Estado Actual de los Algoritmos Post-Cuánticos

Kevin A. Delgado Vargas[1], Gina Gallegos-García[2]
Instituto Politécnico Nacional
Escuela Superior de Ingeniería Mecánica y Eléctrica. Unidad Culhuacan
Sección de Estudios de Posgrado e Investigación
Av. Santa Ana 1000, San Francisco Culhuacan, Culhuacan, 04430, Ciudad de México.
kdelgadov1200@alumno.ipn.mx[1], ggallegosg@ipn.mx[2]

***Resumen*—Desde los inicios de la criptografía, su objetivo siempre ha sido preservar diferentes servicios de seguridad de la información. Sin embargo, dado que el poder de cómputo ha avanzado a pasos agigantados, algunos de los algoritmos que actualmente preservan los servicios de confidencialidad, autenticación, integridad y no repudio, han sido rotos y como consecuencia, los sistemas de la industria que los utilizan, también. Con computadoras cada vez más potentes, como las cuánticas, la criptografía se ha visto amenazada cada vez más y más, es por ello que la comunidad científica ha hecho énfasis en algoritmos que sean capaces de resistir ataques provenientes de cualquier tipo de computadora, haciendo un llamado a una estandarización de nuevos algoritmos llamados algoritmos post-cuánticos.**

***Index Terms*—Algoritmos criptográficos, criptografía post-cuántica, estandarización de algoritmos, primitivas criptográficas, servicios de seguridad**

I. Introducción

A lo largo de los tiempos, la criptografía ha jugado un papel muy importante, debido a que desde sus inicios se ha enfocado en estudiar las técnicas matemáticas relacionadas a los aspectos de la seguridad de la información, tales como, confidencialidad, integridad de los datos, autenticación de entidad y no repudio [1].

Históricamente hablando, esta ciencia se divide en clásica, moderna, cuántica y post-cuántica.

La criptografía clásica tuvo sus inicios aproximadamente en el año 1900, antes de Cristo, con el primer registro de la escritura egipcia [2]. En aquel entonces se hacía uso de sustituciones y permutaciones para poder transformar la información ante terceras entidades no deseadas.

Con la criptografía moderna, alrededor de los años 70's, se introducen dos formas distintas de preservar los servicios de seguridad de la información, ya que en ella se utilizan algoritmos criptográficos de llave simétrica y de llave asimétrica [1].

A la par, en esa misma década, es que se tienen las primeras ideas relacionadas con la criptografía cuántica, las cuales basan su seguridad en los pricipios de la mecánica cuántica, como el principio de la incertidumbre o el principio de la superposición [5], con lo que este tipo de criptografía empezó a representar una amenaza inminente para la gran mayoria de los algoritmos que correspondientes a la criptografía moderna. Es decir, aquellos algoritmos que se creen seguros ante los ataques efectuados por computadoras clásicas. Debido a ello, es que en los años 90's es que surge la criptografía post-cuántica, que trae consigo algoritmos criptográficos que estan diseñados para resistir ataques efectuados por computadoras tanto clásicas como cuánticas.

Con base en lo anterior, en este trabajo se presenta una breve revisión del estado actual que guardan los algoritmos post-cuánticos, para tal fin el resto del artículo se organiza de la siguiente manera, en la Sección II, se presenta una definición de las primitivas criptográficas, y con base en la clasificación de los algoritmos criptográficos, se asocian los servicios de seguridad que pueden preservarse con ambos. La Sección III, especifica lo que es la criptografía post-cuántica, así como los tipos de algoritmos en los que ésta se clasifica. La Sección IV presenta la lista de organizaciones que se han enfocado en el trabajo de la estandarización de los mismos, enfocándose en el nivel de seguridad que ellos deben tener. En la Sección V se listan algunos de los retos que aún presenta el uso de algoritmos post-cuánticos. Por último, se muestran las conclusiones y se listan las referencias.

