Criptografía Post-Cuántica: Desafíos y Oportunidades

Lic. Alberto Bermudez Blanco. Ing
Maestría Profesional en Ciberseguridad
Universidad Internacional San Isidro Labrador
San José, Costa Rica
Beto.an.2498@gmail.com

***Resumen* — Este documento examina la creciente necesidad de desarrollar y adoptar sistemas criptográficos que sean seguros frente a los avances en la computación cuántica. Con el potencial de las computadoras cuánticas para romper la criptografía actual, la criptografía post-cuántica surge como una solución imprescindible. Este artículo presenta una revisión de los desafíos y oportunidades que enfrentan los algoritmos criptográficos post-cuánticos, analizando las diferentes técnicas propuestas, su estado actual, y las perspectivas futuras.**

Palabras clave: Criptografía post-cuántica, computación cuántica, seguridad de la información, algoritmos criptográficos, NIST..

I. INTRODUCCIÓN

La computación cuántica ha capturado la imaginación de científicos y tecnólogos debido a su potencial para resolver problemas que son inabordables para las computadoras clásicas. Sin embargo, este avance también plantea amenazas significativas para la criptografía, que es la base de la seguridad digital moderna. Los algoritmos criptográficos actuales, como RSA y ECC, se basan en la dificultad de resolver problemas matemáticos que, hasta ahora, han sido intratables para las computadoras clásicas. Con la llegada de las computadoras cuánticas, estos problemas podrían resolverse en tiempo polinomial, poniendo en peligro la seguridad de sistemas que protegen todo, desde transacciones financieras hasta comunicaciones gubernamentales.

La criptografía post-cuántica surge como una respuesta a esta amenaza. A diferencia de la criptografía clásica, que se basa en problemas matemáticos actualmente intratables, la criptografía post-cuántica se fundamenta en problemas que, según se cree, son difíciles de resolver tanto para las computadoras clásicas como para las cuánticas. Este artículo se enfoca en una revisión detallada de los desafíos y oportunidades en la criptografía post-cuántica, explorando los enfoques más prometedores, los desafíos de implementación, y las posibles direcciones futuras en este campo.

II. DESARROLLO DE CONTENIDOS

A. Amenazas cuánticas a la criptografía actual

La base de la seguridad en la criptografía moderna es la complejidad computacional. Los sistemas como RSA y ECC dependen de la dificultad para resolver ciertos problemas matemáticos, como la factorización de enteros grandes y el cálculo del logaritmo discreto. Sin embargo, los algoritmos cuánticos, como el algoritmo de Shor, tienen el potencial de resolver estos problemas de manera eficiente utilizando la superposición y el entrelazamiento cuántico. A continuación, se discute en detalle cómo estos algoritmos cuánticos ponen en peligro la seguridad de los sistemas criptográficos actuales:

1. **El Algoritmo de Shor y la Factorización**:
   El algoritmo de Shor, propuesto en 1994, es un algoritmo cuántico que puede factorizar números enteros en tiempo polinomial. Esto representa una amenaza directa para RSA, que basa su seguridad

en la dificultad de factorizar un número grande en sus factores primos. En una computadora clásica, este problema es tan difícil que sirve como la base para la criptografía de clave pública. Sin embargo, una computadora cuántica equipada con el algoritmo de Shor podría resolver este problema en una fracción del tiempo, descomponiendo un número en sus factores primos y, por lo tanto, rompiendo la seguridad de RSA.

