Instituto Superior Tecnológico "Los Andes" ISTLA

CÓDIGO CIENTÍFICO REVISTA DE INVESTIGACIÓN

Vol. 5 – Núm. 1 / Enero – Junio – 2024

Incidencia de la computación cuántica en los algoritmos criptográficos

Impact of quantum computation on cryptographic algorithms.

Impacto da computação quântica nos algoritmos criptográficos

Bernardi-Espín, Oscar Eduardo
Universidad Técnica de Manabí
obernardi6425@utm.edu.ec
https://orcid.org/0009-0004-6571-3965

Quimiz-Moreira, Mauricio Alexander
Universidad Técnica de Manabí
mauricio.quimiz@utm.edu.ec
https://orcid.org/0000-0002-5430-0215

DOI / URL: https://doi.org/10.55813/gaea/ccri/v5/n1/401

Como citar:
Bernardi-Espín, E. O., & Quimiz-Moreira, A. M. (2024). Incidencia de la computación cuántica en los algoritmos criptográficos. *Código Científico Revista De Investigación*, *5*(1), 627–650.

Recibido: *18/05/2024* ***Aceptado:*** *09/06/2024* ***Publicado:*** *30/06/2024*

Resumen
La computación cuántica representa una innovadora frontera tecnológica con el potencial de revolucionar diversas áreas incluyendo la criptografía, que es esencial para garantizar la seguridad y privacidad de la información en el entorno digital actual. Este artículo presenta una revisión sistemática de la literatura (SLR) a través de la metodología Kitchenham acerca de la incidencia de la computación cuántica en los algoritmos criptográficos con el objetivo de recopilar información relevante de estudios relacionados la cual serán analizadas y comparadas para tener un mejor entendimiento general sobre el funcionamiento de los algoritmos criptográficos. Se realizaron filtros de búsqueda para la recopilación de información, se consideró en base al análisis de artículos científicos, trabajos de titulación de máster o doctorado, estudios e investigaciones realizados acerca de este tema. Los resultados de esta recopilación de estudios generaron preguntas significativas las cuales son respondidas mediante la resolución y categorización de estudios relevantes. Se concluye que, aunque la computación cuántica está en sus inicios de desarrollo puede tener un fuerte impacto que conlleva su progreso tecnológico, se deben tomar ciertas medidas de precaución y estándares al desarrollar algoritmos criptográficos para no vulnerar la seguridad de la información.

Palabras clave: Computación cuántica, Algoritmos criptográficos, Criptología cuántica, Qubits

Abstract
Quantum computing represents an innovative technological frontier with the potential to revolutionize several areas including cryptography, which is essential to ensure information security and privacy in today's digital environment. This paper presents a systematic literature review (SLR) through the Kitchenham methodology about the incidence of quantum computing in cryptographic algorithms with the objective of collecting relevant information from related studies which will be analyzed and compared to have a better general understanding about the performance of cryptographic algorithms. Search filters were used to collect information, based on the analysis of scientific articles, master's or doctoral theses, studies and research on this topic. The results of this collection of studies generated significant questions which are answered through the resolution and categorization of relevant studies. It is concluded that, although quantum computing is in its early stages of development and can have a strong impact on technological progress, certain precautionary measures and standards must be taken when developing cryptographic algorithms in order not to violate the security of information.
Keywords: Quantum Computing, Cryptographic Algorithms, Quantum Cryptology, Qubits

Resumo
A computação quântica representa uma fronteira tecnológica inovadora com potencial para revolucionar várias áreas, incluindo a criptografia, que é essencial para garantir a segurança e a privacidade da informação no ambiente digital atual. Este artigo apresenta uma revisão sistemática da literatura (RSL), através da metodologia de Kitchenham, sobre o impacto da computação quântica nos algoritmos criptográficos, com o objetivo de recolher informação relevante de estudos relacionados, que será analisada e comparada para uma melhor compreensão global do funcionamento dos algoritmos criptográficos. Foram utilizados filtros de pesquisa para recolher informação, com base na análise de artigos científicos, teses de mestrado e doutoramento, estudos e investigações sobre este tema. Os resultados desta recolha de estudos geraram questões significativas que são respondidas através da resolução e categorização dos estudos relevantes. Conclui-se que, apesar de a computação quântica estar numa fase inicial de desenvolvimento e poder ter um forte impacto no progresso tecnológico,

devem ser tomadas certas medidas de precaução e normas no desenvolvimento de algoritmos criptográficos para não violar a segurança da informação.
Palavras-chave: Computação quântica, Algoritmos criptográficos, Criptologia quântica, Qubits

Introducción

En las últimas décadas, la computación cuántica (CC) ha surgido como un campo de investigación revolucionario, que promete desafiar los límites tradicionales de la informática. Se encuentra basada en los principios fundamentales de la mecánica cuántica como la superposición y el entrelazamiento, que permiten a las computadoras cuánticas realizar operaciones a una velocidad sin precedentes(Rietsche et al. 2022). Por este motivo esta nueva disciplina ha llamado el interés de los científicos abriendo la puerta a una era de posibilidades y aplicaciones hasta ahora inimaginables.(Alberts et al. 2021).

Dentro de este orden, tiene el potencial de cambiar radicalmente la seguridad de la información. Su habilidad para procesar datos en paralelo a través del concepto de superposición cuántica supera los límites establecidos por la computación tradicional. Adicional, presenta la capacidad de explorar múltiples soluciones en diferentes campos profesionales debido a la superposición y entrelazamiento proporcionando ventajas computacionales sobre la computación clásica (Syrkin 2022) . Al mismo tiempo amenaza con socavar los fundamentos de la criptografía asimétrica y simétrica (González 2020).

Mediante la criptografía se utiliza de diferentes formas para proteger la confidencialidad e integridad de la información. Por este motivo los algoritmos criptográficos son procedimientos definidos o secuencias de reglas, que utilizan operaciones matemáticas para describir los procesos criptográficos como el cifrado, descifrado, generación de claves, autentificación, firmas entre otros (Kumar 2022a).

En la actualidad existen grandes inversores privados que están financiando tecnologías cuánticas como Reino Unido, China y Estados Unidos. Todos compitiendo con la motivación

de ser el número uno en la soberanía digital, la seguridad nacional y la competitividad en la industria, aunque las tecnologías cuánticas se encuentran aún en desarrollos tempranos (Bayerstadler et al. 2021).De igual manera, el surgimiento de herramientas y entornos de desarrollo contribuir a facilitar la programación de computadoras cuánticas con exploraciones a la criptografía, que permitirá definir ambientes de desarrollo seguro y la prevención de ataques cuánticos a través de los algoritmos criptográficos clásicos (Neha & Amarita, 2023).

Mediante el Consejo Nacional de Ciencia y Tecnología de Estados Unidos publicó en septiembre del 2020 una nueva estrategia para el desarrollo de la Ciencia de la Información Cuántica. Anunció una **inversión de cerca de 250 millones de dólares** para llevar a cabo más de una centena de proyectos vinculados a este campo de la ciencia. Mientras tanto en China, el gobierno de Pekín construyó un **nuevo Laboratorio Nacional de Ciencias de Información Cuántica en Hefei**, en la provincia de Anhui, con un costo de unos 65.500 millones de yuanes para proyectos de investigación (García, 2022).

