Revisión sistemática del estado del arte de la criptográfia cuántica, sus usos y aplicaciones

John Harrison Cardona Cardona

Universidad Nacional Abierta y a Distancia

Escuela De Ciencias Básicas, Tecnología e Ingeniería

Ingeniería De Sistemas

Santiago De Cali

2022

Revisión sistemática del estado del arte de la criptográfia cuántica, sus usos y aplicaciones

John Harrison Cardona Cardona

monografía para optar por el

título de ingeniero de sistemas

director

ing. Joel Carroll Vargas m. Sc

Universidad Nacional Abierta y a Distancia

Escuela De Ciencias Básicas, Tecnología e Ingeniería

Ingeniería De Sistemas

Santiago De Cali

2022

Página de aceptación

Nota de aceptación:

Aprobado en cumplimiento de los requisitos

exigidos por la Universidad Nacional Abierta y A

Distancia UNAD para optar por el título de

Ingeniero de Sistemas.

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá DC 02/12/2022.

Agradecimiento

Mi profundo agradecimiento a Ingeniero Joel Carroll Vargas M. Sc director del semillero Kerberos y asesor de este proyecto por ser guía y motivador en la consolidación de esta monografía.

Contenido

Lista de Figuras

Lista de Tablas

Resumen

El uso de métodos de encriptación a la hora de compartir información sensible es indispensable en la actualidad, estos métodos usados han sido basados en esquemas de cifrado por tecnología de computación matemática los cuales en alguna medida han presentado ciertas vulnerabilidades a ser descifrados, es por esto que surge la idea de la criptografía cuántica, la cual funciona aplicando las leyes de la mecánica cuántica y puede ser usada sin restricciones para comunicaciones de datos confiables que en teoría superan los inconvenientes que ha presentado la criptografía tradicional

En la presente monografía se realiza un levantamiento y revisión de la literatura científica relevante que ha estudiado la criptografía cuántica en los últimos 5 años, consolidando su descripción detallada, leyes que la fundamentan, usos, propiedades, nivel de seguridad e integridad de la información que proporciona, vulnerabilidades, como ha sido concebida en forma hipotética y como se pone en práctica, además de su visión a futuro como el campo criptográfico más prometedor y los desafíos que supone pasar a este método de encriptación no tradicional.

Palabras clave: Criptografía Cuántica, Distribución de Claves Cuánticas, Protocolo BB84, Cúbit.

Abstract

The use of encryption methods when sharing sensitive information is indispensable today, these methods used have been based on encryption schemes by mathematical computing technology, which to some extent have presented certain vulnerabilities to be decrypted, which is why the idea of quantum cryptography arises, which works by applying the laws of quantum mechanics and can be used without restrictions for reliable data communications, which in theory overcomes the drawbacks that traditional cryptography has presented.

In this monograph a survey and review of the relevant scientific literature that has studied quantum cryptography in the last 5 years is carried out, consolidating its detailed description, laws that underlie it, uses, properties, level of security and integrity of the information it provides, vulnerabilities, how it has been conceived hypothetically and how it is put into practice, as well as its future vision as the most promising cryptographic field and the challenges of switching to this non-traditional encryption method.

Keywords: Quantum Cryptography, Quantum Key Distribution, BB84 Protocol, Qubit.

Introducción

Con el uso global y la importancia cada vez más trascendental que tienen los datos en la actualidad han hecho que la encriptación de la información sea un tema cada vez más relevante y competente; Las amenazas al acecho y la necesidad de evolución en la materia han hecho de la criptografía cuántica una ciencia para muchos nueva el eje de la protección definitiva de la información a un futuro cercano, pero se hace necesario entender realmente en que consiste y que implica las técnicas derivadas de esta tecnología vanguardista.

Esta monografía es una recopilación documental de producción científica pertinente que pretende ilustrar un estado del arte de la criptografía cuántica en los últimos 5 años que referencia el punto actual y más avanzado sobre esta temática especifica, generando una oportunidad para comprender las definiciones detalladas, leyes de la mecánica cuántica que la soportan, usos, aplicaciones reales, propiedades, nivel de seguridad e integridad de la información que proporciona y que permita un acercamiento y estudio a la temática como campo de la investigación.

Titulo

Revisión sistemática del estado del arte de la criptográfica cuántica, sus usos y aplicaciones

Formulación del problema

Desde que el ser humano empezó a compartir información confidencial nació la necesidad de preservar la privacidad de los datos que se transmiten se empezaron a crear métodos que evitaban que una persona para la cual no fue destinada el mensaje pudiese interpretar su contenido, fue así como se implementó la criptografía, la cual permite que registros normales se pueden convertir en mensajes ininteligibles

En la actualidad la criptografía moderna se utiliza a través de diversos algoritmos y protocolos criptográficos tales como: cifrado simétrico el cual se utiliza para ocultar el contenido de bloques o secuencias de datos de cualquier tamaño, incluidos mensajes, archivos, claves de cifrado y contraseñas, cifrado asimétrico que se utiliza para ocultar pequeños bloques de datos, como claves de cifrado y valores de función hash, que se utilizan en firmas digitales, Algoritmos de integridad de datos los cuales se utilizan para proteger bloques de datos, como mensajes, por alteración y protocolos de autenticación que son esquemas basados en el uso de algoritmos criptográficos diseñados para autenticar la identidad de entidades. (Stallings, 2017)

Los métodos criptográficos usados en la actualidad no están libres de vulnerabilidades, los avances tecnológicos que han sido las herramientas para encriptar la información han sido usados de igual manera para romper estos métodos, actualmente se está haciendo uso de hardware específico para este fin como unidades de procesamiento gráfico para realizar ataques de fuerza bruta capaces de probar un numero exorbitante de combinaciones de todas las claves privadas posibles. (Mok1 & Chai , 2019)

Lo expuesto evidencia que si bien la criptografía tradicional ofrece un nivel de seguridad elevado para que sea lo suficientemente seguro debería de ser imposible descifrar un mensaje si no se conoce la clave. Esta problemática ha despertado la necesidad de utilizar un método que no se base en encriptación matemática como la criptografía tradicional y a su vez no posea sus vulnerabilidades. Para esto se ha creado la técnica de la criptografía cuántica que toma los principios de la mecánica cuántica, como el principio de incertidumbre de Heisenberg, la superposición y el entrelazamiento cuánticos con lo cual se evita la escucha y manipulación a la comunicación, esto con el fin de garantizar la integridad, disponibilidad y confidencialidad de la información, Ahora bien, esto genera la pregunta definitiva para el mundo de la criptografía:

¿Cómo contribuye el uso de Criptografía cuántica en la absoluta confidencialidad de la información transmitida y que implicaciones tiene su aplicación?

Justificación

Vivimos en una era en la cual, casi todas las actividades se realizan a través del internet, los datos cuentan con un valor incalculable, proteger la privacidad de la información es indispensable y cada vez se demandan métodos que tengan la capacidad de ser infalibles ante cualquier vulnerabilidad; la criptografía que se usa en la actualidad la cual está basada en métodos matemáticos ha brindado seguridad, integridad y anonimización en la información, no obstante, se plantean interrogantes de hasta qué punto estos métodos criptográficos son técnica efectiva y si se puede utilizar otra técnica que proporcione una protección adicional en el tratamiento de datos personales.

Los avances tecnológicos especialmente de hardware amenazan con poner en aprietos a la criptografía tradicional como el aumento de descifrado de contraseñas apoyado en GPU que proporcionan una forma de realizar cálculos masivamente paralelos, que representan la mayoría de los ataques de fuerza bruta. Como punto de referencia, en un solo NVidia GTX 1080 GPU es capaz de hacer más de 43 mil millones de conjeturas por segundo, Las GPU han cambiado el descifrado de contraseñas de formas aún más fundamentales que simplemente permiten adivinar más rápido. (Aggarwal, Houshmand, & Weir, 2018)

Las amenazas a la seguridad de la información son las que han impulsado el uso de una alternativa a la criptografía tradicional, sistemas cuánticos diseñados de tal manera que utilizan la mecánica cuántica y depende en gran medida de la física clásica. El concepto básico es que es difícil calcular el estado cuántico de cualquier sistema sin perturbarlo. El principal objetivo de la

criptografía cuántica es crear una clave que se utiliza en el sistema de cifrado para transferir datos con fotones ligeros a través de cualquier fibra óptica o espacio libre, Esto garantizaría en teoría la completa integridad, disponibilidad y confidencialidad de la información compartida. (Moizuddin, Winston, & Qayyum, 2017)

Comprender el concepto de la criptografía cuántica, sus usos y aplicaciones es un proceso complejo, es por esto que en esta monografía se realiza un levantamiento documental de calidad y se recopilan un número significativo de referencias bibliográficas que permiten desarrollar un estado del arte que referencia el punto actual y más avanzado sobre esta temática especifica, generando una oportunidad para comprender cómo la abstracción de un concepto teórico puede materializarse en una realidad. Un estado del arte de la criptografía cuántica en español permitirá un acercamiento y estudio a la temática para profesionales como ingenieros, matemáticos y físicos no solo como herramienta para el reconocimiento e interpretación preliminar también con el fin de motivar la investigación académica y nuevos desarrollos en el área y como base para la toma de decisiones en el campo de la investigación.

Objetivos

Objetivo General

Desarrollo de revisión bibliográfica de los estudios científicos en la ciencia de la criptografía cuántica.

Objetivos Específicos

Clasificar al menos 50 referencias bibliográficas científicas sobre la criptografía cuántica

Desarrollar un estado del arte sobre la criptografía cuántica

Generar un documento publicable sobre la criptografía cuántica

Marco referencial

Marco Metodologico

Tipo de estudio: En la presente monografía se realizará un estudio de revisión sistemática producto de un levantamiento documental exhaustivo que permita generar un estado del arte sobre la criptografía cuántica. El estado del arte es una modalidad de la investigación documental que permite el estudio del conocimiento acumulado dentro de un área específica; Sea cual fuere el abordaje del estado del arte, se considera que su realización implica el desarrollo de contextualización, clasificación y categorización. (Montoya, 2005)

Diseño de investigación: La monografía se desarrollará bajo un diseño descriptivo, basado en la compilación, el análisis y presentación de la información recopilada. Este tipo de diseño es el más apropiado para un documento de recopilación y revisión bibliográfica ya que proporciona al lector una puesta al día sobre conceptos útiles en áreas en constante evolución, generando utilidad en la enseñanza y campos conexos. (Whittemore & Chao, 2014)

Unidad de análisis y muestreo: El objetivo de la monografía es el desarrollo de una revisión bibliográfica de los estudios científicos en la ciencia de la criptografía cuántica, por lo tanto, la unidad de análisis central es la criptografía cuántica, para el levantamiento documental especifico se delimita una variable de tiempo inferior a los 5 años con lo que se espera una recopilación de la ciencia estudiada a un concepto actual y de sus proyecciones a futuro.

Recolección de datos: Para el levantamiento documental con el que se pretende clasificar al menos 50 referencias bibliográficas científicas sobre la criptografía cuántica, se recurrirá a la IEEE Xplore, que es una base de datos de investigación académica que proporciona acceso a

artículos y trabajos sobre ciencias de la Computación, Ingeniería Eléctrica y Electrónica igualmente Springer Link y Nature. Estas bases de datos están en calidad de suscripción a través de la biblioteca de la UNAD. Se delimitarán los documentos incluyendo solo publicaciones con rigor científico y con una fecha de publicación inferior a 5 años excepto algunas publicaciones que por su relevancia teórica e histórica necesitarán ser incluidos.

Marco conceptual

Concepto de Criptografía: El término criptografía deriva de las palabras griegas *"kryptós" y "gráphein"*, que significan "oculto" y "escribir". Por lo tanto, se puede parafrasear como "escritura oculta". La criptografía es la ciencia matemática encargada de transformar los datos para hacer ininteligible su significado, es decir, para ocultar su contenido, evitar su alteración e impedir su uso no autorizado. Si la transformación de los datos es reversible, la criptografía también se ocupa de restaurar datos encriptados a su forma inteligible. (Oppliger, 2021)

La criptografía engloba el proceso de protección de datos en un sentido muy amplio y se rige bajo los principios de seguridad de la información:

- **Confidencialidad:** Especifica que sólo el remitente y el destinatario pueden acceder a los datos.
- **Autenticación:** La autenticación asegura la identidad del usuario y el origen del mensaje.
- **Integridad:** Garantiza que el mensaje no se modifica incluso después de que el remitente lo haya enviado.
- **Control de acceso:** Administra quien puede acceder y a que puede acceder. Se relaciona con dos áreas como la gestión de roles y la gestión de reglas.
- **No repudio:** El remitente no puede desacreditar las transacciones realizadas anteriormente.

- **Disponibilidad:** Enfatiza los recursos que son obtenibles para las partes autorizadas de forma perpetua, la finalidad es evitar la interrupción. (Kahate, 2018)
- **Concepto de Criptoanálisis:** El criptoanálisis, al contrario de la criptografía corresponde a las técnicas que estudian la forma de romper los algoritmos criptográficos. El criptoanálisis es comúnmente usado para comprobar la solidez de los procedimientos de seguridad y en la exploración de las diferentes vulnerabilidades de los cifrados. (Cortez, Sison, & Medina, 2020)

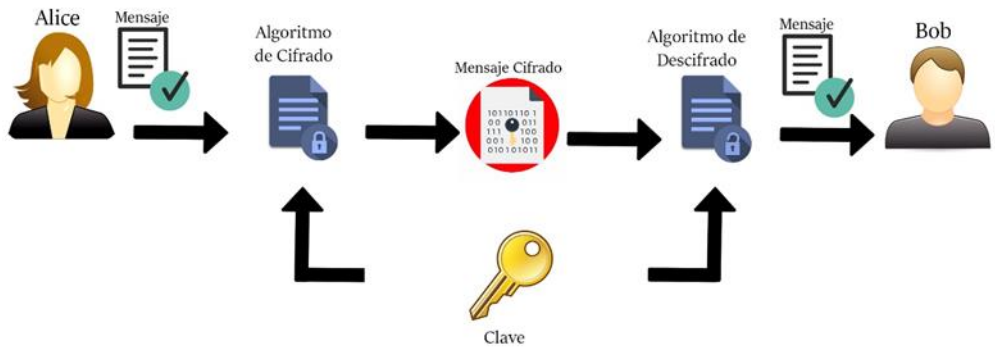
El criptoanálisis ha coevolucionado junto con la criptografía, a medida que nuevas técnicas de cifrado salen a la luz paralelamente se crean técnicas para descifrarlos.

Criptografía Moderna

La criptografía tiene dos características notables: una tiene una larga historia y la otra es que esta soportada fuertemente en la matemática. La técnica criptográfica más antigua es el cifrado, con ella se consigue la confidencialidad. Antes de la era digital la encriptación se utilizaba sobre todo para proteger las comunicaciones militares y gubernamentales hoy en día la criptografía es usada básicamente en cualquier lado sobre todo en Internet. Otras técnicas criptográficas fundamentales criptográficas son las funciones hash criptográficas y los esquemas de firma digital las cuales se utilizan para proteger la integridad y la autenticidad de los datos. (Ma J. , 2020) Además de lograr los objetivos de seguridad mencionados.

En el proceso de encriptación los datos originales, es decir el texto plano del mensaje se transforma en un mensaje codificado, es decir código resultado del algoritmo de cifrado para poder transmitir estos datos a través de canales de comunicación no seguros. Una cadena de datos que conocida como "Clave" se utiliza para controlar la transformación de los datos de texto plano a texto cifrado. Esta disposición ayuda a mantener los datos seguros ya que se requiere siempre de la clave para poder extraer la información original del texto cifrado y sin la clave nadie puede leer los datos.

Figura 1.Sistema criptográfico.



Fuente: Autor

Como se muestra en la Figura 1 el proceso de un sistema criptográfico inicia con el mensaje sin cifrar los datos de este mensaje son cifrados a través de un algoritmo, una vez cifrado viaja por el canal ya codificado cuando llega al destinatario se descifra con la clave y se transforma nuevamente en el mensaje inicial sin cifrar, En la figura se utilizan los nombres de Alice y Bob para hacer referencia a un usuario A y B y el nombre Eve será usado para hacer referencia a un *eavesdropper*, una escucha, un espía que representa el usuario que intermedio que desea interceptar los mensajes enviados y es el objetivo principal a vencer en el cifrado de datos.

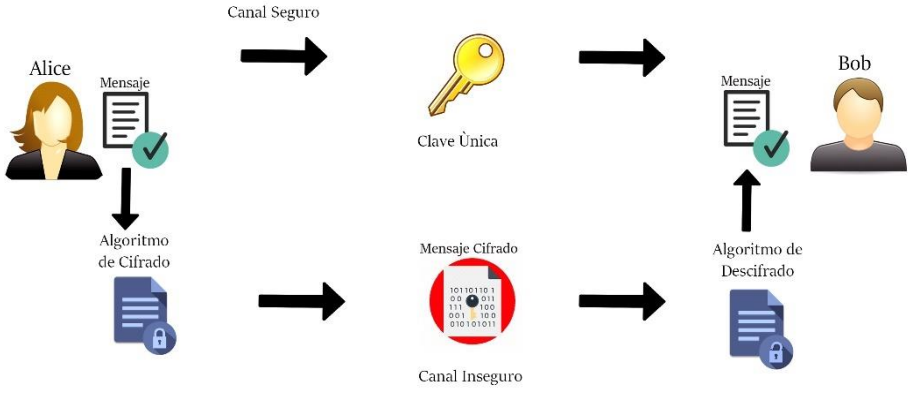
Actualmente la seguridad proporcionada por los criptosistemas de clave en uso se basa en la alta complejidad de problemas matemáticos para la factorización de instancias de número grandes, estos criptosistemas de clave se dividen a su vez dos tipos: Sistemas de cifrado simétrico y sistemas de cifrado asimétrico.

Sistema de cifrado simétrico:

Los sistemas de cifrado simétrico utilizan una sola clave privada tanto para el cifrado como para el descifrado. Como se muestra en la Figura 2 la clave única se intercambia entre Alice y Bob que se comunican antes de la transmisión de los datos por un canal seguro, mientras que el mensaje cifrado se envía por un canal inseguro. Para cifrar el mensaje el algoritmo de encriptación lleva a cabo una serie de sustituciones y transformaciones en el texto plano por su parte el algoritmo de descifrado en el cifrado de clave simétrica es el inverso del algoritmo de cifrado.

Los sistemas de cifrado simétrico son susceptibles a ataque de fuerza bruta y ataque de criptoanálisis en donde el atacante hace uso de características del algoritmo para hacerse con la clave o con el texto descifrado.

Figura 2 . Cifrado Simétrico.

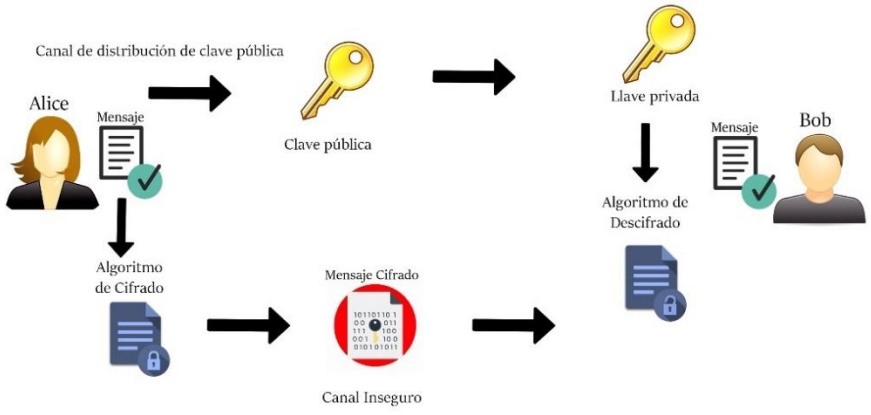


Fuente: Autor

Sistema de cifrado Asimétrico:

Los sistemas de cifrado simétrico se caracterizan por utilizar un par de claves: una clave pública y clave privada, la clave pública se comparte a través de un canal inseguro. Como se muestra en la Figura 3 Bob encripta el mensaje con la clave pública y descifra el mensaje cifrado utilizando la clave privada que solo él posee. A diferencia de la criptografía de clave simétrica la clave secreta no se comparte, sino que cada parte que se comunica calcula la clave secreta con su propia clave privada y pública. El resultado es que Alice y Bob calculan la misma clave secreta sin transmitirla. La característica principal de los criptosistemas asimétricos es el algoritmo de clave pública, algunos algoritmos populares de clave pública son el intercambio de claves Diffie-Hellman, el digital y el algoritmo RSA. (Gajbhiye, Karmakar, Sharma, & Sharma, 2017)

Figura 3. Cifrado Asimétrico.



Fuente: Autor

RSA:

RSA fue inventado por Ron Rivest, Adi Shamir y Leonard Adleman en 1978 y es uno de los principales sistemas de codificación de clave pública para el intercambio de claves, las firmas digitales o el cifrado de bloques de bases de datos y funciona utilizando una clave variable y un bloque de cifrado. La principal ventaja de RSA es que tiene mayor seguridad en comparación con otros algoritmos. De hecho, se encuentra entre los algoritmos más seguros. Sin embargo, está limitado por la baja velocidad de cifrado, la complejidad en la creación de claves y la susceptibilidad a los ataques debido a la baja velocidad. (Al-Shabi, 2018)

Marco teórico

Para lograr un entendimiento del concepto y funcionamiento de la criptografía cuántica debemos remitirnos a la ciencia que la hace posible que es la mecánica cuántica además de los enunciados que sustentan su funcionamiento, inicialmente es pertinente iniciar con una de las teorías de la física moderna que promovió el estudio del campo o posteriores postulaciones.

Universos paralelos (MWI Many-Worlds Interpretation)

En la teoría de los universos paralelos Everett y DeWitt propusieron la interpretación de muchos mundos o estados relativos como solución explícita al problema de cálculo en la teoría de la medición de la mecánica cuántica. En gran medida, la motivación de la teoría de los universos paralelos fue desde el principio el hecho de que podía escribirse en una formulación relativista en este sentido, parecía superior tanto a la mecánica cuántica estándar con colapso como a las teorías de variables ocultas.

Teniendo en cuenta que la teoría de los universos paralelos toma la mecánica cuántica unitaria sin colapso como una teoría completa, se requiere un cambio radical de interpretación del estado cuántico para entender lo que la teoría dice sobre el mundo.

Dado el estado cuántico puro del universo a cualquier subsistema del mismo se le puede asignar siempre un estado cuántico propio en general, este estado no será puro sino mixto. Sin embargo, dado el estado total del universo en un tiempo t, cualquier estado de un subsistema del

universo que tenga una amplitud no nula determina de forma única un estado relativo del resto del universo en el mismo tiempo t , esto es esencialmente toda la teoría.

