¿Podemos proteger nuestra información ante el todopoderoso ordenador cuántico?

Verónica Fernández Mármol

Grupo de Criptografía y Seguridad de la Información

Instituto de Tecnologías Físicas y de la Información (ITEFI)

C/ Serrano, 144, Madrid

CSIC

Email: veronica.fernandez@iec.csic.es

¿Por qué es importante la Criptografía?

Criptografía Clásica

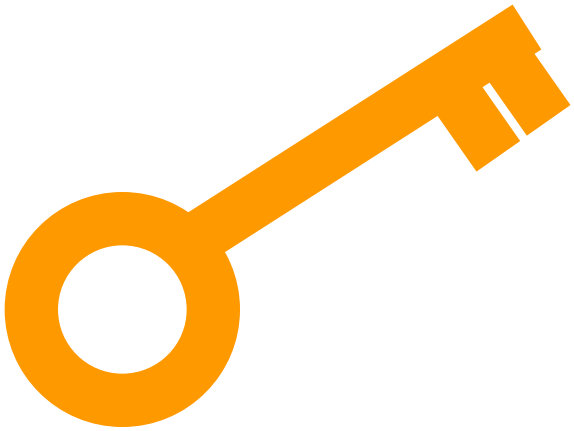
Criptografía simétrica

o

clave secreta

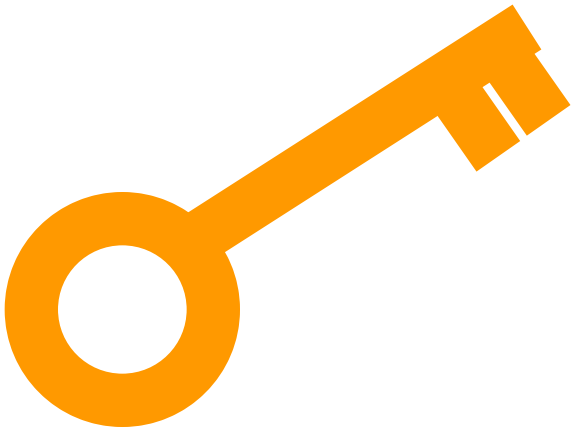
Criptografía Clásica

Una sola clave



Criptografía Clásica

Debe mantenerse en secreto



Criptografía Clásica

AES

Advanced Encrytpion Standard

ejemplo paradigmático

Criptografía Clásica

¿Es seguro AES?

Criptografía Clásica

Longitud

128, 192 y 256 bits

Criptografía Clásica

Son muy rápidos

Criptografía Clásica

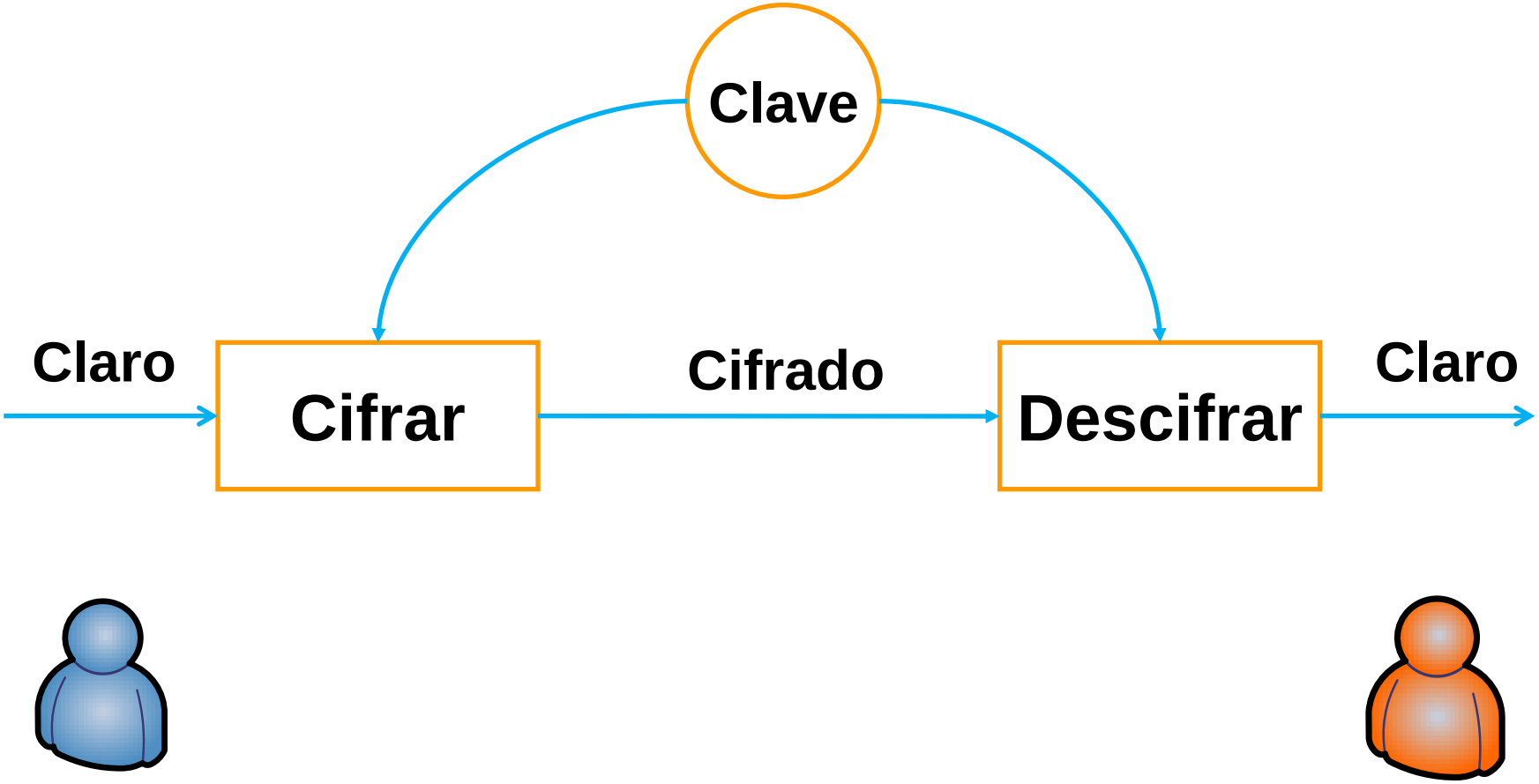
Discos duros

Base de datos

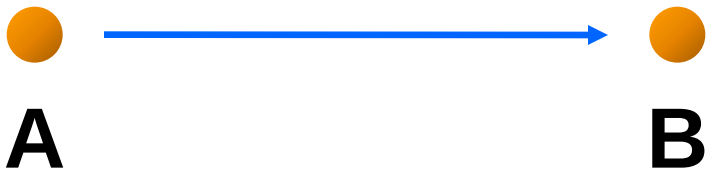
Comunicaciones de red

Cifran cantidades grandes

Criptografía Clásica



Criptografía Clásica



¿Cómo distribuir la clave?

Criptografía Clásica

Criptografía asimétrica
o
de clave pública

Criptografía Clásica

Merkle, Diffie y Hellman (1976)

