Quantum Key Distribution

ALEMAN FLORES CARLOS EDUARDO
PÉREZ DUARTE BRENDA ELIZABETH

Origenes de la criptografía

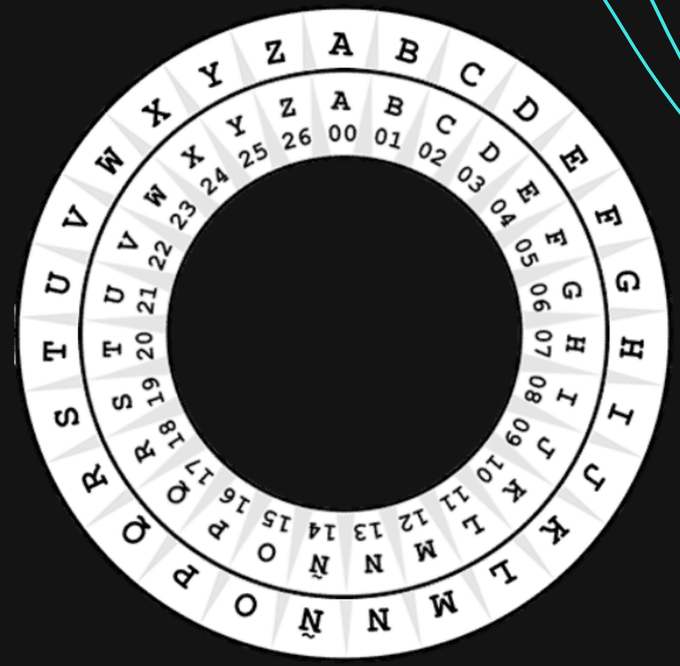
TRANSPOSICIÓN Y SUSTITUCIÓN

ESCITALA

Bastón de determinado grosor en el que se enrollaba una tira de papel o cuero con una serie de letras, que al enrollar en el bastón mostraba el mensaje en la tira.

CIFRADO CÉSAR

Consiste en reemplazar una letra por otra, desplanzando un cierto número de letras, por ejemplo, la A con la D y la B con la E al desplazar 3 letas.



Rompiendo el cifrado monoalfabético

Al-Kindi propone el análisis de frecuencia al notar que al cambiar una letra por otra, ésta mantenía sus características.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Cifrado polialfabético

Cada letra tiene una sustitución diferente, por ejemplo la primer letra se desplaza 4 lugares, la segunda 9 y la tercera 1, obteniendo la llave 491, este método puede hacer que 2 letras diferentes sean sustituidas por la misma letra, por lo que el análisis de frecuencia no sería útil

