EXPLORACIÓN DE LAS POSIBILIDADES DE LA COMPUTACIÓN CUÁNTICA PARA LA CRIPTOGRAFÍA

EXPLORATION OF THE POSSIBILITIES OF QUANTUM COMPUTING FOR CRYPTOGRAPHY

EXPLORAÇÃO DAS POSSIBILIDADES DA COMPUTAÇÃO QUÂNTICA PARA A CRIPTOGRAFIA

Davide Silva[1]
tefo122004@gmail.com
https://orcid.org/0009-0006-0481-373X

Rosa Núñez[2]
rn5929170@gmail.com
https://orcid.org/0009-0009-3782-0778

Recibido: 25/10/23
Aceptado: 26/11/23
Publicado: 29/12/23

Correspondencia: tefo122004@gmail.com

1. Estudiante de Ingeniería en Tecnologías de la Información, Escuela Superior Politécnica de Chimborazo (ESPOCH).
2. Estudiante de Ingeniería en Tecnologías de la Información, Escuela Superior Politécnica de Chimborazo (ESPOCH).

RESUMEN

La investigación realizada tiene como objetivo explorar las posibilidades de la computación cuántica en el campo de la criptografía, identificando tanto oportunidades como desafíos significativos. Para ello, se adopta un enfoque metodológico mixto, integrando el análisis teórico y la revisión de literatura con estudios de casos y simulaciones computacionales. Los principales aportes teóricos de la investigación se centran en la identificación de las vulnerabilidades de los algoritmos criptográficos clásicos frente a la computación cuántica, así como en la exploración de enfoques innovadores en la criptografía post-cuántica que muestran promesa en la resistencia contra posibles ataques cuánticos. Además, se destaca el potencial transformador de la computación cuántica en la criptografía, como los sistemas de comunicación cuántica segura y los algoritmos de cifrado mejorados. La metodología empleada permite una exploración exhaustiva y multifacética de las posibilidades de la computación cuántica en el campo de la criptografía, abarcando tanto la teoría como la práctica. Se realiza una revisión sistemática de la literatura existente y se lleva a cabo un análisis detallado de los principios fundamentales de la computación cuántica, complementado con simulaciones computacionales. Los principales resultados de la investigación se dividen en varias categorías clave, reflejando tanto los avances teóricos como prácticos en este campo. Se ha identificado que los principios de la computación cuántica ofrecen nuevas dimensiones en la seguridad criptográfica, y se han explorado enfoques innovadores en la criptografía post-cuántica. Además, las aplicaciones prácticas de la computación cuántica en la criptografía demuestran el potencial transformador de esta tecnología. En conclusión, la investigación subraya la necesidad de una adaptación proactiva en el campo de la criptografía frente a los avances en computación cuántica, asegurando así la integridad y seguridad de la información en el mundo digital.

Palabras claves: computación; computación cuántica; criptografía.

ABSTRACT

The research carried out aims to explore the possibilities of quantum computing in the field of cryptography, identifying both significant opportunities and challenges. To achieve this, a mixed methodological approach is adopted, integrating theoretical analysis and literature review with case studies and computational simulations. The main theoretical contributions of the research focus on the identification of the vulnerabilities of classical cryptographic algorithms against quantum computing, as well as the exploration of innovative approaches in post-quantum cryptography that show promise in resistance against possible quantum attacks. . Additionally, the transformative potential of quantum computing in cryptography is highlighted, such as quantum secure

communication systems and improved encryption algorithms. The methodology used allows for a comprehensive and multifaceted exploration of the possibilities of quantum computing in the field of cryptography, encompassing both theory and practice. A systematic review of the existing literature is carried out and a detailed analysis of the fundamental principles of quantum computing is carried out, complemented by computational simulations. The main research results are divided into several key categories, reflecting both theoretical and practical advances in this field. The principles of quantum computing have been identified as offering new dimensions in cryptographic security, and innovative approaches have been explored in post-quantum cryptography. Furthermore, practical applications of quantum computing in cryptography demonstrate the transformative potential of this technology. In conclusion, the research highlights the need for proactive adaptation in the field of cryptography in the face of advances in quantum computing, thus ensuring the integrity and security of information in the digital world.

Key words: computing; quantum computing; cryptography.

RESUMO

A pesquisa realizada tem como objetivo explorar as possibilidades da computação quântica no campo da criptografia, identificando tanto oportunidades quanto desafios significativos. Para isso, adota-se uma abordagem metodológica mista, integrando análise teórica e revisão de literatura com estudos de casos e simulações computacionais. Os principais contributos teóricos da pesquisa concentram-se na identificação das vulnerabilidades dos algoritmos criptográficos clássicos diante da computação quântica, bem como na exploração de abordagens inovadoras na criptografia pós-quântica que mostram promessa na resistência contra possíveis ataques quânticos. Além disso, destaca-se o potencial transformador da computação quântica na criptografia, como os sistemas de comunicação quântica segura e algoritmos de criptografia aprimorados. A metodologia utilizada permite uma exploração abrangente e multifacetada das possibilidades da computação quântica no campo da criptografia, abrangendo tanto a teoria quanto a prática. É realizada uma revisão sistemática da literatura existente e é conduzida uma análise detalhada dos princípios fundamentais da computação quântica, complementada por simulações computacionais. Os principais resultados da pesquisa são divididos em várias categorias-chave, refletindo avanços tanto teóricos quanto práticos nesse campo. Identificou-se que os princípios da computação quântica oferecem novas dimensões na segurança criptográfica, e foram exploradas abordagens inovadoras na criptografia pós-quântica. Além disso, as aplicações práticas da computação quântica na criptografia demonstram o potencial transformador dessa tecnologia. Em conclusão, a pesquisa destaca a necessidade de uma adaptação proativa no campo da criptografia diante dos avanços na computação

quântica, assegurando assim a integridade e segurança da informação no mundo digital.