Algoritmo de Diffie-Hellman

Criptografía Clásica

Servicio de Inteligencia británico

Criptografía Clásica

claves: pública y privada

Criptografía Clásica

Clave pública

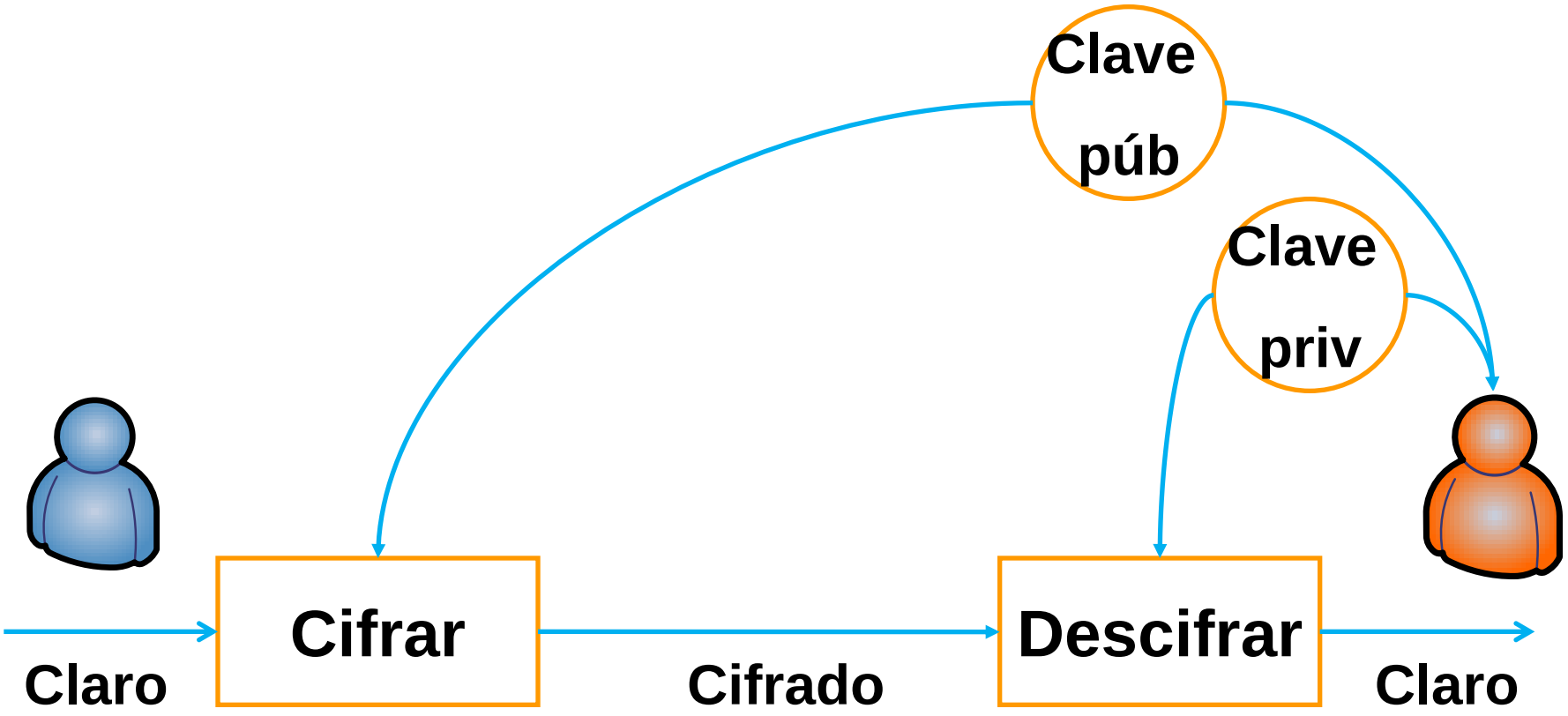
la conoce todo el mundo

Criptografía Clásica

Clave privada

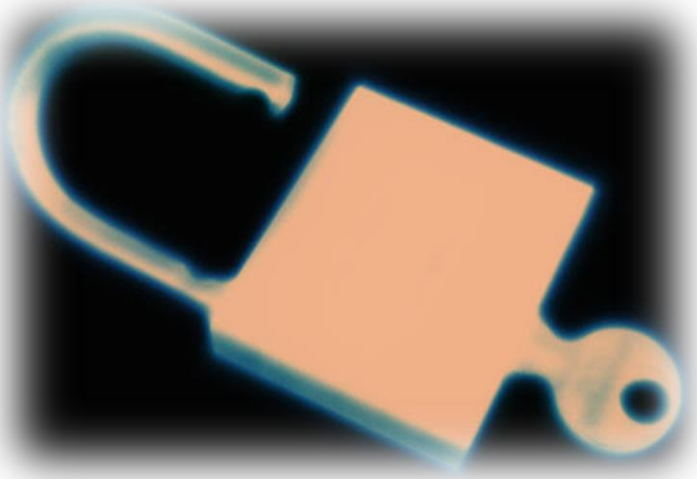
sólo la conoce una persona

Criptografía Clásica



Criptografía Clásica

Criptografía Clásica



Criptografía Clásica

1024

bits de longitud mínima

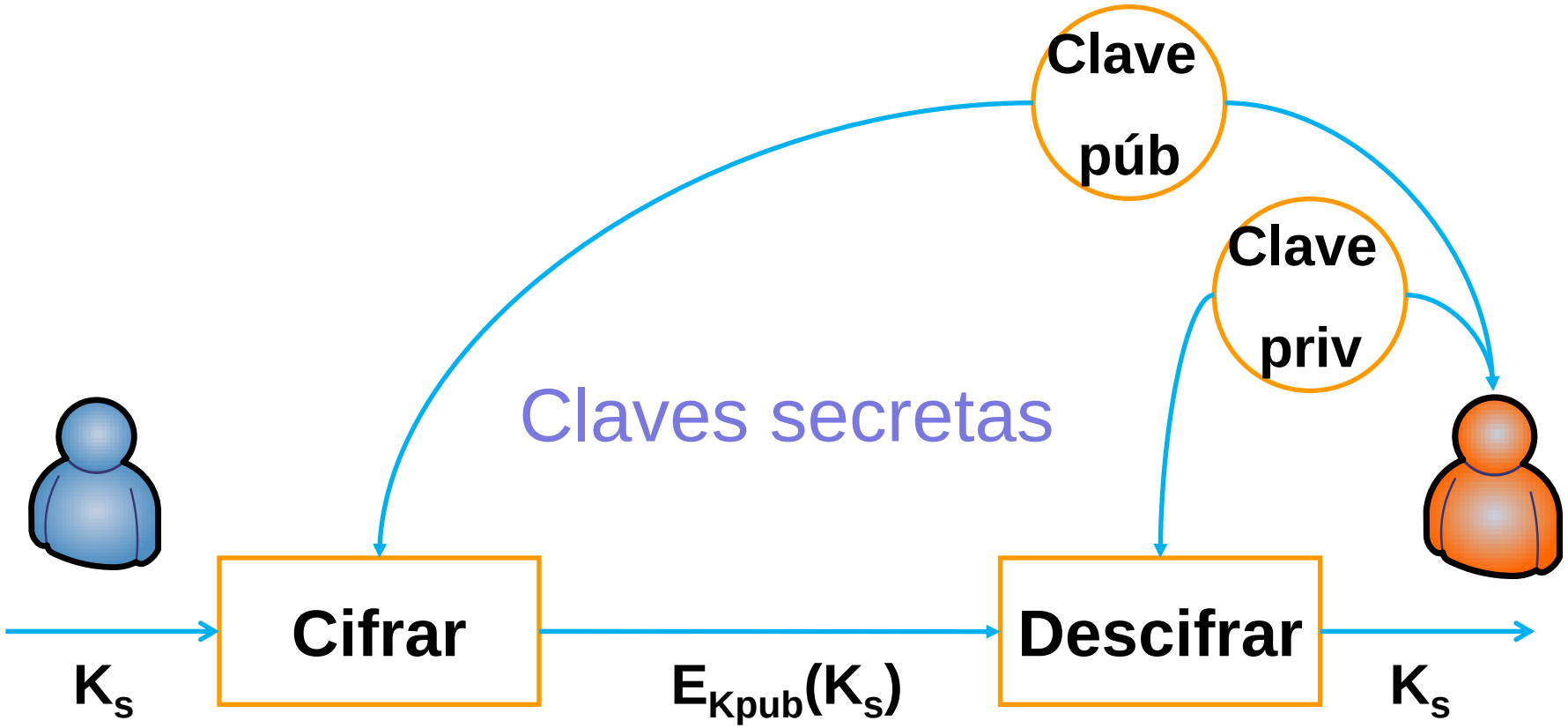
Criptografía Clásica

Son muy lentos

Criptografía Clásica

Cifran cantidades pequeñas

Criptografía Clásica



Criptografía Clásica

RSA (1977)

Criptografía Clásica

¿Es seguro RSA?
Claves:2048 a 4096 bits

Criptografía Clásica

¿En qué se basa su fortaleza?

Problema de la factorización

Criptografía Clásica

¿Factores de 15?

Criptografía Clásica

3 x 5

Criptografía Clásica

¿Factores de 391?

Criptografía Clásica

17 x 23

Criptografía Clásica

Retos RSA
512-bit en 1999,
663-bit en 2005,
y 768-bit en 2009

Criptografía Clásica

¿Cuánto se tarda en hacer operaciones matemáticas?

Sumar dos números de N bits

Criptografía Clásica

Tiempo lineal O(N)

Multiplicar dos números de N bits

Criptografía Clásica

Tiempo cuadrático $O(N^2)$

Criptografía Clásica

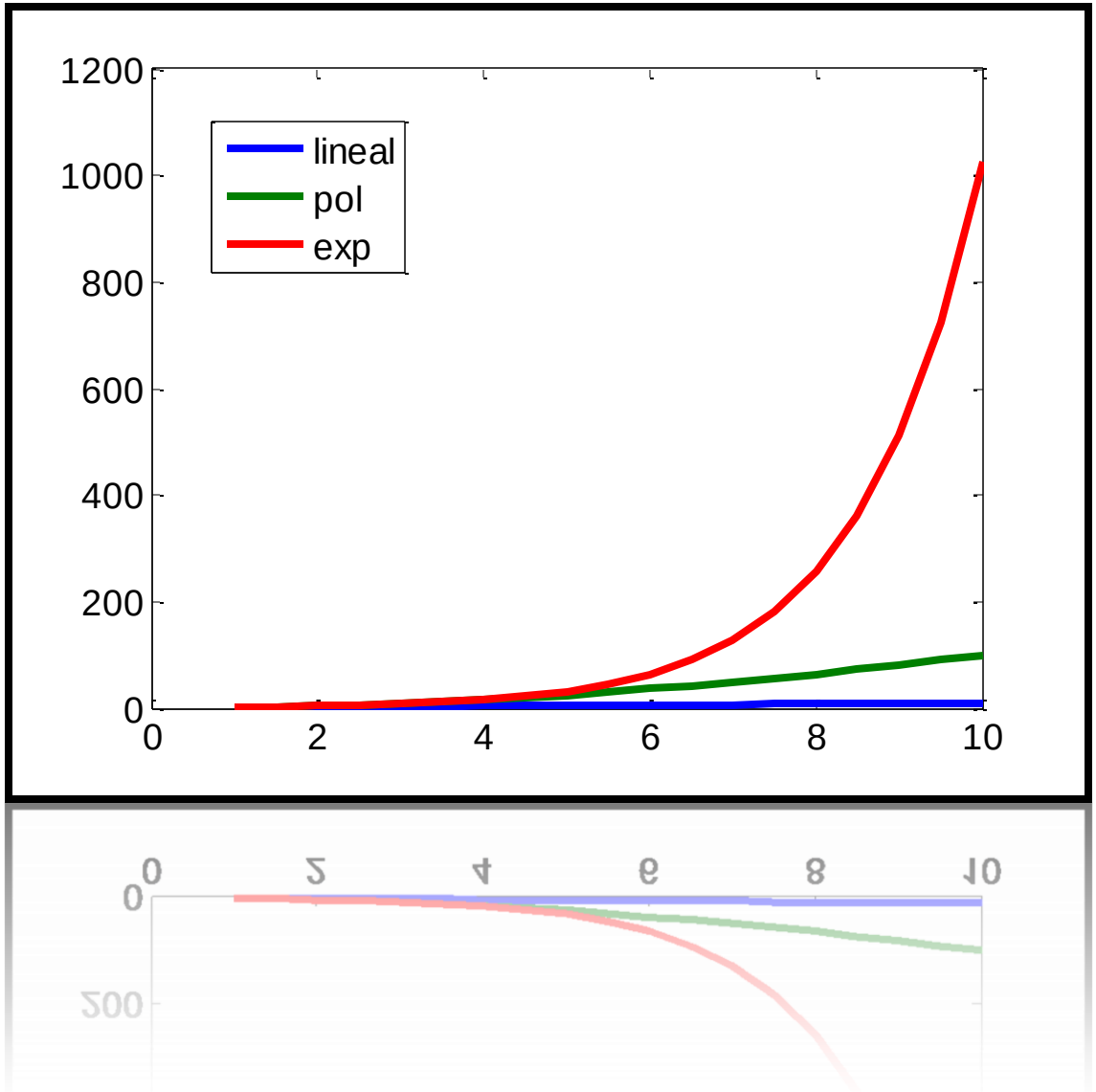
Factorizar un número de N bits

Criptografía Clásica

Tiempo exponencial

$O(e^N)$

Criptografía Clásica



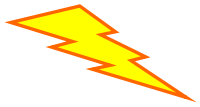
Criptografía Clásica

AMENAZAS:

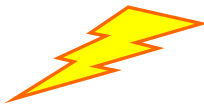
- La dificultad de la factorización no está probada matemáticamente
- Ordenador Cuántico

La amenaza del ordenador cuántico

Algoritmo de Shor (reducción en el tiempo de computación para factorizar de exponencial a polinómico en un ordenador cuantico)

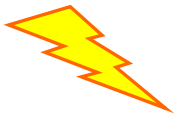


Criptografía de clave pública (RSA)

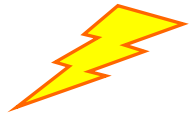


La amenaza del ordenador cuántico

Algoritmo de Grover (reducción en el tiempo de búsqueda de una base de datos con N entradas de N a $N^{1/2}$)



Criptografía simétrica (AES)



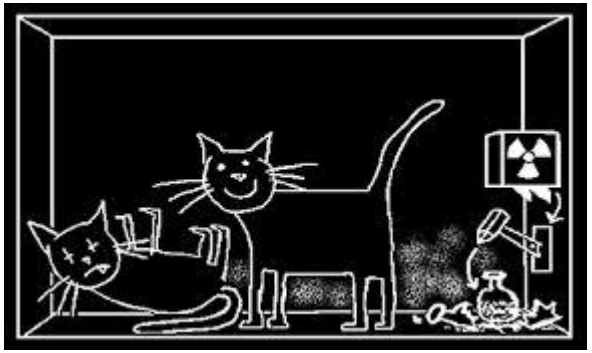
Solución: aumentar longitud de clave

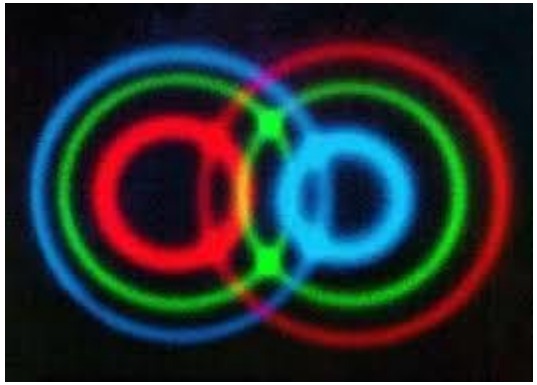
La amenaza del ordenador cuántico

¿En qué se basa la superioridad del ordenador cuántico?

Propiedades en las que se basa el ordenador cuántico

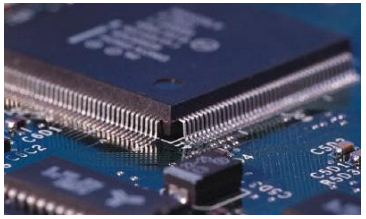
- Superposición cuántica
  - Mach-Zehnder single photon interferometry
  - Double split experiment
- Entrelazamiento





Ordenador Cuántico

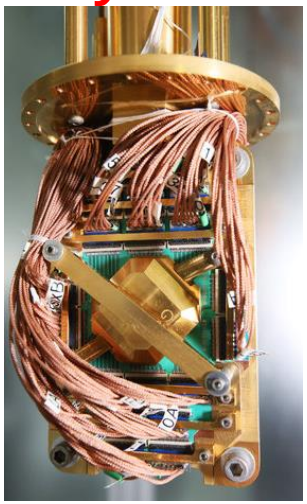
- Bit clásico: 0 (V = 0) ó 1 (V ≠ 0)



Circuito digital

- Bit cuántico o Qubit: 0 y 1
  - Partículas s-1/2

0 1 0 y 1



Ordenador cuántico Orión
512 qubits
D-Wave Systems

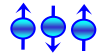
Ordenador Cuántico

- Registro de 3 bits

Registro clásico

000 

001 

010 

011 

100 

101 

110 

111 

Ordenador Cuántico

- Registro de 3 bits

En memoria 2^3 estados

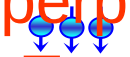
000

Regist

Computación en paralelo

110

111

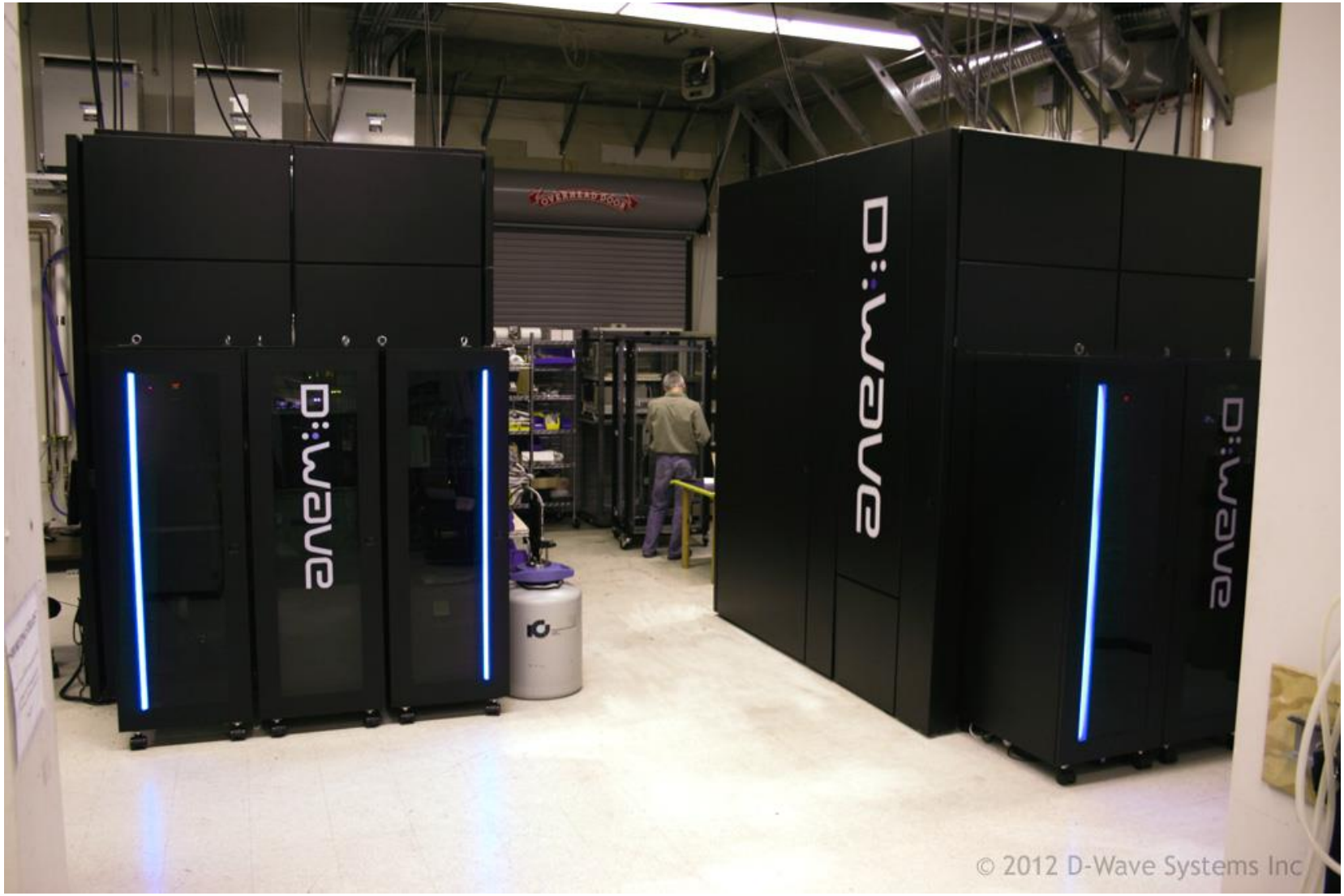


Si aumentamos el número de electrones en superposición a 50...computa 2^{50} bits simultáneamente (1000 Terabytes)

Últimos avances en los ordenadores cuánticos

- Cada ordenador de D-Wave: 10 y 15 millones de dólares, manejan 512 qbits (1000 qubits) y son 3.600 veces más rápidos que un computador convencional
- Polémica: ¿computación cuántica real?
- No es un ordenador de propósito general

Últimos avances en los ordenadores cuánticos



Últimos avances en los ordenadores cuánticos

- Lockheed Martin: mayor contratista militar del mundo
- 1er ordenador cuántico comercial
- Sofisticados sistemas de radar, simulaciones complejas aeroespaciales, etc…

Últimos avances en los ordenadores cuánticos

- Laboratorio de inteligencia artificial basado en computación cuántica para mejorar los sistemas de aprendizaje de la inteligencia artificial que están basados en complejos algoritmos de optimización.

Conclusiones

- La amenaza del ordenador cuántico es real (‘***NSA seeks to build quantum computer that could crack most types of encryption***’, **The Washington Post, Enero 2014**)

- La infraestructura de clave publica está ‘rota’ y es una cuestión del ‘cuando’ más que del ‘cómo’ prescindiremos de ella

¿Solución?

Posible solución para distribución de claves ante un ataque cuántico…

distribución cuántica de claves (QKD)

¿Qué es QKD?

El **único** método de transmitir claves criptográficas en el que la presencia de un intruso es detectada

¿En qué se basa la QKD?