En teoría de los universos paralelos, los sistemas físicos tienen asignados estados cuánticos definidos no de forma absoluta sino relativa al estado de otro sistema en la misma rama. Esto se toma para justificar la intuición de que cada rama en la superposición global puede considerarse que tiene algún tipo de existencia independiente, y que todas las ramas deben ser tratadas en igualdad de condiciones. (Hemmo & Pitowsky, 2017)

Mecánica cuántica

La mecánica cuántica es el conjunto de leyes fundamentales según las cuales todos los objetos se mueven. Para los objetos macroscópicos con los que interactuamos en la vida cotidiana las leyes de la mecánica cuántica se reducen a la mecánica clásica. Sin embargo, para la escala microscópica de los átomos las leyes de la mecánica cuántica dan lugar a un comportamiento muy diferente. Una de las diferencias fundamentales entre ambas es que en la mecánica cuántica un objeto puede estar simultáneamente en varios estados. En la mecánica clásica un objeto puede estar exclusivamente en el punto $r1$ o en el punto $r2$ pero no en ambos.

En la mecánica cuántica un objeto por ejemplo un electrón puede estar en cualquier combinación de los dos estados. Matemáticamente, esto se expresa considerando los dos estados de posición, denotados $|r1\rangle, |r2\rangle$, como vectores base en un espacio vectorial, y permitiendo que

el objeto se encuentre en un estado formado como una combinación lineal de los dos vectores base:

$$|\boldsymbol{\psi}\rangle := \boldsymbol{c1}|\boldsymbol{r1}\rangle + \boldsymbol{c2}|\boldsymbol{r1}\rangle$$

$c1|r1\rangle + c2|r1\rangle \neq c1|r1\rangle + c2|r2\rangle$ por lo tanto, el objeto no está simplemente en una posición obtenida al sumar los dos vectores de posición, sino que está entre algo en $r1$ y algo en $r2$.

Los dos vectores de posición son expresados en número infinito de posiciones en un espacio tridimensional como

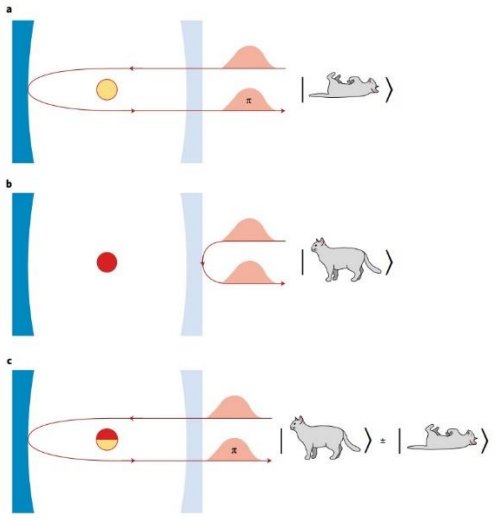
$$|\boldsymbol{\psi}\rangle := \int \boldsymbol{dr}\boldsymbol{\psi}(\boldsymbol{r})|\boldsymbol{r}$$

donde $\psi(r)$ es la función de onda y desempeña el papel de los coeficientes lineales $c1, c2$. Por esta razón, es mejor pensar en los electrones de las moléculas como nubes electrónicas (correspondientes a $\psi(r)$) en lugar de partículas puntuales. (Schütt, Chmiela, von Lilienfeld , Tkatchenko, & Tsuda , 2020)

Gato de Schrödinger

En 1935 Erwin Schrödinger propuso un experimento conocido como "el gato de Schrödinger" que ha generado muchas discusiones y debates en la comunidad cuántica a lo largo de las décadas. En este experimento la emisión de un átomo radiactivo, un fenómeno completamente cuántico desencadena una serie de reacciones que controla la vida o la muerte de un gato, dos acontecimientos distintos en el mundo clásico macroscópico. El trabajo condujo a la noción de estado del gato de Schrödinger, una superposición de distintos estados clásicos distintos, que permite la conexión entre los mundos cuántico y clásico. (Duan, 2019)

Figura 4. Creación determinista de estados del gato de Schrödinger.



Fuente: Duan, L. (2019). Creating Schrödinger-cat states. Nature Photonics . doi:10.1038/s41566-018-0340-z

a) En un experimento con un solo átomo entre dos espejos de diferente reflectividad, si el átomo se prepara en el estado de interacción "off", que no se acopla a la cavidad se produce un pulso en la cavidad que entrará en ella por el espejo de menor reflectividad y saldrá de ella con un desplazamiento de fase de π radianes, que corresponde a un gato de Schrödinger en el estado de muerte.

b) Si el átomo está en el estado de interacción "on", el pulso entrante será ahora fuera de resonancia y rebotando directamente por el espejo de la cavidad sin desplazamiento de fase, lo que corresponde a un gato de Schrödinger en el estado vivo.

c) Cuando el átomo se prepara en una superposición igual de los estados de interacción "on" y "off y luego se detecta en una base de superposición de estos dos estados, el pulso de luz reflejado será correspondientemente en una superposición igual de los estados clásicamente distintos - el estado de gato de Schrödinger.

Principio de incertidumbre de Heisenberg

Uno de los principios fundamentales de la mecánica cuántica es el principio de incertidumbre que impone una condición sobre el grado en que se pueden restringir las probabilidades de futuras mediciones de un sistema cuántico. La forma inicial de principio fue postulada por Werner Heisenberg en el año 1927.

Un enunciado preciso del principio de incertidumbre desde la perspectiva cuántica es la siguiente: Si se prepara un sistema en un estado cuántico particular $\hat{P}$ y posteriormente mide dos observables $\hat{A}$ y $\hat{B}$ del sistema utilizando preparaciones independientes entonces las estadísticas acumuladas de la medición mostrarán las desviaciones que satisfacen la formula:

$$\boldsymbol{\sigma A\, \sigma B} \geq \frac{\mathbf{1}}{\mathbf{2}\boldsymbol{i}} \left|\langle [\widehat{\boldsymbol{A}}, \widehat{\boldsymbol{B}}] \rangle\right|$$

- Una preparación $\hat{P}$ tiene extensiones intrínsecas en $\hat{A}$ y $\hat{B}$ que satisfacen la inecuación
- La estimación simultánea de los valores de $\hat{A}$ y $\hat{B}$ mostrará errores de estimación en la medición que satisfacen la inecuación.
- La estimación de $\hat{A}$ perturbará las estimaciones posteriores de $\hat{B}$ de manera que el error de estimación medido de $\hat{A}$ y la perturbación de $\hat{B}$ satisfacen la inecuación. (Dressel & Nori, 2016)

De manera más sencilla este principio afirma que si se mide una característica no se puede medir otra característica con precisión. Si por ejemplo, Aplicáramos el principio de incertidumbre en la medición de un humano podríamos medir la altura inicialmente, pero no podríamos medir su peso. Esta característica del principio de incertidumbre de Heisenberg solo es válida para el instante en que se trata de medir las características del sistema (perturbación).

En la mecánica cuántica este principio se aplica a los fotones, los fotones tienen una estructura ondulatoria y están polarizados o inclinados en cierta dirección. Al medir la polarización de los fotones todas las mediciones posteriores se ven afectadas por la elección de las medidas que hacen para la polarización. (Pawar & Dinesh G. , 2018) Es esta característica que toma la criptografía cuántica como soporte en la detección de posibles escuchas.

Teorema de No-clonación:

El teorema de no clonación afirma que toda transformación unitaria no puede clonar un estado cuántico arbitrario. Sin embargo, algunas transformaciones unitarias pueden clonar un subconjunto de estados cuánticos puros, lo que muestran que se pueden hacer solo clones imperfectos. (Epstein, 2019)

Se cree que las primeras versiones del teorema de la no-clonación se publicaron en 1982 en dos artículos simultáneos e independientes escritos por Wootters, Zurek, y por Dieks, argumentando que la clonación de estados cuánticos desconocidos es imposible: "La replicación perfecta y segura de cualquier fotón es imposible". (Ortigoso, 2018)

El teorema de No-clonación es una de las bases de la criptografía cuántica ya que permite que no sea posible para un usuario intermedio copiar el mensaje que se ha enviado. Con esto entonces, el emisor del mensaje cifrado puede estar seguro de que cada bit cuántico que envié solo sea transmitido una vez sin riego a ser clonado, una gran ventaja que ofrece la teoría

cuántica a comparación del método clásico en donde la información puede copiarse perfectamente.

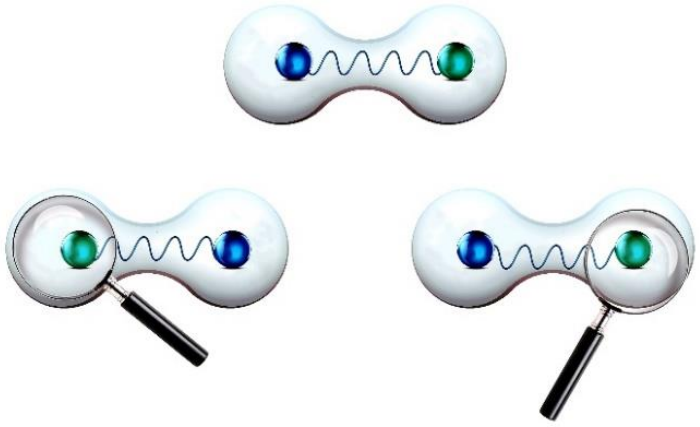
Entrelazamiento cuántico

El entrelazamiento cuántico es una propiedad que poseen los estados cuánticos que no tienen un modelo análogo, el entrelazamiento es el rasgo característico de la mecánica cuántica y el que refuerza el alejamiento de las líneas de pensamiento clásicas.

El entrelazamiento cuántico es el fenómeno físico que se produce cuando un par o grupo de partículas se genera al mismo tiempo, interactúan o comparten proximidad espacial de tal manera que el estado cuántico de cada partícula del par o grupo no puede describirse independientemente del estado de las demás, incluso cuando las partículas estén separadas por una gran distancia. (Wu, 2020)

Las mediciones de propiedades físicas como la posición, el momento, el espín y la polarización realizadas en partículas entrelazadas están perfectamente correlacionadas cómo se visualiza en la Figura 5.

Figura 5. Entrelazamiento Cuántico de dos partículas



Fuente: Autor

Los primeros trabajos mencionados sobre la comprensión del entrelazamiento acabaron siendo la base para el campo de la computación cuántica cuyo objetivo es explotar las extrañas propiedades de los estados cuánticos para tareas de procesamiento de información que no son posibles en el mundo clásico. El entrelazamiento cuántico es el combustible de una serie de protocolos cuánticos como la teletransportación, el cifrado denso y la distribución de claves. (Wang & Wilde, 2020)

Marco histórico de la criptografía Cuántica

De acuerdo con Quantum Bit Commitment and Coin Tossing Protocols que es considerada la primera publicación de estudio oficial de la criptografía cuántica, se expone que a finales de los años 60 el físico Stephen Wiesner tuvo la idea de que el principio de incertidumbre podía utilizarse para la criptografía. Para Wiesner sería posible utilizar un flujo de fotones polarizados para transmitir dos mensajes de forma que sólo uno de ellos fuera legible a elección del receptor. Esta noción, fue llamada "multiplexación".

A finales de la década de 1970, la invención de Wiesner revivió gracias al trabajo de Charles H. Bennett y Gilles Brassard, que dio lugar a un documento de CRYPTO '82 [BBBW82]. Posteriormente, Bennett y Brassard utilizaron los principios criptográficos cuánticos para implementar protocolos criptográficos básicos, como el intercambio de claves secretas y el coin tossing (Protocolo que usa de forma figurativa las probabilidades en el lanzamiento de una moneda) a este intercambio se le conoce como el protocolo BB84 (Brassard & Crbpeau, 1990) el cual será ampliado en el desarrollo del documento.

La preocupación latente que motiva la criptografía cuántica

Los algoritmos criptográficos que se utilizan actualmente en la práctica no proporcionan confidencialidad a largo plazo ya que se basan en la complejidad de cálculos matemáticos y problemas algorítmicos. Esto implica que los criptosistemas basados en la complejidad sólo permanecen seguros durante un determinado periodo de tiempo y este periodo de tiempo es difícil de predecir. (Buchmann, Braun, Demirel, & Geihs, 2017)

Un paso crucial en la evolución de la computación en general podría ser la implantación del ordenador cuántico, los problemas que se han considerado difíciles de resolver con los ordenadores clásicos no serán tan difíciles de resolver con el uso de un ordenador cuántico. Con lo cual se evidencia como problemática que la mayoría de los modelos criptográficos de clave pública actuales se basan en esos problemas, algo que los hace vulnerables cuando se enfrenten a un ordenador cuántico. (Giampouris, Short Review on Quantum Key Distribution Protocols, 2017)

Dada la potencia de los ordenadores cuánticos el siguiente paso para proteger las transmisiones de claves y la transmisión de información sensible es la criptografía cuántica. La criptografía cuántica es muy diferente de la criptografía clásica, porque en lugar de utilizar problemas matemáticos difíciles de resolver se basa en las leyes de la física como base para establecer la seguridad**.** (Oppliger, 2021)

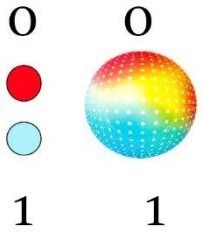
Computación cuántica

El funcionamiento del ordenador cuántico se basa en el principio de superposición de la mecánica cuántica, la paradoja del Gato de Schrödinger que se detalló previamente. El ordenador cuántico trabaja en computación paralela donde un número múltiple de procesos microscópicos se programan y seleccionan basándose en una probabilidad aleatoria. Por ejemplo, si consideramos un registro cuántico de n bits, existen $2n$ estados posibles simultáneamente, lo que se conoce como superposición. Cada función $f(x)$ puede ser representada como un circuito cuántico en el que todos los posibles valores de superposición de x se consideran como entrada y todos los posibles valores de superposición de $y = f(x)$ da como salida. (Mitra, Bappaditya, Bhattacharya, Pal, & Poray, 2017)

Qubits (bits Quánticos)

La criptografía cuántica requiere un canal que lleva un objeto físico llamado Bit Cuántico o alternativamente conocido como qubit, el qubit es la unidad básica de la computación cuántica. Hay dos tipos de canal cuántico, uno es el cable de fibra óptica y el otro es la atmósfera que nos rodea. Durante la transmisión de los qubits de un extremo a otro del canal de transmisión no hay cambio de ningún estado mecánico de los qubits. Los qubits se conectan mediante algunas puertas básicas de qubits. La mayor ventaja de los qubits sobre otros bits convencionales es que los qubits son un sistema bidimensional y pueden expresarse como una forma probabilística intermedia entre dos límites 0 y 1, mientras que los bits convencionales pueden expresarse como 0 o 1.

Figura 6. Un Bit la unidad mínima de la informática y un Qubit la unidad mínima de la computación cuántica.



Fuente: Autor

Principio de polarización de los fotones:

Los fotones son las partículas elementales y responsable de las manifestaciones cuánticas del fenómeno electromagnético de la luz, un fotón puede orientarse o polarizarse en direcciones específicas y, además un filtro de fotones con la polarización correcta sólo puede detectar un fotón polarizado o de lo contrario el fotón será destruido. Esta característica hace ideal para que la criptografía cuántica haga el envío de claves secretas en forma de fotones con sus respectivas polarizaciones: rectilínea para polarización vertical y horizontal, y la base diagonal para +45 y -45.

Recapitulando los principios expuestos, la criptografía cuántica utiliza los esquemas de la mecánica cuántica para realizar tareas criptográficas con el fin de proporcionar un sistema de seguridad infalible y libre de vulnerabilidades. Este enfoque es aplicable en varias áreas que

requieren verdaderos ordenadores cuánticos, que actualmente no son una realidad. Por lo tanto, las aplicaciones son actualmente de naturaleza teórica. Actualmente una de estas aplicaciones la distribución de claves cuánticas (QKD), si es realmente implementable, ya que no requiere ningún cálculo cuántico y puede ejecutarse a través de laser y la fibra óptica. (Nanda, Puthal, Mohanty, & Choppali, 2018)

Protocolo de distribución de claves cuánticas

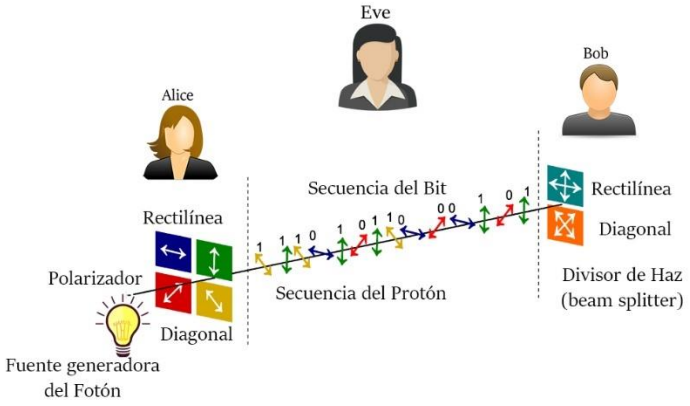
La distribución de claves cuánticas (QKD) utiliza el concepto de la mecánica cuántica para compartir las claves secretas de una parte (Alice) a otra (Bob). No puede impedir que un intruso espíe mientras que permite al usuario legítimo detectar al espía y a abortar la transmisión y desechar la clave si se detecta al intruso y se genera una nueva clave. (Kumar & Garhwal1, 2021)Los protocolos QKD se basan en el concepto del teorema de no clonación, el principio de incertidumbre de Heisenberg y el entrelazamiento cuántico los cuales ya fueron detallados previamente.

Protocolo BB84

BB84(Bennett y Brassard año 1984) fue el primer protocolo de criptografía cuántica que explicaba cómo utilizar el estado de polarización de los fotones para transmitir la información de la clave secreta a través de un canal de comunicación cuántica. Este protocolo se clasifica como QKD basado en la preparación y la medida.

El protocolo BB84 utiliza un solo fotón para transmitir y distribuir bits aleatorios de la clave secreta. El fotón único está polarizado en uno de los cuatro estados de polarización y seleccionado utilizando una de las dos bases conjugadas, la base rectilínea para polarización vertical y horizontal, y la base diagonal para +45 y -45 anti diagonal, El proceso de implementación se divide en: Intercambio Cuántico, Cifrado de clave, reconciliación de la información y amplificación de la privacidad. (Nurhadi & Rachmana Syambas, 2018)

Figura 7. Intercambio cuántico del protocolo BB84.



Fuente: Autor

En la Figura 7 se muestra que Alice transmite los fotones a través de un polarizador que les otorga aleatoriamente una de las cuatro polarizaciones y designaciones de bits posibles: Vertical (Un bit), Horizontal (Cero bit), 45 grados a la derecha (Un bit), o 45 grados a la izquierda (Cero bit).

Los fotones viajan hasta Bob, que utiliza dos divisores de haz o Beam splitter (horizontal/vertical y diagonales) para reconocer la polarización de cada fotón. Bob no sabe qué divisor de haz utilizar para cada fotón y tiene que adivinar cuál utilizar.

Una vez enviado el flujo de fotones, Bob le dice a Alice qué divisor de haz se utilizó para cada uno de los fotones en la secuencia en que se enviaron, y el emisor compara esa información

con la secuencia de polarizadores utilizada para enviar la clave. Los fotones que se leyeron con el divisor de haz equivocado se descartan, y la secuencia de bits resultante se convierte en la clave.

Si un espía (Eve), intenta escuchar la conversación tiene que leer cada fotón. A continuación, debe enviar nuevamente ese fotón a Bob. Al leer el fotón Eve altera el estado cuántico del fotón, lo que introduce errores en la clave cuántica. Esto alerta a Alice y a Bob de que alguien está escuchando y que la clave ha sido comprometida, por lo que abortan y descartan la clave. Alice tiene que enviar a Bob una nueva clave que no esté comprometida, y entonces Bob puede usar esa clave para leer el secreto.

Los fundamentos teóricos que soportan la criptografía cuántica hacen creer que se ha encontrado definitivamente el método infalible para proteger la información y para garantizar la privacidad en el envío de datos, es por esto que se hace necesario conocer cuáles son las verdades fortalezas y posibles amenazas para cuando esta técnica pase de la teoría a la realidad a gran escala, es preciso conocer los estudios recientes que pretenden estudiar su implementación, analizando los resultados que definen su situación actual y el futuro como el campo criptográfico más prometedor.

Esquema Temático

Criptográfica Cuántica Vs Post-Cuántica

El acelerado crecimiento en el poder de cálculo de las computadoras ha puesto en riesgo los criptosistemas que han sido usado para proteger nuestra información. Una computadora cuántica con una cantidad considerable de qubits podría romper la mayoría criptosistemas actualmente en uso, por lo tanto, existe una necesidad urgente de desarrollar algoritmos criptográficos que puedan resistir la ruptura de código clásica y cuántica. Estos son denominados criptosistemas post-cuánticos, se trata de combinar la criptografía post-cuántica con la criptografía cuántica, mientras que la criptografía cuántica se refiere al método de encriptación que utiliza los principios de la mecánica cuántica para reforzar la seguridad y detectar una escucha en las comunicaciones, la criptografía post-cuántica a su vez hace referencia a los algoritmos que pueden tener la capacidad de proteger la información en la era de la computación cuántica. (Bobrysheva & Zapechnikov, 2019)

La criptografía post-cuántica es un área de investigación muy amplia que surgió tras el descubrimiento de algoritmo de Shor que será ampliado más adelante, este algoritmo probo que los principales criptosistemas de protección de datos en uso quedarían completamente obsoletos con una computadora cuántica. Sin embargo, algunos criptosistemas, podrán resistir a los ataques de las computadoras clásicas y cuánticas.

La criptografía post-cuántica agrupa y estudia a los algoritmos que en teoría pueden seguir siendo seguros contra ataques de computadoras cuánticas, la seguridad de la mayoría de los algoritmos estándar actuales se basa en problemas matemáticos muy difíciles de realizar en una computadora clásica, esto significa que los protocolos de cifrado de clave pública actuales como la capa de conexión segura (SSL) y la capa de transporte seguro (TLS) son suficientes para resistir la mayoría de las tecnologías modernas, pero pronto la situación podría cambiar ya que una computadora cuántica que ejecute el algoritmo de Shor podría descifrar estos sistemas basados en matemáticas en muy poco tiempo.

Otro riesgo existente es que, personas o entidades malintencionadas podrían recopilar grandes cantidades de datos cifrados y descifrar estas claves mediante la computación cuántica en un fututo. Por lo tanto, incluso los datos que hoy son seguros podrán ser vulnerados mañana.

Los avances en criptografía post-cuántica han demostrado que cualquier algoritmo criptográfico basado en la complejidad matemática como la factorización y los logaritmos discretos se considera muy vulnerable desde la perspectiva de una computadora cuántica Esto también aplicaría a todos los protocolos de seguridad que utilizan este tipo de algoritmo criptográfico. Los sistemas criptográficos basados en el cifrado simétrico, como AES, se consideran más robustos por su método y que se podría aumentar el tamaño de la clave. Por otro lado, el cifrado asimétrico como un método de clave pública aún no está listo para la criptografía post-cuántica. (Grote, Ahrens, & Benavente-Peces, 2019)

El algoritmo de Shor

En 1994 el profesor de matemática aplicada Peter Shor introdujo un algoritmo capaz de encontrar los factores de cualquier número entero positivo N. Este algoritmo propuesto consta de dos partes:

- **Una Fase Clásica:** El algoritmo reduce en factores el problema de hallar el orden, esta parte se puede realizar en una computadora clásica.
- **Una fase Cuántica:** Un algoritmo cuántico para solucionar el problema de encontrar el periodo, El cual no ha sido llevado a la práctica pues es necesario un computador cuántico con una cantidad de Qubits necesarios por definir.

