UNIVERSIDAD NACIONAL DE CAAGUAZÚ

FACULTAD DE CIENCIAS Y TECNOLOGÍAS

INGENIERÍA EN INFORMÁTICA

Estudio de la criptografía cuántica y su utilidad para la seguridad de la información.

Elaborado por:

GLORIA ELIZABETH ACEVEDO BARRETO

Tutor:

Ing. Víctor Manuel Melgarejo

Co tutor:

Ing. María del Carmen Escobar González

Trabajo de Grado presentado a la Facultad de Ciencias y Tecnologías de la Universidad Nacional de Caaguazú, como requisito para la obtención del título de Ingeniería en Sistemas Informáticos.

CORONEL OVIEDO – PARAGUAY

2021

PÁGINA DE APROBACIÓN

MESA EXAMINADORA DE SUSTENTACIÓN DE TESIS DE GRADO

Carrera de Ingeniería en Sistemas Informáticos

Título de la Tesis: Estudio de la criptografía cuántica y su utilidad para la seguridad de las informaciones.

Calificación Obtenida: _____

_____ Miembro

_____ Miembro

_____ Miembro

_____ Miembro

_____

Presidente

Acta Nª: _____

Fecha: _____

DEDICATORIA

Ésta Tesis va dedicada:

A Dios,

En memoria de quien fue, es, y, será mi gran inspiración

Vicente Acevedo,

A mis padres:

Eleno Acevedo y Francisca Barreto,

A mis hermanos:

Nilda, Elena, Ever, Alicia y Arnaldo

AGRADECIMIENTOS

Primeramente, a Dios, por darme la sabiduría y entendimiento, por la fuerza que me dio a diario para culminar esta etapa de mi vida.

A Vicente, quien siempre estará presente en mi corazón. ¡Ya soy Ingeniera!

A mis padres, por todo el apoyo que me dieron en estos largos años.

A mis hermanos, por darme el espíritu de aliento para seguir continuando.

A mis amigos, por su apoyo incondicional, por estar a mi lado sin importar las circunstancias, por acompañarme en este proceso y por ser mi soporte en todo momento.

A mis profesores, por haber compartido conmigo sus conocimientos.

A la Ing. Carmen Escobar por acompañarme en este arduo camino, por el apoyo incondicional que me ha brindado para la culminación de esta tesis.

A Robert, por haberme apoyado siempre, sobre todo por su paciencia y amor incondicional.

Sin dejar atrás a todas esas personas, que directa e indirectamente me ayudaron en esta larga carrera. ¡Muchas Gracias!

RESUMEN

Con el análisis de la criptografía cuántica en la seguridad de informaciones, lo que se pretende es aumentar la protección de la misma, ya que hasta hoy día no se ha podido demostrar que existe una vulnerabilidad porque la misma utiliza fotones que cambian de estado y alertan al emisor y al receptor cuando el canal no es seguro.

Para ese fin, la metodología que se adoptó en este trabajo es el cuantitativo por la interpretación de los datos relevados, mediante la aplicación de herramientas como la observación, recolección de datos con la revisión bibliográfica, análisis de contenidos, que permitió obtener las informaciones necesarias.

Con referencia a lo anterior el tipo de estudio fue el descriptivo, diseño no experimental. La proposición tecnológica de la criptografía cuántica nos posibilita visualizar un futuro con mayor seguridad en la transmisión de información y todos los procesos investigativos tendientes a ese fin, contribuirán a una implementación más segura.

Para finalizar, se presentan los resultados obtenidos y las conclusiones del proyecto.

Palabras claves: Criptografía Cuántica, Seguridad de la Información

ABSTRACT

With the analysis of quantum cryptography in information security, the aim is to increase its protection, since until today it has not been possible to demonstrate that there is a vulnerability because it uses photons that change state and alert to the sender and receiver when the channel is not secure.

To this, the methodology adopted in this work is qualitative for the interpretation of the data collected, through the application of tools such as observation, data collection with bibliographic review, content analysis, which allowed obtaining the necessary information.

With reference to the above, the type of study was descriptive, non-experimental design. The technological proposition of quantum cryptography enables us to visualize a future with greater security in the transmission of information and all the investigative processes aimed at that cause will contribute to a more secure implementation.

Finally, the results obtained and the conclusions of the project are presented.

Keywords: Quantum Cryptography, Security of the information

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

CAPÍTULO I

1. MARCO INTRODUCTORIO

1.1. INTRODUCCIÓN

El objetivo principal de esta investigación es establecer un análisis de la criptografía cuántica en la seguridad de la información. Actualmente las criptografías cuánticas protegen todas las comunicaciones por internet, cuando esto suceda, necesitaremos haber implementado nuevas formas de criptografía capaces de resistir a estas máquinas.

Desde un entorno histórico, la criptografía cuántica es creada como una idea en el año 1970 y sólo hasta en 1984 fue desarrollada y se publica el primer protocolo, que usa los principios de la mecánica cuántica para garantizar la transmisión de la información de manera segura. Una de las propiedades más resaltantes de la criptografía cuántica es que si una entidad distinta al emisor y receptor intenta utilizar técnicas de eavesdropping para obtener la llave secreta revelara su intención antes de ser transmitida la información privada, cumpliendo así el principio de incertidumbre de Heisenberg el cual afirma que el hecho de medir un sistema cuántico perturba dicho sistema.

La definición de criptografía cuántica más fácil de comprender es, una técnica usada para resolver el envío seguro de llaves criptográficas entre dos partes (emisor y receptor) estas llaves se codifican a través del uso de partículas de luz llamadas fotones, estas partes deben compartir una llave aleatoria, la cual es técnicamente indescifrable, suprimiendo así la posibilidad de interceptación por parte de terceros. Sí un espía pretendiera interceptar alguna de las llaves solo observaría los cambios de estados de los fotones, poniendo al descubierto su intención de ataque. Para poder proteger la información se utiliza criptografía clásica que son algoritmos para la encriptación de claves pseudo aleatorias, las inteligencias humanas junto al progreso de la tecnología han desarrollado técnicas para descifrar la información cifrada que se transmiten por la red, con ello cada vez es menos seguro ya que las potencias de los nuevos ordenadores podrían descifrar las claves en un menor tiempo. Como una solución a esta incertidumbre se ha puesto en práctica la criptografía cuántica como seguridad de la información debido a que son teóricamente aleatorias e indescifrables.

A nivel internacional los científicos están realizando investigaciones para su desarrollo y aplicación de la criptografía cuántica como una alternativa efectiva en la seguridad de la información.

1.2. PLANTEAMIENTO DEL PROBLEMA

La tecnología avanza con el correr del tiempo y las personas hacen uso de esta en las actividades diarias, como en la comunicación vía telefónica, comunicación por internet, compras en línea, manejo de cuentas bancarias, etc., los llamados hackers siempre están interesados en interceptar esta información sin que nos demos cuenta para hacer uso ilícito de dichas informaciones.

En la actualidad se sigue utilizando en gran parte la criptografía tradicional para proteger informaciones, cabe destacar que se ha demostrado la vulnerabilidad de la criptografía tradicional, como también con la aparición de un computador cuántico que está en proceso de desarrollo, fácilmente pondría en riesgo los sistemas criptográficos.

Con el fin de proteger los datos que se utilizan para realizar estas actividades cotidianas a través de la red, se utiliza la criptografía cuántica para cifrar la información transmitida con claves y al ser interceptada no sea legible. Como una solución mucho más efectiva se presenta al área de las comunicaciones experimentalmente los algoritmos cuánticos, que utiliza la física cuántica, por este motivo, utiliza números aleatorios brindando mayor seguridad en la transmisión de datos.

1.3. DELIMITACIÓN Y ALCANCE

El objetivo principal del proyecto de investigación es establecer un análisis de la criptografía cuántica en la seguridad de información sustentando teóricamente mediante una revisión sistemática, el estudio es teórico por que no se incluirán pruebas.

Para el estudio del arte se está aplicando una revisión sistemática, hoy en día implementada para el procedimiento de estudios de revisión bibliográfica, se considera sobresaliente su implementación, estas revisiones tienen como objetivo presentar una evaluación profunda de un tema de investigación usando una metodología confiable y precisa.

1.4. PREGUNTA DE INVESTIGACIÓN

En el marco de la problemática presentada se plantean las siguientes preguntas de investigación.

Pregunta General

¿Por qué se garantiza la absoluta confidencialidad de las informaciones aplicando la Criptografía Cuántica?

Preguntas Específicas

¿Por qué la criptografía cuántica es más segura que la criptografía conocida tradicionalmente?

1.5. OBJETIVOS

1.5.1. OBJETIVO GENERAL

- ✓ Establecer un análisis de la criptografía cuántica en la seguridad de las informaciones.

1.5.2. OBJETIVOS ESPECÍFICOS

- ✓ Describir conceptos fundamentales de la criptografía cuántica
- ✓ Explorar el desarrollo de la criptografía cuántica, y el protocolo fundamental utilizado para generar claves cuánticas para la seguridad de las informaciones.
- ✓ Realizar un análisis comparativo de la criptografía tradicional y la criptografía cuántica para la seguridad de las informaciones.

1.5.3 JUSTIFICACIÓN Y VIABILIDAD

Si bien sabemos que la criptografía tradicional permite en la actualidad mantener una comunicación segura entre dos partes, por otro lado, la criptografía cuántica puede lograr comunicaciones más seguras utilizando leyes de la naturaleza a escala cuántica.

Ocupaciones como compras con tarjetas de crédito, mensajes y conversaciones en teléfonos móviles, email, chats, llamadas en línea, búsquedas seguras en internet, compras en línea, almacenamiento en la nube desde su computadora, transacciones bancarias en línea, comunicación interna y en línea, en todas estas la seguridad juega una labor muy importante, lo que se soluciona aplicando la criptografía cuántica.

Actualmente una información reservada se codifica y se envía mediante redes de comunicación. Para poder transmitir esta información se utilizan los conocidos bits clásicos, es decir 0 y 1, y posteriormente se envía por medio de flujos de pulsos ópticos o eléctricos. Usando un sistema de comunicación clásico, los hackers pueden captar esta información, des encriptar la información, leerla y copiarla sin dejar ninguna señal. La vulnerabilidad de la criptografía tradicional, hace que sea una acción bastante fácil para los ataques informáticos.

