



Criptografía post-cuántica: qué es y por qué importa

Description

La transición a la criptografía post-cuántica será gradual y coordinada, requiriendo actualizaciones en todos los sistemas informáticos. Comenzar el proceso temprano es esencial para garantizar la seguridad a largo plazo.

CONTENIDOS

La amenaza de los ordenadores cuánticos para la seguridad digital

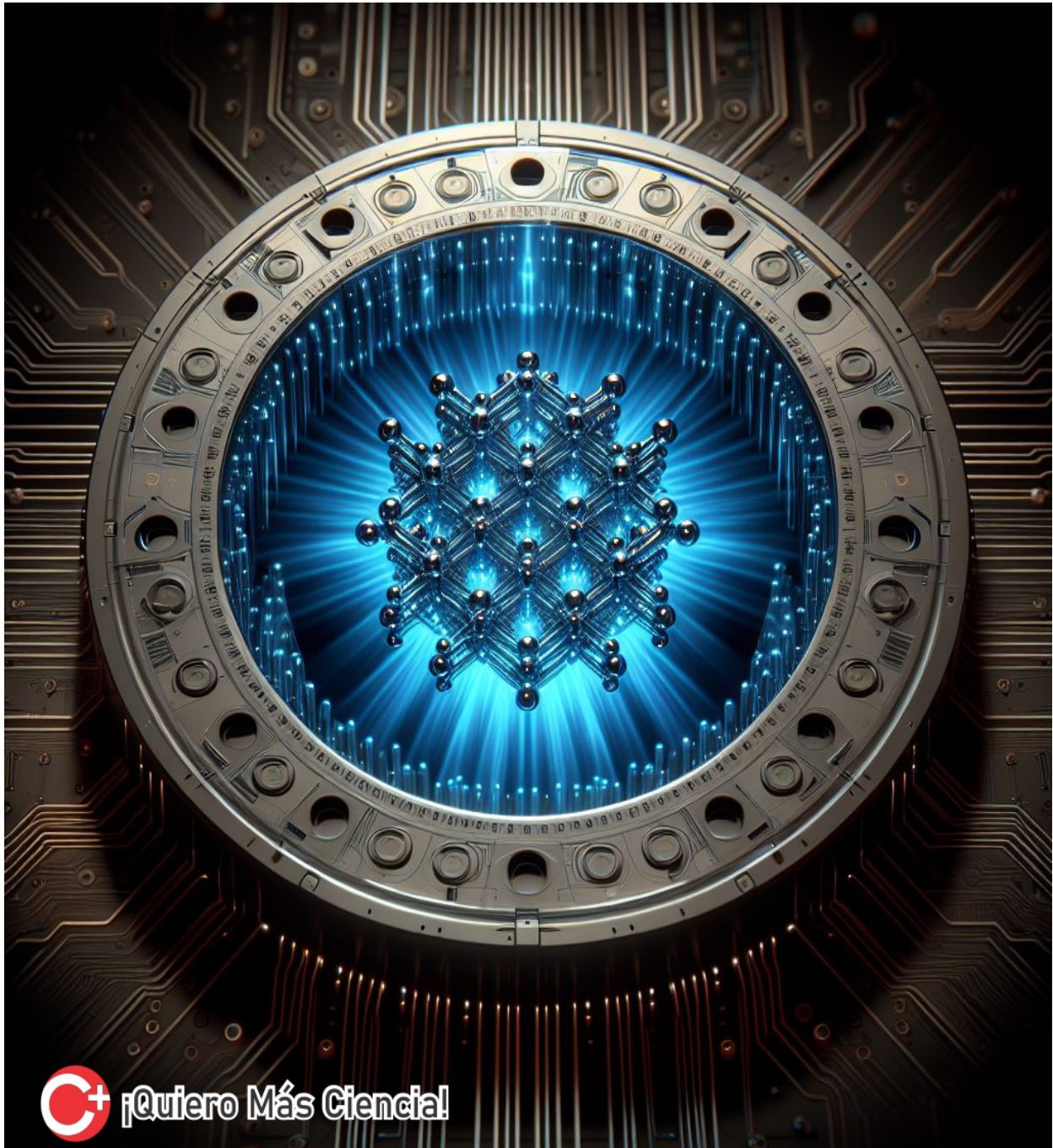
La seguridad digital se basa en el uso de algoritmos criptográficos que permiten cifrar y descifrar los datos que se envían y reciben a través de internet. Estos algoritmos se apoyan en problemas matemáticos difíciles de resolver para un ordenador convencional, como factorizar números grandes o calcular logaritmos discretos. Sin embargo, estos problemas podrían ser resueltos en un tiempo razonable por un ordenador cuántico, una máquina que utiliza las propiedades de la física cuántica para procesar la información. Un ordenador cuántico podría romper los códigos criptográficos actuales y poner en peligro la privacidad y la confidencialidad de las comunicaciones electrónicas.

La carrera por la criptografía post-cuántica

Ante la amenaza de los ordenadores cuánticos, que podrían estar disponibles en las próximas décadas, los expertos en seguridad informática han iniciado una carrera por desarrollar nuevos algoritmos criptográficos que sean resistentes a los ataques cuánticos. Estos algoritmos se conocen como criptografía post-cuántica o criptografía resistente a [la computación cuántica](#). Su objetivo es reemplazar o complementar los sistemas criptográficos tradicionales, como el RSA o la criptografía de curva elíptica, que se consideran vulnerables a la computación cuántica.