De este modo el Centro nacional de Supercomputación en Barcelona España fue elegido en octubre del 2022 para albergar uno de los seis ordenadore de la nueva red de computación cuántica de la Unión Europea, con nodos en otros cinco países: Alemania, Republica Checa, Francia, Italia y Polonia, para el desarrollo de la comunidad científica en la industria y sector público con el objetivo de ampliar la experimentación con estas tecnologías a través de simulaciones de sistemas cuánticos con resultados previstos para finales del 2023 (BBVA 2023).

La investigación acerca de la computación cuántica es sumamente importante y llamativa para los investigadores, ya que abraca aspectos científicos, tecnológicos y económicos. De este modo el objetivo de esta investigación es recopilar estudios relevantes acerca de algoritmos criptográficos en la computación. En la siguiente sección se describe como se realizó el estudio y el proceso de selección de artículos en base a la metodología

planteada Kitchenham. Luego se presentan los resultados obtenidos en base a criterios establecidos de inclusión e exclusión y se plantean preguntas de investigación por los autores para establecer un enfoque más amplio al tema base, resaltando aspectos importantes como el estado actual, simuladores, algoritmos, vulnerabilidades y por ultimo conclusiones

Metodología

En el presente trabajo de investigación se ha realizado una revisión sistemática de la literatura (SLR) a través de la metodología aplicada en (Kitchenham 2004), que se utiliza para mejorar la calidad y transparencia de los informes de revisiones sistemáticas contemplando bases de datos actualizadas en términos de búsqueda específicas para identificar estudios relevantes.

Una búsqueda exhaustiva minimiza el riesgo de sesgo de selección y asegura que la revisión sea completa. Para la recopilación de información se abarcarán temáticas tales como definiciones, implementaciones, estudios previos, aplicaciones y simulaciones que mediante los filtros de cadena de búsqueda y los criterios de inclusión y exclusión permitirán la obtención de resultados de calidad. A continuación, se muestran las fases de la metodología Kitchenham:

- Fase de planeación
- Fase de implementación
- Fase de Resultados

2.1 Fase de planeación

Se identifica el problema **y** las preguntas de investigación que serán respondidas de acuerdo con la revisión sistemática y se desarrolla un protocolo de criterios de inclusión y exclusión para evaluar la calidad de los estudios.

Las preguntas de investigación son incorporadas mediante la metodología planteada por los autores, su objetivo es dar un enfoque más específico buscando brechas encontradas en la

recopilación de estudios y buscar respuestas a estas preguntas, el planteamiento son las siguientes:

- **P1** ¿Cuáles son los algoritmos criptográficos usados actualmente?
- **P2** ¿Cuáles son las limitaciones de los algoritmos criptográficos frente a la computación cuántica?
- **P3** ¿Qué factores inciden en la implementación de la computación cuántica en los algoritmos criptográficos?
- **P4** ¿Qué alcances existen actualmente con respecto a la computación cuántica?

2.1.2 Bases de datos consultadas

Para la selección de artículos científicos, publicaciones e investigaciones se tomó en cuenta los últimos 6 años. Dentro de las bases de datos consultadas se encuentran Science Direct, IEEE explore, Springer, IOP Science, Open Journal System, BASE, DOAJ, ARXIV, EBSCO, SCOPUS, Cell Press, ROAD.

2.1.2 Términos booleanos utilizados

La selección de artículos fue encontrada mediante la búsqueda de palabras claves a través de operadores booleanos (AND OR, NOT), los cuales fueron planteados de la siguiente manera:

- "Computación cuántica" AND "Qubits" OR "Superposicion cuántica"
- "Algoritmos criptográficos" AND "Cifrados" OR "AES")
- "Cryptographic algorithms" AND "Qubits"
- "Cryptographic algorithms" AND "Quantum computing"
- "Cirptographic algorithms" AND "Implementations" OR "Adaptations"

2.1.3 Criterio de inclusión

La selección de estudios relevantes bajo este criterio se considera los siguientes:

- Artículos de implementación enfocados en la computación cuántica.

- Artículos de criptografía simétrica y asimétrica.
- Investigaciones relacionadas a operaciones de Qubit
- Investigaciones que aplican arquitectura y métodos de computación cuántica.

2.1.4 Criterio de exclusión

Se excluyeron una serie de artículos que no cumplían con los siguientes criterios establecidos:

1) Artículos que tengan más de 5 años de publicación

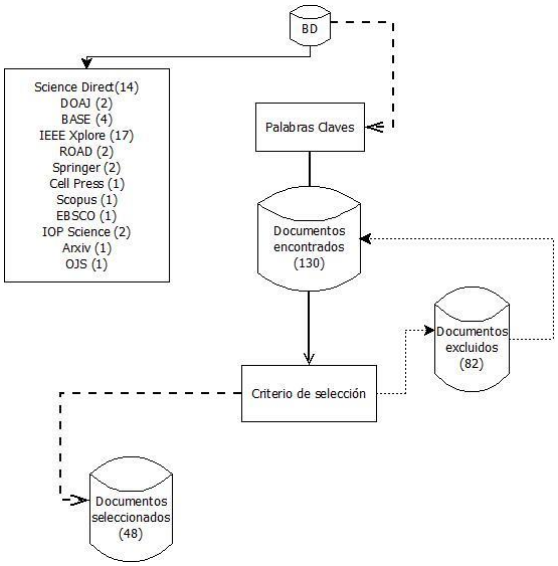
2) Artículos de idiomas distintos a inglés o español.

2.2 Fase de implementación

Se realiza una exhaustiva búsqueda sistemática en base al tema a investigar aplicando los criterios de inclusión y exclusión para seleccionar los estudios pertinentes con el objetivo de dar respuestas a las preguntas de investigación y que aporten la veracidad de la información. A través de estos filtros de búsqueda se identifican estudios primarios y se descartan duplicidad de información. En la *Figura 1* se muestra el proceso de selección de estudios.

Figura 1:

Proceso de la revisión sistemática de la literatura



Nota: Autores (2024)

Resultados

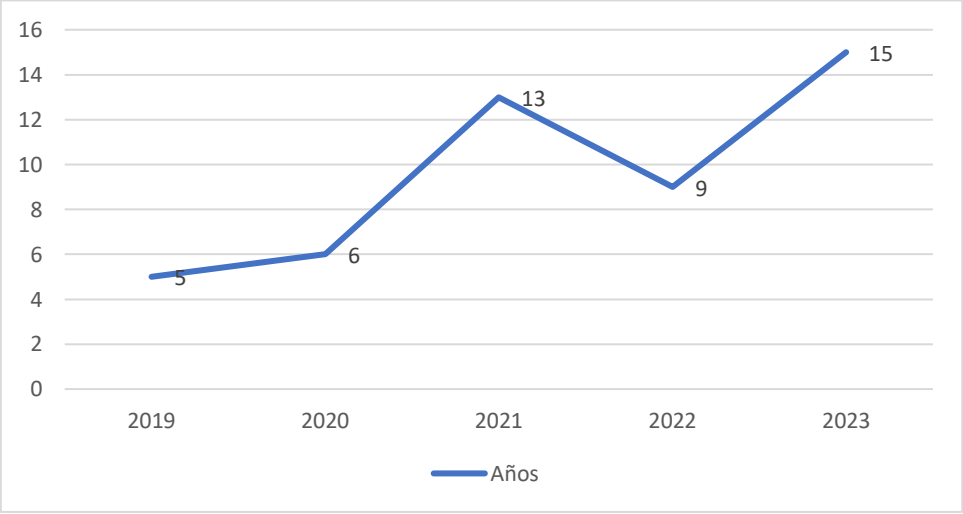
A través de la recopilación de estudios se obtuvieron un total de 130 publicaciones potenciales por medio de la metodología kithchenham. Como resultado de los procedimientos de la metodología en conjunto con los criterios establecidos se seleccionaron 48 artículos indexados en las bases de datos Science Direct, IEEE explore, Springer, IOP Science, Open Journal System, BASE, DOAJ, ARXIV, EBSCO, SCOPUS, Cell Press, ROAD. Posteriormente estos estudios fueron categorizados por año de publicaicon, países y bases de datos indexadas. Mediante estos resultafos se rrespoonden las preguntan de investigación para formar discusión y finalmente conclusiones relacionadas con la computación cuántica y algoritmos criptográficos.