CAPÍTULO II
2. ESTUDIO DEL ARTE

2.1. ESTUDIO DEL ARTE

Actualmente existen numerosos estudios sobre la criptografía cuántica, la mayor parte de ellos son realizados en Estados Unidos y parte de Europa. Las investigaciones realizadas sobre la criptografía cuántica son muy diversas y han servido de gran apoyo al desarrollo de esta tesis. Fueron revisados 51 artículos aproximadamente de los cuales se optó por 7 investigaciones para el estudio del arte.

AÑO DE PUBLICACIÓN	**REVISTAS**	**INVESTIGACIONES**	**ESTUDIO DEL ARTE**
1995	3	4	2
2008	0	7	1
2014	5	11	1
2018	4	9	2
2021	0	1	1
TOTAL SELECCIONADOS	**12**	**32**	**7**

Ilustración 1: *Cantidad de artículos estudiados*

2.1.2 INVESTIGACIONES INTERNACIONALES

Título de la Investigación: Meta análisis del estado actual de la criptografía cuántica identificando las áreas de desarrollo e implementación.

Investigadores: Alexander Hernández Niño y Alexander Reyes Quintero

Fecha: Investigación realizada en la Facultad de Ingeniería de la Universidad Católica de Colombia en el año 2014.

Duración del Proyecto: 3 meses

Objetivo: El desarrollo de un meta análisis del estado actual de la criptografía cuántica.

Criptografía Cuántica: El desarrollo y la implementación de la criptografía cuántica, ha propuesto nuevos paradigmas desde sus propiedades completamente distintas a las informaciones ordinarias que se conocen tradicionalmente.

La criptografía cuántica no pertenece al dominio de la ciencia ficción, pues actualmente se realiza en diversos laboratorios. Se ha logrado la transmisión de mensajes cifrados por este procedimiento entre puntos situados a más de veinte kilómetros conectados por fibra óptica y a varios centenares de metros en el caso de transmisión aérea. (ALEXANDER HERNÁNDEZ NIÑO, 2014)

En la seguridad de la información de la criptografía cuántica, se observarán cambios en la capacidad de asignar mayor integridad a la actual (se refiere a los datos enviados dentro de una comunicación), un impacto como este llevaría a campos como las finanzas y la economía, es por eso el interés del estudio de la criptografía cuántica.

Conclusiones: La gran propuesta tecnológica de la criptografía cuántica nos permite visualizar un futuro con mayor garantía la transmisión de información. Este proyecto de investigación sobre la criptografía cuántica estudiando las áreas de desarrollo e implementación, también da a conocer los protocolos más valorados en estas investigaciones.

Instrumentos: Para dicha investigación se utilizaron equipos de cómputos de los investigadores, paquete básico de Microsoft Office, internet.

Principales Referencias:

ACM Digital, Criptografía cuántica [En línea] [Citada en Febrero 01 de 2014] Disponible en internet:http://dl.acm.org/> CNN-CERT. Glosario [En línea]. Febrero 02 de 2009- [citada en Febrero 10 de 2014]. Disponible en internet:

GISIN Nelson, RIBORDY Gabriel. Quantum Communications and Cryptography. New York: Taylor & Francis Group, 2006. p. 145-150.ISBN 0-8493-8. IBM, SPSS. SPSS Statistics [CD-ROM]: MAC Versión 21. c. 2013. ISBN-10: 1446249182 IConTEC. Norma técnica colombiana NTC 1486. 6 ed. Bogotá D.C.: Contacto grafico Ltda., 2008. ISBN 978-958-9383-81-0. ICONTEC. Norma técnica colombiana NTC 4490. Bogotá D.C.: Contacto grafico Ltda., 1998. ISBN 978-958-9383-81-0.

Título de la Investigación: Distribución de claves criptográficas por fibra óptica mediante técnicas cuánticas.

Investigador: Francisco Javier González Payo

Lugar de la Investigación: Madrid - España

Fecha: Año 2014

Objetivo: Demuestra teóricamente la distribución de claves criptográficas mediante la fibra óptica utilizando técnicas cuánticas.

Criptografía Cuántica: Tras la finalización de la segunda guerra mundial. la criptografía cuántica obtuvo un desarrollo teórico muy importante, siendo Claude Shannon y sus grandes investigaciones sobre la teoría de la información esenciales en dicho desarrollo. Como también los avances en la computación automática suponían una gran amenaza para los sistemas de ese entonces como una oportunidad para el desarrollo de nuevos sistemas. La criptografía cuántica forma parte del campo de la cristología que también engloba el criptoanálisis o la llamada técnica de ruptura de campos. Para poder lograr codificar los mensajes se utilizan algoritmos también conocidos como criptosistemas o cifrado, que no hace más que unir el mensaje con una información denominada clave para poder producir un criptograma. Para que este criptograma sea seguro, tendría que ser imposible de desencriptar sin la clave. Esta condición se modera si se asegura que la desencriptación es posible pero extremadamente difícil, porque lo que importa es que la información protegida permanezca intacta, por lo menos el tiempo suficiente para que cuando se deba extraer sin la clave, ya deje de tener el mismo valor.

Resumen: La criptografía cuántica aparece para preservar las necesidades de la sociedad de poder contar con una forma segura de proteger la información en diferentes áreas de comunicación. Sin embargo, la criptografía clásica cuya seguridad se basa en suposiciones aún no probadas sobre dificultad computacional, se manifiesta progresivamente más insegura antes las evoluciones tecnológicas de nuestra habilidad computacional.

Esta investigación se adentra en el campo de las telecomunicaciones, las redes de fibra óptica que conforman desde hace tiempo el sistema de transmisión por antonomasia, se realizó el estudio profundo de todos los protocolos cuánticos, por la cual se hace constatar que el protocolo BB84 y el protocolo E91 son los más seguros.

Principales Referencias:

Levy, S., Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age, Penguin Books. 1st edition, December 2001.

Friedman, W.F., Military Cryptanalysis: Transposition and Fractionating Systems, Atlantic Books, December 1993.

Khan, D., The Codebreakers: The Story of Secret Writing, The Macmillan Company. First edition, 1967.

Vernam, G.S., "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications," Transactions of the American Institute of Electrical Engineers Vol. XLV, 295-301 (1926).

Sklar, B., Digital Communications. Fundamentals and applications, Prentice-Hall International. Inc., 1988.

Shor, P.W., "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," arXiv:quant-ph/9508027.

Centro Criptográfico Nacional. Ministerio español de la presidencia, Criptografía de empleo en el Esquema Nacional de Seguridad. Guía/Norma seguridad de las TIC (CCN-STIC-807), Junio 2011.

Título de la Investigación: Desarrollo de un simulador para el protocolo de criptografía cuántica E91 en un ambiente distribuido

Investigador: Cáceres Álvarez, Luis; Fritis Palacios, Roberto; Collao Caiconte, Patricio

Lugar de la Investigación: Universidad de Tarapacá - Chile

Fecha: 02 de abril de 1995 – publicado en Ingeniare. Revista Chilena de Ingeniería

Objetivo: Esta investigación se basa en el desarrollo de una aplicación que sea competente para simular el comportamiento de uno de los más importantes protocolos de la criptografía cuántica, el protocolo E91.

Criptografía Cuántica: La criptografía cuántica se encuentra entre una de las áreas más nuevas en investigación dentro de la criptografía, la misma está basada en los principios de la mecánica cuántica para salvaguardar la información, se forma que solo los usuarios autorizados puedan acceder. La certeza de los sistemas criptográficos cuánticos reside en la distribución de las claves.

Un cambio en el estado cuántico del sistema ocurre cuando un intruso captura los bits cuánticos utilizados para la generación de la clave de comunicación. El intruso, entonces, puede ser detectado debido a la modificación que sufre el estado cuántico. (Cáceres Alvarez, Fritis Palacios, & Collao Caiconte, 2015)

Desarrollo de la Aplicación: La arquitectura es la de un modelo cliente/servidor ajustada a los requerimientos y se usará como lenguaje la tecnología de Java RMI para lograr la comunicación distribuida. Por las características que lo definen como un lenguaje vigoroso, se optó por Java como lenguaje y Netbeans como la plataforma.

Configuraciones: Para la prueba realizada, se utilizó la aplicación de manera local, en donde dos participantes que conforman la comunicación y la fuente se ejecutan en un solo equipo. Después se ejecutan las pruebas de manera distribuida, cada elemento es ejecutado en distintos equipos y con diferentes sistemas operativos.

Pruebas de Aplicación: Para llevar a cabo las pruebas se utilizaron varias clases de computadoras, con sus correspondientes sistemas operativos instalados, se utilizó Windows y Mac Os.

Resumen: Dicha investigación llevada a cabo en la Facultad de Ingeniería de la Universidad Tarapacá de Chile, se basa en el desarrollo de una aplicación que sea competente para simular el comportamiento del protocolo E91. Se realiza una gran investigación de los más importantes conceptos y principios de la mecánica cuántica. Utilizaron la codificación conformada por claves secretas en su mayor parte aleatorias de un solo uso, así permitir llevar una comunicación segura. El protocolo utilizado E91 se encuentra basado en el teorema de Bell, la misma utiliza fotones entrelazados.

La investigación trató sobre el desarrollo de una aplicación simulando el comportamiento del protocolo E91, pero usando computadoras clásicas, es por la cual la aplicación desarrollada es netamente demostrativa de carácter académico. Las pruebas permitieron examinar el comportamiento de la aplicación.

Resultados: Se demostró que usando el protocolo E91, un 70% de los bits se desperdician, de acuerdo a la determinación del protocolo, el 30% restantes de bits es considerada como una clave segura, dicha clave se extrajo sin que los usuarios tengan la necesidad de compartir las partículas recibidas.

Principales Referencias:

H. García Molina. “Avances en Informática y Sistemas Computacionales”. Editorial Tabasco. Primera edición. México. Tomo I. 2006. ISBN: 968-5748-98-5.

P.W. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, pp. 125-134. Noviembre de 1994. DOI: 10.1109/SFCS.1994.365700.

D.-H. Shih, H.-S. Chiang and C. David Yen. “Classification methods in the detection of new malicious emails”. Information Sciences. Vol. 172 Nº 1-2, pp. 241-261. 9 de junio de 2005. DOI: 10.1016/j.ins.2004.06.003.

Seok Ko, C. Seong Leem, Y. Ji Na and C. Young Yoon. “Distribution of digital contents based on public key considering execution speed and security”. Information Sciences. Vol. 174 Nº 3-4, pp. 237-250. Agosto de 2005. ISSN: 0020-0255.

