Criptografía en el mundo post-cuántico

Valentina Álvarez Valderrama Silvia Alejandra Cárdenas Santos Paula Uzcátegui León

***Abstract*—En un contexto donde la computación cuántica está cada día más cerca de convertirse en una realidad tangible, este trabajo se sumerge en la criptografía en el mundo poscuántico. Se realizará un análisis exhaustivo del funcionamiento y las vulnerabilidades del algoritmo RSA, evaluando su resistencia en el inminente escenario cuántico. Además, exploraremos los avances emergentes en criptografía cuántica y postcuántica, con el objetivo de proporcionar recomendaciones concretas. Este estudio busca contribuir al entendimiento y la implementación de estrategias seguras en un entorno de seguridad de la información en constante evolución.**

***Index Terms*—Computación cuántica, criptografía, RSA, Algoritmo de Shor**

I. Introducción

Con la rápida evolución de la tecnología, la computación cuántica emerge como un avance multidisciplinario que abarca la ciencia de la computación, la física, las matemáticas y la mecánica cuántica. Usando qubits en lugar de bits, los computadores cuánticos prometen resolver problemas complejos de manera exponencialmente más rápida que las computadoras convencionales.

En este contexto, la seguridad informática se convierte en una preocupación central, los algoritmos criptográficos que son imposibles de romper por un computador tradicional en una cantidad de tiempo razonable se encuentran bajo amenza en el mundo donde la computación cuántica es una realidad.

Un ejemplo de esto es RSA, es uno de los algoritmos de encriptación más usados hoy en día. Para romper un mensaje encriptado con RSA se necesitan encontrar los factores primos de un número gigantesco, un problema que un computador clásico demoraría miles de años. Sin embargo empleando un computador cuántico los suficientemente potente, de alrededor de un millón de qubits, es posible romper esta encriptación usando el algoritmo de Shor. Aunque todavía los computadores cuánticos no son capaces de atacar este tipo de problemas, cada día que pasa la probabilidad aumenta, tan solo en noviembre del año pasado el procesador cuantico de IBM Osprey contaba con 400 qubits.

El mundo digital funciona basado en la confianza que tenemos en la garantía de que nuetra privacidad y datos estan seguros. El fallo de los sistemas de encriptación implicaría el colapso de las comunicaciones por internet. Este trabajo tiene como objetivo recopilar los proncipales avances sobre la criptografía post-cuántica. Investigaremos a fondo el funcionamiento y las vulnerabilidades del algortitmo RSA, exploraremos los avances en criptografía cuántica y postcuántica, y proporcionaremos recomendaciones concretas para prepararse para el mundo post-cuántico.

II. ¿Qué es la computación cuántica?

La computación cuántica es una tecnología que utiliza las leyes de la mecánica cuántica para resolver problemas complejos, dado que sus algoritmos adoptan nuevos enfoques para este tipo de inconvenientes. El poder de procesamiento de un computador cuántico se basa en los cúbits o bits cuánticos, los cuales son representados por partículas cuánticas, a diferencia de los bits que tienen un estado 0 o 1, los cubits pueden representar 0 y 1 simultaneamete, gracias a la superposición de estados.

Mientras que los bits se implementan mediante trasnsistores que mantienen un estado de 0 o 1, el concepto de cúbit es más abstracto y no lleva asociado un sistema físico concreto, por lo que en la prática se puede implementar de diferentes formas [8]. Una forma es la de cúbits-supercondictores, que son diminutos bucles de aluminio o niobio que se comporta como un átomo,los estados de este corresponden a los estados de energía del átomo artifical, que puede ser manipulado con impulsos de microondas. Para poder comportarse como un átomo el cúbits-superconductor debe mantenerse a temperaturas por debajo del cero absoluto, por lo que aunque estos son muy pequeños, el computador cuántico es más grande que una nevera, y también tiene un costo muy elevado. En la figura II se muestra una fotografía del computador cuántico desarrollado por Google y presentado en 2019.

Hay principios cuántico fundamentales para entender como funciona la computadora:

- Superposición: Implica la posibilidad de combinar dos o más estados cuánticos para obtener un nuevo estado cuántico válido. Este fenómeno de superposición de cúbits confiere a las computadoras cuánticas su capacidad intrínseca de procesar millones de operaciones simultáneamente.
- Entrelazamiento: Se manifiesta cuando dos sistemas están tan estrechamente conectados que el conocimiento sobre uno proporciona conocimiento instantáneo sobre el otro, independientemente de la distancia entre ellos. Los procesadores cuánticos pueden realizar mediciones en una partícula para inferir conclusiones sobre otra, lo que permite a las computadoras cuánticas resolver problemas complejos de manera más rápida.
- Decoherencia: Representa la pérdida del estado cuántico en un bit. Factores ambientales, como la radiación, pueden desencadenar el colapso del estado cuántico de los cúbits.

