educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 4

educación IT
CODE YOUR FUTURE

Criptografía cuántica

Fundamentos

La **criptografía cuántica** es la ciencia que utiliza propiedades de la mecánica cuántica para implementar **tareas criptográficas**. Comprende las siguientes áreas:

- **Distribución de claves cuánticas** (QKD) y **cifrado cuántico** en canales de comunicación de fibras ópticas y espacios abiertos
- ***Hash*** cuántico y **firma digital** cuántica.
- **Codificación en sistemas de transmisión** de **información cuántica.**
- **Codificación súper densa cuántica de información** utilizando partículas entrelazadas e hiper entrelazadas (un qubit puede transportar dos bits ordinarios) que incrementa el ancho de banda del canal de comunicación cuántico.

Para la **computación cuántica**, la criptografía se divide en:

Cuánticamente segura

Los algoritmos simétricos son cuánticamente seguros si al menos se duplica la longitud de sus claves.

Cuánticamente insegura

La criptografía asimétrica se considera cuánticamente insegura.

Criptoanálisis

En Criptoanálisis, **los algoritmos cuánticos brindan aceleración exponencial o cuadrática en la resolución de problemas**.

- El **algoritmo de Shor** es un ejemplo de aceleración exponencial.
- El **algoritmo de Grover** es un ejemplo de aceleración cuadrática.

Según la **NIST**, los algoritmos AES, SHA-2, SHA-3, RSA, ECDSA, ECDH y DSA están bajo amenaza cuántica. Se estima un 15% de probabilidad que los algoritmos de clave pública sean rotos en 2025 y 50% que lo sean en 2030.

En 2001, **IBM** implementó el algoritmo de Shor y factorizó 15 como 3 × 5 usando una computadora cuántica con 7 qubits. En 2012 se logró factorizar 21. En 2019 se realizó un intento para factorizar 35 en una IBM Q System One, pero el algoritmo falló por acumulación de errores.

Existen muchos grupos que pretenden haber logrado factorizaciones de números mucho más grandes, pero la implementación usa computación híbrida (clásica y cuántica).

Numerical field sieve method (best known classic algorythm)

$$L_{clas} \approx exp\left(\left(\frac{64}{9}\right)^{\frac{1}{3}} n^{\frac{1}{3}} (ln(n))^{\frac{2}{3}}\right)$$

$$L_{quant} \approx n^2\, ln(n)\, ln\,(ln(n))$$

n -number of binary digits

k - number of decimal places

n= k ln (10)

Shor algorithm (1994)

Classic exascale computer (10^{18} op/sec) vs. megahertz quantum computer (1 million op/sec).			
k – number of decimal digits	$k = 250$	$k = 500$	$k = 1000$
Labor intensity of classic algorithm	200 hours	5 million years	4×10^{17} years
Labor intensity of quantum algorithm	4 seconds	18 seconds	84 seconds

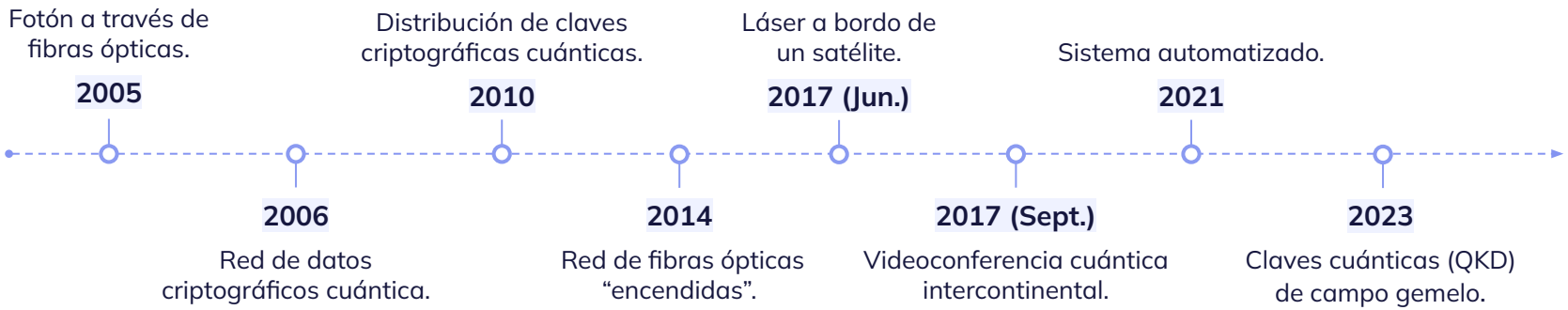
Estimación del tiempo necesario para factorizar un número con computación clásica vs. cuántica.