Y. Fang Chung, Z. Yu Wu and T. Shyong Chen. “Unconditionally secure cryptosystems based on quantum cryptography”. Information Sciences. Vol. 178 Nº 8, pp. 2044-2058. 15 de Abril de 2008. DOI: 10.1016/j. ins.2007.11.013. Y. Fang Chung, Z. Yu Wu and T. Shyong Chen. “Unconditionally secure cryptosystems based on quantum cryptography”. Information Sciences. Vol. 178 Nº 8, pp. 2044-2058. 15 de abril de 2008. DOI: 10.1016/j. ins.2007.11.013.

Título de la Investigación: Criptografía cuántica aplicada

Investigador: Jesús Martínez Mateo

Lugar de la Investigación: Universidad Politécnica de Madrid

Fecha: abril de 2008

Objetivo: Este proyecto de investigación estudio cada uno de los protocolos cuánticos y la implementación a nivel físico.

Criptografía Cuántica: Afirma que la criptografía cuántica no es sólo uso exclusivo de la Ingeniería, ya que puede englobar en otras ramas. Con la publicación de Stephen Wiesner en el año 1983 se llega a desarrollar el primer protocolo denominado BB84, en donde describe para crear billetes imposibles de falsificar, introduciendo un total de 20 trampas de luz en los billetes de 1 dólar, codificando en ellas los posibles valores con un fotón polarizado. La seguridad se lograría con el hecho de que el fotón en cada trampa de luz es polarizado con respecto a una base. Solo con el contenido de esa base se podría volver a recuperar el mismo estado de polarización de cada fotón sin obtener ningún error.

Implementación a nivel físico: Una de las primeras demostraciones prácticas realizada fue en el año 1989 por Charles H. Bennett y Hohn A. Smolin en el centro de investigación de IBM. En esta implementación fue utilizado el fotón como soporte y la polarización para la codificación de las informaciones. Este investigador afirma que esto no solo trató de un experimento científico sino también de un gran avance de la ingeniería para la elaboración del primer prototipo.

Componentes físicos utilizados para la implementación: Pulso láser atenuado, atenuador óptico variable (VOA), detector de fotones (Sistema QKD). El canal de comunicación fue la fibra óptica.

Recomendaciones: Consideraron la elección del lenguaje C + +, por la disponibilidad que tiene en la mayoría de sus plataformas y por su potencia, razón por la cual atendieron bastante para que la implementación sea compatible con distintas plataformas.

Principales Referencias:

https://scholar.google.com.py/scholar?q=%EF%83%98+C.+E.+Shannon,+%E2%80%9CCommunication+theory+of+secrecy+systems%E2%80%9D,+Bell+System+Technical+Journal,+Vol.+28,+1949.&hl=es&as_sdt=0&as_vis=1&oi=scholart

https://researcher.watson.ibm.com/researcher/view_person_pubs.php?person=us-wegman&t=1

https://www.sciencedirect.com/science/article/pii/0022000081900337

https://scholar.google.com.py/scholar?q=%EF%83%98+S.+Wiesner,+%E2%80%9CConjugate+Coding%E2%80%9D,+Sigact+News,+Vol.+15,+No.+1,+1983.&hl=es&as_sdt=0&as_vis=1&oi=scholart

https://core.ac.uk/download/pdf/82447194.pdf

https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.67.661

https://link.springer.com/article/10.1007/BF00191318

https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.68.557

https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.68.312

Título de la Investigación: Estado de la criptografía post-cuántica y simulaciones de algoritmos post-cuánticos.

Investigador: Álvaro Rodrigo Reyes Rosado

Lugar de la Investigación: Universidad Autónoma de Barcelona - Madrid

Fecha: diciembre del 2018

Objetivo: El objetivo de este proyecto de investigación es el estudio del estado de la criptografía post-cuántica y las simulaciones de algoritmos post-cuánticos.

Criptografía Cuántica: La criptografía cuántica es considerada una de las aplicaciones de la computación cuántica con mayor futuro, para poder evitar los ataques cibernéticos todo gracias a los efectos cuánticos en las comunicaciones y así poder detectar en el momento en el que se esté realizando un espionaje de terceros. A través de algoritmos cuánticos.

Conclusión: Con el desarrollo de esta investigación concluyen que muchas empresas están implementando algoritmos cuánticos. La criptografía cuántica necesita ser un tema de investigación e implementación en todo el mundo, ya que es considerada una de las aplicaciones del futuro. En este proyecto estudiaron a fondo todos los algoritmos cuánticos. También detallaron todas las universidades y laboratorios donde se está llevando a cabo investigaciones sobre la criptografía cuántica.

Recomendaciones: Seguir creando nuevos algoritmos cuánticos a futuro, imposibles de ser irrumpidos, analizando el escenario en el que se pueda seguir creando las computadoras cuánticas que si serían capaces de lograr quebrantar los algoritmos criptográficos.

Principales Referencias:

https://www.iis.sinica.edu.tw/papers/byyang/18988-F.pdf

https://www.nist.gov/sites/default/files/documents/2016/10/19/garcia-morchon-paper-lwc2016.pdf

https://nautil.us/blog/-how-classical-cryptography-will-survive-quantum-computers

https://people.maths.bris.ac.uk/~csxam/teaching/history.pdf

https://blogthinkbig.com/computacion-cuantica-record

https://www.researchgate.net/publication/282972925_Quantum_Cryptography_Trends_A_Milestone_in_Information_Security

https://www.quantumcommshub.net/news/phd-studentships-quantum-communications-post-post-quantum-cryptography-projects/

Título de la Investigación: Análisis de algoritmos criptográficos clásicos vs algoritmos cuánticos.

Investigador: Carmen Elena Mantilla Cabrera

Lugar de la Investigación: Escuela superior politécnica de Chimborazo - Ecuador

Fecha: enero 2018

Objetivo: Se realizó un análisis de comparación de los algoritmos criptográficos clásicos y los algoritmos criptográficos cuánticos.

Comparación de los algoritmos criptográficos: Para realizar la comparación entre ambos algoritmos, tanto tradicional como cuántico, en base a una profunda revisión bibliográfica, se optó por cuatro algoritmos tradicionales, realizando unas características más relevantes como número de datos de entrada, número de pasos de cifrado y descifrado y número de operaciones matemáticas y tres algoritmos cuánticos para la comparación de claves, las cuales fueron la unidad estructural de información, la tecnología aplicada y la detección de intrusos. Posterior a lo citado anteriormente realizaron una evaluación de los resultados obtenidos para la comprobación de hipótesis.

Ventajas de la Criptografía Cuántica a diferencia de la Criptografía Tradicional

- ✓ Posee métodos muy efectivos para la detección de posibles ataques, asegurando así la seguridad de los datos.
- ✓ La criptografía cuántica utiliza claves totalmente aleatorias (QKD), basadas en la mecánica cuántica por lo que no son previsible como la criptografía tradicional.
- ✓ Las claves de la criptografía cuántica no se pueden copiar, ya que el hecho de medir un sistema cuántico perturba el sistema eliminando así cualquier posibilidad de interceptación. Cumpliendo así el principio de incertidumbre de Heisenberg. En cambio, en la criptografía tradicional si se pueden copiar.

- ✓ Utiliza una partícula cuántica llamada qbit, la misma tiene una propiedad de permanecer en dos estados diferentes al mismo tiempo. En cambio, en la tradicional solo se puede representar un cero o uno.
- ✓ Con el avance de la tecnología de aquí a unos años la criptografía cuántica permitirá utilizar computadoras cuánticas que brindará seguridad teóricamente al 100%

Resumen: En dicha investigación se realizó una comparación de los algoritmos criptográficos y los algoritmos criptográficos que se conocen tradicionalmente. Desarrollaron un estudio técnico - económico para la implementación de un sistema cuántico para una infraestructura gubernamental del Consejo Nacional Electoral. Se constató con esta investigación que la criptografía cuántica es más apropiada para dicho propósito, con un método estadístico denominado CHI cuadrado.

Tipo de Investigación: La investigación fue mixta, utilizaron datos cualitativos y cuantitativos, de tipo documental ya que realizaron un estudio del arte.

Recomendaciones: Esta investigación deja como recomendación desarrollar un software que pueda permitir una simulación de la generación de claves cuánticos. También recomiendan realizar un seguimiento continuo a la investigación de los algoritmos de la criptografía cuántica, para una actualización de los resultados.

Principales Referencias:

Alexi, W. & Chor, B. (1988). RSA and Rabin functions:certeins parts are hard as the whole. Recuperado 28 de febrero de 2017, a partir de http://www.wisdom.weizmann.ac.il/~oded/X/acgs.pdf

Alayont, F. (2003). Cryptograph y and Cryptanalysis. Recuperado 1 de marzo de 2017, a partir de http://faculty.gvsu.edu/alayontf/talks/crypto.pdf

Beckman, B. (2002). Codebreakers. Arne Burgling and the Swedish Crypto Program during World War II. Recuperado 28 de febrero de 2017, a partir de https://mediatum.ub.tum.de/doc/1323891/1323891.pdf

Bennett, C., Bessette, F., Brassard, G., Salvail, L., & Smolin, J. (1992). Experimental quantum cryptography. Journal of Cryptology, 5(1), 3-28. https://doi.org/10.1007/BF00191318

Beth, Th. (1992). Public-Key Cryptography: State of the Art and Future Directions: E.I.S.S. Workshop, Oberwolfach, Germany.

INVESTIGACIONES LOCALES

Título de la Investigación: Discrete Variable Quantum Key Distribution: A Survey (Distribución de clave cuántica variable discreta).

Investigadores: Mathias Zavala y Benjamín Barán Cegla

Lugar de la Investigación: Universidad Católica Nuestra Señora de la Asunción, Universidad Nacional de Asunción, Universidad Comunera.

Objetivos:

- ✓ Realizar un survey para determinar el avance de QKD junto al protocolo BB84 durante los últimos 10 años
- ✓ Definir criterios de clasificación en base a la implementación teórica del protocolo
- ✓ Definir criterios de clasificación en base a la implementación práctica del protocolo.