El algoritmo de Shor es una amenaza potencial para muchos criptosistemas ya que su seguridad se basa en la suposición de que calcular números grandes es difícil o en la dificultad de calcular fragmentariamente logaritmos discretos. En uno de los métodos criptográficos de mayor uso actualmente el RSA1, la clave pública es el producto $N = pq$ de dos números primos secretos p y q. La seguridad de RSA se basa básicamente en la dificultad de encontrar los factores p, q de N, por lo tanto, la información actual encriptada bajo estos métodos estaría en un riesgo inminente a la aparición de una computadora cuántica que permita implementar el algoritmo.

Algoritmo de Grover

En 1996 el científico informático indio-estadounidense Lov Kumar Grover introdujo un algoritmo que es la base de la mayoría de las aplicaciones activas definidas para la computación cuántica, consiste en la búsqueda en una serie no ordenada de datos con N componentes en un tiempo $O\ (N^{\frac{1}{2}})$.

El algoritmo de Grover al ser de naturaleza cuántica posee un carácter probabilístico, por lo que produce una respuesta que más se acerca con una determinada probabilidad de error, la cual puede llegar a ser tan baja como se desee por medio de una mayor cantidad de iteraciones las cuales pueden llegar a ser posibles con una adecuada cantidad de qubits. Por otro lado, si las operaciones de qubit son lo suficientemente pequeñas y rápidas el algoritmo de Grover se convierte en una amenaza para muchos de los criptosistemas que buscan seguridad, como las claves AES y SHA. Por ahora se recomienda simplemente cambiar a una clave AES de 256 bits o trasladarse a criptosistemas "teóricos de la información" como GMAC y Poly1305 los cuales se protegieron de las computadoras cuánticas sin ninguna modificación y sin presunto impacto. (Bernstein & Lange, 2017)

Tabla 1. Niveles de seguridad pre y post cuántica de diversos tipos de cifrado.

		Función	***Nivel de seguridad Pre Cuántica***	***Nivel de seguridad Post Cuántica***
Criptografía de clave simétrica (llave Secreta)	AES-128	Cifrado simétrico	128	64 (Con algoritmo de Grover)
	AES-256	Cifrado simétrico	256	128 (Con algoritmo de Grover)
	Salsa20	Cifrado simétrico	256	128 (Con algoritmo de Grover)
	GMAC	MAC (código de autenticación de mensaje)	128	128 (Sin presunto impacto)
	Poly1305	MAC (código de autenticación de mensaje)	128	128 (Sin presunto impacto)
	SHA-256	Función Hash	256	128 (Con algoritmo de Grover)
	SHA3-256	Función Hash	256	128 (Con algoritmo de Grover
Criptografía de clave asimétrica (llave Publica)	RSA-3072	Cifrado de firma	128	Descifrado (Con el algoritmo de Shor)
	RSA-3072	Cifrado de firma	128	Descifrado (Con el algoritmo de Shor)
	DH-3072	Intercambio de llaves	128	Descifrado (Con el algoritmo de Shor)
	DSA-3072	Intercambio de llaves	128	Descifrado (Con el algoritmo de Shor)
	256-bit ECDH	Intercambio de llaves	128	Descifrado (Con el algoritmo de Shor)
	256-bit ECDSA	Intercambio de llaves	128	Descifrado (Con el algoritmo de Shor)

Fuente: Bernstein, Daniel J y Tanja Lange. «Post-quantum cryptography.» Nature Vol 549 (2017)

En la Tabla 1 se muestra nivel de seguridad en bits con que cuentan diversos sistemas de cifrado en la actualidad (Pre Cuántica) y el nivel de seguridad en bits con el que contaran en la era post cuántica, además de su comportamiento frente a las dos amenazas más notorias los algoritmos de Shor y Grover, encontrando que la mayoría perderán como mínimo la mitad de su nivel de seguridad y una parte importante de estos será descifrado y por lo tanto inservible con la llegada de la computación cuántica.

Algoritmos Post cuánticos

El desarrollo de algoritmos Post cuánticos es un área de investigación en crecimiento que explora alternativas seguras a futuro de los criptosistemas de clave pública convencionales. La criptografía Post-Cuántica debe tener como mínimo una serie de condiciones para ser segura entre las cuales están:

- Debe de ser resistente tanto a los ataques de la computación cuántica, así como los ataques clásicos
- Debe de estar basado en la web, con funcionalidad en teléfonos inteligentes, en los sensores y en dispositivos que puedan poseer una potencia de cálculo más limitada, por lo tanto, de be de estar planteado en la era de la IOT.
- Debe de ser un método veloz que no ralentice la comunicación, un aumento en los bits del criptosistema afectará directamente la memoria, el procesamiento y la comunicación del dispositivo. Además, puede ralentizar la experiencia del usuario.

Algunos de los Algoritmos que podrían ser resistentes a un ataque de computador cuántico, según estudios preliminares, de forma corta son:

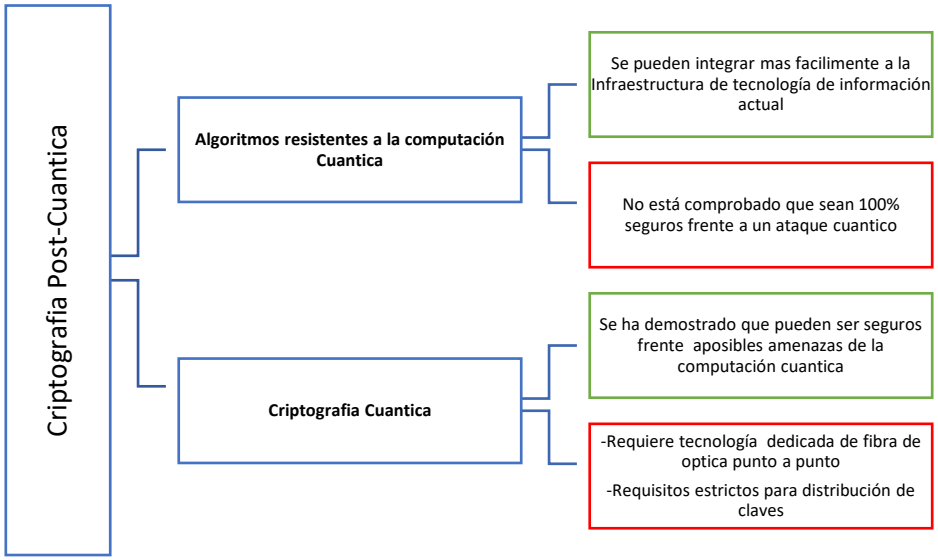
Basados en Código: Los criptosistemas basados en código, como McEliece, usan códigos de corrección de errores para generar claves públicas a partir de matrices privadas con errores insertados intencionalmente.

Basados en Red: El cifrado basado en la red se basa en la dificultad de resolver problemas matemáticos complejos, al igual que RSA. Por ejemplo, para un espacio vectorial de n dimensiones, es muy difícil encontrar el vector más cercano a un punto arbitrario de la red.

Basado en Hash: Introducido en la década de 1970, la seguridad y el rendimiento de los programas hash, como los propuestos por Ralph Merkle, Leslie Lamport y Whitfield Diffie, se han estudiado ampliamente. En la infraestructura criptográfica actual, las firmas digitales se utilizan comúnmente con fines de identificación y autenticación, como la verificación de la correspondencia. (Mailloux, Lewis II, Riggs, & Grimaila, 2016))

Suponiendo que el algoritmo post- cuántico propuesto sea lo suficientemente seguro contra los ataques de la futura computación cuántica, la oportunidad se evalúa principalmente por la longitud de clave requerida, la vida útil de la clave privada y la velocidad computacional, y además un aspecto a tener muy en cuenta es que el criptosistema pueda ser integrado en la infraestructura de la tecnología de la información existente, sin embargo, hasta el momento no se ha implementado con éxito.

Figura 8. Criptografía Post-cuántica



Fuente: Mailloux, L., Lewis II, C., Riggs, C., & Grimaila, M. (Sept.-Oct. de 2016)). Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals. IT Professional (Volume: 18, Issue: 5,. doi:10.1109/MITP.2016.77

En la figura 8 se enfrentan los algoritmos resistentes a la computación cuántica frente la criptografía cuántica mostrando sus ventajas y desventajas como modelo de criptografía post-cuántica.

Normalización y estandarización Post-Cuántica

La era post-cuántica cada vez se acerca a un hecho y esto ha llevado a que se inicien los trabajos de normalización y estandarización competente, actualmente se están adelantando actividades tales como el primer taller para discutir soluciones criptográficas de nueva clave pública y convocatorias abiertas para determinar los algoritmos aptos para la era post cuántica realizada por el Instituto Nacional de Estándares y Tecnología de EE. UU (NIST), esta entidad ha emitido una convocatoria de propuestas para un sistema criptográfico seguro contra computadoras cuánticas. Los algoritmos presentados serán evaluados y algunos de ellos serán estandarizados.

El NIST tiene un papel único que desempeñar en la normalización de la criptografía post-cuántica, como parte de su más importante responsabilidad del desarrollo de normas y directrices para la protección de los sistemas de información federales que no son de seguridad nacional. Muchas normas del NIST, como la Advanced Encryption (AES), se han desarrollado con una amplia participación del mundo académico y de la industria, y han sido ampliamente adoptadas, contribuyendo así a proteger la información y los sistemas de información de los Estados Unidos. La estandarización por parte del NIST de la criptografía post-cuántica probablemente proporcionará beneficios similares a futuro.

En el más reciente informe presentado por el NIST se concluye que no parece haber ningún algoritmo conocido actualmente que pueda servir en la era post-cuántica para lo que se usa exactamente hoy. Un reto que probablemente deberá superarse es que la mayoría de los

algoritmos que puedan ser resistentes a un ataque cuántico tienen tamaños de clave más grandes que los algoritmos que reemplazarán. Esto puede requerir cambios en varios protocolos de internet para intercambio de claves, Por lo tanto, ninguno de los experimentos ha demostrado garantizar la seguridad contra todos los ataques cuánticos, y es posible que se descubra un nuevo algoritmo cuántico para romper algunos de los patrones faltantes. (Chen, y otros, 2018)

La Organización Europea de Normalización ETSI también ha iniciado investigaciones en los criptosistemas post-cuánticos con una serie de publicaciones preliminares, en la más reciente denominada “Post-Quantum Cryptography: Current state and quantum mitigation” Se hace énfasis en que es importante tener reemplazos disponibles primero, cualquier comunicación cifrada interceptada hoy puede ser descifrada por un atacante tan pronto como obtenga acceso a una gran computadora cuántica, ya sea dentro de 5, 10 o 20 años, un ataque que puede ser conocido como un descifrado retrospectivo.

En la sección 2 del informe se presentan las 5 familias principales de algoritmos criptográficos propuestos como candidatos pata la era post-cuántica los cuales están basados en código, isogénicos, basados en hash, basados en red y basado en multidifusión. Estos algoritmos finalistas compiten para que el NIST los considere listos para la estandarización, mientras que se analizan algoritmos que el NIST considera prometedores pero que no están listos para aplicar.

En la seccion 6 están presentandos posibles mecanismos de reducción como la llamada implementación híbrida que usa una mezcla de esquemas pre y post-cuánticos y medición, ambos métodos tienen sus defectos, pero para los propietarios de sistemas que demandan

seguridad a largo plazo de los datos transmitidos, vale la pena considerarlos, por su parte los algoritmos presentados en esta seccion se ocupan de los criptosistemas de clave asimétrica (clave pública), el campo de la criptografía que se veria más afectado por la existencia de las computadoras cuánticas debido a su gran dependencia de la estructura matemática (factorización y problemas logarítmicos discretos). Por el contrario, la clave simétrica (clave compartida) presenta mayor resistencia a la nueva situación . En estos sistemas, la aplicación de claves más grandes se considera una técnica de mitigación fácil de aplicar y eficiente. (ETSI-Instituto Europeo de Normas de Telecomunicaciones, 2019)

Algunos informes se atreven a suponer que para 2028, las computadoras cuánticas podrán implementar el algoritmo de Shor a la escala necesaria para romper los algoritmos criptográficos actuales. También indican que la transición a la era post-cuantica podría ocurrir en 2026. Los anuncios del NIST de los algoritmos finalistas en la ronda del proceso de estándares de la criptografía post-cuántica sugiere que es probable que los estándares preliminares estén disponibles pronto después de que los enfoques tradicionales se vieran comprometidos por la computación cuántica. Esto a su vez, requiere la aplicación de una nueva clase de algoritmos contra los ataques de las computadoras cuánticas, Con el creciente interés en el desarrollo de las computadoras cuánticas universales, el control de los algoritmos post-cuánticos y la criptografía cuántica que pueden reemplazar los sistemas criptográficos modernos es esencial y crítico para la seguridad de todos los datos. (Pattnaik & Kumar, 2020)

Si bien se estan llevando acabo esta serie unificaciones, la estandarización lleva tiempo y pasarán muchos años antes de que la comunidad internacional implemente estos estándares. Sin

embargo las industrias y los gobiernos que necesitan incorporar estos criptosistemas post-cuanticos en sus productos, procesos e infraestructura deberian comenzar a abordar esta tecnologia lo antes posible, ya que cuanto más se espere mayor será el riesgo de no estar preparado para la era post cuántica. No todos los desarrollos en esta área se han hecho públicos, y es muy probable que la primera gran computadora cuántica completamente funcional no esté disponible públicamente y sea secreto de estado.

Efectividad Del Protocolo Bb84 Y Protocolos Alternos

El primer protocolo de distribución de llaves cuánticas fue propuesto por Bennett y Brassard en 1984 y se nombró protocolo BB84. En este protocolo las partes secretas de la clave se codifican en estados cuánticos, como la polarización de un fotón. La incertidumbre inherente de la medición de la polaridad mutua hace que este protocolo sea seguro en teoría.

Las verdaderas pruebas para la seguridad del protocolo BB84 han llegado con los escenarios de implementación con hardware que puede ser defectuoso. Para reducir esta vulnerabilidad del protocolo que puede ser causada por calibres imperfectos esta la alternativa de esquemas MDI(*Measurement Device Independent*). Por otro lado, BB84 tiene un sólido respaldo teórico de seguridad contra una amplia gama de ataques y demostraciones repartidas por todo el mundo, lo que lo convierte en el protocolo estándar para la implementación practica de la distribución de claves cuánticas.

Tabla 2. Taxonomía teórica del protocolo BB84

DIMENSIONES CORRESPONDIENTES AL PROTOCOLO BB84	
Dimensión	**Clasificación**
1) Numero de estados cuánticos	• Basado en Qubits
	• Basado en Qudits
2) Tipo de Protocolo BB84	• BB84 cuatro estados
	• BB84 tres estados
	• BB84 de alta dimensión
3) Métodos generales aplicados al protocolo BB84	• BB84 Puro
	• Tolerante a pérdidas
	• Referencia fuerte
	• Estados señuelo + tolerante a pérdidas
	• Estados señuelo
4)Elección de base	• Imparcial (probabilidades iguales)
	• Sesgado (Probabilidades Distintas)
5) Esquema de codificación	• Polarización
	• Fase
	• Time-Bin (Fase-Tiempo)
	• Frecuencia
	• Momento angular orbital
6) Consideraciones sobre el tamaño de la clave	• clave finita
	• Régimen Asintótico

Fuente: Zavala, Mathias y Beniamín Barán. «QKD BB84. A Taxonomy.» 2021 XLVII Latin American Computing Conference (CLEI). Cartago, Costa Rica: IEEE, 2021.

El protocolo BB84 fue clasificado en forma de taxonomía en un sentido general en el 2021, las dimensiones por las que se clasifico el protocolo desde un punto de vista teórico son: el número de estados cuánticos, tipo de implementación del protocolo BB84, si se aplican procedimientos generales al protocolo BB84, la elección de las bases, y programa de cifrado los cuales se visualizan en la Tabla 2. Por otro lado, también puede clasificarse según: esquema del sistema, números de canales, tipo de fibra, la fuente de fotones individuales y el tipo de detector. Esta nueva clasificación sirve como marco que puede ayudar a los investigadores a identificar

posibles oportunidades de mejora y aplicación, así como a determinar cómo se podría realizar un experimento sobre el tema. De esta manera, los desafíos abiertos que han sido poco estudiados pueden recibir la atención necesaria para que su desarrollo se lleve a cabo. (Zavala & Barán, 2021)

A la fecha existen muchas pruebas de seguridad basadas en las estrategias de ataque de Eve (*Eavesdropper/Espía*) las cuales serán discutidas más adelante, en teoría se asume que el hardware y la óptica utilizados para configurar el protocolo de distribución de llaves cuánticas son perfectos. Es posible que Eve conociera las debilidades de estos dispositivos y pudiera usarlos para descifrar la clave secreta. Este tipo de ataque de canal lateral es muy peligroso en cualquier sistema de distribución de claves porque Eve puede obtener información importante directamente de los dispositivos en uso. Una forma de evitar esto es usar un protocolo de intercambio independiente del dispositivo; sin embargo, no se usa mucho por ahora porque requiere más recursos adicionales que los protocolos de configuración y medición genéricos como BB84, al mismo tiempo que bajaría considerablemente la velocidad de generación de claves. (Biswas, Banerji, Chandravanshi, Kumar, & Singh, 2021)

La implementación de un canal cuántico real genera ruido debido a sus fuentes, canales y detectores imperfectos, estas pérdidas y errores benignos son indistinguibles de los causados por los competidores. Por esta razón, es prudente suponer que todas las pérdidas y errores son causados por un posible espía. El protocolo BB84 en teoría, es seguro siempre que el nivel de ruido esté por debajo de un cierto umbral.

El rendimiento de la ejecución de un sistema de distribución de claves cuánticas se puede medir mediante la tasa de bloqueo R, que indica el número de bloqueos seguros por pulso transmitido. Para el protocolo BB84, esta frecuencia clave no solo depende del ruido y la atenuación, sino también de la intensidad de la fuente láser μ. Se ha demostrado que es ventajoso variar aleatoriamente la cantidad de μ entre pulsos, lo que da como resultado una tasa inicial alcanzable más alta. (Attema , Bosman , & Niels , 2021)

Diferentes estudios en la universidad electrónica del norte de China han demostrado que el protocolo BB84 brinda diferentes niveles de seguridad para la protección de la información del sistema de distribución. Los resultados muestran que se puede mejorar la eficiencia de la distribución de claves cuánticas de múltiples nodos y posiblemente lidiando con una serie de eventos inesperados. El trabajo adicional incluye optimizar la seguridad del sistema QKD y el rendimiento de la generación de claves, analizar el impacto de un entorno de fuente de alimentación determinado en el rendimiento del sistema de distribución, la fase de diseño anti-interferencias y probar la extensión de conexión segura. (Ma, Yi, Guochen, & Zha, 2019)

El protocolo BB84 también ha sido probado en esquemas de firma digital post-cuántica como el propuesto por Labadzea en el cual se utiliza un esquema de firma único en lugar de un esquema de Merkl esto permite reducir la longitud de la firma, para firmar mensajes se generan claves de firma y verificación. Para transferir las claves de verificación se realiza mediante el protocolo BB84. Para ello, se cifra un bit aleatorio con la ayuda de qubits identificando a los oyentes y obteniendo una clave secreta; Para firmar el mensaje se genera un hash. El número mínimo de ceros se coloca antes de la representación binaria para obtener la longitud de la

representación. Como resultado se obtiene un esquema de firma digital basado en hash, que es seguro, ya que utiliza la versión clásica del esquema de un solo uso de y el protocolo BB84, el tamaño de la firma generado es mucho más pequeño que en el caso de un esquema Merkle. (ARQUIT CENTRICUS, 2021)

Protocolo B92

En 1992, Charles H. Bennett propuso un protocolo de distribución de claves cuánticas basado en dos estados no ortogonales llamados B92. El protocolo cuántico B92 es similar al protocolo BB84 pero solo usa dos estados cuánticos en lugar de cuatro.

El protocolo B92 se ha estudiado ampliamente en entornos asimétricos, donde se ha demostrado que tolera una interferencia de canal de hasta el 6,5 % y soporta hasta un 11 % de ruido en entornos asintótico. Se ha propuesto una variante extendida de B92, donde, además de dos estados de codificación no ortogonales usado en el B92, Alice y Bob usan otros dos estados no ortogonales y sin codificación para restringir la información de Eve de manera más estricta. En los estudios solo se han consideraremos qubits ideales y por lo tanto, no se han considerado el impacto de una pérdida potencial en la seguridad del protocolo. Con respecto a esta pérdida, el protocolo B92 original es muy vulnerable a los ataques de discriminación estatal explícitos, mientras que la versión extendida, protege contra tales ataques. (Amer & Krawec, 2020)

En el 2020 Walter O. Kraweca and Sam A. Markelon propusieron un nuevo protocolo de distribución de claves semicuánticas inspirado en el protocolo B92, este trabajo amplía el

protocolo con un segundo esquema de cifrado que permite responder mejor a los ataques de tipo USD (*unambiguous state discrimination*). Además, se ha mejorado la metodología de análisis de seguridad para incluir tipos de ataques más amplios como los ataques colectivos como trabajo futuro.

En este modelo propuesto una de las partes normalmente la A (Alice), es "totalmente cuántica" porque puede realizar todas las operaciones necesarias sobre el qubit. La segunda parte, B (Bob), es "clásica" porque solo puede interactuar con canales cuánticos de forma limitada y clásica. Más específicamente, estos protocolos utilizan canales cuánticos bidireccionales que permiten que la información cuántica se mueva. El usuario "clásico" B tiene dos opciones cuando se trata de obtener el estado cuántico de A. Son: Medir y reenviar, haciendo que los estados entrantes acepten mediciones del estado fundamental de los cálculos a A. y reflejar el estado de regreso a A sin cambiarlo. (Krawec & Markelon, 2020)

Protocolo E91 y otras propuestas

El E91 también conocido como protocolo EPR fue elaborado por Artur Ekert en 1991, el cual se sustentó en el entrelazamiento cuántico de pares de fotones. El esquema de transmisión está basado igualmente en el protocolo BB84; en este esquema Eve puede proporcionar estados separables a Alice y Bob, para que pueda obtener información sobre la llave.

En el 2018 en la universidad de Corea se realizó la implementación experimental de un protocolo de distribución de clave cuánticas de tipo "Plug & Play bidireccional", que utiliza

pulsos de doble acoplamiento en el nivel de fotón único para transmitir información crítica de Alice a Bob a través de un canal cuántico.