Cryptoscheme	Key size, bit	Effective durability, bit	Required number of logical qubits	Required number of physical qubits	Time estimation
AES	128	128	2953	4.61×10^6	2.61×10^{12} years
	192	192	4449	1.68×10^7	1.97×10^{22} years
	256	256	6681	3.36×10^7	2.29×10^{32} years
RSA	1024	80	2290	2.56×10^6	3.58 hours
	2048	112	4338	6.2×10^6	28.63 hours
	4096	128	8434	1.47×10^7	229 hours
ECDLP	256	128	2330	3.21×10^6	10.5 hours
(NIST P-256	386	192	3484	5.01×10^6	37.67 hours
NIST P-386	512	256	4719	7.81×10^6	95 hours
NIST P-521)					
SHA256	N/A	72	2403	2.23×10^6	1.8×10^4 years

Potenciales vulnerabilidades de algunas *blockchains.*

Desarrollo de claves cuánticas (QKD)

Hitos



Hitos

- **2005** (junio): investigadores japoneses transmiten un **fotón a través de fibras ópticas.**
- **2006** (agosto): la Universidad Northwestern y BBN Technologies de Cambridge, Massachusetts, realizan la primera demostración de una **red de datos criptográficos cuántica**.
- **2010** (septiembre): investigadores japoneses lograron **distribuir claves criptográficas cuánticas** a una distancia de 50 km utilizando la transmisión de un emisor de un solo fotón.
- **2014** (abril): se distribuyen claves cuánticas sobre una **red de fibras ópticas "encendidas"**.
- **2017** (junio): investigadores demuestran mediciones terrestres de estados cuánticos enviadas por un **láser a bordo de un satélite** a 38.000 kilómetros sobre la Tierra.
- **2017** (septiembre): primera **videoconferencia cuántica intercontinental** entre Beijing y Viena.

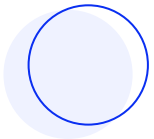
- **2021** (Julio): investigadores demuestran un **sistema automatizado** y fácil de operar de distribución de claves cuánticas (QKD) utilizando la red de fibra en la ciudad de Padua, Italia.
- **2023** (Mayo): distribución de claves cuánticas (QKD) de campo gemelo a través de una **fibra de 1002 km en China**.

Distribución de claves cuánticas (QKD)

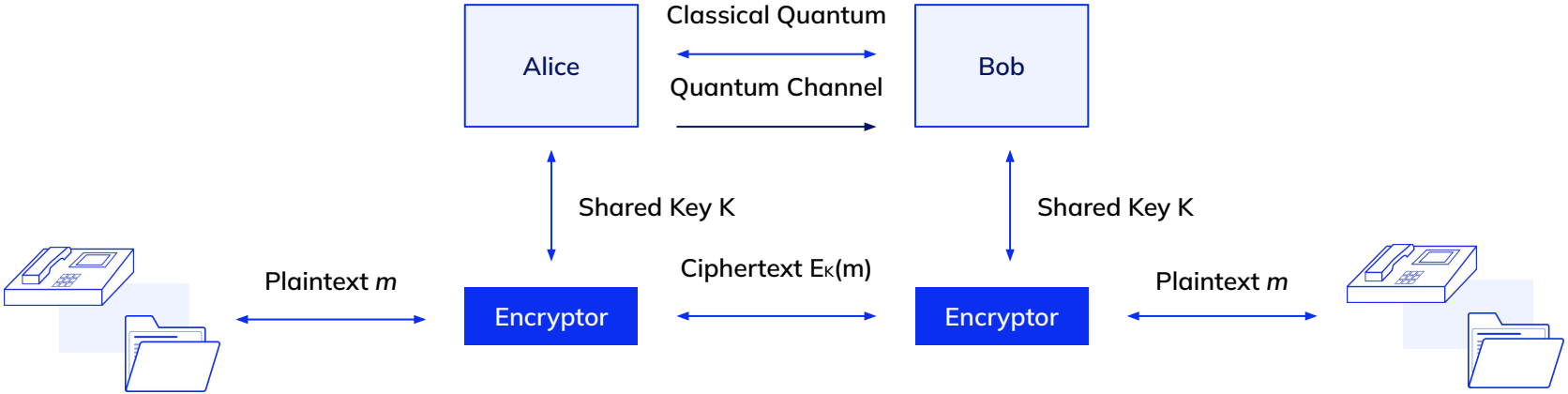
La computación cuántica amenaza el cifrado típico basado en las matemáticas. La QKD funciona mediante el uso de **fotones**, las partículas que transmiten la luz, para transferir datos.

