Ventajas y retos del uso de la criptografía post-cuántica al preservar el servicio de autenticación en dispositivos con recursos limitados

Alfonso F. De Abiega-L'Eglisse[1], Kevin A. Delgado-Vargas[2], Gina Gallegos-García[3], Mariko Nakano-Miyatake[4], Ponciano J. Escamilla-Ambrosio[5]
[1−5] Instituto Politécnico Nacional. [1,4] Escuela Superior de Ingeniería Mecánica y Eléctrica. Unidad Culhuacan. Sección de Estudios de Posgrado e Investigación. Av. Santa Ana 1000, San Francisco Culhuacan, Coyoacan, 04430, Ciudad de México. CDMX.
[2,3,5] Centro de Investigación en Computación, Laboratorio de Ciberseguridad. Av. Juan de Dios Bátiz S/N, Nueva Industrial Vallejo, 07738 Ciudad de México. CDMX.
alfonso.deabiega@gmail.com[1], kdelgadov1200@alumno.ipn.mx[2], ggallegosg@ipn.mx[3], mnakano@ipn.mx[4], pescamilla@cic.ipn.mx[5]

***Resumen*—El uso de las computadoras y de los sistemas de comunicación trajo consigo, desde los años 60's, una demanda por parte del sector privado de contar con medios para proteger la información que se transmitía digitalmente, de forma tal que se pudieran preservar diferentes servicios de seguridad antes, durante y después de su envío y transmisión desde una entidad emisora hasta una entidad receptora. A la fecha, dicha demanda no solo se tiene por parte del sector privado, sino es una necesidad que tiene la sociedad y la industria, al utilizar dispositivos con características diversas día a día para tal fin. Específicamente hablando del servicio de autenticación, la criptografía y la biometría han unido esfuerzos tanto para identificar a las entidades que se comunican dentro de un sistema, como para mantener auténtica la información que viaja entre ellas. Sin embargo, la unión de estas vertientes de investigación trae consigo ventajas y retos cuando se utilizan para diseñar propuestas de solución en dispositivos con recurso limitado. Con base en ello, en este trabajo se presenta un panorama breve de las ventajas y los retos que mantienen los dispositivos de recurso limitado que se utilizan por la biometría, al combinarla con la criptografía post-cuántica. Esto, dentro de escenarios en donde se requiera preservar el servicio de autenticación.**

***Index Terms*—Autenticación, criptografía post-cuántica, dispositivos de recurso limitado, sensores, sistemas empotrados.**

I. Introducción

Autenticación es un servicio relacionado con la identicación, que se aplica tanto a la entidad emisora y a la entidad receptora, como a la información que se transmite entre ellos, de tal forma que las dos entidades se identifican entre sí, del mismo modo que la información entregada a través de un canal de comunicación.

El servicio de autenticación se subdivide en dos clases principales: autenticación de entidad y autenticación de origen de datos, esta última proporciona implícitamente la integridad de los datos. Es decir, si se modifica un mensaje, la fuente podría haber cambiado.

Existen dos líneas de investigación que preservan el servicio de autenticación, la criptografía y la biometría. Cada una de ellas tiene tareas específicas y problemáticas que resuelven de manera independiente, incluso desde hace algunos años han unido esfuerzos para el diseño de propuestas de solución. Con base en ello, en este trabajo se hablará de las ventajas y retos que guarda cada una de ellas, cuando preservan el servicio de autenticación dentro de un escenario con dispositivos de recursos limitados.

II. Autenticación desde un punto de vista criptográfico

Las primitivas criptográficas pueden verse como herramientas abstractas que ayudan a preservar cuatro servicios de seguridad en la información: confidencialidad, integridad de los datos, autenticación y no repudio. Éstas se dividen en aquellas que no hacen uso de una llave criptográfica, aquellas que hacen uso de llave simétrica y aquellas que hacen uso de llave asimétrica. Las firmas digitales son las primitivas criptográficas de llave asimétrica más conocidas para preservar la integridad de los datos y la autenticación (de entidad y autenticación de origen de datos). Adicionalmente a éstas, también existen técnicas criptográficas que son diseñadas para permitir a una entidad (el verificador), asegurarse de que otra entidad (el demadante) es quién dice ser, de tal forma que es posible detectar la falsificación de identidad.