En este prototipo propuesto es de tipo cableado y es presentado como una implementación práctica de un protocolo QKD plug-and-play que utiliza espejos de Faraday para compensar automáticamente los cambios de polarización u oscilaciones de canal que ocurren debido a la distribución de fibra óptica de los interruptores cuánticos. Se utiliza un láser con una longitud de onda de 1550 nm y un fotodetector InGaAs de doble canal con 1 MHz para transmitir y recibir información crítica para el sistema de intercambio de claves cuánticas. La experimentación del prototipo demostró que una clave transmitida a través de un canal cuántico de 25 km tiene una tasa de bloqueo de 100 bits por segundo y un QBER (*Quantum bit error rate*) de alrededor del 3%. (Byungkyu, Jinyoung, Youngjin, & Jun, 2018)

La venganza de Eve: Ataques probados en la criptografía cuántica

La criptografía cuántica se presenta como un método ideal e infalible para proteger el intercambio de información de forma segura en teoría, en la práctica los qubits son fotones con distintas polarizaciones, donde es necesario utilizar fibra óptica, canales, láseres, polarizadores y con todas las fallas que pueden tener estos aparatos, se abren un montón de posibilidades para potenciales atacantes, además de posible desarrollo de un hardware especializado para espionaje en canales cuánticos, por ahora la construcción de un aparato completo de espionaje sigue siendo bastante difícil, podría ser posible con la tecnología actual o en un futuro próximo.

Uno de los posibles ataques a la criptografía cuántica es el "Ataque del Caballo de Troya", el cual ha sido probado de la siguiente forma: consiste en enviar potentes pulsos de luz por el canal que permiten a Eva averiguar cómo está configurado, Eva podría averiguar previamente los ejes que ha elegido Alice y medir todos los qubits sin provocar ni una detección por parte de Bob y Alice.

Se demostró la sostenibilidad experimental de un ataque de troyano aún casi invisible a un solo detector de fotones utilizado en los sistemas de distribución reales de claves cuánticas(QKD), A 192 nm (longitud de onda), se experimentó que la respuesta del ruido del detector a los pulsos de luz se reduce significativamente, y mediante modelos se demostró que el mismo ataque tendrá éxito. La naturaleza invisible del ataque es una amenaza que se puede realizar con la mayoría de los componentes disponibles comercialmente en el mercado. Por lo tanto, existe una necesidad urgente de incorporar contramedidas efectivas en los sistemas QKD

para contener estas amenazas. La más sencilla para proteger el sistema QKD de este ataque es filtrar adecuadamente la luz que entra en el sistema. Por ejemplo, añadir un filtro de paso estrecho en la entrada de Bob que obligará a Eve a utilizar la longitud de onda de la señal λ y reducirá su rendimiento de ataque al fallo original, siempre que se mantengan las propiedades de post pulsación del detector. Otra contramedida sería utilizar un protocolo QKD que no requiera que la configuración del receptor sea secreta, como el BB84 con estados señuelo. (Shihan , Carter, & Nitin, 2017)

Casi todos los sistemas de distribución de claves cuánticas necesitan calibrar el tiempo de activación de los detectores antes de iniciar la distribución de claves. El tiempo de activación de múltiples detectores difiere ligeramente debido a la deriva relacionada con la temperatura en los chips electrónicos con precisión limitada y a las discrepancias en las longitudes de las fibras que los conectan. Lo ideal es que las diferencias de los tiempos de activación de los múltiples detectores tomen valores constantes para minimizar el desajuste de la eficiencia del detector. Sin embargo, las longitudes de las fibras ópticas y los valores establecidos en los chips electrónicos varían con el tiempo y la temperatura, lo que hace casi imposible la inmovilización de las diferencias.

Un ataque cuántico de hombre en el medio en el proceso de calibración del canal cuántico antes del intercambio de claves en un sistema QKD con detectores de fotones individuales de modo cerrado de un solo fotón, puede ser posible si el canal cuántico está bajo el control de Eve en el proceso y los usuarios legítimos no comprueban la legitimidad de las señales de calibración, ya que estas señales no contienen información. Normalmente, estas señales de

calibración sólo contienen un pulso en cada ciclo en los sistemas QKD, si Eve induce algunas disparidades entre el tiempo de activación de diferentes detectores sustituyendo las señales de calibración por otras falsas que contengan más de un pulso en cada ciclo se realizaría un ataque exitoso, para prevenir esto es necesario un método de autocomprobación como instalan un láser especializado con un atenuador óptico al lado de Bob. Después del proceso de calibración, el sistema QKD ejecuta un auto prueba con el láser especializado para verificar. (Yang-Yang , Xiang-Dong , Ming, Wang , & Ma, 2018)

Un tipo de ataque que también puede afectar a la criptografía cuántica es el USD(*unambiguous state discrimination*) Para contrarrestar este ataque se utiliza un estado señuelo que se encuentra como combinación lineal de los estados de señal (estados de Gato de Schrödinger) Estos estados pueden considerarse estados coherentes pares. Así, se puede detectar a Eve simplemente controlando la tasa de detección de los estados señuelo.

El ataque USD es considerado asumiendo que Eve puede dividir el canal en dos, el canal Alice-Bob y el canal Alice-Eve-Bob sin pérdidas o con pérdidas menores donde ella realiza las mediciones de USD. El canal original Alice-Bob es el clásico-cuántico; En el experimento práctico se consideró el enfoque de los protocolos QKD con estados coherentes débiles codificados que desactivan el ataque de USD utilizando estados señuelo del gato de Schrödinger. (Gaidash, Kozubov, & Miroshnichen, 2018)

Recientemente ha aparecido un tipo de ataque denominado "Inyección SQL", que se encuentra entre los más peligrosos. La inyección de SQL es una vulnerabilidad que conduce a un

ataque de lenguaje de consulta estructurado (SQL) en el que un atacante puede explotar la sintaxis y las capacidades del propio SQL. Además, la flexibilidad de la base de datos y la funcionalidad del sistema operativo se ven afectadas por el código incrustado.

En la comunicación cuántica la base de datos está representada por el canal cuántico y el código del programa maligno está representado por un "fotón de programa maligno". En el entorno cuántico, el atacante utiliza las ventajas del entrelazamiento cuántico. En este ataque, Eve inyecta el canal cuántico mediante un "fotón de programa maligno" utilizando el motor de entrelazamiento, que hace que el "fotón malicioso" enredado con el de Alice. Por lo tanto, Eve puede ser capaz de revelar la base de Alice realizando una medición en el "fotón de programa maligno", lo que amenaza la seguridad de la comunicación cuántica y reduce la eficacia de los protocolos QKD. (Amellal, Meslouhi, & Hassouni, 2017)

El hecho de que la mayoría de los dispositivos electrónicos y ópticos que se usan en la criptografía cuántica como los láseres necesitan ventilación para eliminar el exceso de calor producido durante el funcionamiento, esto abre puertas a un nuevo riesgo no tan presente en la criptografía clásica: Los ataques con luz y ventilación, los cuales están relacionados con ataques electromagnéticos. La luz de los dispositivos puede dar información a los atacantes que no pueden llegar al sistema directamente. La mayoría de los dispositivos electrónicos utilizan diodos emisores de luz (LED) para señalar el funcionamiento normal y para un rápido diagnóstico visual.

Estas vías ópticas también abren una puerta trasera para los ataques de inyección óptica, en los que una señal óptica altera el funcionamiento normal del dispositivo. Las señales ópticas tienen niveles de potencia elativamente fuertes y la luz externa se acopla muy débilmente al interior de la fibra óptica y a los otros componentes ópticos. Un atacante necesitaría inyectar una señal con una gran potencia óptica antes de lograr algún efecto. En cambio, la mayoría de los sistemas cuánticos funcionan con unos pocos fotones y necesitan abordar explícitamente los ataques por inyección de luz. (Garcia, Sajeed, & Vadim, 2020)

El modelo de distribución de claves cuánticas tiene que refinarse hasta que capture todas las características relevantes de un sistema real y tiene que tolerar desviaciones en cada sistema diferente, el problema de la seguridad de la implementación está bien fundamentado. En un escenario criptográfico, es necesario repartir las suposiciones de seguridad de forma desigual entre los espías y los usuarios, de modo que la mayor parte de ellas recaiga en los usuarios y sólo la menor parte en el espía. La razón es que las suposiciones sobre un adversario no pueden verificarse, mientras que las del hardware del sistema QKD sí, al menos en principio. En el caso de QKD, en particular, no hay ninguna suposición sobre los recursos de Eve. Por lo tanto, si pudiéramos garantizar el comportamiento "correcto" de los dispositivos QKD, obtendríamos inmediatamente el máximo nivel de seguridad para el sistema. (ETSI-Instituto Europeo de Normas de Telecomunicaciones, 2019)

Tabla 3, Ataques a los que se enfrenta la Distribución de claves cuánticas

PROBLEMA DE SEGURIDAD	***DESCRIPCIÓN***	***CONTRAMEDIDAS***
Ataque de caballo de Troya	Eve prueba el equipo QKD con luz para obtener información sobre la configuración del dispositivo	Amplificación de privacidad (PA), aisladores, filtros
Emisión de fotones múltiples	Cuando se emite más de un fotón en un pulso, la información se codifica de manera redundante en múltiples fotones	(PA), caracterización, estados señuelo, SARG04 y otros protocolos
Codificación imperfecta	Los estados iniciales no se ajustan al protocolo.	(PA), caracterización
Correlación de fase entre pulsos de señal	Los pulsos no aleatorizados en fase filtran más información a Eve, los estados de señuelo fallan	fase de aleatorización, PA
Ataque de luz brillante	Eve manipula los detectores de fotones enviándoles luz brillante.	monitoreo activo, QKD independiente del dispositivo de medición (MDI-QKD)
Desajuste de eficiencia y ataque de cambio de tiempo	Eve puede controlar, al menos parcialmente, en qué detector hacer clic, obteniendo información sobre el bit codificado.	MDI-QKD, simetrización de detectores
Ataque de retroceso	Eve puede aprender qué detector hizo clic y, por lo tanto, conoce el bit	aisladores, MDI-QKD, detector de simetrización
Manipulación de la referencia del oscilador local	En la variable continua QKD (CV-QKD), el oscilador local (LO) puede ser manipulado por Eve si se envía por un canal de comunicaciones	Generar LO en el receptor. Recarga de fase, es decir, sincronizar solo la fase de LO

Fuente: ETSI-Instituto Europeo de Normas de Telecomunicaciones. Implementation Security of Quantum Cryptography. ETSI White Paper No. 27. CEDEX, France, 2019.

En la Tabla 3 se presenta una muestra representativa de los principales ataques contra el sistema de distribución de claves cuánticas con su descripción, así como las contramedidas para evitarlos.

El proceso de protección de la seguridad de la información no es perfecto es más como enfrentamiento sin fin en la que los posibles espías crean estrategias de ataque mientras se

desarrollan contramedidas de protección, este proceso a la vez es un ciclo que finalmente acaba mejorando la seguridad del sistema.

Criptografía Cuántica: sus usos y aplicaciones

La criptografía cuántica es una ciencia que se presenta en teoría como solución a diversas problemáticas y en la aplicación de diferentes ramas entre las cuales se encuentran: la encriptación de datos, firma digital, comunicación segura en el espacio, internet cuántico, intercambio y distribución de claves, red eléctrica avanzada, votación ultra segura, análisis y predicción del ADN y análisis de la estructura funcional del cerebro.

Votaciones limpias con criptografía cuántica

La primera instalación y puesta en práctica mundial de criptografía cuántica en la vida real fue en las elecciones federales en el estado de Ginebra Suiza el 21 de octubre de 2007, El reto para el gobierno de Ginebra era garantizar la máxima seguridad para proteger la autenticidad e integridad de los datos y al mismo tiempo gestionar el proceso con eficacia, también tenían que garantizar el axioma de un ciudadano, un voto.

Normalmente, las urnas selladas se llevan desde los colegios electorales a la estación central de recuento, donde se abren y se cuentan junto con los votos por correo ya entregados. El recuento se realiza manualmente según estrictas normas de procedimiento. Sin embargo, en el mundo moderno este principio se ha reinterpretado: la Comisión electoral lleva a cabo una estrecha vigilancia del recuento y de la introducción de datos, y la autenticidad e integridad de cualquier transferencia de datos posterior se garantiza entonces mediante el más alto nivel de encriptación.

La solución implantada en las elecciones consiste en un cifrado híbrido que utiliza el encriptado de capa 2 de última generación basada en el cifrado AES (Advanced Encryption Standard) de 256 bits combinada con la distribución de claves cuánticas (QKD). La solución Cerberis protege un enlace Gigabit Ethernet punto a punto utilizado para enviar la información de las papeletas de las elecciones desde la estación central de recuento de votos hasta el centro de datos del gobierno de Ginebra. El gobierno de Ginebra ha utilizado con éxito la solución Cerberis de IDQ en todas las elecciones federales desde 2007 como elemento clave para la integridad y la seguridad de las votaciones (ID QUANTIQUE SA, 2017)

En la figura 9 se observa un Cerberis que fue utilizado en el sistema de distribución de claves cuánticas en las elecciones nacionales suizas, el cual se diseñó para proteger la línea exclusiva que transmite las papeletas a la estación de recuento.

Figura 9. QKD Cerberis

Fuente: ID QUANTIQUE SA. (2017). Distribution, Securing Data Transfer for Elections-Ethernet Encryption with Quantum Key. Ginebra, Suiza.

Algunos expertos afirman que las comunidades militares y de inteligencia han utilizado habitualmente estos sistemas de distribución de claves cuánticas. Pero la elección de Ginebra es la primera vez que una organización gubernamental dice abiertamente que utiliza esta técnica.

Desde la implementación de la criptografía cuántica en las elecciones en Suiza se han desarrollado otros prototipos y técnicas para la aplicación de esta tecnología en diferentes sistemas de votaciones; En Odessa Ucrania se propuso un esquema de seguridad criptográfica asistido por ordenador destinado al recuento en unas elecciones. La idea principal es utilizar dos tecnologías de la criptografía cuántica: el compromiso cuántico de bits y el intercambio cuántico.

El esquema de intercambio cuántico del prototipo tiene tres participantes en el procedimiento de intercambio de secretos: Alice, que es la distribuidora, y los otros dos participantes que comparten directamente el secreto: Bob y Charley. Como regla se generaliza un número arbitrario de participantes en el procedimiento de compartir el secreto, al recibir los datos cada uno de los dos agentes ejecuta el intercambio del secreto de acuerdo con el esquema, a continuación, los agentes transfieren cada parte del secreto a cada miembro de la comisión. Para completar el procedimiento de recuento de votos todos los miembros de la comisión deben mostrar sus partes del secreto a los demás. De lo contrario, el recuento de votos no se realiza, de esta forma el esquema hace que sea no sea posible manipular los votos. (Karpinski, Gancarczyk, Klos-Witkowska, Limar, & Vasiliu, 2017)

La criptografía cuántica también ha sido probada en sistemas de votaciones en conjunto con otras tecnologías como el Blockchain cuántico satisfaciendo totalmente los requisitos de seguridad que debe de tener un protocolo de votación electrónico:

- El anonimato está garantizado porque la comunicación segura cuántica prohíbe que otros votantes conozcan la matriz completa.
- Otros votantes no pueden cambiar la papeleta de un votante debido al procedimiento de autenticación de la cadena de bloques cuántica. El propio votante no puede cambiar su papeleta presentada debido a la propiedad de compromiso cuántico.
- La no reutilización se violaría si un votante pudiera añadir con éxito dos papeletas diferentes a la cadena de bloques.

- Cada votante puede comprobar fácilmente si su papeleta enmascarada se ha subido con éxito al blockchain porque por su diseño es una base de datos transparente.
- Sólo los votantes autentificados pueden comunicarse con éxito con los mineros.
- La equidad se destruirá si alguien puede contar parcialmente las papeletas antes de la fase de recuento de votos.
- Los usuarios pueden contar las papeletas simplemente calculando la suma de las papeletas enmascaradas. (Xin , Wang, Piotr , & Sope, 2019)

Para una futura implementación de votaciones utilizando tecnologías basadas en criptografía cuántica se han diseñado reglas de voto cuántico denominadas QLV y QLN. En ambas de ellas las papeletas se lanzan en estados cuánticos y pueden realizarse físicamente con la tecnología actual y la dificultad de la realización física no crece con el aumento del número de votantes. Adicional a estas reglas de voto se planea estudiar el veto y la nominación cuánticos en la situación en la que algunas máquinas de votación cuántica sufran un comportamiento defectuoso. En estas situaciones se utilizarán cadenas de bloques cuánticos como plataforma para ejecutar el veto y la nominación cuántica. (Meiyun, y otros, 2022)

Criptografía cuántica en ciencias de la salud

Abordar la complejidad de ciertas necesidades de las ciencias de la salud está muy por encima de las capacidades que poseen las computadoras clásicas, sin embargo, la unión entre el futuro de las computadoras y la criptografía cuántica podría ser la solución para muchos problemas e interrogantes que aún se plantean en este sector; Como resultado en la actualidad existe una carrera entre industrias hacia aplicaciones cuánticas, en unos años es posible que la computación cuántica sea utilizada ampliamente para resolver problemas que antes se consideraban irresolubles.

En la industria de las ciencias de la vida se espera que la computación y la criptografía cuántica permita una serie de casos de uso innovadores, entre ellos se encuentran: Crear terapias de medicina de precisión vinculando genomas y resultados, afinar los resultados de los pacientes mediante la mejora de la eficiencia de fármacos de moléculas pequeñas y desarrollar nuevos productos biológicos basados en predicciones de plegado de proteínas. (Flöther, Moose, & Tavernelli , 2020)

Existe gran expectativa en el sector de salud con respecto a la criptografía cuántica como medida definitiva para garantizar la completa seguridad y privacidad de la información tanto de entidades prestadoras de servicios de salud, farmacéuticas y de pacientes.

Los datos son sagrados en la industria de las ciencias de la vida, tanto desde la perspectiva de la propiedad intelectual como para garantizar la privacidad de los datos de los

pacientes. La definición de la información personal identificable también está evolucionando junto con las nuevas tecnologías ómicas. El acceso protegido a los historiales médicos y el intercambio seguro de datos mediante de datos mediante encriptación cuántica podrían ser algunas de las primeras aplicaciones de la computación cuántica en las ciencias de la vida. Como la computación cuántica puede asegurar la clave y los datos indefinidamente con una encriptación inviolable, el Instituto Nacional de Estándares y Tecnología (NIST) ha comenzado a centrarse en proporcionar técnicas de encriptación basadas en la tecnología cuántica para aplicaciones de servicios médicos y farmacéuticos. (TATA Consultancy Services , 2021)

En la actualidad se han propuesto diferentes sistemas de protección para entidades de prestación de servicios de salud utilizando criptografía cuántica, como esta en la cual el administrador del hospital y el usuario utilizan la clave cuántica para almacenar y acceder a los datos. La clave cuántica se genera a partir de los qubits obtenidos del administrador y se utiliza tanto para el cifrado como para el descifrado, cuando el usuario envía una solicitud, el administrador detecta los qubits para el usuario y compara los qubits para identificar si el usuario es de confianza o no, esta clave utiliza los fotones aleatorios para representar un solo bit de datos. (Rubesh , Sakthida, & Thangapandiyan, 2018)

La criptografía cuántica también ha sido probada en ayudas medicas como imágenes, se ha propuesto que el personal sanitario pueda cifrar las imágenes médicas importantes mediante el esquema de cifrado cuántico, enviando las imágenes cifradas a la nube en donde el personal sanitario de otro lugar podrá consultarlas descifrando el contenido mediante el método propuesto. Este sistema de cifrado cuántico garantiza una alta confidencialidad para los pacientes

y los usuarios del sistema sanitario; Para el análisis del rendimiento del enfoque propuesto en un ordenador clásico, se emplearon varias simulaciones y métodos numéricos, como la correlación, la entropía de Shannon, análisis de sensibilidad y análisis de histogramas (Abd El-Latif, Abd-El-Atty, & Talha, 2017)

Avances en Infraestructura para la implementación de la criptografía cuántica

Para que sea posible la distribución de claves cuánticas es necesario que se realice una transmisión que debe ser confidencial y segura, actualmente la forma más común utiliza fibras ópticas la cual cuenta con una gran estabilidad, pero una considerable pérdida de canal. Otra tecnología utilizada es el espacio libre entre los satélites y las estaciones terrestres con la cual ha sido posible realizar transmisiones incluso a miles de kilómetros

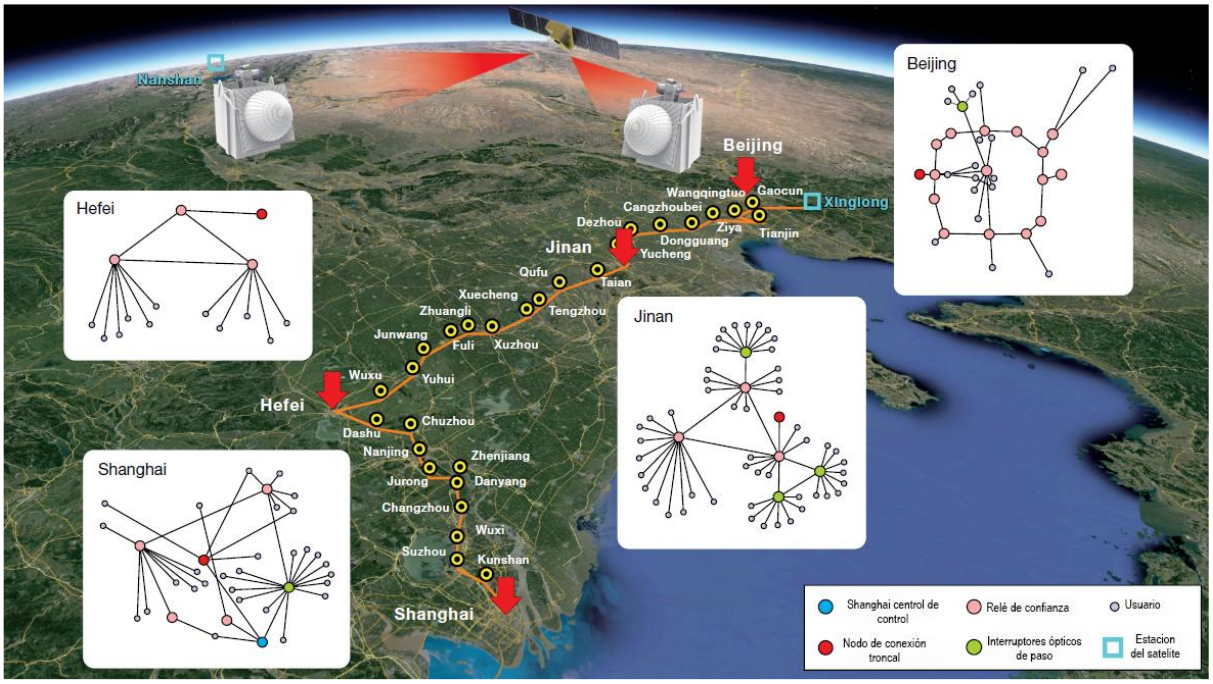
Los satélites se pueden utilizar para establecer comunicaciones cuánticas a distancias mucho más largas de las que se pueden lograr en la tierra y se pueden utilizar como parte de una arquitectura de red cuántica más grande para vincular redes cuánticas terrestres locales a largas distancias, la creación de redes de esta manera construye una red muy parecida a la Internet actual, por lo tanto, los satélites proporcionan un enfoque a corto plazo para construir una red cuántica global.