Programar un computador cuántico involucra crear un circuito cuantico usando un lenguaje de programación especial

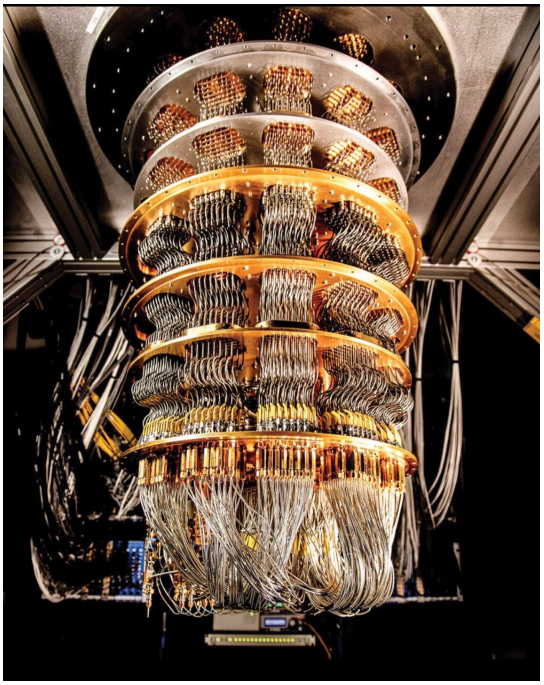

Fig. 1. Computador cuántico de Google con 72 cúbits

para esto, con instrucciones para manipular a los qubits mediante compuertas cuánticas. Estos programas se envian al procesador cuántico, y los resultados se obtienen midiendo el estado de los qubits. Estos computadores estan diseñados para resolver problemas específicos que un computador tradicional no es capaz de resolver, pero no estan pensados para reemplazar a los computadores normales.

Hoy en día compañías como IBM, Google y Rigetti Computing han logrado importantes avances en la construcción de dispositivos cuánticos, presentando avances cada año. La supremacia cuántica, el punto en que se dice un computador cuántico supera a un computador clásico en ciertas tareas fue alcanzado por Google en 2019.

En 2022 IBM logro crear su procesador Osprey que contaba con 433 qubits, y planeaban el procesador Condor con 1121 qubits. Sin embargo, este año el enfoque parece haber cambiado hacia la computación cuántica modular, el procesador Heron con 133 cubits busca mejorar la conectividad entre chips, lo que indica una tendencia hacia sistemas más prácticos e interconectados. [6]

Otras compañías también estan experimentando con enfoques modulares como PsiQuantum, que trabaja con con chips de silicio usando fotones como qubits.

A pesar del progreso, los computadores cuánticos siguen enfrentando dificultades, como sensibilidad al ambiente, que genera ruido y errores y problemas con la coherencia de los qubits. Además todavía se puede considerar un nicho pequeño formado por gente muy especializada, cuyo software todavía se encuentra en una etapa muy inmadura, además de otros mencionados en [7]

III. ¿De qué trata la criptografía?

La criptografía, que se enfoca en salvaguardar la información mediante algoritmos codificados, firmas y hashes, aborda la seguridad de los datos en reposo, en tránsito y durante operaciones computacionales. Sus objetivos incluyen la confidencialidad, integridad, autenticación y no repudio de la información. Inicialmente utilizada para proteger información entre militares y políticos, la criptografía ha evolucionado con avances en seguridad y matemáticas. Hoy en día, es esencial en la sociedad moderna, respaldando aplicaciones como HTTPS, comunicaciones seguras y monedas digitales.

En palabras simples, los algoritmos de cifrado se basan en problemas matemáticos muy dificiles de resolver, que por medio de ingeniosos trucos matemáticos se pueden usar para encriptar y desencriptar un mensaje. Además de esto en la implementación de criptografía en las comunicaciones digitales estos algoritmos deben ser rápidos de implementar para garantizar una comunicación eficiente.

Hay dos funciones fundamentales que cumplen la criptografía para garantizar una comunicación privada y segura: cifrado y firmas digitales. El cifrado consiste en transformar un mensaje de texto plano en uno cifrado, es decir convertirlo en un conjunto de caracteres sin significado que solo el destinatario del mensaje sea capaz de descifrar. Por otro lado las firmas digitales se usan para verificar la identidad del emisario del mensaje.

Existen diferentes métodos de encriptación como claves encripción de clave simetrica, encripción asimetrica de clave pública y funciones hash.