III. Evolución de la criptografía

Históricamente hablando, la criptografía puede clasificarse en: clásica, moderna, cuántica y postcuántica. Pero independientemente de esta clasificación, en la actualidad se define como una ciencia que ha jugado un papel muy importante al dedicar sus esfuerzos a preservar diferentes servicios de seguridad mediante el uso de secuencias algoritmicas definidas bajo un esquema.

Haciendo un breve recorrido por la historia de esta ciencia, se puede destacar que en los años 70's, en plena estandarización de los algoritmos pertenecientes a la criptografía moderna,

por parte del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) [1], es que se tienen las primeras ideas relacionadas con la criptografía cuántica. En los 80's es cuando se muestran las primeras publicaciones de nuevas ideas que basaban su seguridad en los pricipios de la mecánica cuántica, destacando el de la incertidumbre o el principio de la superposición. Dichos principios utilizan láseres para emitir información en un fotón, elemento constituyente de la luz, logrando conducir información a través de fibras ópticas. Lo anterior, para garantizar el servicio de confidencialidad de la información transmitida [2].

IV. La criptografía post-cuántica en dispositivos de recursos limitados

A la fecha, los algoritmos de Shor [3] y Grover [4], son capaces de comprometer algunos de los algoritmos utilizados desde la criptografía moderna hasta estos días. De ahí, que los esquemas criptográficos post-cuánticos surgen de la necesidad de proteger las diferentes propuestas de solución criptográficas, de ataques realizados por computadoras cuánticas a gran escala, ya que estas últimas son capaces de resolver los problemas matemáticos empleados por los esquemas criptográficos modernos de llave asimétrica. Es decir, la criptografía post-cuántica se define como aquella que tiene como objetivo construir esquemas de llave asimétrica que sean seguros inclusive en contra de computadoras cuánticas.

Es por ello que la comunidad científica ha puesto un especial énfasis en la criptografía post-cuántica, enfocando sus esfuerzos en el diseño de esquemas que se clasifican en: aquellos basados en reticulos, basados en ecuaciones de multiples variables, esquemas basados en isogeneas de curvas elípticas y en códigos. Todos ellos capaces de cumplir los requisitos del actual proceso de estandarización [1], prometiendo preservar los diferentes servicios de seguridad de la información, ante ataques efectuados inclusive desde computadoras cuánticas.

El reto al que se enfrentan estos nuevos esquemas, al intentar sustituir los actuales esquemas modernos por los futuros esquemas estándar radica en el desconocimiento del comportamiento y desempeño de ellos, en los diferentes escenarios en donde se tienen entidades y dispositivos con características diversas, incluso con recursos limitados.

V. Clasificación de los dispositivos de recursos limitados

Los dispositivos de recursos limitados, se definen como elementos que combinan hardware y software para realizar tareas especificas con limitaciones de memoria (entre 128Kb y 2Mb aprox), poca potencia computacional (procesadores de 16 a 32 bits), ocasionalmente con pantallas de 97x54 pixeles) y que generalmente se alimentan de baterías [5]. Dadas sus características mínimas, este tipo de dispositivos por lo regular se utilizan en maquinas industriales, automóviles, cámaras, aplicaciones de hogar y equipo médico, por mencionar algunos. Éstos, se pueden ordenar por capacidad, que van desde aquellos que solo fueron diseñados para cumplir una tarea muy específica, como la medición de algún dato, hasta aquellos que tienen una interfaz de usuario.

Los dispositivos de recursos limitados se pueden clasificar en dos tipos: el primer tipo correponde a aquellos de entrada o lectura y el segundo corresponde a aquellos dispositivos de procesamiento.

