TSE'DE
Revista de Investigación Científica
ISSN 2600 - 5557

APLICACIONES DE LA COMPUTACIÓN CUÁNTICA EN LA SEGURIDAD DE DATOS PARA EL INTERNET DE LAS COSAS (IoT)

APPLICATIONS OF QUANTUM COMPUTING IN DATA SECURITY FOR THE INTERNET OF THINGS (IoT)

APLICAÇÕES DA COMPUTAÇÃO QUÂNTICA NA SEGURANÇA DE DADOS PARA A INTERNET DAS COISAS (IoT)

M.Sc. Rocio Mendoza Villamar
rocio.mendoza@uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí
Orcid: 0000-0002-1277-7162

MBA. Ángel Wilson Villarreal
angel.villarreal@uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí
Orcid: 0000-0003-0357-0538

Angie Moreira Huerta
aemh.235067306@gmail.com
Universidad Laica Eloy Alfaro de Manabí
Orcid: 0009-0000-1284-4188

Nayeli Loor Mera
nayeliloor01@gmail.com
Universidad Laica Eloy Alfaro de Manabí
Orcid :0009-0002-4664-9158

REVISTA TSE´DE

Instituto Superior Tecnológico Tsa´chila

ISSN: 2600-5557

Resumen

La computación cuántica pone en riesgo los sistemas criptográficos tradicionales usados en dispositivos del internet de las cosas, ya que puede descifrar claves con algoritmos como Shor o Grover. Este estudio exploró la posibilidad de aplicar medidas de seguridad cuántica, como la distribución cuántica de claves y algoritmos resistentes, como crystals-kyber y ntruencrypt, en entornos IoT con recursos limitados. Se usó una metodología cualitativa documental, basada en revisar literatura y analizar casos. Los resultados muestran que, aunque estas soluciones son muy seguras, enfrentan problemas por el alto consumo energético, el tamaño de las claves y la falta de estándares claros. Se concluye que, para lograr una seguridad cuántica efectiva, será clave optimizar algoritmos, reducir el hardware y definir protocolos eficientes. Este trabajo aporta ideas para proteger los datos en el ecosistema frente a las nuevas amenazas cuánticas en el internet de las cosas.

Palabras clave: algoritmos híbridos; entrelazamiento; miniaturización; retículas; teorema de no clonación

TSE'DE
Revista de Investigación Científica
ISSN 2600 - 5557

Abstract

Quantum computing puts traditional cryptographic systems used in Internet of Things devices at risk, as it can decrypt keys with algorithms such as Shor or Grover. This study explored the possibility of applying quantum security, such as quantum key distribution and robust algorithms, such as crystals kyber and ntruencrypt, in resource limited IoT environments. A qualitative documentary methodology was used, based on a literature review and case analysis. The results show that, although these solutions are highly secure, they face challenges due to high energy consumption, key size, and the lack of clear standards. It is concluded that, to achieve effective quantum security, it will be key to optimize algorithms, reduce hardware requirements, and define efficient protocols. This work provides insights for protecting data in the Internet of Things ecosystem against new quantum threats.

Keywords: entanglement; hybrid algorithms; miniaturization; no-cloning theorem; lattices

Resumo

A computação quântica coloca em risco os sistemas criptográficos tradicionais usados em dispositivos internet das coisas, pois pode descriptografar chaves com algoritmos como Shor ou Grover. Este estudo explorou a possibilidade de aplicar segurança quântica, como distribuição quântica de chaves e algoritmos robustos, como crystals kyber e ntruencrypt, em ambientes IoT com recursos limitados. Foi utilizada uma metodologia documental qualitativa, baseada em revisão de literatura e análise de casos. Os resultados mostram que, embora essas soluções sejam altamente seguras, elas enfrentam desafios devido ao alto consumo de energia, tamanho da chave e à falta de padrões claros. Conclui-se que, para alcançar uma segurança quântica eficaz, será fundamental otimizar algoritmos, reduzir os requisitos de hardware e definir protocolos eficientes. Este trabalho fornece insights para proteger dados no ecossistema internet das coisas contra novas ameaças quânticas.

Palavras-chave: entrelaçamento; algoritmos híbridos; miniaturização; teorema da não clonagem; retículos

Periocidad Semestral
Vol. 8, núm. 3
revistatsede@tsachila.edu.ec

Recepción: 18-06-2025
Aprobación: 30-09-2025
Publicación: 25-12-2025

URL:
http://tsachila.edu.ec/ojs/index.php/TSEDE/issue/archive

Introducción

Al conectar en tiempo real a millones de dispositivos, el internet de las cosas (IoT) ha revolucionado la vida contemporánea. Sin embargo, esta expansión también revela vulnerabilidades importantes, pues la mayoría de los equipos dependen de criptografía convencional como la ECC o RSA, que están amenazadas por los avances en computación cuántica. Algoritmos como el de Short evidencian que las protecciones actuales corren el riesgo de volverse obsoletas en un futuro próximo, poniendo en peligro la integridad de los sistemas que se utilizan ampliamente. (Chen et al., 2021).

Según (Baccelli, 2022)la historia del IoT muestra que, en los años setenta, surgió de la domótica X10 y se convirtió en un ecosistema masivo durante la década del 2010. Al mismo tiempo, la computación cuántica se originó en las décadas de 1980 y 1990 con la formalización de los primeros algoritmos y modelos teóricos, que actualmente constituyen una amenaza directa para la seguridad digital.