3.1 Frecuencia de Publicación

Acerca de la producción anual de los artículos seleccionados para la revisión sistemática en la *Figura 2* se muestra que el año 2023 fue la mayor predominancia en cuanto a publicaciones científicas con 30% (15). Por otra parte, se evidencia un aumento exponencial desde el año 2021 hasta el 2023, con un total del 76% (37) artículos publicados en este periodo.

Figura 2:

Frecuencia de publicación por años



Nota: Autores (2024)

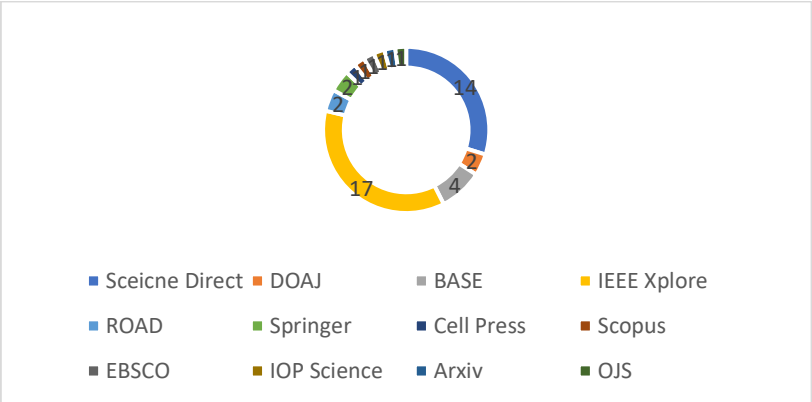
La revisión sistemática de los artículos seleccionados se destaca temas relacionados a través de las preguntas de investigación para mejorar la comprensión de términos y usos de estos algoritmos. Mediante la computación cuántica indica que esta basada en dos propiedades de interacción cuántica como la superposición y en entrelazado la cual permite estar en dos estados al mismo tiempo gracias a los Qubits (Díaz et al., 2021). Sobre los algoritmos criptográficos se encuentran los simétricos (Bühler et al., 2022), (Rudnytskyi et al. 2022), (Kumar 2022) y asimétricos (Valluri et al., 2024).

3.2 Indexación de los artículos seleccionados

Para la revisión sistemática se consideraron publicaciones en revistas indexadas en los principales motores de búsqueda, en la *Figura 3* se muestra que 36% (17 artículos) pertenecen a la base de datos IEEE xplore, un 30% (14 artículos) pertenece a Science Direct, un 8% (4 artículos) pertenece a BASE, un 4% (2 artículos) pertenecen a DOAJ, ROAD, Springer, IOP Science y un 2% (1 articulo) perteneciente a Cell Press, Scopus, EBsco, Arxiv, OJS. Estos artículos científicos corresponden a las diferentes líneas temáticas trazadas por las preguntas de investigación con 58% (28) correspondiente a la
P1, 15% (7) correspondiente a P2, con 10% (5) correspondiente a P3 y 17% (8) correspondiente a P4.

Figura 3:

Indexación de artículos seleccionados



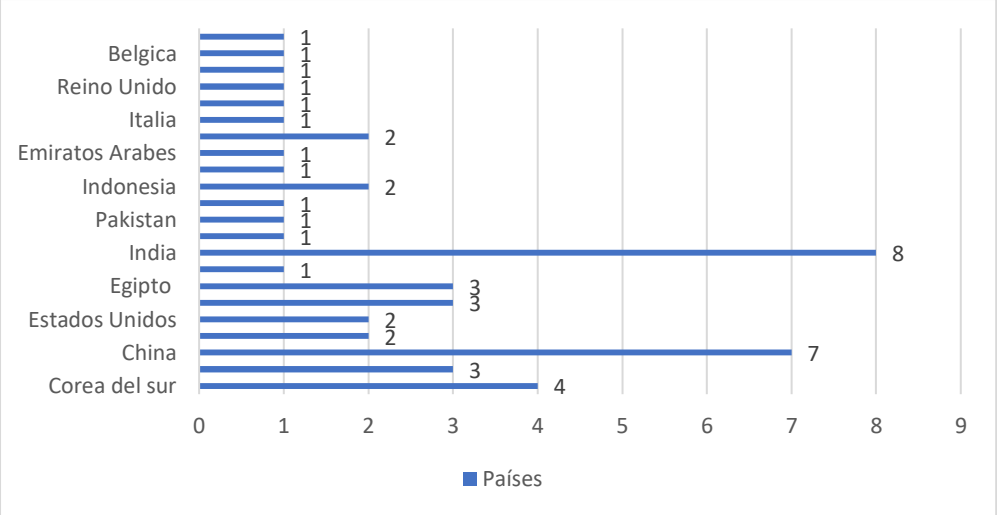
Nota: Autores (2024)

3.3 Estudios por país de procedencia

Esta sección se observan los países con mayor producción científica de los artículos seleccionados como se muestra en la *Figura 4.* Ocupando el primer India con 19% (8 artículos), el segundo lugar China con 17% (7 artículos), en tercer lugar, Corea del sur 8% (4 artículos), en cuarta posición España, Arabia Saudita, Egipto con 6% (3 artículos), en quitan posición se encuentra Estados Unidos, Indonesia, Malasia con 4% (2 artículos) y finalmente en última posición se encuentra Iraq, Israel, Pakistán, Taiwán, Austria, Emiratos Árabes, Italia, Alemania, Reino Unido, Brasil, Bélgica y Países Bajos con 2% (1 articulo).

Figura 4:

Artículos seleccionados por países



Nota: Autores (2024)

El desarrollo de las preguntas de investigación son las siguientes:

P1 ¿Cuáles son los algoritmos criptográficos usados actualmente?

Los algoritmos criptográficos son conjuntos de procedimientos y reglas matemáticas utilizados para cifrar y descifrar información y entre sus funciones de seguridad están la autentificación de usuario, integridad de datos, transmisión y recepción de información (Son et al., 2023).Su objetivo es garantizar la seguridad y privacidad de las comunicaciones. En la *tabla 1* se muestra los tipos de algoritmos:

Tabla 1:

Algoritmos criptográficos

Tipo	Definición	Referencias
Simétricos	Conocidos como algoritmos de clave secreta o cifrado simétrico, son un tipo de algoritmo criptográfico en el que la misma clave se utiliza tanto para cifrar como para descifrar la información. Esto significa que las partes del remitente y destinatario en su comunicación deben compartir previamente la clave secreta.	(Navas 2023)
Asimétricos	Denominada como criptografía de clave publica, utiliza un par de claves matemáticamente relacionadas una clave pública que es el destinario para cifrar el mensaje y una clave privada para descifrarlo.	(Du and Ye 2023).

