COMPUTACIÓN CUÁNTICA: ATAQUE A LA CRIPTOGRAFÍA SIMÉTRICA Y ASIMÉTRICA

Harold Alejandro Villanueva Borda
Ciencias de la Computación
Universidad Católica San Pablo
harold.villanueva@ucsp.edu.pe

***Abstract*—**

***Index Terms*—Criptografía, Seguridad y Privacidad, QFT, algoritmo de Shor, Grover**

I. Introducción

En la década de 1980 el reconocido físico teórico Richard Phillips Feynman notó que la simulación de ciertos efectos de la mecánica cuántica en una computadora clásica no es muy eficiente, debido a esto se ideó la construcción de computadoras cuánticas pero este conlleva un desarrollo lento debido a su complejidad. En 1994 el matemático del MIT Peter Shor Williston diseñó un algoritmo cuántico de tiempo polinomial para la factorización de números enteros [18].

En el mundo de la informática se conoce el bit, a su vez existe el bit cuántico o también llamado qbit, donde este puede ponerse en un estado de superposición que codifica al 0 y al 1. En la computación clásica se usan los procesos paralelos para disminuir el tiempo de procesamiento de algunos cálculos, por otro lado en un sistema cuántico se usa el paralelismo de forma masiva. A diferencia de la computación clásica en donde se puede leer el resultado de un thread paralelo, en la computación cuántica debido que la medición es probabilística no se puede elegir qué resultado leer por lo que el acceso a los resultados es totalmente restringido y para acceder se realiza una medición, dicha solución se viene mejorando con el pasar de los años en donde se involucra algoritmos conocidos como la factorización de Shor, el algoritmo de Grover, sin embargo todas las propuestas recientes tiene problemas de escalabilidad y se requiere de un gran avance para sobrepasar las decenas de qbit [18].

Hoy en día muchos asumen que implementar un algoritmo criptográfico "irrompible" es imposible, por lo que en la actualidad se centran más en resistir el ataque. Los algoritmos de encriptación más usados son el RSA (Rivest, Shamir y Adleman), DES (Data Encryption Standard), AES Advanced Encryption Standard; si bien es cierto estos algoritmos están diseñados para resistir ataques de las computadoras actuales, pero es cuestión de tiempo para que estos sistemas sean sean cada vez menos resistentes. Este problema permitió el desarrollo de la criptografía cuántica en la que se basa en las leyes de la mecánica cuántica con el objetivo de proteger el secreto de los mensajes [14]. Actualmente con las constantes investigaciones acerca de la computación cuántica, estamos por entrar a una nueva era de la criptografía en la que se plantea un nuevo protocolo de distribución de claves cuánticas BB84 desarrollado por Charles Bennet y Gilles Brassard en 1984 [3].

Los algoritmos cuánticos representan un peligro para la criptografía clásica; el más famoso y amenazante es el algoritmo de Shor ya que este resuelve el problema de factorización de enteros, así como también la dificultad de los logaritmos discretos en tiempo polinomial [22]. La transformada Cuántica de Fourier juega un papel importante y se encuentra en el núcleo de los algoritmos.

Actualmente hay 3 direcciones importantes de investigación de los ataques de clave pública de computación cuántica [23]:

1) Mejorar, modificar, simplificar el algoritmo de Shor y si fuera posible inventar uno que supere a Shor.
2) Algoritmos de ataque cuántico basados en computación cuántica adiabática
3) Algoritmos de ataque cuántico basados en el principio de recorrido cuántico

Hoy en día el uso de la computación clásica en la vida cotidiana es normal y para el intercambio de información se hace uso de la criptografía de clave pública como el RSA (Rivest, Shamir y Adleman), en donde la encriptación de envío de datos desde un emisor hacia un receptor es confiable. La protección que brinda diversos algoritmos criptográficos clásicos hasta cierto punto son altamente seguros y eficientes, pero en algún momento estos dejaran de serlo y más aún con el desarrollo de la computación cuántica.

