Criptografía post-cuántica

Actividad colaborativa (M1AC2)

Criptografía post-cuántica: Los métodos avanzados (basados en el estudio de nuevos y viejos problemas matemáticos para los que no haya algoritmos conocidos que los rompan o que no sean vulnerables a la computación cuántica) hacia los que se está moviendo la criptografía moderna para enfrentar con éxito un posible ataque con el poderoso y oscuro (por ahora) ordenador cuántico.

Introducción

La aparición de los ordenadores cuánticos hace necesario buscar nuevos algoritmos de encriptación que sean robustos al aumento de capacidad computacional. Se han publicado algoritmos (K.L. Grover, 1997) mediante los cuales un ordenador cuántico reduciría el tiempo necesario para romper la criptografía simétrica a la raíz cuadrada del tiempo necesario actual. Así, se tardaría el mismo tiempo en realizar una búsqueda exhaustiva en un espacio de claves de 256 bits, que un ordenador actual en un espacio de claves de 128 bits (se podría decir que se reduce la seguridad de la clave a la mitad). Por todo esto la criptografía de clave simétrica no estaría muerta, pero si ligeramente tocada sin duplicar el tamaño de las claves. Sin embargo, la criptografía de clave asimétrica actual sí sería vulnerable, por lo que es necesario investigar nuevos algoritmos.

El NIST ya ha abierto un proceso de búsqueda de nuevos algoritmos. A continuación se exponen algunas de las vías de investigación actuales.

Vías de investigación

Criptografía de ecuaciones cuadráticas y multivariantes.

Criptografía de clave asimétrica basada en polinomios de múltiples variables en un campo finito. Son útiles para la realización de firmas digitales, ya que produce firmas digitales más cortas que otros algoritmos post cuánticos, pero no han demostrado ser los suficientemente seguros para usarlos en el cifrado.

Estos sistemas criptográficos se basan en la resolución de problemas de ecuaciones no lineales en variables sobre cuerpos finitos. La clave privada se compone de dos transformaciones afines y una matriz. La clave pública se compone de una combinación de las tres, de manera que hacer la transformada para obtener la clave privada es computacionalmente difícil.

Criptografía basada en hash

Las funciones hash son algoritmos que al aplicarlos sobre un mensaje, archivo o texto, entregan un resumen de x bits.

Como sabemos, realizan dos papeles importantes en criptografía: verificar la integridad de un mensaje (proporciona una verificación de si el mensaje ha sido modificado mientras se transmitía) y para reducir y adaptar ese mensaje para su firma digital.

Es importante destacar, que una de las cosas más importantes en los hashes, es evitar las colisiones, es decir, obtener el mismo hash (o resumen) con mensajes con distinto contenido (como ya ha ocurrido con SHA-1. Puede consultarse la rotura de este algoritmo en la web https://shattered.it/)

Muchas de las funciones hash utilizadas en la actualidad serían vulnerables a ataques cuánticos que empleasen el algoritmo de Grover (como ya se ha comentado en contribución individual al foro). Por lo tanto las funciones de hash, probablemente se tendrían que duplicar su rango, para asegurar que sigan siendo seguros en un entorno cuántico.

Usando hashes basados en árboles de Merkle, entre los que destacan XMSS y SPHINCS (con claves de 256 bits), se consideran suficientemente sólidos para firmas digitales postcuánticas.

Criptografía basada en código

Para la creación de la clave pública es necesario generar una matriz a través de la multiplicación ciertos códigos lineales llamados códigos de Goppa. El principal problema de este cifrado, es que para generar una clave pública suficientemente segura para la criptografía postcuántica, tendría que estar por encima de 8 millones de bits. El mensaje cifrado, es el resultado de la multiplicación de ésta matriz por el mensaje en claro.

