Fundamentos de Criptografía Cuántica

Jesús García López de Lacalle

Grupo de Investigación en Información
y Computación Cuántica (GIICC)

Escuela Técnica Superior de Ingeniería
de Sistemas Informáticos

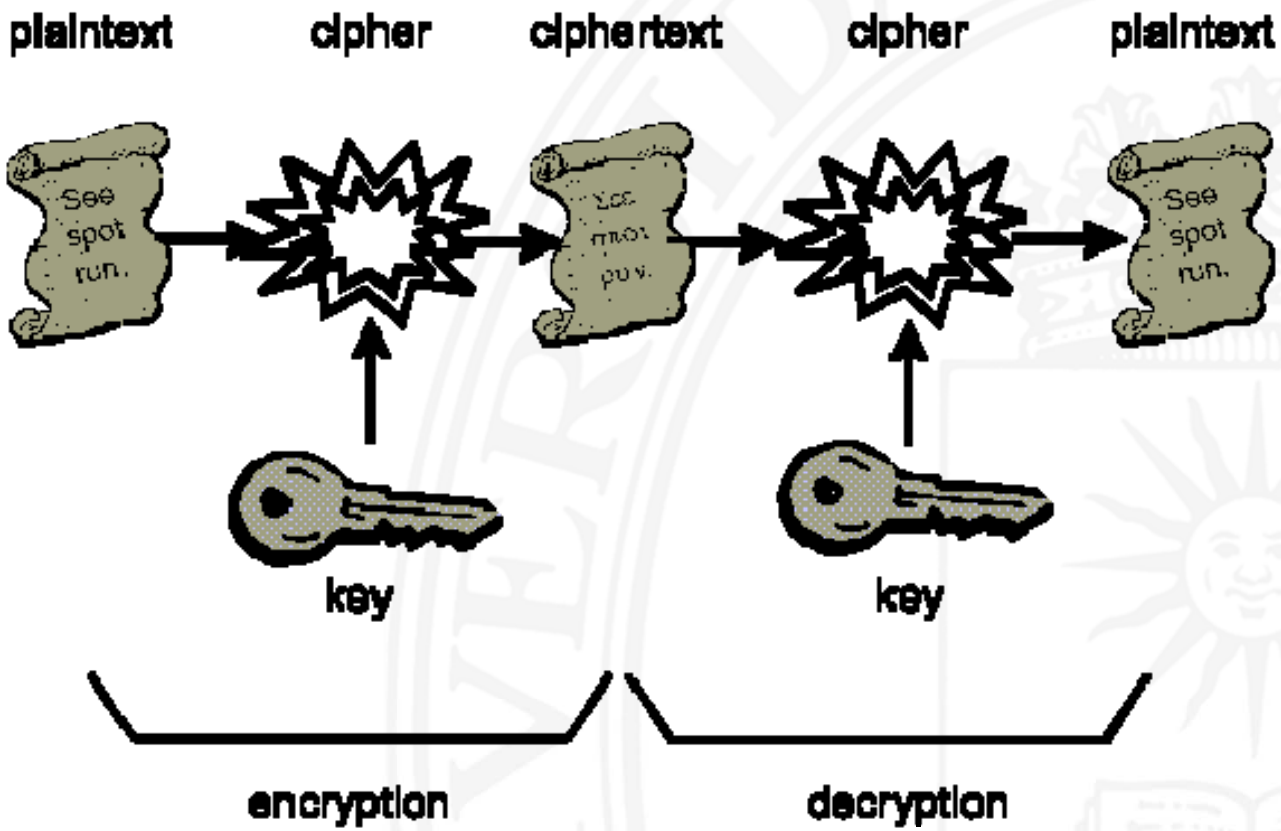
Universidad Politécnica de Madrid

jglopez@etsisi.upm.es

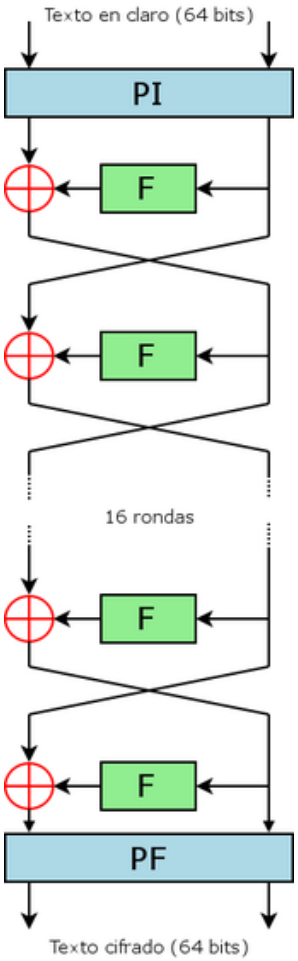
Fundamentos de Criptografía Cuántica

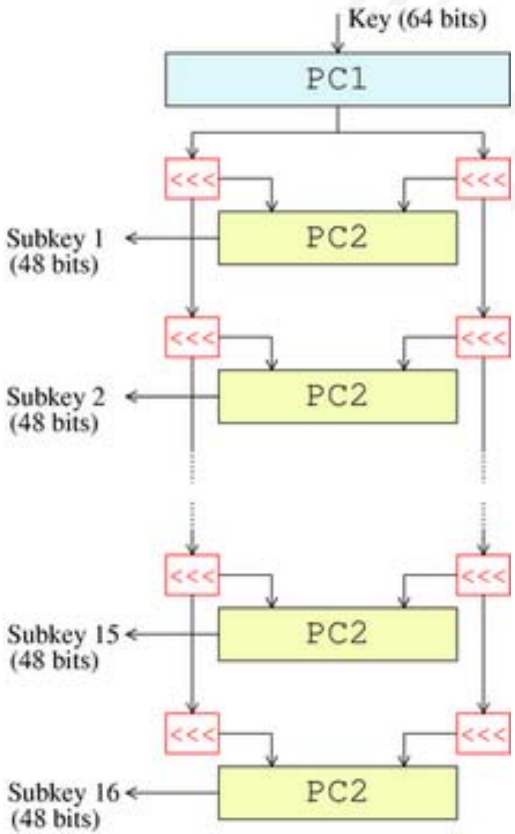
- Criptografía de clave privada
- Criptografía de clave pública
- La Criptografía en la actualidad
- Fundamentos de la Criptografía Cuántica
- Protocolo BB84
- Seguridad del protocolo BB84
- Limitaciones tecnológicas actuales
- Protocolo SARG04
- Criptografía Cuántica comercial