En este survey se muestran conceptos fundamentales de la computación cuántica, así como también se mostrarán algoritmos cuánticos y sus funcionalidades. Por otro lado la investigación en este survey se enfocará en vulnerar la seguridad del

cifrado simétrico y asimétrico, haciendo uso de ideas como el algoritmo de Grover y del algoritmo de Shor para enfrentar la solución de logaritmos discretos y la factorización de números enteros de gran tamaño, así como también, el uso importante y el gran papel que juega la Transformada Cuántica de Fourier.

II. Computación cuántica

- *Circuitos*

  Los circuitos son redes compuestas por cables que transportan valores de bit a compuertas que realizan operaciones elementales en los bits. Todos los circuitos que consideramos serán acíclicos, lo que significa que los bits se mueven a través del circuito de forma lineal y los cables nunca retroalimentan a una ubicación anterior en el circuito. Un circuito es una matriz o red de puertas, que es la terminología que se usa a menudo en el entorno cuántico. Las puertas provienen de una familia finita, y toman información de los cables de entrada y entregan información a lo largo de algunos cables de salida [9].

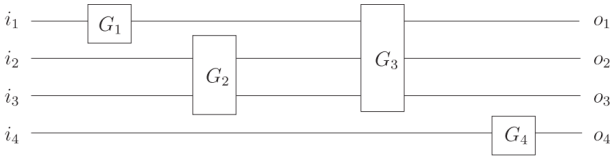


Fig. 1. Diagrama de circuito [9]

Definicion: Un conjunto de compuertas es universal para el cálculo clásico si, para cualquier entero positivo n, m y función $f : \{0,1\}^n \to \{0,1\}^m$, se puede construir un circuito para calcular f usando solo compuertas a partir de ese establecer [9].

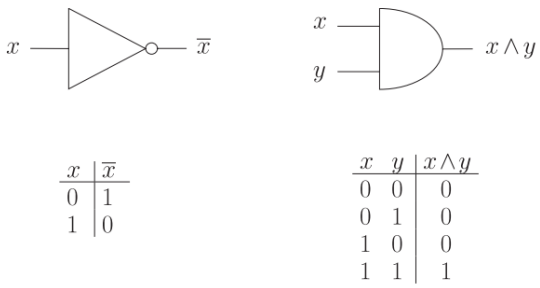
- *Computación reversible*

  La teoría de la computación cuántica está relacionada con una teoría de la computación reversible. Un cálculo es reversible si siempre es posible recuperar de forma única la entrada, dada la salida. Por ejemplo, la operación NOT es reversible, porque si el bit de salida es 0, sabe que el bit de entrada debe haber sido 1, y viceversa. Por otro lado, la operación AND no es reversible [9].

  Cada puerta en una familia finita de puertas se puede hacer reversible agregando algunos cables de entrada y salida adicionales si es necesario [9].

- *Notación Dirac y espacios de Hilbert*

  La notación de Dirac fue inventada por Paul Dirac y se usa a menudo en mecánica cuántica. Dicha notación identifica un vector que se escribe dentro de un 'ket' y se parece a $|a\rangle$ [9]. La base canónica de un espacio



x	$\overline{x}$
0	1
1	0

x	y	$x \wedge y$
0	0	0
0	1	0
1	0	0
1	1	1

Fig. 2. Puertas NOT y AND [9]

vectorial bidimensional tiene dos vectores, denotados por $\{|0\rangle, |1\rangle\}$ en la notación de Dirac, donde $|0\rangle$ y $|1\rangle$ tienen la siguiente representación [16]:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} y\ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1}$$

Estos vectores tienen dos entradas, longitud unitaria y son ortogonales. Entonces, esta base es ortonormal. Se llama base canónica en álgebra lineal y base computacional en computación cuántica. Tenga en cuenta que $|0\rangle$ no es el vector nulo, sino el primer vector de la base canónica. Todas las entradas del vector nulo son iguales a 0 [16].

Los espacios vectoriales están sobre números complejos y son de dimensión finita, lo que simplifica significativamente las matemáticas que se requiere, a su vez, los espacios vectoriales son miembros de una clase de espacios vectoriales llamados espacios de Hilbert y está dada por esta notación $\mathcal{H}$ [9].

