CriptografÃa post-cuÃ¡ntica: quÃ© es y por quÃ© importa

Description

La transiciÃ³n a la criptografÃa post-cuÃ¡ntica serÃ¡ gradual y coordinada, requiriendo actualizaciones en todos los sistemas informÃ¡ticos. Comenzar el proceso temprano es esencial para garantizar la seguridad a largo plazo.

CONTENIDOS

La amenaza de los ordenadores cuÃ¡nticos para la seguridad digital

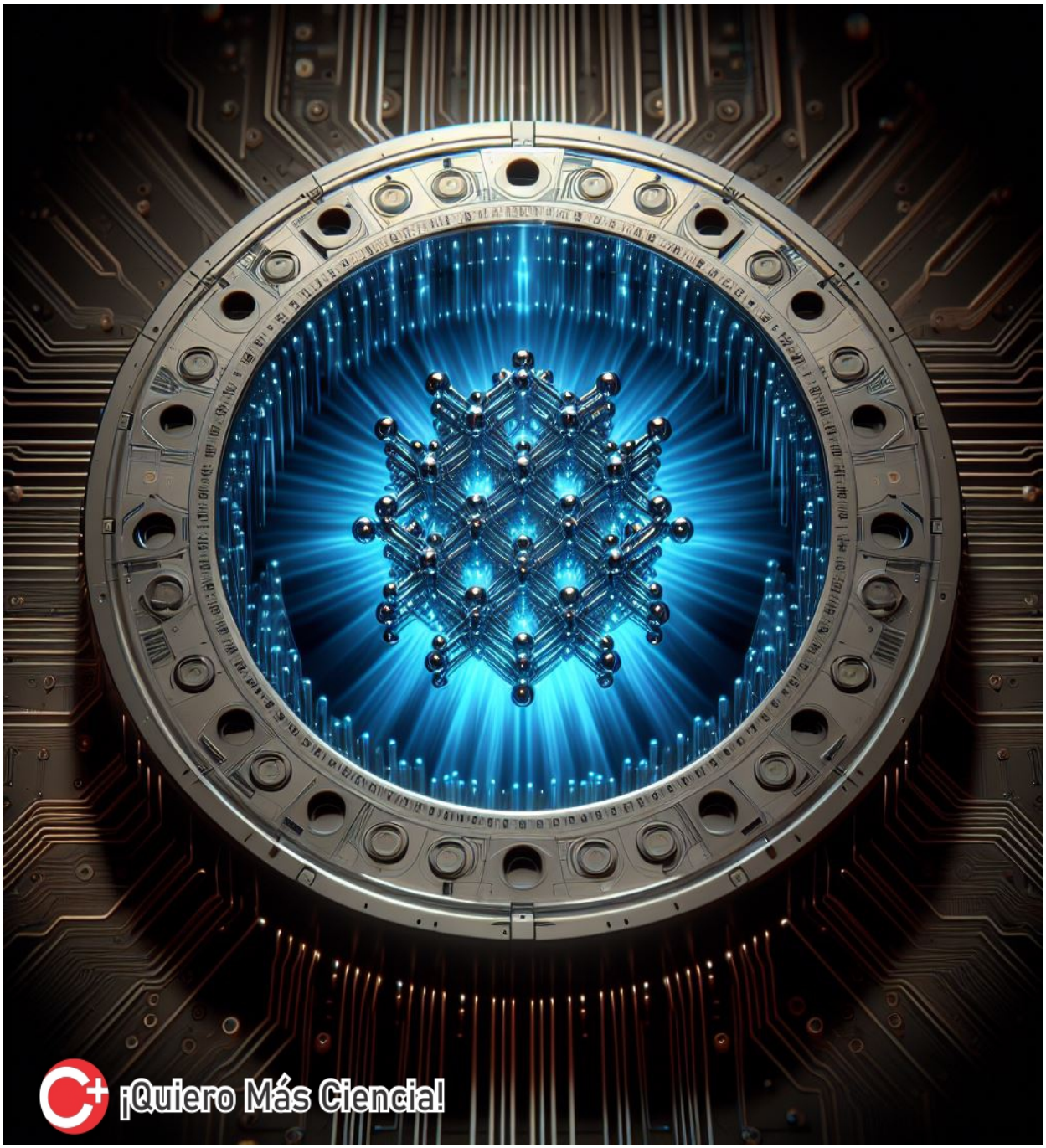
La seguridad digital se basa en el uso de algoritmos criptogrÃ¡ficos que permiten cifrar y descifrar los datos que se envÃan y reciben a travÃ©s de internet. Estos algoritmos se apoyan en problemas matemÃ¡ticos difÃciles de resolver para un ordenador convencional, como factorizar nÃºmeros grandes o calcular logaritmos discretos. Sin embargo, estos problemas podrÃan ser resueltos en un tiempo razonable por un ordenador cuÃ¡ntico, una mÃ¡quina que utiliza las propiedades de la fÃsica cuÃ¡ntica para procesar la informaciÃ³n. Un ordenador cuÃ¡ntico podrÃa romper los cÃ³digos criptogrÃ¡ficos actuales y poner en peligro la privacidad y la confidencialidad de las comunicaciones electrÃ³nicas.