Criptografía de clave privada

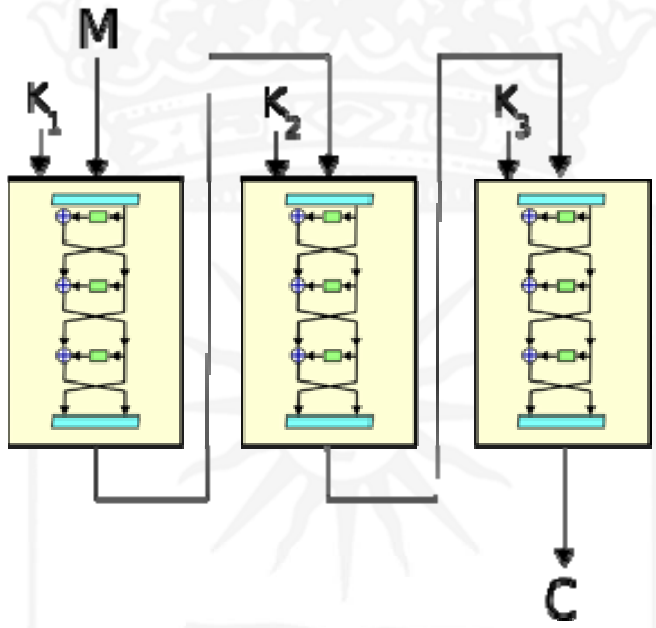


Criptografía de clave privada (TDES)