Nota: Autores (2024)

En la *Tabla 2* muestra los diferentes algoritmos criptográficos simétricos, entre los más importantes se encuentra el AES y Twofish por su seguridad sólida y rendimiento eficiente (Sánchez et al. 2023). Aunque existen otros como el DES, **SHA-1 y RC5 estos no han sido tomados en cuenta debido a sus vulnerabilidades y sus limitantes en la seguridad**(Microsoft Learn, 2023.)**. Debido a que los algoritmos se encuentran en constante evolución y ya no se consideran muy seguros.**

Tabla 2:

Algoritmos criptográficos simétricos

Criptografía simétrica	Características	Estructura y longitud de clave	Referencias
AES (Advanced Encryption Standard)	Es un algoritmo utilizado para proteger la información sensible y confidencial.	Opera mediante red repetitivas de sustitución y permutación de datos. Su tamaño de clave es de 128, 192 y 256 bits	(Huo and Wang 2023),(Langenberg, Pham, and Steinwandt 2021), (Altigani et al. 2021).
3DES (Triple DES)	Una mejora del algoritmo (DES).	Los datos se cifran con la primera clave, se descifran con la segunda clave y luego se cifran nuevamente con la tercera clave, su tamaño puede ser de 56, 112 o 168 bits.	(Abu-Faraj et al. 2022), (Murad and Rahouma 2021).

IDEA (International Data Encryption Algorithm)	Algoritmo de cifrado de bloque simétrico diseñado para proporcionar seguridad en la cifra de datos.	Utiliza una serie de rondas para cifrar o descifrar datos. En cada ronda, se realizan operaciones como sustituciones, permutaciones y combinaciones de datos con la clave, su tamaño es de 128 bits	(Hamad and Farhan 2020), (Kanimozhi and Vimala 2021) ,(Malik, Gupta, and Dhall 2020).
Blowfish	Es conocido por su simplicidad y velocidad de cifrado, y ha sido utilizado en varias aplicaciones a lo largo de los años.	Utiliza una estructura de cifrado que divide el bloque de entrada en dos mitades y realiza una serie de rondas de operaciones sobre estas mitades., su tamaño es 32 bits hasta 448 bits.	(Alotaibi 2021), (Thabit, Alhomdy, and Jagtap 2021).
Twofish	Se conoce por su robustez y ha sido utilizado por aplicaciones de seguridad	Utiliza una estructura de cifrado que divide el bloque de entrada en dos mitades y realiza una serie de rondas de operaciones sobre estas mitades. Admite longitudes de clave de 128, 192 y 256 bits	(Nahmias-Biran, Dadashev, and Levi 2022), (Haq et al. 2021).
RC6 (Rivest Cipher 6)	Es un algoritmo de cifrado de bloque simétrico y es una extensión de RC5	Estructura que divide el bloque de entrada en dos mitades y realiza una serie de rondas de operaciones sobre estas mitades. Las operaciones incluyen sumas y rotaciones, su longitud generalmente entre 0 y 2040 bits.	(Sanap and More 2022),(Ganavi, Prabhudeva, and Nayak 2022).

Nota: Autores (2024)

En la *tabla 3* muestra los algoritmos criptográficos de criptología asimétrica, donde los más relevantes se encuentra el RSA por su simplicidad y eficacia en el rendimiento(Chang et al. 2022) y el algoritmo ECC ofrece niveles de seguridad similares al RSA, pero con longitud de claves más cortas emitiendo una eficiencia en almacenamiento y procesamiento.

Tabla 3:

Algoritmos criptográficos asimétricos

Criptografía asimétrica	Características	Estructura y longitud de clave	Referencias
RSA (Rivest-Shamir-Adleman)	Algoritmo de criptografía de clave pública ampliamente utilizado para la seguridad en la comunicación y la autenticación	Utiliza un par de claves: una clave pública para cifrar y una clave privada para descifrar (o viceversa). Longitudes de clave comunes incluyen 1024, 2048 y 3072 bits.	(Abdelwahab et al. 2021) ,(Farhan and Leman 2023).
DSA (Digital Signature Algorithm)	Algoritmo de firma digital de clave pública, específicamente diseñado para la generación y verificación de firmas digitales.	Se basa en el problema del logaritmo discreto, que implica la dificultad de calcular logaritmos discretos en un campo finito. Los tamaños típicos de clave incluyen 1024, 2048 y 3072 bits.	(Nazal, Pulungan, and Riasetiawan 2019) ,(Huang et al. 2023).
ECC (Elliptic Curve Cryptography	Utiliza propiedades matemáticas de curvas elípticas sobre campos finitos para proporcionar seguridad en la comunicación y autenticación	Se cree que es resistente a ataques cuánticos en comparación con algunos algoritmos de clave pública tradicionales. La seguridad se basa en la dificultad del problema del logaritmo discreto en el contexto de curvas elípticas. Estas curvas son definidas por ecuaciones matemáticas específicas y tienen propiedades únicas que las hacen adecuadas para la criptografía. Una clave ECC de 256 bits puede proporcionar una seguridad comparable a una clave RSA de 3072 bits.	(Shelke et al. 2023), (Kadry et al. 2023). (Javeed, El-Moursy, and Gregg 2023)
NTRU (Nth Degree Truncated Polynomial Ring Unit Lattice)	Ha sido diseñado para ser resistente a ataques cuánticos, específicamente a los algoritmos basados en la factorización de números enteros y en el logaritmo discreto. Estas son las amenazas que podrían desafiar la seguridad	Utiliza retículos polinomiales truncados para su operación. La seguridad del sistema se basa en la dificultad de resolver ciertos problemas matemáticos en el contexto de retículos. El tamaño de las claves puede ser relativamente pequeño en comparación con algunos	(Alexander et al. 2020),(Ahmad et al. 2021).

	de algoritmos más tradicionales como RSA y ECC en un entorno cuántico.	otros algoritmos de clave pública.

Nota: Autores (2024)

P2 ¿Cuáles son las limitaciones de los algoritmos criptográficos frente a la computación cuántica?

Los algoritmos criptográficos se basan en problemas matemáticos que son difíciles de resolver para las computadoras clásicas. Sin embargo, las computadoras cuánticas tienen la capacidad de resolver algunos de estos problemas mucho más rápidamente que las computadoras convencionales. Esto pone en riesgo la criptografía tradicional y hace que se desarrollen nuevos métodos criptográficos resistentes a los ataques cuánticos(Silva and Nuñez 2023). A diferencia de la computación cuántica, los algoritmos criptográficos tienen algunas limitaciones las cuales se basan por sus vulnerabilidades como se muestra en la *Tabla 4.*

Tabla 4:

Algoritmos vulnerables de la computación cuántica

Algoritmos	Criptografía	Descripción
Factorización de Números Enteros:	RSA	Se basa en la dificultad de factorizar grandes números enteros en sus factores primos. Un algoritmo cuántico eficiente llamado algoritmo de Shor puede factorizar grandes números en tiempo polinómico, lo que hace que RSA sea vulnerable a las computadoras cuánticas (Imam et al. 2021).
Problema del Logaritmo Discreto:	Diffie-Hellman, DSA, ElGamal:	Estos algoritmos se basan en la dificultad de calcular logaritmos discretos en ciertos grupos matemáticos. Los algoritmos cuánticos, como el algoritmo de Shor, pueden resolver este problema de manera eficiente, lo que afecta la seguridad de estos algoritmos criptográficos. (Chan et al. 2022).
Algoritmos de Firma Digital:	ECDSA (Elliptic Curve Digital	Se basa en problemas de logaritmos discretos en curvas elípticas y es vulnerable a los algoritmos cuánticos, como el algoritmo de Shor. (Xiao et al. 2022).

