Un algoritmo de cifrado candidato de última etapa que estaba destinado a soportar el descifrado por parte de poderosas computadoras cuánticas en el futuro, se descifró trivialmente al utilizar una computadora con CPU Intel Xeon, en tan solo una hora.

El algoritmo en cuestión es SIKE, abreviatura de Supersingular Isogeny Key Encapsulation, que llegó a la cuarta ronda del proceso de estandarización de criptografía poscuántica (PQC) del Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio de Estados Unidos.

> *«Ejecutado en un solo núcleo, el código Magma adjunto rompe los desafíos de Microsoft SIKE $IKEp182 y $IKEp217 en aproximadamente 4 minutos y 6 minutos, respectivamente»,* dijeron los investigadores de KU Leuven, Wouter Castryck y Thomas Decru.

> *«Una ejecución en los parámetros SIKEp434, que anteriormente se creía que cumplía con el nivel 1 de seguridad cuántica de NIST, tomó alrededor de 62 minutos, nuevamente en un solo núcleo».*

El código se ejecutó en una CPU Intel Xeon E5-2630v2 a 2.60 GHz, que se lanzó en 2013 utilizando la microarquitectura Ivy Bridge del fabricante de chips, explicaron los académicos.

Los hallazgos se producen cuando el NIST, a inicios de julio, anunció el primer conjunto de algoritmos de cifrado resistentes a la cuántica: CRYSTALS-Kyber para cifrado general y CRYSTALS-Dilithium, FALCON y SPHINICS+ para firmas digitales.

> *«SIKE es un conjunto de encapsulación de claves basado en isogenia y caminatas pseudoaleatorias en gráficos de isogenia supersingulares»,* dice la descripción de los autores del algoritmo.

Microsoft, que es uno de los colaboradores clave en el algoritmo, dijo que SIKE utiliza *«operaciones aritméticas en curvas elípticas definidas sobre campos finitos y mapas de cómputo, las llamadas isogenias, entre tales curvas».*

> *«La seguridad de SIDH y SIKE se basa en la dificultad de encontrar una isogenia específica entre dos curvas elípticas de este tipo, o de forma equivalente, de encontrar un camino entre ellas en el gráfico de isogenia»,* explicó el equipo de investigación.

La criptografía resistente a la cuántica es un intento de desarrollar sistemas de encriptación que sean seguros frente a los sistemas informáticos tradicionales y cuánticos, al mismo tiempo que interactúan con los protocolos y redes de comunicaciones existentes.

La idea es garantizar que los datos cifrados hoy utilizando algoritmos actuales como RSA, criptografía de curva elíptica (ECC), AES y ChaCha20, no sean vulnerables a ataques de fuerza bruta en el futuro con la llegada de las computadoras cuánticas.

> *«Cada uno de estos sistemas se basa en algún tipo de problema matemático que es fácil de resolver en una dirección pero difícil en la inversa. Las computadoras cuánticas pueden resolver de forma sencilla los problemas difíciles que subyacen a RSA y ECC, lo que afectaría aproximadamente al 100% del tráfico de Internet encriptado si se construyeran computadoras cuánticas»*, dijo David Jao, uno de los co-inventores de SIKE.

Aunque SIKE se posicionó como uno de los contendientes de PQC designados por el NIST, la investigación más reciente invalida de forma efectiva el algoritmo.

> *«El trabajo de Castryck Decru rompe SIKE. Específicamente, rompe SIDH, el*

> *problema 'difícil' en el que se basa SIKE»,* dijo Jao.

> *«Hay otros criptosistemas basados en isogenia además de SIKE. Algunos de estos, como B-SIDH, también se basan en SIDH, y también están dañados por el nuevo ataque. Algunos de ellos, como CSIDH y SQIsign, no se basan en SIDH, y hasta donde sabemos, no se ven afectados directamente por el nuevo ataque».*

En cuanto a los próximos pasos, Jao dijo que si bien SIDH se puede actualizar para remediar la nueva línea de ataque de recuperación de claves, se espera que se posponga hasta un examen más detenido.

> *«Es posible que SIDH pueda parchearse o arreglarse para evitar el nuevo ataque, y tenemos algunas ideas sobre cómo hacerlo, pero se requiere más análisis del nuevo ataque antes de que podamos hacer una declaración con confianza sobre las posibles soluciones»,* agregó Jao.