QKD permite a dos usuarios distantes, que inicialmente no comparten una clave secreta larga, producir una cadena común y aleatoria de bits secretos, llamada **clave secreta**, a través de un canal cuántico. El canal clásico se utiliza para acordar la validez de la clave cuántica producida.

El **cifrado es "irrompible"** y eso se debe principalmente a la forma en que los datos se transportan a través del fotón. Un fotón no puede ser copiado y cualquier intento de medirlo lo perturbará. Esto significa que una persona que intente interceptar los datos dejará un rastro.



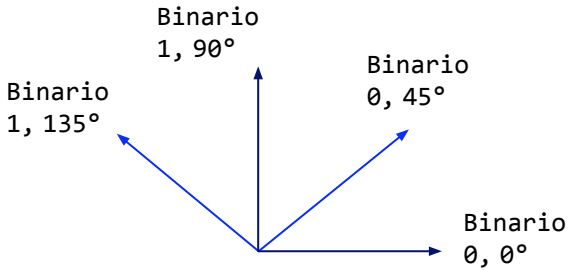
Sistema QKD


Alice
Classical Quantum
Quantum Channel
Bob
Shared Key K
Shared Key K
Plaintext m
Ciphertext EK(m)
Plaintext m
Encryptor
Encryptor

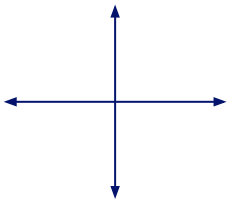
El protocolo BB84: ejemplo

1. Alice enviará una secuencia de fotones a Bob usando un canal cuántico inseguro. Alice y Bob usan cuatro **polarizaciones**: vertical, horizontal, 45 grados, 135 grados.

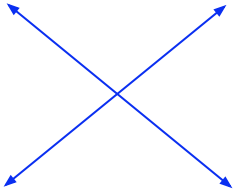
2. Alice crea un bit aleatorio (0 o 1) y entonces selecciona en forma aleatoria una de los dos bases (rectilínea o diagonal) para transmitirlo.



