Anuncios

IBM desarrolla nuevos servicios y tecnología en la nube para ayudar a las empresas a mantener sus datos seguros de los ordenadores cuánticos del futuro

Nuevos servicios de evaluación de riesgos cuánticos disponibles para clientes

IBM Cloud comenzará a proporcionar servicios de criptografía de seguridad cuántica en la nube pública en 2020

IBM Research muestra el primer prototipo de unidad de cinta segura ante la computación cuántica del mundo

IBM dona algoritmos criptográficos de seguridad cuántica a la comunidad de código abierto

Armonk, NY - 23 ago 2019: Hoy, en la Segunda Conferencia de Normalización de la Criptografía Post-Cuántica organizada por el Instituto Nacional de Estándares y Tecnología (NIST), IBM ha dado un paso importante hacia el mantenimiento del más alto nivel de seguridad de los datos y la privacidad de sus clientes ante un futuro con ordenadores cuánticos.

IBM anuncia que comenzará a proporcionar servicios de criptografía de seguridad cuántica en la nube pública de IBM en 2020. Actualmente, IBM Security ofrece una evaluación de riesgo cuántico para ayudar a los clientes a evaluar su riesgo en el mundo cuántico. Además, los criptógrafos de IBM han realizado un prototipo de la primera cinta empresarial segura ante la computación cuántica del mundo, un paso importante antes de su comercialización.

IBM también se compromete a hacer que los algoritmos de seguridad cuántica estén disponibles a través de la comunidad de código abierto. Como industria, solo podemos estar seguros si se prueban nuevos algoritmos de seguridad cuántica, interoperables y fácilmente consumibles en estándares de seguridad comunes. Con este fin, IBM está donando algoritmos y soporte a una serie de proyectos de código abierto como OpenQuantumSafe.org.

Estos nuevos servicios y tecnologías son posibles gracias a la posición de liderazgo de IBM en la computación cuántica, lo que ha supuesto décadas de investigación en criptografía para proteger los datos en reposo y en movimiento.

IBM puso a disposición de los desarrolladores ordenadores cuánticos a través de su nube pública por primera vez en mayo de 2016, en la plataforma IBM Q Experience. Hasta hoy, los usuarios han ejecutado más de 28 millones de experimentos y simulaciones en esta plataforma y se han publicado más de 180 documentos relacionados.

Preparando la ciberseguridad para un mundo cuántico

La computación cuántica es una forma emergente de tecnología que aprovecha los fenómenos de la mecánica cuántica para resolver ciertos tipos de problemas que son, de hecho, imposibles de resolver en las computadoras clásicas. A medida que los sistemas cuánticos se vuelvan más potentes, también se verá afectada la seguridad de la información y obligará a mejorar la seguridad de los datos tanto en las instalaciones “on-premises” como en la nube.

Al ritmo actual de progreso de la computación cuántica, se espera que los datos protegidos por los métodos de encriptación asimétrica utilizados hoy en día puedan volverse inseguros en los próximos 10-30 años. Aunque faltan años, los datos se pueden recoger hoy, almacenarse y descifrarse en el futuro con una computadora cuántica lo suficientemente potente. Si bien la industria aún está finalizando los estándares de criptografía post-cuántica, las empresas y otras organizaciones pueden comenzar a prepararse hoy.

IBM toma medidas para ayudar a los clientes a mantener la seguridad en el futuro mundo de la computación cuántica

Con más empresas recurriendo a la nube para sus datos críticos, IBM une su liderazgo en la nube híbrida junto con su experiencia en investigación cuántica y de seguridad para mantenerse a la vanguardia de las futuras amenazas cuánticas de ciberseguridad.

