Criptografía Post Cuántica

Diego Cordoba[3], Miguel Méndez-Garabetti[1,2]

[1]Univerisdad de Mendoza, Dirección de Posgrado, Facultad de Ingeniería
diego.cordoba@um.edu.ar, miguel.mendez@um.edu.ar

[2]Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET)

[3]Universidad de Mendoza, Facultad de Ingeniería, Subsede San Rafael

RESUMEN

La criptografía es la base de cualquier mecanismo de seguridad informática. Se utiliza habitualmente en un login web, en el envío de correos electrónicos, o incluso cuando se produce la sincronización de archivos en la nube, entre otros. Todos los protocolos de comunicación que utilizan SSL/TLS en TCP/IP [1] hacen uso de criptografía asimétrica para autenticación y firma digital. Estos algoritmos se basan en complejos cálculos matemáticos de una sola vía, es decir, son fáciles de realizar, pero muy difíciles de revertir. Si bien los ordenadores actuales no son capaces de romper estos algoritmos en periodos de tiempo aceptables, las computadoras cuánticas, hoy en sus albores de desarrollo, sí podrán hacerlo fácilmente. Es aquí donde surge la necesidad de algoritmos de cifrado que sean resistentes a ataques cuánticos. Estos algoritmos, denominados post etapas de investigación, resultarán de suma utilidad en un futuro cercano, en el que las técnicas de cifrado asimétrico actuales no puedan brindar la privacidad, autenticación e integridad de los datos en Internet. El presente trabajo de investigación pretende dar luz en este moderno campo de estudio, analizando las implementaciones de software y bibliotecas de programación disponibles en la actualidad.

Palabras clave: *criptografía; post cuántico; seguridad informática; criptografía asimétrica*

CONTEXTO

El presente trabajo de I+D se desarrolla como proyecto se tesis de posgrado de la Maestría en Teleinformática, Dirección de Posgrado, perteneciente a la Facultad de Ingeniería de la Universidad de Mendoza, (Ciudad, Mendoza). El presente proyecto será presentado como propuesta de tesis.

1. INTRODUCCIÓN

El advenimiento de la computación cuántica, al menos hoy en día en forma teórica más que práctica, resulta una amenaza a los algoritmos de cifrado clásicos debido a que un ordenador cuántico puede procesar mucha más información en menos tiempo, que un ordenador clásico. [illegible] en el caso de que un atacante provisto de un ordenador cuántico logre interceptar tráfico de red cifrado en forma tradicional, este podría romper dicho cifrado y obtener el contenido de los mensajes originales.

La seguridad de la criptografía moderna se basa en supuestos de complejidad computacional no demostrados, de modo

que en general, las claves se generan mediante operaciones denominadas "de una sola vía", es decir, operaciones matemáticas muy simples de calcular pero extremadamente difíciles de revertir. Actualmente, por ejemplo, una clave de cifrado puede generarse a partir de la multiplicación de dos números primos grandes. Esta operación es muy simple de calcular con cualquier ordenador clásico. Luego, teniendo el resultado de este producto, un supuesto atacante debería invertir mucho tiempo y procesamiento computacional para encontrar los dos números primos que dieron origen al producto. Hasta hoy, el tiempo necesario es la limitante, ya que las claves de cifrado pueden cambiar periódicamente, por ejemplo, cada hora, de modo que el atacante nunca llegue a tener tiempo suficiente para encontrar la clave y romper el tráfico cifrado que pudo ir acumulando. Si el atacante, por su parte, dispusiera de un ordenador cuántico, encontrar la clave puede ser una tarea muy rápida y permitiría vulnerar casi cualquier tráfico cifrado mediante las técnicas de la criptografía moderna que conocemos.

El algoritmo de Shor[2] fue el primer algoritmo cuántico no trivial que demostró un potencial de crecimiento exponencial de velocidad sobre los algoritmos clásicos. Es un algoritmo cuántico para descomponer en factores un número N en un tiempo $O((\log N)^3)$, y debe su nombre al profesor de matemáticas aplicadas del MIT Peter Shor. Un mensaje cifrado por el algoritmo asimétrico RSA puede ser descifrado descomponiendo en factores la clave pública, que es producto de dos números primos grandes. Los algoritmos clásicos no pueden factorizar la clave pública N de RSA en un tiempo menor a $O((\log N)k)$, para ningún k, por lo que RSA sigue siendo un algoritmo de cifrado seguro[3][4][5]. Este algoritmo es la base del criptoanálisis cuántico, y ha demostrado ser capaz de romper RSA en un tiempo polinómico [2].