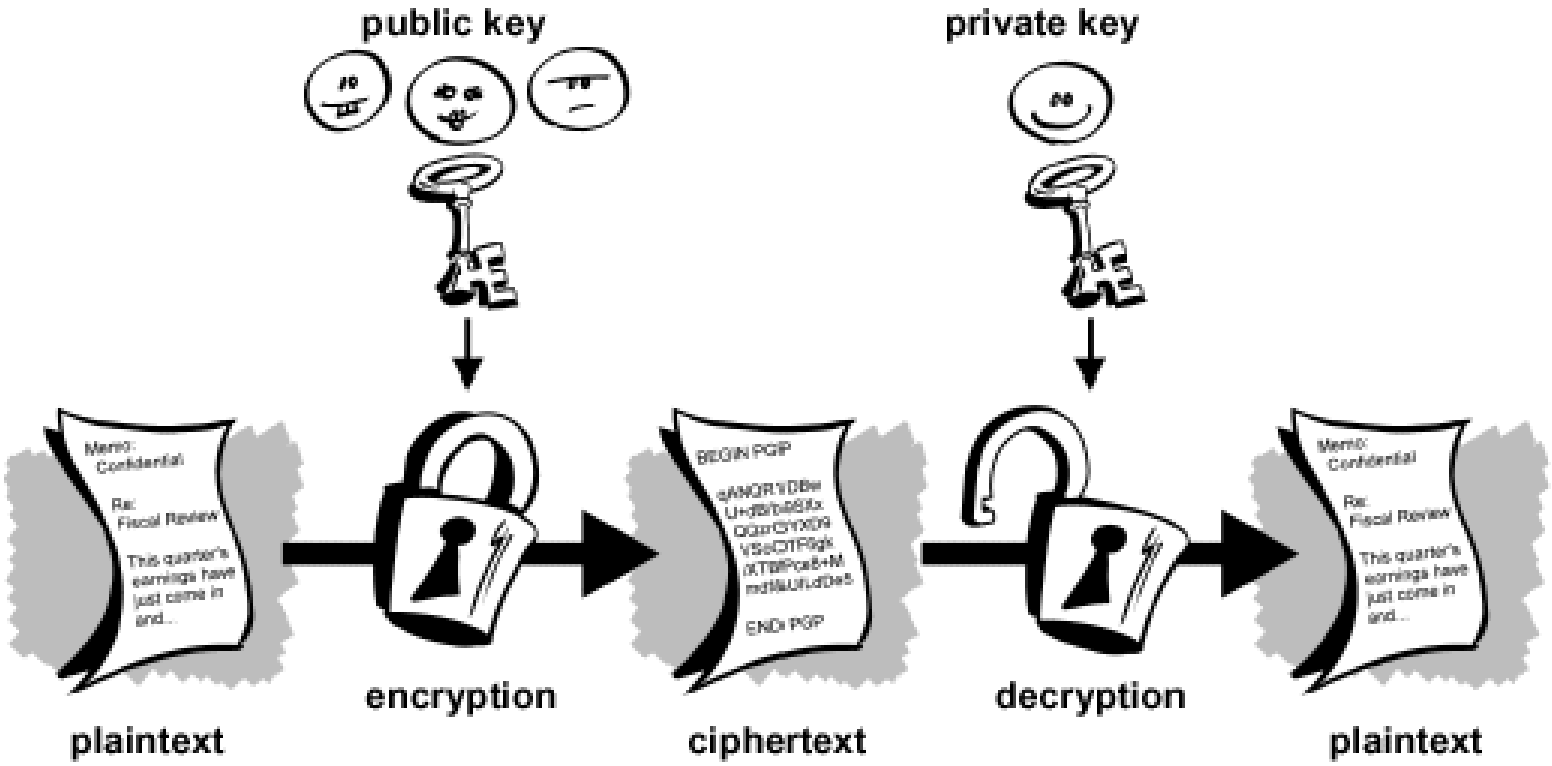




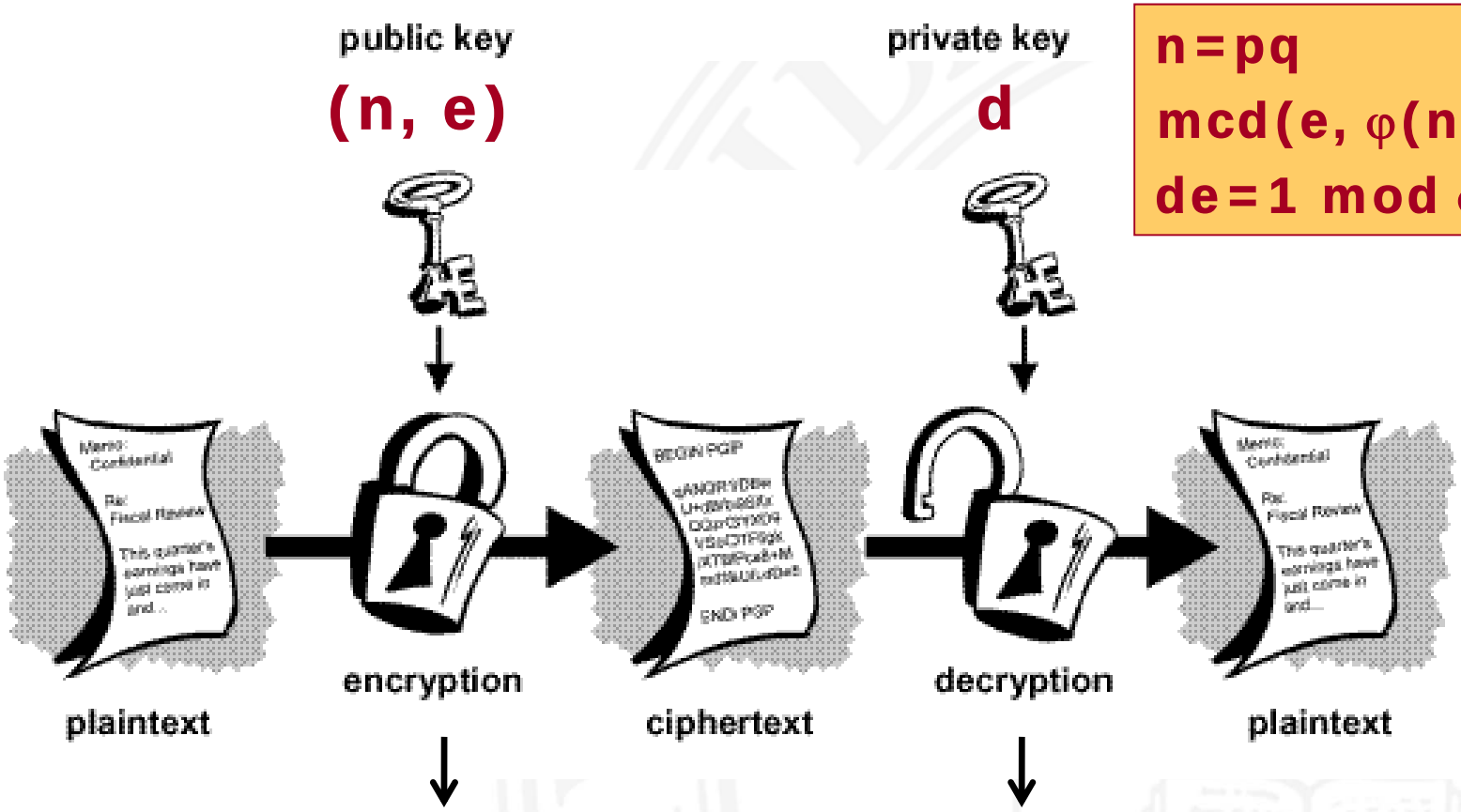
Clave (192 bits)



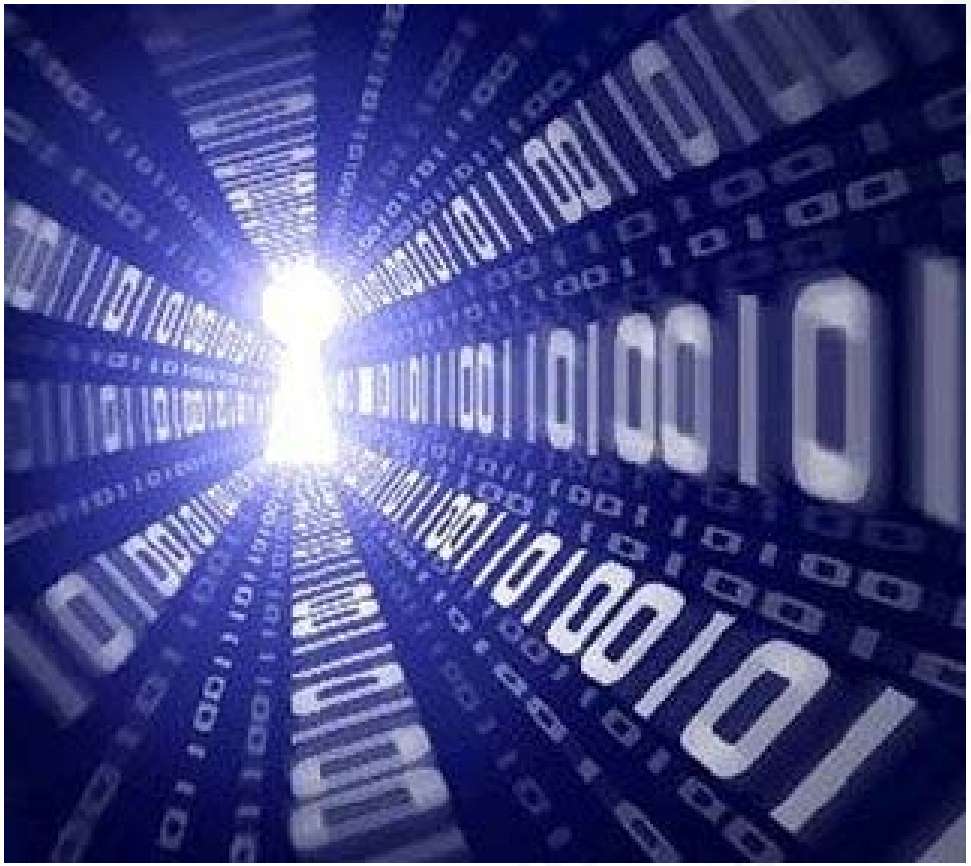
Criptografía de clave pública



Criptografía de clave pública (RSA)