Rompiendo el cifrado polialfabético

PLANTEAMOS UNA CADENA PARA CIFRAR

Tomamos TOBEORNOTTOBE, que al cifrar obtenemos ACULCVUCMACUL

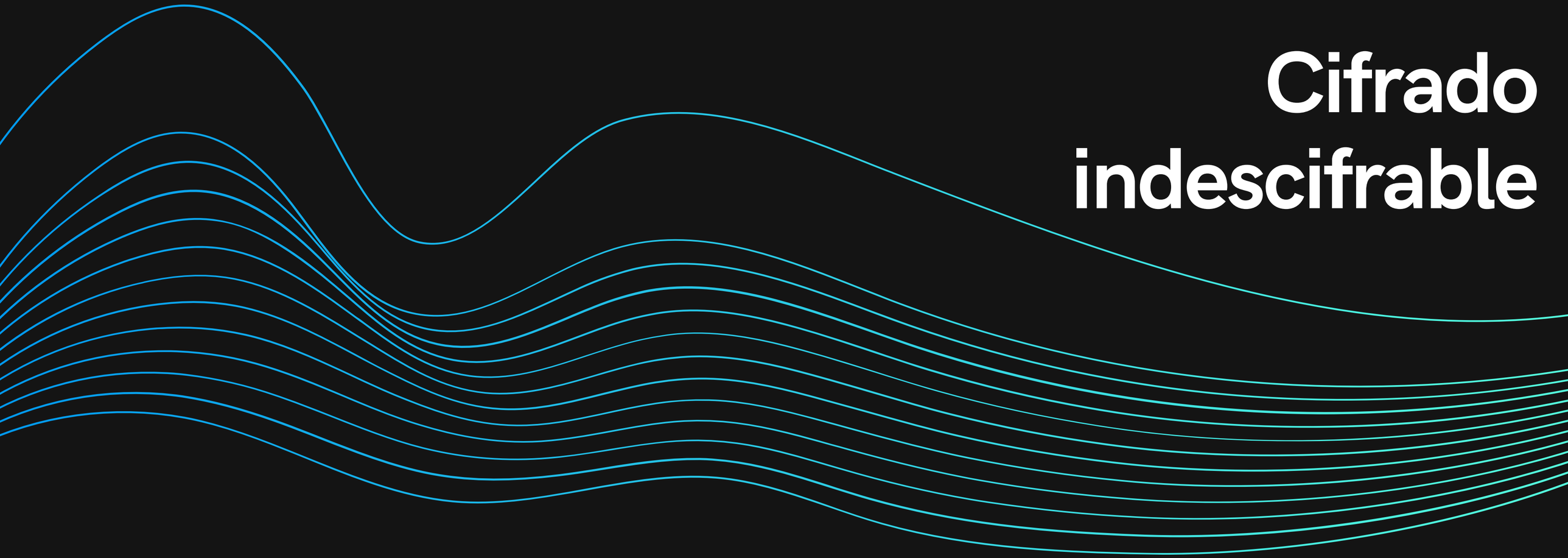
BUSCAMOS PATRONES

Podemos observar que la secuencia ACUL se repite con una distancia de 9, lo que nos dice que la llave es de tamaño 9, 3 o 1

ANÁLISIS DE FRECUENCIA

Conociendo las posibles distancias, hacemos un análisis de frecuencia cada tercer o noveno caracter y alguno revelará el mensaje.

Cifrado indescifrable



ONE-TIME PAD

Basado en el alfabeto binario y su adición, el mensaje se convierte en una cadena de 1's y 0's

CIFRADO

La cadena se suma a una llave de 1's y 0's bajo las reglas de suma binaria obteniendo así la cadena cifrada

DESCIFRADO

La cadena cifrada se suma a la llave y se obtiene el mensaje original

CONDICIONES

Si la llave es secreta, de la misma longitud del mensaje, aleatoria y de un solo uso, entonces es indescifrable

Un nuevo problema

PROBLEMA DE DISTRIBUCIÓN DE LLAVE

Los usuarios deben acordar previamente una llave para realizar el cifrado y transmitir el mensaje con seguridad

SEGURIDAD

Aún con una línea segura no se sabe si es realmente segura ya que puede ser monitoreada de forma pasiva

FÍSICA CLÁSICA

Las propiedades de la física clásica dictan que al medir un objeto no alteramos sus propiedades

Protocolo RSA

VENTAJAS

Evita el problema de distribución de llave al tener una llave pública y una llave privada.

DESVENTAJAS

Basa su seguridad en la dificultad de las computadoras para factorizar números grandes, por lo que si se propone un méotodo más rápido, para factorizar, su seguridad ya no existiría.

Distribución cúantica de llave

FÍSICA CÚANTICA

Los principios de la física cúantica nos dicen que la observación de un estado cúantico causa perturbación de éste

PROTOCOLOS DE QKD

Están diseñados para que asegurar que los intentos de espionaje causen perturbaciones y alerten a los usuarios legítimos

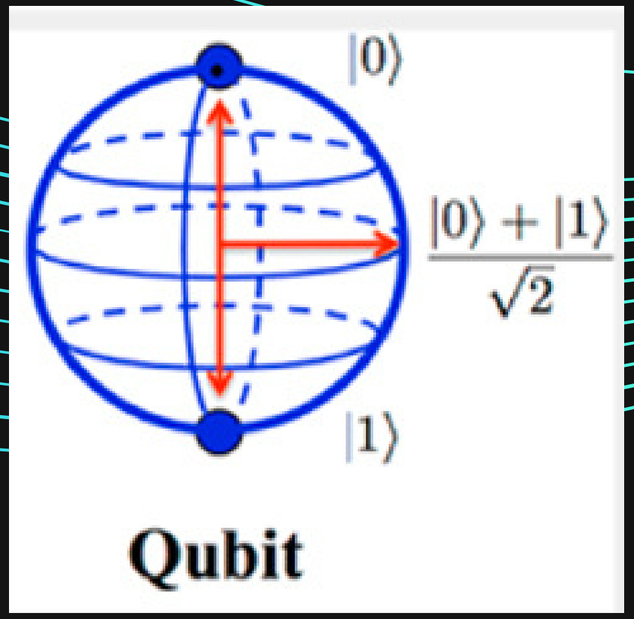
LÍMITACIONES

Al combinarlo con OTP límita el ancho de banda, ya que el OTP debe ser tan largo como el mensaje y la distribución de QKD es entre mil y diez mil veces más lenta que otras comunicaciones

Qubit

Puede verse como una partícula cuántica que no esta limitada por 2 estados.