Recientemente en china se ha establecido la primera red de comunicación cuántica integrada del mundo, la cual combina más de 700 fibras ópticas en tierra con dos enlaces a

satélite la cual permite la distribución de claves cuánticas a una distancia total de 4600 kilómetros recorriendo el este del país desde Shanghái hasta Beijing.

La red cuántica presentada en China consiste en de cuatro QMAN (Redes cuánticas de área metropolitana), una red troncal a escala nacional y una red satélite-tierra-satélite, la topología en estrella es la estructura clave en las cuatro redes y los transmisores del dispositivo de medición y BB84 son esencialmente los mismos. Por lo tanto, los sistemas transmisores de la red de fibra actual pueden utilizarse también para realizar la red QKD independiente de las mediciones. Además, con la ampliación de la red troncal, se formará una topología más sofisticada que mejorará el tiempo-frecuencia, la gravedad cuántica e interferometría a gran escala para aplicaciones de metrología. Y también podrá ser posible realizar la computación distribuida y repetidores cuánticos en grandes áreas en un futuro próximo. (Chen, Zhang, Chen, & Wen-Qi , 2021)

Figura 10. Red integrada de comunicación cuántica espacio-tierra



Fuente: Chen, Y.-A., Zhang, Q., Chen, T.-Y., & Wen-Qi , C. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature(589), 214–219. doi:10.1038/s41586-020-03093-8

En la figura 10 se observa la red cuántica integrada de espacio-tierra. La red consta de cuatro QMAN (en Pekín, Jinan, Shangai y Heifei- flechas rojas), un enlace de fibra troncal de más de 2.000 km (línea naranja) y dos enlaces satélite-satélite que conectan Xinglong y Nanshan (cuadrados azules), separados por 600 km. Hay tres tipos de nodos en la red: los nodos de usuario (círculos morados). Un satélite cuántico está conectado a las estaciones terrestres de Xinglong y Nanshan; Xinglong también está conectado al QMAN de Pekín por fibra.

En el futuro, se tiene previsto ampliar la red en China y con sus socios internacionales de Austria, Italia, Rusia y Canadá. También pretenden desarrollar satélites QKD a pequeña escala y económicos, así como receptores en tierra y satélites de órbita terrestre media y alta para conseguir una QKD a tiempo completo y a 10.000 kilómetros.

Recientemente, la empresa británica Arqit ha anunciado sus planes para empezar a construir una red QKD mediante satélites. Los satélites se lanzarán en 2023 a través de Virgin Galactic. Esto marca una transición en la comunicación cuántica por satélite hacia el sector privado. (ARQUIT CENTRICUS, 2021)

Carrera comercial por la criptografía cuántica

Actualmente tres empresas son pioneras en el campo de la criptografía cuantica: BBN Technologies de Boston (EE.UU.), MagiQ de Nueva York (EE.UU.) e ID Quantique de Ginebra (Suiza). Todas ellas han probado sistemas de criptografía cuántica con clientes como bancos y otras instituciones financieras, sin embargo, existen muchas otras entidades incursionando en el negocio con diferentes aplicaciones de encriptación comercial.

Qrypt : Es un startup con sede en Nueva York que tiene su propia solución criptográfica. La empresa afirma que su solución de cifrado es capaz de proteger a las empresas y la información privada en el presente y en el futuro.

"El cifrado de seguridad cuántica de Qrypt ofrece a las personas las herramientas que necesitan para asegurar de forma inmutable sus datos y su derecho a la privacidad. A través de grandes alianzas y un equipo inigualable, hemos construido métodos y aplicaciones de cifrado patentados que permiten a todos reclamar su derecho a la autonomía digital". www.qrypt.com

Single Quantum: La empresa con sede en los Países Bajos ofrece soluciones para la detección de fotones en el extremo del receptor con una alta precisión.

"Fundado en 2012, Single Quantum surgió como auténticos pioneros de la tecnología de detección de fotones individuales: fuimos de los primeros en fabricar y comercializar detectores de fotones individuales de nanohilos superconductores. Desde entonces, nuestro sistema multicanal de detección de fotones Single Quantum Eos ha sido elegido por más de 100 laboratorios académicos e industriales de todo el mundo para realizar complejas mediciones ópticas, Single Quantum desarrollará los sensores de luz más rápidos y sensibles del mundo, limitados únicamente por las leyes de la física". https://singlequantum.com/

Post-Quantum: La empresa proporciona soluciones de protección contra la amenaza cuántica y ofrece soluciones comerciales y gubernamentales. Post-Quantum dispone de soluciones como algoritmos de cifrado y soluciones de ciberseguridad.

"Hoy en día hemos construido un conjunto de productos utilizables y seguros desde el punto de vista cuántico que abarcan el cifrado, la transmisión y la identidad. Estos productos protegen los datos desde el momento en que se crean, mientras se transmiten y frente a riesgos

adyacentes como los ataques a la identidad cuántica. Nuestra tecnología se combina para ayudar a las organizaciones a conseguir un "ecosistema seguro desde el punto de vista cuántico" que proteja cada punto de vulnerabilidad". www.post-quantum.com

Crypto Quantique: Los productos, plataformas y servicios tecnológicos de Crypto Quantique proporcionan seguridad de extremo a extremo en todas las redes de IoT con ciberseguridad impulsada por la tecnología cuántica. La empresa afirma tener una seguridad impulsada por la cuántica en un chip que puede generar múltiples claves criptográficas que no necesitan ser almacenadas y utilizadas independientemente en múltiples aplicaciones.

"Crypto Quantique es un pionero de la seguridad del IoT. Hemos combinado la criptografía y la física cuántica para desarrollar productos de seguridad que impulsan la seguridad de extremo a extremo y desbloquean la escalabilidad de las redes de IoT". www.cryptoquantique.com/

ID Quantique: Fundada en 2001 como un spin-off del Grupo de Física Aplicada de la Universidad de Ginebra, ID Quantique es el líder mundial en soluciones criptográficas de seguridad cuántica, diseñadas para proteger los datos del futuro. La empresa ofrece cifrado de redes seguro desde el punto de vista cuántico, generación de claves cuánticas seguras y soluciones de distribución de claves cuánticas, así como servicios al sector financiero, las empresas y las organizaciones gubernamentales de todo el mundo.

“Los productos de IDQ son utilizados por clientes gubernamentales, empresariales y académicos en más de 60 países y en todos los continentes. Como empresa privada suiza centrada en el crecimiento sostenible, IDQ está orgullosa de su independencia y neutralidad, y cree en el establecimiento de relaciones a largo plazo y de confianza con sus clientes y socios”. www.idquantique.com/

El naciente interés en la criptografía cuántica la convierte en un campo de batalla comercial en la cual una cantidad cada vez más elevada de empresas se pelean por la supremacía no solo gubernamental y militar si no por una implementación de tecnologías y productos al público común a futuro cercano.

Resultados esperados

Terminada la realización del proyecto de grado se espera la generación de una monografía de recopilación fruto del estudio de la revisión sistemática y levantamiento documental exhaustivo sobre la criptografía cuántica, adicional un documento tipo *paper* que pueda ser publicable acerca del estado del arte actual de la criptografía cuántica que incluya sus usos y aplicaciones actuales.

Divulgación

Yo John Harrison Cardona Cardona autorizo a la Universidad Nacional abierta y a Distancia - UNAD, a la distribución, comunicación, y puesta a disposición electrónica de la presente monografía, para que pueda ser consultada de forma libre por quien lo desee.

Conclusiones

En el presente proyecto de monografía se desarrolló una revisión bibliográfica de estudios científicos relevantes en la ciencia de la criptografía cuántica, la cual cumple a cabalidad con los objetivos planteados.

Se clasificaron 63 referencias bibliográficas obtenidas de bases de datos científicas que dieron como resultado el desarrollo de un estado del arte sobre la criptografía cuántica. Adicionalmente enmarcado en el desarrollo de la presente monografía se puede concluir lo siguiente:

La criptografía cuántica tendrá uso como medida paralela a la criptografía post cuántica para codificar la transmisión de información de forma segura durante la era de computación cuántica salvaguardando información sensible que podrá ser vulnerable a este tipo de computadoras en un futuro cercano.

La criptografía cuántica ha demostrado resistencia a los diferentes ataques informáticos a los que se ha puesto a prueba y ha demostrado una capacidad de mejora continua a vulnerabilidades encontradas lo que la convierte en un método de encriptación seguro y confiable para su implementación.

La distribución de claves cuánticas (QKD) es la única tecnología perteneciente a la criptografía cuántica que está siendo comercializada a la fecha ya que no requiere el uso de un

computador cuántico y puede ser implementada con tecnología que ya se comercializa sin restricción, pero aun así sin ser de aplicación general.

La Normalización y estandarización de tecnologías de computación y criptografía post cuántica realizadas por la ANSI (Instituto Nacional Estadounidense de Estándares) y la ENISA (Agencia Europea de Seguridad de las Redes y de la Información) dan a entender que la era de la computación cuántica esta próxima a ocurrir y con una alta posibilidad de que sea en la presente década.

Muchos países han realizado estudios, pruebas e implementaciones basados en criptografía cuántica sin embargo es China el país que está a la vanguardia y lleva un paso adelante con respecto a avances e implementaciones reales, además de promover la investigación y e desarrollo contante en esta área a través de los programas de la Fundación Nacional de Ciencias Naturales de China.

Muchos avances actuales de la criptografía cuántica aún son desconocidos para el público común por ser parte de programas gubernamentales y militares y no se descarta que esta ciencia este siendo investigada como parte de una carrera armamentista entre países que están rivalizados como medio de ataque y/o protección de la información confidencial de un país.

Bibliografía

Abd El-Latif, A., Abd-El-Atty, B., & Talha, M. (2017). Robust Encryption of Quantum Medical Images. (IEEE, Ed.) *IEEE Access , 6*, 1073 - 1081. doi:10.1109/ACCESS.2017.2777869

Aggarwal, S., Houshmand, S., & Weir, M. (2018). *New Technologies in Password Cracking Techniques.* Santa Clara University. doi:10.1007/978-3-319-75307-2_11

Al-Shabi, M. A. (2018). A Survey on Symmetric and Asymmetric Cryptography. *International Journal of Scientific and Research Publications, 9*(3). doi:10.29322/

Amellal, H., Meslouhi, A., & Hassouni, Y. (2017). SQL injection principle against BB84 protocol. *International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS).* Rabat, Morocco: IEEE. doi:10.1109/WITS.2017.7934654

Amer, O., & Krawec, W. O. (2020). Finite Key Analysis of the Extended B92 Protocol. *2020 IEEE International Symposium on Information Theory (ISIT).* Los Angeles, USA: IEEE. doi:10.1109/ISIT44484.2020.9174018

ARQUIT CENTRICUS. (21 de 05 de 2021). *Centricus Acquisition Corp. To Combine With.* Obtenido de ARQUIT: https://dcswhimef-res.cloudinary.com/image/upload/v1620817479/WhitePapers/CENTRICUS_ACQUISITION_CORP._TO_COMBINE_WITH_ARQIT_LIMITED_A_LEADER_IN_QUANTUM_ENCRYPTION_TECHNOLOGY_.pdf

Attema , T., Bosman , J., & Niels , M. (2021). Optimizing the decoy-state BB84 QKD protocol parameters. *Quantum Information Processing, 20*. doi:10.1007/s11128-021-03078-0

Bernstein, D., & Lange, T. (14 de September de 2017). Post-quantum cryptography. *Nature Vol 549*. doi:10.1038/nature23461

Biswas, A., Banerji, A., Chandravanshi, P., Kumar, R., & Singh, R. (September de 2021). Experimental Side Channel Analysis of BB84 QKD Source. *IEEE Journal of Quantum Electronics, Volume: 57*(Issue: 6). doi:10.1109/JQE.2021.3111332

Bobrysheva, J., & Zapechnikov, S. (2019). Post-Quantum Security of Communication and New Perspectives. *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus).* Moscow, Russia: IEEE. doi:10.1109/EIConRus.2019.8657136

Brassard, G., & Crbpeau, C. (1990). Quantum Bit Commitment. *Lecture Notes in Computer Science · January.*

Buchmann, J., Braun, J., Demirel, D., & Geihs, M. (2017). *Quantum Cryptography: a view from classical cryptography.* IopScience.

Byungkyu, A., Jinyoung, H., Youngjin, S., & Jun, H. (2018). Implementation of Plug & Play Quantum Key Distribution Protocol. *Tenth International Conference on Ubiquitous and Future Networks (ICUFN).* Prague, Czech Republic: IEEE. doi:10.1109/ICUFN.2018.8436633

Chen, L., Jordan, S., Yi-Kai, L., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2018). *Report on Post-Quantum Cryptography.* National Institute of Standards and Technology, Gaithersburg, MD. doi:10.6028/NIST.IR.8105

Chen, Y.-A., Zhang, Q., Chen, T.-Y., & Wen-Qi , C. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*(589), 214–219. doi:10.1038/s41586-020-03093-8

Cortez, D. M., Sison, A., & Medina, R. (2020). Cryptanalysis of the Modified SHA256. *Conference on Big Data and Artificial Intelligence.* doi:10.1145/3409501.3409513

Dressel, J., & Nori, F. (2016). *Certainty in Heisenberg's uncertainty principle: Revisiting definitions for estimation.* American Physical Society. doi:10.1103/physreva.89.022106

Duan, L. (2019). Creating Schrödinger-cat states. *Nature Photonics* . doi:10.1038/s41566-018-0340-z

Durniak, A. (2000). *Welcome to IEEE Xplore. IEEE Power Engineering Review.* doi:10.1109/39.883281

ENISA. (2021). *Post-Quantum Cryptography: Current state and quantum mitigation.* ENISA. Attiki, Athens: ENISA. doi:10.2824/92307

Epstein, S. (Septeimber de 2019). Algorithmic No-Cloning Theorem. *IEEE TRANSACTIONS ON INFORMATION THEORY, 65*(9). doi:10.1109/tit.2019.2910562

ETSI-Instituto Europeo de Normas de Telecomunicaciones. (2019). *Implementation Security of Quantum Cryptography.* ETSI White Paper No. 27, CEDEX, France. Obtenido de https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf

Flöther, F., Moose, C., & Tavernelli , I. (2020). *Exploring quantum computing use cases for life sciences.* IBM . Institute for Bussines Value IBM. Obtenido de https://www.ibm.com/downloads/cas/EVBKAZGJ

Gaidash, A., Kozubov, A., & Miroshnichen, G. (2018). Overcoming unambiguous state discrimination attack with the help of Schrödinger Cat decoy states. *Optica , X*. doi:https://arxiv.org/abs/1808.08145

Gajbhiye, S., Karmakar, S., Sharma, M., & Sharma, S. (2017). Paradigm Shift from Classical Cryptography to. *Proceedings of the International Conference on Intelligent Sustainable Systems.* Palladam, India. doi:10.1109/ISS1.2017.8389231

Garcia, J., Sajeed, S., & Vadim, M. (2020). Attacking quantum key distribution by light. *PLoS ONE, 15*. doi:10.1371/journal.pone.0236630

Giampouris, D. (2017). *Short Review on Quantum Key Distribution.* PubliMed. doi:10.1007/978-3-319-56246-9_12

Giampouris, D. (2017). Short Review on Quantum Key Distribution Protocols. *Advances in Experimental Medicine and Biology, 988*, 149–157. Obtenido de https://link.springer.com/chapter/10.1007/978-3-319-56246-9_12

Grote, O., Ahrens, A., & Benavente-Peces, C. (2019). A Review of Post-quantum Cryptography and Crypto-agility Strategies. Wismar, Germany: IEEE. doi:10.1109/IIPHDW.2019.8755433

Guzman, F. H. (2018). *El viaje al centro de la tierra.* Bacelona, España: Person Vue.

Hemmo, M., & Pitowsky, I. (2017). Quantum probability and many worlds. *Studies in History and Philosophy of Modern Physics, 38*, 333-350. doi:10.1016/j.shpsb.2006.04.005

ID QUANTIQUE SA. (2017). *Distribution, Securing Data Transfer for Elections-Ethernet Encryption with Quantum Key.* Ginebra, Suiza. Obtenido de https://marketing.idquantique.com/acton/attachment/11868/f-020f/1/-/-/-/-/Geneva%20Govt_%20DCI%20QKD%20Use%20Case.pdf

Kahate, A. (2018). *Cryptography and Network Security.* McGraw-Hill Education Pvt. Ltd.

Karpinski, M., Gancarczyk, T., Klos-Witkowska, A., Limar, I., & Vasiliu, Y. (2017). Security Amplification of the Computer-Aided. *9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS).* Bucharest, Romania: IEEE. doi:10.1109/IDAACS.2017.8095056

Krawec, W., & Markelon, S. (2020). A Semi-Quantum Extended B92 Protocol and its Analysis. *Quantum Information Science, Sensing, and Computation XII.* Connecticut, USA: SPIE. doi:10.1117/12.2558200

Kumar, A., & Garhwal1, S. (2021). State-of-the-Art Survey of Quantum Cryptography. *Archives of Computational Methods in Engineering*. doi:10.1007/s11831-021-09561-2

Labadzea, G., Iavichb, ,., & Iashvilib, G. (2021). Proceedings of the 26th International Conference on Information Society and University Studies. Kaunas, Lithuania: Information Society and University Studies. Obtenido de http://ceur-ws.org/Vol-2915/paper5.pdf

Ma, J. (2020). Basic application of mathematics in cryptography. *International Conference on Modem Education and Information Management.* Santa Barbara-Usa. doi:10.1109/ICMEIM51375.2020.00192

Ma, Y., Yi, L., Guochen, W., & Zha, X. (2019). Performance optimization of decoy-state BB84- and MDI- QKD protocol and. (ScienceDirect, Ed.) *Optical Fiber Technology, 52*. doi:10.1016/j.yofte.2019.101944

Mailloux, L., Lewis II, C., Riggs, C., & Grimaila, M. (Sept.-Oct. de 2016)). Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals. *IT Professional (Volume: 18, Issue: 5,*. doi:10.1109/MITP.2016.77

Meiyun, G., Kulicki, P., Sopek, M., Qiu, D., He, F., & Xin, S. (2022). Distributed Quantum Vote Based on Quantum Logical. *Project: Quantum-enhanced Logic-based Blockchain.* Lublin-Poland.

Mendez, E. C. (Marzo de 2016). *El tiempo*. Obtenido de Etica en los sectores profesionales: http://www.ccnaexam.net/ccna-2-v7-srwe-practice-pt-skills-assessment-part-1/7478

Mitra, S., Bappaditya, J., Bhattacharya, S., Pal, P., & Poray, J. (Nov de 2017). Quantum Cryptography: Overview,Security Issues and Future Challenges. *International Conference on Opto-Electronics and Applied Optics (Optronix).* doi:10.1109/OPTRONIX.2017.8350006

Moizuddin, M., Winston, D., & Qayyum, M. (2017). Comprehensive Survey: Quantum Cryptography. *2017 2nd International Conference on Anti-Cyber Crimes (ICACC).* doi:10.1109/Anti-Cybercrime.2017.7905271

Mok1, C. J., & Chai , W. (2019). An Intelligence Brute Force Attack on RSA Cryptosystem. *Communications in Computational and Applied Mathematics, , 1*(1), 1-7.

Montoya, N. P. (2005). ¿Qué es el estado del arte? En *Cienc Tecnol Salud Vis Ocul.* Bogotá: Universidad de La Salle. doi:https://doi.org/10.19052/sv.1666

Nanda, A., Puthal, D., Mohanty, S., & Choppali, U. (Nov de 2018). A Computing Perspective on Quantum Cryptography. *IEEE Consumer Electronics Magazine*, 59.

Nurhadi, A. I., & Rachmana Syambas, N. (2018). Quantum Key Distribution (QKD) Protocols: A. *4th International Conference on Wireless and Telematics (ICWT).* doi:10.1109/icwt.2018.8527822

Oppliger, R. (2021). *Cryptography 101 From Theory to Practice.* Artech House.

Ortigoso, J. (March de 2018). Twelve years before the quantum no-cloning theorem. *Am. J. Phys, 86*(3). doi:10.1119/1.5021356

Pattnaik, P., & Kumar, M. (2020). Post Quantum Cryptography(PQC) - An overview. *2020 IEEE High Performance Extreme Computing Conference (HPEC).* Waltham, MA, USA: IEEE. doi:10.1109/HPEC43674.2020.9286147

Pawar, H. R., & Dinesh G. , H. (2018). Classical and Quantum Cryptography for Image Encryption & Decryption. *International Conference on Research in Intelligent and Computing in Engineering (RICE).* Badnera-India. doi:10.1109/RICE.2018.8509035

Rubesh , M., Sakthida, K., & Thangapandiyan, M. (2018). Quantum Key Distribution and Cryptography. *International Conference on Communication and Signal Processing (ICCSP).* Chennai, India: IEEE. doi:10.1109/ICCSP.2018.8524298

Schütt, K. T., Chmiela, S., von Lilienfeld , A., Tkatchenko, A., & Tsuda , K. (2020). Quantum Mechanics. En *Machine Learning Meets Quantum Physics* (págs. 15-17). Berlin: Springer. doi:10.1007/978-3-030-40245-7

Shihan , S., Carter, M., & Nitin, J. (2017). Invisible Trojan-horse attack. *Scientific Reports , 7*. doi:https://doi.org/10.1038/s41598-017-08279-

Stallings, W. (2017). *Cryptography And Network Security Principles And Practice* (Vol. Seventh Edition). Essex: Pearson.

TATA Consultancy Services . (2021). *Life sciences research and and quantum computing: The future is almost here.* Bombay, India. Obtenido de https://www.tcs.com/content/dam/tcs/pdf/Industries/life-sciences-and-healthcare/insights/quantum-computing-use-life-sciences-future-ready.pdf

Wang, X., & Wilde, M. (2020). Cost of Quantum Entanglement Simplified. *PHYSICAL REVIEW LETTERS, 125*.

Whittemore, R., & Chao, A. (2014). Methods for knowledge synthesis: an overview. En *Methods for knowledge synthesis: an overview.* doi:10.1016/j.hrtlng.2014.05.014

Wu, E. T. (Jun de 2020). Photon Polarization and Entanglement Interpreted by Yangton. *Journal Of Applied Physics, 12*(3).