QKD (Quantum Key Distribution): La distribución de claves cuánticas (Quantum Key Distribution - QKD) es un método de criptografía cuántica que consiste en la generación y distribución de claves. Dichas claves son compartidas entre las partes (Bob y Alice) con el objetivo de establecer una conexión incondicionalmente segura. (Mathias Zavala, 2021)

Resumen: Esta investigación se basa en una encuesta sobre la distribución de clave cuántica variable discreta. El protocolo BB84 ha sido ampliamente estudiado, por lo que ha alcanzado la madurez suficiente para tener soluciones disponibles en el mercado. Sin embargo, aún quedan ciertos obstáculos que dificultan su adopción en masa. Unas variadas gamas de técnicas han sido utilizadas para mejorar el rendimiento del protocolo en implementaciones reales. Este trabajo revisa el progreso realizado durante los últimos 10 años.

Resultados: Se realizaron tablas comparativas sobre los temas analizados, teniendo en cuenta criterios como el tipo de tema y año de publicación. Posterior a esto, se realiza una clasificación en base a criterios que corresponden a la implementación teórica y práctica del protocolo BB84. En cuanto a la implementación teórica, se identifican seis dimensiones distintas. Por otra parte, se identifican otras cinco dimensiones con respecto a la implementación práctica.

Conclusión: En las implementaciones actuales con el protocolo BB84 se encuentran muy lejos los requerimientos para lograr una adopción de un esquema de cifrado. Sin embargo, se puede llegar a utilizar las claves generadas en aplicaciones de menor envergadura. También técnicas como Dense Wavelenght Division Multiplexing paradigmas como Quantum Networking.

Principales Referencias:

Arash Bahrami.

Quantum key distribution integration with optical dense wavelength division multiplexing: a review. IET Quantum Communication, 1:9--15(6), July 2020.

Charles H. Bennett and Gilles Brassard.

Quantum cryptography: Public key distribution and coin tossing.

Theoretical Computer Science, 560:7–11, Dec 2014.

G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi,

T. Ferreira da Silva, G. B. Xavier, and G. Lima.

High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers.

Phys. Rev. A, 96:022317, Aug 2017.

Eleni Diamanti, Hoi-Kwong Lo, and Zhiliang Yuan.

Practical challenges in quantum key distribution.

npj Quantum Information, 2(1):16025, 2016.

Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki.

Secure quantum key distribution.

Nature Photonics, 8(8):595--604, 2014.

A. Sharma and A. Kumar.

A survey on quantum key distribution.

In 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), volume 1, pages 1--4, 2019

CAPÍTULO III

3. MARCO TEÓRICO

3.1. ACERCAMIENTO HISTÓRICO DE LA CRIPTOGRAFÍA CUÁNTICA

Las leyes de la física dicen que la criptografía cuántica es inquebrantable. No es en la carrera armamentista interminable. Entre los guardas secretos y los descifradores de códigos, las leyes de la mecánica cuántica parecían tener el potencial de darles la ventaja a los guardianes secretos. Una técnica llamada criptografía cuántica puede, en principio, permitirle encriptar un mensaje de tal manera que nunca sea leído por alguien cuyos ojos no sean para él.

Entra en la fría y dura realidad. En los últimos años, se ha demostrado que los métodos que alguna vez se consideraron fundamentalmente irrompibles son todo lo contrario. Debido a los errores de la máquina y otras peculiaridades, incluso la criptografía cuántica tiene sus límites.

Si lo construyes correctamente, ningún hacker puede hackear el sistema. La pregunta es qué significa construirlo correctamente ", dijo el físico Renato Renner, del Instituto de Física Teórica de Zúrich, quien presentará una charla sobre el cálculo de la tasa de falla de los diferentes sistemas de criptografía cuántica en la Conferencia de 2013 sobre láser y electroóptica. En San José, California, el 11 de junio.

El cifrado regular no cuántico puede funcionar de varias maneras, pero generalmente un mensaje se codifica y solo se puede descifrar usando una clave secreta. Romper la clave privada en un sistema criptográfico moderno generalmente requeriría descubrir los factores de un número que es el producto de dos números primos increíblemente enormes . Los números se eligen para que sean tan grandes que, con la potencia de procesamiento dada de las computadoras, un algoritmo tardaría más que la vida útil del universo en factorizar su producto.

Pero tales técnicas de encriptación tienen sus vulnerabilidades. Algunos productos, denominados claves débiles, resultan ser más fáciles de factorizar que otros. Además, la Ley de Moore aumenta continuamente el poder de procesamiento de nuestras computadoras. Aún más importante, los matemáticos están desarrollando constantemente nuevos algoritmos que permiten una factorización más fácil.

La criptografía cuántica evita todos estos problemas. La clave está encriptada en una serie de fotones que pasan entre dos puntos que intentan compartir información secreta. El Principio de incertidumbre de Heisenberg dicta que un adversario no puede mirar estos fotones sin cambiarlos o destruirlos.

En este caso, no tiene mucha importancia qué la tecnología tenga el adversario, nunca podrán violar las leyes de la física, dijo el físico Richard Hughes del Laboratorio Nacional de Los Alamos en Nuevo México, que trabaja en criptografía cuántica.

Pero en la práctica, la criptografía cuántica viene con su propia carga de debilidades. Se reconoció en 2010, por ejemplo, que un pirata informático podría cegar un detector con un pulso fuerte , por lo que no podría ver los fotones que guardan secretos.

Renner señala muchos otros problemas. Los fotones a menudo se generan usando un láser sintonizado a una intensidad tan baja que produce un solo fotón a la vez. Existe una cierta probabilidad de que el láser produzca un fotón codificado con su información secreta y luego un segundo fotón con esa misma información. En este caso, todo lo que un enemigo tiene que hacer es robar ese segundo fotón y podría obtener acceso a sus datos sin que usted sea más sabio.

Alternativamente, notar cuándo ha llegado un solo fotón puede ser complicado. Es posible que los detectores no registren que una partícula los golpeó, lo que le hace pensar que su sistema ha sido pirateado cuando es realmente bastante seguro. (Sandberg, 2013)

3.2. EVOLUCIÓN DE LA CRIPTOGRAFÍA

La evolución de los algoritmos criptográficos llevó a la aparición de los sistemas de clave asimétrica. Estos utilizan un mecanismo de claves que permite el intercambio de información sin que se requiera compartir la clave de forma previa**.** Este sistema utiliza dos elementos, uno privado y uno público.

El privado lo guardamos en un lugar seguro, y el público se muestra a todo el mundo para que puedan interactuar con nosotros. La peculiaridad de este sistema es que, para

cada persona, existen un par claves, y cuando se quiere enviar información a alguien, se requiere primero su clave pública, se genera el mensaje cifrado y se envía a la persona. Está podrá recuperarlo utilizando su clave privada.

Una manera sencilla de entenderlo es imaginar la clave privada como una llave, y la clave pública como una caja que solo se abre con esta llave. Si nosotros queremos que nos envíen mensajes, dejamos cientos de cajas (todas iguales) en diversos lugares. De esta manera, cualquier persona podrá ir, coger nuestra caja (que no vale nada de momento, es una caja vacía), introducir el mensaje que nos quiera hacer llegar y cerrarla. En el momento en que se cierra, ya solo nosotros con nuestra llave maestra podemos abrir la caja, así, quien nos envía el mensaje puede enviar la caja de la forma que quiera y estar seguro de que solo nosotros seremos capaces de abrirla.

La mayor ventaja de la criptografía asimétrica es que la distribución de claves es más fácil y segura ya que la clave que se distribuye es la pública manteniéndose la privada para el uso exclusivo del propietario, pero este sistema tiene bastantes desventajas:

- ✓ Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
- ✓ Las claves deben ser de mayor tamaño que las simétricas (generalmente son cinco o más veces de mayor tamaño que las claves simétricas).
- ✓ El mensaje cifrado ocupa más espacio que el original.

Los nuevos sistemas de clave asimétrica basado en curvas elípticas tienen características menos costosas. En el mundo de las criptomonedas esta es la opción más usada para garantizar que la información compartida está bien protegida. Esto gracias al uso de ECDSA y más específicamente de las curva secp256k1.

- ✓ Entre las principales características de este sistema podemos mencionar:
- ✓ La clave pública debe ser conocida por todo el mundo, pero la clave privada sólo debe conocerla su propietario.
- ✓ A partir del conocimiento de la clave pública o del texto cifrado no se puede obtener la clave privada.
- ✓ Lo que se cifra con una clave, sólo puede descifrarse con la otra.

- ✓ Cualquiera puede cifrar un mensaje con la clave pública, pero sólo el propietario de la clave privada puede descifrarlo.
- ✓ Proporciona confidencialidad.
- ✓ Si el propietario de la clave privada cifra con ella un mensaje, cualquiera puede descifrarlo con la correspondiente clave pública.
- ✓ Proporciona integridad, autenticación y no repudio. (Maldonado, 2019)

3.3. LA CRIPTOGRAFÍA

La criptografía es conocida como la técnica que protege documentos y datos. La criptografía funciona con la utilización de cifras o códigos para escribir algo que solo tú debes de saber en documentos y datos confidenciales que circulan en redes locales o en internet.

Después de la evolución de las computadoras convencionales, la criptografía fue conocida, trabajada y modificada, creándose así con los algoritmos matemáticos.

La criptografía preserva la integridad de la web, la autenticación del usuario, así como también la del remitente, el destinatario y de la actualidad del mensaje o del acceso.

3.4. TIPOS DE CLAVES CRIPTOGRÁFICAS

- ✓ **Criptografía de llave única:** La criptografía de llave única usa siempre una misma llave tanto para codificar como para decodificar mensajes. A pesar de que este método es bastante eficiente en relación al tiempo de procesamiento, o sea, el tiempo que gasta para codificar y decodificar mensajes, tiene como principal desventaja la necesidad de utilización de un medio seguro para que la llave pueda ser compartida entre personas o entidades que deseen intercambiar información criptográfica.
- ✓ **Criptografía de llaves pública y privada**: La criptografía de llaves pública y privada utiliza dos llaves distintas, una para codificar y otra para decodificar mensajes. Con este método cada persona o entidad mantiene dos llaves: una pública, que puede ser divulgada libremente, y otra privada, que debe ser mantenida en secreto por su dueño. Los mensajes codificados con la llave

pública sólo pueden ser decodificados con la llave privada. (Tecnología Informática, 2020)

3.5. LA CRIPTOGRAFÍA CUÁNTICA

La criptografía cuántica es una de las aplicaciones más importantes, también conocida como unas de las primeras aplicaciones de interés comercial de la mecánica cuántica. La computación cuántica se empezó a desarrollar en la década de los ochenta a raíz de las propuestas de Deutsch y Feymann, que sugirieron independientemente que la propia evolución de los sistemas cuánticos se podría utilizar como herramienta de cálculo. En 1994 aparece el primer resultado verdaderamente importante en computación cuántica. Se trata de los algoritmos polinomiales para la factorización de números enteros y cálculo de logaritmos discretos propuestos por P. Shor que abren la posibilidad de que los ordenadores cuánticos puedan romper los criptosistemas de clave pública.