V-A. Dispositivos de lectura

Los del primer tipo son aquellos que a partir de una señal analógica o mecánica, entregan una señal digital. Ejemplos de ellos son los sensores corporales o los sensores biométricos. De hecho, uno de los escenarios de aplicación en donde es posible observar este tipo de dispositivos es en los escenarios médicos, con las conocidas redes de sensores, puesto que permiten monitorizar el estatus de los pacientes a través de las Redes Inalámbricas de Área Corporal (WBAN, por su acrónimo en inglés) [6], [7]. Estas redes involucran distintos sensores que están interconectados entre sí, y colocados en el cuerpo humano. La Figura 1 muestra la representación gráfica de una WBAN.

El otro ejemplo antes citado, corresponde a los sensores

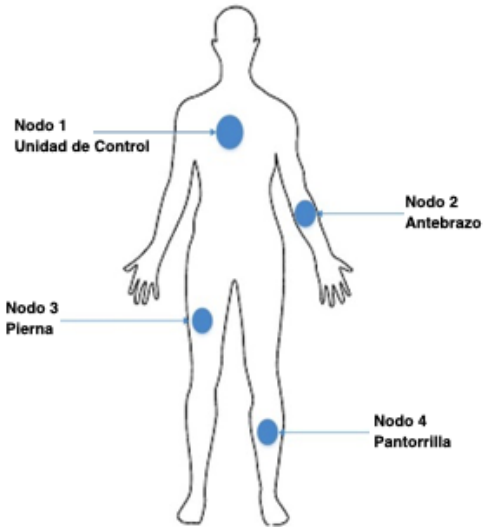

Figura 1. Distribución de sensores de lectura dentro de una Red Inalámbrica de Área Corporal

biométricos, definidos como aquellos dispositivos que transforman los rasgos biológicos, como el rostro, el iris o las huellas digitales; son escaneadas por medio de estos sensores y después de convertirlas en imagenes usando un convertidor analógico - digital de un individuo en señales eléctricas. Esta información digital de los datos biométricos son almacenados en memoria y utilizados para la verificación o autenticación de la identidad de una persona, conviertiéndose cada vez, en dispositivos importantes, útiles, efectivos, precisos y brindan seguridad. La Figura 2, muestra algunos de estos dispositivos biométricos. El escenario más reciente en donde se puede observar el uso de ellos es en la mayoría de los teléfonos inteligentes modernos, ya que incluyen al menos un sensor de huella digital para autenticar al usuario, mientras que los teléfonos

de gama alta proporcionan sensores biométricos adicionales como escáneres de iris y tecnología de reconocimineto facial.

Figura 2. Dispositivos de lectura de rasgos biológicos. Fuente: https://www.digitalavmagazine.com/2013/09/23/los-terminales-de-control-de-acceso-virdi-se-introducen-en-espana-de-la-mano-de-sti-card/

V-B. Dispositivos de procesamiento

El segundo tipo de dispositivos, son capaces de manejar todos los datos recibidos de los dispositivos de lectura o de otros de procesamiento.
Este tipo de dispositivos son diseñados para realizar una o algunas pocas funciones dedicadas, las cuales se obtienen a través de la programación, en lenguaje ensamblador, del microcontrolador o microprocesador incorporado sobre el mismo, o también, utilizando compiladores específicos o también se utilizan lenguajes como C o C++ [8]. En algunos casos, cuando el tiempo de respuesta no es un factor crítico, también, pueden usarse lenguajes Orientados a Objetos como JAVA.
Ejemplos de este tipo de dispositivos son mejor conocidos como sistemas embebidos o empotrados, como Arduino, Raspberry Pi, y BeagleBone, entre otros. Ellos son utilizados para cubrir necesidades específicas y la mayoría de sus componentes se encuentran incluidos en la placa base, utilizando un procesador relativamente pequeño y una memoria pequeña, como los que se observan en la Figura 3.