Xin , S., Wang, Q., Piotr , K., & Sope, M. (2019). A Simple Voting Protocol on Quantum Blockchain. En Springer (Ed.), *International Journal of Theoretical Physics*, (págs. 275-281). doi:https://doi.org/10.1007/s10773-018-3929-6

Yang-Yang , F., Xiang-Dong , M., Ming, G., Wang , H., & Ma, Z. (2018). Quantum man-in-the-middle attack on the calibration process of quantum key distribution. (Nature, Ed.) *Scientific Reports, 8*. doi:10.1038/s41598-018-22700-3

Zavala, M., & Barán, B. (2021). QKD BB84. A Taxonomy. *2021 XLVII Latin American Computing Conference (CLEI).* Cartago, Costa Rica: IEEE. doi:10.1109/CLEI53233.2021.9639932

Anexos

anexo 1. RAE

RESUMEN ANALÍTICO ESPECIALIZADO RAE	
1. Título.	Revisión sistemática del estado del arte de la criptográfica cuántica, sus usos y aplicaciones
2. Autor:	CARDONA, Cardona, JOHN Harrison
3. Edición	N/A
4. Fecha	10/05/2022
5. Palabras Claves,	Criptografía Cuántica, Distribución de Claves Cuánticas, Protocolo BB84, Cúbit
6. Descripción.	Monografía como trabajo de grado para optar al título de Ingeniero de Sistemas en la Universidad UNAD que tiene como temática central la criptografía cuántica. En la presente monografía se realiza un levantamiento y revisión de la literatura científica relevante que ha estudiado la criptografía cuántica en los últimos 5 años, consolidando su descripción detallada, leyes que la fundamentan, usos, propiedades, nivel de seguridad e integridad de la información que proporciona, vulnerabilidades, como ha sido concebida en forma hipotética y como se pone en práctica, además de su visión a futuro como el campo criptográfico más prometedor y los desafíos que supone pasar a este método de encriptación no tradicional.
7. Fuentes.	Para el desarrollo de la monografía se realizó un levantamiento documental que se sustentó en 63 fuentes consultadas, todas publicaciones de rigor científico extraídas de bases de consulta como IEEE y Springer Nature.
8. Contenidos.	El desarrollo de la monografía inicia con una introducción al concepto de criptografía enumerando los principios de seguridad que engloban el concepto; se describe la historia de la criptografía llegando a la criptografía moderna estudiando los sistemas de cifrado simétrico y asimétrico. Para poder lograr una compresión adecuada del concepto de criptografía cuántica se exponen los conceptos de varios mundos y los principios de la mecánica cuántica que soportan a este metido de encriptación: la paradoja del gato de Schrödinger, el principio de incertidumbre de Heisenberg, el Teorema de No-clonación y el entrelazamiento cuántico. Se

	encapsulan el concepto de Bits cuánticos ¨Qbits¨ como unidad de medida mínima en la computación cuántica. Se realiza un comparativo entre la criptografía cuántica vs la criptografía post-cuántica, se expone la importancia y la gravedad para la seguridad de la información la implementación del algoritmo de Shor y el algoritmo de Glover y los posibles algoritmos de seguridad que podrían soportar la llegada e implementación del computador cuántico. Se describe la normalización y estandarización que esta siendo llevada por la ANSI y la ENISA. Se exponen las pruebas a las que ha sido sometido el protocolo BB84 y se enumeran los protocolos alternos como el B92 y E91 además de los ataques probados y la respuesta de la criptografía cuántica demostrando su nivel de seguridad real y por último en la monografía se enumeran los usos y aplicaciones describiendo los sistemas de votaciones usos en las ciencias de la salud. y se concluye la monografía con la descripción de la carrera comercial para desarrollar y llegar al público común y se enumeran las empresas que lo están realizando.
9. Metodología.	La monografía se desarrolló bajo un diseño descriptivo, basado en la compilación, el análisis y presentación de la información recopilada. La unidad de análisis central es la criptografía cuántica, para el levantamiento documental especifico se delimita una variable de tiempo inferior a los 5 años que genera una recopilación de la ciencia estudiada a un concepto actual.
10. Conclusiones.	La criptografía cuántica tendrá uso como medida paralela a la criptografía post cuántica para codificar la transmisión de información de forma segura durante la era de computación cuántica salvaguardando información sensible que podrá ser vulnerable a este tipo de computadoras en un futuro cercano. La criptografía cuántica ha demostrado resistencia a los diferentes ataques informáticos a los que se ha puesto a prueba y ha demostrado una capacidad de mejora continua a vulnerabilidades encontradas lo que la convierte en un método de encriptación seguro y confiable para su implementación.

	La distribución de claves cuánticas (QKD) es la única tecnología perteneciente a la criptografía cuántica que está siendo comercializada a la fecha ya que no requiere el uso de un computador cuántico y puede ser implementada con tecnología que ya se comercializa sin restricción, pero aun así sin ser de aplicación general. La Normalización y estandarización de tecnologías de computación y criptografía post cuántica realizadas por la ANSI (Instituto Nacional Estadounidense de Estándares) y la ENISA (Agencia Europea de Seguridad de las Redes y de la Información) dan a entender que la era de la computación cuántica esta próxima a ocurrir y con una alta posibilidad de que sea en la presente década. Muchos países han realizado estudios, pruebas e implementaciones basados en criptografía cuántica sin embargo es China el país que está a la vanguardia y lleva un paso adelante con respecto a avances e implementaciones reales, además de promover la investigación y e desarrollo contante en esta área a través de los programas de la Fundación Nacional de Ciencias Naturales de China. Muchos avances actuales de la criptografía cuántica aún son desconocidos para el público común por ser parte de programas gubernamentales y militares y no se descarta que esta ciencia este siendo investigada como parte de una carrera armamentista entre países que están rivalizados como medio de ataque y/o protección de la información confidencial de un país.
11. Autor del RAE.	John Harrison Cardona Cardona

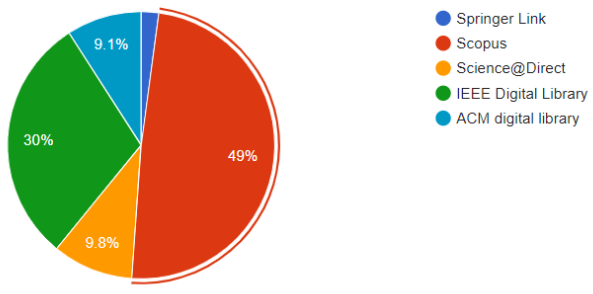
Anexo 2. Documento tipo paper

Revisión sistemática del estado del arte de la criptográfica cuántica, sus usos y aplicaciones

John Harrison Cardona Cardona. Autor

***Abstract*—El uso de métodos de encriptación a la hora de compartir información sensible es indispensable en la actualidad, estos métodos usados han sido basados en esquemas de cifrado por tecnología de computación matemática, los cuales en alguna medida han presentado ciertas vulnerabilidades a ser descifrados, es por esto que surge la idea de la criptografía cuántica, la cual funciona aplicando las leyes de la mecánica cuántica y puede ser usada sin restricciones para comunicaciones de datos confiables, que en teoría superan los inconvenientes que ha presentado la criptografía tradicional.**

En la presente documento se realiza un levantamiento y revisión de la literatura científica relevante que ha estudiado la criptografía cuántica en los últimos 5 años, consolidando su descripción detallada, leyes que la fundamentan, usos, propiedades, nivel de seguridad e integridad de la información que proporciona, vulnerabilidades, como ha sido concebida en forma hipotética y como se pone en práctica, además de su visión a futuro como el campo criptográfico más prometedor y los desafíos que supone pasar a este método de encriptación no tradicional



Bases consultadas para la consolidación del estado del arte.

***Palabras claves*— Criptografía Cuántica, Distribución de Claves Cuánticas, Protocolo BB84, Cúbit**

INTRODUCCIÓN

Vivimos en una era en la cual, casi todas las actividades se realizan a través del internet, los datos cuentan con un valor incalculable, proteger la privacidad de la información es indispensable y cada vez se demandan métodos que tengan la capacidad de ser infalibles ante cualquier vulnerabilidad; la criptografía que se usa en la actualidad la cual está basada en métodos matemáticos ha brindado seguridad, integridad y anonimización en la información, no obstante, se plantean interrogantes de hasta qué punto estos métodos criptográficos son técnica efectiva y si se puede utilizar otra técnica que proporcione una protección adicional en el tratamiento de datos personales.

Los avances tecnológicos especialmente de hardware amenazan con poner en aprietos a la criptografía tradicional como el aumento de descifrado de contraseñas apoyado en GPU que proporcionan una forma de realizar cálculos masivamente paralelos, que representan la mayoría de los ataques de fuerza bruta. Como punto de referencia, en un solo NVidia GTX 1080 GPU es capaz de hacer más de 43 mil millones de conjeturas por segundo, Las GPU han cambiado el descifrado de contraseñas de formas aún más fundamentales que simplemente permiten adivinar más rápido. (Aggarwal, Houshmand, & Weir, 2018)

Las amenazas a la seguridad de la información son las que han impulsado el uso de una alternativa a la criptografía tradicional, sistemas cuánticos diseñados de tal manera que

utilizan la mecánica cuántica y depende en gran medida de la física clásica. El concepto básico es que es difícil calcular el estado cuántico de cualquier sistema sin perturbarlo. El principal objetivo de la criptografía cuántica es crear una clave que se utiliza en el sistema de cifrado para transferir datos con fotones ligeros a través de cualquier fibra óptica o espacio libre. (Moizuddin, Winston, & Qayyum, 2017) Esto garantizaría en teoría la completa integridad, disponibilidad y confidencialidad de la información compartida.

Comprender el concepto de la criptografía cuántica, sus usos y aplicaciones es proceso complejo, es por esto que en esta monografía se realiza un levantamiento documental de calidad y recopilan un número significativo de referencias bibliográficas que permiten desarrollar un estado del arte que referencia el punto actual y más avanzado sobre esta temática especifica, generando una oportunidad para comprender cómo la abstracción de un concepto teórico puede materializarse en una realidad. Un estado del arte de la criptografía cuántica en español permitirá un acercamiento y estudio a la temática para profesionales como ingenieros, matemáticos y físicos no solo como herramienta para el reconocimiento e interpretación preliminar también con el fin de motivar la investigación académica y nuevos desarrollos en el área y como base para la toma de decisiones en el campo de la investigación.

REVISIÓN SISTEMATICA DE CONCEPTOS

Definiciones:

El término criptografía deriva de las palabras griegas "kryptós" y "gráphein", que significan "oculto" y "escribir". Por lo tanto, se puede parafrasear como "escritura oculta". La criptografía es la ciencia matemática encargada de transformar los datos para hacer ininteligible su significado, es decir, para ocultar su contenido, evitar su alteración e impedir su uso no autorizado. Si la transformación de los datos es reversible, la criptografía también se ocupa de restaurar datos encriptados a su forma inteligible. (Oppliger, 2021)

La criptografía engloba el proceso de protección de datos en un sentido muy amplio y se rige bajo los principios de seguridad de la información:

- Confidencialidad: Especifica que sólo el remitente y el destinatario pueden acceder a los datos.
- Autenticación: La autenticación asegura la identidad del usuario y el origen del mensaje.
- Integridad: Garantiza que el mensaje no se modifica incluso después de que el remitente lo haya enviado.
- Control de acceso: Administra quien puede acceder y a que puede acceder. Se relaciona con dos áreas como la gestión de roles y la gestión de reglas.
- No repudio: El remitente no puede desacreditar las transacciones realizadas anteriormente.
- Disponibilidad: Enfatiza los recursos que son obtenibles para las partes autorizadas de forma perpetua, la finalidad es evitar la interrupción. (Kahate, 2018)

Concepto de Criptoanálisis: El criptoanálisis, al contrario de la criptografía corresponde a las técnicas que estudian la forma de romper los algoritmos criptográficos. El criptoanálisis es comúnmente usado para comprobar la solidez de los procedimientos de seguridad y en la exploración de las diferentes vulnerabilidades de los cifrados. (Cortez, Sison, & Medina, 2020)

Criptografía Moderna

Antes de la era digital, la encriptación se utilizaba sobre todo para proteger las comunicaciones militares y gubernamentales hoy en día la criptografía es usada básicamente en cualquier lado sobre todo en Internet. Otras técnicas criptográficas fundamentales criptográficas son las funciones hash criptográficas y los esquemas de firma digital las cuales se utilizan para proteger la integridad y la autenticidad de los datos. (Ma J. , 2020)

En el proceso de encriptación los datos originales, es decir el texto plano del mensaje se transforma en un mensaje codificado, es decir código resultado del algoritmo de cifrado para poder transmitir estos datos a través de canales de comunicación no seguros. Una cadena de datos que conocida como "Clave" se utiliza para controlar la transformación de los datos de texto plano a texto cifrado. Esta disposición ayuda a mantener los datos seguros ya que se requiere siempre de la clave para poder extraer la información original del texto cifrado y sin la clave nadie puede leer los datos.

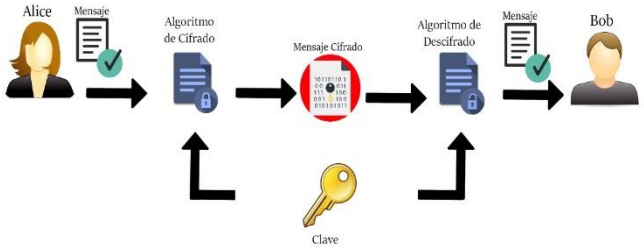


Fig 1 el proceso de un sistema criptográfico inicia con el mensaje sin cifrar los datos de este mensaje son cifrados a través de un algoritmo, una vez cifrado viaja por el canal ya codificado cuando llega al destinatario se descifra con la clave y se transforma nuevamente en el mensaje inicial sin cifrar, En la figura se utilizan los nombres de Alice y Bob para hacer referencia a un usuario A y B y el nombre Eve será usado para hacer referencia a un eavesdropper, una escucha, un espía que representa el usuario que intermedio que desea interceptar los mensajes enviados y es el objetivo principal a vencer en el cifrado de datos

Sistema de cifrado simétrico

Los sistemas de cifrado simétrico son susceptibles a ataque de fuerza bruta y ataque de criptoanálisis en donde el atacante hace uso de características del algoritmo para hacerse con la clave o con el texto descifrado.

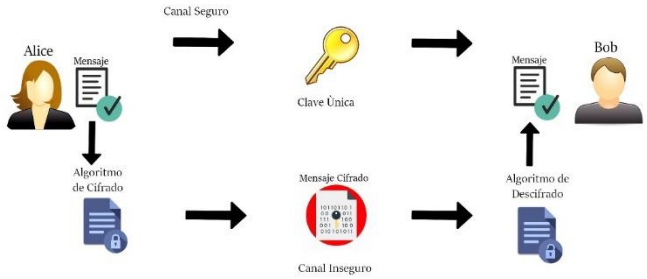


Figura 2 la clave única se intercambia entre Alice y Bob que se comunican antes de la transmisión de los datos por un canal seguro, mientras que el mensaje cifrado se envía por un canal inseguro. Para cifrar el mensaje el algoritmo de encriptación lleva a cabo una serie de sustituciones y transformaciones en el texto plano por su parte el algoritmo de descifrado en el cifrado de clave simétrica es el inverso del algoritmo de cifrado.

Sistema de cifrado Asimétrico

Los sistemas de cifrado simétrico se caracterizan por utilizar un par de claves: una clave pública y clave privada, la clave pública se comparte a través de un canal inseguro.

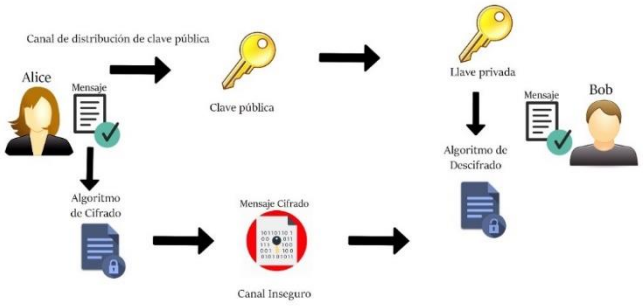


Figura 3 Bob encripta el mensaje con la clave pública y descifra el mensaje cifrado utilizando la clave privada que solo él posee. A diferencia de la criptografía de clave simétrica la clave secreta no se comparte, sino que cada parte que se comunica calcula la clave secreta con su propia clave privada y pública. El resultado es que Alice y Bob calculan la misma clave secreta sin transmitirla. (Gajbhiye, Karmakar, Sharma, & Sharma, 2017)

Mecánica cuántica

La mecánica cuántica es el conjunto de leyes fundamentales según las cuales todos los objetos se mueven. Para los objetos macroscópicos con los que interactuamos en la vida cotidiana las leyes de la mecánica cuántica se reducen a la mecánica clásica. Sin embargo, para la escala microscópica de los átomos las leyes de la mecánica cuántica dan lugar a un comportamiento muy diferente. Una de las diferencias fundamentales entre ambas es que en la mecánica cuántica un objeto puede estar simultáneamente en varios estados. En la mecánica clásica un objeto puede estar en ambos. (Schütt, Chmiela, von Lilienfeld , Tkatchenko, & Tsuda , 2020)

Gato de Schrödinger

En 1935 Erwin Schrödinger propuso un experimento conocido como "el gato de Schrödinger" que ha generado muchas discusiones y debates en la comunidad cuántica a lo largo de las décadas. En este experimento la emisión de un átomo radiactivo, un fenómeno completamente cuántico desencadena una serie de reacciones que controla la vida o la muerte de un gato dos acontecimientos distintos en el mundo clásico macroscópico. El trabajo condujo a la noción de estado del gato de Schrödinger, una superposición de distintos estados clásicos distintos, que permite la conexión entre los mundos cuántico y clásico. (Duan, 2019)

Principio de incertidumbre de Heisenberg

Uno de los principios fundamentales de la mecánica cuántica es el principio de incertidumbre que impone una restricción sobre el grado en que se pueden restringir las probabilidades de futuras mediciones de un sistema cuántico De manera más sencilla este principio afirma que, si se mide una característica no se puede medir otra característica con precisión. Esta característica del principio de incertidumbre de Heisenberg solo es válida para el instante en que se trata de medir las características del sistema (perturbación).
En la mecánica cuántica este principio se aplica a los fotones. Los fotones tienen una estructura ondulatoria y están polarizados o inclinados en cierta dirección. Al medir la polarización de los fotones, todas las mediciones posteriores se ven afectadas por la elección de las medidas que hacen para la polarización. (Pawar & Dinesh G. , 2018)

Teorema de No-clonación:

El teorema de no clonación afirma que toda transformación unitaria no puede clonar un estado cuántico arbitrario. Sin embargo, algunas transformaciones unitarias pueden clonar un subconjunto de estados cuánticos puros, lo que muestran que se pueden hacer solo clones imperfectos. (Epstein, 2019)

El teorema de No-clonación es una de las bases de la criptografía cuántica ya que permita que no sea posible para un usuario intermedio copiar el mensaje que se ha enviado. Con esto entonces, el emisor del mensaje cifrado puede estar seguro de que cada bit cuántico que envié solo sea transmitido una vez sin riego a ser clonado, una gran ventaja que ofrece la teoría cuántica a comparación del método clásico en donde la información puede copiarse perfectamente. (Ortigoso, 2018)

Entrelazamiento cuántico

El entrelazamiento cuántico es el fenómeno físico que se produce cuando un par o grupo de partículas se genera al mismo tiempo, interactúan o comparten proximidad espacial de tal manera que el estado cuántico de cada partícula del par o grupo no puede describirse independientemente del estado de las demás, incluso cuando las partículas estén separadas por una gran distancia. (Wu, 2020)

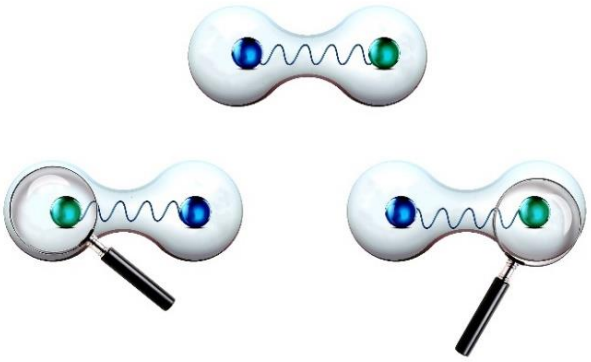


Fig 4 Las mediciones de propiedades físicas como la posición, el momento, el espín y la polarización realizadas en partículas entrelazadas están perfectamente correlacionadas

. Los primeros trabajos mencionados sobre la comprensión del entrelazamiento acabaron siendo la base para el campo de la computación cuántica, cuyo objetivo es explotar las extrañas propiedades de los estados cuánticos para tareas de procesamiento de información que no son posibles en el mundo clásico. El entrelazamiento cuántico es el combustible de una serie de protocolos cuánticos como la teletransportación, el cifrado denso y la distribución de claves. (Wang & Wilde, 2020)

Computación cuántica

El ordenador cuántico trabaja en computación paralela donde un número múltiple de procesos microscópicos se programan y seleccionan basándose en una probabilidad aleatoria. Por ejemplo, si consideramos un registro cuántico de n bits, existen 2n estados posibles simultáneamente, lo que se conoce como superposición. Cada función f(x) puede ser representada como un circuito cuántico en el que todos los posibles valores de superposición de x se consideran como entrada y todos los posibles valores de superposición de y = f(x) da como salida. (Mitra, Bappaditya, Bhattacharya, Pal, & Poray, 2017)

Un paso crucial en la evolución de la computación, en general podría ser la implantación del ordenador cuántico. Los problemas que se han considerado difíciles de resolver con los ordenadores clásicos no serán tan difíciles de resolver con el uso de un ordenador cuántico. Con lo cual se evidencia como problemática que la mayoría de los modelos criptográficos de clave pública actuales se basan en esos problemas, algo que los hace vulnerables cuando se enfrenten a un ordenador cuántico. (Giampouris, Short Review on Quantum Key Distribution Protocols, 2017)

Dada la potencia de los ordenadores cuánticos, el siguiente paso para proteger las transmisiones de claves y la transmisión de información sensible es la criptografía cuántica. La criptografía cuántica es muy diferente de la criptografía clásica, porque en lugar de utilizar problemas matemáticos difíciles de resolver, se basa en las leyes de la física como base para establecer la seguridad.

Qubits (bits Quánticos)

La criptografía cuántica requiere un canal que lleva un objeto físico llamados Bits Cuánticos o alternativamente conocidos como qubits, el qubit es la unidad básica de la computación cuántica. Hay dos tipos de canal cuántico uno es el cable de fibra óptica y el otro es la atmósfera que nos rodea. Durante la transmisión de los qubits de un extremo a otro del canal de transmisión no hay cambio de ningún estado mecánico de los qubits. Los qubits se conectan mediante algunas puertas básicas de qubits. La mayor ventaja de los qubits sobre otros bits convencionales es que los qubits es que son un sistema bidimensional y pueden expresarse como una forma probabilística intermedia entre dos límites 0 y 1, mientras que los bits convencionales pueden expresarse como 0 o 1.

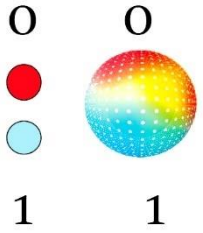


Fig 5 Un Bit la unidad mínima de la informática y un Qubit la unidad mínima de la computación cuántica. Fuente: Autor

Principio de polarización de los fotones

Los fotones son las partículas elementales y responsable de las manifestaciones cuánticas del fenómeno electromagnético de la luz, un fotón puede orientarse o polarizarse en direcciones específicas y además, un filtro de fotones con la polarización correcta sólo puede detectar un fotón polarizado o de lo contrario, el fotón será destruido. Esta característica hace ideal que la criptografía cuántica haga el envío de claves secretas en forma de fotones con sus respectivas polarizaciones, rectilínea para polarización vertical y horizontal, y la base diagonal para +45 y -45. (Nanda, Puthal, Mohanty, & Choppali, 2018)

Protocolo BB84

BB84(Bennett y Brassard año 1984) fue el primer protocolo de criptografía cuántica que explicaba cómo utilizar el estado de polarización de los fotones para transmitir la información de la clave secreta a través de un canal de comunicación cuántica. Este protocolo se clasifica como QKD basado en la preparación y la medida.