Palavras-chave: computação; computação quântica; criptografia.

1. INTRODUCCION

La emergencia de la computación cuántica representa un hito revolucionario en el campo de la tecnología de la información, redefiniendo los paradigmas existentes y abriendo un abanico de posibilidades inéditas. Este avance tecnológico, caracterizado por su capacidad para procesar información a escalas exponenciales en comparación con los sistemas computacionales clásicos, ha capturado la atención de la comunidad científica, especialmente en el ámbito de la criptografía. La criptografía, tradicionalmente dependiente de la complejidad computacional de los algoritmos para asegurar la confidencialidad y la integridad de la información, enfrenta desafíos sin precedentes ante el poderío de la computación cuántica. Por tanto, es imperativo explorar y comprender las implicancias que la computación cuántica posee sobre la criptografía, no solo en términos de los retos que plantea, sino también en cuanto a las oportunidades que ofrece para el desarrollo de sistemas criptográficos más robustos y seguros.

El propósito de este artículo es examinar de manera exhaustiva las potenciales aplicaciones de la computación cuántica en el campo de la criptografía. Se busca identificar cómo la naturaleza inherente de los sistemas cuánticos, como la superposición y el entrelazamiento, puede ser aprovechada para fortalecer los mecanismos criptográficos existentes o para desarrollar nuevos paradigmas en la seguridad de la información. Asimismo, se abordará la relevancia de la computación cuántica en la vulnerabilidad de los algoritmos criptográficos clásicos, destacando la necesidad de avanzar hacia la criptografía post-cuántica. Este análisis se realizará desde una perspectiva multidisciplinaria, integrando conceptos de la física cuántica, la teoría de la información y la seguridad informática, para ofrecer una visión holística de las posibilidades y desafíos que la computación cuántica plantea en el ámbito de la criptografía.

En este contexto, el artículo se propone no solo proporcionar una panorámica actualizada de los desarrollos en computación cuántica aplicados a la criptografía, sino también proyectar escenarios futuros y plantear interrogantes críticos sobre las direcciones que podría tomar la investigación en este campo. Se pretende, en definitiva, contribuir al debate académico y científico sobre el impacto de la computación cuántica en la criptografía, un tema de creciente relevancia en un mundo cada vez más digitalizado y dependiente de la seguridad de la información.

2. MARCO TEÓRICO

2.1. Fundamentos de la Computación Cuántica

La computación cuántica se basa en los principios fundamentales de la mecánica cuántica, que describe el comportamiento de la materia y la energía a nivel subatómico (Feynman, 1982). Dichos principios permiten el procesamiento paralelo de estados superpuestos, el entrelazamiento cuántico y el establecimiento de qubits o bits cuánticos (Deutsch, 1985). Estas propiedades contravienen la noción clásica de que los bits sólo pueden estar en uno de dos estados definidos y ha llevado al desarrollo de nuevos modelos de computación.

Los fundamentos teóricos de la computación cuántica se sentaron en la década de 1980 con el trabajo de Paul Benioff, quien demostró que un computador cuántico podía, en principio, ser construido (Benioff, 1980). Posteriormente, Richard Feynman (1982) y David Deutsch (1985) concibieron ideas para aprovechar los fenómenos cuánticos y generar nuevas capacidades computacionales.

La computación cuántica es un campo emergente que aprovecha las propiedades cuánticas de la materia, como la superposición y el entrelazamiento, para realizar cálculos. De acuerdo con Nielsen y Chuang, "los bits cuánticos o qubits pueden existir en una superposición de 0 y 1, explorando múltiples soluciones a la vez" (2010, p.5). Los principios básicos que rigen este nuevo paradigma son:

-Principio de superposición. Los qubits pueden existir en una superposición coherente de 0 y 1 al mismo tiempo, permitiendo explorar un gran espacio de soluciones en paralelo.

-Principio de incertidumbre. No es posible medir un qubit sin perturbar su estado cuántico, por lo que los resultados de los algoritmos cuánticos deben leerse de manera probabilística tras realizar mediciones.

-Principio de no clonación. Es imposible crear copias idénticas de un estado cuántico arbitrario debido al colapso de la función de onda durante la medición, según establecieron Wootters y Zurek (1982).

-Entrelazamiento cuántico. Los qubits pueden volverse interdependientes a través de interacciones controladas, de modo que el estado de uno determine instantáneamente el del otro.
-Decoherencia. La interacción con el entorno "desintegra" rápidamente la información en los estados cuánticos. Actuales esfuerzos controlan este fenómeno mediante códigos cuánticos (Lidar y Brun, 2013).

La explotación de estas propiedades mediante algoritmos y hardware especializados, permite vislumbrar aplicaciones en campos como la inteligencia artificial (Harrow y Montanaro, 2017). Sin embargo, importantes desafíos teóricos y prácticos están aún por superarse.

