ISSN-e: 2954-4408

UNIVERSIDAD ANÁHUAC MR
VINCE IN BONO MALUM
MÉXICO

REVISTA

+ CIENCIA

DE LA FACULTAD DE INGENIERÍA

Año 14, N.º 42, Septiembre-Diciembre 2026

Los MOF: materiales a la medida para hacer frente a los desafíos del siglo xxi

La simplicidad en la ciencia: de Newton a SpaceX

La biotecnología detrás de la nanotecnología dermatológica

Cuando la ingeniería trasciende las aulas • Las plantas: fábricas químicas de metabolitos secundarios • ¿Y si tu maquillaje pudiera adaptarse a ti? • *Scooters*: 100 años de un vehículo a gran velocidad • Con sangre, sudor y lágrimas • El héroe que todos ocupamos alguna vez • El estado del arte de la computación cuántica y el impacto en la encriptación moderna • Endometriosis: La lucha contra el sufrimiento femenino • La IA más allá de tus tareas

EL ESTADO DEL ARTE DE LA COMPUTACIÓN CUÁNTICA Y EL IMPACTO EN LA ENCRIPTACIÓN MODERNA

LUIS EDUARDO ORDOÑEZ IRINEO
Facultad de Ciencias Físico Matemáticas, Benemérita Universidad Autónoma de Puebla

IVÁN FUENTECILLA CÁRCAMO
Profesor de la Escuela de Ingeniería y Actuaría, Universidad Anáhuac, Campus Puebla

GERARDO BARRERA FLORES
Facultad de Ciencias Físico Matemáticas, Benemérita Universidad Autónoma de Puebla

JOSÉ ALEJANDRO HERNÁNDEZ LÓPEZ
Facultad de Ciencias Físico Matemáticas, Benemérita Universidad Autónoma de Puebla

LAURA ALEJANDRA TEPANECATL FUENTES
Facultad de Ciencias Físico Matemáticas, Benemérita Universidad Autónoma de Puebla

YESMIN PANECATL BERNAL
Centro Tecnológico Aragón, Facultad de Estudios Superiores Aragón,
Universidad Nacional Autónoma de México
Universidad Nacional s/n, Bosques de Aragón, Ciudad Nezahualcóyotl, C.P. 57171, México

Resumen

La seguridad de las comunicaciones digitales modernas depende de la dificultad computacional de factorizar grandes números enteros, principio sobre el que se sostienen algoritmos como RSA, TLS y ECC. La computación cuántica representa una amenaza directa a este paradigma: desde 1994, el algoritmo de Shor demostró teóricamente que una computadora cuántica con corrección de errores podría resolver dicho problema en tiempo polinomial, comprometiendo los esquemas de encriptación vigentes.

En este trabajo se describe el uso del algoritmo de Shor para la vulneración de los algoritmos de encriptación vigentes y su estado de implementación actual, incluyendo avances recientes que reducen los requerimientos de escala. Se analiza la arquitectura de trampa de iones como plataforma *hardware* prioritaria por sus bajas tasas de error.

Los resultados reportados indican que, si bien ningún sistema actual alcanza la escala necesaria para comprometer cifrados de 2048 bits, el avance en corrección de errores y el surgimiento de nuevos algoritmos como el JVG acortan significativamente ese horizonte, validando la premisa de vulnerabilidad de la encriptación clásica ante la computación cuántica.

Introducción

La seguridad de las comunicaciones digitales actuales se basa principalmente en la dificultad computacional de factorizar grandes números enteros en sus factores primos. Algoritmos ampliamente adoptados como el Transport Layer Security (TLS), Rivest-Shamir-Adleman (RSA) y la criptografía elíptica (ECC) son vulnerables en la medida que exista la suficiente capacidad de cómputo para convertirlo de un problema de tiempo no polinomial (NP) a polinomial (P); la aparición de la computación cuántica ha transformado esta perspectiva [1].