En cuanto a la computación cuántica, esta surgió en los años ochenta con la sugerencia de Paul Benioff de una máquina de Turing cuántica. David Deutsch, además, formalizó el concepto de una computadora cuántica universal. Los algoritmos de Shor y Grover, desarrollados en los años noventa y dos mil, constituyeron un hito, al igual que la creación de los qubits por laboratorios como IBM y Los Álamos, lo cual sentó las bases para una revolución cuántica (Bonillo, 2013).

El reto presente consiste en identificar métodos de seguridad factibles para los dispositivos IoT, que se ven afectados por restricciones energéticas, de procesamiento y de costos; Estas limitaciones obstaculizan la implementación de soluciones cuánticas sofisticadas. El problema principal de investigación es esta disparidad entre

la amenaza inmediata y las soluciones prácticas: ¿de qué manera salvar al IoT frente a los peligros de la computación cuántica sin perjudicar su accesibilidad y eficacia?

El marco teórico se sustenta en cinco ejes: los fundamentos del internet de las cosas y la computación cuántica, la mecánica cuántica aplicada a la seguridad, criptografía cuántica, los algoritmos cuánticos, y las limitaciones prácticas de su implementación. (Alagic et al., 2023).

Metodología

La investigación se desarrolló en un entorno de análisis documental sin delimitación geográfica, centrándose en una revisión bibliográfica global sobre el uso de la computación cuántica en la seguridad de datos para el internet de las cosas. Se adoptó un enfoque cualitativo con un nivel explicativo, utilizando un diseño no experimental de tipo bibliográfico-documental. Este diseño permitió explorar la factibilidad de implementar soluciones de criptografía cuántica en entornos del internet de las cosas, apoyándose en fuentes teóricas disponibles públicamente.

Población, Muestra y Muestreo

La población de estudio incluyó fuentes académicas y técnicas relacionadas con la computación cuántica, la criptografía cuántica y la seguridad en el internet de las cosas, abarcando libros, artículos científicos y documentos técnicos publicados hasta 2025. Se empleó un muestreo no probabilístico intencional, seleccionando fuentes relevantes como IEEE Xplore, ScienceDirect y ResearchGate, así como publicaciones de organismos como el NIST (Instituto Nacional de Estándares y Tecnología) y la UIT (Unión Internacional de Telecomunicaciones). Se dio prioridad a documentos que

abordaran tecnologías específicas, como la distribución cuántica de claves, algoritmos basados en retículas y enfoques híbridos en entornos del internet de las cosas.

Variables de Estudio

Las variables principales analizadas incluyeron: Viabilidad de implementación: Evaluada en función del consumo energético, el tamaño de las claves y la compatibilidad con dispositivos del internet de las cosas de recursos limitados. Resistencia a ataques cuánticos: Centrada en la capacidad de algoritmos cuánticos y distribución de claves para proteger datos frente a algoritmos cuánticos como los de Shor y Grover. Limitaciones técnicas: Enfocadas en restricciones de hardware, falta de estandarización y escalabilidad en sistemas IoT.

Métodos y Técnicas

Se empleó una metodología de revisión bibliográfica sistemática, siguiendo un protocolo estructurado para garantizar la reproducibilidad. Los pasos realizados fueron los siguientes:

Delimitación del tema: Se definieron los conceptos clave (computación cuántica, criptografía cuántica, seguridad) y los objetivos de la investigación.

Búsqueda sistemática: Se realizaron búsquedas en bases de datos académicas utilizando palabras clave como "quantum computing", "IoT security", "QKD". Se priorizaron artículos de revistas indexadas, libros y documentos técnicos del NIST.

Selección de fuentes: Se evaluaron los resúmenes y se seleccionaron documentos relevantes según su pertinencia, calidad y relación con los objetivos del estudio. Se excluyeron publicaciones no revisadas por pares o con información obsoleta.

Análisis de casos: Se examinaron casos documentados sobre implementaciones de criptografía cuántica en el internet de las cosas, así como experimentos con distribución de claves en redes restringidas.

No se utilizaron métodos o técnicas inusuales, pero se adaptó el análisis comparativo para incluir esquemas visuales, como la Tabla 1, que sintetizó las características de algoritmos cuánticos (crystals kyber, saber, ntruencrypt, mceliece) en términos de consumo energético, tamaño de claves y rendimiento en dispositivos IoT.

Instrumentos de Recogida de Datos

Las principales herramientas fueron las fuentes de bases de datos académicas mencionadas, que permitieron organizar y citar fuentes de forma eficiente. No se crearon instrumentos específicos, ya que el estudio se basó en literatura existente. Las técnicas de recolección incluyeron lectura crítica, síntesis de información y elaboración de resúmenes analíticos

Métodos de Análisis

El análisis fue cualitativo, basado en la interpretación crítica de las fuentes. No se emplearon herramientas estadísticas, dado el enfoque documental. Se utilizaron esquemas comparativos y categorías analíticas para identificar fortalezas, limitaciones y tendencias de las tecnologías estudiadas. Los resultados se presentaron en tablas, como un esquema (Tabla 2) que mostró la compatibilidad de los algoritmos con el internet de las cosas.

El Internet de las cosas (IoT)

El internet de las cosas o IoT por sus siglas en inglés, se trata de una tecnología capaz de comunicar objetos físicos con el internet haciéndolos capaces de darles una

inteligencia artificial y lo que hace posible que estos hagan acciones a través de sensores y otros dispositivos, todo esto bajo una estructura de comunicación que les permite recibir mandatos y dar respuestas (Andrés, 2018).