- *Principio de Incertidumbre de Heisenberg*

Heisenberg

Heisenberg

$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

- *Teorema de No-Cloning*

En qué consiste la QKD

Alice

(Emisor)

Eve

Bob

(Receptor)

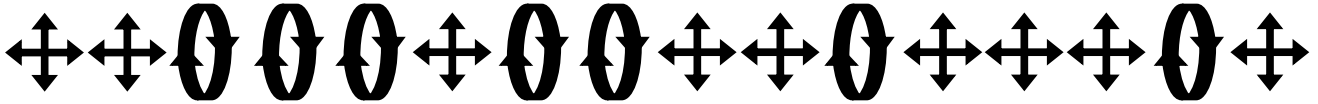
- Dos partes: Alice y Bob
- Dos canales de comunicación: cuántico y clásico
- Por el canal cuántico se transmiten fotones individuales
- Canal clásico para discusión pública
- Se puede detectar la presencia de un adversario!!

Protocolo BB84

ALICE

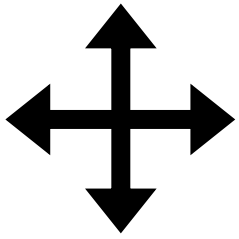
Secuencia aleatoria Base

0 1 1 0 1 0 0 1 1 0 0 0 1 0 1 1

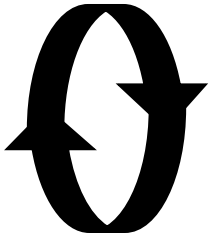


Alice quiere mandar una secuencia aleatoria a Bob

Alice utiliza aleatoriamente las bases:



Rectilínea



Circular

Protocolo BB84

ALICE

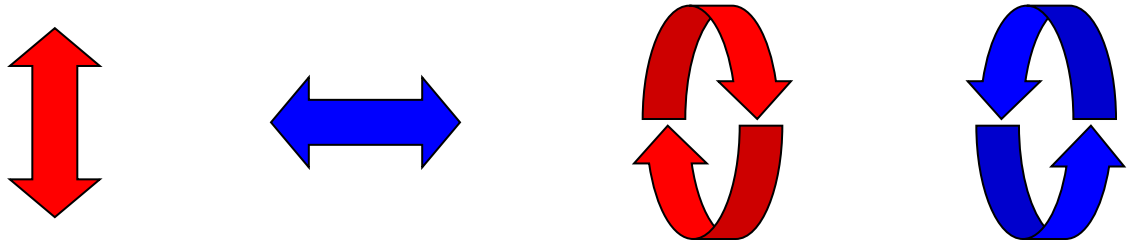
Secuencia aleatoria

0 1 1 0 1 0 0 1 1 0 0 0 1 0 1 1

Base

Polarización

Alice utiliza uno de los cuatro posibles estados de polarización para codificar sus estados



0 **1** **0** **1**

Protocolo BB84

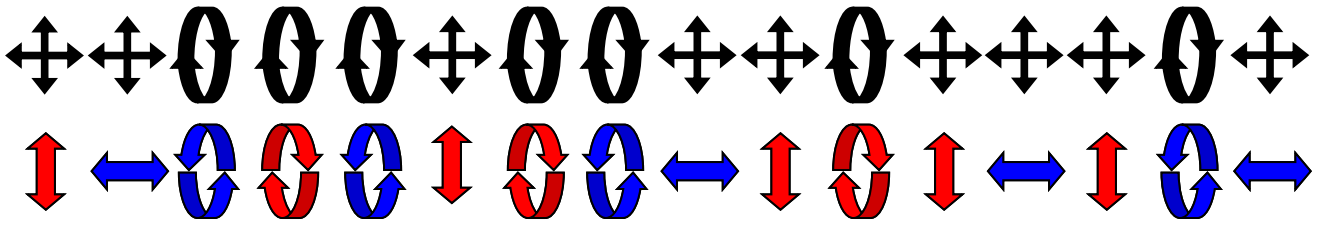
ALICE

Secuencia aleatoria

0 1 1 0 1 0 0 1 1 0 0 0 1 0 1 1

Base

Polarización



BOB

Alice manda su secuencia de fotones aleatoriamente codificados a Bob

Protocolo BB84

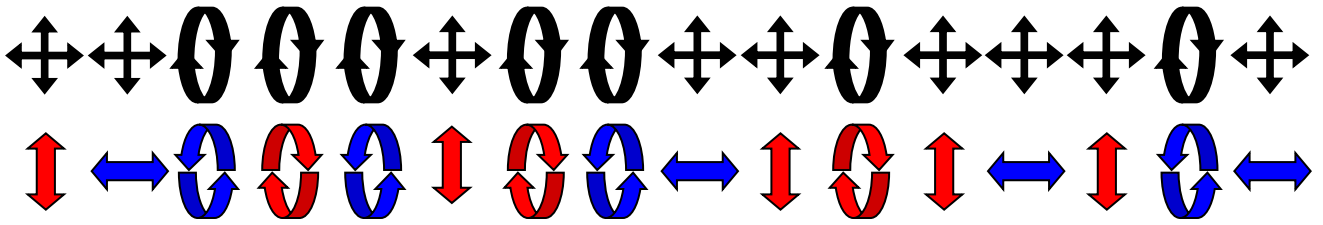
ALICE

Secuencia aleatoria

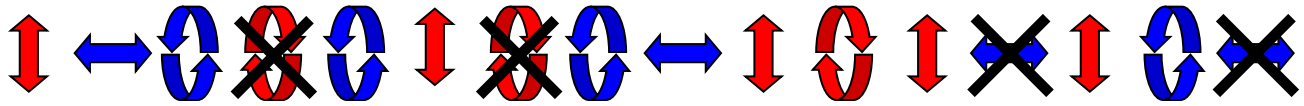
0 1 1 0 1 0 0 1 1 0 0 0 1 0 1 1

Base

Polarización



BOB



No todos los fotones que manda Alice son recibidos por Bob. Algunos se pierden como consecuencia de la absorción del canal cuántico

Protocolo BB84

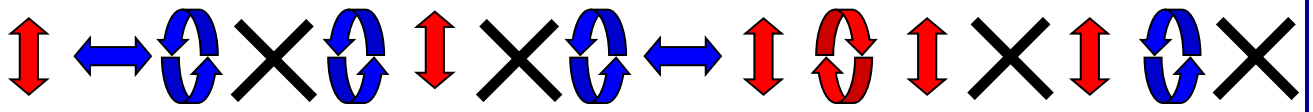
ALICE

Secuencia aleatoria

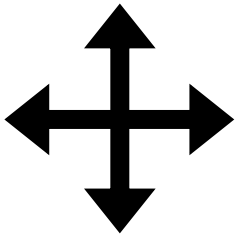
0 1 1 0 1 0 0 1 1 0 0 0 1 0 1 1

Base

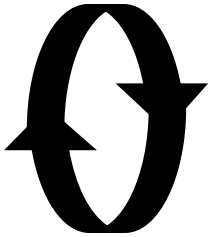
Polarización



BOB



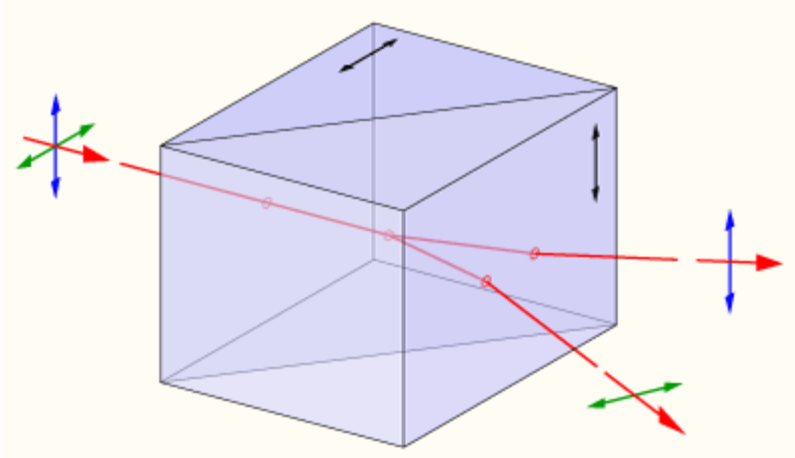
Rectilinea



Circular

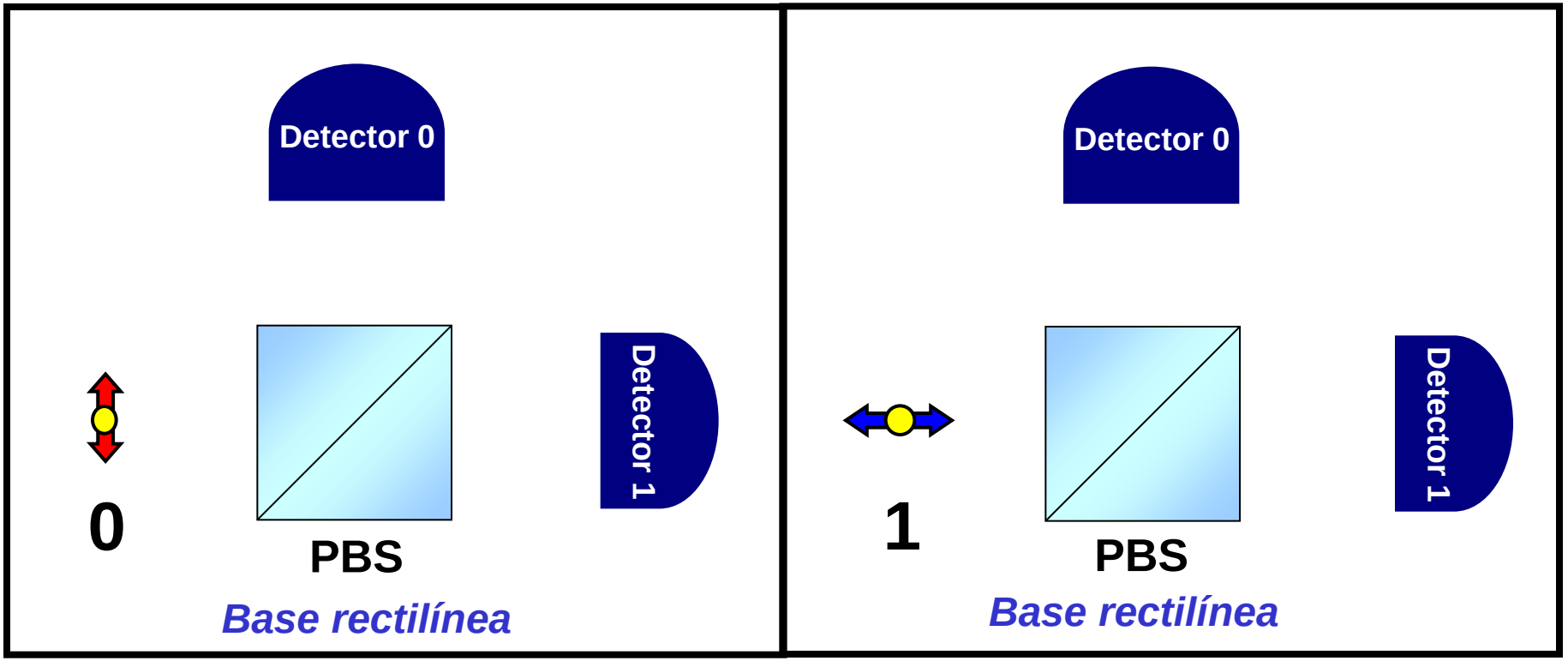
Bob utiliza la base circular o rectilinea de forma aleatoria para medir los fotones recibidos