Desde la formulación del algoritmo de Shor en 1994, se sabe que una computadora cuántica con corrección de errores podría factorizar grandes números en tiempo polinomial, comprometiendo los esquemas de encriptación como el TLS, RSA y ECC, que están basados en dicha dificultad. No obstante, el estado actual del *hardware* cuántico todavía no alcanza la escala necesaria para comprometer cifrados de 2048 bits, pero la brecha se reduce año con año con mejoras como los métodos de corrección y el número de qubits [2].

Aquí se describe el uso del algoritmo de Shor para la vulneración de los algoritmos de encriptación actuales y se asume que, con corrección de errores operacionales, es técnicamente posible vulnerar los métodos de encriptación actuales [1].

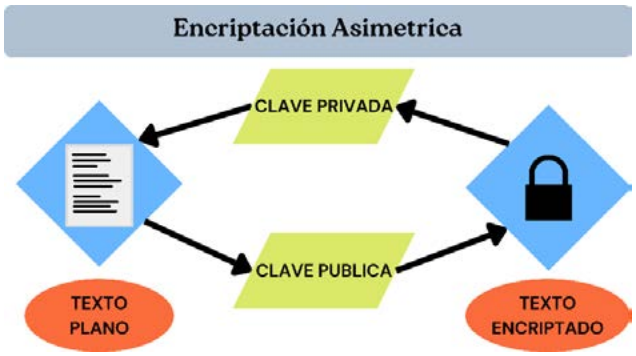

Figura. 1 El algoritmo de encriptación RSA funciona por medio de una encriptación asimétrica. Cualquiera con la clave publica, pero solo se puede desencriptar el mensaje haciendo uso de la clave privada.

Criptografía clásica y el problema de factorización

Los sistemas de claves públicas como el RSA cifran nuestra información mediante fórmulas que involucran el producto, n, de dos números primos, p y q; y la descifran usando los valores de p y q. La factorización de n resulta computacionalmente imposible para nuestros ordenadores clásicos [3]. Sin embargo, a pesar de la robustez de los métodos actuales de encriptación y considerando la disponibilidad de la información, existe un problema conocido como *harvest now decrypt later*, basado en la recolección de la información, que, aunque sea imposible de descifrarla con ordenadores actuales, se almacena con la esperanza de que se alcance la potencia computacional cuántica necesaria para decriptarla [4]. En pos de evitar que organizaciones que gestionan datos con larga vida útil de confidencialidad (véase registros médicos, contratos, direcciones, información bancaria o fiscal, entre otros), el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST, por sus siglas en inglés) publicó en 2024 los primeros estándares de criptografía post-cuántica: ML-KEM (FIPS 203) para establecimiento de claves, ML-DSA (FIPS 204) para firmas digitales y SLH-DSA (FIPS 205) como estándar de firma basado en funciones *hash* [4].

El algoritmo de Shor

En 1994 el matemático Peter Shor demostró que la factorización de enteros podía realizarse en tiempo polinomial mediante una computadora cuántica [2]. El algoritmo de Shor se apoya en la Transformada de Fourier Cuántica (QFT) para detectar la periodicidad de funciones modulares, lo que permite deducir los factores primos de un número compuesto de manera eficiente [1, 3]. La implementación del algoritmo de Shor en *hardware* real se ejecutó por primera vez en 2001 por IBM sobre una computadora de 7 qubits, logrando factorizar el número 15 en sus factores primos, 3 y 5 [5]. Sin embargo, factorizar números de relevancia criptográfica, del orden de 2048 bits, requiere miles de qubits lógicos tolerantes a fallos, una capacidad que ningún sistema actual posee [1, 3].