1) **Criptografía de Clave Simétrica** La criptografía de clave simétrica implica el uso de claves idénticas tanto para cifrar como para descifrar datos. Es necesario que todos los receptores compartan la misma clave. Cifrar el mensaje sería como encerrar el mensaje un cofre, unicamente el emisor y el receptor poseen una copia de la llave. Como se ilustra en la figura 1 El algortimo más usado para este tipo de cifrado es AES (Advanced Encryption Standard), es usado para encriptar la información más sensible. Consiste en claves de 128, 192 o 256 bits. De la clave compartida se derivan una serie de claves con la que se encripta el mensaje por rondas, donde se combina la data con la clave en cada ronda, además de otras transformaciones. Mientras más larga la clave, más segura es la clave. AES es de los mecanismos más rápidos y seguros para proteger la información, además que es muy bueno para encriptar grandes cantidades de data. Es lo que se usa por ejemplo para hacer copias seguras de bases de datos en bancos y entidades gubernamentales.
2) **Criptografía Asimétrica (de Clave Pública)** La criptografía asimétrica emplea algoritmos basados en problemas matemáticos de difícil inversión. Este sistema utiliza claves pública y privada para operaciones de cifrado y descifrado. donde La clave pública se distribuye ampliamente, mientras que la clave privada se mantiene en

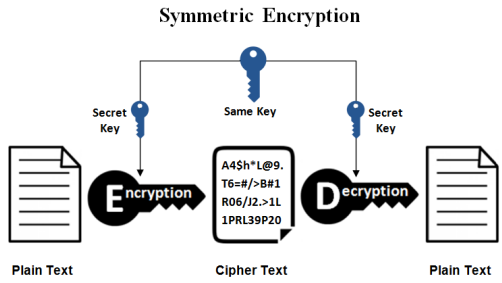

Fig. 2. Esquema de funcionamiento de criptografía de clave simétrica

secreto. Es como si el emisor cerrar el mensaje con un candado público del receptor, y solo el receptor posee la llave que abre ese candado. Como se ilustra en la figura 2. Este método de encriptación es escencial para compartir claves secretas, como intercambiar las claves de AES (de lo contrario habria que físicamente copiar las claves de un sistema a otro para poder usar claves simetricas). Además se usa para hacer firmas digitales, donde el emisor encripta su mensaje con su clave privada y el receptor puede verificar su autenticidad desencriptandolo con la clave pública del emisor. Los dos algortimos más usados de clave asimétrica son RSA y Diffie-Helman.

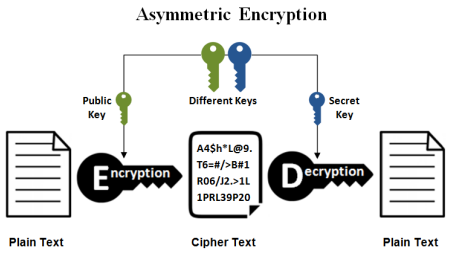

Fig. 3. Esquema de encriptación de clave asimetrica.

3) **Funciones Hash** Las funciones hash criptográficas convierten datos en ”huellas digitales” de longitud fija, diseñadas para dificultar la colisión de huellas digitales idénticas para diferentes entradas. A diferencia de otros esquemas criptográficos, las funciones hash carecen de una clave y son fundamentales en diversos algoritmos y protocolos criptográficos. La funcion es deterministica, es decir que dado un input siempre produce el mismo resultado, además es computacionalmente imposible conseguir dos inputs que retornen el mismo output. Una función hash toma un input y realiza ciertas operaciones matemáticas ireversibles obeteniendo un output que no puede ser convertido de nuevo a su valor original. Este método es el que se usa por ejemplo, para almacenar contraseñas en una base de datos de forma segura, en lugar de guardar el texto plano de la contraseña, se pasa por una función hash. También se puede usar para firmas digitales.

A continuación nos enfocaremos principalmente en los algoritmos que actualmente se prevee pueden ser rotos con ordenadores cuánticos, y se encuentran bajo mayor amenaza, que son los de clave asimétrica, ya que estos funcionan bajo funciones reversibles.

- **RSA (River-Shamir-Adleman)**: Genera un par de claves públicas y privadas, siendo cada una de un tipo, para cifrarlo se basa en la dificultad de factorizar el producto de dos grandes números enteros.
- **Diffie-Hellman**: Se crean dos claves secretas, estableciendo una clave en común, basandose en el problema del logaritmo discreto.
- **Elliptic Curve Cryptography (ECC)**: Se basa en el problema de resolver problemas de logaritmo de curva elíptica.

IV. ¿Qué problemas puede resolver un computador cuántico? (y más importante aún, cuáles no puede resolver)

Cualquier problema imposible para resolver por un computador clásico también sera imposible de resolver por un computador cuántico. Los problemas en que se basa la criptografía asimetrica no son imposibles de resolver, pero son muy dificiles de resolver en una cantidad de tiempo razonable por un computador clásico. La ventaja de los computadores cuánticos es que pueden acelerar ese proceso.