II. Primitivas y Clasificación de Algoritmos Criptográficos

Criptográficamente hablando, las primitivas criptográficas son herramientas utilizadas para preservar los servicios de seguridad antes mencionados. Estas pueden ser evaluadas con respecto a cinco criterios, siendo estos los que se enlistan a continuación:

1. Nivel de seguridad: Este normalmente es difícil de cuantificar. Sin embargo, el nivel de seguridad se da en términos del número de operaciones requeridas para derrotar un objetivo previsto.
2. Funcionalidad: Las primitivas deben combinarse para preservar un servicio de seguridad. La determinación de la mejor primitiva para preservar un servicio está determinada por la propiedad de la misma.
3. Métodos de operación: Las primitivas, dependiendo de la manera en la que se empleen y de las entradas que tengan, van a obtener características diferentes; por lo tanto, una misma primitiva puede presentar una funcionalidad diferente dependiendo de su modo de operación o su uso.
4. Desempeño: Este criterio hace referencia a la eficiencia de una primitiva en un modo particular de operación.
5. Facilidad de implementación: Implica la complejidad de implementar una primitiva en una instalación práctica,

ISSN: 3061-8991

ya sea un entorno de software o hardware [1].

De manera general estas herramientas abstractas se clasifican en: primitivas criptográficas sin llave, primitivas con llave, de hash y de números pseudoaleatorios. Esta clasificación está vinculada con los algoritmos criptográficos que permiten que dichas abstracciones materialicen los distintos servicios de seguridad de la información. De ahí, que con base en la cantidad de llaves que se utilizan, los algoritmos pueden clasificarse en algoritmos de llave simétrica y algoritmos de llave asimétrica. Los algoritmos criptográficos simétricos utilizan una sola llave para hacer/deshacer las transformaciones hechas a la información.
Estos, a su vez y considerando la forma en como manipulan la información, se dividen en algoritmos de bloque y algoritmos de flujo. Los primeros manipulan la información en bloques de longitud k, siendo k definido por el algoritmo en específico. Los de flujo, manipulan la información con correspondencias bit a bit sobre el flujo mismo. Por otro lado, los algoritmos de llave asimétrica utilizan un par de llaves para llevar a cabo las transformaciones a la información.
Ambos son utilizados en computadoras con arquitectura Von Neumann y Harvard y han ido evolucionando a tal grado que con el advenimiento de computadoras cada vez más potentes y con el aumento de su uso para procesar y transmitir información rápidamente, se presentan nuevas exigencias frente a los algoritmos criptográficos, surgiendo la necesidad de utilizar algoritmos capaces de resistir ataques de computadoras cuánticas. Lo anterior, aunado al rompimiento de algoritmos simétricos y asimétricos, ha hecho que la comunidad científica se enfoque en un reciente conjunto de algoritmos llamados, post-cuánticos.

III. Rompimiento de Algoritmos Modernos

En los años 90's los algoritmos criptográficos modernos empezaron a verse afectados por la computación cuántica, y que el matemático Peter Shor, desarrolló un algoritmo para encontrar factores de un número de una forma eficiente. Su implementación pudo llevarse a cabo de manera clásica o utilizando circuitos cuánticos [3]. Este algoritmo basa su potencia en determinar el periodo de una función, para que de esta manera se puedan encontrar factores primos para un entero. De ahí que un ordenador cuántico con un número suficiente de qubits que ejecuten el algoritmo de Shor, podría utilizarse para romper algoritmos modernos de llave asimétrica.
Por otro lado, en 1997, K. L. Grover, publicó el llamado Algoritmo de Grover [4], siendo desde aquel entonces, una amenaza para algunos de los algoritmos criptográficos modernos, ya que este reduce efectivamente a la mitad los niveles de seguridad. Esto, ya que para el caso del algoritmo simétrico AES-256, este se renderiza igual que AES-128 ejecutando el algoritmo de Grover en un ordenador cuántico suficientemente potente.
Por lo tanto, los algoritmos post-cuánticos no necesitan cambiar significativamente de la criptografía simétrica moderna, siguiendo obteniendo los niveles de seguridad actuales.

IV. Algoritmos Criptográficos Post-cuánticos

Dependiendo de la funcionalidad y del problema en el que basan su seguridad, los algoritmos post-cuánticos se clasifican en 4 tipos, algoritmos basados en código, algoritmos basados en Hash, basados en rejillas (Lattices) y algoritmos basados en polinomios cuadráticos multivariables.

IV-A. Algoritmos basados en Código

Son aquellos que usan, como elemento fundamental, un código de corrección de errores C. Este elemento fundamental puede consistir en añadir un error a una palabra de C o en calcular un síndrome respecto a una matriz de comprobación de paridad de C. Uno de los primeros algoritmos basados en código, es el algoritmo de McEliece [6], base de los algoritmos que actualmente están siendo diseñados.