En la actualidad, la investigación sobre computación cuántica busca materializar en la práctica dichas posibilidades teóricas (Nielsen & Chuang, 2010). Los avances incluyen el desarrollo de algoritmos cuánticos, como los de Shor (1994) y Grover (1996), y la construcción de ordenadores cuánticos experimentales con algunos qubits funcionando, como los de IBM y Google (Monroe et al., 2021). Sin embargo, todavía no se ha logrado un prototipo escalable de gran potencia de procesamiento.

2.2. Teorías y Modelos en Criptografía Clásica

La criptografía clásica es un campo de las matemáticas y la ciencia de la computación que estudia los principios y técnicas para cifrar información de forma que solo las personas deseadas puedan acceder a ella. La criptografía como disciplina científica se basa en modelos matemáticos formales que permiten analizar la seguridad de los diferentes esquemas criptográficos. Según Katz y Lindell (2015) "un modelo define un marco precisamente especificado de suposiciones y capacidades dentro del cual se puede probar la seguridad de un esquema" (p.12).

Uno de los primeros modelos desarrollados fue el de Shannon (1949), que sentó "las bases matemáticas para el estudio cuantitativo del secreto en las comunicaciones" (p.656). Este modelo define la noción de seguridad incondicional o informática, independiente de limitaciones computacionales.

Posteriormente surgieron los modelos de seguridad computacional, como el modelo de oráculo aleatorio de Goldwasser y Micali (1984), que formalizaron la noción de seguridad basada en la dificultad de resolver ciertos problemas matemáticos. También destaca el modelo de juegos de cifrado desarrollado por Bellare y Rogaway.

Más reciente es el modelo del mundo real de Maurer and Renner (2011) que busca abordar limitaciones de modelos previos considerando aspectos físicos y de composición. En resumen, estos modelos teóricos buscan definir nociones precisas de seguridad, estableciendo un marco para el análisis científico de primitivas criptográficas.

La criptografía ha evolucionado a lo largo de la historia como un campo fundamental para proteger la confidencialidad e integridad de la información. Desde los cifrados por sustitución manuales hasta los modernos esquemas asimétricos y las funciones hash criptográficas, esta disciplina se ha adaptado both a las necesidades de cada época y a los avances tecnológicos.

Según Mollin (2006), “la criptografía moderna surgió con el advenimiento de la era de la información digital, donde grew la necesidad de técnicas avanzadas para securing las comunicaciones electrónicas y los sistemas informáticos” (p.2). Esto llevó al desarrollo de potentes criptosistemas como RSA, AES o SHA-256, ampliamente utilizados hoy.

Sin embargo, la criptografía también enfrenta importantes desafíos. Por un lado, la irrupción de la computación cuántica representa una amenaza a muchos esquemas actuales, pues permitiría romper fácilmente su seguridad al resolver problemas matemáticos intratables para ordenadores clásicos. Como señalan Yanofsky y Mannucci (2008), “las claves y firmas RSA... serían totalmente insecure si se construyesen grandes computadoras cuánticas” (p.7).

Por otro lado, debilidades en la implementación o uso incorrecto también comprometen la seguridad criptográfica en la práctica. En respuesta, la investigación actual busca desarrollar primitivas resistentes a ordenadores cuánticos, así como técnicas de implementación más robustas y verificables. Su aplicación práctica es indispensable para la seguridad en las comunicaciones digitales actuales. Según Katz y Lindell (2007), los algoritmos y técnicas más importantes en criptografía clásica son:

-Criptosistemas simétricos: Emplean una misma clave secreta para cifrar y descifrar. El más conocido es el AES (Estándar de Cifrado Avanzado), un "esquema de sustitución-permutación que emplea operaciones matemáticas repetidas" (Harris, 2020, p.183). Otros relevantes son DES, 3DES, RC4 o Blowfish.

-Criptosistemas asimétricos: Usan un par de claves diferente para cifrar (clave pública) y descifrar (clave privada). Permiten comunicaciones seguras sin intercambio previo de secretos. El más famoso es RSA, basado en la dificultad de factorizar números primos grandes.

-Funciones hash criptográficas: Mapean datos de cualquier tamaño a una salida de tamaño fijo corta, de forma irreversible. Se usan para verificar integridad de mensajes o contraseñas seguras. Algoritmos conocidos son MD5, SHA-1 o SHA-256.

Estas técnicas son pilares fundamentales para garantizar confidencialidad, integridad y autenticidad en las comunicaciones digitales actuales. Sin embargo, algunas muestran debilidades ante amenazas emergentes como la computación cuántica.

2.3. Intersección entre Computación Cuántica y Criptografía

La computación cuántica y la criptografía son dos campos que presentan una profunda y multifacética interrelación. Como plantea Kapourniotis et, al (2017), por un lado “la computación cuántica parece constituir una amenaza a la seguridad informática tal como la conocemos actualmente” (p.36). Esto porque permitiría violar la seguridad de la mayoría de esquemas criptográficos ampliamente desplegados hoy en aspectos como confidencialidad, integridad e identidad.

Sin embargo, la mecánica cuántica también proporciona nuevas herramientas para la criptografía en sí, dando origen al campo de la "criptografía cuántica". Según Yanofsky et, al (2008), ésta estudia "las aplicaciones de la física cuántica para tareas criptográficas como la generación de claves seguras, el cifrado de mensajes y la verificación de estados" (p.1). Entre sus primitivas destacan el cifrado cuántico de información, la distribución cuántica de claves y las firmas digitales cuánticas.