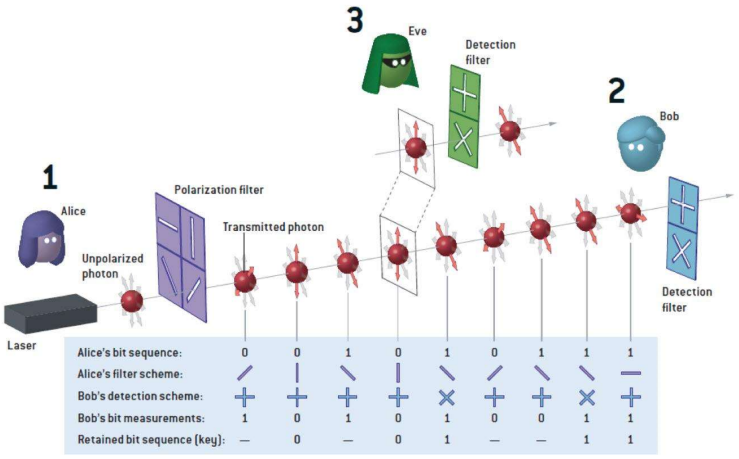

Ilustración 2: Principio físico en el cual se fundamenta la criptografía cuántica

Nota.Adaptado Cinvestav Queretaro [Fotografía] por Laboratorio Bx. Tecnologías para comunicaciones avanzadas(http://qro.cinvestav.mx/slabs/edificio-b/232-laboratorio-bx-tecnologias-cuanticas-para-comunicaciones-avanzadas).

Sabemos que la codificación usando claves privadas aleatorias de un solo uso (cifrado de Vernam) permite llevar a cabo una comunicación segura. Pero presenta la dificultad práctica de la distribución segura de las claves. Las leyes de la mecánica cuántica ofrecen herramientas para sobrellevar este problema. La aportación cuántica a la seguridad del proceso de distribución de claves consiste principalmente en que un espía no puede extraer información sin revelar su presencia a los comunicantes, de acuerdo a las leyes de la mecánica cuántica no es posible copiar estados. Hay diversos protocolos para la distribución cuántica de claves privadas. El más sencillo fue propuesto en 1984 por C.H. Bennett y G. Brassard que se conoce como BB84. Después se propusieron diversas modificaciones que dan lugar a otros protocolos esencialmente equivalentes. (Lacalle, 2015)

La criptografía cuántica usa la física para desarrollar un criptosistema completamente seguro para evadir verse comprometido si se desconoce el remitente o del destinatario del mensaje. Una de las acepciones de la palabra hace referencia a la conducta más fundamental de las partículas más pequeñas de la materia y la energía. La criptografía cuántica es distinta de los sistemas criptográficos tradicionales porque depende más de la física que de las matemáticas, como un aspecto clave de su modelo de seguridad.

En esencia, la criptografía cuántica se basa en el uso de partículas luminosas (fotones) individuales y sus propiedades cuánticas intrínsecas para desarrollar un criptosistema inquebrantable, cabe destacar que el estado cuántico es imposible de medir si haberlo perturbado. La criptografía cuántica usa fotones para transmitir una clave. Una vez transmitida la clave, se puede codificar y encriptar mediante el método normal de clave secreta. (Banafa, 2015)

3.6. CONCEPTOS DE FÍSICA CUÁNTICA USADOS EN CRIPTOGRAFÍA

En 1927, Werner Heisenberg encontró un principio fundamental de la mecánica cuántica que lleva su nombre: el principio de incertidumbre de Heisenberg. La misma dice que algunos pares de propiedades físicas están relacionados de tal forma que cuando se adquiere información sobre una de ellas, se reduce la información que se puede extraer sobre la otra. Este es el caso de la posición de las partículas y el momentum: cuando se mide la posición con exactitud, esto hace que la medición del momentum tenga menos certeza, y viceversa.

En el caso específico de la criptografía cuántica, en el que es necesario medir la polarización de los fotones, la elección sobre qué dirección medir afecta todas las medidas que se realizarán después. A continuación, se presenta un ejemplo descrito por Salvatore Vittorio en el artículo Quantum Cryptography: Privacy Through Uncertainty, publicado en 2002 [CSA].

3.7. POLARIZACIÓN DE UN FOTÓN

Los fotones son el mejor recurso para transportar información cuántica a largas distancias, son partículas que no tienen carga eléctrica. En la polarización lineal, el campo eléctrico del fotón se mantiene en el mismo plano, en cambio en la polarización circular, la luz del campo eléctrico rota a cierta frecuencia mientras el fotón se propaga. La criptografía cuántica puede implementarse con cualquiera de estos dos casos, o con una combinación de ellos. (Clearwater, 1998)

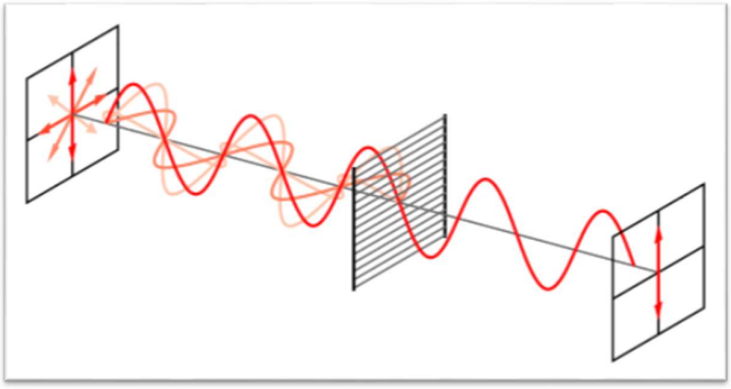

Ilustración 3: En la luz polarizada la oscilación del campo magnético o eléctrico del fotón sólo está orientado en una dirección, a diferencia de la que produce una fuente luminosa común.

Nota.Adaptado Panorama del Henares [Fotografía] Agosto 01, 2018 (https://www.panoramahenares.com/2018/08/criptografia-cuantica-en-que-consiste.html).

3.8. QUBITS

Un qubit, a groso modo, es un bit, implementado mediante algún observable, como el spin, de un sistema cuántico. Elegimos lógica de dos estados, como en computación electrónica, así que aprovechamos sistemas de dos niveles. Esto nos hace favorables al uso de partículas de spin 1/2, como electrones. Es importante observar que elegir spin semientero nos lleva a estados antisimétricos. Los qubits no se pueden medir como los bits, en el sentido descrito por el postulado de la medida de la mecánica cuántica. Un estado que no podemos medir sin alterarlo parece que no nos sirve de mucho. Esta es una dificultad a la que nos enfrentamos, y para la que existen respuestas. Por otra parte, cada nuevo bit duplica el número de estados posibles codificables, mientras que cada nuevo qubit aumenta al doble la dimensión del espacio en el que existen los estados con los que hacemos los cálculos. En ausencia de requisitos de simetría esto supone una infinidad de nuevos estados. (Miranda, 2014)

La diferencia entre el bit convencional y el qubit cuántico es que el primero solo puede entregar resultado binario (0,1), mientras la segunda aprovecha las propiedades de la mecánica cuántica que puede tener ambos valores al mismo tiempo, lo que le permite una mayor velocidad de procesamiento.

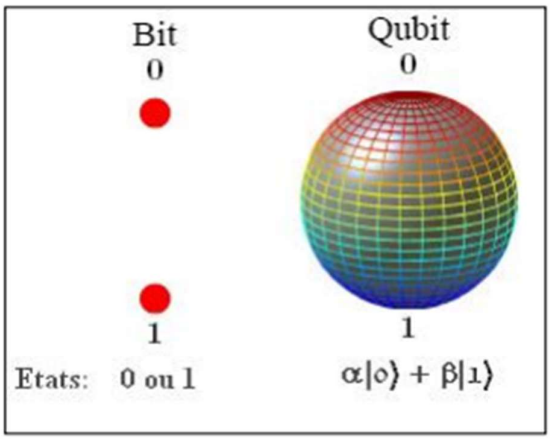

Ilustración 4: Se observa en el gráfico el bit y el qbits

Nota.Adaptado Steemit [Fotografia] por Quantum computers 2019 (https://steemit.com/bitcoin/@libertarianec/quantum-computers).

3.9. TEOREMA DE NO-CLONACIÓN

Significó un avance fundamental para el desarrollo tanto de la teoría de información cuántica como de la criptografía cuántica. Si fuera posible para un espía copiar los estados cuánticos mientras viajan del emisor al receptor, la criptografía cuántica no tendría sentido Quantum Computation and Quantum Information (Chuang, página 532)

El teorema de no clonado asegura que no existe ningún procedimiento por el cual pueda copiarse en el estado cuántico de un sistema a otro sistema idéntico. En contrapartida, el teorema de no clonado es esencial para la criptografía cuántica, ya que asegura que es imposible que un tercer observador (espía) copie la señal que las dos partes amigas intercambian entre sí. Así, pues, si el emisor del mensaje cifrado se asegura que cada bit cuántico se envía tan sólo una vez (una sola copia del sistema cuántico que transporta el mensaje), la criptografía cuántica es infalible. (La web de física, 2004)

3.10. PROTOCOLO E91

La criptografía es una disciplina que permite generar un mensaje que no puede ser descifrado por personas no autorizadas, dentro del amplio campo de la criptografía cuántica se encuentra el criptoanálisis que es conocida como el estudio de métodos para recuperar el significado de un mensaje cifrado sin tener acceso a la información secreta que es normalmente requerida para poder recuperar la información. Para poder generar este mensaje secreto se tiene que utilizar un algoritmo para combinar el mensaje original a transmitir una clave adicional y así poder producir lo que se denomina criptograma. Dicha técnica es considerada como una encriptación. Para que un criptosistema sea seguro debe de ser imposible obtener la información sin la clave.

Existen dos tipos de criptosistemas, dependiendo si el emisor y el receptor usan la misma clave. Un algoritmo que fue propuesto por Diffie y Hellman que consiste en utilizar diferentes claves

El protocolo E91 o protocolo EPR propuesto por Artur Ekert en 1991, Este protocolo está basado en el entrelazamiento de pares de fotones.

