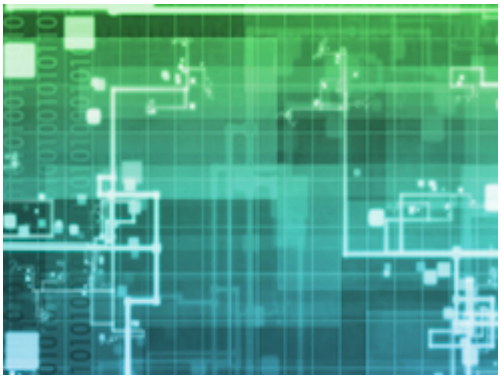
Asegurar el cifrado de datos ante la amenaza de los futuros ordenadores cuánticos

Cuando los ordenadores cuánticos estén disponibles, un algoritmo ya existente supondrá una amenaza para las técnicas de cifrado que se consideran seguras en la actualidad. La labor realizada por un proyecto financiado por la Unión Europea está sentando las bases para encontrar una solución.



© kentoh, Shutterstock

En un artículo publicado recientemente en la revista «Nature», un equipo de investigadores describió diversos métodos con los que desarrollar nuevas técnicas de cifrado frente a ataques cuánticos. Una estrategia evidente es el desarrollo de nuevas técnicas de cifrado que sustituyan a las actuales dado que estas últimas podrían ser ineficaces en el futuro.

El problema de los métodos de cifrado actuales

A día de hoy, la seguridad en Internet depende en gran medida de lo que se conoce como sistema RSA (Rivest-Shamir-Adleman), empleado de forma mayoritaria para el cifrado de datos. Este sistema se basa en el uso de claves públicas que consisten en el producto de dos números primos. En la actualidad, incluso los ordenadores más potentes requerirían de una enorme cantidad de tiempo para factorizar dicho producto, esto es, identificar los dos números primos utilizados para el cifrado.

En el otro extremo se encuentra el receptor del mensaje, que posee una clave secreta a modo de cifra que sólo conocen él y el remitente. Los dos números primos necesarios para descifrar el mensaje se obtienen con la clave secreta mediante una operación matemática. Siempre que no se intercepte esta clave, el sistema de cifrado es fiable.

No obstante, los ordenadores cuánticos son más potentes y están a la vuelta de la esquina; con ellos se dispondrá de la capacidad de procesamiento requerida para factorizar los números primos. Esto hará que lo que hasta ahora suponía un sistema altamente seguro pase a ser bastante menos fiable. Este hecho se conoce desde el año 1994, en el que se publicó un algoritmo diseñado para ordenadores cuánticos que podría factorizar una clave de grandes dimensiones en su par de números primos en cuestión de segundos o de minutos.

Los investigadores identifican una solución en las primeras fases

El equipo de PQCRYPTO (Post-Quantum CRYPTOgraphyfor long-term security) identificó una estrategia bimembre: en paralelo a la asunción de que cabe encontrar una solución factible basada en el desarrollo de nuevas técnicas de cifrado, también conviene trabajar en técnicas que impliquen operaciones matemáticas para las que los ordenadores cuánticos no resulten eficientes.

Los investigadores pusieron de relieve diversas restricciones para las técnicas a desarrollar. Éstas deberían generar confianza, no ser demasiado costosas ni demasiado exigentes en lo que respecta a los sistemas informáticos. También deberán evitarse las claves excesivamente largas. Los autores insisten en un aspecto importante para el desarrollo de futuros sistemas de cifrado postcuánticos, prestar una atención inmediata a las cuestiones relacionadas con la normalización, de manera que todos los usuarios tengan que emplear los mismos sistemas de cifrado.

Para más información, consulte:
Sitio web del proyecto PQCRYPTO

Países

Países Bajos

Proyectos conexos

PROYECTO

Post-quantum cryptography for long-term security

PQCRYPTO

7 Septiembre 2023

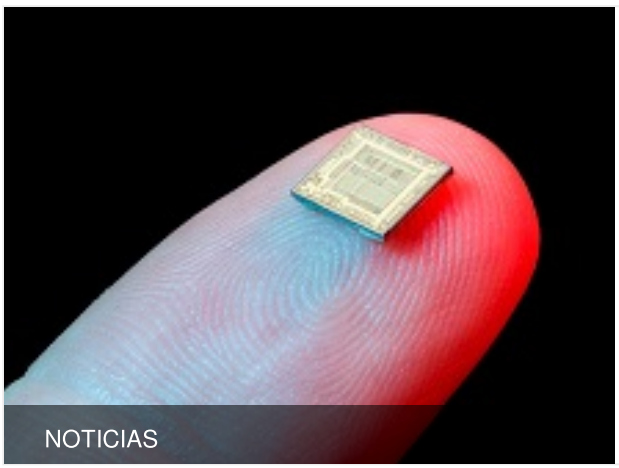
Artículos conexos

NOTICIAS

AVANCES CIENTÍFICOS

¿Se pueden prevenir los ciberataques cuánticos? Una iniciativa de la Unión Europea dice que sí y muestra cómo hacerlo

26 Marzo 2020



NOTICIAS

AVANCES CIENTÍFICOS

Un salto cuántico en los chips de silicio: logrado el acoplamiento espín-fotón

27 Febrero 2018

AVANCES CIENTÍFICOS

Los beneficios de los efectos cuánticos para las redes biológicas, sociales y tecnológicas

9 Febrero 2018

AVANCES CIENTÍFICOS

Un salto cuántico para la medición ultraprecisa y la codificación de información

24 Noviembre 2017

Última actualización: 11 Octubre 2017

Permalink: https://cordis.europa.eu/article/id/122627-securing-encryption-data-against-the-threat-of-future-quantum-computers/es