- *Qubit y superposición*

  La unidad de memoria básica de una computadora clásica es el bit, que asume 0 o 1. Por lo general, el bit se implementa usando dos voltajes distintos, siguiendo la convención de que el voltaje bajo o nulo representa el bit 0 y el voltaje alto representa el bit 1. La unidad de memoria básica de una computadora cuántica es el qubit, que también asume, al final del cálculo, 0 o 1 [16].

  La diferencia con el dispositivo clásico ocurre durante el cómputo ya que el qubit admite la coexistencia simultánea de 0 y 1, es decir, antes de la medición, el estado de un qubit está representado por un vector bidimensional $norma - 1$ y los estados de un qubit correspondientes a 0 y 1 son $|0\rangle$ y $|1\rangle$. La coexistencia cuántica se representa matemáticamente mediante una combinación lineal de vectores ortonormales de la siguiente manera [16]:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2}$$

donde α y β son números complejos que obedecen la restricción.

$$|\alpha|^2 + |\beta|^2 = 1 \tag{3}$$

El estado del qubit es el vector $|\psi\rangle$ de la norma 1 con las entradas α y β. Los números complejos α y β son las amplitudes del estado $|\psi\rangle$.

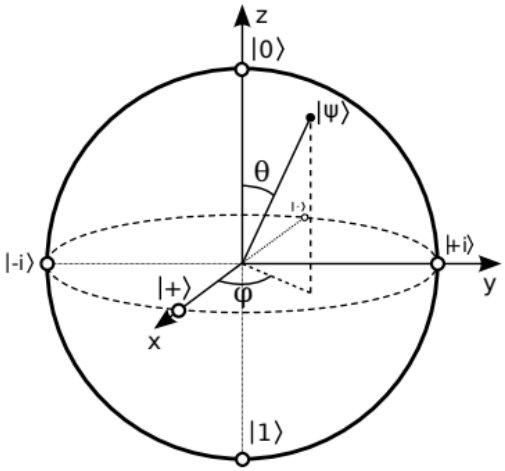


Fig. 3. Esfera de Bloch y ubicación de los estados $|0\rangle$, $|1\rangle$, $|\pm\rangle$ y $|\pm\rangle$. Se muestra un estado arbitrario $|\psi\rangle$ con ángulos esféricos θ y φ [16].

- *Circuito de una función Booleana*

Ahora se mostrarácómo obtener el circuito cuántico de una tabla de verdad; esto se logrará mediante puertas Toffoli multiqubit. Para mostrar que las puertas de Toffoli multiqubit puede implementar cualquier función booleana en una computadora cuántica, tomemos como ejemplo la función booleana de 3 bits $f(a, b, c)$ definida por la siguiente tabla de verdad [16]:

a	b	c	$f(a,b,c)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

Fig. 4. Circuito que implementa f [16]

Como f tiene tres bits de entrada, usamos puertas Toffoli multiqubit con tres controles. El cuarto qubit es el objetivo. La salida de f es la salida de una medición del qubit objetivo. Como f tiene dos cláusulas en la forma normal disyuntiva, usamos dos compuertas Toffoli multiqubit. La primera compuerta debe ser activada por la entrada $|001\rangle$ y la segunda por $|110\rangle$, que corresponden a las filas de la tabla de verdad cuya salida es [16]:

El siguiente circuito implementa f:

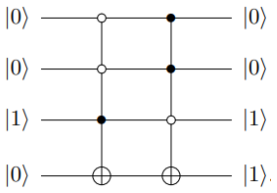


Fig. 5. Circuito que implementa f [16]

Tenga en cuenta que si la entrada es $|a, b, c\rangle|0\rangle$, entonces la salida es $|a, b, c\rangle|f(a, b, c)\rangle$. Esto muestra que la computadora cuántica puede calcular cualquier función booleana de n bits utilizando una puerta Toffoli multiqubit con $(n + 1)$ qubits para cada salida 1 de la tabla de verdad. Desafortunadamente, esta técnica de construcción de circuitos cuánticos para calcular tablas de verdad no es eficiente, ya que el número de puertas de Toffoli multiqubit aumenta exponencialmente en función del número de qubits en el peor de los casos [16].