El protocolo BB84 utiliza un solo fotón para transmitir y distribuir bits aleatorios de la clave secreta. El fotón único está polarizado en uno de los cuatro estados de polarización y seleccionado utilizando una de las dos bases conjugadas, la base rectilínea para polarización vertical y horizontal, y la base diagonal para +45 y -45 anti diagonal, El proceso de implementación se divide en: Intercambio Cuántico, Cifrado de clave, reconciliación de la información y amplificación de la privacidad. (Nurhadi & Rachmana Syambas, 2018)

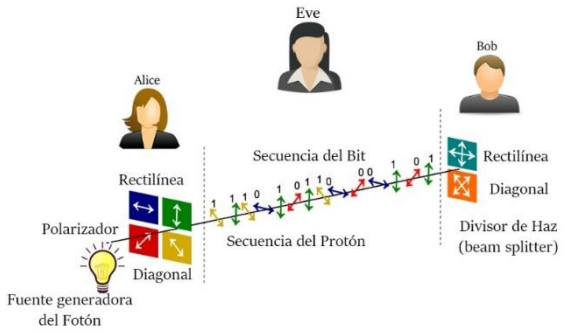


Fig 6 Alice transmite los fotones a través de un polarizador que les otorga aleatoriamente una de las cuatro polarizaciones y designaciones de bits posibles: Vertical (Un bit), Horizontal (Cero bit), 45 grados a la derecha (Un bit), o 45 grados a la izquierda (Cero bit).

CRIPTOGRAFIA CUANTICA VS CRIPTOGRAFIA POST-CUANTICA

Una computadora cuántica con una cantidad considerable de qubits podría romper la mayoría criptosistemas actualmente en uso, por lo tanto, existe una necesidad urgente de desarrollar algoritmos criptográficos que puedan resistir la ruptura de código clásica y cuántica. Estos son denominados criptosistemas post-cuánticos, se trata de combinar la criptografía post-cuántica con la criptografía cuántica, mientras que la criptografía cuántica se refiere al método de encriptación que utiliza los principios de la mecánica cuántica para reforzar la seguridad y detectar una escucha en las comunicaciones, la criptografía post-cuántica a su vez hace referencia a los algoritmos que pueden tener la capacidad de proteger la información en la era de la computación cuántica. (Bobrysheva & Zapechnikov, 2019)

Los avances en criptografía post-cuántica han demostrado que cualquier algoritmo criptográfico basado en la complejidad matemática como la factorización y los logaritmos discretos se considera muy vulnerable desde la perspectiva de una computadora cuántica Esto también aplicaría a todos los protocolos de seguridad que utilizan este tipo de algoritmo criptográfico. Los sistemas criptográficos basados en el cifrado simétrico, como AES, se consideran más robustos por su método y que se podría aumentar el tamaño de la clave. Por otro lado, el cifrado asimétrico como un método de clave pública aún no está listo para la criptografía post-cuántica. (Grote, Ahrens, & Benavente-Peces, 2019)

El algoritmo de Shor

En 1994 el profesor de matemática aplicada Peter Shor introdujo un algoritmo capaz de encontrar los factores de cualquier número entero positivo N. El algoritmo de Shor es una amenaza potencial para muchos criptosistemas ya que su seguridad se basa en la suposición de que calcular números grandes es difícil o en la dificultad de calcular fragmentariamente logaritmos discretos.

Algoritmo de Grover

El algoritmo de Grover al ser de naturaleza cuántica posee un carácter probabilístico, por lo que produce una respuesta que más se acerca con una determinada probabilidad de error, la cual puede llegar a ser tan baja como se desee por medio de una mayor cantidad de iteraciones las cuales pueden llegar a ser posibles con una adecuada cantidad de qubits. Por otro lado, si las operaciones de qubit son lo suficientemente pequeñas y rápidas el algoritmo de Grover se convierte en una amenaza para muchos de los criptosistemas que buscan seguridad, como las claves AES y SHA. (Bernstein & Lange, 2017)

		Función	***Nivel de seguridad Pre Cuántica***	***Nivel de seguridad Post Cuántica***
Criptografía de clave simétrica (llave Secreta)	AES-128	Cifrado simétrico	128	64 (Con algoritmo de Grover)
	AES-256	Cifrado simétrico	256	128 (Con algoritmo de Grover)
	Salsa20	Cifrado simétrico	256	128 (Con algoritmo de Grover)
	GMAC	MAC (código de autenticación de mensaje)	128	128 (Sin presunto impacto)
	Poly1305	MAC (código de autenticación de mensaje)	128	128 (Sin presunto impacto)
	SHA-256	Función Hash	256	128 (Con algoritmo de Grover)
	SHA3-256	Función Hash	256	128 (Con algoritmo de Grover
Criptografía de clave asimétrica (llave Publica)	RSA-3072	Cifrado de firma	128	Descifrado (Con el algoritmo de Shor)
	RSA-3072	Cifrado de firma	128	Descifrado (Con el algoritmo de Shor)
	DH-3072	Intercambio de llaves	128	Descifrado (Con el algoritmo de Shor)
	DSA-3072	Intercambio de llaves	128	Descifrado (Con el algoritmo de Shor)
	256-bit ECDH	Intercambio de llaves	128	Descifrado (Con el algoritmo de Shor)
	256-bit ECDSA	Intercambio de llaves	128	Descifrado (Con el algoritmo de Shor)

Tabla1. Nivel de seguridad en bits con que cuentan diversos sistemas de cifrado en la actualidad y el nivel de seguridad en bits con el que contaran en la era post cuántica, además de su comportamiento frente a las dos amenazas más notorias los algoritmos de Shor y Grover.

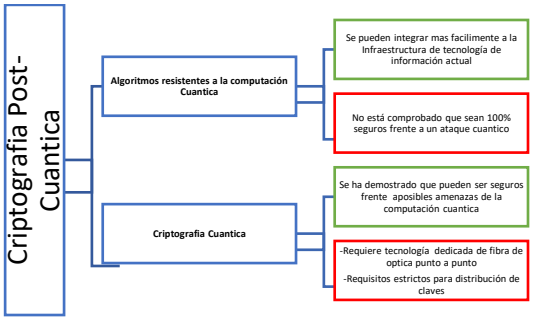


Fig 7 se enfrentan los algoritmos resistentes a la computación cuántica

frente la criptografía cuántica mostrando sus ventajas y desventajas como modelo de criptografía post-cuántica.

Normalización y estandarización Post-Cuántica

En el más reciente informe presentado por el NIST se concluye que no parece haber ningún algoritmo conocido actualmente que pueda servir en la era post-cuántica para lo que se usa exactamente hoy. Un reto que probablemente deberá superarse es que la mayoría de los algoritmos que puedan ser resistentes a un ataque cuántico tienen tamaños de clave más grandes que los algoritmos que reemplazarán. Esto puede requerir cambios en varios protocolos de internet para intercambio de claves, Por lo tanto, ninguno de los experimentos ha demostrado garantizar la seguridad contra todos los ataques cuánticos, y es posible que se descubra un nuevo algoritmo cuántico para romper algunos de los patrones faltantes. (Chen, y otros, 2018)

La Organización Europea de Normalización ETSI también ha iniciado investigaciones en los criptosistemas post-cuánticos con una serie de publicaciones preliminares, en la más reciente denominada "Post-Quantum Cryptography: Current state and quantum mitigation" Se hace énfasis en que es importante tener reemplazos disponibles primero, cualquier comunicación cifrada interceptada hoy puede ser descifrada por un atacante tan pronto como obtenga acceso a una gran computadora cuántica, ya sea dentro de 5, 10 o 20 años, un ataque que puede ser conocido como un descifrado retrospectivo. (ENISA, 2021)

EFECTIVIDAD DEL PROTOCOLO BB84 Y PROTOCOLOS ALTERNOS

Las verdaderas pruebas para la seguridad del protocolo BB84 han llegado con los escenarios de implementación con hardware que puede ser defectuoso. Para reducir esta vulnerabilidad del protocolo que puede ser causada por calibres imperfectos esta la alternativa de esquemas MDI(Measurement Device Independent). Por otro lado, BB84 tiene un sólido respaldo teórico de seguridad contra una amplia gama de ataques y demostraciones repartidas por todo el mundo, lo que lo convierte en el protocolo estándar para la implementación practica de la distribución de claves cuánticas.

DIMENSIONES CORRESPONDIENTES AL PROTOCOLO BB84

Dimensión	**Clasificación**
1) Numero de estados cuánticos	• Basado en Qubits
	• Basado en Qudits
2) Tipo de Protocolo BB84	• BB84 cuatro estados
	• BB84 tres estados
	• BB84 de alta dimensión
3) Métodos generales aplicados al protocolo BB84	• BB84 Puro
	• Tolerante a pérdidas
	• Referencia fuerte
	• Estados señuelo + tolerante a pérdidas
	• Estados señuelo
4)Elección de base	• Imparcial (probabilidades iguales)
	• Sesgado (Probabilidades Distintas)
5) Esquema de codificación	• Polarización
	• Fase
	• Time-Bin (Fase-Tiempo)
	• Frecuencia
	• Momento angular orbital
6) Consideraciones sobre el tamaño de la clave	• clave finita
	• Régimen Asintótico

Tabla 2, El protocolo BB84 fue clasificado en forma de taxonomía en un sentido general en el 2021, las dimensiones por las que se clasifico el protocolo desde un punto de vista teórico son: el número de estados cuánticos, tipo de implementación del protocolo BB84, si se aplican procedimientos generales al protocolo BB84, la elección de las bases, y programa de cifrado. (Zavala & Barán, 2021)

Diferentes estudios en la universidad electrónica del norte de China han demostrado que el protocolo BB84 brinda diferentes niveles de seguridad para la protección de la información del sistema de distribución. Los resultados muestran que se puede mejorar la eficiencia de la distribución de claves cuánticas de múltiples nodos y posiblemente lidiando con una serie de eventos inesperados. El trabajo adicional incluye optimizar la seguridad del sistema QKD y el rendimiento de la generación de claves, analizar el impacto de un entorno de fuente de alimentación determinado en el rendimiento del sistema de distribución, la fase de diseño anti-interferencias y probar la extensión de conexión segura. (Ma, Yi, Guochen, & Zha, 2019)

El protocolo BB84 también ha sido probado en esquemas de firma digital post-cuántica como el propuesto por Labadzea en el cual se utiliza un esquema de firma único en lugar de un esquema de Merkl esto permite reducir la longitud de la firma, para firmar mensajes se generan claves de firma y verificación. Para transferir las claves de verificación se realiza mediante el protocolo BB84. Para ello, se cifra un bit aleatorio con la ayuda de qubits identificando a los oyentes y obteniendo una clave secreta; Para firmar el mensaje se genera un hash. El número mínimo de ceros se coloca antes de la representación binaria para obtener la longitud de la representación. Como resultado se obtiene un esquema de firma digital basado en hash, que es seguro, ya que utiliza la versión clásica del esquema de un solo uso de y el protocolo BB84, el tamaño de la firma generado es mucho más pequeño que en el caso de un esquema Merkle. (Labadzea, Iavichb, & Iashvilib, 2021)

Protocolo B92

El protocolo B92 se ha estudiado ampliamente en entornos asimétricos, donde se ha demostrado que tolera una interferencia de canal de hasta el 6,5 % y soporta hasta un 11 % de ruido en entornos asintótico. Se ha propuesto una variante extendida de B92, donde, además de dos estados de codificación no ortogonales usado en el B92, Alice y Bob usan otros dos estados no ortogonales y sin codificación para

restringir la información de Eve de manera más estricta.. Con respecto a la pérdida, el protocolo B92 original es muy vulnerable a los ataques de discriminación estatal explícitos, mientras que la versión extendida, protege contra tales ataques. (Amer & Krawec, 2020)

En el 2020 Walter O. Kraweca and Sam A. Markelon propusieron un nuevo protocolo de distribución de claves semicuánticas inspirado en el protocolo B92, este trabajo amplía el protocolo con un segundo esquema de cifrado que permite responder mejor a los ataques de tipo USD (unambiguous state discrimination). Además, se ha mejorado la metodología de análisis de seguridad para incluir tipos de ataques más amplios como los ataques colectivos como trabajo futuro.

En este modelo propuesto, una de las partes, normalmente la A (Alice), es "totalmente cuántica" porque puede realizar todas las operaciones necesarias sobre el qubit. La segunda parte, B (Bob), es "clásica" porque solo puede interactuar con canales cuánticos de forma limitada y clásica. Más específicamente, estos protocolos utilizan canales cuánticos bidireccionales que permiten que la información cuántica se mueva. El usuario "clásico" B tiene dos opciones cuando se trata de obtener el estado cuántico de A. Son: Medir y reenviar, haciendo que los estados entrantes acepten mediciones del estado fundamental de los cálculos a A. y reflejar el estado de regreso a A sin cambiarlo. (Krawec & Markelon, 2020)

Protocolo E91 y otras propuestas

El E91 también conocido como protocolo EPR fue elaborado por Artur Ekert en 1991, el cual se sustentó en el entrelazamiento cuántico de pares de fotones. El esquema de transmisión está basado igualmente en el protocolo BB84; en este esquema Eve puede proporcionar estados separables a Alice y Bob, para que pueda obtener información sobre la llave.

En el 2018 en la universidad de Corea se realizó la implementación experimental de un protocolo de distribución de clave cuánticas de tipo "Plug & Play bidireccional", que utiliza pulsos de doble acoplamiento en el nivel de fotón único para transmitir información crítica de Alice a Bob a través de un canal cuántico.

En este prototipo propuesto es de tipo cableado y es presentado como una implementación práctica de un protocolo QKD plug-and-play que utiliza espejos de Faraday para compensar automáticamente los cambios de polarización u oscilaciones de canal, que ocurren debido a la distribución de fibra óptica de los interruptores cuánticos. La experimentación del prototipo demostró que una clave transmitida a través de un canal cuántico de 25 km tiene una tasa de bloqueo de 100 bits por segundo y un QBER (Quantum bit error rate) de alrededor del 3%. (Byungkyu, Jinyoung, Youngjin, & Jun, 2018)

LA VENGANZA DE EVE: ATAQUES PROBADOS EN LA CRIPTOGRAFIA CUANTICA

La criptografía cuántica se presenta como un método ideal e infalible para proteger el intercambio de información de forma segura en teoría, en la práctica los qubits son fotones con distintas polarizaciones, donde es necesario utilizar fibra óptica, canales, láseres, polarizadores y con todas las fallas que pueden tener estos aparatos, se abren un montón de posibilidades para potenciales atacantes, además de posible desarrollo de un hardware especializado para espionaje en canales cuánticos, por ahora la construcción de un aparato completo de espionaje sigue siendo bastante difícil, podría ser posible con la tecnología actual o en un futuro próximo.

Uno de los posibles ataques a la criptografía cuántica es el “Ataque del Caballo de Troya”, el cual ha sido probado de la siguiente forma: consiste en enviar potentes pulsos de luz por el canal que permiten a Eva averiguar cómo está configurado, Eva podría averiguar previamente los ejes que ha elegido Alice y medir todos los qubits sin provocar ni una detección por parte de Bob y Alice.

Se demostró la sostenibilidad experimental de un ataque de troyano aún casi invisible a un solo detector de fotones utilizado en los sistemas de distribución reales de claves cuánticas (QKD). Por lo tanto, existe una necesidad urgente de incorporar contramedidas efectivas en los sistemas QKD para contener estas amenazas. La más sencilla para proteger el sistema QKD de este ataque es filtrar adecuadamente la luz que entra en el sistema. (Shihan , Carter, & Nitin, 2017)

Un ataque cuántico de hombre en el medio en el proceso de calibración del canal cuántico antes del intercambio de claves en un sistema QKD con detectores de fotones individuales de modo cerrado de un solo fotón, puede ser posible si el canal cuántico está bajo el control de Eve en el proceso y los usuarios legítimos no comprueban la legitimidad de las señales de calibración, ya que estas señales no contienen información. (Yang-Yang , Xiang-Dong , Ming, Wang , & Ma, 2018)

El ataque USD(unambiguous state discrimination) es considerado asumiendo que Eve puede dividir el canal en dos, el canal Alice-Bob y el canal Alice-Eve-Bob sin pérdidas o con pérdidas menores donde ella realiza las mediciones de USD. El canal original Alice-Bob es el clásico-cuántico; En el experimento práctico se consideró el enfoque de los protocolos QKD con estados coherentes débiles codificados que desactivan el ataque de USD utilizando estados señuelo del gato de Schrödinger. (Gaidash, Kozubov, & Miroshnichen, 2018)

La inyección de SQL es una vulnerabilidad que conduce a un ataque de lenguaje de consulta estructurado (SQL) en el que un atacante puede explotar la sintaxis y las capacidades del propio SQL.En la comunicación cuántica la base de datos está representada por el canal cuántico y el código del programa maligno está representado por un "fotón de programa maligno". (Amellal, Meslouhi, & Hassouni, 2017)

Un nuevo riesgo no tan presente en la criptografía clásica: Los ataques con luz y ventilación, los cuales están relacionados con ataques electromagnéticos. La luz de los dispositivos puede dar información a los atacantes que no pueden llegar al sistema directamente. La mayoría de los dispositivos electrónicos utilizan diodos emisores de luz (LED) para señalar el funcionamiento normal y para un rápido diagnóstico visual. Estas vías ópticas también abren una puerta trasera para los ataques de inyección óptica, en los que una señal óptica altera el funcionamiento normal del dispositivo. (Garcia, Sajeed, & Vadim, 2020)

PROBLEMA DE SEGURIDAD	***DESCRIPCIÓN***	***CONTRAMEDIDAS***
Ataque de caballo de Troya	Eve prueba el equipo QKD con luz para obtener información sobre la configuración del dispositivo	Amplificación de privacidad (PA), aisladores, filtros
Emisión de fotones múltiples	Cuando se emite más de un fotón en un pulso, la información se codifica de manera redundante en múltiples fotones	(PA), caracterización, estados señuelo, SARG04 y otros protocolos
Codificación imperfecta	Los estados iniciales no se ajustan al protocolo.	(PA), caracterización
Correlación de fase entre pulsos de señal	Los pulsos no aleatorizados en fase filtran más información a Eve, los estados de señuelo fallan	fase de aleatorización, PA
Ataque de luz brillante	Eve manipula los detectores de fotones enviándoles luz brillante.	monitoreo activo, QKD independiente del dispositivo de medición (MDI-QKD)
Desajuste de eficiencia y ataque de cambio de tiempo	Eve puede controlar, al menos parcialmente, en qué detector hacer clic, obteniendo información sobre el bit codificado.	MDI-QKD, simetrización de detectores
Ataque de retroceso	Eve puede aprender qué detector hizo clic y, por lo tanto, conoce el bit	aisladores, MDI-QKD, detector de simetrización
Manipulación de la referencia del oscilador local	En la variable continua QKD (CV-QKD), el oscilador local (LO) puede ser manipulado por Eve si se envía por un canal de comunicaciones	Generar LO en el receptor. Recarga de fase, es decir, sincronizar solo la fase de LO

Tabla 3 se presenta una muestra representativa de los principales ataques contra el sistema de distribución de claves cuánticas con su descripción, así como las contramedidas para evitarlos.

CRIPTOGRAFÍA CUÁNTICA: SUS USOS Y APLICACIONES

La criptografía cuántica es una ciencia que se presenta en teoría como solución a diversas problemáticas y en la aplicación de diferentes ramas entre las cuales se encuentran: la encriptación de datos, firma digital, comunicación segura en el espacio, internet cuántico, intercambio y distribución de claves, red eléctrica avanzada, votación ultra segura, análisis y predicción del ADN y análisis de la estructura funcional del cerebro.

Votaciones limpias con criptografía cuántica

La primera instalación y puesta en práctica mundial de criptografía cuántica en la vida real fue en las elecciones federales en el estado de Ginebra Suiza el 21 de octubre de 2007, El reto para el gobierno de Ginebra era garantizar la máxima seguridad para proteger la autenticidad e integridad de los datos y al mismo tiempo gestionar el proceso con eficacia, también tenían que garantizar el axioma de un ciudadano, un voto.

Normalmente, las urnas selladas se llevan desde los colegios electorales a la estación central de recuento, donde se abren y se cuentan junto con los votos por correo ya entregados. El recuento se realiza manualmente según estrictas normas de procedimiento. Sin embargo, en el mundo moderno este principio se ha reinterpretado: la comisión electoral lleva a cabo una estrecha vigilancia del recuento y de la introducción de datos, y la autenticidad e integridad de cualquier transferencia de datos posterior se garantiza entonces mediante el más alto nivel de encriptación.

La solución implantada en las elecciones consiste en un cifrado híbrido que utiliza el encriptado de capa 2 de última generación basada en el cifrado AES (Advanced Encryption Standard) de 256 bits combinada con la distribución de claves cuánticas (QKD). La solución Cerberis protege un enlace Gigabit Ethernet punto a punto utilizado para enviar la información de las papeletas de las elecciones desde la estación central de recuento de votos hasta el centro de datos del gobierno de Ginebra. El gobierno de Ginebra ha utilizado con éxito la solución Cerberis de IDQ en todas las elecciones federales desde 2007 como elemento clave para la integridad y la seguridad de las votaciones. (ID QUANTIQUE SA, 2017)

Fig 8 se observa un Cerberis que fue utilizado en el sistema de distribución de claves cuánticas en las elecciones nacionales suizas, el cual se diseñó para proteger la línea exclusiva que transmite las papeletas a la estación de recuento.

Algunos expertos afirman que las comunidades militares y de inteligencia han utilizado habitualmente estos sistemas de distribución de claves cuánticas. Pero la elección de Ginebra es la primera vez que una organización gubernamental dice abiertamente que utiliza esta técnica.

Desde la implementación de la criptografía cuántica en las elecciones en Suiza se han desarrollado otros prototipos y técnicas para la aplicación de esta tecnología en diferentes sistemas de votaciones; En Odessa Ucrania se propuso un esquema de seguridad criptográfica asistido por ordenador destinado al recuento en unas elecciones. La idea principal es utilizar dos tecnologías de la criptografía cuántica: el compromiso cuántico de bits y el intercambio cuántico.