El **algoritmo de Shor** [9] es un algoritmo cuántico desarrollado por el matemático Peter Shor en 1994, con el que se puede resolver de forma eficiente problemas de tipo $n = p \times q$ o de logaritmo discreto tipo $x = g \times e \mod (p)$. Por lo que en teoría es posible romper los algoritmos asimétricos de Diffie-Hellman, RSA y curva elíptica.

También está el algoritmo cuántico de Grover con el que es posible encontrar las claves de AES [10], Sin embargo se ha descubierto que al duplicar el tamaño de la key es posible contraatacar este algoritmo, por lo que AES seguirá siendo seguro.

La pregunta de qué problemas un computador cuántico no puede resolver es un poco más dificil, ya que las posibilidades de un computador cuántico todavía estan por descubrirse. Sin embargo, por ahora se cree que problemas que involucren usar grandes cantidades de memoria no pueden ser abordados por un computador cuántico. Además algoritmos de encriptación irreversibles como las funciones Hash siguen siendo seguros.

V. Amenazas a la seguridad de sistemas criptográficos

Actualmente en criptografía, romper un algoritmo no es la única forma de descrifrar un mensaje. Existen otros métodos a su vez, que hacen que esta disciplina se deba mezclar con más funcionalidades que garanticen un sistema de seguridad completo. En comparación con los ciberataques tradicionales, en este caso nos enfocamos en nuevas vulnerabilidades que se dirigen a la implementación física del sistema o al hardware, en lugar del software; los llamados **ataques de canal lateral**. Se presentan como una forma de ingeniería inversa al obtener

información acerca del algoritmo a partir de factores externos a su ejecución; patrones de salida propios de un sistema que se producen durante las operaciones de cifrado como el análisis de tiempo, el consumo de energía de los componentes, las señales acústicas, las emisiones de calor y electromagnéticas de monitores o de un disco duro se vuelven fuentes viables de información para un atacante.

En consecuencia a esto, se multiplican riesgos para inferir datos confidenciales como claves de cifrado, contraseñas, accesos indeseados y más; el problema adicional radica en que este tipo de ataques suelen ser prácticamente invisibles o mucho más complejos de detectar que las amenazas comunes como el *phishing* o el *malware*, ya que de la misma forma que uilizan información indirecta para el ataque, su detección o prevención debe hacerse a través de estos canales indirectos enfatizado en la mejora de la seguridad del hardware y del diseño, complementado con prácticas de codificación segura y el análisis regular de dichos canales secundarios. Entre otras técnicas usadas para mitigar las fugas de información incluyen pre-cargar registros y buses para prevenir que exista una lectura de energía que se base en el cambio de valores mientras los datos pasan por el bus.

En concreto para la temática, el cifrado RSA ya ha sido objeto de varios ataques de canal lateral en el pasado, por aspectos como el sonido que generaban las claves de encriptación y el tiempo de funcionamiento de los algoritmos. Aunque son un tipo de ataque que no rompen RSA directamente, usa información de su implementación para dar pistas a los atacantes sobre el proceso de encriptación. Estos ataques pueden incluir cosas como el análisis de la cantidad de energía que se está utilizando o el análisis de predicción de ramificaciones, que utiliza mediciones del tiempo de ejecución para descubrir la clave privada. En estos algoritmos usualmente se lleva a cabo una multiplicación solo si el bit exponente que esta siendo procesado es 1. Entonces el atacante podría simplemente medir los cambios en la corriente para, a partir de ahí, derivar la llave de cifrado un bit a la vez.

En sistemas de red, los ataques de canal lateral se basan en sincronización; si un atacante tiene la capacidad de medir el tiempo de descifrado en una computadora para una cantidad de mensajes cifrados diferentes, esta información puede hacer posible que el atacante determine la clave privada del objetivo. La mayoría de las implementaciones de RSA evitan este ataque con el cegamiento criptográfico, que funciona agregando un valor único durante el proceso de cifrado, lo que elimina esta correlación.

A medida que la tecnología evoluciona, los ataques de canal lateral pueden apuntar a una gama más amplia de dispositivos y sistemas, incluidas tecnologías emergentes como la computación cuántica y la inteligencia artificial.