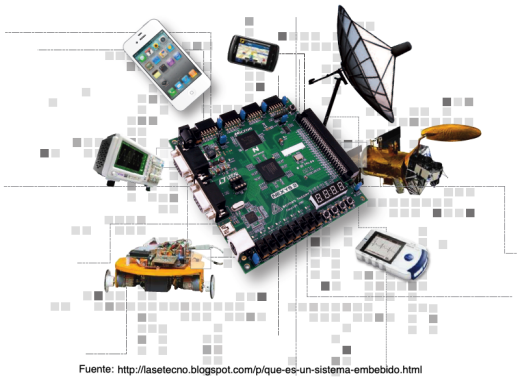

Figura 3. Dispositivos empotrados encargados del procesamiento de datos. Fuente: http://lasetecno.blogspot.com/p/que-es-un-sistema-embebido.html

VI. Identificación de ventajas y retos del uso de la criptografía post-cuántica en dispositivos con recursos limitados

Por lo regular, las propuestas de solución diseñadas para preservar un servicio de seguridad, como el servicio de autenticación, hacen uso de una combinación de dispositivos de lectura y procesamiento, quedando en una mezcla de dispositivos con características diversas y limitadas.
Específicamente hablando del servicio de autenticación, en los escenarios actuales, donde los dispositivos son cada vez más pequeños llegando a la restricción de tener recursos limitados, es que toma fuerza la importancia de que las entidades, que dicen estarse comunicando entre sí, son quienes dicen ser.
De hecho, los dispositivos de entrada tienen la ventaja de que pueden cumplir, de la manera mas óptima, con la función para la que fueron diseñados. Sin embargo, una de sus mayores desventajas es que estos dispositivos están “cerrados” por el fabricante, es decir que no se pueden reprogramar. Adicionalmente a esto, su calibración no es exacta, lo cual genera un margen de error. Uno de los retos asociados a este tipo de dispositivos, al momento de preservar el servicio de autenticación, es el diseñar el propio dispositivo de hardware criptográfico, creado a partir de la identificación de los requisitos que debe cumplir el dispositivo creado para la tarea que esté destinado a desarrollar.
Algunas de las carencias que se encuentran en los dispositivos de lectura, se compensan con los dispositivos de procesamiento, ya que estos se pueden programar y es posible almacenar y/o manejar los datos provenientes de los dispositivos de lectura. Es decir, éstos pueden tener tantos módulos de lectura como sean necesarios, así como una amplia gama de aplicaciones y propuestas de solución que de manera conjunta resuelvan problemas específicos.
Las diferentes propuestas de solución, enfocadas en preservar el servicio de autenticación, llegan a ser demasiado elaboradas, lo cual se ha llegado a solucionar haciendo uso de la criptografía de peso ligero, la cual demanda mínimamente el recurso del dispositivo. Un ejemplo de ello se puede observar dentro de las WBAN, ya que en este tipo de redes existen propuestas de solución que utilizan esquemas criptográficos de llave asimétrica para proveer el servicio de autenticación, con la característica de ser de peso ligero. Algunos otros hacen uso de algoritmos de curva elíptica, con la desventaja de que las soluciones que involucran el uso de la criptografía de curva elíptica consume aún más recursos, quedando un gran reto referente a la forma en cómo se comportarían los esquemas post-cuánticos dentro del escenario de las redes de sensores corporales.
Aunado a ello, otro reto existente reside en balancear la seguridad vs el desempeño y decidir qué vertiente de la criptografía post-cuántica debería considerarse para diseñar una propuesta de solución ecaminada a preservar el servicio de autenticación, ya que cada vertiente podría tener un comportamiento, velocidad de respuesta y uso de recurso diferente, cuando sea ejecutado en un dispositivo con las mis-

mas características. Esto, considerando que en los esquemas post-cuánticos, las claves son de una longitud considerable, generando que el nivel de seguridad que proporciona sea alto perdiendo velocidad de respuesta [9].
Además, hablando específicamente de la primitiva de firma y con base en la longitud de sus repectivas llaves, es evidente el tamaño de la firma digital que será obtenida. Ante esto, se deja ver como reto, el analizar si es posible que los algoritmos post-cuánticos, encargados de preservar el servicio de autenticación, pueden proveer el mismo nivel de seguridad que ofrecen los esquemas modernos Lo anterior, considerando el éxito que han tenido los esquemas criptográficos de peso ligero dentro de sensores de procesamiento con recursos limitados.