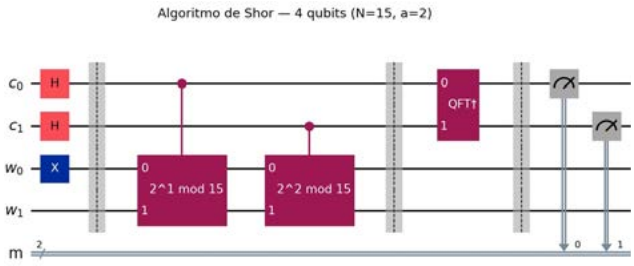

Figura. 2 El algoritmo de Shor hace uso de compuertas cuánticas (CC) para hacer operaciones sobre los qubits (C0, C1), algunas de las CC que lo componen son la Hadamard (H), Pauli-X (X) y la QTF. Las CC actúan como matrices sobre los qubits representados como vectores.

Los requerimientos de escala son precisamente el principal problema que ralentiza los avances en computación cuántica. Investigaciones recientes estiman que para romper el algoritmo RSA-1024, algoritmo RSA de 1024 bits, necesitaría aproximadamente 2300 qubits lógicos; y para RSA-2048 se necesitaría alrededor de 1730 qubits, según un estudio de 2024 realizado por Chevignard *et al*. [6]. Esto si se combina el algoritmo de Shor con técnicas clásicas de tipo *hash trick*, técnica que convierte características arbitrarias, como texto o categorías, en un vector de tamaño fijo y disperso aplicando una *función hash*. En diciembre de 2025 el investigador Craig Gidney de Google Quantum AI mostró que podría reducirse aún más el umbral mediante el uso de aritmética residual aproximada y códigos de superficie de bajo costo, potencialmente factorizando el RSA-2048 en menos de una semana con un 1x10^6 de qubits físicos [7]. Más recientemente, en marzo de 2026, el Advanced Quantum Technologies Institute (AQTI) anunció el algoritmo JVG (Jesse-Victor-Gharabaghi), que reduciría los recursos necesarios en un factor de mil respecto al algoritmo de Shor, requiriendo potencialmente menos de 5x10^3 qubits para romper RSA y ECC [8]. Si estas proyecciones se confirman, el uso de computadoras cuánticas para decriptación clásica se acortaría significativamente.

Implementación en trampa de iones

Una de las arquitecturas más prometedoras para ejecutar el algoritmo de Shor a escala es la trampa de iones; en estos dispositivos, los qubits se codifican en los estados electrónicos de iones individuales confinados por campos eléctricos y manipulados mediante pulsos de luz láser [9]. La arquitectura de trampa de iones fue la primera en demostrar una compuerta lógica cuántica física en 1995, y hasta la fecha sigue mostrando las menores tasas de error entre todas las arquitecturas de computación cuántica [9]. Un estudio experimental de Monz *et al*. (Universidad de Innsbruck) y Chuang *et al*. (MIT) demostró que cinco iones son suficientes para ejecutar el algoritmo de Shor de manera funcional, restringiendo la medición a un qubit de salida para evitar la corrupción de los cuatro qubits de cómputo [8]. Esta arquitectura es teóricamente escalable, mientras la trampa pueda mantener iones estables, el mismo principio es extensible a operaciones de mayor complejidad. En el plano de la corrección de errores, los sistemas de trampa de iones evalúan el impacto de tasas de error más bajas sobre los códigos de corrección cuántica, en contraste con los sistemas de qubits superconductores que priorizan el escalado en número [9]. En 2024, el equipo de Google Quantum AI [10], mediante su procesador Willow, ofrecieron evidencia de que la corrección de errores escala con el tamaño del código; los sistemas de trampa de iones se enfocan en demostrar que las tasas de error menores tienen impacto proporcional en la fiabilidad lógica [10].

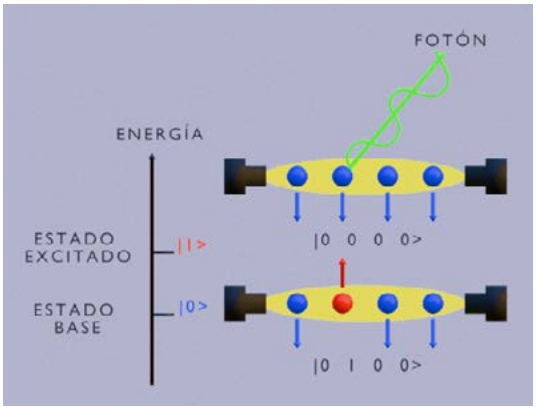

Figura. 3 Esquema de una trampa de iones. Las trampas de iones nos permiten confinar iones como 40Ca+, 88Sr+ o 138Ba+ por medio de campos electromagnéticos (amarillo) para ser excitados por medio de un láser (verde).