Computación cuántica

La computación cuántica está basada en la mecánica cuántica, a diferencia de una computadora normal que usa bits, en la computación cuántica se usa qubits que se caracterizan por tener múltiples estados al mismo tiempo, lo que los hace capaces de resolver los problemas complejos en menor tiempo, esta tecnología supera incluso el procesamiento de las supercomputadoras actuales, aunque su único problema es la escalabilidad y errores que se podrán corregir a futuro (Awasthi, 2024).

Seguridad en el internet de las cosas

El ambiente del internet de las cosas es ampliamente inseguro por tener envió de información bidireccional y muchos dispositivos interconectados, esto lo hace susceptible a ataques como robo de información, malware que corrompan el software y deteriore el funcionamiento. Esto es terrible porque el IoT entre todos sus servicios integra la seguridad de hogares u oficinas, donde de fallar podría traer grandes consecuencias (Aryan, 2025).

Internet de las cosas + Computación cuántica

La computación cuántica es una solución viable e innovadora ante los problemas de inseguridad en el internet de las cosas ya que tiene herramientas de seguridad como la distribución de claves que protege las comunicaciones al detectar cualquier intento malintencionado. Ya los sistemas actuales usados en el internet de las cosas no son suficientes ya que son vulnerados con la computación cuántico como el algoritmo shor

que rompe la criptografía actual como son los sistemas criptográficos RSA y ECC (Chawla & Mehra, 2023).

Criptografía contra ataques cuánticos

Como ya vimos la criptografía se basa en el cifrado por claves de sus datos para evitar que este expuesta y a la vez su descifrado permite a los datos volver a su estado normal siempre y cuando se usa la clave adecuada. Tanto la simétrica como la asimétrica son fundamentales, aunque al ser vulneradas por la computación cuántica son una alternativa a combinar con sistemas cuánticos para incrementar sus beneficios (Rodríguez, 2024).

Criptografía basada en hash

Entre las criptografías actuales que se usan como defensa ante ataques cuánticos esta la criptografía hash, esta se caracteriza por usar algoritmos matemáticos para convertir la longitud de los datos de un valor variable aun fijo, esto le permite proteger contraseñas al ser muy difícil de descifrar, incluso es más resistente a ataques cuánticos que los sistemas tradicionales. Pero necesita hardware optimizado en el caso del interne de las cosas debido a sus recursos limitados (Navarro, 2024).

Criptografía basada en ecuaciones multivariable

Otra de las criptografías usada en la lucha contra ataques cuánticos es la basada en ecuaciones multivariable, que como su nombre lo dice resuelve sistemas de ecuaciones con múltiples variables y se basa en esta dificultad para proteger la información. Usando dos enfoques, primero el enfoque estándar que usa matemáticas lineales para ocultar algo que se puede revertir, y segundo los sistemas mixtos que

son más elaborados, mezclando herramientas algebraicas para que el sistema aguante mejor los intentos de ataques cuánticos (Díaz, 2018).

Criptografía basada en códigos correctores

Este tipo de criptografía usa códigos, como los de Hamming, y funciona añadiendo capas de seguridad matemática al mensaje. Estas capas hacen que el mensaje sea súper difícil de descifrar sin la clave correcta, porque el mensaje está escondido en estructuras matemáticas complicadas, como un laberinto algebraico. Esto vuelve a esta criptografía un dolor de cabeza para descifrar, incluso para los ataques cuánticos (Tolrá, 2019).

Criptografía basada en retículos

Una de las criptografías más usadas y recomendadas para protegerse ante ataques cuánticos es la basada en retículos, igual que las anteriores se apoya en problemas matemáticos muy complejos. Pero la idea clave aquí son las retículas, que son como cuadrículas geométricas en las que cada punto está conectado de forma matemática. Para romper esta criptografía, alguien tendría que resolver problemas como el problema del vector más corto o el problema del vector más. Estos problemas son un dolor de cabeza incluso para las computadoras cuánticas, porque requieren cálculos extremadamente complejos, como buscar una aguja en un pajar infinito (Sancho, 2022).

Criptografía basada en isogenias entre curvas elípticas supersingulares

También existe la criptografía basada en isogenias que son muy seguras, pero pueden ser vulnerables a futuro contra los ataques cuánticos, Aquí es donde entran las curvas elípticas supersingulares y la criptografía basada en isogenias. Estas curvas son una

versión mejorada que elimina esas propiedades conmutativas, haciendo que el candado sea mucho más difícil de forzar, incluso para una computadora cuántica. Intentar descifrar este tipo de sistema sería como intentar ir a un destino exacto sin un mapa (Sánchez, 2021).

Criptografía basada en sistemas híbridos

Las soluciones hibridas nacen como una solución innovadora al combinar algoritmos clásicos con algoritmos nuevos post cuánticos usados en seguridad contra ataques cuánticos, un ejemplo común usado es la combinación de ECDH que es un algoritmo clásico basado en curvas elípticas y new hope que es un algoritmo reciente y prometedor, usa aritmética polinomial en anillos para generar ruido matemático en la información, y evitar interferencias. Además, esta mezcla asegura que los sistemas actuales sigan funcionando sin problemas, porque el componente clásico mantiene la compatibilidad (Mohamed, Yussoff, Saleh, & Hashim, 2020).