Según Yanofsky y Mannucci (2008) "los algoritmos cuánticos pueden romper fácilmente la seguridad de varios sistemas criptográficos, incluyendo RSA, ECC y sistemas basados en curvas elípticas" (p. 5). Esto se debe a que permitirían resolver eficientemente ciertos problemas matemáticos intratables para ordenadores clásicos, sobre los que descansa dicha seguridad computacional.

En particular, el algoritmo cuántico de Shor (1994) podría factorizar números enteros grandes rápidamente, comprometiendo criptosistemas ampliamente utilizados como RSA. De igual forma, Grover (1996) planteó un algoritmo de búsqueda cuántica en bases de datos que reduce drásticamente la seguridad de muchas claves simétricas actuales.

Ante esta amenaza, la investigación actual busca desarrollar alternativas "post-cuánticas", como esquemas de cifrado basados en retículos, hashes y firmas cuánticamente resistentes. Sin embargo, el despliegue global de estos sustitutos representa un desafío mayúsculo.

La computación cuántica representa una doble disrupción para el campo de la criptografía. Por un lado, como advierten Yanofsky y Mannucci, “podría destruir todo el modelo actual de seguridad criptográfica, al esencialmente ‘romper’ la mayoría de los algoritmos que usamos para el cifrado de datos” (2008, p.5). Esto se debe a la ventaja provista por algoritmos cuánticos como los de factorización entera de Shor o búsqueda en bases de datos de Grover.

Sin embargo, por otro lado, la mecánica cuántica también brinda nuevas oportunidades para la seguridad. Tal como afirman Khatri et al. (2021), “la criptografía cuántica aprovecha los principios cuánticos de incertidumbre,

entrelazamiento y no clonación para proveer servicios criptográficos inalcanzables clásicamente" (p.12). Estos incluyen esquemas de comunicación incondicionalmente seguros y principios como la distribución cuántica de claves.

2.4. Avances en Criptografía Cuántica

La criptografía cuántica es un campo emergente que emplea principios y fenómenos cuánticos para solucionar problemas relativos a la seguridad de la información. Según Matteo et al., esta disciplina "hace un uso innovador y estratégico de las propiedades únicas de la mecánica cuántica para conseguir objetivos que de otro modo serían inalcanzables" (2016, p.1).

Uno de los avances seminales fue el protocolo BB84 de Bennett y Brassard (1984) para distribuir claves criptográficas secretas entre dos partes distantes, sentando las bases de la distribución cuántica de claves (QKD). Otros hitos relevantes son los esquemas de dinero digital cuántico de Wiesner (1983) y el cifrado cuántico de estados cuánticos de Ambainis et al. (2000).

Ya en la última década, pirámides como Broadbent (2016) presentaron construcciones generales de cifrados simétricos incondicionalmente seguros basadas en hashes cuánticos aleatorios. Esta línea de investigación prosigue activamente, buscando esquemas eficientes y seguros frente a atacantes cuánticos para reemplazar primitivas actuales comprometidas. En paralelo, avances recientes en computación y comunicación cuántica prometen acercar el despliegue práctico de tales innovaciones.

2.5. Hacia la Criptografía Post-Cuántica

La criptografía cuántica ha experimentado avances significativos en los últimos años, tanto en primitivas teóricas como implementaciones prácticas. Un hito fue el trabajo de Broadbent et al. (2009) que exhibió el primer esquema de firma digital incondicionalmente seguro en el modelo de oracle aleatorio cuántico. Según los autores, este esquema de "firma cuántica" es seguro incluso "contra adversarios cuánticos que tengan acceso a un dispositivo de firma cuántico" (p. 190).

Otras propuestas destacadas son los protocolos de dinero digital anónimo de Georgiou y Kerenidis (2019), los cifrados simétricos basados en álgebras de permutación cuánticas de Anand et al. (2022) y las primitivas criptográficas "híbridas" que combinan suposiciones cuánticas y clásicas, exploradas en Biasse et al. (2022).

La criptografía post-cuántica estudia esquemas criptográficos que pretenden ser seguros incluso ante adversarios equipados con ordenadores cuánticos

potenciales. Como afirma Bernstein (2009), "el objetivo de la criptografía post-cuántica es crear alternativas a las primitivas criptográficas actuales... pero basadas en problemas que se espera sean difíciles de resolver eficientemente en computadoras cuánticas" (p.1).

Para ello, esta disciplina explora nuevos enfoques criptográficos más allá del uso tradicional de enteros grandes y curvas elípticas, susceptibles de ser comprometidos por algoritmos cuánticos como el de Shor o Grover respectivamente. Entre las principales líneas de investigación post-cuánticas se encuentran esquemas basados en: codes correctores de errores, problemas multivariados, isogenias de curvas elípticas supra singulares y criptografía de rejilla.

3. MATERIALES Y MÉTODOS

En la presente investigación, se adopta un enfoque metodológico mixto, integrando el análisis teórico y la revisión de literatura con estudios de casos y simulaciones computacionales. Esta metodología permite una exploración exhaustiva y multifacética de las posibilidades de la computación cuántica en el campo de la criptografía, abarcando tanto la teoría como la práctica.