La carrera por la criptografÃa post-cuÃ¡ntica

Ante la amenaza de los ordenadores cuÃ¡nticos, que podrÃan estar disponibles en las prÃ³ximas dÃ©cadas, los expertos en seguridad informÃ¡tica han iniciado una carrera por desarrollar nuevos algoritmos criptogrÃ¡ficos que sean resistentes a los ataques cuÃ¡nticos. Estos algoritmos se conocen como criptografÃa post-cuÃ¡ntica o criptografÃa resistente a la computaciÃ³n cuÃ¡ntica. Su objetivo es reemplazar o complementar los sistemas criptogrÃ¡ficos tradicionales, como el RSA o la criptografÃa de curva elÃptica, que se consideran vulnerables a la computaciÃ³n cuÃ¡ntica.

Los desafÃos de la criptografÃa post-cuÃ¡ntica

La criptografÃa post-cuÃ¡ntica no es una tarea fÃ¡cil. Los algoritmos criptogrÃ¡ficos deben ser seguros, eficientes y compatibles con los sistemas informÃ¡ticos actuales. AdemÃ¡s, deben basarse en problemas matemÃ¡ticos que se cree que son difÃciles de resolver tanto para los ordenadores clÃ¡sicos como para los cuÃ¡nticos. Estos problemas deben ser elegidos con cuidado, ya que no se puede garantizar que no exista una soluciÃ³n rÃ¡pida para ellos, ni siquiera con un ordenador cuÃ¡ntico. Por eso, los criptÃ³grafos buscan diversificar las opciones y probar la robustez de los algoritmos propuestos.



Para un hipotÃ©tico ordenador cuÃ¡ntico del futuro, los beneficios de la criptografÃa post-cuÃ¡ntica van mÃ¡s allÃ¡ de la resistencia a ataques cuÃ¡nticos, ofreciendo mejoras en velocidad, eficiencia y seguridad general de las comunicaciones digitales.

Las familias de algoritmos post-cuÃ¡nticos

Entre las familias de algoritmos mÃ¡s prometedoras para proporcionar seguridad post-cuÃ¡ntica se encuentran:

- La criptografÃa basada en cÃ³digo, que se basa en el uso de cÃ³digos de correcciÃ³n de errores para crear criptografÃa de clave pÃºblica. Fue propuesta por primera vez por Robert McEliece en 1978. El principal problema de este sistema es el gran tamaÃ±o de las claves pÃºblica y privada.

- La criptografÃa basada en hash, que se basa en el uso de funciones hash para crear criptografÃa de clave pÃºblica. Las funciones hash son una de las herramientas criptogrÃ¡ficas mÃ¡s utilizadas. Este tipo de criptografÃa 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 despuÃ©s de cada uso.
- La criptografÃa basada en retÃculas, que se basa en el uso de estructuras matemÃ¡ticas llamadas retÃculas para crear criptografÃa de clave pÃºblica. Las retÃculas son conjuntos de puntos que forman un patrÃ³n regular en el espacio. Los problemas relacionados con las retÃculas se consideran muy difÃciles de resolver, incluso con un ordenador cuÃ¡ntico. La criptografÃa basada en retÃculas tiene la ventaja de ser eficiente y versÃ¡til, pero tambiÃ©n tiene el riesgo de que se descubra un algoritmo que la rompa.