III. Algoritmos Cuánticos

- *The Deutsch Algorithm*

Este algoritmo se basa en la Transformada Cuántica de Fourier, así mismo, ilustra las ideas clave del paralelismo e interferencia cuántica que se usan en todos los algoritmos útiles [10]. Por otro lado este es el primer algoritmo que explota el paralelismo cuántico utilizando solo 2 qbits, dicho algoritmo ha inspirado la construcción de varios algoritmos cuánticos que son mucho más eficientes [15].

El problema de Deutsch fue planteado en 1985, aun sin usar el modelo de circuito cuántico. Una generalización del algoritmo de Deutsch es el algoritmo de Deutsch-Jozsa [15] tiene exactamente la misma estructura que su versión anterior y al igual que con el algoritmo de Deutsch, tenemos un circuito reversible que implementa una función desconocida f, pero esta vez f es una función de cadenas de n bits a un solo bit [10].

El problema de Deutsch

Entrada: una caja negra para calcular una función desconocida función $f : \{0,1\} \to \{0,1\}$.

Problema: Determinar el valor de $f(0) \oplus f(1)$ haciendo consultas a f.

Supongamos que se tiene un circuito reversible para calcular una función desconocida de 1 bit $f : \{0,1\} \to \{0,1\}$: Tratamos al circuito reversible como una caja negra, esto quiere decir que al aplicar el circuito para obtener valores de $f(x)$ para x entradas, no se obtendrá ninguna información del funcionamiento interno del circuito para aprender sobre la función f. Clásicamente el número de consultas que realiza para determinar $f(0) \oplus f(1)$ es 2 [10].

- *Quantum Transform Fourier*

  La transformada de Fourier convierte una función en el dominio del tiempo en las frecuencias que la componen en el dominio de la frecuencia, transformando una lista de muestras de funciones espaciadas uniformemente en una lista de coeficientes para una secuencia finita de sinusoides complejos, ordenados por frecuencia. En computación cuántica, la QFT (Quantum Transform Fourier) es el análogo cuántico de la DFT (Discret Fourier Transform). El QFT se puede realizar de manera eficiente en una computadora cuántica utilizando exponencialmente menos puertas de las que se requieren para calcular clásicamente. En QIP (procesamiento de información cuántica), la QFT es una generalización de la transformada de Hadamard y ambas son bastante similares, con la excepción de que la QFT introduce una fase [19].

  En el procesamiento de información cuántica (QIP), la transformada cuántica de Fourier (QFT) tiene una gran cantidad de aplicaciones: el algoritmo de Shor y la estimación de fase son solo algunos ejemplos bien conocidos. El algoritmo de factorización cuántica de Shor, uno de los algoritmos cuánticos más citados, se basa en gran medida en la QFT y encuentra eficientemente factores primos enteros de grandes números en computadoras cuánticas [19].

- *Grover Algorithm*

  Este algoritmo cántico brinda una aceleración polinomial sobre los algoritmos clásicos más conocidos para solucionar muchos problemas importantes . Este algoritmo de búsqueda cuántica realiza una búsqueda genérica, por ejemplo, dado un entero grande N, se puede reconocer eficientemente si un entero p es un factor no trivial de N. La búsqueda cuántica es una herramienta para acelerar este tipo de búsquedas genéricas [8].

El problema de búsqueda

Entrada: Una caja negra U_f para calcular una función desconocida $f : \{0,1\}^n \to \{0,1\}$.

Problema: Encuentra una entrada $x \in \{0,1\}^n$ tal que $f(x) = 1$..