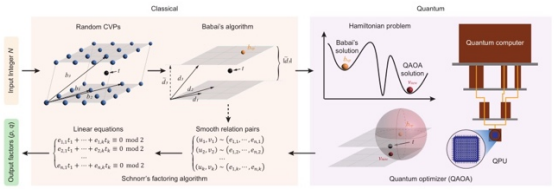

Figura 1 cuántica al cifrado RSA

2. **El Algoritmo de Shor y el Logaritmo Discreto:**
   Además de la factorización, el algoritmo de Shor también puede resolver el problema del logaritmo discreto, que es la base de la seguridad en ECC (Elliptic Curve Cryptography). ECC es ampliamente utilizado debido a su eficiencia y seguridad en comparación con otros métodos de clave pública. Sin embargo, si una computadora cuántica puede resolver el logaritmo discreto, como lo permite el algoritmo de Shor, todo el sistema ECC estaría en riesgo.
3. **El Algoritmo de Grover y la Búsqueda en Espacio de Claves:**
   Aunque el algoritmo de Grover no puede romper la criptografía de clave pública como lo hace el algoritmo de Shor, tiene implicaciones significativas para los algoritmos de clave simétrica. Grover permite una búsqueda cuadrática en el espacio de claves, lo que reduce el tiempo necesario para un ataque de fuerza bruta. Por ejemplo, si un sistema criptográfico utiliza una clave de 256 bits, Grover podría reducir la efectividad de esa clave a una de 128 bits, lo que requiere que los tamaños de clave sean reconsiderados para mantener la seguridad.

B. Principales enfoques en criptografía post-cuántica

Enfoque	Descripción	Ventajas	Desventajas
Criptografía basada en retículas	Utiliza problemas geométricos difíciles como el problema del vector más corto.	Alta seguridad y flexibilidad, adecuado para múltiples aplicaciones.	Claves más grandes, mayor complejidad computacional.
Criptografía basada en códigos	Se basa en problemas de decodificación de códigos, como los códigos Goppa.	Probado con el tiempo, altamente seguro frente a ataques cuánticos.	Claves públicas grandes, menos eficiente en ciertas aplicaciones.
Funciones hash	Emplea funciones hash resistentes a colisiones para crear firmas y cifrados.	Resistente a ataques cuánticos, paralelizable y eficiente.	No tan flexible como otros enfoques para ciertas aplicaciones.
Isogenias de curvas elípticas	Utiliza la dificultad de encontrar isogenias entre curvas elípticas.	Ofrece un buen equilibrio entre seguridad y eficiencia.	Complejo de implementar, todavía en desarrollo.

Tabla 1 Comparación de Enfoques de Criptografía Post-Cuántica

Con el avance de la computación cuántica, se han propuesto varios enfoques para desarrollar algoritmos criptográficos que puedan resistir ataques cuánticos. Estos enfoques están diseñados para ser seguros tanto para computadoras clásicas como cuánticas. A continuación, se describen en detalle los enfoques más destacados:

1. **Criptografía basada en retículas (lattices)**
   La criptografía basada en retículas es uno de los enfoques más prometedores para la criptografía post-cuántica. Las retículas son estructuras geométricas que permiten la formulación de problemas matemáticos complejos, como el problema del vector más corto (SVP) y el problema de la decodificación con errores (LWE). Estos problemas son difíciles de resolver tanto para computadoras clásicas como cuánticas, lo que los convierte en una base sólida para la criptografía post-cuántica.
   - **NTRU:** Un sistema de criptografía de clave pública basado en retículas, NTRU, ha demostrado ser eficiente y seguro. Su estructura matemática le permite resistir ataques cuánticos, lo que lo convierte en un candidato fuerte para la estandarización. NTRU es especialmente relevante en aplicaciones donde la velocidad y la eficiencia son críticas.

- **Learning With Errors (LWE):** LWE es otro enfoque basado en retículas que ha ganado popularidad. Su flexibilidad le permite ser utilizado en una variedad de aplicaciones criptográficas, incluyendo cifrado, firmas digitales y esquemas de intercambio de claves. LWE es especialmente valorado por su seguridad y la dificultad de resolverlo incluso para computadoras cuánticas.

2. **Criptografía basada en códigos** La criptografía basada en códigos se basa en problemas de teoría de códigos, como el problema de la decodificación de códigos lineales. Un ejemplo clásico de criptografía basada en códigos es el sistema McEliece, que utiliza códigos Goppa para construir un sistema de cifrado de clave pública. McEliece ha resistido la prueba del tiempo y es considerado seguro frente a ataques cuánticos.
    - **Sistema McEliece:** Aunque McEliece ofrece una alta seguridad, uno de sus principales inconvenientes es el tamaño grande de las claves públicas. Sin embargo, en aplicaciones donde la seguridad es primordial, como en comunicaciones gubernamentales y militares, McEliece sigue siendo una opción viable.