Criptografía tradicional vs Criptografía Cuántica

Los sistemas tradicionales que se usan en encriptación de las comunicaciones en el internet de las cosas son RSA y ECC, pero como lo dijimos anteriormente estos son vulnerables ante herramientas de computación cuántica (Shor, 1994). Algunas de las vulnerabilidades identificadas son las causadas por el algoritmo shor, ya que este puede factorizar números enteros muy grandes descifrando sistemas de criptografía con facilidad o ayudando a descifrar mediante muchos intentos. También están la expuesta por el algoritmo Grover que acelerando la búsqueda de en funciones hash y cifrados simétricos reduce la seguridad a la mitad obligando a implementar sistemas con claves mucho más largas y robustas (Grover, 1996).

Contra estas vulnerabilidades nace la criptografía cuántica que busca proteger la comunicación que se da en el internet de las cosas, otorgando estados cuánticos a los datos de la comunicación para no poder ser interceptado y si el estado cuántico se rompe a detectar más facial a quien quiere tener acceso. Aunque esto suena genial, la computación cuántica aún está en desarrollo, tiene limitaciones y falta mucha investigación para poder disfrutar netamente de estas características (Bennett & Brassard, 2014).

Claves y algoritmos

Criptografía simétrica y asimétrica

Criptografía Simétrica (Clave Privada)

Existes formas de cifrar la información de manera tradicional y una es la criptografía simétrica que usa una sola clave para cifrar y descifrar, esta usa la técnica de confusión y difusión para el cifrado de bloques. Lo que la hace rápida y con un buen nivel de seguridad. Pero esto antes de la llegada de la computación cuántica porque esta criptografía es susceptible a algoritmos como grover más los ataques de fuerza bruta (Sánchez, 2021).

Criptografía Asimétrica (Clave Pública)

Por otro lado, está la criptografía asimétrica que usa una clave publica para cifra y una privada para descifrar, como solución a la distribución de claves. Esto le permite tener claves más cortas lo que la hace ideal para el internet de las cosas. Pero de igual manera es susceptible a la computación cuántica como el algoritmo shot que puede debilitar su seguridad (Herrera, 2021).

Algoritmos SHOR y GROVER

Algoritmo de Shor

El algoritmo shor es un punto de inflexión dentro de la criptografía, hay un antes y un después en su aparición, ya que su facilidad en factorizar números enteros grandes es impensable para otros métodos. Este utiliza una subrutina cuántica que se usa en matemáticas llamada “estimación fase”, implementada para resolver problemas. Su impacto fue tal que revoluciono la criptografía actual como RSA Y ECC (Sánchez, 2021).

Algoritmo de Grover

Por otro lado, está el algoritmo de grover el cual aumenta las posibilidades de encontrar las claves correctas y descifrar los sistemas criptográficos actuales. Funciona acelerando las búsquedas en bases de datos no estructuradas, esto no descifra como tal, pero si debilita las claves y obliga a duplicar la protección para que no sea comprometida (Guo, 2023).

Seguridad en el internet de las cosas ante ataques cuánticos

Con la llegada de la computación cuántica se intensificaron los riesgos en seguridad en diversas tecnologías entre ellas el internet de las cosas, además de las criptografías que ya vimos que se implementan para proteger la información, existe otra forma de protegerse frente a las amenazas de la computación cuántica, esta es la distribución cuántica de claves, que usa la mecánica cuántica para generar claves teóricamente inviolables (Bennett & Brassard, 2014).

Distribución cuántica de claves (QKD)

La distribución cuántica de claves da introducción a un enfoque innovador para la seguridad en el internet de las cosas contra ataques cuánticos. Hablamos de un método para compartir claves ultrasecretas entre dispositivos, que usando partículas cuánticas, como fotones de luz. Lo diferente de este método es que no depende de matemáticas complicadas que una computadora potente podría romper, sino de reglas de la mecánica cuántica, que son prácticamente indescifrables. Esta tecnología se apoya en fundamentos teóricos clave: Entrelazamiento cuántico, teorema de no-clonación, QRNG y criptografía cuántica (Xu, Ma, Zhang, Lo, & Pan, 2020).

El entrelazamiento cuántico

El entrelazamiento cuántico en palabras simples es cuando dos partículas quedan conectadas de una manera cuántica, de modo que el estado de una afecta a la otra al instante, sin importar si están a metros o años luz de distancia. Lo más loco es que esta conexión entre ambas no depende de cables, señales ni nada físico. Es como si los dispositivos tuvieran un pacto secreto que solo ellos entienden, y cualquier persona malintencionada que intente colarse rompe el pacto, quedando expuesto (Pirandola et al., 2025).

El teorema de no clonación

También tenemos el método del teorema de no clonación que al igual que el entrelazamiento cuántico al usar la distribución de claves comunica los dispositivos mediante partículas. La diferencia está en que el teorema de no clonación en caso de que una persona mal intencionada intentase copiar una clave, la original se arruina y todos se darían cuenta. El teorema de no clonación protege las claves de ser

duplicadas, y el entrelazamiento asegura que las comunicaciones sean auténticas y seguras. Ambos se complementan y hacen casi imposibles de hackear, incluso con tecnología cuántica (Fan et al., 2025).