El esquema de comunicación es similar al del protocolo BB84. La diferencia es que se necesita además una fuente que produzca una serie de pares de fotones entrelazados. Dicha fuente puede estar en manos de Alice, Bob o algún tercero, lo importante es que, de cada par de fotones entrelazados producidos, un fotón llegue a Alice y el otro a Bob.

Los posibles estados a los que puede colapsar un qubit:

Por lo que cuando dos qubits están entrelazados, una vez realicemos una medida, ambos qubits colapsan al mismo valor.

Se supone que la primera persona quiere enviar información a una segunda persona; para ello se genera una secuencia de qubits entrelazados y cada uno de nuestros comunicadores puede enviar uno de los pares. Una vez ambos estén en comunicación,

no importa quién haga primero la medida porque al estar entrelazados ambos obtendrán el mismo valor aleatorio.

Al igual que en otros protocolos, la medida de un qubit se puede expresar en distintas bases. En este caso, renombramos "x" y "+" para distinguirlas.

El procedimiento consta de 3 pasos:

Primer paso: Se origina una secuencia de qubits entrelazadas parra Alice y Bob

Segundo paso: Alice y Bob eligen de manera independiente una secuencia de bases para medir la serie. (htt1)

	Medición 1	Medición 2	Medición 3	Medición 4	Medición 5	Medición 6
Esquema de Alice[6]	⊕	⊘	⊖	⊕	⊕	⊘
Partículas de Alice	$\|\downarrow\rangle$	$\|\uparrow\rangle$	$\|\downarrow\rangle$	$\|\uparrow\rangle$	$\|\uparrow\rangle$	$\|\downarrow\rangle$
Esquema de Bob[6]	⊕	⊘	⊘	⊘	⊕	⊘
Partículas de Bob	$\|\uparrow\rangle$	$\|\downarrow\rangle$	$\|\uparrow\rangle$	$\|\downarrow\rangle$	$\|\downarrow\rangle$	$\|\uparrow\rangle$
Coincidencias en las Bases	✓	✗	✗	✗	✓	✓
Clave	0				1	0

Ilustración 5: Protocolo E91

Nota.Adaptado ResearchGate [Fotografia] por Luis Marco Cáceres Alvarez abril 2015 (https://www.researchgate.net/figure/Figura-4-Ejemplo-de-Comunicacion-del-Protocolo-E91_fig2_282821048)

Sabemos que la codificación usando claves secretas aleatorias de un solo uso (one time pad) [8] permite llevar a cabo una comunicación segura, pero presenta la dificultad práctica de la distribución segura de las claves. Afortunadamente, las leyes de la mecánica cuántica proporcionan herramientas para abordar el problema de la distribución segura de claves secretas. La contribución cuántica a la seguridad del proceso consiste esencialmente en que un espía no puede extraer información sin revelar su presencia a los comunicantes, ya que por las leyes de la mecánica cuántica no es posible copiar estados.

Existen diversos protocolos para la distribución cuántica de claves secretas. En un proceso de distribución cuántica de claves, intervienen un emisor y un receptor y dos canales de comunicación, uno cuántico para enviar fotones u otras partículas

subatómicas y otro clásico y posiblemente público para conciliar y depurar la información. Los dos comunicantes usan un trozo de su clave para detectar la presencia de espías. Un posible espía puede acceder al canal clásico, y también puede acceder al canal cuántico y usar todos los medios que desee con la única restricción de que sean compatibles con las leyes de la mecánica cuántica.
Este protocolo criptográfico fue desarrollado por Artur Ekert en 1991 y se encuentra basado en el Teorema de Bell [13]. El protocolo E91 utiliza fotones entrelazados. Estos pueden ser preparados por Alice, Bob o algún tercero, y son distribuidos de manera que Alice y Bob tengan un fotón de cada par. El modelo se fundamenta en propiedades del entrelazamiento cuántico.

A pesar de que muchas cantidades físicas (observables) pueden ser utilizadas para explicar la creación del entrelazamiento cuántico, Ekert utiliza los estados cuánticos llamados singlet de spin.

El entrelazamiento cuántico es la incapacidad para definir el estado cuántico de un objeto sin referenciar al estado cuántico de otro objeto, el cual puede estar o no, alejado especialmente del primero. Aunque no se pueden establecer conclusiones acerca de los estados individuales de los objetos, el estado cuántico de ambos objetos está bien definido.

A continuación, se detalla paso a paso el funcionamiento del protocolo de acuerdo al trabajo original de 1991, el siguiente pseudocódigo detalla el proceso completo de generación e intercambio de claves:

1. Alice le indica a la fuente la longitud de la clave.
2. La fuente crea todos los pares entrelazados.
3. La fuente comienza el envío de partículas entrelazadas en paralelo hacia Alice y Bob
4. A medida que van llegando las partículas entrelazadas, Alice y Bob generan una base de forma aleatoria e independiente entre ellos.
5. Una vez terminado el envío de los pares entrelazados desde la fuente a Alice y a Bob, la fuente le envía una señal a Alice y a Bob comunicándose el hecho.
6. Una vez recibida la señal por parte de la fuente, Alice y Bob comienzan el intercambio de sus respectivas bases.

7. Cuando finaliza el envío de las bases de ambos participantes, Alice y Bob se disponen a comparar sus propias bases con las bases del otro.
8. Se forman 2 grupos de datos, el primer grupo corresponde a aquellos donde se detectan bases contrarias y el segundo grupo aquellas en que se utilizan las mismas bases.
9. El primer grupo es descartado, ya que para efecto de esta simulación no es necesario su utilización.
10. El segundo grupo, las cuales corresponde a aquellas donde Alice y Bob utilizaron las mismas bases, su anti correlación está demostrada, así que se dispone a la medición de las partículas entrelazadas que se encuentra almacenada en la misma posición que la base (por parte de Alice y de Bob).
11. Las medidas obtenidas se pueden convertir en una cadena secreta de bits o sea la clave. Está clave secreta puede entonces ser utilizada en una comunicación criptográfica convencional entre Alice y Bob.

Para detectar si Eve (intruso) ha estado espiando en la comunicación, Alice y Bob comparan las claves rechazadas (primer grupo que corresponden a aquellos donde se detectan bases contrarias). Debido al hecho de que Eve tiene que realizar una medición sobre una de las partículas del par entrelazado para poder leer la información pertinente a la comunicación, ella rompe las propiedades propias del entrelazamiento y luego al comprobar la presencia de intrusos utilizando la desigualdad de Bell, se produce la detección de Eve en la comunicación, de manera oportuna.

3.11. PROTOCOLO BB84

El protocolo BB84 ha sido el primer codificador cuántico de la información clásica que se propuso de tal forma que el receptor, pudiese recuperar con un 100% de confidencialidad.

Fue propuesto por Bennett y Brassard en la International Conference on Computers, Systems and Signal celebrada en Los Álamos, California, durante el año 1984. En la propuesta original la propiedad en la que se codifica la información que transporta el fotón es la polarización. Esta propiedad describe en qué plano vibra el campo electromagnético en la dirección de propagación del haz. Si hacemos pasar un fotón con una polarización α a través de un filtro polarizador con una orientación β, el

fotón pasará cambiando su polarización a β con probabilidad cos2 (α − β), o será absorbido con la probabilidad complementaria, sin2 (α − β). Si las diferencia α − β es exactamente 90º el fotón nunca pasa, y si es 0º pasa siempre sin ver afectada su polarización. Si la diferencia es de 45º, la mitad de las veces pasa adquiriendo una polarización β, y la otra mitad de veces es absorbido. Habitualmente se usan dos bases de polarización, una la horizontal-vertical (B+), y otra oblicua o diagonal (B×). En la base B + tomamos como bit lógico 1 al qubit con estado de polarización vertical, y como 0 al horizontal. Una elección semejante se hace en el caso de la base oblicua, con el 1 a 45º y el 0 a 135º. Si preparamos un fotón en horizontal y lo medimos en la base diagonal, la mitad de las veces obtenemos 1 y la otra mitad 0. Lo mismo ocurre con un fotón preparado como 1 en la base B× que es medido en la base B +, la mayor parte de las veces se obtiene el resultado correcto y la otra mitad el incorrecto. La única forma de obtener con certeza cuál era el estado original es conocer en qué base fue preparado y hacer la medición en la misma, el protocolo BB84 se mide con respecto a la propagación.

El protocolo BB84 está formado por 4 estados cuánticos.

1. Alice genera una secuencia de valores aleatorios que corresponderá con la clave que desea intercambiar con Bob.

2. Alice genera otra secuencia aleatoria, ahora con las bases que utilizará para la codificación de la clave generada en el paso anterior.

3. Alice codifica cada valor de la clave con la base correspondiente, y envía la secuencia de qubits a Bob.

4. Bob genera una secuencia aleatoria con las bases que utilizará para decodificar la secuencia de estados recibidos de Alice.

5. Bob mide cada estado recibido en la base correspondiente a la secuencia generada.

6. Bob envía a Alice la secuencia de bases utilizada a través de un canal público autenticado.

7. Alice compara la secuencia de bases que ha utilizado para codificación de la clave con la secuencia proporcionada por Bob en el paso anterior, quedándose sólo con aquellas mediciones para las que han coincidido ambas bases. 8. Alice y Bob comparten ahora una secuencia de valores formada por aquellos en los que las posiciones donde las bases de preparación y medición han coincidido.

9. Después de los puntos anteriores existe un pos proceso cuyo objetivo es estimar la presencia de un espía, corregir los errores, y amplificar la privacidad. Estos pasos siempre se ejecutan en un proceso de QKD, aunque formalmente no se consideren parte del protocolo BB84.

3.12. PROTOCOLO B92

En el año 1992, surge una propuesta de modificación del protocolo BB84 por Charles H. Bennett, que utiliza solo dos estados para la codificación de cada clave.

Este nuevo protocolo no posee grandes ventajas sobre su predecesor, el protocolo BB84, por lo que su interés no va más allá del académico. A pesar de esto, hemos querido presentarlo dado que, en su modo de trabajo podemos encontrar cierta similitud con el protocolo que describiremos a continuación, el SARG 04. Esa similitud viene dada por el hecho de que el protocolo no publica las bases utilizadas, sino parte del resultado obtenido. Protocolo basado en dos estados cuánticos, no ortogonales.