Si la función f sólo se proporciona como una caja negra, entonces son necesarias $\Omega(\sqrt{2}^n)$ aplicaciones de la caja negra para resolver el problema de búsqueda con alta probabilidad para cualquier entrada. Por lo tanto, los algoritmos cuánticos pueden proporcionar, como máximo, una aceleración cuadrática sobre la búsqueda exhaustiva clásica. El algoritmo de Grover realiza la búsqueda cuadráticamente más rápido de lo que se puede hacer de forma clásica. Si hay exactamente una solución, una búsqueda de fuerza bruta determinista clásica toma $2^n 1$ consultas en el peor de los casos. De hecho, cualquier algoritmo clásico, que para cualquier función encuentra una solución con una probabilidad de al menos $\frac{2}{3}$, debe realizar consultas $\Omega(2^n)$ en el peor de los casos. El algoritmo de búsqueda cuántica de Grover solo toma $O(\sqrt{2}^n)$ = $O(\sqrt{2}^{\frac{n}{2}})$ consultas [8].

En particular, el algoritmo de Grover proporciona una aceleración cuadrática en la solución de problemas NP-completos , que explican muchos de los problemas difíciles importantes en informática [8]. Por otro lado, el poder de los algoritmos cuánticos, tal como lo descubrió Lov Grover, es que $\frac{N}{2}$ se puede mejorar a $O(N^{1/2})$. En comparación con un algoritmo clásico de búsqueda aleatoria, el factor $\frac{1}{2}$ entra en el exponente, lo que es una gran mejora. Ahora explicaremos cómo y por qué funciona el algoritmo [12].

- *Shor's Algorithm*

  El algoritmo de Shor se presentó en 1994 en una conferencia, este describe dos algoritmos cuánticos para la factorización de enteros y logaritmos discretos que se ejecutan en tiempo polinomial. Shor explota no solo el paralelismo cuántico sino también el entrelazamiento [17].

  1) Idea general

     En el algoritmo de factorización de Shor (SFA), el objetivo es encontrar un factor no trivial de un número entero compuesto N. Dicho brevemente, SFA funciona de la siguiente manera. Elige

aleatoriamente un número entero $y < N$ y comprueba si y y N son coprimos. Si y es coprimo con N, entonces SFA ejecuta una subrutina cuántica especial para obtener el orden $2r$ de N con cierta probabilidad ($2r$ es aquí un número entero). En el SFA original y en todos los SFA anteriores, si $2r$ era un número entero par y $y^r \not\equiv -1(\text{mod } N)$, entonces SFA usa y y $2r$ para obtener un factor no trivial de N. Sin embargo, si el resultado r obtenido por la subrutina de búsqueda de orden cuántico no era $2r$, o $2r$ no era un número entero par, o $y^r \equiv -1(\text{mod } N)$, entonces la subrutina cuántica tendría que ejecutarse nuevamente [13].

2) Explicación detallada del algoritmo Shor [27]
   - Elige un número d con factores primos pequeños tal que $2n^2 \leq d \leq 3n^2$.
   - Elija un número entero aleatorio x que sea coprimo de n.
   - Repita los siguientes pasos, registre d veces usando la misma x cada vez:
     * Cree un registro de memoria cuántica de $2d$ enteros no negativos módulo n y divídelo en dos mitades llamadas reg1 y reg2. Para el estado de todo el registro escribimos el vector ket $|reg1, reg2\rangle$.
     * Cargue reg1 con los enteros $0, 1, ..., d-1$ y reg2 con ceros en todos los lugares, luego normalice el registro de manera que podamos escribir el estado de todo el registro como ket vector (notación de Dirac).