	Signature Algorithm)	
Algoritmos de intercambio de clave	Diffie-Hellman ECDH:	Ambos algoritmos se basan en problemas de logaritmos discretos y son vulnerables a los ataques cuánticos (Sangwan et al. 2021).
Funciones Hash Criptográficas	SHA-2	Aunque las funciones hash como SHA-2 no son directamente vulnerables a los algoritmos cuánticos, la seguridad de las firmas digitales y otros protocolos que utilizan funciones hash puede verse comprometida si se utilizan algoritmos cuánticos para romper las claves públicas asociadas (Martino and Cilardo 2020).
Criptografía de Llave Pública en General	RSA y ECC	Son vulnerables a los algoritmos cuánticos debido a su dependencia de problemas matemáticos difíciles de resolver para las computadoras clásicas (Vahdati et al. 2019).

Nota: Autores (2024)

P3 ¿Qué factores inciden en la implementación de la computación cuántica en los algoritmos criptográficos?

La ejecución de un algoritmo cuántico requiere de tareas y procesamientos matemáticos complejos(Weder et al. 2020).Las instituciones encargadas de la seguridad fomentan la migración de sistemas informáticos a la computación cuántica, sin embargo, por ser una tecnología relativamente nueva deben superar unas series de retos a gran escala, como se muestra en la *Tabla 5*.

Tabla 5:

Retos de adaptación de gran escala en la computación cuántica

Adaptación	Definición	Referencia
Retos técnicos	Pueden ser difíciles de comprender y aplicar las complejas arquitecturas que conlleva la computación cuántica. Los equipos utilizados para la criptografía cuántica, como los detectores de fotón único y los sistemas de distribución cuántica de claves (QKD), también pueden ser difíciles de producir y mantener	(Holter et al., 2023).
Interoperabilidad	Uno de los principales retos de la criptografía cuántica segura es garantizar su compatibilidad con los sistemas e infraestructuras criptográficas existentes. Esto requiere una ardua y cuidadosa planificación y coordinación, así como el desarrollo de nuevos algoritmos y protocolos criptográficos. Algunos de estos	(Chawla and Mehra 2022).

	enfoques más prometedores de la criptografía cuántica segura son la criptografía basada en celosías, la criptografía multivariante y la criptografía basada en hash	
Escalabilidad:	Los sistemas de criptografía cuántica pueden ser caros y complejos, y pueden no ser adecuados para despliegues a gran escala debido a sus imitaciones, infraestructuras y recursos costosos.	(Yalamuri, Honnavalli, and Eswaran 2022).
Seguridad	La criptografía cuántica se basa en los principios de la mecánica cuántica, pero sigue siendo vulnerable a ciertos tipos de ataques, como las escuchas y los ataques de intermediario. Además, es posible que en el futuro los ordenadores cuánticos puedan descifrar el cifrado utilizado en la criptografía cuántica.	(Fernandez & Fraga, 2020)**.**

Nota: Autores (2024)

P4 ¿Qué alcances existen actualmente con respecto a la computación cuántica?

La criptografía cuántica es un campo de investigación activo, y se están explorando y desarrollando continuamente nuevos algoritmos y esquemas para garantizar la seguridad de las comunicaciones y la protección de la información en la era de la computación cuántica (Bastos et al., 2021). Es importante destacar que estos algoritmos están en constante evolución, y su seguridad está sujeta a evaluaciones y pruebas rigurosas (Caballero 2023).Para garantizar su robustez y resistencia frente a posibles ataques cuánticos. A continuación, en la *Tabla 6* se muestra las definiciones de los algoritmos más utilizados actualmente:

Tabla 6:

Algoritmos resistentes

Definición	Algoritmos	Referencia
Algoritmos basados en retículos	NTRU (N-th Degree Truncated Polynomial Ring Unit Lattice) por sus siglas en inglés, es un algoritmo criptográfico de clave pública basado en retículos. Se basa en la dificultad del problema de la reducción en retículos para resolver ecuaciones polinómicas. NTRU es considerado uno de los candidatos más fuertes para reemplazar al algoritmo RSA en un entorno poscuántico.	(Cheng, Li, and Duan 2019). (D'anvers et al., 2023).

Criptografía basada en códigos de corrección de errores	McEliece es un algoritmo criptográfico de clave pública basado en códigos de corrección de errores. Se basa en la dificultad del problema de decodificación de códigos lineales. Aunque McEliece tiene un alto grado de seguridad poscuántica, también tiene un tamaño de clave relativamente grande	(Lee et al. 2019), (Mariot et al., 2023).
Esquemas de cifrado basados en isogenias de curvas elípticas	(Supersingular Isogeny Diffie-Hellman) por sus siglas en inglés, es un esquema de intercambio de claves de clave pública basado en isogenias de curvas elípticas. Se basa en el problema de isogenias computacionales y proporciona seguridad poscuántica para el intercambio de claves	(Liu et al. 2019), (Chung 2021)

Nota: Autores (2024)

Discusión

En base a la revisión los distintos artículos se indica que la computación cuántica y la criptografía tradicional abarca varios aspectos fundamentales que impactan en la seguridad de la información(Okhrimenko et al.,2023). Uno de los puntos centrales es la necesidad de entender cómo la computación cuántica afectará la seguridad de los sistemas criptográficos actuales. La CC tiene una amenaza potencial para la criptología simétrica actual, permitiendo la resolución de problemas de manera eficiente como la factorización de números enteros grandes en tiempos reducidos(Navarrete 2021).Como es el caso del algoritmo Shor.

Estos problemas radican en la vulnerabilidad de la seguridad en los sistemas criptográficos que utilizan claves públicas, como es el caso de conectarse a un banco, realizar pagos, llamadas e incluso enviar mensajes a través de aplicaciones de mensajería o la utilización de firmas digitales. Por este motivo se deben diseñar sistemas de claves públicas que sean resistentes a estos ataques cuánticos (Escribano 2022)

Existen varios tipos de problemas técnicos en el camino de la implementación de sistemas de computación cuántica. La decoherencia es uno de estos problemas, cuando los Qubits cambian su estado al interactuar con el medio ambiente esto hace que se estropee la

información en el camino hacia su destino(Xiong et al. 2022). Esto es causado por una variedad de factores que incluye la radiación de objetos, campos magnéticos y eléctricos. Es por este motivo que es un desafío la implementación práctica de las TIC para un futuro (Suau et al., 2020).

Otro problema se encuentra en las infraestructuras de tecnologías de nueva generación (Wang et al. 2023). Desde el punto de vista cuántico la comunicación es una tecnología nueva donde sus recursos no disponen de una infraestructura para su implementación y los científicos no están invirtiendo en nuevos dispositivos que puedan superar en la deficiencia de estos recursos (Hasan et al., 2023).