IBM comenzará a presentar servicios de criptografía de seguridad cuántica en su nube pública en 2020. Para ayudar a los clientes a lograr la protección de sus datos de seguridad cuántica mientras está en tránsito dentro de IBM Cloud, IBM mejorará sus implementaciones TLS / SSL en los servicios de IBM Cloud utilizando algoritmos diseñados para ser cuánticamente seguros aprovechando estándares abiertos y tecnología de código abierto. IBM también está evaluando enfoques para proporcionar servicios que brinden firmas digitales de seguridad cuántica.

"IBM Cloud está tomando los pasos críticos necesarios para ayudar a las empresas a garantizar que sus datos se mantengan seguros en un futuro cuántico", dijo Harish Grama, director general de IBM Cloud. "A partir de 2020, IBM Cloud lanzará nuevos servicios que ayudarán a mantener los datos seguros y privados de los desafíos emergentes de seguridad cibernética presentados por las futuras computadoras cuánticas".

IBM Research dona algoritmos criptográficos a la comunidad de código abierto y presenta el primer prototipo de almacenamiento de cinta con seguridad cuántica

“Para prepararse para el impacto que se espera que tengan las computadoras cuánticas en la seguridad de los datos, IBM Research ha estado desarrollando algoritmos criptográficos diseñados para resistir las posibles preocupaciones de seguridad planteadas por las computadoras cuánticas”, dijo Vadim Lyubashevsky, criptógrafo de IBM Research "Nuestros algoritmos de seguridad cuántica desarrollados conjuntamente, parten de una suite de criptografía de celosía llamada CRYSTALS, que se basan en la dificultad de los problemas matemáticos que se han estudiado desde la década de 1980 y no han sucumbido a ningún ataque algorítmico, ni clásico ni cuántico. Es por eso que hemos creado nuestros algoritmos de código abierto y los hemos enviado al NIST para su estandarización".

IBM ha apoyado activamente al NIST en su viaje para estandarizar criptografía segura ante la computación. Continuaremos este compromiso contribuyendo con nuestro aprendizaje a medida que migremos los sistemas y servicios de IBM para que sean cuánticamente seguros según los estándares de la NIST, que se espera estén disponibles entre 2022-2024.

CRYSTALS (Cryptographic Suite for Algebraic Lattices) se desarrolla conjuntamente en colaboración con varios socios académicos y comerciales. Se basa en dos criptografías primitivas resistentes a la computación

cuántica: Kyber, un mecanismo de encapsulación de clave segura, y Dilithium, un algoritmo de firma digital seguro. CRYSTALS ha sido donado a OpenQuantumSafe.org, para seguir desarrollando estándares abiertos.

IBM ha probado CRYSTALS con éxito en el prototipo de unidad de cinta TS1160 de IBM, utilizando ambos Kyber y Dilithium en combinación con encriptación simétrica AES-256 para crear la primera unidad de cinta segura de computación cuántica del mundo. Los nuevos algoritmos se implementan como parte del firmware de la unidad de cinta y podrían proporcionarse a los clientes como una actualización de firmware para las unidades de cinta existentes y/o incluirse en el firmware de las generaciones futuras de unidades de cinta.

Para ayudar a los clientes a evaluar sus riesgos potenciales y comenzar el viaje a la seguridad cuántica, IBM Security también ofrece un servicio de evaluación de riesgos de datos cuánticos para ayudar a los clientes a desarrollar una estrategia de implementación de criptografía de seguridad cuántica.

Para formar a los expertos en seguridad sobre la migración a la próxima generación de criptografía, IBM Research ha lanzado recientemente un servicio de suscripción de seguridad que ofrece informes y seminarios trimestrales. El próximo seminario está previsto para el 2 de octubre de 2019 en Zúrich, Suiza.

Para obtener más información sobre la computación cuántica y su impacto en la seguridad de la información, descargue el informe del IBM Institute for Business Value: Blandiendo un arma de doble filo: preparando la ciberseguridad ahora para un mundo cuántico

Contacto(s)

Patricia Torralba

Departamento de Comunicación 637 80 41 48 patricia.torralba@es.ibm.com