Generadores de números aleatorios cuánticos (QRNG)

Otro método usado son los generadores que usa las leyes de la física cuántica para crear números totalmente aleatorios a diferencia de los métodos anteriores esta crea claves criptográficas imposibles de predecir, perfectas para proteger dispositivos en el internet de las cosas contra ataques, incluso los cuánticos. Es una opción muy viable ya que se puede implementar fácil en el internet de las cosas adaptando el hardware, su parte mala es que su costo es algo alto. (Mannalatha, Mishraa, & Pathak, 2023)

Criptografía cuántica

Esta herramienta nace como un complemento a la distribución de claves cuánticas, y como ya la vimos anteriormente se tratan de problemas matemáticos que sean de una dificultad alta y difíciles incluso para las computadoras cuánticas, para así proteger la seguridad en la comunicación de los dispositivos. La combinación de la distribución de claves y la criptografía cuántica se perfila como la solución más robusta para garantizar la seguridad a largo plazo (NIST, 2022).

Algoritmos para criptografía cuántica

Los dispositivos dentro del internet de las cosas requieren algoritmos que equilibren seguridad con un bajo consumo de recursos. A continuación, se destacan los esquemas más adecuados y clasificados por su función y eficiencia:

Tabla 1

Adaptado de Ikim, (2021) y (2025)

Algoritmo	Tipo	Tamaño Clave Pública	Cifrado (bytes)	Velocidad	Consumo Memoria	Seguridad NIST	¿Adecuado para IoT?	Razón
CRYSTALS-Kyber	KEM (Cifrado)	800-1,184	768-1,088	Muy rápido	Bajo	Nivel 1-5	Si	Claves pequeñas, eficiente en energía
NTRU	KEM (Cifrado)	930-1,230	750-1,020	Rápido	Bajo	Nivel 1-3	Si	Seguridad probada, claves más grandes que Kyber
CRYSTALS-Dilithium	Firma Digital	2400-3,800	1,700-2,500	Moderado	Moderado	Nivel 1-5	Depende	Firmas pequeñas, Usa más memoria que Kyber
Falcon	Firma Digital	800-1,200	1,200-1,700	Lento	Alto	Nivel 1-5	No	Difícil en dispositivos limitados
McEllece (Clásico)	KEM (Cifrado)	1Mill – 3Mill	-	Muy lento	Muy Alto	Nivel 1-3	No	Claves enormes, consume muchos recursos
Rainbow	Firma Digital	-	66-130	Moderado	Bajo	Nivel 1-3	Riesgoso	Firmas pequeñas con vulnerabilidades

Fuente: Elaboración propia

Aplicación de la computación cuántica a él internet de las cosas

La criptografía cuántica en dispositivos dentro del internet de las cosas enfrenta retos por las limitaciones de los dispositivos ante el gran consumo de recursos que generan las tecnologías cuánticas. Algunos algoritmos actuales, aunque si son resistentes a ataques cuánticos, usan claves estivamente grandes que demandan mucha memoria y energía. Podemos ver también los sistemas de ecuaciones multivariables, que ofrecen firmas compactas, pero el descifrado es lento. Además, los esquemas basados en retículas, como que son más eficientes, aunque la gran mayoría requieren

optimización de hardware. Finalmente, los sistemas híbridos, que combinan criptografía clásica y cuántica, son viables a corto plazo, pero menos eficientes a largo plazo debido a la carga computacional (Sánchez, 2021).

Futuro de la computación cuántica en el internet de las cosas

La integración de criptografía cuántica en dispositivos dentro del internet de las cosas enfrenta retos significativos debido a las limitaciones de recursos y la complejidad de los algoritmos. Algoritmos como: CRYSTALS-Kyber, que son basados en retículas, consumen más memoria y energía que los esquemas clásicos como RSA y ECC, lo que afecta el rendimiento en tiempo real y la duración de baterías. Además, las claves de mayor tamaño plantean desafíos de almacenamiento y ancho de banda, mientras que la escalabilidad y las restricciones de hardware complican su despliegue en el internet de las cosas (Mahdi & Abdullah, 2025).

Para superar estos obstáculos, las futuras estrategias incluyen optimizar algoritmos para minimizar el uso de recursos, incorporar chips para acelerar el hardware y desarrollar sistemas híbridos que combinen criptografía clásica y cuántica. Por otro lado, será clave crear reglas protocolos para que todos los dispositivos hablen el mismo idioma, garantizar que trabajen juntos sin problemas y diseñar sistemas inteligentes para manejar las claves criptográficas de forma segura (ITC, 2025).

Resultados y Discusión

Esta investigación analizó críticamente las posibilidades de aplicar criptografía cuántica en dispositivos del internet de las cosas, evaluando la viabilidad de soluciones como: la criptografía cuántica, la distribución cuántica de claves y algoritmos como:

crystals kyber, saber y ntruencrypt. Los resultados muestran que, aunque estas tecnologías ofrecen alta seguridad frente a ataques cuánticos, su implementación en el internet de las cosas está limitada por el consumo energético, la capacidad de procesamiento y las características del hardware y toca esperar nuevos avaneces en disminución de microcontroladores (Mahdi & Abdullah, 2025).

Con la información obtenida se nos muestra la eficacia de esquemas híbridos que combinan criptografía de algoritmos clásica y cuántica, en esta investigación se encontró que estos modelos, aunque útiles teóricamente para la seguridad, generan una carga computacional significativa en dispositivos de bajo consumo, afectando su eficiencia y aumentando sus costos. Además, los hallazgos confirman la amenaza del algoritmo de Shor a sistemas tradicionales actuales como RSA y ECC, esto genera la necesidad de adoptar esquemas basados en retículas que según este estudio son los más compatibles con IoT (Gidney & Ekera, 2020).