En la última década se ha visto un avance en el campo de la criptografía cuántica, aunque ha sido de manera experimental. Pero es importante destacar que hay investigaciones relacionadas al desarrollo de cifrados capaces de sobrevivir a algoritmos cuánticos de desencriptación denominado como criptología poscuantica (Guérin et al., 2021). Sin embargo, debido a la potencia de cálculo, estos dispositivos pueden bastar muchos procesos en pocos segundos para resolver problemas que a diferencia de un ordenador clásico podría tomar un mayor lapso en el procesamiento. Adicional los sistemas de refrigeración son muy costosos los cuales requieren de mayor espacio físico, por lo tanto, disponer de ordenadores cuánticos es algo que se visualiza a largo plazo y se deben de encontrar materiales estables para la implementación física de Qubits (Ilisie, 2022).

Conclusión

En esta revisión bibliográfica se examinaron 48 artículos científicos los cuales de acuerdo con los resultados se destaca el interés científico de los investigadores en los últimos años en crear nuevas formas de transformar la seguridad de la información. Los estudios han

abordado diversas formas de evaluaciones de algoritmos criptográficos tradicionales para el estudio y desarrollo de algoritmos resistentes a ataques cuánticos

La criptografía poscuántica ha surgido como un campo de investigación y desarrollo clave para abordar esta amenaza potencial. Se han propuesto nuevos algoritmos criptográficos que se basan en problemas matemáticos difíciles de resolver en una computadora cuántica, lo que garantiza la seguridad en un entorno poscuántico. Estos algoritmos, como los basados en retículos y las isogenias de curvas elípticas, ofrecen nuevas alternativas frente a los ataques de las computadoras cuánticas.

En última instancia, si bien la computación cuántica presenta desafíos significativos, también ofrece oportunidades para la innovación y el desarrollo de nuevas formas de proteger la información y garantizar la privacidad en un entorno tecnológico en constante cambio. La investigación y el avance continuo en la criptografía poscuántica son esenciales para garantizar un futuro seguro en la era de la computación cuántica.

Sobre trabajos futuro es esencial abordar los desafíos emergentes y desarrollar soluciones efectivas en un entorno poscuántico. A medida que la tecnología avanza y los algoritmos cuánticos se vuelven más poderosos, es importante seguir investigando y trabajando en diversas áreas relacionadas, como el desarrollo de nuevos algoritmos criptográficos que resistan la computación cuántica, establecer estándares y certificaciones para garantizar su interoperabilidad y seguridad.

Referencias bibliográficas

Abdelwahab, Osama F., Aziza I. Hussein, Hesham F. A. Hamed, Hamdy M. Kelash, and Ashraf A. M. Khalaf. 2021. "Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data." *Procedia Computer Science* 182:5–12. doi: 10.1016/j.procs.2021.02.002.

Abu-Faraj, Mua'Ad, Abeer Al-Hyari, Khaled Aldebei, Ziad A. Alqadi, and Bilal Al-Ahmad. 2022. "Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography." *IEEE Access* 10(July):69388–97. doi: 10.1109/ACCESS.2022.3187317.

Ahmad, Khaleel, Afsar Kamal, Khairol Amali Bin Ahmad, Manju Khari, and Rubén González Crespo. 2021. "Fast Hybrid-MixNet for Security and Privacy Using NTRU Algorithm." *Journal of Information Security and Applications* 60(June). doi: 10.1016/j.jisa.2021.102872.

Alberts, Garrelt J. N., M. Adriaan Rol, Thorsten Last, Benno W. Broer, Cornelis C. Bultink, Matthijs S. C. Rijlaarsdam, and Amber E. Van Hauwermeiren. 2021. "Accelerating Quantum Computer Developments." *EPJ Quantum Technology* 8(1). doi: 10.1140/epjqt/s40507-021-00107-w.

Alexander, Thomas, Naoki Kanazawa, Daniel J, Egger, Lauren Capelluto, Christopher J, Wood, Ali Javadi-Abhari, and David C McKay. 2020. "Qiskit Pulse: Programming Quantum Computers through the Cloud with Pulses." *Quantum Science and Technology* 5(4). doi: 10.1088/2058-9565/aba404.

Allard Guérin, Philippe, Veronika Baumann, Flavio Del Santo, and Časlav Brukner. 2021. "A No-Go Theorem for the Persistent Reality of Wigner's Friend's Perception." *Communications Physics* 4(1). doi: 10.1038/s42005-021-00589-1.

Alotaibi, Majid. 2021. "Improved Blowfish Algorithm-Based Secure Routing Technique in IoT-Based WSN." *IEEE Access* 9:159187–97. doi: 10.1109/ACCESS.2021.3130005.

Altigani, Abdelrahman, Shafaatunnur Hasan, Bazara Barry, Shiraz Naserelden, Muawia A. Elsadig, and Huwaida T. Elshoush. 2021. "A Polymorphic Advanced Encryption Standard - A Novel Approach." *IEEE Access* 9:20191–207. doi: 10.1109/ACCESS.2021.3051556.

Anon. n.d. "CA5350: No Usar Algoritmos Criptográficos No Seguros (Análisis de Código) - .NET | Microsoft Learn." Retrieved March 23, 2024 (https://learn.microsoft.com/es-es/dotnet/fundamentals/code-analysis/quality-rules/ca5350).

Bastos, Daniel Chicayban, and Luis Antonio Brasil Kowada. 2021. "How to Detect Whether Shor's Algorithm Succeeds against Large Integers without a Quantum Computer." *Procedia Computer Science* 195:145–51. doi: 10.1016/j.procs.2021.11.020.

Bayerstadler, Andreas, Guillaume Becquin, Julia Binder, Thierry Botter, Hans Ehm, Thomas Ehmer, Marvin Erdmann, Norbert Gaus, Philipp Harbach, Maximilian Hess, Johannes Klepsch, Martin Leib, Sebastian Luber, Andre Luckow, Maximilian Mansky, Wolfgang Mauerer, Florian Neukart, Christoph Niedermeier, Lilly Palackal, Ruben Pfeiffer, Carsten Polenz, Johanna Sepulveda, Tammo Sievers, Brian Standen, Michael Streif, Thomas Strohm, Clemens Utschig-Utschig, Daniel Volz, Horst Weiss, and Fabian Winter. 2021. "Industry Quantum Computing Applications." *EPJ Quantum Technology* 8(1). doi: 10.1140/epjqt/s40507-021-00114-x.

BBVA. 2023. *Mapa Mundial de La Computación Cuantica*.

Bühler, Heiko, Andreas Walz, and Axel Sikora. 2022. "Benchmarking of Symmetric Cryptographic Algorithms on a Deeply Embedded System." Pp. 266–71 in *IFAC-PapersOnLine*. Vol. 55. Elsevier B.V.

Caballero-Gil, Pino. 2023. *Criptografía En La Administración Pública: Una Perspectiva Integral*. Vol. 2.

Chan, Koon Ming, Swee Huay Heng, Wei Chuen Yau, and Shing Chiang Tan. 2022. "Trapdoor Privacy in Public Key Encryption With Keyword Search: A Review." *IEEE Access* 10:21584–98. doi: 10.1109/ACCESS.2022.3151429.