La Criptografía en la actualidad



Es imprescindible

Clave privada:

- Rápida
- Generalizada

Clave pública:

- Lenta
- Distrib. claves
- Autenticación

Fundamentos de la Criptografía Cuántica

- Objetivo: distribución de claves privadas (QKD)
- Principio básico de seguridad: codificar los bits de la clave privada en qubits no ortogonales elegidos aleatoriamente
- Efectos de esta codificación:
  - ✓ El espía (Eva) no puede distinguir los qubits
  - ✓ Si Eva intenta obtener información introducirá errores detectables en la transmisión
  - ✓ El destinatario (Benito) tampoco puede distinguir los qubits y decidirá aleatoriamente cómo leerlos

Fundamentos de la Criptografía Cuántica

- Corrección de los errores de Benito:
  - ✓ Benito está en la misma situación que Eva
  - ✓ Para no dar ninguna información a Eva realizan un proceso de "reconciliación de los esquemas de codificación", una vez finalizada la transmisión de qubits
  - ✓ Desechan las posiciones de la clave privada en las que la lectura de Benito no ha sido compatible con la codificación de Alicia

Protocolo BB84

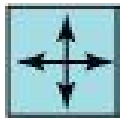
1. **Alicia genera una clave aleatoria**

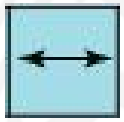
1001100

2. **Alicia codifica cada bit en un qubit y se lo envía a Benito**

Protocolo BB84

3. Utiliza dos alfabetos para codificar la clave

A1  **:**

 **= 0** $|0\rangle$

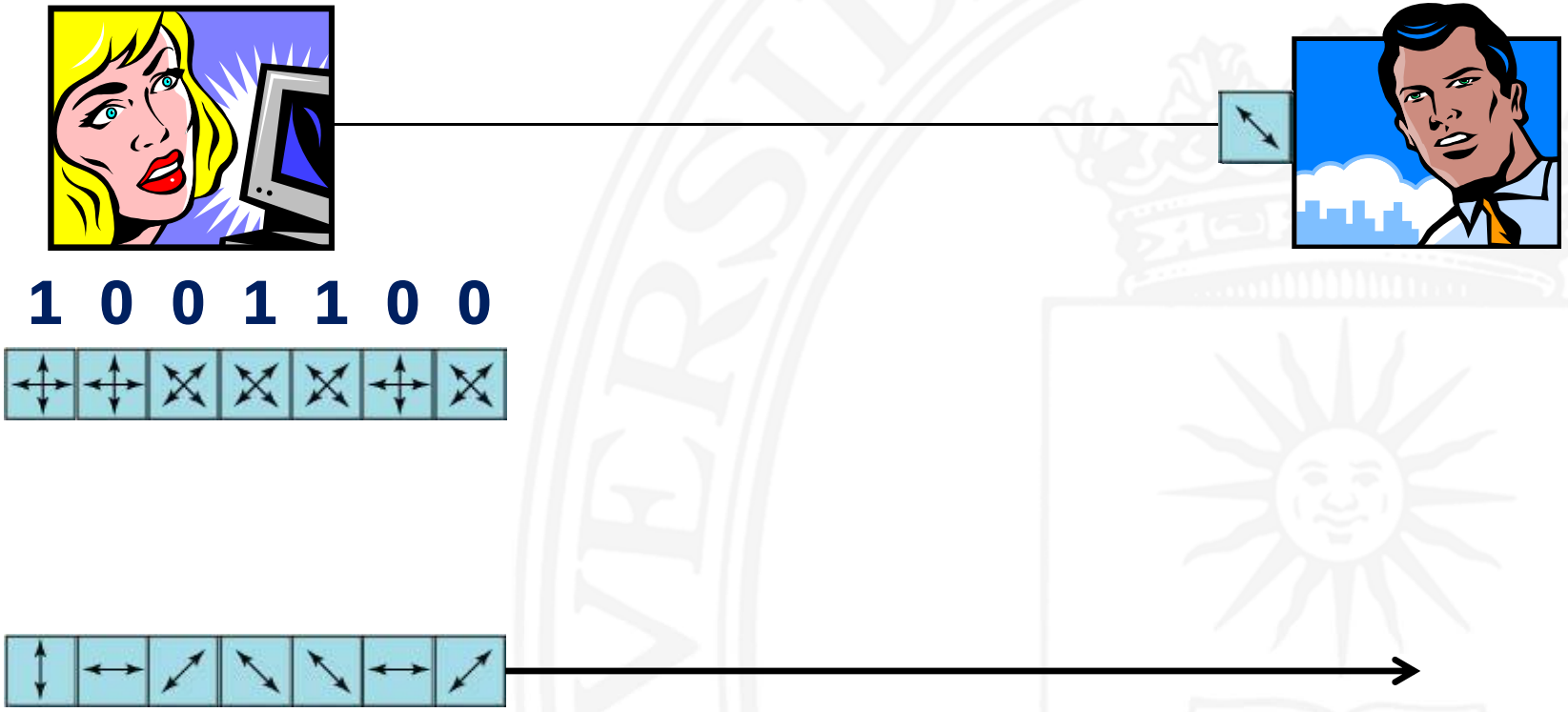
 **= 1** $|1\rangle$

A2  **:**

 **= 0** $|0\rangle + |1\rangle$

 **= 1** $|0\rangle - |1\rangle$

Protocolo BB84



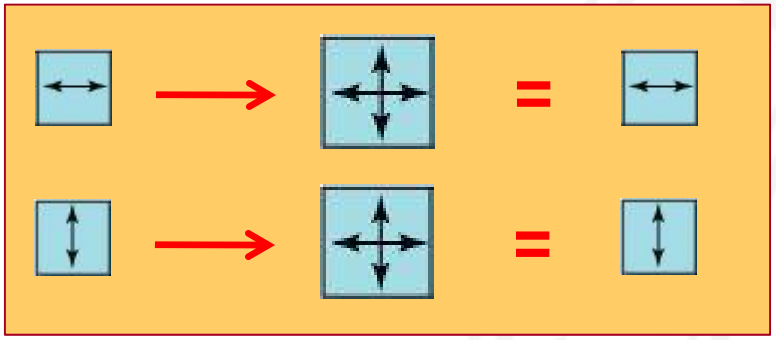
Protocolo BB84

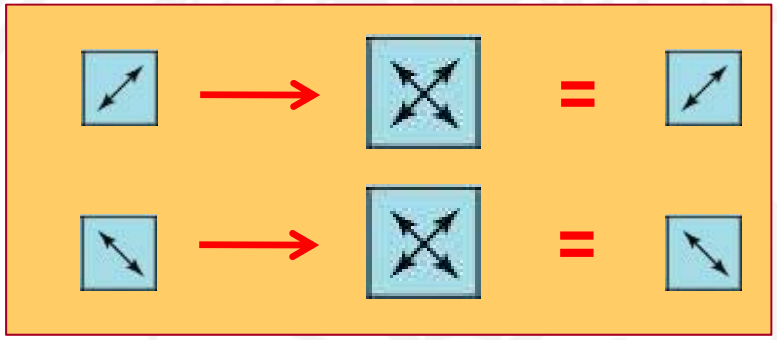
4. Benito elige aleatoriamente el alfabeto para medir

Protocolo BB84

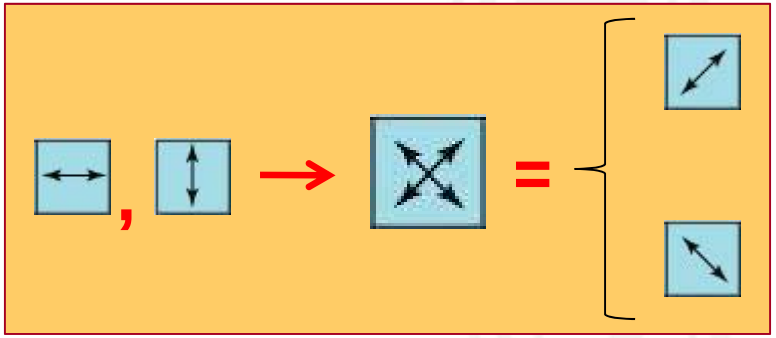
Resultados de Benito

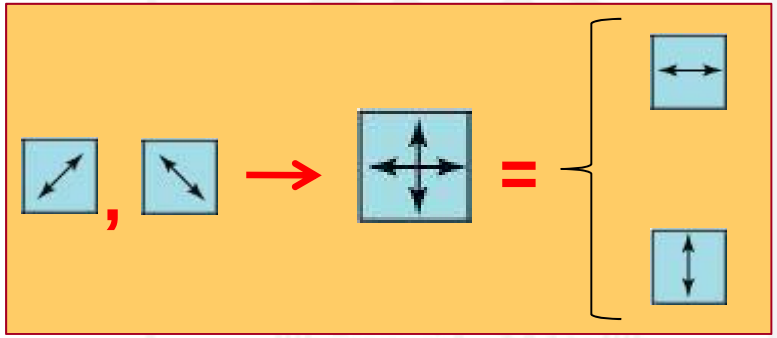
Si coinciden los alfabetos de Alicia y Benito:





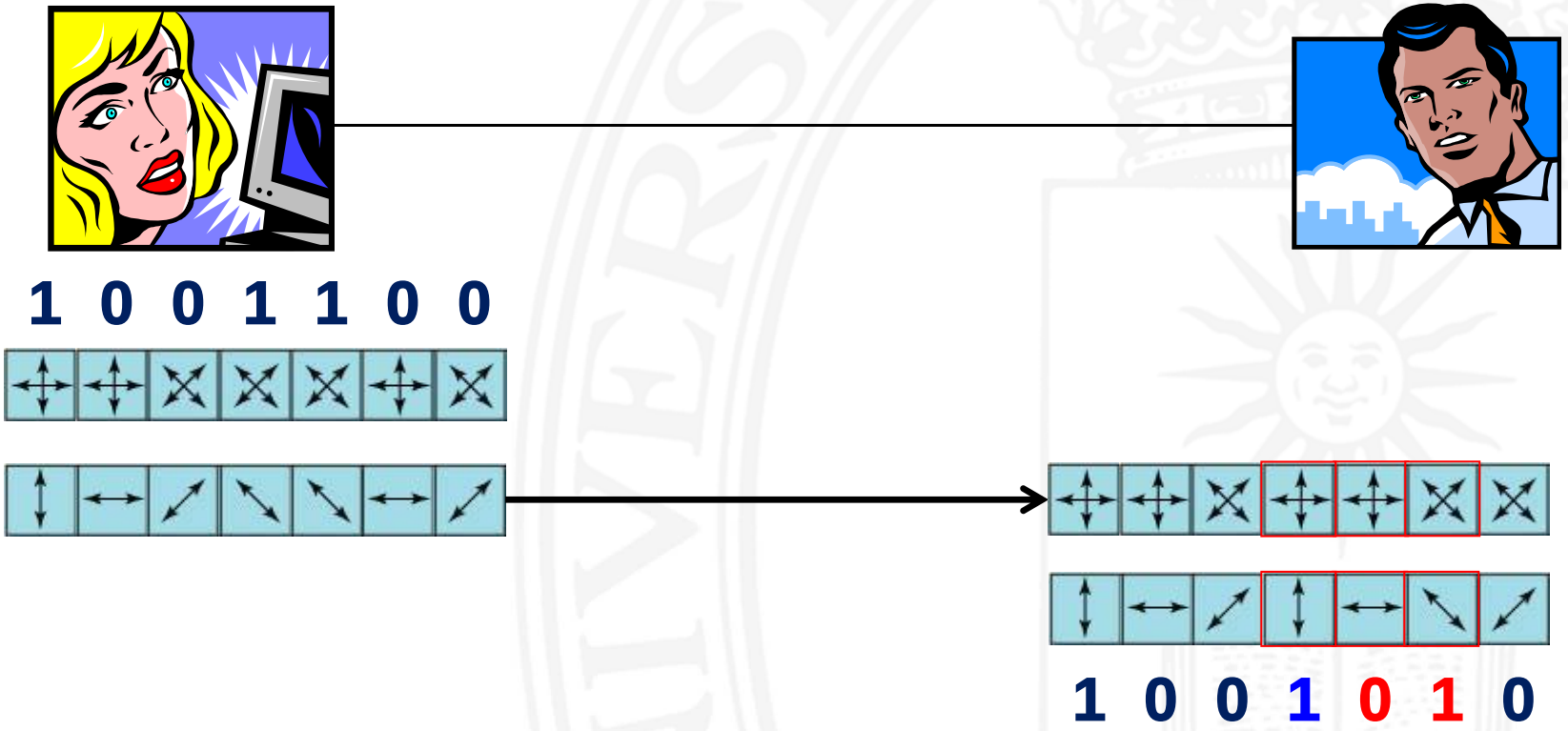
Si no coinciden los alfabetos de Alicia y Benito:





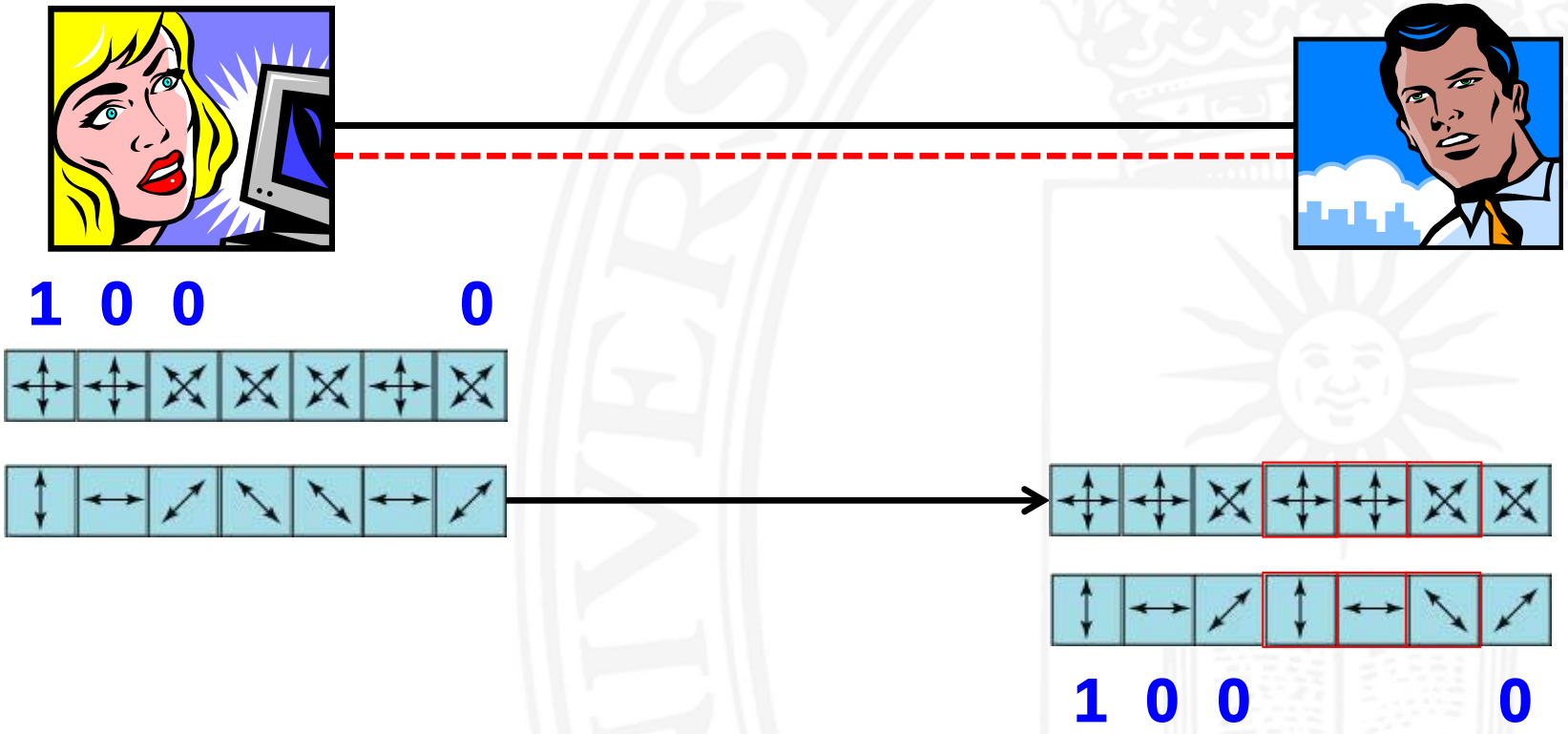
Protocolo BB84

4. Benito elige aleatoriamente el alfabeto para medir

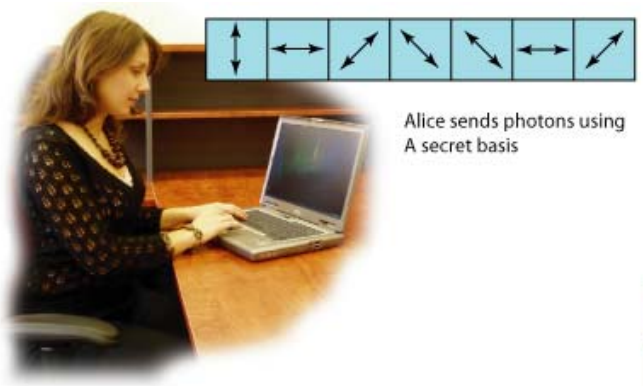


Protocolo BB84

5. Alice y Bob desechan las posiciones en las que no han coincidido los alfabetos

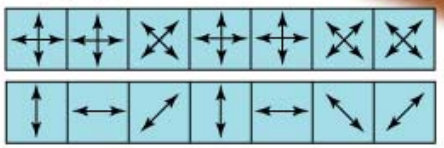


Protocolo BB84

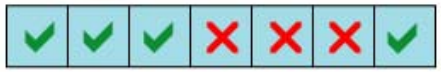


Alice sends photons using
A secret basis

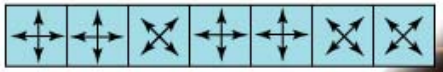
Bob uses a random detector orientation to measure the photons. He only gets some correct.

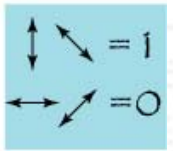


Alice indicates to Bob what measurements will be correct. These become the new key.



