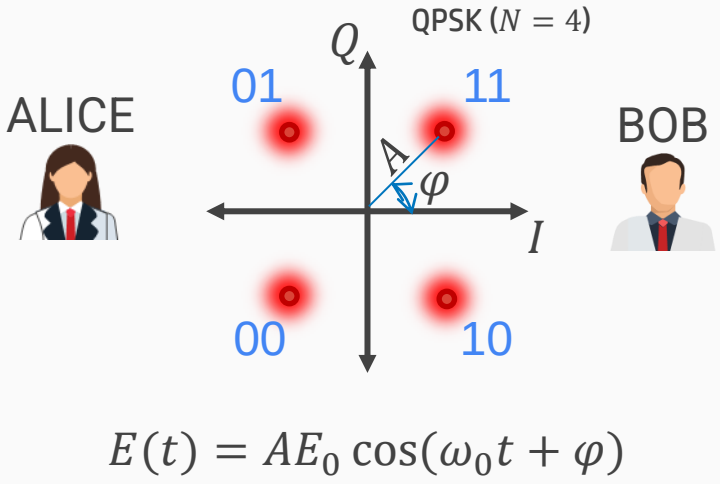
Implementación de protocolos de QKD



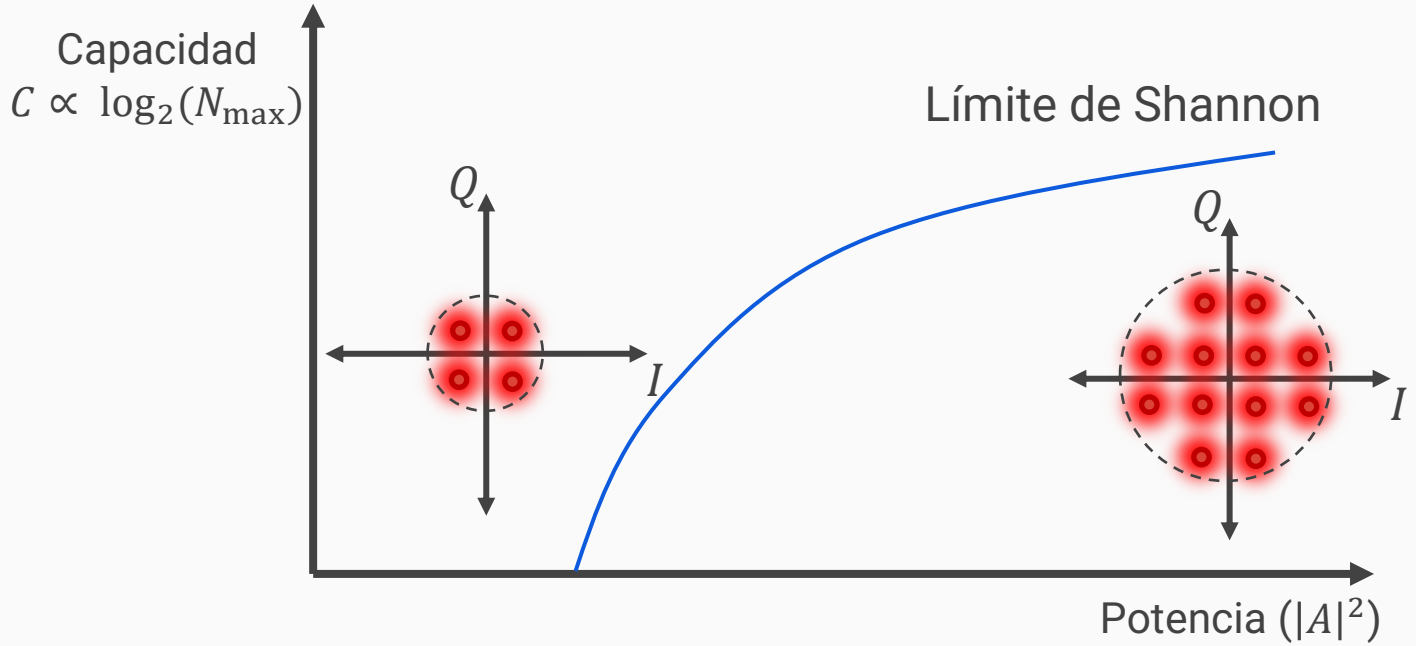
QKD de variable contínua (CV-QKD):

- Alice y Bob están equipados con un transmisor y receptor coherentes, comúnmente utilizados en los sistemas de comunicación óptica actuales.
- Alice codifica la clave en la amplitud (A) y la fase (φ) de una onda contínua de baja intensidad.
- Bob recupera la clave midiendo I y Q.
- El resultado de estas mediciones presenta una incertidumbre fundamental (ruido cuántico).
- Cualquier intervención de Eve incrementa el ruido de las mediciones.
- Estos protocolos requieren mayor procesamiento de las mediciones y las pruebas de seguridad son más complicadas.