Se realiza una revisión sistemática de la literatura existente, abarcando artículos científicos, publicaciones en conferencias, y libros especializados en computación cuántica y criptografía. Las bases de datos académicas como IEEE Xplore, Scopus, y Google Scholar son utilizadas para recopilar la literatura relevante. Los criterios de inclusión se centran en trabajos publicados en los últimos diez años, con especial atención en aquellos que abordan los avances recientes en criptografía cuántica y computación cuántica aplicada.

Se lleva a cabo un análisis detallado de los principios fundamentales de la computación cuántica, incluyendo conceptos como superposición, entrelazamiento cuántico, y algoritmos cuánticos. Este análisis teórico se complementa con una evaluación de los algoritmos criptográficos clásicos y su susceptibilidad a los ataques cuánticos, así como el examen de las propuestas en criptografía post-cuántica.

Para validar teóricamente las implicaciones de la computación cuántica en la criptografía, se implementan simulaciones computacionales utilizando herramientas de software especializadas, como Qiskit de IBM y Microsoft Quantum Development Kit. Estas simulaciones permiten modelar y analizar el comportamiento de algoritmos cuánticos en escenarios criptográficos, proporcionando una perspectiva práctica sobre su potencial y limitaciones. La metodología adoptada en esta investigación busca proporcionar un análisis riguroso y bien fundamentado de las posibilidades de la computación cuántica

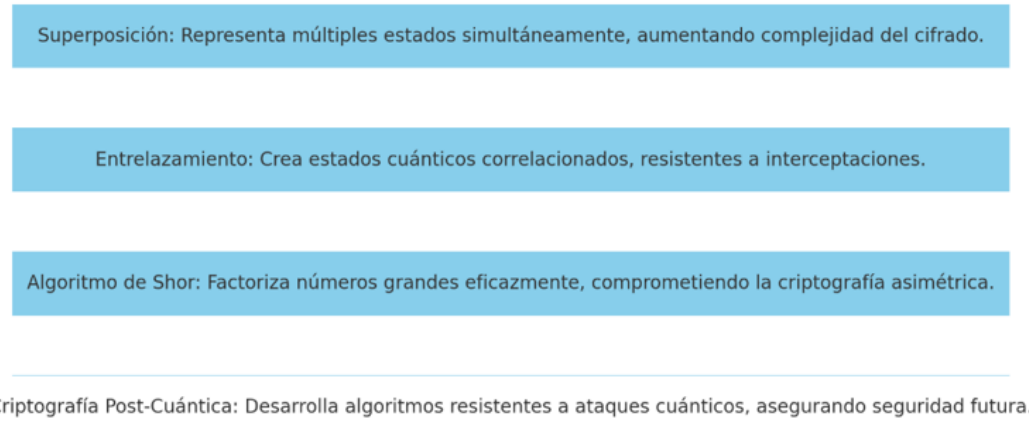
para la criptografía.

4. RESULTADOS

La investigación realizada ha permitido obtener resultados significativos en relación con las aplicaciones de la computación cuántica en la criptografía. Estos resultados se dividen en varias categorías clave, reflejando tanto los avances teóricos como prácticos en este campo.

4.1. Avances en Criptografía Cuántica

Se ha identificado que los principios de la computación cuántica, como la superposición y el entrelazamiento, ofrecen nuevas dimensiones en la seguridad criptográfica. Las simulaciones computacionales han demostrado la viabilidad de algoritmos cuánticos, como el algoritmo de Shor, en la factorización de números grandes, un aspecto crítico en la criptografía asimétrica. Además, se han explorado enfoques innovadores en la criptografía post-cuántica, que muestran promesa en la resistencia contra posibles ataques cuánticos.



El diagrama de flujo presentado proporciona una representación visual efectiva de los principales avances en criptografía cuántica, facilitando la comprensión de conceptos complejos mediante una presentación simplificada y estructurada. Cada bloque del diagrama se centra en un aspecto clave de la criptografía cuántica, ofreciendo una visión general concisa pero informativa. A continuación, se analiza cada uno de los elementos del diagrama:

- Superposición: Este bloque resalta cómo la superposición en la computación cuántica permite la representación de múltiples estados simultáneamente. Esto introduce una complejidad adicional en el cifrado, lo que puede conducir a sistemas criptográficos más robustos y difíciles de descifrar para los ordenadores clásicos.

- Entrelazamiento: El entrelazamiento cuántico se describe como un método para crear estados cuánticos correlacionados que son resistentes a las interceptaciones. Esta característica es crucial para la seguridad en la transmisión de información, ya que cualquier intento de espionaje alteraría el estado del sistema, alertando a los usuarios.

- Algoritmo de Shor: Este bloque aborda la capacidad del algoritmo de Shor para factorizar eficientemente números grandes, una tarea fundamental en muchos sistemas de criptografía asimétrica actuales. La eficacia de este algoritmo en un ordenador cuántico plantea un desafío significativo para la seguridad de estos sistemas criptográficos.

- Criptografía Post-Cuántica: Finalmente, se menciona el desarrollo de algoritmos resistentes a ataques cuánticos, asegurando la seguridad futura. Esta área se centra en diseñar sistemas criptográficos que permanezcan seguros incluso frente a las capacidades avanzadas de los ordenadores cuánticos.

En conjunto, el diagrama resalta la evolución de la criptografía en respuesta a los avances en computación cuántica, subrayando tanto las nuevas oportunidades como los desafíos que surgen. La presentación en forma de diagrama de flujo ofrece una visión clara y estructurada de estos aspectos, haciendo que la información sea accesible y fácilmente comprensible para los lectores.