Polarizaciones

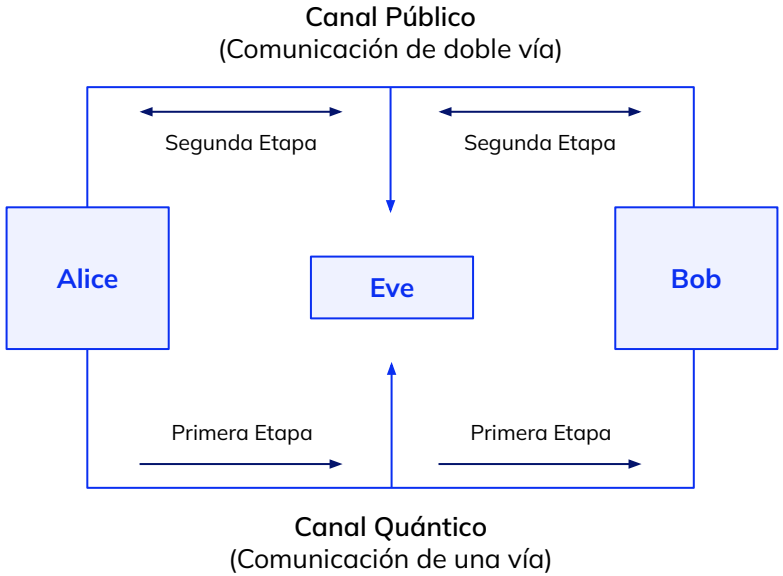


Base rectilínea



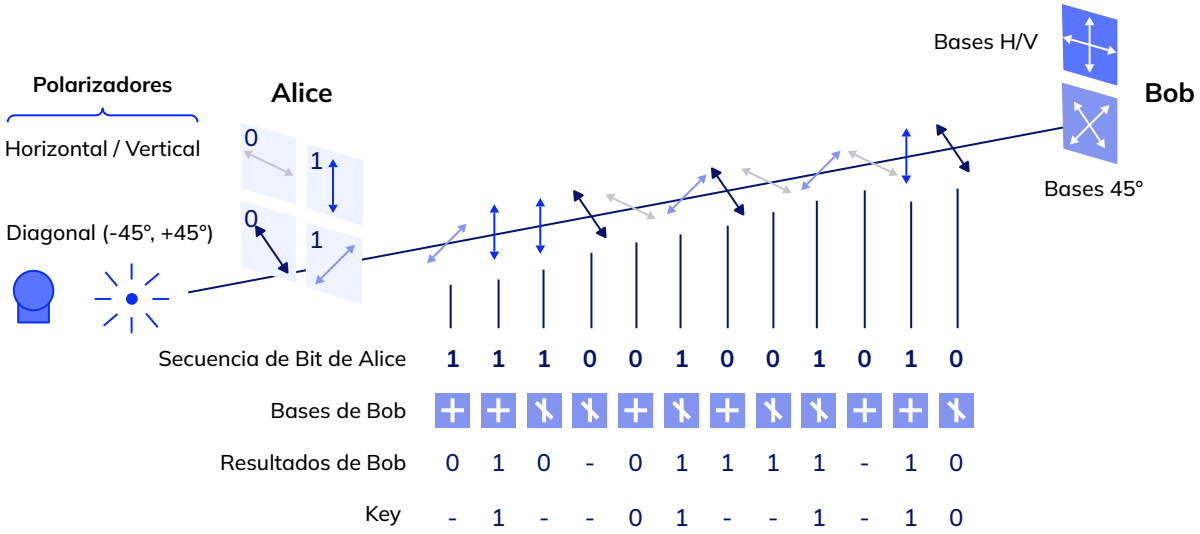
Base Diagonal

3. Luego, Alice transmite un solo fotón en el estado especificado hacia Bob, usando el **canal cuántico**. Este proceso es entonces repetido a partir de la **etapa del bit aleatorio**, con Alice registrando el estado, base y tiempo de cada fotón enviado.