Capacidad de las Comunicaciones Cuánticas



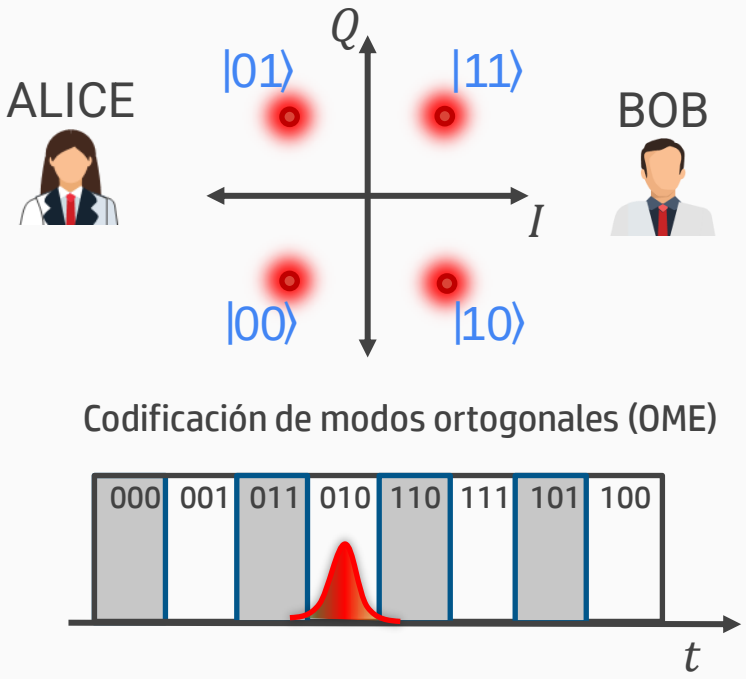
$$E(t) = AE_0 \cos(\omega_0 t + \varphi)$$

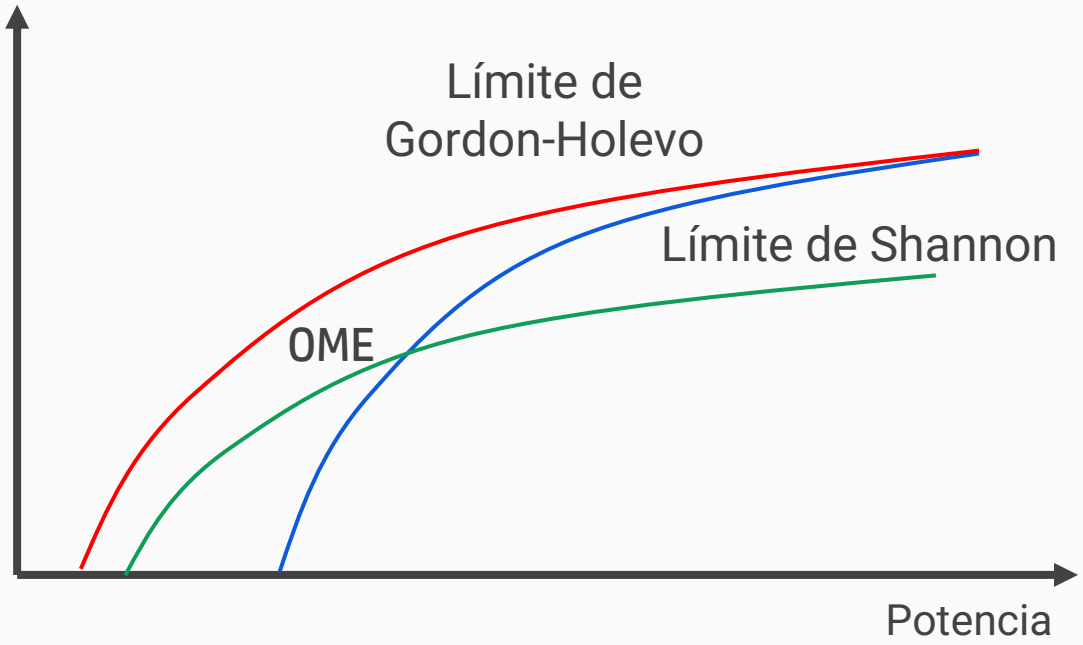


Comunicaciones coherentes en un canal ideal:

- Los bits transmitidos se codifican mediante N diferentes puntos en el plano I-Q (constelación).
- La capacidad del canal es la máxima cantidad de bits que pueden transmitirse por unidad de tiempo.
- La capacidad depende de la potencia de la señal transmitida.
- El cálculo teórico de la capacidad se conoce como límite de Shannon.

Capacidad de las Comunicaciones Cuánticas





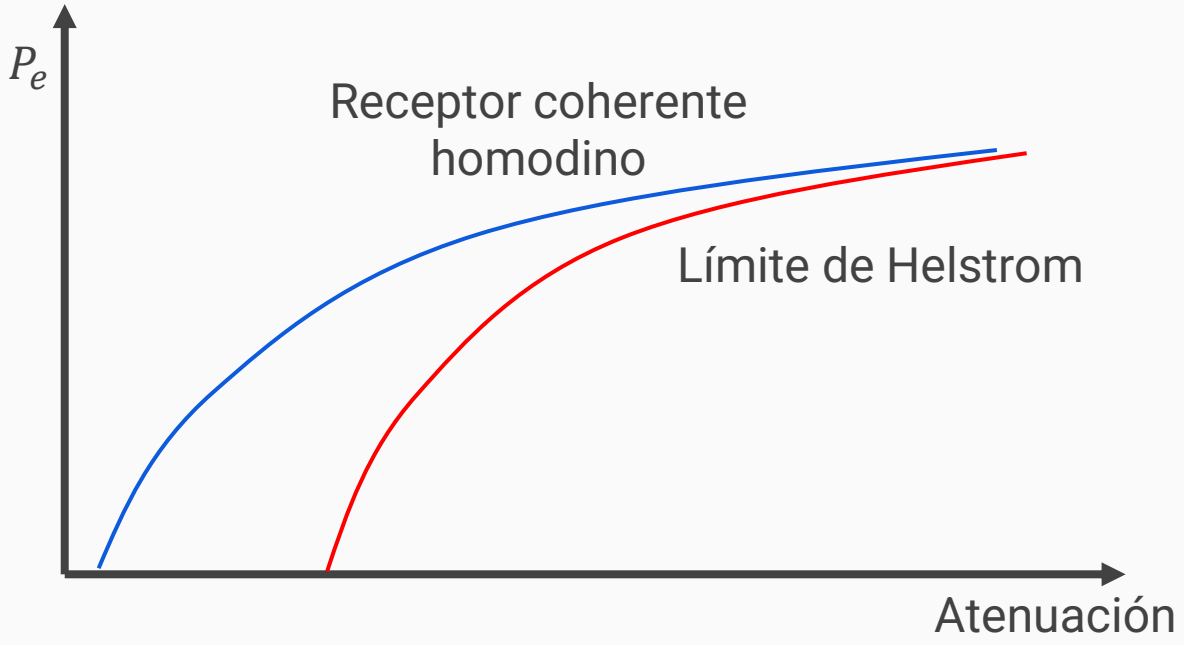
Comunicaciones cuánticas en un canal ideal:

- El cálculo teórico de la capacidad del canal, teniendo en cuenta la naturaleza cuántica de la luz, se conoce como límite de Gordon-Holevo.
- Existe un gap entre los límites de Shannon y Gordon Holevo.
- Si Bob cuenta con un detector de fotones individuales, el formato OME sobrepasa el límite de Shannon.
- Nuevos formatos podrían acercarse más al límite de Gordon-Holevo.

