“Algoritmos de encriptación resistentes frente a la computación cuántica”

Alumno: Soria Gava, Lucas Damian. 42670460.

Docentes a cargo:

Leiton, Ruth.

Navarro, Diego

Cátedra: Trabajo Integrador Final 1 (TIF).

Carrera: Ingeniería en informática.

Año: 2021.

Sede: Central.

Fecha de entrega: Junio 20, 2021.

Introducción:

Junto con el desarrollo de la computación cuántica, surgen interrogantes que competen al área de la seguridad informática, más específicamente la encriptación. Se estima que cuando la computación cuántica sea accesible para las masas, ésta podrá ser usada para desencriptar información protegida por los métodos de encriptación tradicionales. Es frente a este peligro que surge la propuesta o necesidad de generar métodos de encriptación “resistentes a la computación cuántica” o “a prueba de cuántica”.

El Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST por sus siglas en inglés) decidió, en 2016, hacer una convocatoria para desarrollar un nuevo método estándar de encriptación “post-cuántico”, para el año 2022. A este proyecto se le llamó “NIST Post-Quantum Cryptography Standardization Process”.

Gigantes tecnológicos como Microsoft e IBM han colaborado en el proceso iniciado por el NIST, apoyando o presentando sus propias ideas. En el caso de IBM, colaborando en el proyecto de código abierto, Crystal. Mientras que Microsoft apuesta por la fortaleza de los números, colaborando en el desarrollo de 4 proyectos: FrodoKEM, SIKE, Picnic y qTesla. Con la esperanza de que alguno pase a la etapa final del proceso de estandarización del NIST.

Durante la lectura de este ensayo, se espera poder hacer evidente la necesidad y urgencia de desarrollar nuevos algoritmos que resistan a la computación cuántica y estándares para la protección de la información sensible, a pesar de que esta no represente una amenaza inminente. Es primordial empezar cuanto antes, ya que una preparación temprana evitará graves problemas en el futuro.

Desarrollo:

La clave de los algoritmos de encriptación actuales reside en el aprovechamiento del artificio matemático de la factorización de números grandes que han sido generados a partir de la multiplicación de números primos. La complejidad de esta tarea es tal que, una computadora tradicional tarda tanto tiempo en llegar a una respuesta que, para el momento en que se logra desencriptar la información (encontrar los primos que componen este gran número), esta ya no es útil para el atacante o ya cambió. Como señala el equipo de Emerging Technology de arXiv (2019): “These encryption systems have never been unbreakable. Instead, their security is based on the huge amount of time it would take for a classical computer to do the job”.

Sin embargo, la computación cuántica permite resolver estos problemas en un tiempo considerablemente menor al que le toma a las computadoras tradicionales actuales. En palabras de Chad Boutin (2020), escritor científico para el NIST:

> “Classical computers have many strengths, but they find some problems intractable — such as quickly factoring large numbers. Current cryptographic systems exploit this difficulty to protect the details of online bank transactions and other sensitive information. Quantum computers could solve many of these previously intractable problems easily, and while the technology remains in its infancy, it will be able to defeat many current cryptosystems as it matures”.

Otros autores, como Jeremy Hsu (2020) y Amy Nordrum (2016) también están de acuerdo en que si bien este problema todavía es lejano, representa un riesgo potencial y por tanto, se deben tomar cartas en el asunto. Por otro lado, Samuel K. Moore (2019) y otros, si bien alientan el desarrollo de un nuevo algoritmo de encriptación, no creen que este sea un problema tan apremiante.

En el año 1994 el matemático Peter W. Shor publicó “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”. En este paper Shor propuso un algoritmo que años más tarde le permitiría a las computadoras cuánticas factorizar números enteros,

encontrando los números primos que lo componen. En palabras de Tom Simonite (2015), jefe de oficinas del MIT Technology Review's en San Francisco:

> "By using quantum states to exploit the mathematical structure of the problem, such a computer could effectively take a shortcut to the right answer. Shor's algorithm can also be modified to crack a stronger alternative to RSA encryption, known as elliptic curve cryptography, which is becoming more common and is also used with TLS to secure online data".

