Comunicados

Algoritmos desarrollados por IBM son los primeros estándares de criptografía post-cuántica del mundo

Con el rápido avance de las computadoras cuánticas, el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) publicó nuevos algoritmos desarrollados por IBM, en colaboración con aliados del sector, para proteger los datos contra potenciales ataques cuánticos.

Yorktown Heights, Nueva York, Agosto 13 de 2024 - Dos algoritmos desarrollados por IBM fueron oficialmente formalizados dentro de los tres primeros estándares de criptografía post-cuántica del mundo, que fueron publicados hoy por el Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio de Estados Unidos.

Los estándares incluyen tres algoritmos de criptografía post-cuántica: dos de ellos, ML-KEM (originalmente conocido como CRYSTAL-Kyber) y ML-DSA (originalmente CRYSTAL-Dilithium) fueron desarrollados por investigadores de IBM en colaboración con aliados de varias industrias y la academia. El tercer algoritmo publicado, SLH-DSA (inicialmente presentado como SPHINCS+) fue codesarrollado por un investigador que desde entonces se unió a IBM. Además, se ha seleccionado un cuarto algoritmo desarrollado por IBM, FN-DSA (originalmente llamado FALCON), para su futura estandarización.

La publicación oficial de estos algoritmos marca un hito crucial para avanzar en la protección de los datos cifrados del mundo contra ciberataques que podrían intentarse mediante el poder único de las computadoras cuánticas, pues están progresando rápidamente hacia la relevancia criptográfica. Es decir, al punto en el que las computadoras cuánticas aprovecharán suficiente poder computacional para descifrar los estándares de cifrado que son usados por la mayoría de los datos y la infraestructura del mundo actual.

“La misión de IBM en computación cuántica tiene dos líneas: entregar al mundo una computación cuántica útil y hacer que el mundo cuántico-seguro. Estamos entusiasmados con el increíble progreso que hemos logrado con las computadoras cuánticas actuales, que se están utilizando en las industrias a nivel global para explorar problemas a medida que avanzamos hacia sistemas con corrección total de errores”, dijo Jay Gambetta, vicepresidente de IBM Quantum. "Sin embargo, entendemos que estos avances podrían suponer un cambio radical en la seguridad de nuestros datos y sistemas más sensibles. La publicación del NIST de los tres primeros estándares globales de criptografía post-cuántica marca un paso importante en los esfuerzos por construir un futuro cuántico-seguro junto con la computación cuántica”.

Como una rama completamente nueva de la informática, las computadoras cuánticas se están acelerando rápidamente para convertirse en sistemas útiles y de gran escala, como lo demuestran los hitos de hardware y software alcanzados por IBM según su *roadmap* o Plan de Desarrollo Cuántico. Por ejemplo, IBM proyecta que entregará su primer sistema cuántico con corrección de errores para 2029. Se prevé que este sistema ejecutará cientos de millones de operaciones cuánticas para arrojar resultados precisos para problemas complejos y valiosos que actualmente son inaccesibles para las computadoras clásicas. Con la mirada en el futuro, el *roadmap* incluye planes para ampliar este sistema para que pueda ejecutar más de mil millones de operaciones cuánticas para 2033. A medida que IBM avanza hacia estos objetivos, la compañía ya ha equipado a expertos en salud y ciencias biológicas; finanzas; desarrollo de materiales; logística; y otros campos con sistemas de utilidad cuántica a escala para comenzar a aplicar y escalar sus desafíos más urgentes a las computadoras cuánticas a medida que avanzan.

Sin embargo, la llegada de computadoras cuánticas más potentes podría conllevar riesgos para los protocolos de ciberseguridad actuales. A medida que sus niveles de velocidad y capacidad de corrección de errores crezcan, es probable que también abarquen la capacidad de descifrar los esquemas criptográficos más utilizados en la actualidad, como RSA, que durante mucho tiempo ha protegido los datos globales. Comenzando con el trabajo iniciado hace varias décadas, el equipo de IBM formado por los principales expertos en criptografía del mundo continúa liderando la industria en el desarrollo de algoritmos para proteger los datos contra amenazas futuras, que ahora están posicionados para eventualmente reemplazar los esquemas de cifrado actuales.

Los estándares recientemente publicados por el NIST están diseñados para salvaguardar los datos intercambiados en las redes públicas, además de las firmas digitales para la autenticación de identidad. Ahora formalizados, establecerán el estándar para que los gobiernos e industrias en todo el mundo comiencen a adoptar estrategias de ciberseguridad post cuánticas.

En 2016, el NIST pidió a los criptógrafos de todo el mundo que desarrollaran y presentaran nuevos esquemas criptográficos cuánticos seguros para ser considerados para una futura estandarización. En 2022, entre 69 participantes elegidos, fueron seleccionados cuatro algoritmos de cifrado para una evaluación adicional: CRYSTAL S-Kyber, CRYSTAL S-Dilithium, Falcon, y SPHINCS+.

Además de las evaluaciones continuas para anunciar a Falcon como el cuarto estándar oficial, NIST continúa identificando y evaluando algoritmos adicionales para diversificar su kit de herramientas de algoritmos criptográficos post-cuánticos, incluyendo otros desarrollados por investigadores de IBM. Los criptógrafos de IBM se encuentran entre los pioneros en la expansión de estas herramientas, incluyendo tres nuevos sistemas de firma digital presentados que ya han sido aceptados para su consideración por el NIST y que están siendo sometidos a la ronda inicial de evaluación.

Hacia su misión de hacer que el mundo sea cuántico-seguro, IBM continúa explorando cómo la criptografía post quantum se puede integrar en muchos de sus propios productos, incluidos IBM z16 e IBM Cloud. En 2023, la compañía dio a conocer el IBM Quantum Safe *roadmap*, un plan de tres pasos para trazar los hitos hacia una tecnología cuántica segura cada vez más avanzada, y definido por fases de descubrimiento, observación y transformación. Además del *roadmap*, la compañía también presentó la tecnología IBM Quantum Safe y los servicios de transformación IBM Quantum Safe para ayudar a los clientes en su camino hacia la seguridad cuántica. Estas tecnologías incluyen la introducción de la Lista de Materiales Criptográficos (CBOM), un nuevo estándar para capturar e intercambiar información sobre activos criptográficos en software y sistemas.

Para obtener más información sobre las tecnologías IBM Quantum Safe y los servicios disponibles, visite: https://www.ibm.com/quantum/quantum-safe.