VII. Conclusiones

La importancia que tienen los diferentes servicios de seguridad radica en el escenario de aplicación en donde se preserva cada uno de ellos. Específicamente hablando del servicio de autenticación, el cual se utiliza en la mayoría de las tareas ejecutadas tanto en la industria como en la sociedad de manera cotidiana, poco a poco ha tomado mayor importancia. Esto, ya que las soluciones criptográficas que basan su seguridad en la dificultad de resolver problemas que se cree son difíciles, con la llegada de las computadoras cuánticas, serán vulneradas con mayor facilidad.
En la actualidad, aun cuando IBM y Google ya han anunciado que poseen computadoras cuánticas, no se tiene una fecha segura que indique cuándo, las computadoras cuánticas se usarán como computadoras personales o portátiles. Sin embargo, no se debe esperar su llegada para dar inicio a la identificación de las ventajas y los retos que traerá consigo dentro de escenarios de aplicación en donde interactúen dispositivos con características diversas.
Los dispositivos con recursos limitados son cada vez más comunes dentro de la sociedad y la industria en dónde dependiendo de las características del escenario, siempre deberá considerarse un balance entre el nivel de seguridad que se quiera obtener y la velocidad de respuesta que se tiene, de ahí que será importante contar con los diferentes estudios y comparativas que marquen la pauta de una dirección a seguir en términos de dicho balance.
Desde un punto de vista criptográfico cabe destacar que la criptografía post-cuántica representa una nueva etapa de la criptografía, la cual ha avanzado de la mano de los dispositivos en donde es utilizada. Ante esto, diferentes estudios indican que los esquemas post-cuánticos presentan velocidad de respuesta mayor al que presentan los esquemas modernos, dejando abierto el camino para conseguir que seran capaces de igualar o reducir los tiempos de procesamientos que muestran dentro de arquitecturas físicas diversas.
La combinación de la criptografía post-cuántica y la biometría parecen ser un buen aliado para la seguridad de los diferentes escenarios en la industria y en la sociedad. Desde el punto de vista biométrico, el diseño de dipositivos de lectura cada vez más pequeños, parecen ser necesitados cada día más y más, lo cual da pie a explorar sobre el diseño de dispositivos de lectura con capacidad propia de procesamiento, sin la necesidad de requerir de un dispositivo adicional.

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, SIP-20190264, SIP-20194938 y SIP-20196694.

Referencias

[1] National Institute of Standards and Technology. (2018). Retrieved from https://www.nist.gov/
[2] L. Chen, Y. L. Jordan, D. Moody, R. Peralta y D. Smith-Tone.*Report on Post-Quantum Cryptography* (2016).
[3] P. Shor, *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] T. Agarwal. *A Brief About Embedded System their Classifications and Applications.* 15-11-16, de Edgefx Technologies Pvt Ltd. (2015), Sitio web: https://www.efxkits.us/classification-of-embedded-systems/
[6] B. Latre, B. Braem, I. Moerman, C. Blondia, and P. Demeester, *A survey on wireless body area networks.* Wireless Networks, (2011), 17(1):1-18.
[7] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia,I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, *Acomprehensive survey of wireless body area networks.* Journal of Medical Systems, (2012), 36(3):1065-1094.
[8] Salas Arriarán, Sergio. *Todo sobre sistemas embebidos*, SAXO, (2017).
[9] Delgado Vargas, Kevin Andrae. De Abiega L'Eglisse, Alfonso Francisco. Gallegos-Garcia, Gina y Cabarcas, Daniel. *Un acercamiento a la línea del tiempo de los algoritmos criptográficos*. Revista Digital Universitaria (RDU). (2019). Vol. 20, Núm. 5 Septiembre-Octubre. DOI:http://doi.org/10.22201/codeic.16076079e.2019.v20n5.a7