El esquema de intercambio cuántico del prototipo tiene tres participantes en el procedimiento de intercambio de secretos: Alice, que es la distribuidora, y los otros dos participantes que comparten directamente el secreto: Bob y Charley. Como regla se generaliza un número arbitrario de participantes en el procedimiento de compartir el secreto, al recibir los datos cada uno de los dos agentes ejecuta el intercambio del secreto de acuerdo con el esquema, a continuación, los agentes transfieren cada parte del secreto a cada miembro de la comisión. Para completar el procedimiento de recuento de votos todos los miembros de la comisión deben mostrar sus partes del secreto a los demás. De lo contrario, el recuento de votos es no se realiza, de esta forma el esquema hace que sea no sea posible manipular los votos. (Karpinski, Gancarczyk, Klos-Witkowska, Limar, & Vasiliu, 2017)

La criptografía cuántica también ha sido probada en sistemas de votaciones en conjunto con otras tecnologías como el Blockchain cuántico satisfaciendo totalmente los requisitos de seguridad que debe de tener un protocolo de votación electrónico:

- El anonimato está garantizado porque la comunicación segura cuántica prohíbe que otros votantes conozcan la matriz completa.
- Otros votantes no pueden cambiar la papeleta de un votante debido al procedimiento de autenticación de la cadena de bloques cuántica. El propio votante no puede cambiar su papeleta presentada debido a la propiedad de compromiso cuántico.
- La no reutilización se violaría si un votante pudiera añadir con éxito dos papeletas diferentes a la cadena de bloques.
- Cada votante puede comprobar fácilmente si su papeleta enmascarada se ha subido con éxito a la blockchain porque por su diseño es una base de datos transparente.
- Sólo los votantes autentificados pueden comunicarse con éxito con los mineros.
- La equidad se destruirá si alguien puede contar parcialmente las papeletas antes de la fase de recuento de votos.
- Los usuarios pueden contar las papeletas simplemente calculando la suma de las papeletas enmascaradas. (Xin , Wang, Piotr , & Sope, 2019)

Para una futura implementación de votaciones utilizando tecnologías basadas en criptografía cuántica se han diseñado reglas de voto cuántico denominadas QLV y QLN. En ambas de ellas las papeletas se lanzan en estados cuánticos y pueden realizarse físicamente con la tecnología actual y la dificultad de la realización física no crece con el aumento del número de votantes. Adicional a estas reglas de voto se planea estudiar el veto y la nominación cuánticos en la situación en la que algunas máquinas de votación cuántica sufran un comportamiento defectuoso. En estas situaciones se utilizarán cadenas de bloques cuánticos como plataforma para ejecutar el veto y la nominación cuántica. (Meiyun, y otros, 2022)

Criptografía cuántica en ciencias de la salud

En la industria de las ciencias de la vida, se espera que la computación y la criptografía cuántica permita una serie de casos de uso innovadores, entre ellos se encuentran: Crear terapias de medicina de precisión vinculando genomas y resultados, afinar los resultados de los pacientes mediante la mejora de la eficiencia de fármacos de moléculas pequeñas y desarrollar nuevos productos biológicos basados en predicciones de plegado de proteínas. (Flöther, Moose, & Tavernelli , 2020)

Existe gran expectativa en el sector de salud con respecto a la criptografía cuántica como medida definitiva para garantizar la completa seguridad y privacidad de la información tanto de entidades prestadoras de servicios de salud, farmacéuticas y de pacientes.

Los datos son sagrados en la industria de las ciencias de la vida, tanto desde la perspectiva de la propiedad intelectual como para garantizar la privacidad de los datos de los pacientes. La definición de la información personal

identificable también está evolucionando junto con las nuevas tecnologías ómicas. El acceso protegido a los historiales médicos y el intercambio seguro de datos mediante de datos mediante encriptación cuántica podrían ser algunas de las primeras aplicaciones de la computación cuántica en las ciencias de la vida. Como la computación cuántica puede asegurar la clave y los datos indefinidamente con una encriptación inviolable, el Instituto Nacional de Estándares y Tecnología (NIST) ha comenzado a centrarse en proporcionar técnicas de encriptación basadas en la tecnología cuántica para aplicaciones de servicios médicos y farmacéuticos. (TATA Consultancy Services , 2021)

En la actualidad se han propuesto diferentes sistemas de protección para entidades de prestación de servicios de salud utilizando criptografía cuántica, como esta en la cual el administrador del hospital y el usuario utilizan la clave cuántica para almacenar y acceder a los datos. La clave cuántica se genera a partir de los qubits obtenidos del administrador y se utiliza tanto para el cifrado como para el descifrado, cuando el usuario envía una solicitud, el administrador detecta los qubits para el usuario y compara los qubits para identificar si el usuario es de confianza o no, esta clave utiliza los fotones aleatorios para representar un solo bit de datos. (Rubesh , Sakthida, & Thangapandiyan, 2018)

La criptografía cuántica también ha sido probada en ayudas medicas como imágenes, se ha propuesto que el personal sanitario pueda cifrar las imágenes médicas importantes mediante el esquema de cifrado cuántico, enviando las imágenes cifradas a la nube en donde el personal sanitario de otro lugar podrá consultarlas descifrando el contenido mediante el método propuesto. Este sistema de cifrado cuántico garantiza una alta confidencialidad para los pacientes y los usuarios del sistema sanitario; Para el análisis del rendimiento del enfoque propuesto en un ordenador clásico, se emplearon varias simulaciones y métodos numéricos, como la correlación, la entropía de Shannon, análisis de sensibilidad y análisis de histogramas (Abd El-Latif, Abd-El-Atty, & Talha, 2017)

Avances en Infraestructura para la implementación de la criptografía cuántica

Para que sea posible la distribución de claves cuánticas es necesario que se realice una transmisión que debe ser confidencial y segura, actualmente la forma más común utiliza fibras ópticas la cual cuenta con una gran estabilidad, pero una considerable pérdida de canal. Otra tecnología utilizada es el espacio libre entre los satélites y las estaciones terrestres con la cual ha sido posible realizar transmisiones incluso a miles de kilómetros

Los satélites se pueden utilizar para establecer comunicaciones cuánticas a distancias mucho más largas de las que se pueden lograr en la tierra y se pueden utilizar como parte de una arquitectura de red cuántica más grande para vincular redes cuánticas terrestres locales a largas distancias, la creación de redes de esta manera construye una red muy parecida a la Internet actual, por lo tanto, los satélites proporcionan un enfoque a corto plazo para construir una red cuántica global.

Recientemente en china se ha establecido la primera red de comunicación cuántica integrada del mundo, la cual combina más de 700 fibras ópticas en tierra con dos enlaces a satélite la cual permite la distribución de claves cuánticas a una distancia total de 4600 kilómetros recorriendo el este del país desde Shanghái hasta Beijing.

La red cuántica presentada en China consiste en de cuatro QMAN (Redes cuánticas de área metropolitana), una red troncal a escala nacional y una red satélite-tierra-satélite, la topología en estrella es la estructura clave en las cuatro redes y los transmisores del dispositivo de medición y BB84 son esencialmente los mismos. Por lo tanto, los sistemas transmisores de la red de fibra actual pueden utilizarse también para realizar la red QKD independiente de las mediciones. Además, con la ampliación de la red troncal, se formará una topología más sofisticada que mejorará el tiempo-frecuencia, la gravedad cuántica e interferometría a gran escala para aplicaciones de metrología. Y también podrá ser posible realizar la computación distribuida y repetidores cuánticos en grandes áreas en un futuro próximo. (Chen, Zhang, Chen, & Wen-Qi , 2021)

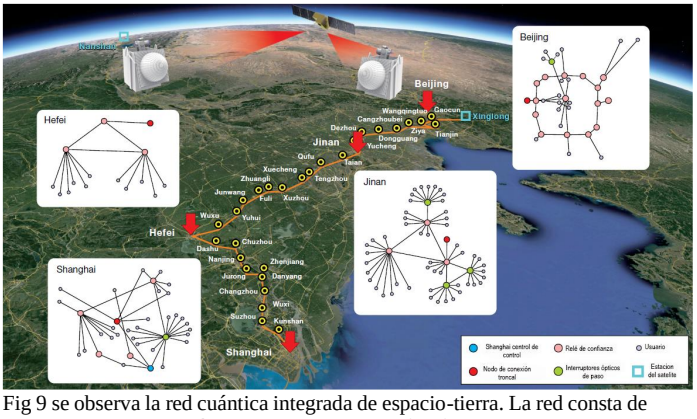


Fig 9 se observa la red cuántica integrada de espacio-tierra. La red consta de cuatro QMAN (en Pekín, Jinan, Shangai y Heifei; flechas rojas), un enlace de fibra troncal de más de 2.000 km (línea naranja) y dos enlaces satélite-satélite que conectan Xinglong y Nanshan (cuadrados azules), separados por 600 km. Hay tres tipos de nodos en la red: los nodos de usuario (círculos morados). Un satélite cuántico está conectado a las estaciones terrestres de Xinglong y Nanshan; Xinglong también está conectado al QMAN de Pekín por fibra.

En el futuro, se tiene previsto ampliar la red en China y con sus socios internacionales de Austria, Italia, Rusia y Canadá. También pretenden desarrollar satélites QKD a pequeña escala y económicos, así como receptores en tierra y satélites de órbita terrestre media y alta para conseguir una QKD a tiempo completo y a 10.000 kilómetros.

Recientemente, la empresa británica Arqit ha anunciado sus planes para empezar a construir una red QKD mediante satélites. Los satélites se lanzarán en 2023 a través de Virgin

Galactic. Esto marca una transición en la comunicación cuántica por satélite hacia el sector privado. (ARQUIT CENTRICUS, 2021)

•*Carrera comercial por la criptografía cuántica*

Actualmente tres empresas son pioneras en el campo de la criptografía cuantica: BBN Technologies de Boston (EE.UU.), MagiQ de Nueva York (EE.UU.) e ID Quantique de Ginebra (Suiza). Todas ellas han probado sistemas de criptografía cuántica con clientes como bancos y otras instituciones financieras, sin embargo, existen muchas otras entidades incursionando en el negocio con diferentes aplicaciones de encriptación comercial.

Qrypt : Es un startup con sede en Nueva York que tiene su propia solución criptográfica. La empresa afirma que su solución de cifrado es capaz de proteger a las empresas y la información privada en el presente y en el futuro.

"El cifrado de seguridad cuántica de Qrypt ofrece a las personas las herramientas que necesitan para asegurar de forma inmutable sus datos y su derecho a la privacidad. A través de grandes alianzas y un equipo inigualable, hemos construido métodos y aplicaciones de cifrado patentados que permiten a todos reclamar su derecho a la autonomía digital". www.qrypt.com

Single Quantum: La empresa con sede en los Países Bajos ofrece soluciones para la detección de fotones en el extremo del receptor con una alta precisión.

"Fundado en 2012, Single Quantum surgió como auténticos pioneros de la tecnología de detección de fotones individuales: fuimos de los primeros en fabricar y comercializar detectores de fotones individuales de nanohilos superconductores. Desde entonces, nuestro sistema multicanal de detección de fotones Single Quantum Eos ha sido elegido por más de 100 laboratorios académicos e industriales de todo el mundo para realizar complejas mediciones ópticas, Single Quantum desarrollará los sensores de luz más rápidos y sensibles del mundo, limitados únicamente por las leyes de la física". https://singlequantum.com/

Post-Quantum: La empresa proporciona soluciones de protección contra la amenaza cuántica y ofrece soluciones comerciales y gubernamentales. Post-Quantum dispone de soluciones como algoritmos de cifrado y soluciones de ciberseguridad.

"Hoy en día hemos construido un conjunto de productos utilizables y seguros desde el punto de vista cuántico que abarcan el cifrado, la transmisión y la identidad. Estos productos protegen los datos desde el momento en que se crean, mientras se transmiten y frente a riesgos adyacentes como los ataques a la identidad cuántica. Nuestra tecnología se combina para ayudar a las organizaciones a conseguir un "ecosistema seguro desde el punto de vista cuántico" que proteja cada punto de vulnerabilidad". www.post-quantum.com

Crypto Quantique: Los productos, plataformas y servicios tecnológicos de Crypto Quantique proporcionan seguridad de extremo a extremo en todas las redes de IoT con ciberseguridad impulsada por la tecnología cuántica. La empresa afirma tener una seguridad impulsada por la cuántica en un chip que puede generar múltiples claves criptográficas que no necesitan ser almacenadas y utilizadas independientemente en múltiples aplicaciones.

"Crypto Quantique es un pionero de la seguridad del IoT. Hemos combinado la criptografía y la física cuántica para desarrollar productos de seguridad que impulsan la seguridad de extremo a extremo y desbloquean la escalabilidad de las redes de IoT". www.cryptoquantique.com/

ID Quantique: Fundada en 2001 como un spin-off del Grupo de Física Aplicada de la Universidad de Ginebra, ID Quantique es el líder mundial en soluciones criptográficas de seguridad cuántica, diseñadas para proteger los datos del futuro. La empresa ofrece cifrado de redes seguro desde el punto de vista cuántico, generación de claves cuánticas seguras y soluciones de distribución de claves cuánticas, así como servicios al sector financiero, las empresas y las organizaciones gubernamentales de todo el mundo.

"Los productos de IDQ son utilizados por clientes gubernamentales, empresariales y académicos en más de 60 países y en todos los continentes. Como empresa privada suiza centrada en el crecimiento sostenible, IDQ está orgullosa de su independencia y neutralidad, y cree en el establecimiento de relaciones a largo plazo y de confianza con sus clientes y socios". www.idquantique.com/

El naciente interés en la criptografía cuántica la convierte en un campo de batalla comercial en la cual una cantidad cada vez más elevada de empresas se pelean por la supremacía no solo gubernamental y militar si no por una implementación de tecnologías y productos al público común a futuro cercano.

CONCLUSIONES

La criptografía cuántica tendrá uso como medida paralela a la criptografía post cuántica para codificar la transmisión de información de forma segura durante la era de computación cuántica salvaguardando información sensible que podrá ser vulnerable a este tipo de computadoras en un futuro cercano.

La criptografía cuántica ha demostrado resistencia a los diferentes ataques informáticos a los que se ha puesto a prueba y ha demostrado una capacidad de mejora continua a vulnerabilidades encontradas lo que la convierte en un

método de encriptación seguro y confiable para su implementación.

La distribución de claves cuánticas (QKD) es la única tecnología perteneciente a la criptografía cuántica que está siendo comercializada a la fecha ya que no requiere el uso de un computador cuántico y puede ser implementada con tecnología que ya se comercializa sin restricción, pero aun así sin ser de aplicación general.

La Normalización y estandarización de tecnologías de computación y criptografía post cuántica realizadas por la ANSI (Instituto Nacional Estadounidense de Estándares) y la ENISA (Agencia Europea de Seguridad de las Redes y de la Información) dan a entender que la era de la computación cuántica esta próxima a ocurrir y con una alta posibilidad de que sea en la presente década.

Varios países han realizado estudios, pruebas e implementaciones basados en criptografía cuántica sin embargo es China el país que está a la vanguardia y lleva un paso adelante con respecto a avances e implementaciones reales, además de promover la investigación y e desarrollo contante en esta área a través de los programas de la Fundación Nacional de Ciencias Naturales de China.

Una gran cantidad de los avances actuales de la criptografía cuántica aún son desconocidos para el público común por ser parte de programas gubernamentales y militares y no se descarta que esta ciencia este siendo investigada como parte de una carrera armamentista entre países que están rivalizados como medio de ataque y/o protección de la información confidencial de un país.

REFERENCIAS

[1] S. Aggarwal, S. Houshmand y M. Weir, New Technologies in Password Cracking Techniques, Santa Clara University, 2018, p. 181.

[2] M. Moizuddin, D. Winston y M. Qayyum, «Comprehensive Survey: Quantum Cryptography,» de 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), 2017.

[3] R. Oppliger, Cryptography 101 From Theory to Practice, Artech House, 2021, p. 1.

[4] A. Kahate, Cryptography and Network Security, McGraw-Hill Education Pvt. Ltd, 2018.

[5] D. M. A. Cortez, A. M. Sison y R. P. Medina, «Cryptanalysis of the Modified SHA256,» de Conference on Big Data and Artificial Intelligence, 2020.

[6] J. Ma, «Basic application of mathematics in cryptography,» de International Conference on Modem Education and Information Management, Santa Barbara-Usa, 2020.

[7] S. Gajbhiye, S. Karmakar, M. Sharma y S. Sharma, «Paradigm Shift from Classical Cryptography to,» de Proceedings of the International Conference on Intelligent Sustainable Systems, Palladam, India, 2017.

[8] K. T. Schütt, S. Chmiela, A. von Lilienfeld , A. Tkatchenko y K. Tsuda , «Quantum Mechanics,» de Machine Learning Meets Quantum Physics, Berlin, Springer, 2020, pp. 15-17.

[9] L. Duan, «Creating Schrödinger-cat states,» Nature Photonics , 2019.

[10] H. R. Pawar y H. Dinesh G. , «Classical and Quantum Cryptography for Image Encryption & Decryption,» de International Conference on Research in Intelligent and Computing in Engineering (RICE), Badnera-India, 2018.

[11] S. Epstein, «Algorithmic No-Cloning Theorem,» IEEE TRANSACTIONS ON INFORMATION THEORY, vol. 65, nº 9, Septeimber 2019.

[12] J. Ortigoso, «Twelve years before the quantum no-cloning theorem,» Am. J. Phys, vol. 86, nº 3, March 2018.

[13] E. T. H. Wu, «Photon Polarization and Entanglement Interpreted by Yangton,» Journal Of Applied Physics, vol. 12, nº 3, Jun 2020.

[14] X. Wang y M. M. Wilde, «Cost of Quantum Entanglement Simplified,» PHYSICAL REVIEW LETTERS, vol. 125, 2020.

[15] S. Mitra, J. Bappaditya, S. Bhattacharya, P. Pal y J. Poray, «Quantum Cryptography: Overview,Security Issues and Future Challenges,» de International Conference on Opto-Electronics and Applied Optics (Optronix), 2017.

[16] D. Giampouris, «Short Review on Quantum Key Distribution Protocols,» Advances in Experimental Medicine and Biology, vol. 988, p. 149–157, 2017.

[17] A. Nanda, D. Puthal, S. P. Mohanty y U. Choppali, «A Computing Perspective on Quantum Cryptography,» IEEE Consumer Electronics Magazine, p. 59, Nov 2018.

[18] A. I. Nurhadi y N. Rachmana Syambas, «Quantum Key Distribution (QKD) Protocols: A,» de 4th International Conference on Wireless and Telematics (ICWT), 2018.

[19] J. Bobrysheva y S. Zapechnikov, «Post-Quantum Security of Communication and New Perspectives,» de IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, Russia, 2019.

[20] O. Grote, A. Ahrens y C. Benavente-Peces, «A Review of Post-quantum Cryptography and Crypto-agility Strategies,» Wismar, Germany, 2019.

[21] D. J. Bernstein y T. Lange, «Post-quantum cryptography,» Nature Vol 549, 14 September 2017.

[22] L. Chen, S. Jordan, L. Yi-Kai, D. Moody, R. Peralta, R. Perlner y D. Smith-Tone, «Report on Post-Quantum Cryptography,» Gaithersburg, MD, 2018.

[23] ENISA, «Post-Quantum Cryptography: Current state and quantum mitigation,» ENISA, Attiki, Athens, 2021.

[24] M. Zavala y B. Barán, «QKD BB84. A Taxonomy,» de 2021 XLVII Latin American Computing Conference (CLEI), Cartago, Costa Rica, 2021.

[25] Y. Ma, L. Yi, W. Guochen y X. Zha, «Performance optimization of decoy-state BB84- and MDI- QKD protocol and,» Optical Fiber Technology, vol. 52, 2019.

[26] G. Labadzea, ,. Iavichb y G. Iashvilib, «Proceedings of the 26th International Conference on Information Society and University Studies,» Kaunas, Lithuania, 2021.

[27] O. Amer y W. O. Krawec, «Finite Key Analysis of the Extended B92 Protocol,» de 2020 IEEE International Symposium on Information Theory (ISIT), Los Angeles, USA, 2020.

[28] W. O. Krawec y S. A. Markelon, «A Semi-Quantum Extended B92 Protocol and its Analysis,» de Quantum Information Science, Sensing, and Computation XII, Connecticut, USA, 2020.

[29] A. Byungkyu, H. Jinyoung, S. Youngjin y H. Jun, «Implementation of Plug & Play Quantum Key Distribution Protocol,» de Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, Czech Republic, 2018.

[30] . S. Shihan , M. Carter y J. Nitin, «Invisible Trojan-horse attack,» Scientific Reports , vol. 7, 2017.

[31] F. Yang-Yang , M. Xiang-Dong , G. Ming, H. Wang y Z. Ma, «Quantum man-in-the-middle attack on the calibration process of quantum key distribution,» Scientific Reports, vol. 8, 2018.

[32] A. Gaidash, A. Kozubov y G. Miroshnichen, «Overcoming unambiguous state discrimination attack with the help of Schrödinger Cat decoy states,» Optica , vol. X, 2018.

[33] H. Amellal, A. Meslouhi y Y. Hassouni, «SQL injection principle against BB84 protocol,» de International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), Rabat, Morocco, 2017.

[34] J. C. Garcia, S. Sajeed y M. Vadim, «Attacking quantum key distribution by light,» PLoS ONE, vol. 15, 2020.

[35] ID QUANTIQUE SA, «Distribution, Securing Data Transfer for Elections-Ethernet Encryption with Quantum Key,» Ginebra, Suiza, 2017.

[36] M. Karpinski, T. Gancarczyk, A. Klos-Witkowska, I. Limar y Y. Vasiliu, «Security Amplification of the Computer-Aided,» de 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Bucharest, Romania, 2017.

[37] S. Xin , Q. Wang, K. Piotr y M. Sope, «A Simple Voting Protocol on Quantum Blockchain,» de International Journal of Theoretical Physics, 2019.

[38] G. Meiyun, P. Kulicki, M. Sopek, D. Qiu, F. He y S. Xin, «Distributed Quantum Vote Based on Quantum Logical,» de Project: Quantum-enhanced Logic-based Blockchain, Lublin-Poland, 2022.

[39] F. Flöther, C. Moose y I. Tavernelli , «Exploring quantum computing use cases for life sciences,» Institute for Bussines Value IBM, 2020.

[40] TATA Consultancy Services , «Life sciences research and and quantum computing: The future is almost here,» Bombay, India, 2021.

[41] M. Rubesh , K. Sakthida y M. Thangapandiyan, «Quantum Key Distribution and Cryptography,» de International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2018.

[42] A. A. Abd El-Latif, B. Abd-El-Atty y M. Talha, «Robust Encryption of Quantum Medical Images,» IEEE Access , vol. 6, pp. 1073 - 1081, 2017.

[43] Y.-A. Chen, Q. Zhang, T.-Y. Chen y C. Wen-Qi , «An integrated space-to-ground quantum communication network over 4,600 kilometres,» Nature, nº 589, p. 214–219, 2021.

[44] ARQUIT CENTRICUS, «Centricus Acquisition Corp. To Combine With,» 21 05 2021. [En línea]. Available: https://dcswhimef-res.cloudinary.com/image/upload/v1620817479/WhitePapers/CENTRICUS_ACQUISITION_CORP._TO_COMBINE_WITH_ARQIT_LIMITED_A_LEADER_IN_QUANTUM_ENCRYPTION_TECHNOLOGY_.pdf.

8.