M1AC2. Actividad colaborativa 2

Calificación: 95

José Alberto Peña Rodríguez.
José Hernán Pérez Zúñiga.
David Potsch.
Víctor Rodríguez Boyero.
César Arturo Sarmiento Martínez.

Criptografía post cuántica. Algoritmos.

La criptografía postcuántica engloba los algoritmos criptográficos capaces de resistir ataques realizados a través de la computación cuántica.

El problema con los algoritmos actuales es que su seguridad se puede romper fácilmente en un ordenador cuántico suficientemente potente que ejecute el algoritmo de Shor y, aunque los actuales ordenadores cuánticos experimentales no son aún capaces de atacar cualquier algoritmo criptográfico real, muchos criptógrafos están diseñando algoritmos resistentes para adelantarse a la amenaza. Existen varias alternativas:

1. Criptografía de ecuaciones cuadráticas y multivariantes.

Uno de los sistemas Criptográficos que se cree que resistirán a la computación cuántica son las criptografías de ecuaciones cuadráticas y multivariantes.

Es una 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 postcuánticos, 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 a fines 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.

2. Criptografía basada en hash.

Otra de las alternativas la criptografía afectada por la computación cuántica es la criptografía basada en hashes, actualmente el algoritmo más usado es el SHA256, no se espera que los algoritmos basados en hash actuales se vean afectados por la computación cuántica, ya que se considera que el algoritmo de Grover no puede romper un hash como

SHA256. Su desventaja es que generan firmas relativamente largas, pero es una de las alternativas con más fuerza para reemplazar a RSA y ECDSA.

El árbol de hashes, o árbol de Merkle, es una invención de Ralph Merkle, en la práctica se busca relacionar una serie de datos separados en un único hash raíz para reducir el tiempo y recursos empleados en verificar la integridad de una cantidad de información, esta estructura relaciona todas las transacciones y las agrupa entre pares para obtener el "root hast" el cual están basados en todos los hash del árbol. Es el sistema usado en Bitcoin y Blockchain.

La estructura está formada por un árbol invertido de hashes, el hash raíz se encuentra en la parte superior y de él se van generando ramas hacia abajo, que van conteniendo los hashes de otras ramas de niveles inferiores, hasta llegar a las "hojas" del árbol, que en el caso de una cadena de bloques representan los eventos o transacciones.

Verificar todas las transacciones de una red sería algo extremadamente lento e ineficiente, por eso se implementó este sistema: Si un hash es cambiado, cambiarían todos los demás hasta llegar a la raíz (root hash)

En un Árbol de Merkle los hashes se agrupan en pares en una relación 2n, donde 'n', es la cantidad de pares, y no existe un número máximo determinado, pueden ser 2, 4, 8, 16… los límites los establece el tamaño del bloque.

De esta forma, validar 10.000 transacciones en la red cuestan lo mismo que validar una única transacción.

Cualquier intento de manipulación de una transacción de un bloque validado provocaría un cambio en los hashes propagados, hasta llegar al root hash.

El root hash no se puede modificar, ya que depende de otras ramificaciones. Si se detecta un intento de cambio, este se invalida automáticamente, lo mismo sucedería si se intentan añadir transacciones.

3. Criptografía basada en código.

Con la construcción de computadoras cuánticas, los criptosistemas comunes de clave pública como RSA, El Gamal y la criptografía de curva elíptica ya no serán seguros. Dado este hecho, la susceptibilidad o resistencia de otros criptosistemas de clave pública a los ataques cuánticos es de interés fundamental. Los criptosistemas basados en código (McEliece y Niederreiter) no son susceptibles a los ataques cuánticos de muestreo de Fourier que paralizan RSA y El Gamal, siempre que el código subyacente satisfaga ciertas propiedades algebraicas.

Si bien existen ataques clásicos conocidos en estos sistemas para el caso de los códigos de Goppa racionales, la mayoría de investigaciones, aún apuntan que se consideran seguros en términos clásicos. Si bien estos resultados no descartan otros ataques cuánticos, sí se

siguen considerando resistentes a los tipos de algoritmos cuánticos que han demostrado ser tan poderosos para los problemas de la teoría de números.

4. Criptografía basada en isogenias de las curvas elípticas supersingulares.

La criptografía de curva elíptica es una de las más populares, es extremadamente segura desde el punto de vista matemático y comparado con RSA, ECDSA utiliza claves más pequeñas y una implementación más eficiente, nos permitirá obtener una clave pública a partir de una clave privada. Con ambas claves ya podremos firmar transacciones y verificar luego las firmas. ECDSA es por el momento el esquema utilizado por la mayor parte de los protocolos blockchain.