VI. Tipos de algoritmos cuanticamente seguros

La criptografía postcuántica (PQC) busca desarrollar algoritmos resistentes a la amenaza que representa una computadora cuántica a gran escala. Para esto se buscan problemas matemáticos que sean dificiles de resolver tanto para computadores cuánticos como para computadores clásicos. Y además deben ser de fácil implementación en un algoritmo. Hay seis familias en las que se pueden agrupar a los algoritmos cuanticamente seguros, según el problema matemático en que estan basados: Criptografía basada en reticulas, firmas digitales basada en funciones hash, criptografía basada en código, criptografía basada en isogenia, criptografía basada en funciones polinomiales multivariable y criptografía basada en grupo de trenzas. [11]

VII. Criptografía basada en -Reticulas

Hablaremos principalmente de la criptografía basada en reticulas, que es de las más populares en la investigación de algortimos cuanticamente seguros debido a que presenta muchas ventajas como:

- Utiliza simples operaciones lineales como multiplicaciones de vectores para su implementación, lo que lo hace eficiente.
- Puede resistir ataques cuánticos (hasta el momento)
- Garantiza la seguridad incluso en los peores casos de confidencialidad.
- Adicionalmente es posible hacer criptografía basada en reticulas que cuenten con la propiedad de hacer cifrado homomórfico [13], es decir que se puedan hacer operaciones en el mensaje cifrado sin necesidad de descifrarlo, lo que abre las puertas a otro gran número de aplicaciones.

Se basa en el concepto matemático de una Reticula (Lattice en inglés). Una reticula de n dimensiones esta construida por n vectores, estos se les conoce como la base, se pueden sumar, restar y cambiar su dirección de diferentes formas para llegar a todos los puntos que conforman la reticula. La clave para aplicar este problema a algoritmos criptográficos está en que diferentes bases pueden construir la misma reticula. Como se observa en la figura VII los vectores verdes pueden construir la reticula al igual que los vectores rojos. Estos ultimos, que estan más cercanos entre si por lo que se conocen como una ”base mala”, mientras que los vectores verdes, que son ortogonales serían una ”buena base”. Mientras peor es la base, más dificil es resolver porblemas de reticula.

Los dos problemas fundamentales en este tipo de criptografía son: el problema de los vectores más cortos (Smallest Vector Problem, SVP) que involucra encontrar el vector no nulo más corto a un punto. Y el de los vectores más cercanos (Closest Vector Problem, CVP) que va de encontrar el vector más cercano a un punto en la reticula que no forma parte de la reticula como tal. Estos son problemas muy dificiles de resolver especialmente con reticulas de muchas dimensiones, ya que hay muchas formas de combinar la base para acercarse a estos puntos. Además de esto para los algoritmos basados en reticulas también se agregan otros niveles de dificultan usando problemas de aprender con error (Learing with errors, LWE), que consisten en agregar un error a las claves de encriptación para aumentar mucho más su complejidad.

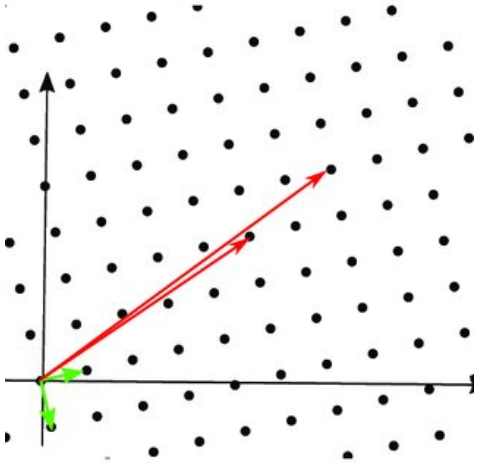

Fig. 4. Ejemplo de rejilla de dos dimensiones

VIII. Firmas digitales basada en funciones hash

El algoritmo de firma digital basado en funciones hash se basa en la propiedad de que si dos mensajes son iguales, entonces sus hashes también lo son, dado que son funciones matemáticas que convierten un mensaje de cualquier longitud en un valor de longitud fija; esto significa que si un atacante intenta modificar el mensaje firmado, el receptor podrá comprobar el cambio que sufrió el hash, ya que este también será modificado. Matemáticamente hablando, se utiliza la función de multiplicación modular la cual es una operación matemática que se realiza en números enteros módulo un número primo, basada en la propiedad de que si dos números son iguales, entonces su producto módulo N también es igual. En el caso del enfoque basado en la función hash SHA-256, la seguridad del algoritmo se basa en la dificultad de factorizar números primos. El hash del mensaje es un valor de 256 bits, que se puede representar como un número entero. Si el atacante pudiera factorizar este número, podría generar un mensaje con el mismo hash que el mensaje original. Sin embargo, factorizar un número primo de 256 bits es un problema NP-hard, lo que significa que es muy difícil de resolver incluso para los ordenadores cuánticos. El algoritmo funciona de la siguiente manera:

- El emisor genera una clave pública y una clave privada, la primer mencionada se comparte con el receptor y la segunda se mantiene en secreto.
- Tambien genera un hash del mensaje que desea firmar, siendo este un valor único que representa el mensaje.
- Finalmente cifra el hash utilizando su clave privada.
- Se envía el mensaje junto a la clave pública al receptor.
- Si el hash decifrado coincide con el hash del mensaje original, entonces la firma es válida.