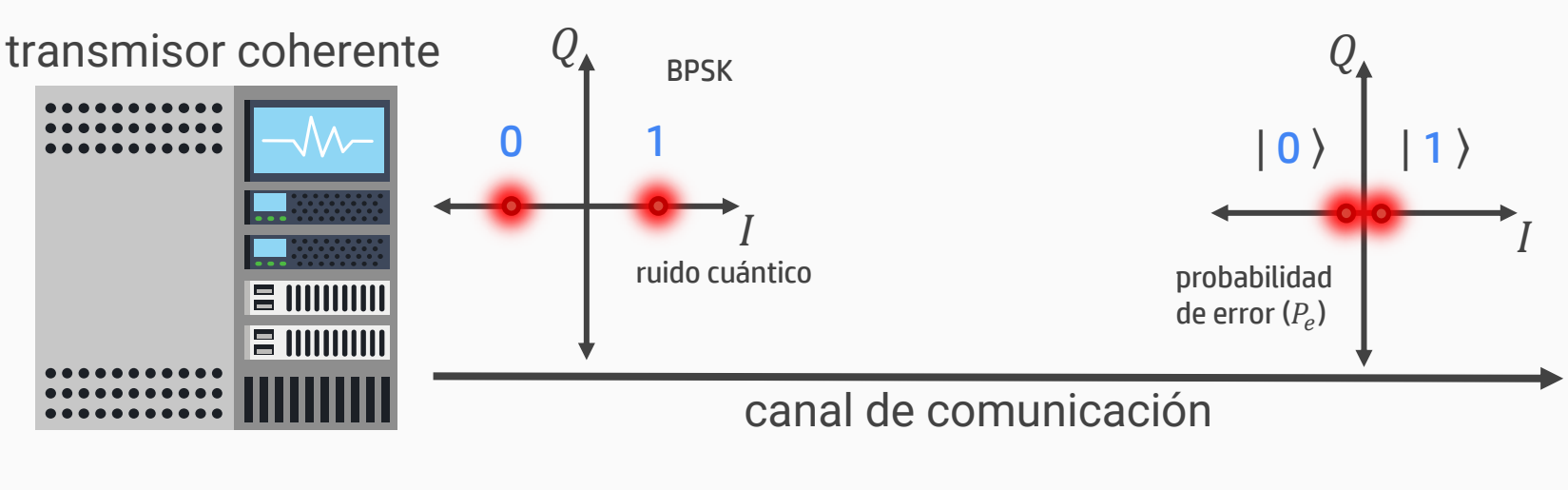
Receptores Mejorados Cuánticamente

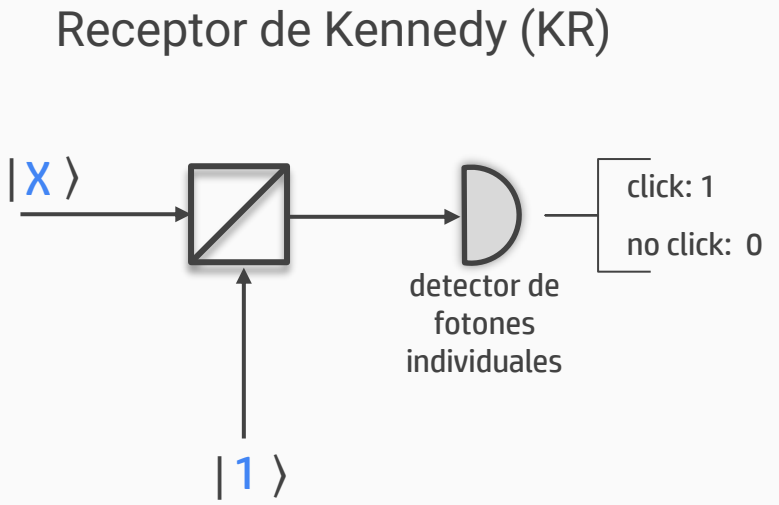
Comunicaciones coherentes en un canal ideal con atenuación:

- El mejor receptor clásico conocido es el receptor coherente homodino.
- Si se tiene en cuenta la naturaleza cuántica de la luz, es posible obtener menor probabilidad de error (límite de Helstrom).