Los fotones son excelentes para la comunicación cuántica para transmitir sobre largas distancias



Ventajas

La gran cantidad de información que contiene

Teletransportación Cuántica

Fue propuesta en 1993 por Bennett y es u
importante protocolo con aplicaciones en re
cuánticas y computación cuántica.

Otro protocolo de transportación es el QND donde el estado cuántico no es destruido y la información cuántica restante que esta almacenada en otros niveles está intacta.

Computadora Cuántica

El principal motivo para crear una maquina cuantica es la capacidad de cáculo que pueede resolver problemas con una velocidad exponencialmente más rápida que los equipos clásicos.

SUPERPOSICIÓN

Permite que los algoritmos cuánticos uriliceen otros fenómenos

INTERFERENCIA

Los estados de los qubits pueden intererir entre si.

ENTRELAZAMIENTO

Los qubits pueden presentar entrelazamiento cuántico.

Esquemas básicos de cifrado

PROTOCOLO BENNETT - BRASSARD

Mejor conocido como BB84

ESQUEMA DE EKERT

Protocolo BB84

$B_X = [|+\rangle, |-\rangle]$ $\quad |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$B_1 = [|0\rangle, |1\rangle]$ $\quad |0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle), \; |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$

Estado	Medido con B_1 se obtiene	Medido con B_X se obtiene
$\|0\rangle$	$\|0\rangle$, con probabilidad p=1	$\|+\rangle$ con prob. p=1/2 $\|-\rangle$ con prob. p=1/2
$\|1\rangle$	$\|1\rangle$, con probabilidad p=1	$\|+\rangle$ con prob. p=1/2 $\|-\rangle$ con prob. p=1/2
$\|+\rangle$	$\|0\rangle$, con probabilidad p=1/2 $\|1\rangle$, con probabilidad p=1/2	$\|+\rangle$ con prob. p=1
$\|-\rangle$	$\|0\rangle$, con probabilidad p=1/2 $\|1\rangle$, con probabilidad p=1/2	$\|-\rangle$ con prob. p=1

GIEMATIC

Protocolo Ekert

Esta desigualdad es usada para checar que un estado entrelazado cuántico compartido entre 2 partes no se viole

Un one time pad consiste en una serie de número saleatorios compartidos entre 2 partes que sirven como llave para cifrar o descifrar.

Un ejemplo

Mensaje	0	0	1	0	1	1	0	0	0	1
Base elegida	B_1	B_X	B_1	B_X	B_1	B_X	B_1	B_1	B_X	B_X
Codificación	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$
Polarización	→	↗	↑	↗	↑	↘	→	→	↗	↘
B mide con	B_1	B_1	B_X	B_X	B_X	B_1	B_1	B_1	B_X	B_X
Resultado	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$
Reconciliación	0			0			0	0	0	1

Espionaje

Existe la posibilidad de que un espía, convencionalmente llamada Eva, intercepte los qubits envíados por Eva y los reenvíe a Bob, sin embargo por propiedades de la cúantica ésto podría modificar el estado del qubit. ¿Qué podría pasar?

Posibles escenarios

ESCENARIO 1

Eva mide el qubit en el mismo eje que fue preparado el qubit, por lo que no perturbaría el estado inicial del qubit, regresando el qubit a Bob pasando inadvertida.

ESCENARIO 2

Eva mide el qubit en el eje contrario al que fue preparado, destruyendo el estado inicial, regresa el qubit a Bob, si Bob mide en un eje diferente al que fue preparado por Alice, Eva pasa desapercibida

ESCENARIO 3

Eva mide el qubit en el eje contrario al que fue preparado, lo regresa a Bob, si Bob mide en el eje que fue preparado originalmente, puede obtener el estado en el que se preparó, por lo que Eva pasaría desapercibida.