Prisma de Wollaston



Divisor de haz por polarización (PBS)

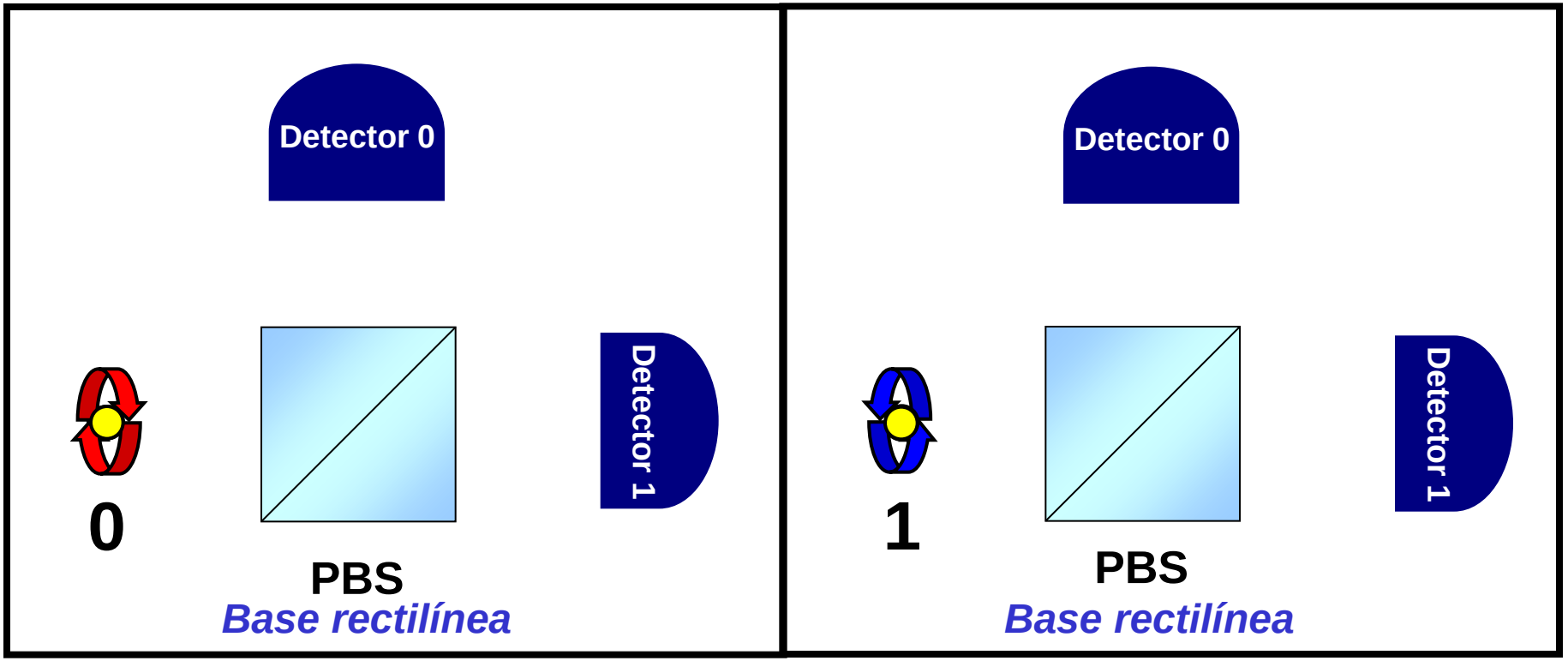
Protocolo BB84



Detecta '**0**' con 100% de probabilidad

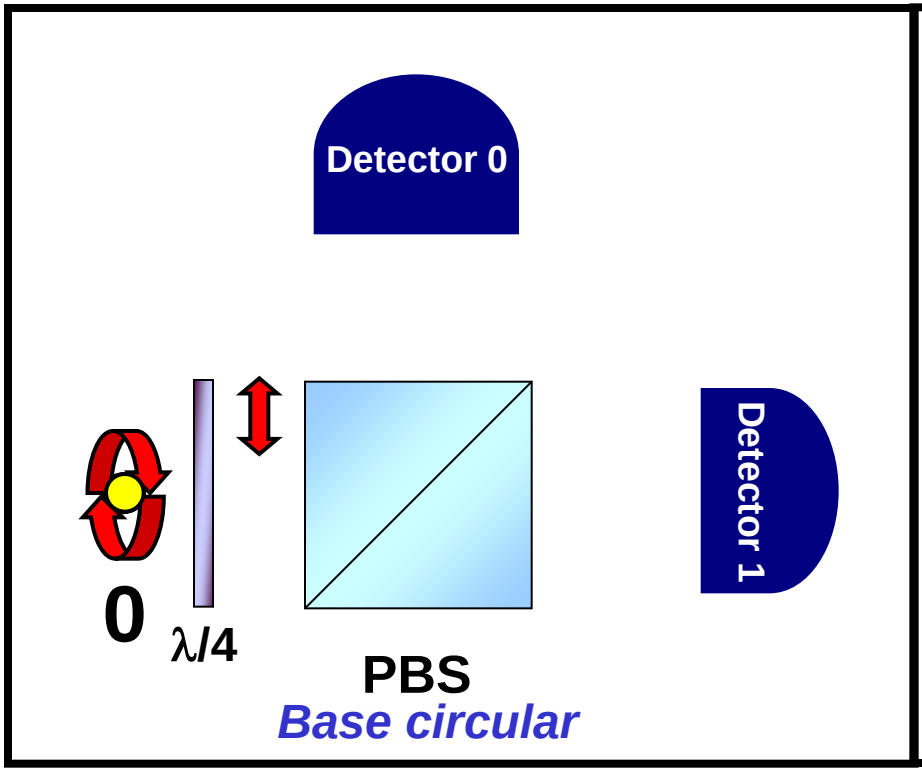
Detecta '**1**' con 100% de probabilidad