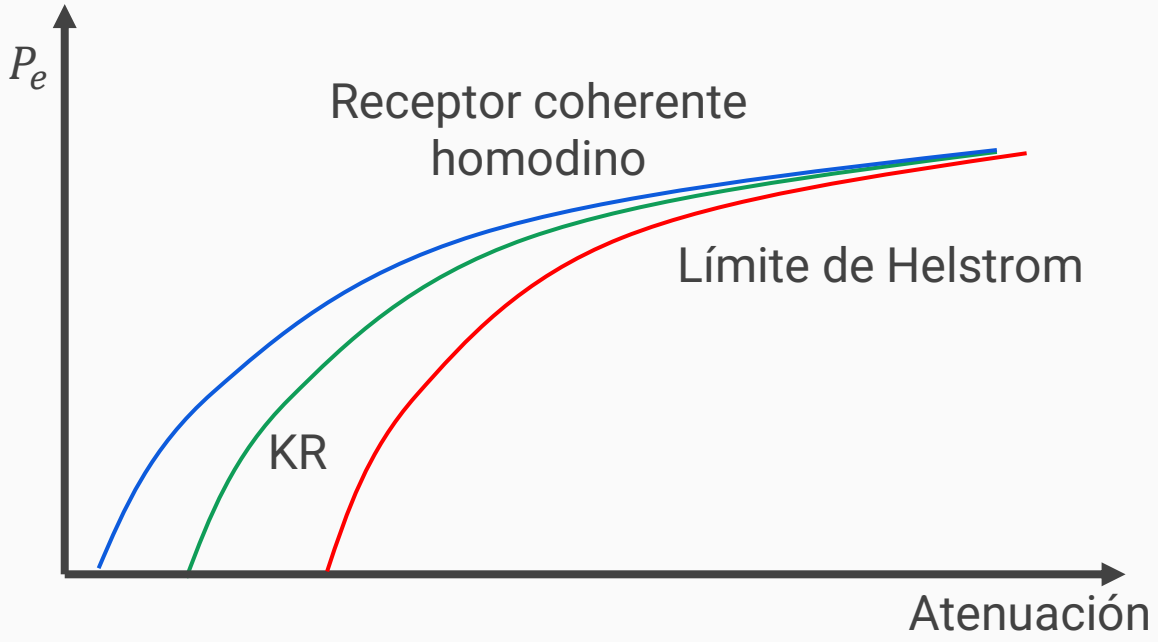
Receptores Mejorados Cuánticamente





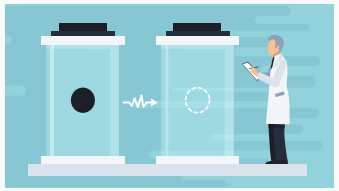
Comunicaciones coherentes en un canal ideal con atenuación:

- El mejor receptor clásico conocido es el receptor coherente homodino.
- Si se tiene en cuenta la naturaleza cuántica de la luz, es posible obtener menor probabilidad de error (límite de Helstrom).
- El receptor de Kennedy logra una mejor distinción de los estados coherentes.
- Nuevos detectores podrían acercarse más al límite de Helstrom, incluso para otros formatos de modulación.



Línea de Investigación

Comunicaciones Cuánticas

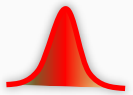
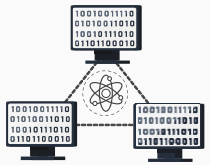
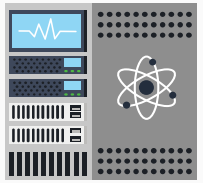


Seguridad

- DV- QKD
- CV- QKD

Capacidad

- Canales de alta capacidad
- Receptores cuánticos

TEORÍA		OBJETIVOS
Óptica cuántica [1]		*Nuevas fuentes de fotones individuales* [2], *nuevas implementaciones de los protocolos* [3]
Pruebas de seguridad		*Nuevos formatos*
Límite de Gordon-Holevo [4]		
Límite de Helstrom		*Nuevos receptores*

[1] J. Bonetti, S. M. Hernandez & D. F. Grosz (2021). Master equation approach to propagation in nonlinear fibers. *Optics Letters*, 46(3), 665-668.
[2] J. Bonetti, N. Linale & D. F. Grosz (2022). Heralded single-photon sources based on 2D-decorated nanowires. *Physics Letters A*, 432, 128018.
[3] J. Bonetti, S. M. Hernandez & D. F. Grosz (2018). A frequency-coded QKD scheme with an extension to qu-quarts. *arXiv preprint,* arXiv:1806.10971.
[4] J. Bonetti, D. F. Grosz & S. M. Hernandez (2021). Quantum Noise in Fibers with Arbitrary Nonlinear Profiles. *Physical Review Letters*, 126(21), 213602.

¡MUCHAS GRACIAS!