Para entender por qué estos algoritmos son vulnerables ante la computación cuántica, primero debemos entender cómo funcionan.

RSA (Rivest–Shamir–Adleman):

RSA, que obtiene su nombre de las iniciales de los creadores del método, es la implementación de un sistema criptográfico de clave pública, donde la clave pública, es un archivo revelado o disponible al público. Mientras que la clave privada es un archivo del que solo debe tener acceso una entidad.

Los mensajes son encriptados cuando pasan por un algoritmo que los representa numéricamente, eleva ese número obtenido a la e-aba potencia, conocida gracias al archivo de clave pública y se toma el resto de la división por un número *n*, también conocido.

Como se dijo al principio del ensayo, la seguridad del método reside en dicho número *n*, el cual es el producto de dos números primos grandes, que se mantienen ocultos. La factorización de números grandes es un problema extremadamente difícil de resolver para las computadoras tradicionales y por lo tanto se supone que el tiempo que se tarda en encontrar esos dos números primos es tal que, resulta impracticable.

Siendo así, para poder encriptar información, el emisor utiliza la llave pública del receptor, lo que le permite enviarle el mensaje encriptado a través de un medio no seguro. Una vez recibido el mensaje, el receptor utiliza su propia llave privada para desencriptar dicho mensaje.

RSA surgió cuando el correo electrónico empezó a popularizarse, como una propuesta para transmitir mensajes privados y "firmados" digitalmente a través de un medio no seguro.

ECC (Elliptic Curve Cryptography):

Este método promete ser más veloz y seguro que estándares de criptografía de clave pública como RSA, utilizando claves más pequeñas.

La función que usa este método es la multiplicación entre *k* y *P*, siendo *k* un entero y *P* un punto en una curva elíptica, que da como resultado *Q*. Cuando se conocen *P* y *Q*, la operación que permite recuperar *k* se llama "Elliptic Curve Discrete Logarithm Problem" (ECDLP). Hasta la fecha no existe un algoritmo de tiempo subexponencial capaz de resolver este problema, siendo tiempo subexponencial un tiempo de ejecución de algún algoritmo que puede crecer más rápido que cualquier función polinomial, pero que aún es significativamente más pequeño que una función exponencial.

Por último, las siguientes figuras, extraídas del paper "Elliptic Curve Cryptography And Its Applications", demuestran que ECC utiliza tamaños de claves más pequeñas que RSA para conseguir el mismo nivel de seguridad.

Symmetric-key	ECC	RSA/DLP
64 bit	128 bit	700 bit
80 bit	160 bit	1024 bit
128 bit	256 bit	2048-3072 bit

"Key length for public-key and symmetric-key cryptography" (p.2).

ECC Key Size (bits)	RSA Key Size (bits)	Key Size ratio
160 bit	1024 bit	1:6
224 bit	2048 bit	1:9
256 bit	3072 bit	1:12
512 bit	15360 bit	1:30

"Equivalent Key Sizes for ECC and RSA" (p.4).

En 2001, Isaac Chuang y su grupo de investigadores del MIT, lograron factorizar, con el algoritmo de Shor, el número 15 utilizando 5 qubits, cuando antes se creía que para ello se necesitaban 12. La encriptación RSA utiliza típicamente un tamaño de llave de entre 2048 bits a 4096 bits, que se presume casi imposible de crackear por una computadora tradicional. Según el artículo antes citado del equipo de Emerging Technology de arXiv (2019), se creía que para que una computadora cuántica pueda factorizar 2048 bits se necesitaban 10^9 (mil millones) qubits, hasta que, las investigaciones de Craig Gidney y Martin Ekerå, investigadores de Google, revelaron que este cálculo podría hacerse con $2x10^7$ (veinte millones) de qubits, disminuyendo el número en 2 magnitudes.

Esta disminución se debe al desarrollo de una forma más eficiente de realizar los cálculos de exponenciación modular, que resulta ser la operación computacionalmente más costosa del algoritmo de Shor, en términos de qubits.