Protocolo BB84

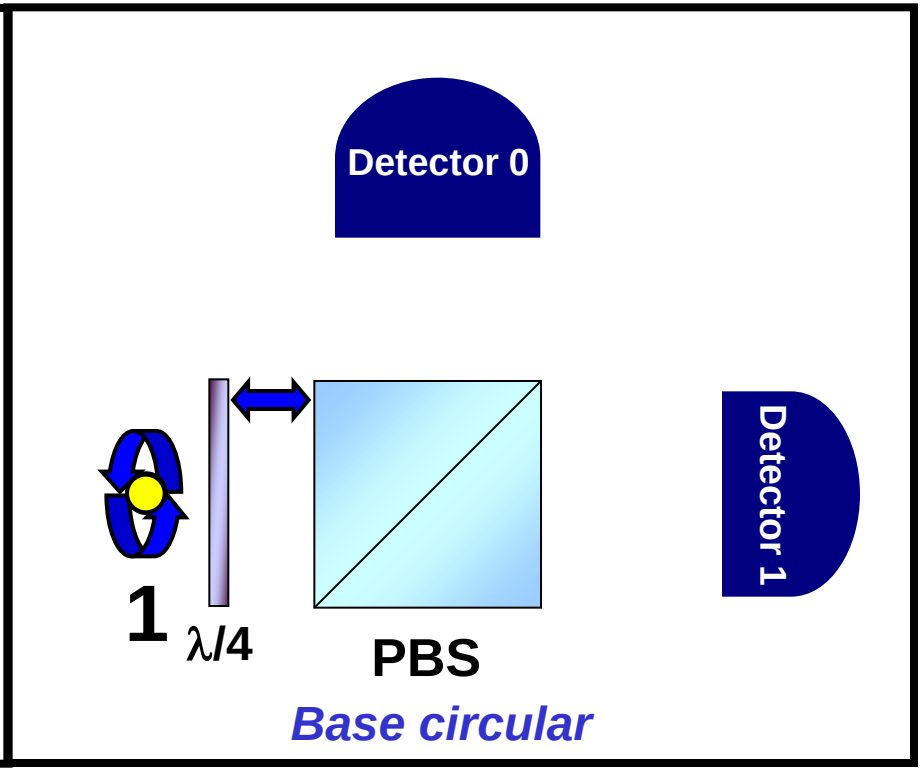


‘**0**’ o ‘**1**’ con 50% de probabilidad

Protocolo BB84

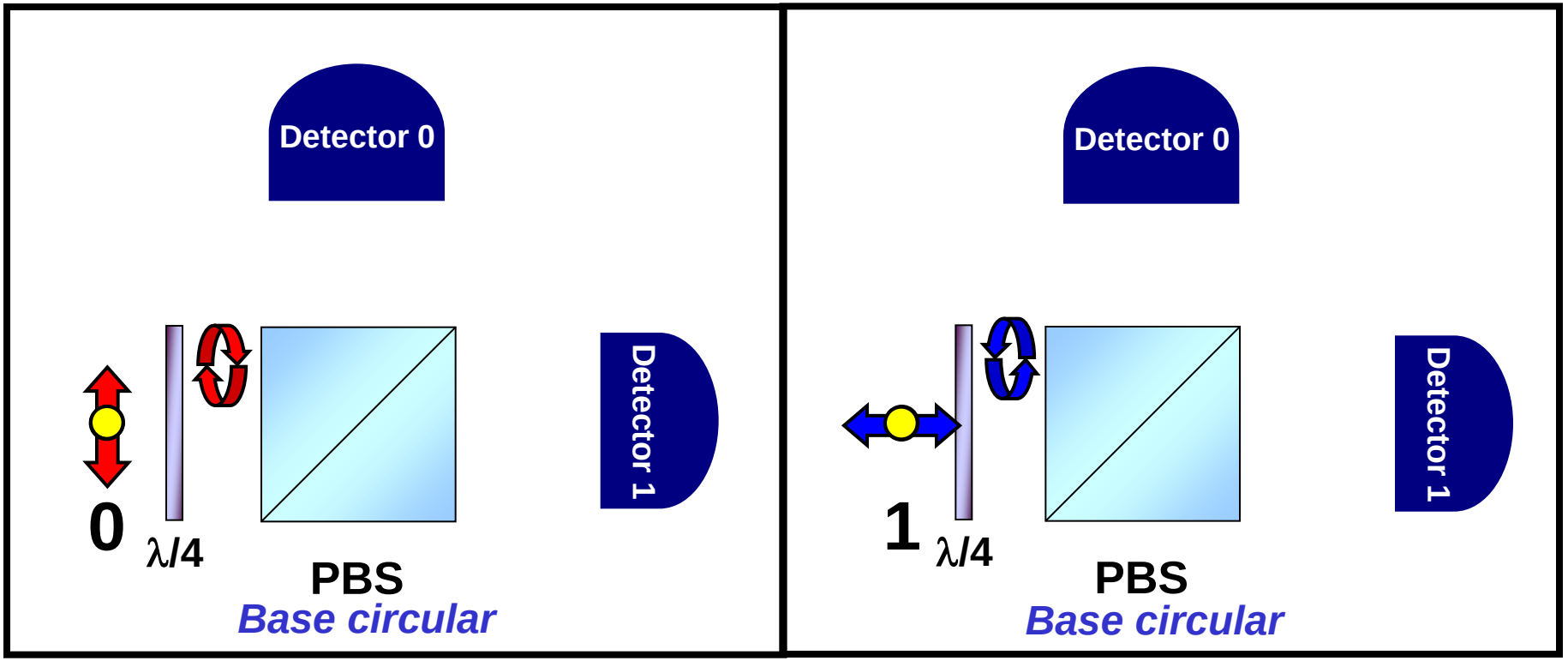


‘0’ con 100% de probabilidad



‘1’ con 100% de probabilidad

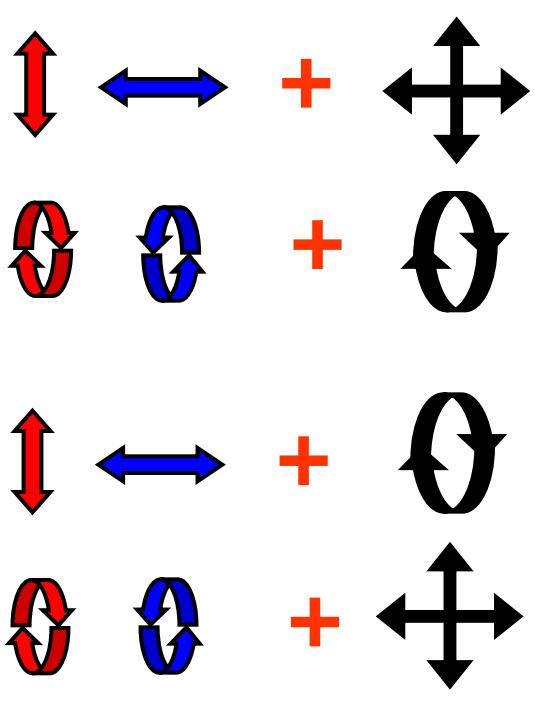
Protocolo BB84



‘**0**’ o ‘**1**’ con 50% de probabilidad

Protocolo BB84

- 4 tipos de medidas:
  - 2 deterministas:
  - 2 ambiguas:



Protocolo BB84

ALICE

Secuencia aleatoria: 0 1 1 0 1 0 0 1 1 0 0 0 1 0 1 1

Base

Polarización

BOB

Rectilinear

Circular

Por cada fotón recibido Bob mide aleatoriamente con la base rectilínea o circular

Protocolo BB84

ALICE

Secuencia aleatoria 0 1 1 0 1 0 0 1 1 0 0 0 1 0 1 1

Base

Polarización

BOB

Base

Protocolo BB84

ALICE

Secuencia aleatoria 0 1 1 0 1 0 0 1 1 0 0 0 1 0 1 1

Base

Polarización

BOB

Base

0 0 1 × 1 0 × 1 1 1 0 0 × 0 0 ×

Protocolo BB84

ALICE

Secuencia aleatoria 0 1 1 0 1 0 0 1 1 0 0 0 1 0 1 1

Base ✢ ✢ 0 0 0 ✢ 0 0 ✢ ✢ 0 ✢ ✢ ✢ 0 ✢

BOB

Base ✢ 0 ✢ ✢ 0 ✢ 0 0 ✢ 0 0 ✢ 0 ✢ ✢ 0

0 0 1 × 1 0 × 1 1 1 0 0 × 0 0 ×

Protocolo BB84

ALICE

Alice y Bob comparan las bases a través de un canal público

Secuencia aleatoria	0	1	1	0	1	0	0	1	1	0	0	0	1	0	1	1
Base	✣	✣	0	0	0	✣	0	0	✣	✣	0	✣	✣	✣	0	✣

BOB

Base	✣	0	✣	✣	0	✣	0	0	✣	0	0	✣	0	✣	✣	0
	0	0	1	×	1	0	×	1	1	1	0	0	×	0	0	×
	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗

Protocolo BB84

ALICE

Alice y Bob desechan los bits que en los que no han utilizado la misma base

Secuencia aleatoria	0	1	1	0	1	0	0	1	1	0	0	0	1	0	1	1
Base	✣	✣	0	0	0	✣	0	0	✣	✣	0	✣	✣	✣	0	✣

BOB

Base	✣	0	✣	✣	0	✣	0	0	✣	0	0	✣	0	✣	✣	0
	0	0	1	×	1	0	×	1	1	1	0	0	×	0	0	×
	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗

Protocolo BB84

ALICE

Alice y Bob desechan los bits en los que Bob no midió ningún fotón

Secuencia aleatoria 0 1 0 0 1 1 0 0 0

Base ✢ ✢ ✢ ✢ ✢ ✢ ✢ ✢ ✢

Base ✢ ✢ ✢ ✢ ✢ ✢ ✢ ✢ ✢

0 1 0 × 1 1 0 0 0

✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓

BOB

Protocolo BB84

ALICE

Dejando una secuencia común final

Secuencia aleatoria	0		1	0	1	1	0	0	0
Base	✣		✣	✣	✣	✣	✣	✣	✣
Base	✣		✣	✣	✣	✣	✣	✣	✣
	0		1	0	1	1	0	0	0
	✓		✓	✓	✓	✓	✓	✓	✓

BOB

Protocolo BB84

ALICE

BOB

Dejando una secuencia común final

0 1 0 1 1 0 0 0

0 1 0 1 1 0 0 0

0 1 0 1 1 0 0 0

Alice y Bob nunca revelan el valor del bit en su discusión

Detección de intrusos

Alice
(Emisor)

Eve

Bob
(Receptor)

¿Pueden Alice y Bob detectar la presencia de intrusos en el canal cuántico?

Sí

Un intruso introducirá un error detectable por Alice y Bob

Detección de intrusos

Alice
(Emisor)

Eve

Bob
(Receptor)

El ataque más simple

Un intruso introducirá un 25% de error

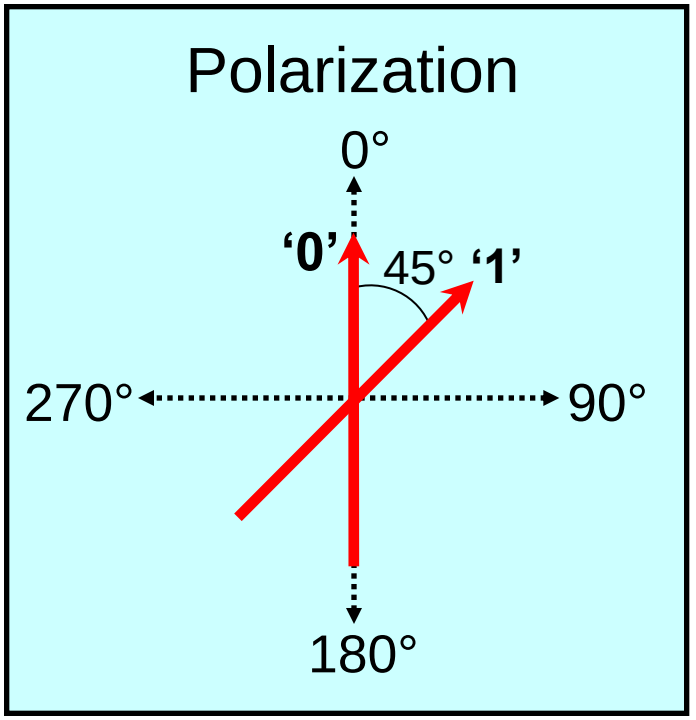
Error que introduce el intruso

Alice	Eve	Bob	
			✓ No
			
			✓ Sí, 1/2
			
			✓ No
			
			✓ Sí, 1/2
			

$$P_{error} = \frac{1/2+1/2}{4} = 1/4$$

Protocolo B92

- Dos estados no ortogonales
  (Bennett 1992)
- Codificados en polarización
- 0° polarización representa un “0” 45° polarización representa un “1”