Aún así, el cifrado y el descifrado se consideran eficientes, y la principal ventaja para aplicar criptografía basada en código, es que para deshacer la multiplicación que genera la matriz (que necesitaría un potencial atacante para descubrir el mensaje en claro) no se conoce ningún método para deshacer estas matrices, con lo que parece viable usarlos de forma segura para cripto postcuántica.

Algunos ejemplos de cifrado en códigos es el cifrado McEliece y el criptosistema de Niederreiter.

Criptografía Isogenética de la Curva Elíptica Supersingular (SIDH)

Algoritmo post cuántico cuyo objetivo es el intercambio de claves, y que busca sustituir a los algoritmos de Diffie-Hellman Exchange (DHE) y Elliptic Curve Diffie Hellman (ECDHE) en la era cuántica. Fue creado en 2011 por De Feo, Jao, and Plut. Debido a que funciona de forma similar a los mismos actualmente se considera una opción muy interesante.

Criptografía basada en retículos

Criptografía de clave asimétrica basada en problemas matemáticos de retículos. Se considera una buena candidata para la criptografía post cuántica ya que para algunos de los problemas que surgen no existen algoritmos conocidos capaces de resolverlos ni siquiera con la capacidad computacional de los ordenadores cuánticos.

Uno de estos problemas es el SVP (Shortest Vector Problem). Este problema consiste en encontrar el vector más corto no nulo del retículo con menor norma euclídea. Para resolver de manera eficiente este problema se necesita resolver el problema de reducción de base del retículo.

Algoritmos cuánticos recientes parecía que habían descartado este método pero se ha visto que había errores en el diseño de los mismos y por ahora sigue siendo un sistema resistente a la computación cuántica.

Conclusiones

Las conclusiones tras analizar el estado del arte actual de la criptografía postcuántica son las siguientes:

- No estamos preparados todavía para la criptografía pos-cuántica, se está empezando a trabajar en ella, pero debemos comenzar esta transición mucho antes de que lleguen los ordenadores cuánticos.
- Se necesita más tiempo para mejorar su eficiencia, sobre todo para que las claves usadas en los algoritmos sean más pequeñas, más implementables..
- Se tiene que demostrar que estos algoritmos son seguros, al menos hasta el mismo nivel que tenemos ahora.
- Se debe mejorar la usabilidad para los usuarios de este tipo de sistemas.
- Comparando la criptografía simétrica actual con la postcuántica, simplemente generando claves más grandes en algunos casos, “podría” mantenerse su nivel de seguridad.
- La criptografía asimétrica postcuántica, aunque ya hay propuestas, se debería esperar a que el NIST apruebe y estandarice esos nuevos algoritmos, pero se estima que tarde años en definirse.
- El proceso de estandarización de los nuevos algoritmos tardará varios años, ya que tras su presentación, se abre un periodo de análisis de seguridad y vulnerabilidad, de manera que se consiga la confianza suficiente en su invulnerabilidad.

Anexo I: Bibliografía

Frente al computador cuántico, Criptografía postcuántica (CSIC-UAM)
https://www.youtube.com/watch?v=-fKOCr2J2MU

La criptografía Post-Quantum
https://ciberseguridad.blog/la-criptografia-post-quantum/

Report on Post-Quantum Cryptography
https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

Computación cuántica, ¿un Armagedón criptográfico?
https://www.welivesecurity.com/la-es/2016/06/14/computacion-cuantica-armagedon-criptografico/

Informe eSAMCid sobre criptografía post-cuántica
https://mat-web.upc.edu/people/jorge.villar/esamcid/rep/posq/reportpostqse3.html

SPHINCS: practical stateless hash-based signatures
https://sphincs.cr.yp.to/

Las Matemáticas en la evolución de la Criptografía
https://cybercamp.es/sites/default/files/contenidos/videos/adjuntos/cybercamp2017-las_matematicas_en_la_evolucion_de_la_criptografia_consuelo_martinez_lopez.pdf

¿Hay criptografía después del gato? https://www.incibe-cert.es/blog/hay-criptografia-despues-del-gato