Chang, Xiangyu, Wei Li, Aimin Yan, Peter Wai Ming Tsang, and Ting Chung Poon. 2022. "Asymmetric Cryptosystem Based on Optical Scanning Cryptography and Elliptic Curve Algorithm." *Scientific Reports* 12(1). doi: 10.1038/s41598-022-11861-x.

Chawla, Diksha, and Pawan Singh Mehra. 2022. "A Survey on Quantum Computing for Internet of Things Security." *Procedia Computer Science* 218:2191–2200. doi: 10.1016/j.procs.2023.01.195.

Cheng, Sipei, Mengdong Li, and Yuwei Duan. 2019. "An Improved Scheme of Searchable Encryption Algorithm Based on NTRU." in *Journal of Physics: Conference Series*. Vol. 1345. Institute of Physics Publishing.

Chung, Seog. 2021. "SIKE on GPU: Accelerating Supersingular Isogeny-Based Key Encapsulation Mechanism on Graphic Processing Units." *IEEE Access* 9:116731–44. doi: 10.1109/ACCESS.2021.3106551.

D'anvers, Jan Pieter, Michiel Van Beirendonck, and Ingrid Verbauwhede. 2023. "Revisiting Higher-Order Masked Comparison for Lattice-Based Cryptography: Algorithms and Bit-Sliced Implementations." *IEEE Transactions on Computers* 72(2):321–32. doi: 10.1109/TC.2022.3197074.

Díaz-Toro, Gilberto Javier, Luiz Angelo Steffenel, and Carlos J. Barrios-Hernández. 2021. "On the Resource Consumption of Software Quantum Computing Simulators." *DYNA (Colombia)* 88(218):72–80. doi: 10.15446/dyna.v88n218.90781.

Du, Simin, and Guodong Ye. 2023. "IWT and RSA Based Asymmetric Image Encryption Algorithm." *Alexandria Engineering Journal* 66:979–91. doi: 10.1016/j.aej.2022.10.066.

Escribano, José. 2022. "Criptografía Segura Frente a adversarios Cuánticos. Análisis Y de Propuestas Para."

Farhan, Faiz, and Dedi Leman. 2023. "Implementasi Metode Rivest Shamir Adleman (RSA) Untuk Kerahasiaan Database Perum Bulog Kanwil SUMUT." *Journal of Machine Learning and Data Analytics (MALDA)* 2(1):18–27.

Fernandez-Carames, Tiago M., and Paula Fraga-Lamas. 2020. "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks." *IEEE Access* 8:21091–116. doi: 10.1109/ACCESS.2020.2968985.

Ganavi, M., S. Prabhudeva, and Sankhya N. Nayak. 2022. "A Secure Image Encryption and Embedding Approach Using MRSA and RC6 with DCT Transformation." *International Journal of Computer Networks and Applications* 9(3):262–78. doi: 10.22247/ijcna/2022/212553.

González, Antonio. 2020. "Computación Cuántica y Aplicaciones." *Revista General de Marina* 278(4):635–40.

Hamad, Atyaf, and Alaa Farhan. 2020. "Image Encryption Algorithm Based on Substitution Principle and Shuffling Scheme." *Engineering and Technology Journal* 38(3B):98–103. doi: 10.30684/etj.v38i3b.433.

Haq, Tanveer Ul, Tariq Shah, Ghazanfar Farooq Siddiqui, Muhammad Zafar Iqbal, Ibrahim A. Hameed, and Huma Jamil. 2021. "Improved Twofish Algorithm: A Digital Image Enciphering Application." *IEEE Access* 9:76518–30. doi: 10.1109/ACCESS.2021.3081792.

Hasan, Syed Rakib, Mostafa Zaman Chowdhury, Md Saiam, and Yeong Min Jang. 2023. "Quantum Communication Systems: Vision, Protocols, Applications, and Challenges." *IEEE Access* 11:15855–77.

Ten Holter, Carolyn, Philip Inglesant, and Marina Jirotka. 2023. "Reading the Road: Challenges and Opportunities on the Path to Responsible Innovation in Quantum Computing." *Technology Analysis and Strategic Management* 35(7):844–56. doi: 10.1080/09537325.2021.1988070.

Huang, Xiaoling, Youxia Dong, Guodong Ye, Wun She Yap, and Bok Min Goi. 2023. "Visually Meaningful Image Encryption Algorithm Based on Digital Signature." *Digital Communications and Networks* 9(1):159–65.

Huo, Xiaoyan, and Xuemei Wang. 2023. "Internet of Things for Smart Manufacturing Based on Advanced Encryption Standard (AES) Algorithm with Chaotic System." *Results in Engineering* 20(November):101589. doi: 10.1016/j.rineng.2023.101589.

Ilisie, Victor. 2022. *Computación Cuántica: ¿De Dónde Venimos y Hacia Dónde Nos Dirigimos?*

Imam, Raza, Qazi Mohammad Areeb, Abdulrahman Alturki, and Faisal Anwer. 2021. "Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status." *IEEE Access* 9:155949–76. doi: 10.1109/ACCESS.2021.3129224.

Javeed, Khalid, Ali El-Moursy, and David Gregg. 2023. "EC-Crypto: Highly Efficient Area-Delay Optimized Elliptic Curve Cryptography Processor." *IEEE Access* 11(June):56649–62. doi: 10.1109/ACCESS.2023.3282781.

Kadry, Heba, Ahmed Farouk, Elnomery A. Zanaty, and Omar Reyad. 2023. "Intrusion Detection Model Using Optimized Quantum Neural Network and Elliptical Curve Cryptography for Data Security." *Alexandria Engineering Journal* 71:491–500. doi: 10.1016/j.aej.2023.03.072.

Kanimozhi, Ms A., and N. Vimala. 2021. "An Efficient Privacy Preserving Using Map Reduce Based International Data Encryption Algorithm and Weighted Auto Encoder." 2492–2504.

Kitchenham, Barbara. 2004. "Procedures for Performing Systematic Reviews."

Kumar, Manish. 2022a. "Post-Quantum Cryptography Algorithm's Standardization and Performance Analysis." *Array* 15(April):100242. doi: 10.1016/j.array.2022.100242.

Kumar, Manish. 2022b. "Post-Quantum Cryptography Algorithm's Standardization and Performance Analysis." *Array* 15. doi: 10.1016/j.array.2022.100242.

Langenberg, Brandon, Hai Pham, and Rainer Steinwandt. 2021. "Reducing the Cost of Implementing the Advanced Encryption Standard as a Quantum Circuit." *IEEE Transactions on Quantum Engineering* 1:1–12. doi: 10.1109/tqe.2020.2965697.

Lee, Eunsang, Young Sik Kim, Jong Seon No, Minki Song, and Dong Joon Shin. 2019. "Modification of Frodokem Using Gray and Error-Correcting Codes." *IEEE Access* 7:179564–74. doi: 10.1109/ACCESS.2019.2959042.

Liu, Weiqiang, Jian Ni, Zhe Liu, Chunyang Liu, and Maire O'Neill. 2019. "Optimized Modular Multiplication for Supersingular Isogeny Diffie-Hellman." *IEEE Transactions on Computers* 68(8):1249–55. doi: 10.1109/TC.2019.2899847.