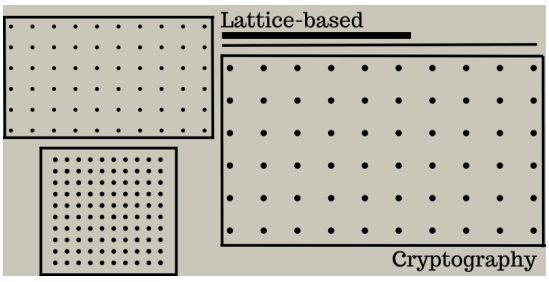

Figura 2 Criptografía basada en retículas

- **LDPC y códigos polares:** Los códigos de baja densidad de paridad (LDPC) y los códigos polares también han sido investigados en el contexto de la criptografía post-cuántica. Estos códigos, que se utilizan ampliamente en comunicaciones modernas, están siendo adaptados para su uso en esquemas criptográficos que sean resistentes a ataques cuánticos.

3. **Funciones hash y árboles de Merkle**: Las funciones hash son fundamentales en la criptografía moderna, utilizadas en una amplia gama de aplicaciones, desde la firma digital hasta la integridad de los datos. En el contexto de la criptografía post-cuántica, las funciones hash resistentes a colisiones se utilizan para construir esquemas criptográficos que sean seguros frente a ataques cuánticos.
    - **Árboles de Merkle:** Los árboles de Merkle se utilizan para generar firmas digitales seguras. Estas firmas son resistentes a ataques cuánticos debido a la dificultad de encontrar colisiones en las funciones hash utilizadas. Además, las funciones hash son inherentemente paralelizables, lo que las hace adecuadas para la computación en hardware especializado.
    - **Esquemas basados en funciones hash:** Los esquemas de cifrado y firma digital basados en funciones hash están siendo cada vez más investigados como soluciones post-cuánticas. Estos esquemas aprovechan la eficiencia y la resistencia de las funciones hash para crear sistemas criptográficos seguros.
4. **Isogenias de curvas elípticas**: Las isogenias entre curvas elípticas representan un enfoque más reciente en la criptografía post-cuántica. Este enfoque se basa en la dificultad de encontrar isogenias entre curvas elípticas, lo que proporciona una base segura para la construcción de esquemas criptográficos.
    - **SIDH (Supersingular Isogeny Diffie-Hellman):** SIDH es un protocolo que ha ganado atención como un candidato viable para la criptografía post-cuántica. Ofrece un equilibrio interesante entre seguridad y

eficiencia, y su estructura matemática única lo hace resistente a ataques cuánticos conocidos. Sin embargo, la implementación práctica de SIDH todavía enfrenta desafíos, particularmente en términos de rendimiento y resistencia a ciertos tipos de ataques.

C. Estandarización y evaluación por parte del NIST:

El proceso de estandarización de la criptografía post-cuántica es un paso crucial para su adopción a nivel global. El Instituto Nacional de Estándares y Tecnología (NIST) ha estado liderando el esfuerzo para evaluar y seleccionar algoritmos criptográficos que sean seguros frente a ataques cuánticos. Este proceso ha involucrado la evaluación exhaustiva de múltiples candidatos, teniendo en cuenta factores como la seguridad, la eficiencia, y la facilidad de implementación.

1. **Fases de evaluación del NIST**
   El proceso de estandarización del NIST se ha dividido en varias fases. En la primera fase, se recibieron decenas de propuestas de algoritmos post-cuánticos, que fueron evaluadas en términos de seguridad y eficiencia. Los algoritmos más prometedores fueron seleccionados para la segunda fase, donde se realizó una evaluación más detallada de su viabilidad práctica y resistencia a ataques conocidos.
   - **Algoritmos seleccionados:** Entre los algoritmos seleccionados en la segunda fase se encuentran aquellos basados en retículas, como CRYSTALS-Kyber y CRYSTALS-Dilithium, que han demostrado un equilibrio entre seguridad y eficiencia. Otros candidatos incluyen esquemas basados en funciones hash y códigos, cada uno con sus propias ventajas y desventajas en términos de implementación y resistencia a ataques.
2. **Criterios de selección:**
   El NIST ha establecido criterios rigurosos para la selección de algoritmos post-cuánticos, incluyendo la resistencia a ataques cuánticos conocidos, la eficiencia en diferentes plataformas, y la facilidad de implementación. Estos criterios son esenciales para garantizar que los algoritmos seleccionados sean viables para su adopción en una amplia gama de aplicaciones, desde dispositivos de bajo consumo hasta infraestructuras críticas.
3. **Impacto de la estandarización**: La estandarización de la criptografía post-cuántica tendrá un impacto significativo en la seguridad global. Los algoritmos seleccionados por el NIST se convertirán en la base de la próxima generación de sistemas criptográficos, protegiendo la información en un mundo donde las computadoras cuánticas son una realidad. La adopción de estos algoritmos requerirá una actualización masiva de la infraestructura criptográfica global, lo que plantea desafíos técnicos y logísticos, pero también ofrece la oportunidad de mejorar la seguridad a largo plazo.