Actualmente, las computadoras cuánticas poseen cerca de 65 qubits. A pesar de ello, Adrian Cho expresa en su artículo en la revista Science (2020) que IBM quiere desarrollar una computadora cuántica con 1000 qubits para el año 2023, pasando por etapas intermedias de 127 qubits para el año 2021 y 433 para 2022. Para poder alcanzar la supremacía cuántica se requieren aproximadamente 50 qubits. La supremacía cuántica o ventaja cuántica, es el potencial de una computadora cuántica de resolver problemas más velozmente que una computadora tradicional.

En virtud de estas circunstancias es que es necesario y urgente el desarrollo de un nuevo algoritmo de encriptación “post-cuántico”. A pesar de que se estima que todavía faltan entre 15 y 30 años para llegar al punto en que la encriptación actual pueda ser crackeada por una computadora cuántica, es urgente el desarrollo de este algoritmo porque también se estima que la adopción del mismo tardará 1 década o más. El mismo NIST en la página de su proyecto “NIST Post-Quantum Cryptography Standardization Process”, lanzado en 2016, expresa en su trasfondo: “Historically, it has taken almost two decades to deploy our modern public key cryptography infrastructure”.

Dicho proyecto resulta sumamente interesante, en los últimos cinco años han pasado por 3 etapas de selección de propuestas de métodos y algoritmos capaces de resistir el inmenso poder computacional de las computadoras

cuánticas, actualmente se encuentran en la tercera etapa. A partir de estas etapas han publicado 3 reportes de estado.

El primer reporte de estado describe la situación en la que se encuentra la criptografía, haciendo hincapié en la capacidad que tienen las computadoras cuánticas de inutilizar los mecanismos utilizados hoy en día.

Es del NISTIR 8105 (2016) que se extrajo la información contenida en la siguiente tabla, la cual refleja el impacto de la computación cuántica en los algoritmos criptográficos actuales:

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

"Impact of Quantum Computing on Common Cryptographic Algorithms" (p.2)

Las funcionalidades que le interesan al NIST son: encriptación de clave pública, firma digital y algoritmos de intercambio de claves, y pretenden seleccionar al menos uno de cada funcionalidad para su estandarización.

Como resultado de la primera etapa se publicó el reporte NISTIR 8240, donde se informa que de las 82 propuestas originales, solo 69 cumplían con los requisitos mínimos para ingresar a la primera etapa, y que en esta, únicamente 26 propuestas fueron aprobadas para la segunda etapa. Esas 26 propuestas pueden ser divididas en dos grupos, 17 candidatas a algoritmos de encriptación de clave pública y algoritmos de establecimiento de claves, y 9 candidatos a firmas digitales.

Para esta etapa se tuvieron en cuenta 3 aspectos de evaluación:

1. Seguridad:

   Este es el aspecto más importante. El algoritmo elegido debe poder usarse en una gran variedad de protocolos.

2. Costo y performance:

   Segundo aspecto más importante. El tamaño de la clave pública, el texto cifrado, las firmas, la eficiencia computacional de la generación de la clave y la probabilidad de errores de descifrado son algunas de las características que se tuvieron en cuenta para la evaluación de este aspecto.

3. Características del algoritmo y la implementación:

   Buscan simpleza, elegancia, flexibilidad, eficiencia y paralelismo.

Tras la segunda etapa NIST publicó el reporte NISTIR 8309. Donde se realizaron revisiones más rigurosas de los aspectos que analizados en la etapa anterior.

La fase culminó con la selección de 7 algoritmos “finalistas” que luego pasarían a la tercera etapa de evaluación, que actualmente se está llevando a cabo. Además de estos finalistas, seleccionaron 8 “alternativas” que seguirán siendo evaluadas, pero que podrían ser elegidas como parte del primer estándar de encriptación post-cuántico, a pesar de que actualmente están inmaduros o aplican a situaciones muy específicas.