El cifrado perfecto

Si la clave es **aleatoria**, **tan larga como el mensaje** y se utiliza solo **una vez**, Gilbert Vernam (1926)

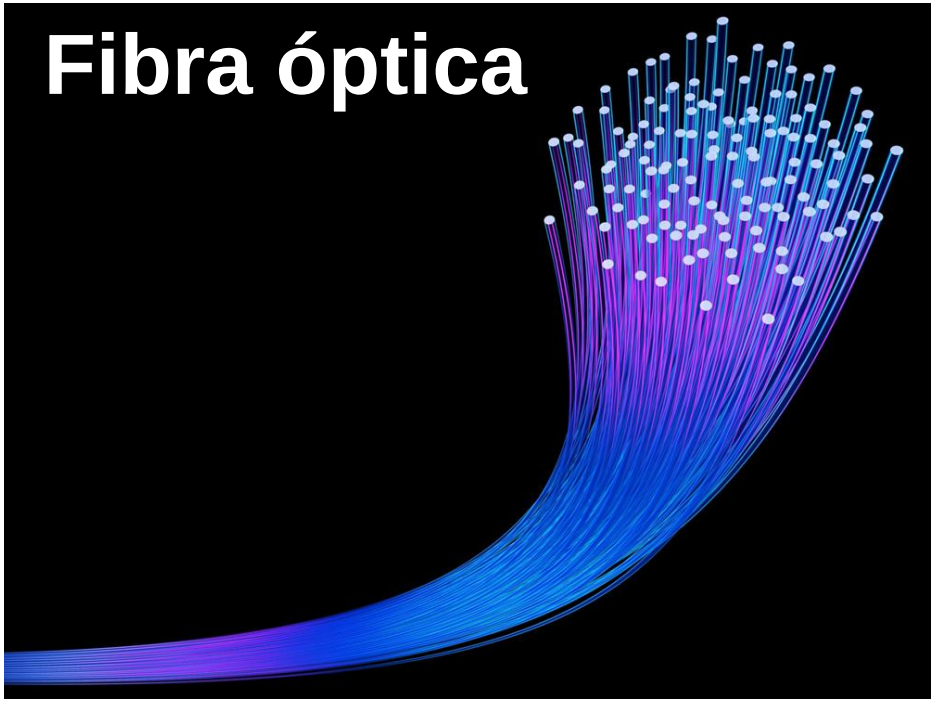
Cifrado absolutamente seguro

(Claude Shannon, 1948)

Cifrado con QKD

- Comunicaciones altamente seguras: QKD+Vernam
- Comunicaciones de menor exigencia en seguridad: QKD+AES

Canal: fibra óptica o espacio libre



Canal: espacio libre

VENTAJAS:

- **No dispersivo**
- **No birrefringente**
- **Ventanas de transmisión compatibles con tecnologías comerciales: Silicio o InGaAs**
- **Posibilidad de QKD global a través de satélite**

INCONVENIENTES:

- **Dependiente de condiciones meteorológicas**
- **Línea de visión directa necesaria**
- **Curvatura de la Tierra**

Fibra óptica

Ventajas:

- Distancia (record 250 km)
- Flexibilidad
- Independencia de condiciones externas
- Redes de comunicaciones
    - La fibra óptica es pervasiva

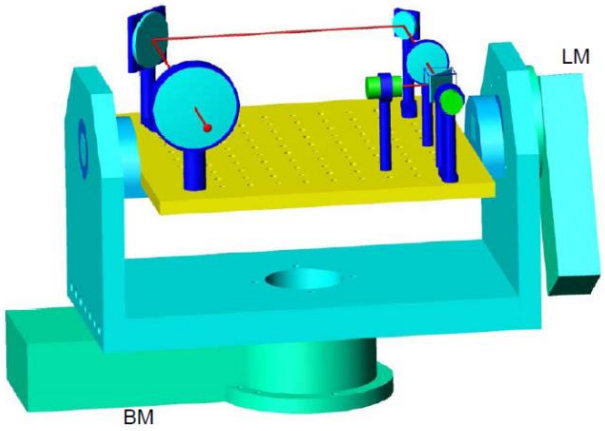
Problemas:

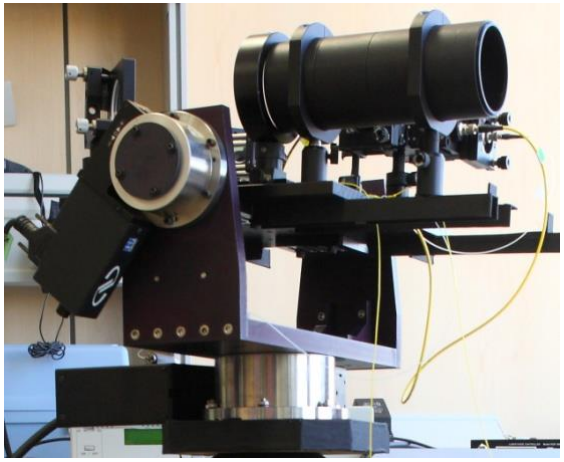
- Integración en redes de comunicaciones compartidas
    - Una red exclusiva es muy cara.
- Limitación en distancia: repetidores cuánticos o nodos confiables

Sistema de QKD desarrollado por el CSIC

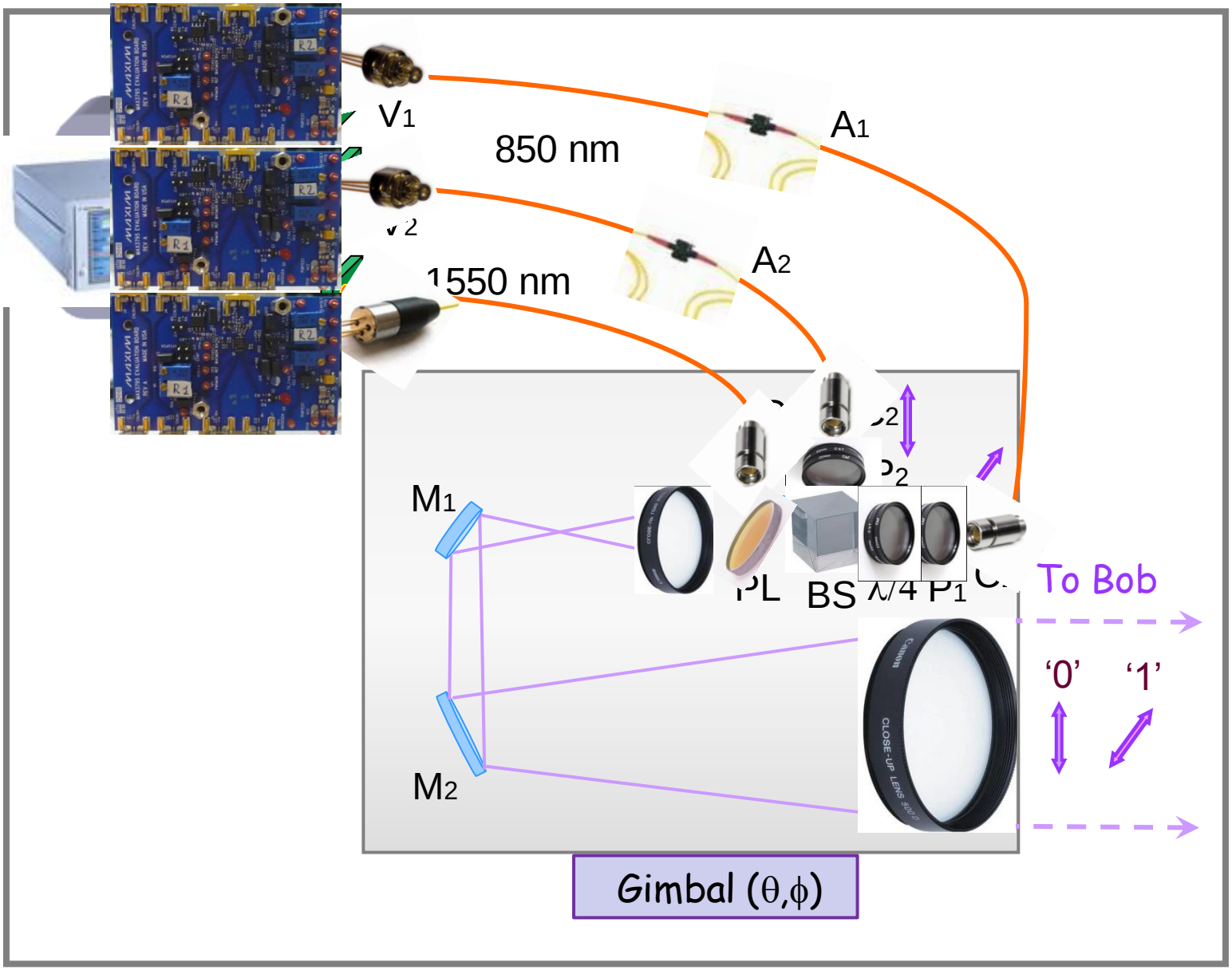
- Link urbano de QKD en espacio libre a alta velocidad
- Para integración futura en redes metropolitanas
- Enlaces punto a punto entre organismos militares gubernamentales o financieros que requieran mayor ancho de banda