IV-B. Algoritmos basados en Hash

La seguridad de los esquemas de firma digital que se usan en la práctica actual, a menudo se basan en la dificultad de factorizar enteros grandes y calcular logaritmos discretos. Las firmas digitales han llegado a ser un elemento clave para preservar autenticidad, integridad y no repudio de los datos. Los algoritmos de firma digital usados en la práctica hoy en día, no son inmunes a ataques efectuados por computadoras cuánticas, dado que su seguridad recae en la dificultad de factorizar enteros grandes y calcular logaritmos discretos. De ahí, que los algoritmos de firma basados en hash y que resisten ataques hechos por computadoras cuánticas, utilizan una función hash, al igual que las demás, pero con la diferencia de que su seguridad recae en la resistencia a colisiones de la propia función hash. De hecho, la existencia de funciones hash resistentes a colisiones se puede ver como un requisito mínimo para la existencia de un algoritmo de firma post-cuántico, esto dado que los algoritmos de firma mapean documentos de longitud arbitraria hacia firmas digitales de longitud fija, lo que muestra que el algoritmo de firma es en sí, una función hash.
Los primeros autores en presentar este tipo de construcciones fueron Lamport [7], siendo mejorados por Merkle [8] y Winternitz, donde la propuesta una sola via de Winternitz es una generalización de la propuesta de una sola vía de Merkle [9].

IV-C. Algoritmos basados en Rejillas (Lattices)

Las construcciones criptográficas basadas en rejillas son una gran promesa como parte de los algoritmos post-cuánticos. Muchos de ellos son bastante eficientes, y algunos otros compiten con las alternativas más conocidas, son simples para implementar y por supuesto, se creen seguros en contra de computadoras cuánticas. En términos de seguridad, las construcciones criptográficas basadas en rejillas, se dividen en dos tipos, el primer tipo incluye propuestas clásicas que son típicamente eficientes, pero carecen de pruebas de seguridad. El segundo tipo ofrece garantías de seguridad demostrable para los problemas de lattices del $peorcaso$. Es decir, que el rompimiento de la construcción criptográfica, inclusive con

probabilidad no-despreciable, es al menos tan difícil como resolver algunos problemas de las rejillas en el $peorcaso$. En otras palabras, romper la construcción criptográfica implica un algoritmo eficiente para resolver cualquier instancia de algún problema de rejilla en cuestión. La primera propuesta de algoritmo basado en rejillas fue hecho por Hoffstein, Pipher y Silverman en los años 90's, lo llamaron NTRU [10] y tiene la característica de trabajar con llaves más pequeñas que las que se tiene en el algoritmo McEliece [6].

IV-D. Algoritmos basada en Polinomios Cuadráticos Multivariables

También conocida como criptografía basada en polinomios multivariable, es el término general para definir aquellos algoritmos que trabajan con polinomios de multiples variables sobre un campo finito como su elemento público. De ahí que, por ejemplo, si los polinomios tienen grado dos, entonces se está hablando de polinomios cuadrados multivariables. Su seguridad descansa en la $dificultad - NP$ del problema para resolver ecuaciones no lineales sobre campos finitos. Esta familia, se considera como una de las familias más grandes de llave asimétrica que pudieran resistir poderosos ataques efectuados por computadoras cuánticas. Los algoritmos correspondientes a esta clasificación permiten un rápido cifrado y descifrado de datos así como una veloz generación y verificación de firmas. El primer registro de algoritmos multivariables fue el Imaí-Matsumoto en el año 1988 [11].

V. Estandarización de algoritmos post-cuánticos

Algunos cuerpos de estandarización han reconocido la urgencia de cambiar y utilizar algoritmos que sean seguros ante ataques hechos por computadoras cuánticas. Esto es muy importante dado que muchas aplicaciones criptográficas requieren que todas las entidades participantes utilicen el mismo algoritmo, de ahí que la estandarización de algoritmos es un pre-requisito para el amplio uso de los mismos.

De hecho, algunos estándares de-facto son tomados por distintos cuerpos de estandarización, pero los procesos formales de estandarización son ampliamente vistos como una forma de reducir riesgos.