Más datos obtenidos de la investigación indican que algoritmos cuánticos como: mceliece, que requieren claves extensas, son poco prácticos en el internet de las cosas debido a sus altas demandas de memoria y almacenamiento. En cambio, algoritmos como crystals kyber, respaldados por el NIST, destacan por su fluides para entornos con recursos limitados, mostrando mayor adaptabilidad. Estos resultados resaltan que la computación cuántica impulsa tanto una amenaza como una oportunidad para innovar en estrategias de seguridad digital (Sánchez, 2021).

Los hallazgos también señalan la necesidad urgente de rediseñar los sistemas de seguridad en el internet de las cosas, priorizando algoritmos cuánticos ligeros, la estandarización de protocolos (para mejorar las comunicaciones) y el desarrollo de

hardware especializado. Así se facilita una transición segura hacia la era cuántica, manteniendo la funcionalidad y vida útil de los dispositivos (ITC, 2025).

La revisión bibliográfica realizada proporcionó información clave sobre la viabilidad de implementar distribución de claves y criptografía cuántica en entornos IoT. los temas propuestos responden a los objetivos del estudio mediante análisis comparativos de algoritmos y respuesta a posibles interrogantes, consolidando una base sólida para futuras investigaciones y desarrollos en seguridad (Mahdi & Abdullah, 2025).

¿Qué tan viables son las soluciones de criptografía cuántica en dispositivos IoT con recursos limitados?

Los datos plasmados en el marco teórico revelan que algoritmos cuánticos como: crystals kyber, saber y ntruencrypt ofrecen una fuerte resistencia frente a ataques cuánticos, especialmente contra el algoritmo de Shor, quien ya vimos que pone en riesgo sistemas tradicionales como RSA y ECC. Analizando cada uno como se plasmó en la Tabla 1 donde se expuso su: velocidad, almacenamiento, la capacidad de memoria, tiempos de cifrado obtenidos de diversas fuentes y si es compatible con el internet de las cosas, se hizo una evaluación de algoritmos cuánticos donde:

- **McEliece:** aunque en seguridad llega a nivel 3, utiliza claves de hasta 1 MB, lo que lo hace poco práctico para dispositivos en el internet de las cosas con memoria limitada (Sánchez, 2021).
- **Crystals Kyber**: respaldado por el NIST es uno de los más seguro llegando hasta nivel 5, se distingue por generar claves compactas y gracias a ello su bajo consumo y además por su eficiencia en chips microcontroladores, logrando

tiempos de cifrado y descifrado cortos, lo hace ideal para el internet de las cosas (Mahdi & Abdullah, 2025).

- **Ntruencrypt:** logran un balance entre seguridad con un nivel 3 y consumo de memoria, sus implementaciones en hardware reducen los tiempos de operación. Sin embargo, su consumo energético sigue siendo algo alto para los estándares, lo que afecta la duración de la batería en dispositivos en el internet de las cosas (Sánchez, 2021).

Estos resultados destacan que la optimización de algoritmos basados en retículas es crucial para su adopción en IoT. La discusión subraya que, aunque los algoritmos cuánticos son teóricamente viables, su implementación práctica requiere avances en miniaturización de hardware y optimización de software para reducir la sobrecarga computacional (ITC, 2025).

Tabla 2

Comparación de algoritmos cuánticos en IoT. Extraído de (Ikim, Ducas, Pöppelmann, & Schwabe, 2020)

Algoritmo	Tamaño de clave (bytes)	Tiempo de cifrado (ms)	Consumo energético	Compatibilidad con IoT
crystals Kyber	800-1,184	0.1-0.3	Moderado	Alta
saber	1,000-1,500	0.2-0.4	Moderado	Alta
ntruencrypt	700-1,000	0.3-0.5	Moderado	Media-Alta
mceliece	~1,000,000	1.0-2.0	Alto	Baja

Fuente: Elaboración Propia

Análisis en la práctica:

Crystals Kyber: Tiene la mejor relación entre eficiencia y seguridad; su cifrado de tiempo corto y sus claves compactas lo convierten en la opción perfecta para los microcontroladores que consumen poca energía.

Saber: Tiene un equilibrio adecuado entre velocidad y memoria, aunque con claves un poco más largas, continúa siendo compatible con IoT

NTRUEncrypt: A pesar de ser eficaz en hardware específico, su alto consumo energético impacta la autonomía de los dispositivos IoT.

McEliece: Debido a que presenta llaves excesivamente grandes (hasta 1 MB), se vuelve inviable para sensores y aparatos con poca memoria.

¿Cómo impacta la distribución cuántica de claves en la seguridad de IoT?

La distribución de claves cuántica es un método innovador que complementa a la criptografía cuántica y ayuda a crear sistemas más seguros, en el contexto del internet de las cosas permite que la comunicación entre dispositivos sea inviolable usando bases de la mecánica cuántica y detectando intrusos aun sin una conexión física, usando la conexión entre partículas para dicho propósito. Su parte negativa es que es algo relativamente nuevo y aunque proporciona seguridad incondicional, su implementación en el internet de las cosas depende de avances en la miniaturización de componentes cuánticos. Además de que su arquitectura aun no es la indicada, haciendo que sus costos sean altos y de implementarse su consumo de energía duplicaría al de un sistema normal (Xu, Ma, Zhang, Lo, & Pan, 2020).

¿Qué desafíos persisten en la adopción de criptografía cuántica en IoT?