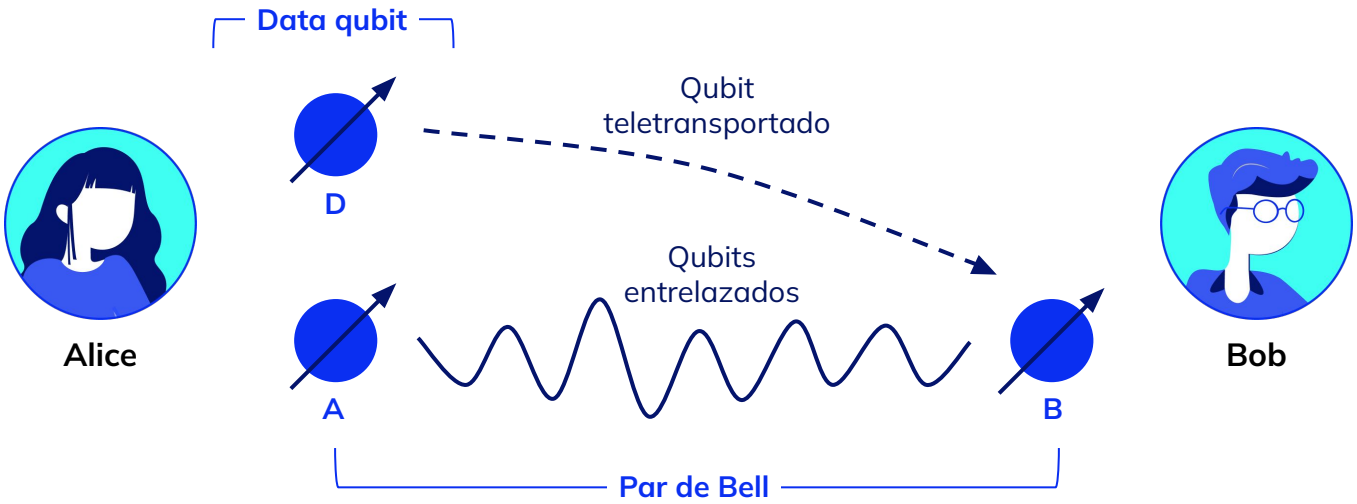


4. Como Bob no conoce la base de codificación de los fotones, selecciona una **base aleatoria** para medirlo.

Él realiza esto para cada fotón que recibe, registrando el tiempo, la base de medición usada y el resultado de la medición.



5. Al finalizar la transmisión Bob le comunica a Alice que base seleccionó para cada medición a través de un **canal público autenticado**.
6. Alice le comunica a Bob los fotones que arrojaron resultados correctos pero no le indica cuál fue su polarización a través de un **canal inseguro**.
7. Alice y Bob mantienen las **polarizaciones correctas**, y este *string* de aproximadamente un 50% de los fotones emitidos es un ***one time pad* de Vernam de longitud n/2**, siendo **n** la cantidad de fotones transmitidos.
8. Si Eve intenta espiar la secuencia de fotones, al no conocer de antemano si la polarización del próximo fotón es diagonal o rectilínea, no podrá medirlo sin correr el riesgo de perturbarlo de tal forma que se introduzca un error.
9. Finalmente, Alice y Bob verifican el **nivel de error de la clave** final para validarla. Esto lo hacen haciendo públicos una cierta cantidad de bits. Si encuentran diferencias en sus bits, tienen una razón para sospechar que están siendo espiados y deberán descartar todos los datos y comenzar nuevamente el intercambio de fotones.


Data qubit
Qubit
teletransportado
D
Qubits
entrelazados
Alice
A
B
Bob
Par de Bell

Otros protocolos de QKD

E91 (Ekert 1991)

Utiliza el entrelazamiento de pares de fotones. Cuando dos qubits se entrelazan, el estado de uno queda indisolublemente unido al otro: la información podría ser transmitida y procesada “a distancia”, en forma no local (el cambio en un qubit automáticamente modificaría al otro entrelazado aunque estuviera en la otra punta del universo). Ambos qubits forman un **par de *Bell*** (por el físico que ideó una forma de probar el entrelazamiento).

B92

Es una modificación del protocolo BB84.

MDIQKD

Distribución de clave cuántica independiente del dispositivo de medición, Mayers y Yao (1998).

TFQKD

Distribución de claves cuánticas por campos gemelos (2018).

Ataques sobre QKD

Ataques *Man in the Middle* (MITM)

En la misma medida que cualquiera de los protocolos clásicos, QKD es vulnerable a los ataques MITM cuando no se utiliza la autenticación. Ningún principio conocido de la mecánica cuántica resuelve el problema de la autenticación. Alice y Bob no pueden establecer una conexión segura sin verificar sus identidades respectivas.

Ataque de división del número de fotones

Muchas implementaciones utilizan pulsos láser atenuados a un nivel muy bajo para enviar los estados cuánticos. Estos pulsos láser contienen un número muy pequeño de fotones por pulso. Si el pulso contiene más de un fotón, entonces Eve puede separar los fotones adicionales y enviar el fotón único restante a Bob.

Denegación de servicios (DoS)

Un canal cuántico es un canal especial que conecta dos participantes punto a punto, con sus fuentes y detectores de fotones. Los enlaces punto a punto incrementan las posibilidades de DoS.

Ataques de troyanos

Eve podría enviar luz brillante al canal cuántico y analizar los reflejos. Se ha demostrado que Eve podría discernir la elección de la base secreta de Bob con una probabilidad superior al 90%.

Otros ataques conocidos

Ataques de estado falso, ataques de reasignación de fase, y ataques de desplazamiento temporal.

¡Sigamos trabajando!