ESCENARIO 4

Eva mide el qubit en el eje contrario al que fue preparado, lo regresa a Bob, si Bob mide en el eje que fue preparado originalmente y no obtiene el estado en el que fue preparado por Alice, por lo que Alice podría darse cuenta y detener el protocolo.

PROBABILIDAES

Con un qubit, Eva tiene un 25% de probabilidad de ser descubierta, pero, con 10 qubits, la probabilidad aumenta a un 95% y con 50 qubits aumenta a 99.9999% de ser descubierta.

Ataques y mitigación

Existen diferentes métodos de ataque hacía la QKD, pero esto ha provocado que también se desarrollen métodos de mitigación a éstos.

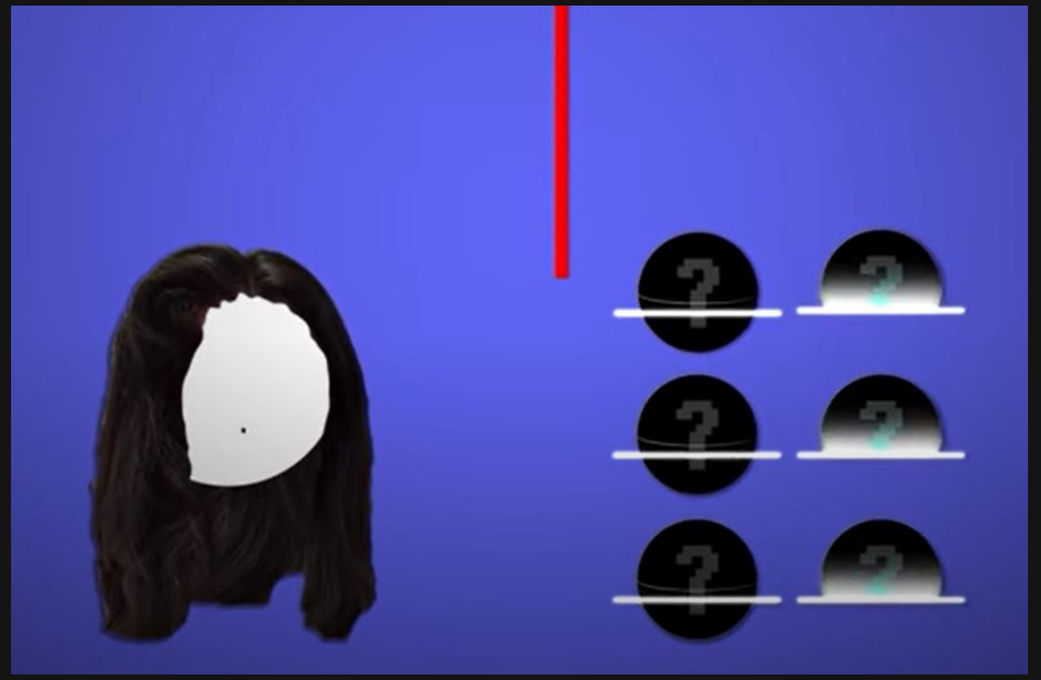
Clonación de qubits

ATAQUE

Clonar los qubits enviados por Alice, enviar los originales a Bob y medirlos hasyas que se publiquen los resultados.

MITIGACIÓN

No se pueden clonar los qubits si no se conoce su estado.