Por otro lado, el algoritmo de Shor, como todos los algoritmos de computación cuántica, da su resultado en forma probabilística con un determinado grado de acierto, por lo que se requieren ejecuciones sucesivas del mismo para aumentar el porcentaje de exactitud del resultado.

En la práctica, un grupo de trabajo de computación cuántica de IBM liderado por Isaac Chuang logró por primera vez factorizar el número 15, el menor número que valida el algoritmo de Shor, en sus factores 3 y 5 mediante una computadora cuántica de 7 qubits. Luego, en marzo del 2016, el mismo Chuang, junto a un grupo de investigadores del MIT, lograron crear un ordenador cuántico de 5 qubits que también pudo correr el algoritmo de Shor para factorizar en número 15 con una confianza del 99%.

Es importante tener en cuenta que, la aparición de las computadoras cuánticas y su posterior comercialización, deja obsoletos muchos de los algoritmos criptográficos que actualmente son seguros; tales como RSA, DSA o ECDSA [3][6][7][8]. No obstante, esto no es razón suficiente para decir que la computación cuántica destruirá la criptografía. Hay muchas clases importantes de criptografía más allá de los algoritmos conocidos:

1. *Criptografía basada en hash (hash-based):* incluye sistemas criptográficos como las firmas Lamport y el esquema de firmas Merkle [3] . Particularmente estas últimas, creadas en 1970, son de especial importancia como posibles

sucesores a las firmas digitales RSA y DSA actuales. Perdió importancia en su momento ante las firmas RSA, pero luego tomó mayor renombre al ser un sistema de firmas resistente a los ataques cuánticos.

2. *Criptografía basada en código (code-based):* aquí el ejemplo clásico es el esquema de firmas McEliece con códigos aleatorios Goppa, y ha sido recomendado por el Post Quantum Cryptography Study Group[3][9] (patrocinado por la unión europea) como candidato para la protección contra ataques cuánticos.

3. *Criptografía basada en sistemas de ecuaciones multivariable*: aquí se encuentran los sistemas criptográficos como el esquema Rainbow[10] basado en la dificultad de solucionar sistemas de ecuaciones con múltiples variables. Aunque varios sistemas de cifrado basado en ecuaciones multivariables han fracasado, Rainbow podría proporcionar las bases para firmas digitales a prueba de ataques cuánticos.

4. *Criptografía basada en enrejado (lattice based):* incluye sistemas criptográficos como el algoritmo de intercambio de claves de aprendizaje con errores, o las firmas de anillos de aprendizaje con errores, los sistemas de cifrado NTRU y GGH, y las firmas digitales NTRU y BLISS. Actualmente se está estudiando la variante Stehle-Steinfeld de NTRU para su estandarización como algoritmo postcuántico válido[11].

5. *Cifrado simétrico basado en clave secreta de Rijndael*: éste hoy llamado AES, sigue siendo un cifrado seguro contra ataques cuánticos siempre y cuando la longitud de la clave sea mayor, y acorde a las capacidades de cálculo.

Todos estos algoritmos y técnicas son cuánticamente seguros, y por consecuencia, a ninguno se le ha podido aplicar el algoritmo de Shor.

En la actualidad casi la totalidad del tráfico web en Internet corre sobre SSL/TLS. El intercambio de datos de autenticación o números de tarjetas de crédito suelen protegerse mediante HTTPS[12]. Debido a esto, surgió la necesidad de comenzar a pensar e implementar algoritmos post cuánticos para proteger este tipo de tráfico en Internet. Con el fin de nuclear el desarrollo de implementaciones prototípicas de algoritmos criptográficos post cuánticos, vio la luz el proyecto Open Quantum Safe (OQS)[13].

Las ramas de desarrollo de OQS se dividen en dos. Por un lado, el desarrollo de una biblioteca de cifrado post cuántico implementada en lenguaje C, liboqs, y por otro, prototipos de las integraciones de esta biblioteca en implementaciones tradicionales. liboqs es open source licenciado bajo los términos de la licencia del MIT, lo que le permite a cualquier desarrollador disponer del código fuente y utilizar la librería para sus propias implementaciones.

Una aplicación prototipo importante, propuesta por el proyecto OQS, es un fork de OpenSSL v1.0.2, que hace uso de liboqs para poder cifrar comunicaciones con algoritmos resistente a ataques cuánticos.

2. LINEAS DE INVESTIGACIÓN Y DESARROLLO

Las líneas de investigación y desarrollo en criptografía post-cuántica son numerosas, principalmente debido a que la criptografía forma parte de prácticamente todos los mecanismos de seguridad de datos en Internet. Entre ellas podemos enumerar las siguientes.