Algoritmos finalistas de encriptación de clave pública / KEMs:

- Classic McEliece: Es inusual, su clave pública es muy larga, pero los textos cifrados son más pequeños que los de todos los competidores. Esto no es bueno para el uso con los protocolos de internet actuales.
- CRYSTALS-KYBER: Es un algoritmo lattice based. Su seguridad está basada en la complejidad del problema de Module Learning With Errors (MLWE). El esquema tiene excelente performance para la mayoría de aplicaciones y NIST lo ve como uno de los finalistas más prometedores. Además, comparte un marco de trabajo con CRYSTALS-DILITHIUM, un esquema de firmas finalista.
- NTRU: Es otro algoritmo Lattice-based. No está el nivel de performance de KYBER o SABER porque tiene un esquema de generación de clave más lento, pero aun así resulta prometedor.
- SABER: Su seguridad se basa en Module Learning With Rounding (MLWR), una variante de MLWE. También es lattice based. Tiene una

performance excelente y sería apropiado para aplicaciones de uso general inmediatamente. Es una de las propuestas más prometedoras.

Algoritmos finalistas de firma digital:

- CRYSTALS-DILITHIUM: Su seguridad depende de los problemas MLWE y Module Short Integer Solutions (MSIS). Es un algoritmo lattice based. En general, posee una performance fuerte y balanceada en términos de tamaños de clave y firmas. Posee eficientes algoritmos de generación de claves, firmado y verificación. La implementación del algoritmo es sencilla. Sin embargo, tiene el nivel de seguridad más bajo entre todas las propuestas presentadas.
- FALCON: Utiliza el paradigma “hash and sign”, su algoritmo tambien es lattice based. Su seguridad está basada en la dificultad de los problemas Short Integer Solution (SIS). Su implementación es más compleja que la de DILITHIUM, pero ofrece tamaños de clave pública y tamaños de firmas más pequeños. Es eficiente en la firma y verificación, pero la generación de claves es más lenta. FALCON fácilmente puede ser usado en protocolos existentes y presenta una buena performance en general.
- Rainbow: Esquema de firmado multivariable basado en el esquema de firmados Unbalanced Oil-Vinegar (UOV). Ofrece un firmado rápido y verificación con firmas muy cortas, pero tiene llaves públicas muy largas. Debido a esto, no es un método apropiado para reemplazar los algoritmos de propósito general usados hoy en día.

Las alternativas que tomaron son 5 algoritmos de criptografía de clave pública (BIKE, FrodoKEM, HQC, NTRU Prime y SIKE) y 3 algoritmos de firma digital (GeMSS, Picnic y SPHINCS+).

A pesar de que todas las propuestas que pasaron a la tercera etapa son muy buenas, todas tienen defectos en alguna de las 5 categorías de seguridad que definió el NIST, además de aquellos defectos detallados anteriormente. Se espera que estos sean corregidos durante la tercera etapa o tras su selección como el nuevo estándar de encriptación.

El formato del proceso de estandarización originalmente se pensó como una competencia entre los investigadores, pero resultó ser uno bastante

cooperativo, donde muchos investigadores colaboran en distintas propuestas o en donde los investigadores intercambian nuevos descubrimientos entre sí.

No obstante, los mismos investigadores han expresado su frustración con respecto al avance del proceso. Los mismos piensan que el proyecto avanza muy rápido y esto desembocará en errores o en falta de innovación. En palabras de un encuestado, citado en "How the United States Is Developing Post-Quantum Cryptography": "NIST should not be aiming to conclude the process and have standards written by 2022 [...] This is simply too fast to get proper answers... Much more research is needed."

Otra persona encuestada en el mismo artículo expresa: "NIST should hold off creating any standard before 2025 and fund research efforts to look at all the candidates until that time,[...in order] to give researchers a chance to innovate."

Conclusión:

A pesar de que en la actualidad las computadoras cuánticas no representan una amenaza para los estándares de encriptación actuales, aquellos que se dedican a investigar cuándo y de qué forma estas nuevas computadoras harán obsoletos los estándares, descubren nuevos métodos o propiedades que acortan la “fecha de caducidad” de estos estándares.