Malik, Anjali, Shailender Gupta, and Sangeeta Dhall. 2020. "Analysis of Traditional and Modern Image Encryption Algorithms under Realistic Ambience." *Multimedia Tools and Applications* 79(37–38):27941–93. doi: 10.1007/s11042-020-09279-6.

Mariot, Luca, Stjepan Picek, and Radinka Yorgova. 2023. "On McEliece-Type Cryptosystems Using Self-Dual Codes With Large Minimum Weight." *IEEE Access* 11(April):43511–19. doi: 10.1109/ACCESS.2023.3271767.

Martino, Raffaele, and Alessandro Cilardo. 2020. "SHA-2 Acceleration Meeting the Needs of Emerging Applications: A Comparative Survey." *IEEE Access* 8:28415–36. doi: 10.1109/ACCESS.2020.2972265.

Murad, Sherief H., and Kamel H. Rahouma. 2021. "Implementation and Performance Analysis of Hybrid Cryptographic Schemes Applied in Cloud Computing Environment." *Procedia Computer Science* 194:165–72. doi: 10.1016/j.procs.2021.10.070.

Nahmias-Biran, Bat-Hen, Gabriel Dadashev, and Yedidya Levi. 2022. "Demand Exploration of Automated Mobility On-Demand Services Using an Innovative Simulation Tool." *IEEE Open Journal of Intelligent Transportation Systems* 3(December 2021):580–91. doi: 10.1109/ojits.2022.3197709.

Navarrete, Álvaro. 2021. "Towards Secure and Practical Quantum Key Distribution."

Navas Damas, Manuel. 2023. "CRIPTOGRAFÍA SIMÉTRICA Y ASIMÉTRICA." 1–145.

Nazal, Muhammad Asghar, Reza Pulungan, and Mardhani Riasetiawan. 2019. "Data Integrity and Security Using Keccak and Digital Signature Algorithm (DSA)." *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)* 13(3):273. doi: 10.22146/ijccs.47267.

Neha, Kumari, and . Amrita. 2023. "Quantum Programming: Working with IBM'S Qiskit Tool." *The Scientific Temper* 14(01):93–99. doi: 10.58414/scientifictemper.2023.14.1.11.

Okhrimenko, Tetiana, Serhii Dorozhynskyi, and Bohdan Horbakha. 2023. "ANALYSIS OF QUANTUM SECURE DIRECT COMMUNICATION PROTOCOLS." *Computer Systems and Information Technologies* (1):62–67. doi: 10.31891/csit-2023-1-8.

Rietsche, Roman, Christian Dremel, Samuel Bosch, Léa Steinacker, Miriam Meckel, and Jan Marco Leimeister. 2022. "Quantum Computing." *Electronic Markets* 32(4):2525–36. doi: 10.1007/s12525-022-00570-y.

Rudnytskyi, Volodymyr, Oleksandr Korchenko, Nataliia Lada, Ruslana Ziubina, Lukasz Wieclaw, and Lukasz Hamera. 2022. "Cryptographic Encoding in Modern Symmetric and Asymmetric Encryption." Pp. 54–63 in *Procedia Computer Science*. Vol. 207. Elsevier B.V.

Sanap, Sarita, and Vijayshree More. 2022. "Field Programmable Gate Arrays (FPGA) Based Implementation of Efficient RC6 Block Cipher." *Journal of Integrated Science and Technology* 10(2):168–72.

Sánchez, Jossel, Eduardo Alejandro, Delgado Pionce, and Adriana Michelle Cobos Villafuerte. 2023. "Análisis de Los Algoritmos Criptográficos Modernos y Su Efectividad En La Protección de Datos Personales." doi: 10.47230/Journal.TechInnovation.v2.n1.2023.57-61.

Sangwan, Yashwant Singh, Shyam Lal, Pankaj Bhambri, and Anil Kumar. 2021. "Advancements In Social Data Security And Encryption : A Review." 8(4):15353–62.

Shelke, Chetan J., Kavin Marx, Aishwarya Rajesh, Rathnakar Achary, Chetan J. Shelke, Kavin Marx, and Aishwarya Rajesh. 2023. "Security Implementation on IoT Using CoAP and Elliptical Curve Cryptography." *Procedia Computer Science* 230(2023):493–502. doi: 10.1016/j.procs.2023.12.105.

Silva, Davide, and Rosa Nuñez. 2023. "EXPLORACIÓN DE LAS POSIBILIDADES DE LA COMPUTACIÓN CUÁNTICA PARA LA CRIPTOGRAFÍA." (2023).

Son, Jun Young, Taewoo Tak, and Hahm Inhye. 2023. "Modeling Cryptographic Algorithms Validation and Developing Block Ciphers with Electronic Code Book for a Control System at Nuclear Power Plants." *Nuclear Engineering and Technology* 55(1):25–36. doi: 10.1016/j.net.2022.07.026.

Souto García, Valentín. 2022. "Sociedad Del Riesgo y Computación Cuántica." 4–5.

Suau, Adrien, Gabriel Staffelbach, and Henri Calandra. 2020. "Practical Quantum Computing: Solving the Wave Equation Using a Quantum Approach." doi: 10.1145/3430030.

Syrkin, M. 2022. "HyperScience International Journal Foundations of Quantum Computing: I-Demystifying Quantum Paradoxes." *HIJ* 2(3):76–82. doi: 10.55672/hij2022pp76-82.

Thabit, Fursan, Sharaf Alhomdy, and Sudhir Jagtap. 2021. "Security Analysis and Performance Evaluation of a New Lightweight Cryptographic Algorithm for Cloud Computing." *Global Transitions Proceedings* 2(1):100–110. doi: 10.1016/j.gltp.2021.01.014.

Vahdati, Zeinab, Sharifah Yasin, A. L. I. Ghasempour, and Mohammad Salehi. 2019. "COMPARISON OF ECC AND RSA ALGORITHMS IN IOT.Pdf." 97(16).

Valluri, Bhanu Priyanka, and Nitin Sharma. 2024. "Exceptional Key Based Node Validation for Secure Data Transmission Using Asymmetric Cryptography in Wireless Sensor Networks." *Measurement: Sensors* 33:101150. doi: 10.1016/j.measen.2024.101150.

Wang, Sai, Xiumei Sun, Xuhui Cong, and Yongkun Gao. 2023. "Input Efficiency Measurement and Improvement Strategies of New Infrastructure under High-Quality Development." *Systems* 11(5). doi: 10.3390/systems11050243.

Weder, Benjamin, Uwe Breitenbucher, Frank Leymann, and Karoline Wild. 2020. "Integrating Quantum Computing into Workflow Modeling and Execution." *Proceedings - 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing, UCC 2020* 279–91. doi: 10.1109/UCC48980.2020.00046.

Xiao, Ligang, Daowen Qiu, Le Luo, and Paulo Mateus. 2022. "Distributed Shor's Algorithm."

Xiong, Heng Na, Lingfeng Li, Zhe Sun, Ze Jin Yang, Zichun Le, Yixiao Huang, and Xiaoguang Wang. 2022. "Information Preservation of Two Qubits in a Structured Environment." *New Journal of Physics* 24(12). doi: 10.1088/1367-2630/aca559.

Yalamuri, Gagan, Prasad Honnavalli, and Sivaraman Eswaran. 2022. "A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats." *Procedia Computer Science* 215:834–45. doi: 10.1016/j.procs.2022.12.086.