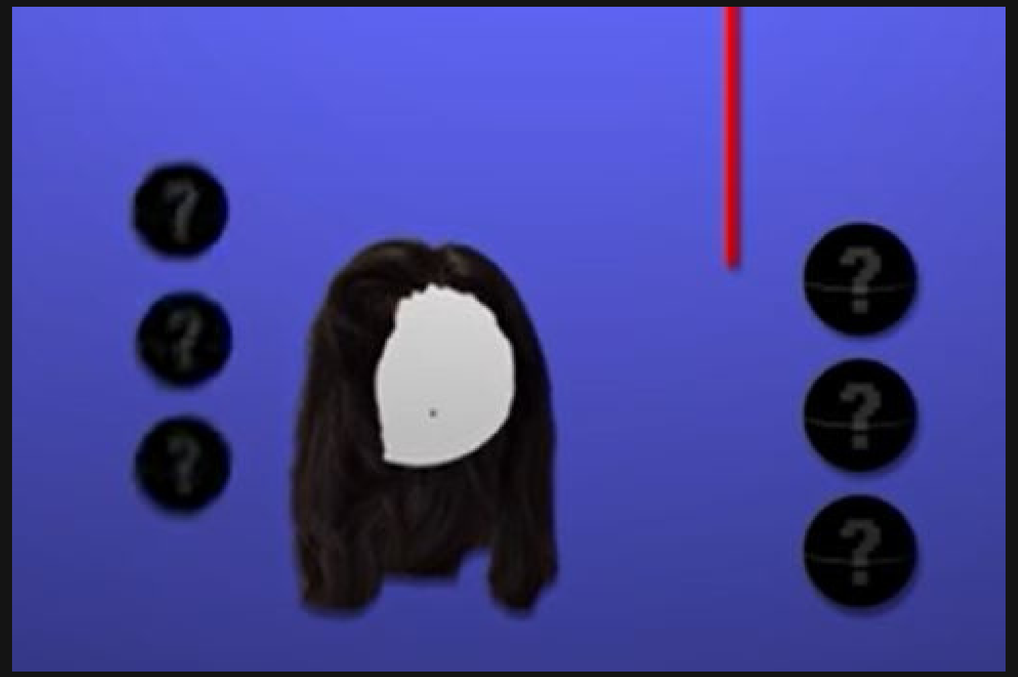
Envío de otros qubits

ATAQUE

Tomar los qubits enviados por Alice y envíar a Bob unos preparados por Eva, medir los qubits originales cuando se publiquen los resultados

MITIGACIÓN

Habría grandes diferencias entre los valores de Alice y Bob, lo que abortaría el protocolo.



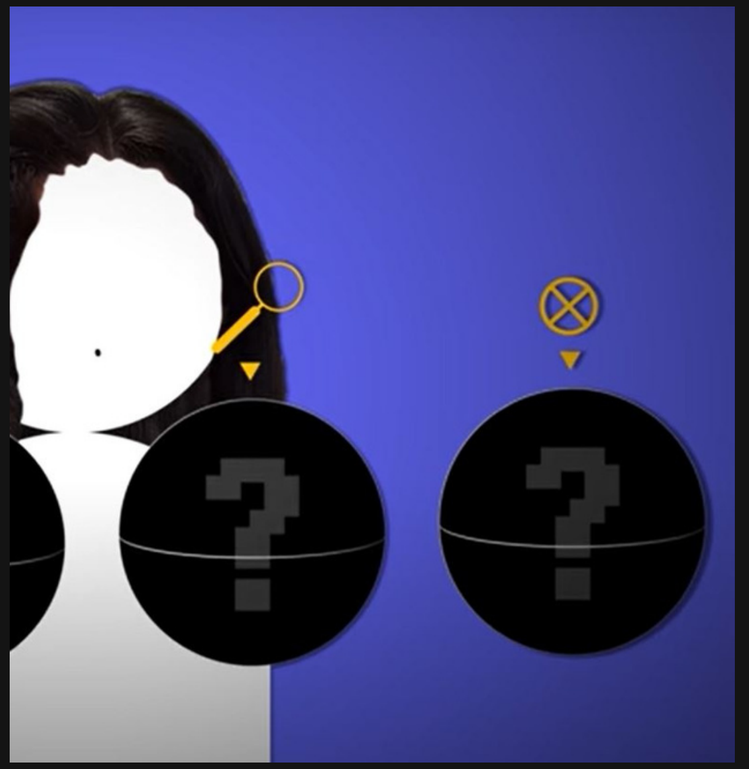
Medición de menos qubits

ATAQUE

Medir de forma salteada los qubits, esto disminuye la probabilidad de ser descubierta

MITIGACIÓN

Aumentar la cantidad de qubits de seguridad aumentaría la probabilidad de descubrir a Eva.