Los desafíos que son un punto importante por mejorar al momento de adoptar esta tecnología a él internet de las cosas son el consumo energético, el tamaño de las

claves y la comunicación entre dispositivos. En el caso del consumo el hardware usado en para la criptografía cuántica como chips, tienden a aumentar el consumo y deteriorar las baterías debido a su alto procesamiento, algoritmos como crystals Kyber por ejemplo requieren más recursos que los sistemas tradicionales, por otro lado, el tamaño de las claves producido por algunos sistemas criptográficos cuánticos genera mayor memoria, generando problemas en el almacenamiento. Y por último la comunicación se torna un problema por la falta de protocolos globales para los dispositivos, ya que sin eso se vuelve tedioso el proceso (Kannwischer, Niederhagen, Rodríguez-Henríquez, & Schwabe, 2023).

¿Qué tan efectivos son los sistemas híbridos en la transición hacia la criptografía cuántica?

La criptografía basada en sistemas híbridos como lo vimos anteriormente en la combinación de algoritmos clásicos como ECDH y algoritmos nuevos basado en mecánica cuántica como new hope, en las pruebas realizadas en Google con la misma combinación de algoritmos reflejo que facilitan la compatibilidad con las infraestructuras actuales en el internet de las cosas. En cuanto a consumo energético tienen un punto negativo ya que aumenta hasta en eun 25% el consumo, pero sus tiempos de cifrado son relativamente bajos muy parecidos a los algoritmos clásicos con un máximo de 0.4 ms (Langley, 2020).

Conclusiones

La computación cuántica es un hito para la seguridad de internet de las cosas, ya que tiene el potencial de hacer obsoletos los sistemas criptográficos tradicionales y, al

mismo tiempo, permite desarrollar soluciones más sólidas y sostenibles. Los resultados de esta investigación evidencian que evidencian que los algoritmos post-cuánticos basados en retículas , específicamente Crystals Kyber y Saber, brindan un equilibrio entre eficiencia los algoritmos post-cuánticos basado seguridad que los hace los postulantes más factibles para aparatos con recursos restringidos en retículas, específicamente Crystals Kyber y Saber, brindan un equilibrio entre eficiencia y seguridad que los hace los postulantes más factibles para aparatos con recursos restringidos. No sin embargo, la aplicación de sistemas híbridos y la distribución cuántica de claves aún se enfrenta a obstáculos en lo que respeta a la estandarización de los protocolos, el consumo de energía y la miniaturización del hardware. Así, queda demostrado que la posibilidad de fusionar innovaciones cuánticas con diseños optimizados y accesibles será lo que determinará el futuro de la seguridad en IoT. De este modo, se asegura una transición paulatina hacia un entorno capaz de resistir las amenazas emergentes de la era cuántica.

Referencias Bibliográfica

Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., . . . Smith-Tone, D. (2023). *Estándares de criptografía post-cuántica (NIST PQC Project).* NIST. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf

Andrés, M. B. (2018). *INTERNET DE LAS COSAS.* Madrid: © Editorial Reus, S. A. Retrieved from https://www.editorialreus.es/media/pdf/primeraspaginas_9788429020380_internetdelascosas.pdf

Aryan, N. (2025). IoT Security Risks: Challenges and Solutions for a Connected World. *IJARISCT*, 10. Retrieved from https://www.researchgate.net/publication/390555670_IoT_Security_Risks_Challenges_and_Solutions_for_a_Connected_World

Awasthi, B. K. (2024). *Theory of Quantum Computing.* Retrieved from https://www.researchgate.net/publication/378475288_Theory_of_Quantum_Computing

Baccelli, E. (2022). *Internet de las cosas IoT.* Francia: Inria. Retrieved from https://www.inria.cl/sites/default/files/2022-12/libro-blanco-iot-es.pdf

Bennett, C., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *sciencedirect*, 8. Retrieved from https://pdf.sciencedirectassets.com/271538/1-s2.0-S0304397514X00411/1-s2.0-S0304397514004241/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEE4aCXVzLWVhc3QtMSJHMEUCIAd3Nwmi%2B10dtF4PDb7BxlPhFaTniLKGaPpK1H87%2BAvBAiEAvVMbR93kjXJNmyobCfz3%2FyiloCPw79ZUAoib%2

Bonillo, V. (2013). *Principios Fundamentales de la Computacion Cuantica.* Coruña: Universidad de Coruña. Retrieved from https://enginyeriainformatica.cat/wp-content/uploads/2016/05/PRINCIPIOS-FUNDAMENTALES-DE-COMPUTACI%C3%93N-CU%C3%81NTICA.pdf

Chawla, D., & Mehra, P. S. (2023). A Survey on Quantum Computing for Internet of Things Security. *Elsevier B.V.*, 10. doi:https://doi.org/10.1016/j.procs.2023.01.195

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2021). *Report on Post-Quantum Cryptography.* NIST. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

Díaz, J. L. (2018). *Métodos Algebraicos en Criptografía Multivariable .* Madrid. Retrieved from https://www.icmat.es/Thesis/2018/Tesis_Jorge_Linde.pdf

Einstein, A., Podolsky, B., & Rosen, N. (1935). Can Quantum-Mechanical Description of Physical Reality be Considered Complete? *American Physical Society*, 7. Retrieved from https://cds.cern.ch/record/1060284/files/PhysRev.48.696.pdf