1. Analizar y documentar los algoritmos de cifrado resistentes a ataques cuánticos disponibles en la actualidad.

2. Estudiar las librerías de programación disponibles en la actualidad para escribir aplicaciones criptográficas que utilicen algoritmos de cifrado post-cuánticos. Entre ellas, liboqs, del proyecto OQS, libntruencrypt, del proyecto NTRU Open Source Project, y NFLlib, una librería que implementa fast lattice basada en NTT (Numerical Theoretic Transform).

3. Analizar la viabilidad de proyectos de software que implementen el protocolo SSL, para su uso en servicios en producción. Se pretenden medir parámetros de rendimiento para los algoritmos de cifrado post-cuántico soportados, realizar pruebas de testing y detección de fallos para poder ayudar a la toma de decisiones sobre su implementación en sistemas de producción. En este punto se pretenden estudiar el fork de OpenSSL v1.0.2 del proyecto OQS, y el fork de OpenSSL v1.0.2e de vscrypto, denominado OpenSSL-ringlwe, que implementa de manera práctica el protocolo de intercambio de claves RingLWE.

4. Analizar la estabilidad y viabilidad de StrongSwan para el establecimiento de túneles VPN con IPSec haciendo uso de algoritmos NTRU.

5. Analizar la estabilidad y viabilidad de CodeCrypt, una implementación abierta GNUPG-like como reemplazo a GNUPG para el cifrado asimétrico.

6. Analizar e implementar sistemas de cifrado para almacenamiento de datos en la nube mediante algoritmos de cifrado resistentes. Aquí se pretenden estudiar EncFS y CryFS[14].

3. RESULTADOS ESPERADOS

Luego de analizar los algoritmos post cuánticos disponibles, las bibliotecas de programación, y las herramientas de software que ya hacen uso de estas bibliotecas, se pretende determinar la viabilidad del uso de estas implementaciones en sistemas en producción.
Como resultados intermedios, también se obtendrán muestras de rendimiento de los algoritmos post cuánticos en el uso de comunicaciones SSL/TLS donde hoy se implementa cifrado asimétrico no resistente a ataques cuánticos, y realizar comparaciones de performance con las herramientas actuales.
Por otro lado, el análisis de las implementaciones de software y bibliotecas de cifrado post cuántico también permitirá detectar errores de funcionamiento, o bugs, y se podrán plantear soluciones de mejora.

4. FORMACIÓN DE RECURSOS HUMANOS

La línea de I+D presentada está vinculada con el desarrollo de una tesis de posgrado por parte del Ing. Diego Córdoba, quien es estudiante de la Maestría en

Teleinformática de la Universidad de Mendoza.

5. BIBLIOGRAFÍA

[1] W. Stallings, Data and computer communication, Prentice Hall, 2006

[2] P. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Compute,AT&T Researc, 1996

[3] D. J. Bernstein, J. Buchmann, E. Dahme, Post Quantum Cryptograph, Bernstein - Buchmann - Dahme, 2009

[4] R. Rivest, A. Shamir, L. Adlema, A Method for Obtaining Digital Signatures and Public-Key Cryptosystem, Communications of the AC, 1978

[5] E. W. Weisstein, RSA-640 Factored, MathWorld Headline New, 200, http://mathworld.wolfram.com/news/2005-11-08/rsa-640/

[6] M. Campagna, L. Che, Quantum Safe Cryptography, An introduction, benefits, enablers and challenge,ETSI White Pape, 2015

[7] T. Takagi, Post-Quantum Cryptography – 7th International Workshop, PQCrypt,Springe, 2016

[8] R. A. Perlner, D. A. Cooper, Quantum Resistant Public Key Cryptography: A Surve, National Institute of Standards and Technolog, -

[9] D. J. Bernstein, T. Lange, C. Peter, Attacking and Defending, the McEliece cryptosyste, PQCrypt, 2008

[10] P. Oechsli, Making a Faster Cryptanalytical Time-Memory Trade-Of, Advances in Cryptology: Proceedings of CRYPT, 2003

[11] T. Lange, Initial recommendations of long-term secure post-quantum systems - Horizon 2020 ICT-64562,PQCRYPTO.E, 2015

[12] EC Council, Network Defense, Fundamentals & Protocol, EC Council Press, 2010

[13] D. Stebila, M. Mosc, Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Projec, Department of Computing and Software, Mc Master Universit, 2016

[14] S. Messmer, CryFS: Design and Implementation of a Provably Secure Encrypted Cloud Filesyste, Institute of Theoretical Informatics, Karlsruhe Institute of Technolog, 2015