3.13. SEGURIDAD EN PROTOCOLO QKD (Quantum Key Distribution - QKD)

Los protocolos QKD llevan una seguridad única e incondicional que son las que proporcionan las leyes de la mecánica cuántica. El QKD usa la mecánica cuántica, aprovechando la noción de que la luz, entendida como una onda, puede comportarse también como una partícula. Así, los cables permiten explotar el comportamiento de las partículas de luz (fotones) y crear una especie de bits de información.

En cada extremo del cable, los sistemas QKD usan unos láseres para emitir información en las pulsaciones de luz y conducir esos datos a través del cable. Si alguna de las partes del cable por donde pasa la información es interceptada y ésta no llega en el nanosegundo que se espera, tanto el emisor como el receptor sabrán que la comunicación ha sido comprometida.

La mecánica cuántica crea una comunicación segura en la que cualquier individuo que esté a la escucha puede ser detectado, se lee en un informe sobre esta cuestión elaborado por la Comisión Europea.

A diferencia de la criptografía tradicional, que usa las matemáticas, el QKD usa la cuántica para crear códigos imposibles de romper.

El cable QKD bajo el túnel Holland fue desarrollado por Quantum Xchange, una empresa tecnológica pionera en cifrado inquebrantable y en computaciones cuánticas con base en Maryland, Estados Unidos.

La misión de la compañía, según explica en su sitio web, es darle a las empresas comerciales y agencias gubernamentales el mejor y más innovador sistema de defensa para mantener sus datos seguros hoy y en el futuro. (BBC NEWS , 2020)

3.14. DIFERENCIA DE BITS Y QUBITS

Bit: Acrónimo de Binary digit que significa dígito binario en español. Se corresponde con un dígito del sistema de numeración binario y representa la capacidad de almacenamiento de una memoria digital.

Qubit: se parece en cierta forma con un bit clásico ya que puede tener dos posibles valores 0 o 1; pero un bit puede ser 0 o 1 únicamente, y a diferencia un qubit puede ser 0, 1 o una superposición cuántica de ambos. Dos qubits pueden estar en cualquiera de los cuatro estados de superposición cuántica, y tres qubits en cualquiera de las 8 superposiciones.

Por lo que una computadora cuántica con N qubits, puede estar en una superposición cuántica arbitraria de 2 elevado a la N estados simultáneamente a diferencia de una computadora normal que solo puede estar en uno de esos 2 estados.

Las posibilidades son infinitas porque los qubits no expresan magnitudes discretas como los bits, sino continuas. Los grupos de qubits no solo permiten albergar una infinidad de valores, sino que hacen que la capacidad de procesar información de forma simultánea crezca exponencialmente

Con los qubit cada uno de sus procesos es independiente. por lo que en la computación clásica la resolución de problemas es lineal y la computación cuántica puede resolver más de una operación al mismo tiempo con el paralelismo de datos.

Un qubit es el elemento básico de la computación cuántica, también conocido como quantum bit por sus siglas en inglés.

El concepto de qubit es abstracto, no lleva asociado un sistema físico concreto. En la práctica, se han preparado diferentes sistemas físicos que, en ciertas condiciones,

pueden describirse como qubits o conjuntos de qubits. Los sistemas pueden ser macroscópicos, como una muestra de resonancia magnética nuclear o un circuito superconductor, o microscópico, como iones suspendidos mediante campos eléctricos o defectos cristalográficos en el diamante. (htt2)

CAPÍTULO IV

4. MARCO METODOLÓGICO

4.1. TIPO DE INVESTIGACIÓN

El tipo de investigación que se adoptó en este trabajo es el cuantitativo por la revisión bibliográfica, la recolección de datos, mediante la aplicación de herramientas como documentos, registros y materiales (Roberto Hernandez Sampieri, 2010)

Tipo documental, dado que es un proceso enfocado a la búsqueda, recopilación análisis críticos e interpretación de datos secundarios, es decir los datos obtenidos y registrados por otros investigadores en fuentes documentales. Con el fin de llevar a cabo el trabajo de grado se requiere de la metodología de revisión documental de este proyecto en el arte para la cual es indispensable hacer una recopilación de datos.

4.2. TIPOS DE ESTUDIO

El tipo de estudio será descriptivo, diseño no experimental. Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a un análisis. Miden, evalúan o recolectan datos sobre diversos aspectos, dimensiones o componentes del fenómeno a investigar. Desde el punto de vista científico, describir es recolectar datos. Esto es, en un estudio descriptivo se selecciona una serie de cuestiones y se mide o recolecta información sobre cada una de ellas, para así describir lo que se investiga. (Sampieri, 2008)

4.3. DISEÑO DE INVESTIGACIÓN

Se determinó el diseño de la investigación un análisis de la criptografía cuántica, se obtuvo como punto de inicio el análisis del estudio del arte sobre la criptografía cuántica que permitieron obtener resultados generales de la investigación.

4.4. OBSERVACIÓN

Se procedió a la utilización de la recolección de datos con la revisión bibliográfica, análisis de contenidos, que permitió conseguir las informaciones necesarias.

CAPÍTULO V
5. ANÁLISIS DE RESULTADOS

5.1 BENEFICIARIOS

De acuerdo al análisis que se venía realizando sobre la aplicación de la criptografía cuántica y teniendo en cuenta todos los fundamentos implantados en la investigación la misma beneficiará altamente a Ingenieros, matemáticos, físicos para un acercamiento a la Criptografía Cuántica, con el fin de motivar la investigación a nuevos desarrollos en el área y por sobre todo los mayores beneficiarios son las entidades tanto públicas como privadas que salvaguardan de una forma 100% segura sus informaciones.

5.2 ESPECIFICACIONES DE ACTIVIDADES Y TAREAS REALIZADAS

- ✓ Estudio bibliográfico de investigaciones realizadas por Universidades Internacionales
- ✓ Análisis de condiciones actuales
- ✓ Análisis de la factibilidad de la aplicación de la criptografía cuántica

5.3. BENEFICIOS

La aplicación de la criptografía cuántica metodológicamente a través de una revisión sistemática, puede alcanzar comunicaciones seguras utilizando leyes de la naturaleza a escala cuántica, como el principio de incertidumbre de Heisenberg, la superposición cuántica y el enmarañado cuántico, con el fin de motivar el uso de nuevas tecnologías para los próximos sistemas desarrollos en el área.

5.4. DIFERENCIA ENTRE LA CRIPTOGRAFÍA TRADICIONAL Y LA CRIPTOGRAFÍA CUÁNTICA

CRIPTOGRAFÍA TRADICIONAL	CRIPTOGRAFÍA CUÁNTICA
- Utiliza algoritmos matemáticos	- Utiliza principios de la mecánica cuántica
- Se transmite a través de bits (que puede ser 0 o 1)	- Se transmite a través de qubits(que puede ser 0 y 1 a la vez)

5.5. ANÁLISIS DE SELECCIÓN DE LA CRIPTOGRAFÍA CUÁNTICA EN LA SEGURIDAD DE INFORMACIONES

La criptografía cuántica es distinta de los sistemas criptográficos tradicionales porque depende más de la física que de las matemáticas, como un aspecto clave de su modelo de seguridad.

La criptografía cuántica utiliza la física para desarrollar un criptosistema completamente seguro para evitar verse comprometido si se desconoce el remitente o del destinatario del mensaje. Una de las acepciones de la palabra *cuanto* hace referencia a la conducta más fundamental de las partículas más pequeñas de la materia y la energía.

En esencia, la criptografía cuántica se basa en el uso de partículas/ondas luminosas llamadas fotones individuales y sus propiedades cuánticas intrínsecas para desarrollar un criptosistema inquebrantable.

Al principio se consideraba que la criptografía que se basaba en algoritmos matemáticos eran bastante seguras, pero ya después con la llegada de la internet que permitió la conexión de varias máquinas en línea, se pudo comprobar que la criptografía tradicional es bastante sencilla de penetrar, en cambio con la aplicación de la criptografía cuántica hasta hoy día no se ha podido demostrar que existe una vulnerabilidad ya que la misma utiliza fotones que cambian de estado que introducen errores en el proceso de comparación de bases lo que alerta al emisor y al receptor que los canales que están utilizando no son seguros.

Dicho esto, y de acuerdo al análisis realizado para la aplicación de la criptografía cuántica en la red óptica se puede afirmar que el mismo es mucho más seguro teniendo en cuenta que la prioridad principal es la de salvaguardar la información entre el emisor y receptor.

5.6. ANÁLISIS DE DATOS CUANTITATIVOS

5.6.1. Resumen de análisis cuantitativo de la confidencialidad de las informaciones aplicando la criptografía cuántica.

	RESULTADOS
Media	3
Mediana	3
Desviación estándar	3
Varianza del coeficiente	8
Rango	4
Investigaciones que no garantizan	1
Investigaciones que garantizan	5
Total de investigaciones	6
Cuenta	2

Fuente: Revisión Bibliográfica
Elaborado por: Gloria Acevedo, 2021

Ilustración 6: Tabla de resultados análisis de datos de confidencialidad

5.6.2. Resumen de análisis cuantitativo comparativo entre la criptografía cuántica y la criptografía tradicional.

	VENTAJAS		DESVENTAJAS
Media	5	Media	1
Error típico	0	Error típico	0
Mediana	5	Mediana	1
Rango	0	Rango	0
Mínimo	5	Mínimo	1
Máximo	5	Máximo	1
Total ventajas	5	Total desventajas	1
Cuenta	1	Cuenta	1