Los desafíos de la criptografía post-cuántica

La criptografía post-cuántica no es una tarea fácil. Los algoritmos criptográficos deben ser seguros, eficientes y compatibles con los sistemas informáticos actuales. Además, deben basarse en problemas matemáticos que se cree que son difíciles de resolver tanto para los ordenadores clásicos como para los cuánticos. Estos problemas deben ser elegidos con cuidado, ya que no se puede garantizar que no exista una solución rápida para ellos, ni siquiera con un ordenador cuántico. Por eso, los criptógrafos buscan diversificar las opciones y probar la robustez de los algoritmos propuestos.



Para un hipotético ordenador cuántico del futuro, los beneficios de la criptografía post-cuántica van más allá de la resistencia a ataques cuánticos, ofreciendo mejoras en velocidad, eficiencia y seguridad general de las comunicaciones digitales.

Las familias de algoritmos post-cuánticos

Entre las familias de algoritmos más prometedoras para proporcionar seguridad post-cuántica se encuentran:

- La criptografía basada en código, que se basa en el uso de códigos de corrección de errores para crear criptografía de clave pública. Fue propuesta por primera vez por Robert McEliece en 1978. El principal problema de este sistema es el gran tamaño de las claves pública y privada.

- La criptografía basada en hash, que se basa en el uso de funciones hash para crear criptografía de clave pública. Las funciones hash son una de las herramientas criptográficas más utilizadas. Este tipo de criptografía basada en hash es flexible y puede cumplir con diferentes expectativas de rendimiento. El principal inconveniente es que los esquemas de firma basados en hash son principalmente con estado, lo que significa que la clave privada debe actualizarse después de cada uso.
- La criptografía basada en retículas, que se basa en el uso de estructuras matemáticas llamadas retículas para crear criptografía de clave pública. Las retículas son conjuntos de puntos que forman un patrón regular en el espacio. Los problemas relacionados con las retículas se consideran muy difíciles de resolver, incluso con un ordenador cuántico. La criptografía basada en retículas tiene la ventaja de ser eficiente y versátil, pero también tiene el riesgo de que se descubra un algoritmo que la rompa.

El proceso de estandarización de la criptografía post-cuántica

Para que la criptografía post-cuántica se pueda implementar de forma generalizada, es necesario que se establezcan unos estándares que definan cómo se deben usar los algoritmos. Estos estándares deben ser consensuados por la comunidad científica y la industria, y deben garantizar la interoperabilidad y la compatibilidad de los sistemas. Uno de los organismos encargados de este proceso es el Instituto Nacional de Estándares y Tecnología (NIST) de EE.UU., que inició un concurso público en 2016 para seleccionar los mejores [algoritmos post-cuánticos](#). Después de cuatro rondas de evaluación, el NIST eligió un ganador, llamado CRYSTALS-Kyber, en la categoría de cifrado de clave pública, y tres ganadores en la categoría de firma digital. El NIST está ahora trabajando con los investigadores para estandarizar los algoritmos ganadores y facilitar su adopción.

Te Puede Interesar:

La transición a la criptografía post-cuántica

La transición a la criptografía post-cuántica no será inmediata ni sencilla. Requerirá un cambio gradual y coordinado de todos los sistemas informáticos que utilizan criptografía. Cada empresa, organización e institución tendrá que actualizar sus protocolos, requisitos y dispositivos para adaptarse a los nuevos algoritmos. Además, habrá que tener en cuenta la compatibilidad con los sistemas antiguos y la seguridad de los datos históricos. Se estima que este proceso llevará muchos años, si no décadas, por lo que es importante empezar cuanto antes. Como dice la criptógrafa Britta Hale, "todo el mundo está mirando sus relojes y diciendo: 'Ya es tarde'".

Los beneficios de la criptografía post-cuántica

La criptografía post-cuántica no solo es una necesidad para protegerse de los futuros ataques cuánticos, sino también una oportunidad para mejorar la seguridad y la eficiencia de las comunicaciones digitales. Los nuevos algoritmos post-cuánticos podrán ofrecer ventajas sobre los actuales, como una mayor velocidad, un menor consumo de recursos o una mayor resistencia a otros tipos de ataques. Además, la criptografía post-cuántica podrá impulsar el desarrollo de otras tecnologías relacionadas, como la computación en la nube, el internet de las cosas o la [inteligencia artificial](#). La criptografía post-cuántica podrá ser, en definitiva, una revolución para la sociedad de la información.

Para seguir pensando

La criptografía post-cuántica es diferente a la criptografía cuántica, que consiste en utilizar fenómenos cuánticos para lograr el secreto y detectar el espionaje. La criptografía cuántica se basa en el uso de partículas como los fotones para transmitir las claves criptográficas. Estas partículas tienen la propiedad de que cualquier intento de medirlas o manipularlas altera su estado, lo que permite detectar la presencia de un intruso. La criptografía cuántica ofrece una seguridad teóricamente perfecta, pero también tiene limitaciones prácticas, como la distancia, el ruido o el coste. La criptografía post-cuántica y la criptografía cuántica no son excluyentes, sino complementarias. Se pueden combinar para obtener lo mejor de ambos mundos: una seguridad a prueba de ordenadores cuánticos y una detección de ataques.