El proceso de estandarizaciÃ³n de la criptografÃa post-cuÃ¡ntica

Para que la criptografÃa post-cuÃ¡ntica se pueda implementar de forma generalizada, es necesario que se establezcan unos estÃ¡ndares que definan cÃ³mo se deben usar los algoritmos. Estos estÃ¡ndares deben ser consensuados por la comunidad cientÃfica 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 EstÃ¡ndares y TecnologÃa (NIST) de EE.UU., que iniciÃ³ un concurso pÃºblico en 2016 para seleccionar los mejores algoritmos post-cuÃ¡nticos. DespuÃ©s de cuatro rondas de evaluaciÃ³n, el NIST eligiÃ³ un ganador, llamado CRYSTALS-Kyber, en la categorÃa de cifrado de clave pÃºblica, y tres ganadores en la categorÃa de firma digital. El NIST estÃ¡ ahora trabajando con los investigadores para estandarizar los algoritmos ganadores y facilitar su adopciÃ³n.

Te Puede Interesar:

La transiciÃ³n a la criptografÃa post-cuÃ¡ntica

La transiciÃ³n a la criptografÃa post-cuÃ¡ntica no serÃ¡ inmediata ni sencilla. RequerirÃ¡ un cambio gradual y coordinado de todos los sistemas informÃ¡ticos que utilizan criptografÃa. Cada empresa, organizaciÃ³n e instituciÃ³n tendrÃ¡ que actualizar sus protocolos, requisitos y dispositivos para adaptarse a los nuevos algoritmos. AdemÃ¡s, habrÃ¡ que tener en cuenta la compatibilidad con los sistemas antiguos y la seguridad de los datos histÃ³ricos. Se estima que este proceso llevarÃ¡ muchos aÃ±os, si no dÃ©cadas, por lo que es importante empezar cuanto antes. Como dice la criptÃ³grafa Britta Hale, â??todo el mundo estÃ¡ mirando sus relojes y diciendo: â??Ya es tardeâ??â?•.

Los beneficios de la criptografÃa post-cuÃ¡ntica

La criptografÃa post-cuÃ¡ntica no solo es una necesidad para protegerse de los futuros ataques cuÃ¡nticos, sino tambiÃ©n una oportunidad para mejorar la seguridad y la eficiencia de las comunicaciones digitales. Los nuevos algoritmos post-cuÃ¡nticos podrÃan ofrecer ventajas sobre los actuales, como una mayor velocidad, un menor consumo de recursos o una mayor resistencia a otros tipos de ataques. AdemÃ¡s, la criptografÃa post-cuÃ¡ntica podrÃa impulsar el desarrollo de otras tecnologÃas relacionadas, como la computaciÃ³n en la nube, el internet de las cosas o la inteligencia artificial. La criptografÃa post-cuÃ¡ntica podrÃa ser, en definitiva, una revoluciÃ³n para la sociedad de la informaciÃ³n.

Para seguir pensando

La criptografÃa post-cuÃ¡ntica es diferente a la criptografÃa cuÃ¡ntica, que consiste en utilizar fenÃ³menoscuÃ¡nticos para lograr el secreto y detectar el espionaje. La criptografÃa cuÃ¡ntica se basa en el uso de partÃculascomo los fotones para transmitir las claves criptogrÃ¡ficas. Estas partÃculas tienen la propiedad de que cualquierintento de medirlas o manipularlas altera su estado, lo que permite detectar la presencia de un intruso. La criptografÃa cuÃ¡ntica ofrece una seguridad teÃ³ricamente perfecta, pero tambiÃ©n tiene limitaciones prÃ¡cticas, como ladistancia, el ruido o el coste. La criptografÃa post-cuÃ¡ntica y la criptografÃa cuÃ¡ntica no son excluyentes, sinocomplementarias. Se pueden combinar para obtener lo mejor de ambos mundos: una seguridad a prueba deordenadores cuÃ¡nticos y una detecciÃ³n de ataques.