Emisor: Alice

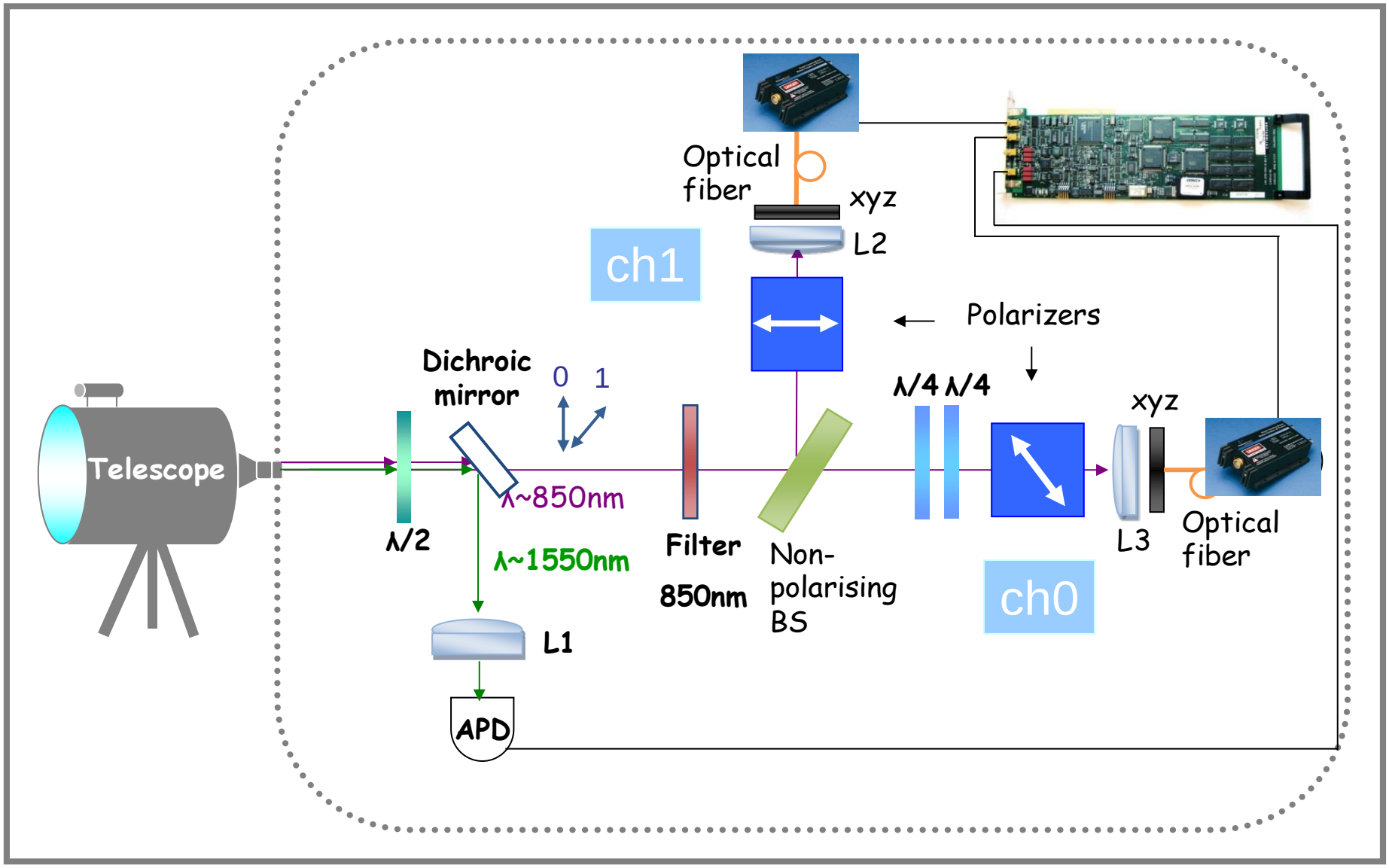




Alice



Bob


Optical fiber
xyz
L2
ch1
Polarizers
Dichroic mirror
0 1
λ/4 λ/4
xyz
Telescope
λ~850nm
λ/2
λ~1550nm
Filter
850nm
Non-polarising BS
L3
Optical fiber
ch0
L1
APD

Receptor: Bob

Enlace a 300m

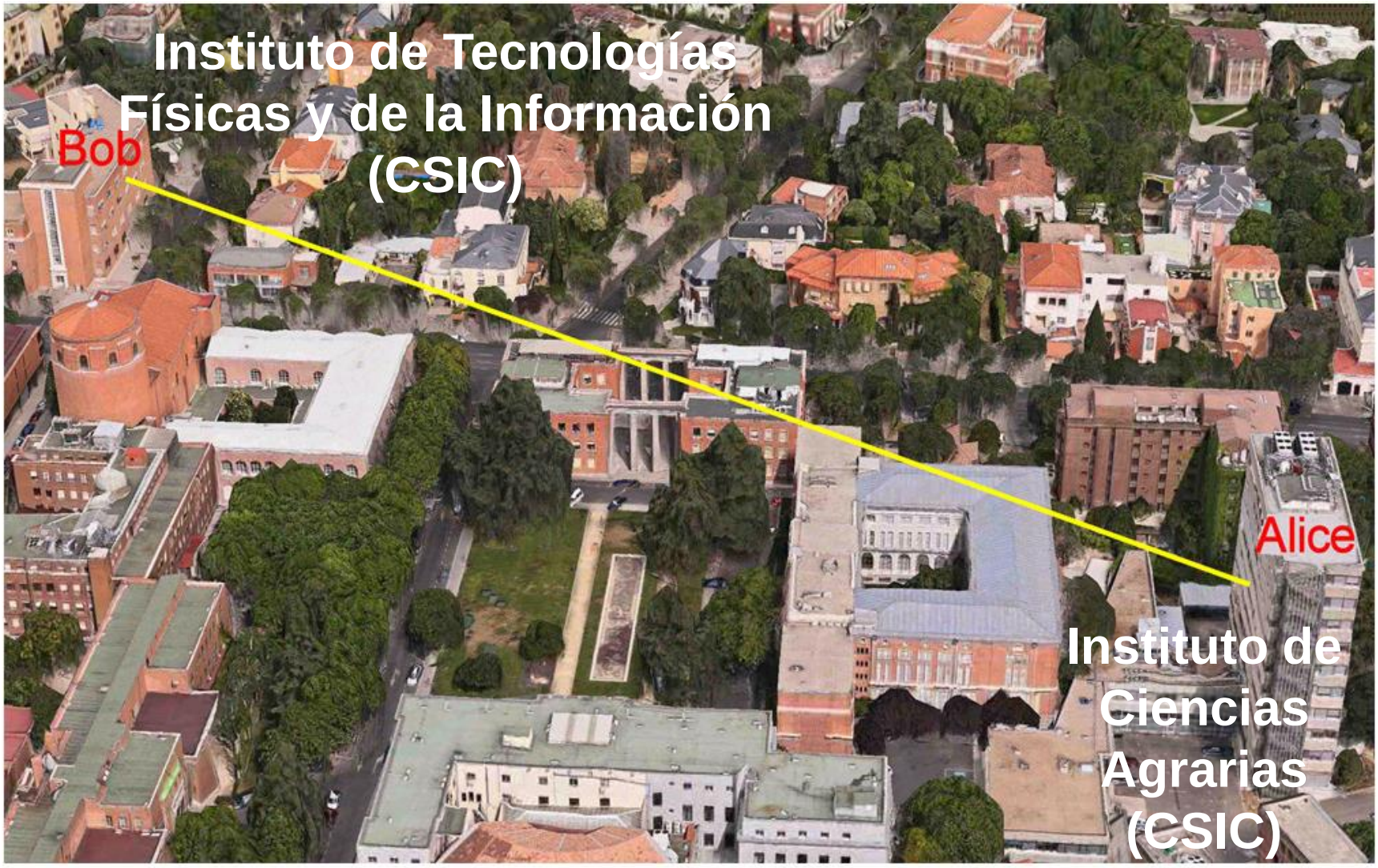
Instituto de Tecnologías Físicas y de la Información (ITEFI)

CSIC
Consejo Superior de Investigaciones Científicas

Instituto de Ciencias Agrarias

CSIC
Consejo Superior de Investigaciones Científicas

Enlace de 300 metros



Link de QKD en espacio libre 300m

- El sistema de QKD implementado transmite claves depuradas con una velocidad que es **4 veces mayor** que la máxima alcanzada anteriormente por sistemas similares
- Hemos conseguido que el sistema opere con tasas de **transmisión de clave secreta** máxima de **700 kbps de día y 1Mbps de noche**, **un orden de magnitud superior** que la reportada por sistemas similares
- Máxima distancia de operación el sistema de QKD:
  - **4,5 km** para un régimen de turbulencia intermedia
  - **3,4 km** para un régimen de turbulencia fuerte

Sistemas comerciales y records mundiales (fibra óptica)

Basados en fibra óptica (λ ~ 1550 nm)

En la actualidad, la criptografía cuántica está generando muchas expectativas, con varios fabricantes ofreciendo sus sistemas o prototipos en desarrollo:

- IdQuantique (Suiza)
- NEC (Japón)
- NTT (Japón)
- Toshiba (Reino Unido, Japón)
- SeQureNet (Francia, variables continuas)
- AIT (Austria, pares entrelazados)
- Quintessence (Australia, variables continuas)
- Qasky (China)

Además de muchos laboratorios de desarrollo.

Records:

- ✓ Distancia: 250 km de transmisión segura a muy bajo rate
- ✓ Clave secreta: 1 Mbps a 20 km

✓ Futuro: integración en redes

Sistemas comerciales y records mundiales (espacio libre)

- No existen aún prototipos comerciales
- Record mundiales:
  - Distancia: 144km
  - Velocidad: difícil porque la velocidad no es facilmente escalable con distancia
  - Sifted bit rate a 300m:
    - NIST: 313 kbit/s
    - CSIC: 1,8 Mbit/s (~4 veces mayor)
  - Secret key rate a 300m:
    - NIST: No reportan nada
    - CSIC:1 Mbit/s calculada suponiendo dos ataques simultáneos (PNS y USD)

Retos

- Retos de la QKD:
  - Mejorar la velocidad y la distancia:
    - Desarrollar repetidores cuánticos
    - Comunicación vía satélite
    - Mejorar los detectores y los protocolos

Conclusiones

- Amenaza demostrada del ordenador cuántico a la criptografía de clave pública (RSA)
- Solución: Distribución cuántica de clave
  - Seguridad basada en las leyes de la Mecánica Cuántica
  - Único sistema que detecta intrusos
  - Resuelve distribución segura de claves
- Protocolo BB84
- Sistema de QKD experimental del ITEFI (sistema en espacio libre, record en velocidad)

Preguntas