Durante la lectura del ensayo se fue proporcionando evidencia de estos avances y de la amenaza que representa la computación cuántica para la criptografía en el futuro. A lo largo del ensayo se defendió la urgencia de empezar a buscar un nuevo algoritmo, un nuevo estándar, para que cuando llegue el momento en que la computación cuántica sea algo accesible o distribuido a gran escala, las computadoras estén preparadas para contrarrestar la superioridad computacional de aquellas que sean cuánticas.

En palabras de Dustin Moody, citado en “NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat”: “So if and when someone does build a large-scale quantum computer, we want to have algorithms in place that it can't crack”.

El proceso de estandarización del NIST es un gran paso para conseguir un algoritmo que nos permita resistir la computación cuántica, a pesar de que las propuestas que están siendo analizadas en la tercera etapa aún están madurando. Se espera que lo hagan con el tiempo, pero definir una base de la cual empezar es crucial para el desarrollo del algoritmo o algoritmos.

Referencia bibliográfica:

Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2020, July 22). Status report on the second round of the NIST Post-Quantum cryptography standardization process. NIST. https://csrc.nist.gov/publications/detail/nistir/8309/final

Amara, M., Siad A., "Elliptic Curve Cryptography and its applications," International Workshop on Systems, Signal Processing and their Applications, WOSSPA, 2011, pp. 247-250, doi: 10.1109/WOSSPA.2011.5931464.

Boutin, C. (2018a, January 8). NIST asks public to help Future-Proof electronic information. NIST. https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information

Boutin, C. (2018b, January 8). NIST kicks off effort to defend encrypted data from quantum computer threat. NIST. https://www.nist.gov/news-events/news/2016/04/nist-kicks-effort-defend-encrypted-data-quantum-computer-threat

Boutin, C. (2020, July 22). NIST's Post-Quantum Cryptography Program Enters 'Selection Round.' NIST. https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round

Cho, A. (2020, September 16). IBM promises 1000-qubit quantum computer—a milestone—by 2023. Science | AAAS. https://www.sciencemag.org/news/2020/09/ibm-promises-1000-qubit-quantum-computer-milestone-2023

Hsu, J. (2019, September 6). How the united states is developing Post-Quantum cryptography. IEEE Spectrum: Technology, Engineering, and Science News. https://spectrum.ieee.org/tech-talk/telecom/security/how-the-us-is-preparing-for-quantum-computings-threat-to-end-secrecy

Hsu, J. (2020, October 22). Intel creating cryptographic codes that quantum computers can't crack. IEEE Spectrum: Technology, Engineering, and Science News. https://spectrum.ieee.org/tech-talk/computing/hardware/how-to-protect-the-internet-of-things-in-the-quantum-computing-era

Moore, S. K. (2019, February 20). Circuit secures the IoT against quantum attack. IEEE Spectrum: Technology, Engineering, and Science News. https://spectrum.ieee.org/tech-talk/computing/embedded-systems/circuit-secures-the-iot-against-quantum-attack

National Institute of Standards and Technology (NIST). (2016a, April). Report on post-quantum cryptography (No. 8105). https://doi.org/10.6028/NIST.IR.8105

National Institute of Standards and Technology (NIST). (2016b, December 20). Announcing request for nominations for Public-Key Post-Quantum cryptographic algorithms. NIST. https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms

National Institute of Standards and Technology (NIST). (2019, January). Status report on the first round of the NIST Post-Quantum cryptography standardization process (No. 8240). https://doi.org/10.6028/NIST.IR.8240

National Institute of Standards and Technology (NIST). (2020, July). Status report on the second round of the NIST Post-Quantum cryptography standardization process (No. 8309). https://doi.org/10.6028/NIST.IR.8309

Nordrum, A. (2016, March 3). Quantum computer comes closer to cracking RSA encryption. IEEE Spectrum: Technology, Engineering, and Science News. https://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment

Ohlheiser, A., Basu, T., Ferguson, C., & Guo, E. (2020, April 2). How a quantum computer could break 2048-bit RSA encryption in 8 hours. MIT Technology Review.

https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/

Simonite, T. (2020, April 2). Securing today's data against tomorrow's quantum computers. MIT Technology Review. https://www.technologyreview.com/2015/08/03/110124/securing-todays-data-against-tomorrows-quantum-computers/