IX. Criptografía basada en código

La criptografía basada en código es un algoritmo seguro que utiliza códigos para cifrar y descifrar datos basado principalmente en códigos de corrección de errores, como el McEliece, Niederreiter y esquemas relaciones. En el primer mencionado, la seguridad se basa en aleatorizar el mensaje añadiendo errores aleatorios, donde la clave es un código binario aleatorio Goppa [17], la clave pública es una matriz generadora aleatoria realizada a partir de una permutación aleatoria de ese código y el texto cifrado es una palabra clave agregada por el error, por lo que sólo el destinatario conoce la clave privada que puede eliminar esos errores. En general la seguridad de la criptografía en código se basa en el hecho de que para un ordenador cuántico es complejo recuperar el mensaje original a partir del mensaje cifrado, esto se debe a que los códigos correctores de errores son NP-hard, ya que usan problemas mátematicos como:

- El problema del logaritmo discreto: Calcular el logaritmo discreto de un número n en una base g es el número x tal que $g^x = n$.
- El problema de la factorización de enteros: Se basa en factorizar un número entero en sus factores primos.
- El problema del vector más cercano: Se enfoca en encontrar el vector más cercano a otro vector en un conjunto de vectores.

X. Criptografía basada en isogenia

Los criptosistemas de este tipo se basan en la propiedad de gráficos congruentes de curvas elípticas sobre campos finitos, o gráficos de congruencia súper anómalos, para crear un sistema seguro. Una isogenia entre dos curvas elípticas es una función polinómica que mapea un punto entre estas, son invertibles por lo que es posible recuperar el punto original a partir del mapeado. En esto se basan varios esquemas específicos, como el esquema de intercambio de claves CSIDH, un candidato de ataque cuántico alternativo al esquema de intercambio de claves Diffie-Hellman, se está utilizando la actual curva elíptica de Diffie-Hellman, o el esquema de firma digital SQISign. Además, un cifrado de clave pública basado en isogenia, SIKE, es un PKE/KEM seleccionado después de la tercera ronda del NIST, y existen algunos estudios sobre este esquema [18]. La seguridad de esta criptografía se basa en el hecho de que es difícil calcular isogenias entre curvas elípticas de gran tamaño.

XI. Criptografía basada en funciones polinomiales multivariable

La criptografía multivariable es un cifrado asimétrico basado en polinomios multivariables sobre un campo finito. Un polinomio multivariable es una función polinómica de dos o más variables, la resolución de estos se basa en encontrar raíces. Se ha demostrado que la resolución del problema polinómico multivariable es un tiempo polinómico (NP-hard) completo no determinista, por lo que es adecuado para la criptografía post-cuantica, al ser computacionalmente costoso en polinomios multivariables grandes. Se sabe que este algoritmo es muy eficiente al diseñar criptoanálisis, se utiliza en la generación de firmas digitales y se considera que produce la firma digital más corta de los algoritmos PQC. Varios

esquemas de firma digital, como Rainbow, TTS, QUARTZ y QUAD, se basan en este método.

XII. Criptografía basada en grupo de trenzas

Esta técnica utiliza la teoría de las trenzas, siendo cada una de estas un tipo de objeto matemático que se representa como una serie de hilos que se entrelazan entre sí. Los grupos tienen como elementos todas las posiciones diferentes en las que se pueden entrelazar las trenzas (infinitas), generalmente se utiliza el grupo B_n que contiene todos los entrelazamientos de n trenzas. Donde una operación σ consiste en enredar dos de los hilos de la trenza y agregar más operaciones para crear una trenza cada vez más compleja.

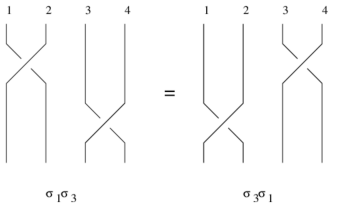

Fig. 5. Simulación de las trenzas

El problema consiste en generar dos trenzas realizando diferentes opciones de entrelazamiento, donde lo verdaderamente complejo es decidir si las dos trenzas que se entrelazaron son equivalentes, teniendo en cuenta el problema de la conjugación; de los cuales no se conoce una solución eficiente con computadores cuánticos hasta la fecha.

XIII. Algortimos post-cuánticos en camino a la estandarización

En 2016 el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) inició un proceso para identificar y estandarizar algoritmos criptográficos cuanticamente seguros. Cientificos de todo el mundo postularon sus soluciones, y los elegidos para estandarización fueron publicados en 2022 [12], se seleccionaron cuatro: RYSTALS-KYBER para encripción de clave pública e intercambio de claves, y CRYSTALS-DILITHIUM, FALCON, y SPHINCS+ para firmas digitales. De estos, los primeros tres se basan en reticulas, y el ultimo en funciones Hash.