El grupo de trabajo de ingeniería en internet, IETF por sus siglas en ingles [12], y su rama de investigación IRTF se encuentran como líderes terminando la estandarización de algoritmos de firma basados en hash. Algunas otras organizaciones que están interesados en la estandarización de la criptografía post-cuántica son la ETSI [13], con su grupo de trabajo llamado "quantum-safe". De igual forma, ISO [14] con SC27 WG2 y OASIS [15] con el estándar de KMIP. Por su parte el Instituto Nacional de Estándares y Tecnología (por sus siglas en ingles NIST) en el año 2017 empezó un proceso de solicitud, evaluación y estandarización de uno o más algoritmos de asimétricos, resistentes a ataques cuánticos. Este proceso será de múltiples rondas de evaluación y durará aproximadamente de 3 a 5 años [16]. Cabe destacar que en la primera ronda de evaluación se recibieron alrededor de 70 propuestas, las cuales tuvieron que cumplir con los requisitos mínimos de aceptabilidad, presentación y de evaluación para los algoritmos candidatos. De los candidatos recibidos en esta ronda de evaluación, al menos 5 fueron descartadas debido a las críticas realizadas por la comunidad científica.

V-A. Niveles de seguridad aplicables a los algoritmos post-cuánticos

En el año 2001 el NIST emitió el Estándar Federales de Procesamiento de la Información 140-2 (FIPS por sus siglas en Inglés) el cual se enfoca en detallar la acreditación de módulos criptográficos desde el punto de vista de componentes de software y desde el punto de vista de hardware [17]. Este estándar considera, entre otras cosas, los 4 niveles de seguridad a los que se deben ajustar todos los módulos criptográficos y son los niveles en los que basan su seguridad, aquellos algoritmos post-cuánticos que están siendo estandarizados, actualmente, por el NIST. Estos son descritos a continuación:

Nivel 1: El nivel más bajo de seguridad, no especifica un mecanismo de seguridad físico, pero si impone requisitos de seguridad básicos. Es utilizado para componentes de software y firmware de un módulo criptográfico.

Nivel 2: Este nivel de seguridad requiere, como mínimo, la autenticación basada en roles en la que un módulo criptográfico autentica la autorización de un operador basado en el cargo del usuario.

Nivel 3: En este nivel de seguridad, se añade una resistencia a la intrusión física. Así mismo incluye protección criptográfica eficaz y administración de llaves, además de la autenticación basada en identidad y separación física o lógica.

Nivel 4: El máximo nivel de seguridad incluye protección avanzada contra intrusos, además de que este puede funcionar en entornos que no estén protegidos físicamente.

V-B. Algoritmos post-cuánticos clasificados por el Instituto Nacional de Estándares y Tecnología

Las propuestas de algoritmos recibidas por el NIST se basan en la clasificación de los cuatro tipos que se mencionaron en la Sección III, siendo estos: algoritmos basados en códigos, algoritmos basados en hash, algoritmos basados en rejillas y basados en criptografía multivariable. Cabe destacar que varias de las propuestas recibidas se enfocan en preservar diferentes servicios, esto con base en sus respectivas primitivas criptográficas. Es decir, a la fecha se está trabajando en la estandarización de algoritmos post-cuánticos de llave publica para la primitiva de cifrado y firma, así como en algoritmos de intercambio de llaves. Ejemplo de ello, son los algoritmos post-cuánticos que basan su funcionalidad en rejillas y en polinomios multivariables, que tienen propuestas para cifrado y firma.

VI. Retos existentes dentro de los algoritmos post-cuanticos

De todas las propuestas antes mencionadas enviadas al NIST, se puede hacer una clasificación de los algoritmos dependiendo de su tipo de criptografía.

En términos generales una de las preocupaciones que se tiene con los algoritmos post-cuánticos, es el uso de ellos dentro de los sistemas de la industria, de ahí los restos y áreas de oportunidad se citan a continuación:

- Tamaño de llaves. En muchos de los casos, los algoritmos hacen uso de llaves muy grandes, esto genera que la velocidad de procesamiento se vea reducida significativamente.
- Firmas cortas. Si el tamaño de las llaves disminuye, entonces el tamaño de las firmas también lo hará, generando una velocidad de firmado más rápida.
- Velocidad en cifrado, firma y verificación. Existe una relación entre la velocidad y los tamaños de firmas y de llaves, puesto que mientras más grande sean estos, la velocidad disminuye.
- Flexibilidad y adaptación entre distintos algoritmos. El proceso de estandarización no especifica que los algoritmos deben trabajar solos, es decir, que no pueden trabajar en conjunto con algún otro algoritmo. Algunos de los algoritmos post-cuánticos son capaces de trabajar mano a mano con otros algoritmos, por lo cual generan mayor protección, esto les da una ventaja sobre los demás competidores.
- Utilizar como base algoritmos cuya resistencia este comprobada ante ataques cuánticos. Existen algunos algoritmos que se creen seguros ante ataques de computadoras cuánticas, pero la mayoría de los algoritmos recibidos por el NIST, no hacen uso de ellos por lo tanto su resistencia ante los ataques cuánticos no está comprobado.
- Eficiencia de memoria. La ventaja que tienen estos algoritmos es el poco espacio de memoria que requieren para funcionar, pero aún podrían utilizar menos espacio si se reducen los tamaños de firmas y llaves.
- Facilidad de implementación. Los algoritmos postcuanticos deben poder ser implementados de una manera sencilla en cualquier tipo de sistema dentro de la industria que así lo requiera, entre los que se destacan sistemas embebidos con muy pocos bits o computadoras clásicas.