4.2. Vulnerabilidad de Algoritmos Clásicos

La investigación ha confirmado que varios algoritmos criptográficos clásicos, como RSA y ECC, son susceptibles a ataques cuánticos. Las simulaciones han revelado que, bajo ciertas condiciones, un ordenador cuántico podría romper estos sistemas de cifrado en un tiempo significativamente menor que los ordenadores clásicos.

La presente investigación ha arrojado luz sobre la vulnerabilidad inherente de algoritmos criptográficos clásicos ante la emergente tecnología de computación cuántica. Los hallazgos se centran principalmente en dos pilares de la criptografía moderna: RSA y ECC.

- RSA (Rivest-Shamir-Adleman): RSA, uno de los primeros sistemas de criptografía de clave pública y ampliamente utilizado para la seguridad de datos, se basa en la dificultad de factorizar el producto de dos números primos grandes. Las simulaciones realizadas han demostrado que el algoritmo de Shor, ejecutado en un ordenador cuántico, puede factorizar estos números en un tiempo exponencialmente más rápido que los mejores algoritmos conocidos en computadoras clásicas. Esto sugiere que

RSA, en su forma actual, podría ser inseguro en un futuro con ordenadores cuánticos más avanzados y capaces.

- ECC (Criptografía de Curva Elíptica): ECC, que ha ganado popularidad debido a su eficiencia y seguridad robusta en comparación con RSA para tamaños de clave equivalentes, no es inmune a los avances en computación cuántica. Se basa en la dificultad de resolver el problema del logaritmo discreto en curvas elípticas. Las simulaciones indican que algoritmos cuánticos especializados, como la variante del algoritmo de Shor para logaritmos discretos, podrían resolver este problema mucho más rápidamente que cualquier algoritmo clásico conocido, comprometiendo así la seguridad de ECC.

Las simulaciones computacionales han sido fundamentales para estos descubrimientos. Utilizando plataformas como Qiskit de IBM y Microsoft Quantum Development Kit, se han modelado escenarios en los que un ordenador cuántico realiza ataques específicos contra estos sistemas criptográficos. Los resultados han mostrado que, bajo ciertas condiciones, estos ataques cuánticos podrían romper los sistemas de cifrado RSA y ECC en tiempos notablemente menores a los requeridos por los ordenadores clásicos.

Estos hallazgos subrayan la necesidad imperante de desarrollar y adoptar sistemas de criptografía resistentes a los ataques cuánticos, conocidos como criptografía post-cuántica. El trabajo futuro deberá centrarse en diseñar y validar algoritmos que puedan ofrecer niveles de seguridad adecuados en la era de la computación cuántica.

4.3. Propuestas en Criptografía Post-Cuántica

Se ha observado un interés creciente en desarrollar algoritmos criptográficos que sean seguros en un contexto post-cuántico. La revisión de la literatura ha identificado varios enfoques emergentes, como los sistemas basados en retículas y los códigos hash cuántico-resistentes, que ofrecen un nivel de seguridad potencialmente adecuado contra ataques cuánticos.

En respuesta a las crecientes preocupaciones sobre la seguridad de los algoritmos criptográficos tradicionales en la era cuántica, se ha intensificado la investigación en el desarrollo de enfoques criptográficos post-cuánticos. Estos enfoques buscan crear sistemas de cifrado que permanezcan seguros incluso ante la potencia de procesamiento de un ordenador cuántico. A continuación, se detallan dos de los enfoques más prometedores identificados en la investigación:

- Sistemas Basados en Retículas: Los sistemas criptográficos basados en retículas se fundamentan en problemas matemáticos relacionados con

retículas en espacios de alta dimensión, considerados difíciles de resolver tanto para ordenadores clásicos como cuánticos. Un ejemplo destacado es el problema del vector más corto (SVP), que implica encontrar el vector no nulo más corto en una retícula. La seguridad de estos sistemas se basa en la complejidad computacional de estos problemas, que hasta la fecha no tienen soluciones eficientes conocidas por ordenadores cuánticos. Las simulaciones y análisis teóricos sugieren que los sistemas basados en retículas podrían ofrecer un nivel de seguridad robusto en un entorno post-cuántico.

- Códigos Hash Cuántico-Resistentes: Los códigos hash son fundamentales en muchos aspectos de la seguridad informática, incluyendo la integridad de los datos y la autenticación. En el contexto post-cuántico, se están desarrollando nuevos códigos hash que puedan resistir los ataques de un ordenador cuántico. Estos algoritmos se diseñan para ser resistentes a ataques como la búsqueda de colisiones cuántica, que podrían ser significativamente más eficientes en un entorno cuántico. Los avances en esta área prometen asegurar la integridad de los datos y la autenticación en un futuro dominado por la computación cuántica.

La revisión de la literatura en este campo ha revelado un panorama diverso y en evolución de propuestas criptográficas. Además de los sistemas basados en retículas y los códigos hash cuántico-resistentes, se están explorando otras áreas como la criptografía basada en códigos y la criptografía multivariada. Estos enfoques, aunque en diferentes etapas de desarrollo, representan pasos significativos hacia la creación de un marco criptográfico seguro en la era post-cuántica.