Conclusiones

El algoritmo de Shor representa la amenaza cuántica más directa a los sistemas de encriptación clásicos basados en la factorización de números primos. Su ejecución a escala, computacionalmente relevante, requiere *hardware* que aún no existe, pero cuyo avance en su desarrollo es constante. Las trampas de iones constituyen la implementación en *hardware* más relevante para el algoritmo de Shor debido a sus bajas tazas de error. Los avances recientes en corrección de errores cuánticos, tanto en sistemas superconductores como en iones atrapados, acercan la viabilidad de una computadora cuántica tolerante a fallos. La premisa de que una computadora cuántica con corrección de errores puede romper los algoritmos de encriptación actuales se mantiene válida a la luz de la literatura revisada, aunque el cuándo sigue siendo incierto.

Referencias

[1] National Academies of Sciences, Quantum Computing's Implications for Cryptography. *Quantum Computing: Progress and Prospects*. Washington (DC): The National Academies Press; 2019, [citado 2026 mayo]. Disponible en: https://www.nationalacademies.org/read/25196/chapter/6

[2] Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. En *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994 nov 20-22, Santa Fe, NM. Piscataway (NJ): IEEE.

[3] Turner L. E.. Shor's Algorithm and RSA Encryption. *Quantum Algorithms Institute* [Internet]., 2024 [citado 2026 mayo]. Disponible en: https://www.qai.ca/resource-library/shors-algorithm-and-rsa-encryptionnbsp

[4] Auer A, Lin P, Ogundola J, Canadian Centre for Cyber Security, NIST. Breaking RSA: How Quantum Computing Threatens Today's Digital Security [Internet]. *ResearchGate*; 2025 jul [citado 2026 mayo]. Disponible en: https://www.researchgate.net/publication/393519992

[5] Hempel C. Trapped-Ion Quantum Computers. En Jang-Jaccard J., Caroff P., Blezinger E., Mulder V., Mermoud A., y Lenders V. (eds.), *Quantum Technologies*, Cham: Springer; 2025. Capítulo 2; [citado 2026 mayo]. Disponible en: https://link.springer.com/chapter/10.1007/978-3-031-90727-2_2

[6] Chevignard C, Fouque, P.A, Schrottenloher A. Reducing the number of qubits in quantum factoring [preprint]. arXiv:2405.xxxxx; 2024.

[7] Gidney C, y Ekera M. How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits [Internet]. *Quantum Physics*. 2025 dic [citado 2026 mayo]. Disponible en: https://www.nationalacademies.org/read/25196/chapter/6

[8] Van Griensven, J. JVG. Quantum decryption algorithm announcement. Advanced Quantum Technologies Institute (AQTI) [Internet]; 2026 mar 2 [citado 2026 mayo]. Disponible en: https://www.honeywell.com/us/en/solutions/ot-cybersecurity/secure-media-exchange?utm_source=google&utm_medium=cpc&utm_campaign=CORP-26-Cyber-Search-SMX&utm_content=203865915088&utm_term=kwd-373510395986&s_kwcid=AL!7892!3!816149619089!b!!g!!removable%20media%20security&gad_source=1&gad_

[9] Chuang IL, Vandersypen LM, Zhou X, Leung DW, Lloyd R, Kubinec MG. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature. 2001;414(6866):883-887. [Véase también para trampa de iones: IEEE Spectrum; 2023. Disponible en: https://spectrum.ieee.org/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment

[10] Google Quantum AI and Collaborators. Quantum error correction below the surface code threshold. Nature. 2025;638:920-926. Disponible en https://www.nature.com/articles/s41586-024-08449-y