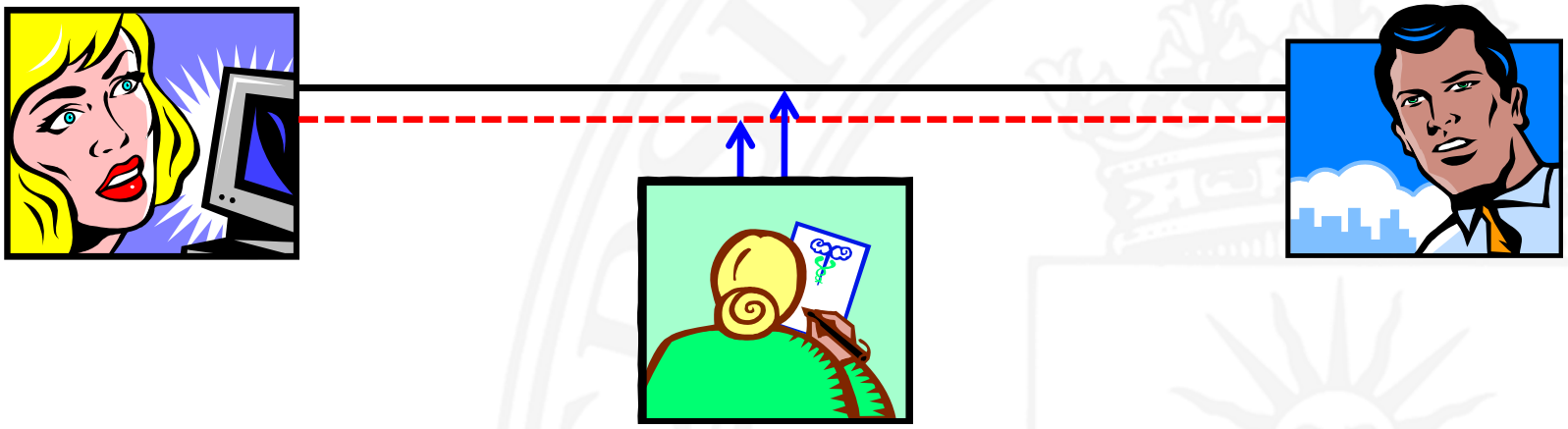
Bob phones Alice and tells her over a public channel what basis he used.





Seguridad del protocolo BB84

Si Eva hace lo mismo que Benito:



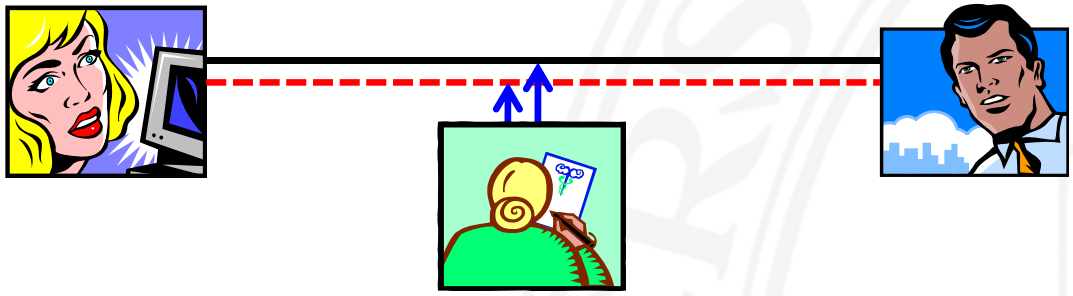
Información de Eva: 75%

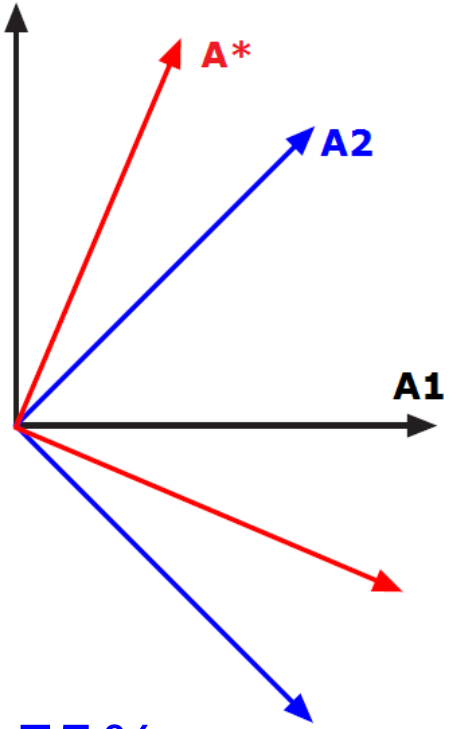
Información de Benito: 75%

Alicia y Benito pueden detectar a Eva

Seguridad del protocolo BB84

Si Eva hace mide en la base "intermedia" A*:





Inf. de Eva: $\cos^2(\pi/8) = 85.4\%$

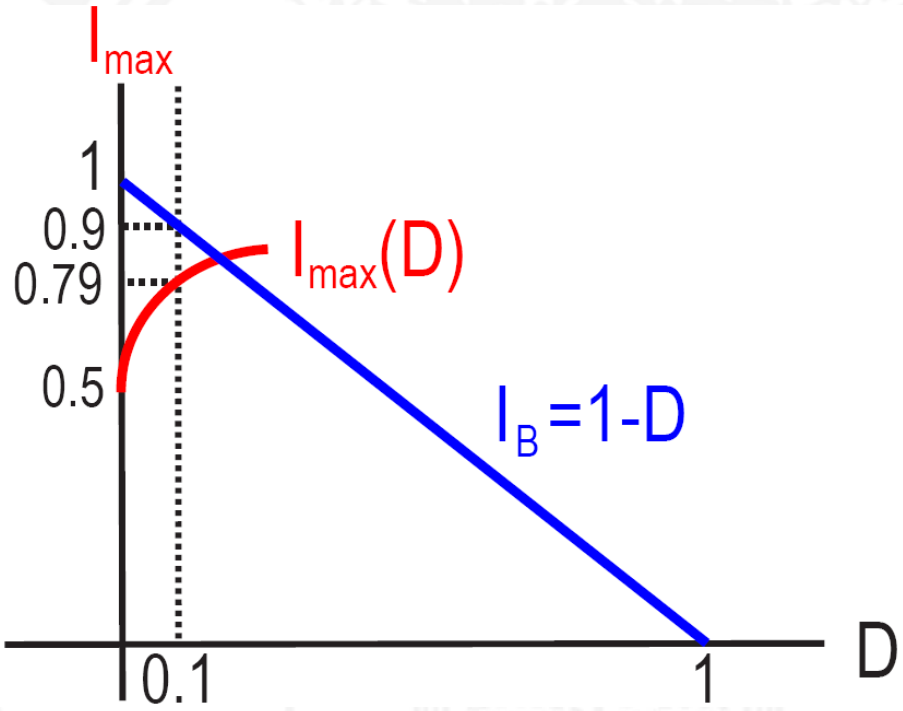
Inf. de Benito: $\cos^4(\pi/8) + \sin^4(\pi/8) = 75\%$