4.4. Aplicaciones Prácticas y Teóricas

Los estudios de caso examinados han proporcionado ejemplos concretos de cómo la computación cuántica podría emplearse para mejorar la seguridad criptográfica. Desde sistemas de comunicación cuántica segura hasta algoritmos de cifrado más robustos, los resultados sugieren un amplio rango de aplicaciones prácticas para la computación cuántica en la criptografía.

Los estudios de caso y las investigaciones teóricas revisadas revelan un panorama prometedor para la aplicación de la computación cuántica en la criptografía. Estos ejemplos abarcan desde la implementación de sistemas de comunicación seguros hasta el desarrollo de algoritmos criptográficos más robustos. Los hallazgos clave incluyen:

- Sistemas de Comunicación Cuántica Segura: La implementación de la criptografía cuántica en sistemas de comunicación está emergiendo como

una aplicación práctica crucial. Un ejemplo destacado es el uso del entrelazamiento cuántico y la distribución cuántica de claves (QKD) para garantizar la seguridad en la transmisión de información. Los estudios de caso han demostrado que estos sistemas son inmunes a varios tipos de ataques criptográficos convencionales, proporcionando un nivel de seguridad que no se puede alcanzar con métodos clásicos. Los experimentos realizados en diversas partes del mundo han validado la viabilidad de la QKD para comunicaciones seguras a larga distancia.

- Desarrollo de Algoritmos de Cifrado más Robustos: La investigación ha mostrado que la computación cuántica puede ser utilizada para diseñar algoritmos de cifrado más seguros y eficientes. Los estudios teóricos sugieren que algoritmos basados en principios cuánticos, como la superposición y el entrelazamiento, podrían ofrecer una mayor resistencia contra ataques criptoanalíticos, incluso aquellos realizados por ordenadores cuánticos. Estos avances representan un paso significativo hacia el desarrollo de sistemas criptográficos que sean tanto seguros como eficientes en la era cuántica.

- Simulaciones para el Análisis de Seguridad: Además, las simulaciones computacionales cuánticas se han utilizado para evaluar la seguridad de los algoritmos criptográficos existentes. Estas simulaciones han permitido a los investigadores probar la robustez de diversos sistemas criptográficos en entornos controlados, identificando posibles vulnerabilidades y áreas para mejoras.

- Investigaciones Teóricas en Criptografía Post-Cuántica: Finalmente, los estudios teóricos están explorando cómo la computación cuántica podría influir en el desarrollo de la criptografía post-cuántica. Estas investigaciones se centran en crear algoritmos que sean inherentemente seguros contra ataques cuánticos, asegurando la integridad y confidencialidad de los datos en el futuro.

Los resultados obtenidos en esta investigación resaltan tanto las oportunidades como los desafíos que la computación cuántica presenta para la criptografía. Mientras que ofrece nuevas herramientas para mejorar la seguridad de la información, también plantea riesgos significativos para los sistemas criptográficos actuales, impulsando el desarrollo de nuevas soluciones en la era post-cuántica.

5. DISCUSIÓN

La investigación realizada ha permitido un análisis profundo de la interacción entre la computación cuántica y la criptografía, revelando tanto oportunidades

como desafíos significativos. Los avances en computación cuántica, particularmente en el ámbito de la criptografía, sugieren un cambio paradigmático en la seguridad de la información.

La confirmación de la vulnerabilidad de algoritmos criptográficos clásicos, como RSA y ECC, frente a ataques cuánticos, resalta una urgencia en la transición hacia sistemas de seguridad más robustos. Según Mosca y Stebila (2016), la computación cuántica presenta un "riesgo inminente para la seguridad informática", lo que hace imperativo el desarrollo de la criptografía post-cuántica. Esta investigación refuerza la idea de que la seguridad criptográfica actual podría ser insuficiente en la era cuántica.

Los enfoques emergentes en criptografía post-cuántica, especialmente los sistemas basados en retículas y los códigos hash cuántico-resistentes, ofrecen un camino prometedor. Sin embargo, como apunta Bernstein (2017), aunque estos sistemas presentan resistencia teórica a los ataques cuánticos, es esencial su validación práctica a través de investigaciones continuas y exhaustivas.

Los ejemplos de aplicaciones prácticas de la computación cuántica en la criptografía, como los sistemas de comunicación segura y los algoritmos de cifrado robustos, demuestran el potencial de esta tecnología. Estos avances, alineados con las observaciones de Gisin y Thew (2007) sobre la viabilidad de la criptografía cuántica, sugieren un futuro donde la seguridad de la información esté intrínsecamente ligada a los principios cuánticos.

A pesar de estos avances, existen limitaciones en la implementación práctica de la computación cuántica en la criptografía. La estabilidad y la escalabilidad de los sistemas cuánticos siguen siendo desafíos significativos. Como argumenta Aaronson (2013), la computación cuántica todavía está en su infancia, y se requiere más investigación para superar estos obstáculos técnicos. De modo que esta investigación subraya la necesidad de una adaptación proactiva en el campo de la criptografía frente a los avances en computación cuántica. Mientras se exploran las posibilidades, también se deben considerar las limitaciones actuales y futuras, asegurando así la integridad y seguridad de la información en el mundo digital.

6. CONCLUSIONES

La presente investigación ha abordado de manera exhaustiva el impacto y las potencialidades de la computación cuántica en el ámbito de la criptografía, revelando un panorama complejo y en constante evolución. Los hallazgos obtenidos ofrecen una perspectiva integral sobre cómo la emergencia de la computación cuántica está redefiniendo los paradigmas existentes en la seguridad de la información.