XIV. ¿Qué podemos hacer mientras tanto para proteger nuestros sistemas?

Aunque ya se tienen algoritmos de cifrado poscuántico, todavía hay un largo camino por recorrer antes de poder implementarlos a todos los sistemas para asegurar la privacidad de las comunicaciones. Para sistemas que esten usando aún algoritmos poco seguros para encriptar proteger sus sistemas debería ser algo de gran preocupación, ya que un atacante podría estar haciendo copias de la data encriptada para desencriptarla dentro de unos años cuando la computación cuántica se convierta en una realidad. A continuación mencionamos algunas de las recomendaciones de los expertos para proteger los datos:

1) **Saber dónde están los datos, y quién tiene acceso a estos**
   Comprender la ubicación y propiedad de los datos sensibles es un paso fundamental en la protección de datos. Esto implica mantener un inventario completo de los repositorios de datos, ya sea en servidores locales, plataformas en la nube o cualquier otro medio de almacenamiento. Saber quién tiene acceso a estos datos ayuda a implementar controles de acceso adecuados y monitoreo para evitar accesos no autorizados. Auditorías y evaluaciones regulares pueden ayudar a garantizar la seguridad de los lugares de almacenamiento de datos.
2) **Sensibilidad al Tiempo (¿Por cuánto tiempo es prudente protegerla, tenerla bajo secreto?):**
   La sensibilidad al tiempo en la protección de datos implica evaluar la vida útil de la sensibilidad de los datos. No todos los datos requieren el mismo nivel de protección indefinidamente. Algunos datos pueden ser altamente sensibles por un tiempo limitado, después del cual su importancia disminuye. La implementación de controles de acceso basados en el tiempo y políticas de cifrado puede ayudar a adaptar el nivel de protección de acuerdo con la relevancia de los datos. Revisiones y actualizaciones regulares de las políticas de seguridad garantizan que las medidas de protección se alineen con la sensibilidad en evolución de los datos.
3) **Agilidad criptográfica (¿Es posible cambiar un algoritmo por otro fácilmente?):**
   La agilidad en la protección de datos se refiere a la capacidad de adaptarse rápidamente a amenazas emergentes y tecnologías. Esto incluye la capacidad de cambiar algoritmos criptográficos rápidamente en respuesta a avances en la computación cuántica o al descubrimiento de vulnerabilidades en algoritmos existentes. Una estrategia de seguridad ágil implica mantenerse informado sobre los últimos avances en computación cuántica y criptografía, y contar con mecanismos para actualizar protocolos criptográficos de manera rápida en todos los sistemas.
4) **Transición a algoritmos Criptográficos Seguros ante la Computación Cuántica:**
   Considerando que los cuatro algoritmos poscuánticos mencionados en la sección anterior han sido aceptados y en su mayoría estandarizados, las organizaciones comenzarán a incorporarlos con mayor confianza, emprendiendo la transición de la cifra actual a la cifra poscuántica, de esta manera, los usuarios pueden escoger cambiarse a opciones más seguras en caso de vulneración o compromiso del algoritmo, asegurando así la agilidad criptográfica.

XV. Discusión

Es imposible negar que la computación cuántica cuenta con el potencial de revolucionar muchos campos del conocimiento humano, siendo uno de estos la seguridad informática. Como se expuso anteriormente, estos ordenadores pueden llegar a ser

utilizados para romper algoritmos de encriptación actuales, lo que genera graves consecuencias en la privacidad de los datos y el campo de la ciberseguridad. La criptografía postcuántica es claramente una respuesta a la inminente amenaza de la computación cuántica al ser diseñados para resistir ataques de este tipo; a pesar de encontrarse en una fase de desarrollo, el algoritmo basado en retículas emerge como el más aceptado hasta la fecha, aunque aún no haya una técnica estandarizada, se avanza en esa dirección. A pesar de todos los desafíos a los que se enfrenta la PQC, es muy importante que esta se siga investigando y desarrollando, al ser esencial para proteger la seguridad de las comunicaciones y los datos en un mundo donde la computación cuántica es cada vez más poderosa. Como recomendaciones con el fin de promover la continua mejora de la seguridad de la información en las comunicaciones, encontramos:

- Obtener inversiones significativas de entidades gubernamentales y empresariales para impulsar la investigación y desarrollo en criptografía postcuántica.
- Planificar la migración de organizaciones a algoritmos de criptografía postcuántica.
- Concientizar a los usuarios de redes sobre los riesgos actuales de la computación cuántica, instándolos a adoptar medidas proactivas para proteger su información.