Alicia y Benito pueden detectar a Eva

Seguridad del protocolo BB84

Alicia y Benito siempre detectan a Eva

$$I_{max}(d) = \frac{1}{2} + \sqrt{d(1-d)}$$



Limitaciones tecnológicas actuales

- Distancia (hasta 30 km):

  La fibra óptica absorbe los fotones

- Eficiencia de los detectores (~10%)
- Velocidad de transmisión (~5 MHz):

  Tiempo de relajación de los detectores (~200 ns)

- Fuentes de fotones únicos:

  Número medio de fotones por pulso (~0.3)

  Número de pulsos sin fotón (~90%)

Protocolo SARG04

- Alicia codifica el **0** en $|\mathbf{0}\rangle$ ó $|\mathbf{1}\rangle$
- Alicia codifica el **1** en $|\mathbf{+}\rangle$ ó $|-\rangle$
- Benito mide en la base $\mathbf{B_1}$ ó $\mathbf{B_x}$
- Reconciliación: Alicia publica en cuál de los siguientes conjuntos está cada uno de los qubits transmitidos

  $\{|0\rangle, |+\rangle\}$, $\{|0\rangle, |-\rangle\}$, $\{|1\rangle, |+\rangle\}$ ó $\{|1\rangle, |-\rangle\}$

Protocolo SARG04

- Benito considera que su medida es consistente si en la medida obtiene un estado ortogonal a uno de los del conjunto indicado por Alicia:

B_x	$\|+\rangle$	$\|0\rangle$
$\{\|0\rangle, \|-\rangle\}$	$\|-\rangle$	?

- Se desecha el 75% de los qubits

Protocolo SARG04

- Si Eva hace un ataque PNS:
  - ✓ Tiene un estado que pertenece al conjunto indicado por Alicia

$$q \in \{|0\rangle, |-\rangle\}$$

  - ✓ Mide igual que Benito pero siempre se queda con un estado

B_x	$\|+\rangle$	$\|0\rangle$
$\{\|0\rangle, \|-\rangle\}$	$\|-\rangle$	$\|-\rangle$

Protocolo SARG04

- Benito obtiene el 75% de los bits codificados con dos fotones

$$I_{max}(d) = \frac{3}{4} p + \left[\frac{1}{2} + \sqrt{d(1-d)} \right] (1-p)$$

SARG04 es seguro con pulsos de 1 ó 2 fotones

Criptografía Cuántica comercial

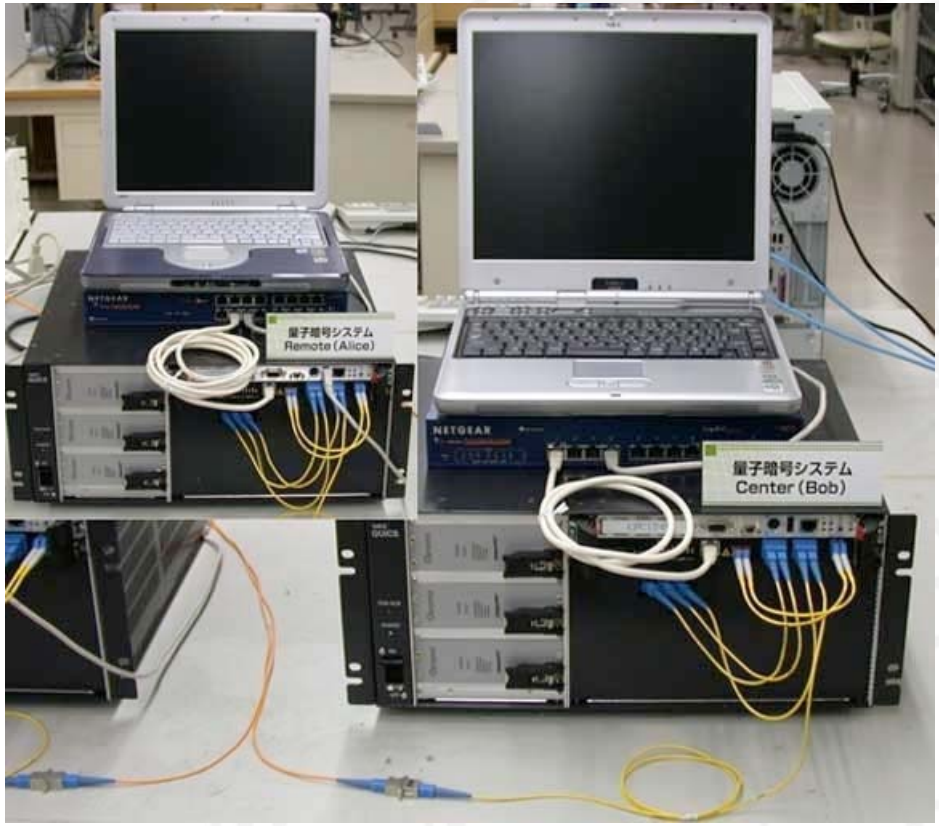
id Quantique

Criptografía Cuántica comercial

From Computer Desktop Encyclopedia
© 2005 MagiQ Technologies

MagiQTech

Criptografía Cuántica comercial



NEC

Criptografía Cuántica comercial

Toshiba