ECDSA utiliza una serie de operaciones aritméticas especiales sobre puntos en una curva elíptica. Para ello se recurre a dos tipos de operaciones especiales: la suma y la multiplicación de puntos en la curva. Las fórmulas aritméticas nos suelen dar resultados con decimales y eso ocasiona un problema que hay que resolver, para solucionar este problema deberemos usar sólo los puntos de la curva que se puedan representar con números enteros, sin decimales. Todos los demás los obviamos.

Puntos importantes:

- La clave privada no es más que un número aleatorio sobre el que podemos realizar cálculos matemáticos normales.
- La clave pública en cambio es un punto en una curva elíptica sobre el que sólo se pueden realizar operaciones de suma y multiplicación, pero no se pueden dividir.
- Es fácil calcular la clave pública usando el sistema de multiplicación escalar y prácticamente imposible de obtener la clave privada mediante fuerza bruta.
- Es muy importante que la clave privada sea aleatoria. La mayor parte de los problemas de seguridad detectados hasta el momento se deben a una mala implementación a la hora de generar la clave privada.

5. Criptografía basada en retículos.

Criptografía de clave asimétrica cuyas primitivas se basan en retículos. Los criptosistemas basados en retículos son bastante eficientes y sencillos de implementar, pero la resolución de las matemáticas subyacentes es complicada y aparentemente resistente a la computación cuántica que no ha logrado todavía encontrar un algoritmo con mayor eficiencia que los que utilizan computación tradicional.

Es un término genérico para la construcción de primitivas criptográficas que utilizan retículos, bien en la propia construcción, bien en la prueba de seguridad. Las construcciones basadas en retículos son, en la actualidad, candidatos importantes para la denominada criptografía postcuántica, ya que, a diferencia de los esquemas de clave pública más utilizados, como son los RSA, Diffie-Hellman o la criptografía de curva elíptica, que pueden ser fácilmente atacables usando un computador cuántico.

Varias construcciones basadas en retículos parecen ser resistentes a los ataques basados tanto en computación cuántica como clásica. Además, se ha demostrado que muchas construcciones basadas en retículos son seguras asumiendo que no es posible resolver de forma eficiente ciertos problemas bien conocidos de retículos.

Se basa en el problema del Aprendizaje con Errores (LWE, aprendizaje automático o machine learning) y en una versión definida sobre un anillo: Ring-LWE.

• Protocolos de acuerdo de clave tipo DH (basados en distribuciones estadísticas y R-LWE): Peikert-2014, Bos et al.-2015 y Alkim et al.-2015 (NewHope).

• Cifrado, firma y hashes: NTRU, Ajtai-Dwork (basados en LWE).

Existen distintas propuestas para construir cifrado de clave pública a partir de este problema y de problemas relacionados, como el llamado problema del vector más próximo o "closest vector problema". Mencionamos los más destacados:

- Esquema de Regev: primera propuesta basada en LWE. Esencialmente académica.
- NTRU: propuesto en 1998, no es completamente homomórficopero mantiene bien la estructura para un número prefijado de cálculos con dos operaciones no demasiado grande (según implementaciones).
- BGV: completamente homomórfico, implementado en la librería HELib. Es una variante del aclamado esquema de Gentry que usa el problema LWE sobre anillos (llamado también RLWE).

Notas y referencias:

Bernstein, D., Buchmann, J. & Dahmén, E. (2009). Post-quantum cryptography. Berlin: Springer.

https://es.wikipedia.org/wiki/Criptografía_postcuántica
https://es.wikipedia.org/wiki/Árbol_de_Merkle
https://ciberseguridad.blog/la-criptografia-post-quantum/
https://blog.elevenpaths.com/2019/01/futuro-post-cuantico-ciberseguridad.html
https://bitcoin.es/criptomonedas/funciones-hash-y-arboles-de-merkle-protegen-blockchain/
http://www.criptored.upm.es/crypt4you/temas/ECC/leccion1/leccion1.html#04
https://www.exabyteinformatica.com/uoc/Informatica/Criptografia_avanzada/Criptografia_avanzada_(Modulo_4).pdf
https://libroblockchain.com/ecdsa/
https://www.oroyfinanzas.com/2014/01/criptografia-curva-eliptica-bitcoin-por-que-utiliza-ecdsa/
https://cybercamp.es/sites/default/files/contenidos/videos/adjuntos/cybercamp2017-las_matematicas_en_la_evolucion_de_la_criptografia_consuelo_martinez_lopez.pdf
https://www.incibe-cert.es/blog/hay-criptografia-despues-del-gato
https://es.wikipedia.org/wiki/Criptograf%C3%ADa_basada_en_ret%C3%ADculos
https://www.ccn-cert.cni.es/pdf/documentos-publicos/xi-jornadas-stic-ccn-cert/2599-m31-02-frente-al-computador-cuantico/file.html
https://mat-web.upc.edu/people/jorge.villar/esamcid/rep/posq/reportpostqse3.html#x5-100003.4