Ataque de escisión del número de fotones

EXPLICACIÓN

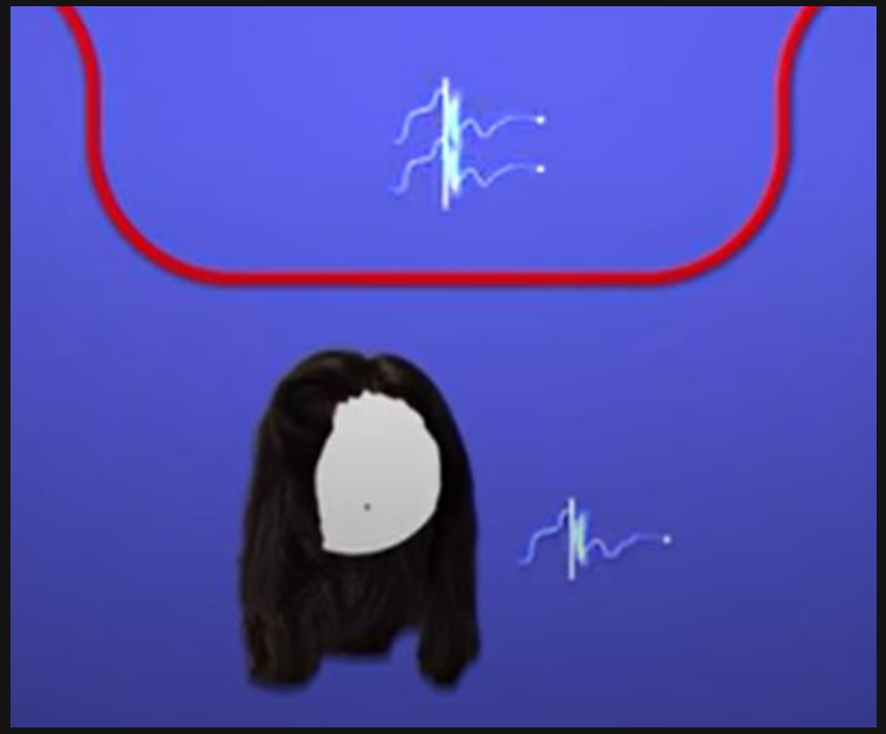
Al preparar los qubits se pueden programar en más de un fotón.

ATAQUE

Tomar solo un fotón y permitir el paso a los demás fotones.

MITIGACIÓN

Realizar un conteo de los fotones envíados y recibidos.



Ataque del caballo de Troya

ATAQUE

Envíar pulsos de luz por el canal hacia el emisor para determinar la configuración del emisor

MITIGACIÓN

Se implementa un canal de una sola dirección.

QKD en el mundo

La QKD ha sido comercializada por empresas como IDQ desde el 2007, usada para asegurar las elecciones de Ginebra en 2007, actualmente esusada en bancos y gobiernos al rededor del mundo.

Referencias

QUANTUMFRACTURE. (2019). HACKEANDO MENSAJES CUÁNTICOS: LA VENGANZA DE EVA. RETRIEVED 9 MAY 2022, FROM HTTPS://WWW.YOUTUBE.COM/WATCH?V=IBUVXJ0VXFC&AB_CHANNEL=QUANTUMFRACTURE

QUANTUMFRACTURE. (2019). CÓMO MANDAR UN MENSAJE SECRETO CON FÍSICA CUÁNTICA | ENCRIPTACIÓN CUÁNTICA. RETRIEVED 9 MAY 2022, FROM HTTPS://WWW.YOUTUBE.COM/WATCH?V=7R7DNT2043M&AB_CHANNEL=QUANTUMFRACTURE

QKD TECHNOLOGY. RETRIEVED 9 MAY 2022, FROM HTTPS://WWW.IDQUANTIQUE.COM/QUANTUM-SAFE-SECURITY/QUANTUM-KEY-DISTRIBUTION/

GARCÍA, A., GARCÍA, F., & GARCÍA, J. (2014, 24 JUNIO). MOOC CRYPT4YOU UPM. CRYPT4YOU AULA VIRTUAL. RECUPERADO 9 DE MAYO DE 2022, DE HTTP://WWW.CRIPTORED.UPM.ES/CRYPT4YOU/TEMAS/CUANTICA/LECCION2/LECCION02.HTML

Referencias

MICROSOFT. (S. F.). ¿QUÉ ES UN QUBIT? | MICROSOFT AZURE. MICROSOFT AZURE. RECUPERADO 9 DE MAYO DE 2022, DE HTTPS://AZURE.MICROSOFT.COM/ES-MX/OVERVIEW/WHAT-IS-A-QUBIT/#SUPERPOSITION-INTERFERENCE-ENTANGLEMENT

PETRITSCH, K. (2018). QUANTUM INFORMATION SCIENCE: THE NEW FRONTIER IN QUANTUM COMPUTATION, SECURE COMMUNICATION, AND SENSING. ARCLER PRESS.

SERGIENKO, A., V. (2005). QUANTUM COMMUNICATIONS AND CRYPTOGRAPHY. CRC PRESS.