Conclusiones

La revisión y el análisis de las referencias consultadas dejaron ver que aún queda mucha tarea por hacer y por corregir, esto, dado que una de las mayores preocupaciones reside en la forma en cómo se comportarían los algoritmos criptográficos post-cuánticos dentro de la industria, muestra de ello es la notoria participación de la comunidad científica tanto para diseñar este tipo de algoritmos como para estandarizarlos, lo cual conlleva a afirmar que no es solo una organización ni un solo grupo científico, sino, son varios los grupos de trabajo que alrededor del mundo, se encuentran llevando a cabo estas tareas, muestra de ello se ve con el NIST.

Parámetros como longitud de llaves, velocidad de cómputo y eficiencia, aún siguen siendo revisados y estudiados con mayor detalle. Esto, con la finalidad de mejorar aún más el comportamiento que tendrían estos algoritmos de manera conjunta con la industria.

Posibles trabajos a futuro consistirían en analizar la viabilidad del uso de algoritmos post-cuánticos dentro de propuestas de solución que interactúen de manera directa con la industria. Lo anterior, en escenarios industriales que hagan uso de diferentes redes de sensores, sistemas embebidos, aplicaciones móviles, bibliotecas criptográficas y lenguajes de programación, por mencionar algunos.

Agradecimientos

Los autores agradecen al Instituto Politécnico Nacional por el apoyo otorgado para la realización de este trabajo, a través de los proyectos SIP 1917 y 20180505.

Referencias

[1] A. Menezes, P. van Oorsschot, y S. Vanstone, *Handbook of Applied Cryptography*, primera edición, CRC Press, 1996.
[2] Caballero, P. (2002), *Introducción a la Criptografía.* Ed. Ra-Ma. Madrid
[3] Shor, P., *Algorithms for quantum computation: Discrete logarithms and Factoring.*, Proceedings 35th Annual Symposium on Foundations of Computer Science (1994), 124-134.
[4] K.L. Grover, *Quantum mechanicshelpsin searchingfora needlein a haystack*, Phys. Rev. Lett.79 (1997), 325-328.
[5] Chen, Lily; Jordan, Yi-Kai Liu; Moody, Dustin; Peralta, Rene; Smith-Tone, Daniel (April 2016). *Report on Post-Quantum Cryptography*
[6] McEliece y R. J. *A public-key cryptosystem based on algebraic coding theory* 1978.
[7] Lamport, L., *Constructing digital signatures from a one way function.* Technical Report, 1979.
[8] Merkle, R.C., *"A certified digital signature." in Proccedings on Advances in Cryptology* - CRYPTO '89 Proceedings,Springer-Verlag New York, Inc., 1989.
[9] Anders Fog, Bunzel, (2015). *Hash Based Digital Signature Schemes*.
[10] Hoffstein J., Pipher J.y Silverman J., *NTRU – A ring based public key cryptosystem*, LNCS 1423, 1998.
[11] Tsutomu Matsumoto y Hideki Imai, *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*, Springer, Berlin, 1988.
[12] IETF, 2018. [Online]. Available: https://www.ietf.org/. [Accessed: 07- Sep- 2018].
[13] S. Dahmen-Lhuissier, *"Quantum-Safe Cryptography"*, ETSI, 2018. [Online]. Available: https://www.etsi.org/ [Accessed: 08- Sep- 2018].
[14] "ISO - International Organization for Standardization", Iso.org, 2018. [Online]. Available: https://www.iso.org/home.html. [Accessed: 07- Sep- 2018].
[15] OASIS — Advancing open standards for the information society, Oasis-open.org, 2018. [Online]. Available: https://www.oasis-open.org/. [Accessed: 07- Sep- 2018].
[16] "Post-Quantum Cryptography Standardization — NIST". [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
[17] NIST, *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*, 2001.