Figura 3 Estructura NIST

D. Desafíos en la implementación práctica de criptografía post-cuántica:

La transición hacia la criptografía post-cuántica no está exenta de desafíos. La implementación práctica de estos algoritmos enfrenta una serie de obstáculos, desde la eficiencia y el rendimiento hasta la compatibilidad con sistemas existentes. A continuación, se detallan algunos de los principales desafíos en la implementación de criptografía post-cuántica:

1. **Eficiencia y rendimiento**
   Uno de los mayores desafíos en la implementación de criptografía post-cuántica es la eficiencia. Muchos algoritmos post-cuánticos requieren

claves más grandes y más operaciones computacionales que sus contrapartes clásicas, lo que puede afectar el rendimiento en aplicaciones donde la velocidad y la eficiencia son críticas. Por ejemplo, los esquemas basados en retículas, aunque seguros, suelen tener claves más grandes y operaciones más complejas que RSA o ECC.

- **Impacto en dispositivos de bajo consumo:** Los dispositivos IoT y otros sistemas embebidos, que operan con recursos limitados, pueden encontrar dificultades para implementar algoritmos post-cuánticos debido a su alta demanda de recursos. Esto podría requerir el desarrollo de versiones optimizadas de estos algoritmos o la adopción de soluciones híbridas que combinen criptografía clásica y post-cuántica.
- **Optimización de algoritmos:** La optimización de algoritmos post-cuánticos para su uso en diferentes plataformas es un área activa de investigación. Esto incluye la reducción del tamaño de las claves, la mejora de la velocidad de las operaciones criptográficas, y la adaptación de los algoritmos para su implementación en hardware especializado.

2. **Compatibilidad y transición**: La transición a la criptografía post-cuántica también plantea desafíos en términos de compatibilidad con sistemas existentes. La infraestructura criptográfica global está basada en algoritmos clásicos, y la adopción de nuevos algoritmos requerirá una actualización masiva de esta infraestructura.
   - **Soluciones híbridas:** Durante el período de transición, es probable que se utilicen soluciones híbridas que combinen algoritmos clásicos y post-cuánticos. Esto permitirá una migración gradual a la criptografía post-cuántica mientras se mantiene la compatibilidad con sistemas existentes.
   - **Migración de sistemas críticos:** La migración de sistemas críticos, como infraestructuras financieras y gubernamentales, a la criptografía post-cuántica requerirá una planificación cuidadosa y una ejecución meticulosa. Esto incluye la evaluación de riesgos, la implementación de nuevos algoritmos, y la capacitación del personal en la administración de sistemas post-cuánticos.
3. **Estándares y regulaciones:** La creación de estándares y regulaciones para la criptografía post-cuántica es esencial para su adopción generalizada. Los estándares garantizarán que los algoritmos seleccionados sean seguros y eficientes, mientras que las regulaciones definirán cómo y cuándo deben implementarse estos algoritmos.
   - **Papel de las organizaciones internacionales:** Organizaciones internacionales como ISO y NIST jugarán un papel crucial en la creación de estándares para la criptografía post-cuántica. Estos estándares serán adoptados por gobiernos y empresas en todo el mundo, lo que facilitará la transición a la nueva tecnología.
   - **Cumplimiento regulatorio:** Las regulaciones establecerán los requisitos para el cumplimiento de la criptografía post-cuántica en diferentes sectores, incluyendo el financiero, el sanitario, y el gubernamental. Esto garantizará que las organizaciones adopten la nueva tecnología de manera oportuna y segura.