Fan, H., Wang, Y.-N., Jing, L., Yue, J.-D., Shi, H.-D., Zhang, Y.-L., & Mu, L.-Z. (2014). Quantum Cloning Machines and the Applications. *QUANT-PH*, 97. Retrieved from https://arxiv.org/pdf/1301.2956

Gidney, C., & Ekera, M. (2020). *How to factor 2048 bit RSA integers in 8 hours using 20 millon noisy qubits.* arxiv. Retrieved from https://arxiv.org/pdf/1905.09749

Grover, L. (1996). A fast quantum mechanical algorithm for database search. *arxiv*, 8. Retrieved from https://arxiv.org/pdf/quant-ph/9605043

Guo, C. (2023). Grover's Algorithm – Implementations and Implications. *TPCEE*, 15. Retrieved from https://www.researchgate.net/publication/369470958_Grover's_Algorithm_-_Implementations_and_Implications

Herrera, G. M. (2021). Encriptación y cifrado de datos en plataformas IOT. *Escuela Técnica Superior de Ingeniería*, 58. Retrieved from https://biblus.us.es/bibing/proyectos/abreproy/93764/fichero/TFG-3764+MART%C3%8DNEZ+HERRERA%2C+GUILLERMO.pdf

ITC. (2025). *Quantum Technologies And The Future Of Learning.* r&d. Retrieved from https://www.itcilo.org/sites/default/files/2025-04/Quantum%20for%20learning_WEB-2.pdf

Kannwischer, M. J., Niederhagen, R., Rodríguez-Henríquez, F., & Schwabe, P. (2023). *Post-Quantum Implementations.* ISTE. Retrieved from https://kannwischer.eu/papers/2023_pqimpl.pdf

Langley, A. H. (2020). *Elliptic curves for security.* google. Retrieved from https://www.rfc-editor.org/rfc/rfc7748.txt

lkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2020). *Post-quantum key exchange on ARM Cortex-M0. Journal of Cryptographic Engineering.* IEEE. Retrieved from https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_alkim.pdf

Mahdi, L. H., & Abdullah, A. A. (2025). ortifying Future IoT Security: A Comprehensive Review on Lightweight Post-Quantum Cryptography. *Engineering, Technology & Applied Science Research*, 20. Retrieved from https://www.researchgate.net/publication/390506689_Fortifying_Future_IoT_Security_A_Comprehensive_Review_on_Lightweight_Post-Quantum_Cryptography

Mannalatha, V., Mishraa, S., & Pathak, A. (2023). A Comprehensive Review of Quantum Random Number Generators: Concepts, Classification and the Origin. *QUANT-PH*, 44. Retrieved from https://arxiv.org/pdf/2203.00261

Mohamed, N. N., Yussoff, Y. M., Saleh, M. A., & Hashim, H. (2020). Hybrid Cryptographic Approach For Internet Of Things Applications: A REVIEW. *Journal of ICT*, 10. Retrieved from https://www.researchgate.net/publication/342159335_HYBRID_CRYPTOGRAPHIC_APPROACH_FOR_INTERNET_OF_THINGS_APPLICATIONS_A_REVIEW

Navarro, A. I. (2024). Una función hash desde cero. *Universidad Politécnica De Madrid*, 59. Retrieved from https://oa.upm.es/83727/1/TFG_ANA_ISABEL_TOLEDO_NAVARRO.pdf

NIST. (2022). NIST Post-Quantum Cryptography. *NIST*, 100. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

Pirandola, Andersen., Banchi, ., B., Bunandar, Colbec, . . . Gehring. (2025). Advances in Quantum Cryptography. *DTU*, 119. Retrieved from https://backend.orbit.dtu.dk/ws/portalfiles/portal/257296437/1906.01645.pdf

Proos, J., & Zalka, C. (2024). Shor's discrete logarithm quantum algorithm for elliptic curves. *arxiv*, 34. Retrieved from https://arxiv.org/pdf/quant-ph/0301141

Rodríguez, M. R. (2024). *Criptografía Postcuántica.* Villadolid: Universidad de Villadolid. Retrieved from https://uvadoc.uva.es/bitstream/handle/10324/71196/TFG-G6850.pdf?sequence=1

Rosado, Á. R. (2018). *Estado de la criptografía post-cuántica y simulaciones de algoritmos post-cuánticos.* Madrid. Retrieved from https://openaccess.uoc.edu/bitstream/10609/89026/6/alvaroreyesTFM1218memoria.pdf

Sánchez, J. S. (2021). Aplicación de Sistemas Post-Cuánticos a la Seguridad de Nodos IoT. *upm*, 80. Retrieved from https://oa.upm.es/66693/1/TFM_JAIME_SENOR_SANCHEZ.pdf

Sancho, A. L. (2022). Criptografía basada en retículos. *Universidad de Zaragoza*, 39. Retrieved from https://zaguan.unizar.es/record/125089/files/TAZ-TFG-2022-3439.pdf;

Shor, P. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *IEEE*, 11. Retrieved from https://cc.ee.ntu.edu.tw/~rbwu/rapid_content/course/QC/Shor1994.pdf

Tolrá, D. M. (2019). *Criptografía post-cuántica y códigos correctores de errores.* Retrieved from https://upcommons.upc.edu/bitstream/handle/2117/133124/136200.pdf

Xu, F., Ma, X., Zhang, Q., Lo, H.-K., & Pan, J.-W. (2020). Secure quantum key distribution with realistic devices. *Institute for Interdisciplinary Information Sciences*, 68. Retrieved from https://arxiv.org/pdf/1903.09051