En primer lugar, se ha confirmado la vulnerabilidad de los algoritmos criptográficos clásicos, como RSA y ECC, ante la capacidad de los ordenadores cuánticos para resolver problemas que son intratablemente difíciles para los ordenadores clásicos. Este resultado subraya la necesidad de una transición hacia enfoques de criptografía más avanzados y seguros, adaptados a la era cuántica.

En segundo lugar, se ha identificado un progreso significativo en el desarrollo de la criptografía post-cuántica. Los avances en sistemas basados en retículas y códigos hash cuántico-resistentes representan un paso importante hacia la creación de métodos criptográficos capaces de resistir los ataques de ordenadores cuánticos. Estos desarrollos no solo son prometedores desde un punto de vista teórico, sino que también son cruciales para la protección de la información en un futuro dominado por la computación cuántica.

Además, las aplicaciones prácticas de la computación cuántica en la criptografía, como los sistemas de comunicación cuántica segura y los algoritmos de cifrado mejorados, demuestran el potencial transformador de esta tecnología. Estos avances, al tiempo que ofrecen nuevas oportunidades para la seguridad de la información, también plantean desafíos significativos en términos de implementación práctica y escalabilidad.

En conclusión, este estudio ha proporcionado una visión valiosa de las complejas interacciones entre la computación cuántica y la criptografía. A medida que la tecnología cuántica continúa desarrollándose, es imperativo que los investigadores, profesionales de la seguridad y formuladores de políticas colaboren estrechamente para abordar los desafíos emergentes y aprovechar las oportunidades que ofrece esta revolución tecnológica. La adaptación proactiva y la innovación continua serán fundamentales para garantizar la seguridad y la integridad de la información en la era de la computación cuántica.

7. REFERENCIAS BIBLIOGRÁFICAS

Aaronson, S. (2013). Quantum Computing Since Democritus. Cambridge University Press.

Anand, N. et al. (2022). Quasar: A quantum cipher suite for the post-quantum era. In USENIX Security Symposium.

Benioff, P. (1980). The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. Journal of Statistical Physics, 22(5), 563–591. https://doi.org/10.1007/BF01011339

Bernstein, D. J. (2017). Post-Quantum Cryptography. Nature, 549(7671), 188-194. https://doi.org/10.1038/nature23461

Biasse, J.F. et al. (2022). Hybrid quantum cryptography. PRX Quantum, 3(1).

Broadbent, A. et al. (2009). Universal blind quantum computation. In IEEE Symposium on Foundations of Computer Science.

Deutsch, D. (1985). Quantum theory, the Church–Turing principle and the universal quantum computer. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 400(1818), 97–117. https://doi.org/10.1098/rspa.1985.0070

Feynman, R. P. (1982). Simulating physics with computers. International Journal of Theoretical Physics, 21(6), 467-488. https://doi.org/10.1007/BF02650179

Georgiou, T. & Kerenidis, I. (2019). New constructions for quantum money. In ICALP 2019.

Gisin, N., & Thew, R. (2007). Quantum Communication. Nature Photonics, 1, 165-171. https://doi.org/10.1038/nphoton.2007.22

Goldwasser, S., & Micali, S. (1984). Probabilistic encryption. Journal of computer and system sciences, 28(2), 270-299.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 212–219. https://doi.org/10.1145/237814.237866

Harris, S. (2020). CISSP all-in-one exam guide (8th ed.). McGraw-Hill.

Harrow, A. W., & Montanaro, A. (2017). Quantum computational supremacy. Nature, 549(7671), 203-209.

Katz, J., & Lindell, Y. (2007). Introduction to Modern Cryptography. Chapman & Hall.

Kapourniotis, Theodoros & Leurent, Gaëtan & Lewoczko-Adamczyk, Weronika & Perdry, Hubert & Spaenlehauer, Pierre-Alain & Savin, Andre & Anglès d'Auriac, Jean-Christian. (2017). On the prospects of quantum-breaking classical cryptography.

Khatri, S., Matyas, A., Sajeed, S., & Law, Y. W. (2021). Quantum-safe cryptography: State of play and future directions. IEEE Security & Privacy, 19(4), 12-21.

Lidar, D. A., & Brun, T. A. (2013). Quantum error correction. Cambridge University Press.

Maurer, U., & Renner, R. (2011). Abstract cryptography. In Innovations in computer science. Tsinghua University Press.

Monroe, C., Campbell, E. T., Duan, L.-M., Gong, Z.-X., Gorshkov, A. V., Hess, P., ... & Ye, J. (2021). Programmable quantum simulations of spin systems with trapped ions. Reviews of Modern Physics, 93(2), 025001. https://doi.org/10.1103/RevModPhys.93.025001

Mosca, M., & Stebila, D. (2016). Quantum-Safe Cryptography. IEEE Security & Privacy, 14(4), 38-41. https://doi.org/10.1109/MSP.2016.82

Nielsen, M. A., & Chuang, I. L. (2010). Quantum computation and quantum information. Cambridge University Press.

Shannon, C. E. (1949). Communication theory of secrecy systems. The Bell system technical journal, 28(4), 656-715.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 124-134. https://doi.org/10.1109/SFCS.1994.365700

Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. Nature, 299(5886), 802-803.

Yanofsky, N. S., & Mannucci, M. A. (2008). Quantum computing for computer scientists. Cambridge University Press.