E. Oportunidades para la criptografía post-cuántica:

A pesar de los desafíos, la criptografía post-cuántica también presenta una serie de oportunidades. Estos incluyen la mejora de la seguridad global, el desarrollo de nuevas aplicaciones criptográficas, y la innovación en la teoría de la información.

1. **Mejora de la seguridad global**: La adopción de criptografía post-cuántica mejorará significativamente la seguridad global al proteger la información contra ataques cuánticos. Esto es especialmente importante en sectores donde la seguridad es crítica, como la banca, la defensa, y las comunicaciones gubernamentales.
    - **Protección de infraestructuras críticas:** La criptografía post-cuántica protegerá infraestructuras críticas como redes eléctricas, sistemas de transporte, y redes de telecomunicaciones contra ataques cuánticos, asegurando la continuidad de los servicios esenciales.
    - **Seguridad a largo plazo:** A medida que la computación cuántica evolucione, la criptografía post-cuántica garantizará que la información permanezca segura a largo plazo, incluso frente a futuros avances tecnológicos.
2. **Desarrollo de nuevas aplicaciones criptográficas:**
   La criptografía post-cuántica también abrirá la puerta al desarrollo de nuevas aplicaciones criptográficas. Estos incluyen la criptografía homomórfica, que permite realizar cálculos sobre datos cifrados sin necesidad de descifrarlos, y la criptografía basada en identidades, que simplifica la gestión de claves en redes complejas.
    - **Criptografía homomórfica:** La criptografía homomórfica es una de las áreas más prometedoras de la criptografía post-cuántica. Permite realizar operaciones sobre datos cifrados, lo que tiene aplicaciones en la computación en la nube, la protección de la privacidad, y el análisis de grandes datos.
    - **Criptografía basada en identidades:** La criptografía basada en identidades simplifica la gestión de claves al permitir que las claves públicas sean derivadas de identidades, como direcciones de correo electrónico o nombres de usuario. Esto facilita la implementación de criptografía en redes distribuidas y entornos de IoT.
3. **Innovación en la teoría de la información**:
   La criptografía post-cuántica también impulsará la innovación en la teoría de la información, con nuevos enfoques y paradigmas que mejoren la comprensión de la seguridad y la complejidad computacional.
    - **Nuevos problemas matemáticos:** La investigación en criptografía post-cuántica está llevando al descubrimiento de nuevos problemas matemáticos que podrían servir como base para futuros sistemas criptográficos. Estos problemas son fundamentalmente diferentes de los utilizados en la criptografía clásica, lo que podría conducir a una mayor diversidad en los algoritmos criptográficos.
    - **Teoría de la complejidad cuántica:** La teoría de la complejidad cuántica está en constante evolución, y la criptografía post-cuántica está desempeñando un papel importante en este campo. La comprensión de la complejidad computacional en el contexto cuántico mejorará la capacidad de diseñar algoritmos seguros y eficientes.

III. CONCLUSIONES

La criptografía post-cuántica representa un campo crítico en la seguridad de la información, especialmente en el contexto de la rápida evolución de la computación cuántica. Aunque enfrenta desafíos significativos en términos de eficiencia, compatibilidad, y estandarización, las oportunidades que ofrece para mejorar la seguridad global y desarrollar nuevas aplicaciones criptográficas son inmensas. A medida que la computación cuántica continúe avanzando, la criptografía post-cuántica jugará un papel crucial en la protección de la información y la infraestructura digital en las próximas décadas.

REFERENCIAS

[1] D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography. Springer, 2009.

[2] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 1994, pp. 124-134.

[3] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography," [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography. [Accessed: Aug. 8, 2024].

[4] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 1423. Springer, 1998, pp. 267-288.

[5] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," DSN Progress Report, vol. 42, pp. 114-116, 1978.

[6] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," SIAM Journal on Computing, vol. 18, no. 1, pp. 186-208, 1989.

[7] V. Shoup, "A computational introduction to number theory and algebra," 2nd ed., Cambridge University Press, 2009.

[8] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp. 212-219, 1996.

[9] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?," IEEE Security & Privacy, vol. 16, no. 5, pp. 38-41, Sept.-Oct. 2018.

[10] C. Peikert, "A decade of lattice cryptography," Foundations and Trends in Theoretical Computer Science, vol. 10, no. 4, pp. 283-424, 2016.