Hasta que se pueda llegar a implementar lo anteriormente mencionado, se le recomienda a los usuarios tener especial cuidado con la información que proporcionan en las redes de comunicación, ya que aquellos algoritmos de encriptación que aun no han sido rotos por algoritmos como el de Shor, en un futuro cercano podrían serlo, por lo que se hace especial enfasis nuevamente en comprender donde se encuentran sus datos y quienes tienen acceso a estos, al menos hasta que se establezca una infraestructura global de seguridad cuántica.

REFERENCES

[1] ¿Qué es la criptografía? - Explicación sobre la criptografía - AWS. (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/cryptography/

[2] KeepCoding, R. (2022, 4 agosto). ¿Qué es la criptografía postcuántica? KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-la-criptografia-postcuantica/

[3] ¿En qué consiste la computación cuántica? - Explicación sobre la computación cuántica - AWS. (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/quantum-computing/

[4] ¿Qué es quantum computing? — IBM. (s. f.). https://www.ibm.com/mx-es/topics/quantum-computing

[5] Castelvecchi, Davide. "Are Quantum Computers about to Break Online Privacy?" Nature, vol. 613, no. 7943, 6 Jan. 2023, pp. 221–222, www.nature.com/articles/d41586-023-00017-0, https://doi.org/10.1038/d41586-023-00017-0.

[6] Website, Michael. "What's next for Quantum Computing." MIT Technology Review, 6 Jan. 2023, www.technologyreview.com/2023/01/06/1066317/whats-next-for-quantum-computing/.

[7] Website, Swayne, Matt. "What Are the Remaining Challenges of Quantum Computing?" The Quantum Insider, 24 Mar. 2023, thequantuminsider.com/2023/03/24/quantum-computing-challenges/#:\~:text=Most\%20experts\%20would\%20consider\%20this. Accessed 29 Nov. 2023.

[8] Wright, Katherine. "What's a Qubit? 3 Ways Scientists Build Quantum Computers." Scientific American, 28 Aug. 2023, www.scientificamerican.com/article/whats-a-qubit-3-ways-scientists-build-quantum-computers/#:\~:text=The\%20Superconducting\%20Qubit&text=Google. Accessed 29 Nov. 2023.

[9] Shor, Peter W. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." SIAM Journal on Computing, vol. 26, no. 5, Oct. 1997, pp. 1484–1509, arxiv.org/abs/quant-ph/9508027, https://doi.org/10.1137/s0097539795293172.

[10] Grassl, Markus, et al. "Applying Grover's Algorithm to AES: Quantum Resource Estimates." Post-Quantum Cryptography, 2016, pp. 29–43, https://doi.org/10.1007/978-3-319-29360-8_3.

[11] Bavdekar, Ritik, et al. "Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research." ArXiv:2202.02826 [Cs], 6 Feb. 2022, arxiv.org/abs/2202.02826.

[12] NIST. "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms." NIST, 5 July 2022, www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

[13] Yi, Xun, et al. "Homomorphic Encryption." Homomorphic Encryption and Applications, 2014, pp. 27–46, https://doi.org/10.1007/978-3-319-12229-8_2.

[14] Hameed, S., Jumaa, G. G. (2017). Digital signature based on hash functions. ResearchGate. https://www.researchgate.net/publication/313707065_Digital_Signature_Based_on_Hash_Functions

[15] Editor knowledgecuddle. (2015). Secure digital signature schemes based on hash functions. academia.edu. https://www.academia.edu/12120019/Secure_Digital_Signature_Schemes_based_on_Hash_Functions

[16] Dam, D., Tran, T., Hoang, V., Pham, C., Hoang, T. (2023). A survey of Post-Quantum Cryptography: Start of a new race. Cryptography, 7(3), 40. https://doi.org/10.3390/cryptography7030040

[17] Kuo, Y.-M.; -Herrero, F.G.; Ruano, O.; Maestro, J.A. RISC-V Galois Field ISA Extension for Non-binary Error-correction Codes and Classical and Post-quantum Cryptography. IEEE Trans. Comput. 2022, 72, 682–692.

[18] Elkhatib, R.; Koziel, B.; Azarderakhsh, R.; Kermani, M.M. Accelerated RISC-V for Post-quantum SIKE. IEEE Trans. Circ. Syst. I Regul. Pap. (TCAS-I) 2022, 69, 2490–2501.

[19] Gómez, J. D. F. (2023, 3 agosto). Vulnerabilidades en algoritmos de criptografíapost-cuántica. Cyte. https://www.cyte.co/post/vulnerabilidades-en-algoritmos-de-criptografia-postcuantica#:\~:text=Una%20de%20las%20t%C3%A9cnicas%20m%C3%A1s,la%20topolog%C3%ADa%20de%20las%20trenzas