Fuente: Revisión Bibliográfica
Elaborado por: Gloria Acevedo, 2021

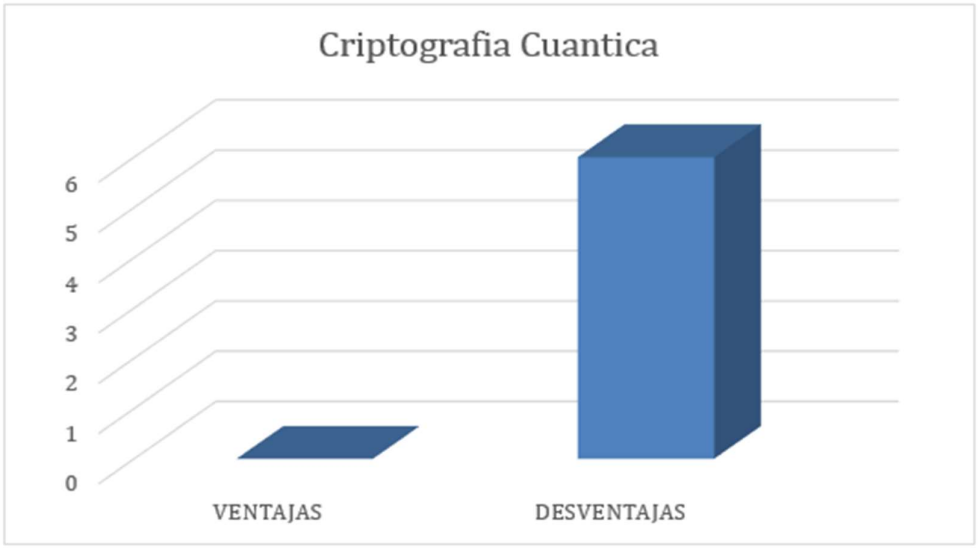

Ilustración 7: Tabla de resultados análisis de datos de ventajas y desventajas de la criptografía cuántica

	VENTAJAS		DESVENTAJAS
Media	0	Media	6
Error típico	0	Error típico	0
Mediana	0	Mediana	6
Rango	0	Rango	0
Mínimo	0	Mínimo	6
Máximo	0	Máximo	6
Total ventajas	0	Total desventajas	6
Cuenta	1	Cuenta	1

Fuente: Revisión Bibliográfica

Elaborado por: Gloria Acevedo, 2021

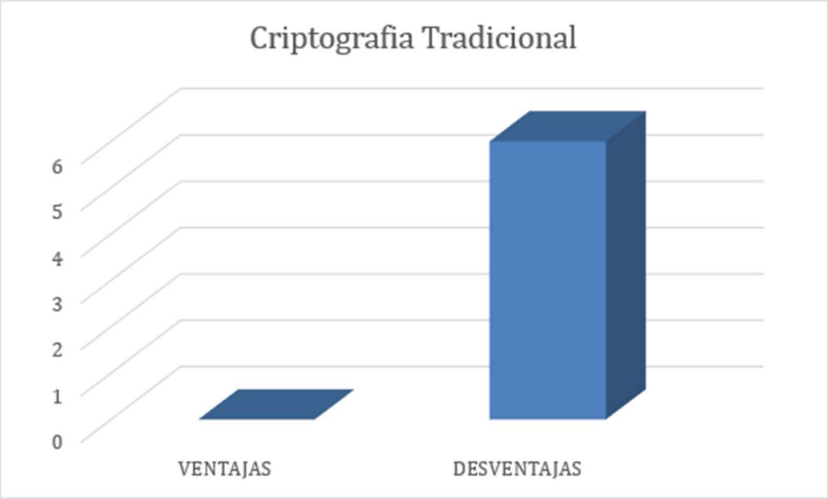

Ilustración 8: Tabla de resultados análisis de datos de las ventajas y desventajas de la criptografía tradicional.

5.6.3. RESUMEN DE ANÁLISIS CUANTITATIVOS DE PROTOCOLOS CRIPTOGRÁFICOS.

	RESULTADOS
Media	2
Mediana	2
Desviación estándar	2
Rango	4
Mínimo	0
Maximo	4
Suma	6
Cuenta	3

Fuente: Revisión Bibliográfica

Elaborado por: Gloria Acevedo, 2021

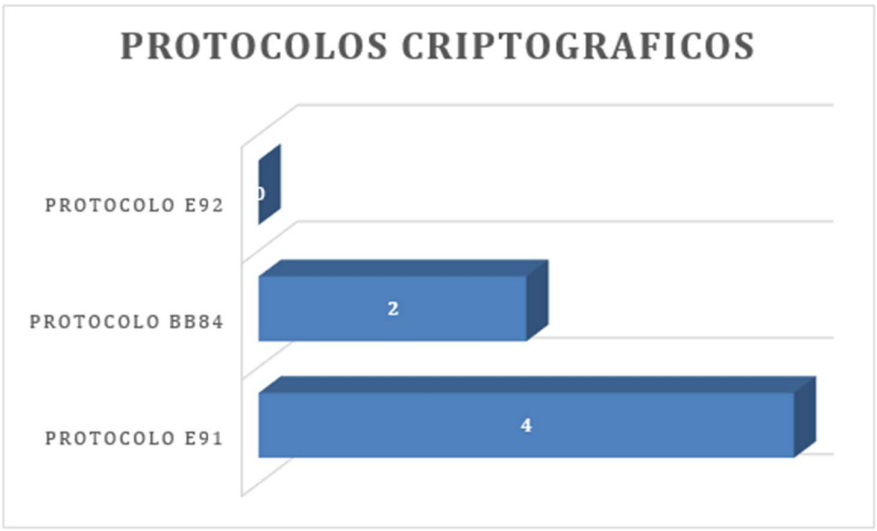

Ilustración 9: Tabla de resultados análisis de datos de los protocolos criptográficos cuantitativos.

En la ilustración 8 se observa que el protocolo E91 es considerada una de las más seguras hasta la fecha según la revisión bibliográfica realizada es el proyecto de investigación.

CAPÍTULO VI

6. CONCLUSION Y RECOMENDACION

6.1. CONCLUSIÓN

Este proyecto de investigación trata de la criptografía cuántica, una de las aplicaciones prácticas más fascinantes de la computación cuántica, que más avance tecnológico viene demostrando hasta la fecha. Tuvo como objetivo establecer un análisis de la criptografía cuántica en la seguridad de información.

Se estudió los diferentes protocolos cuánticos utilizados en la criptografía cuántica. El protocolo E91 un algoritmo que consiste en utilizar diferentes claves cuánticos, el protocolo BB84 que ha sido el primer codificador cuántico de la información clásica que está basado por cuatro estados cuánticos, el protocolo cuántico B92 que es una versión mejorada que la anterior, basada en dos estados cuánticos.

Estos dos últimos protocolos fueron propuestos de tal forma que el receptor pudiese recuperar con un 100% de confidencialidad.

Por más que la criptografía cuántica no sea muy practicada aún hoy en día en algunas regiones, es la rama de la computación cuántica que más presenta avances y que tiene implicaciones más severas en sus resultados. A diferencia de los sistemas criptográficos asimétricos, su seguridad ha sido demostrada 100% segura sin importar con qué recursos computacionales se cuente. Actualmente funciona entre distancias cortas. Con algo más de avance técnico, se logrará la implementación de redes de comunicación que transmitan mensajes secretos entre usuarios separados por distancias más largas. Las diferencias funcionales y conceptuales que presenta con otras técnicas criptográficas, dan mucho valor a la investigación y exploración de ideas nuevas para proteger la información.

.

6.2. RECOMENDACIONES

Durante el desarrollo de esta tesis, estudiando cada protocolo cuántico se recomienda utilizar el protocolo E91 debido a que intercambia el problema, almacena de manera segura una clave ya estipulada por mediciones con diferentes polarizadores, por el problema de almacenar estados cuánticos sin medirlos, es decir, en un estado de superposición o estado coherente. A diferencia del protocolo BB84, la clave debe ser almacenada clásicamente hasta que se va usar. Así que, aunque fue creada incondicionalmente segura, su seguridad al pasar el tiempo solo será tan grande como la seguridad de su almacenamiento.

Insto a nuestros investigadores de las diferentes Universidades públicas y privadas a que se animen a tomar la iniciativa de realizar este tipo de investigaciones sobre la criptografía cuántica y llevar a cabo su implementación a futuro.

REFERENCIAS

Mathias Zavala, B. B. (2021). *Sociedad Científica del Paraguay.* Obtenido de http://sociedadcientifica.org.py/

Roberto Hernandez Sampieri, C. F. (2010). Metodología de la Investigación.

Sampieri, R. H. (2008). Metodología de la Investigación.

La web de física. (2004). Obtenido de https://www.lawebdefisica.com/dicc/noclonat/#:~:text=2.2%20En%20la%20criptograf%C3%ADa%20cu%C3%A1ntica,amigas%20se%20intercambian%20entre%20si.

Lacalle, A. G. (2015).

Maldonado, J. (2019). Obtenido de https://www.bitcobie.com/evolucion-de-la-criptografia-y-su-futuro-en-la-blockchain/

Sandberg, A. (2013). Obtenido de https://www.wired.com/2013/06/quantum-cryptography-hack/

Tecnología Informática. (2020). Obtenido de https://www.tecnologia-informatica.com/que-es-la-criptografia/

Scientific Electronic Library Online, Ingeniare. Revista chilena de ingeniería (2015). Obtenido de

https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-33052015000200009

Anexo A

GLOSARIO DE TÉRMINOS

A

ATENUADOR ÓPTICO VARIABLE. VOA: El atenuador óptico variable (VOA) es un dispositivo diseñado para atenuar la señal óptica o un nivel de entrada de manera controlada, para producir una señal de salida con diversas intensidades de atenuación, se forman de una estructura de bloqueo entre una señal de entrada y una salida.

C

CRIPTOGRAFÍA: se define como la parte de la criptología que se ocupa de las técnicas, bien sea aplicadas al arte o la ciencia, que alteran las representaciones lingüísticas de mensajes, mediante técnicas de cifrado o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes. Por tanto, el único objetivo de la criptografía era conseguir la confidencialidad de los mensajes.

CRIPTOGRAFÍA CUÁNTICA: es la criptografía que utiliza principios de la mecánica cuántica para garantizar la absoluta confidencialidad de la información transmitida. La criptografía cuántica permite a dos personas crear, de forma segura una comunicación, con una propiedad única de la física cuántica para cifrar y descifrar mensajes. Utiliza como medio de transmisión los fotones. La criptografía cuántica como idea se propuso en 1970, pero no es hasta 1984 que se publica el primer protocolo.

F

FOTÓN: es la partícula elemental responsable de las manifestaciones cuánticas del fenómeno electromagnético. Es la partícula portadora de todas las formas de radiación electromagnética, incluyendo los rayos gamma, los rayos X, la luz ultravioleta, la luz visible (espectro electromagnético), la luz infrarroja, las microondas y las ondas de radio.

Q

QUBIT: un qubit o bit cuántico (quantum bit) es una unidad de información cuántica (la versión cuántica del tradicional bit) con dimensiones adicionales asociadas a las propiedades cuánticas de los átomos físicos. Un bit puede ser 0 o 1, un qubit puede ser 0, 1 o una superposición cuántica de ambos.