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a, 0\rangle \tag{4}$$

     * Realice la transformación $x \to x^a(\text{mod } .n)$ (usando paralelismo cuántico) en cada número (no normalizado) en reg1 y coloque los resultados en los lugares correspondientes en reg2. Denote por r el período de la transformación anterior. Entonces el estado del registro completo (normalizado) se vuelve

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a, x^a(\text{mod } .n)\rangle \tag{5}$$

     * Medir el contenido de reg2 mediante el operador hermitiano A. Entonces esto colapsa a algún k y tiene el efecto de proyectar el estado de reg1 para que sea una superposición de exactamente aquellos valores de a para los cuales $x^a = k(\text{mod } .n)$. Por tanto, el estado del registro completo es

$$|\psi\rangle = \frac{1}{\#M} \sum_{a' \in M} |a', k\rangle \tag{6}$$

donde $M := \left\{a' : x^{a'} = k(\text{mod}.n)\right\}$

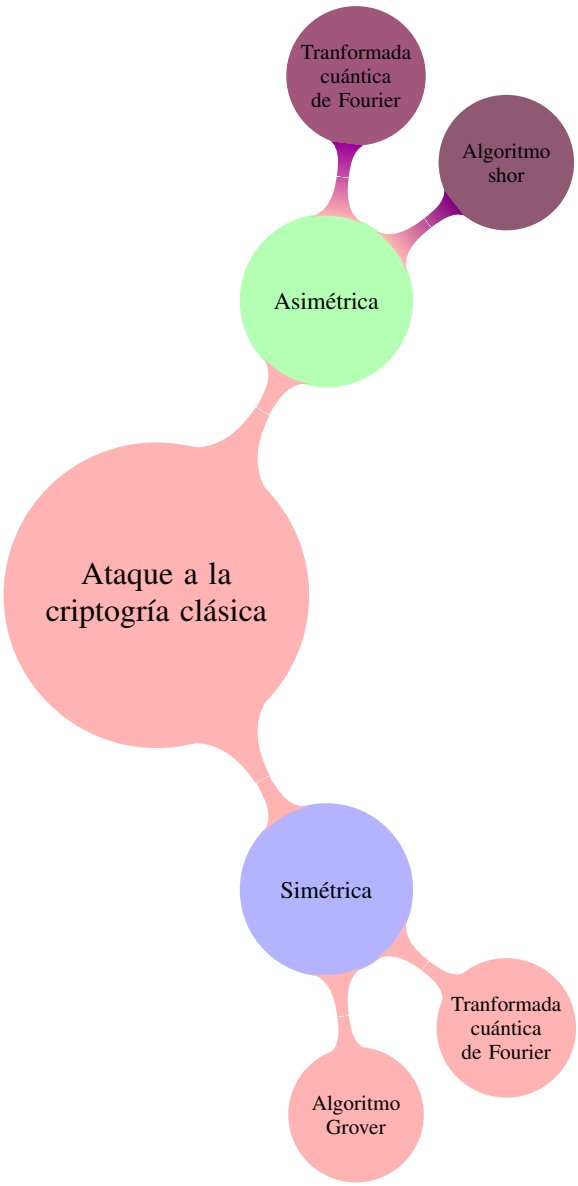
     * Calcule la transformada de Fourier discreta (rápida) del estado proyectado en reg1 y devuelva este resultado a reg1. Esto mapea el estado proyectado en reg1 en una superposición

$$|\psi\rangle = \frac{1}{\#M} \sum_{a' \in M} |a', k\rangle \tag{7}$$

     * Ahora, la transformada de Fourier en reg1 es una función periódica con un pico en múltiplos del período inverso $\frac{1}{r}$. Los estados correspondientes a múltiplos enteros de $\frac{1}{r}$ y los cercanos a ellos aparecen con mayores amplitudes de probabilidad que los que no corresponden a múltiplos enteros del periodo inverso. Entonces, en cada paso, obtenemos un número h' tal que $\frac{h'}{d}$ está cerca del múltiplo $\frac{\lambda}{r}$ del período inverso del mapa exponencial para algún $\lambda \in \mathbb{N}$. Para estimar λ, se puede calcular la expansión de fracción continua de $\frac{h'}{d}$ siempre que el denominador sea menor que n y luego retener la fracción más cercana como $\frac{\lambda}{r}$. Si esto se hace con suficiente frecuencia, tenemos suficientes muestras de λ_i que conducen a una conjetura del verdadero λ y, por lo tanto, de r.
   - Ahora que conocemos r, podemos determinar los factores de n con alta probabilidad [27].

Observamos que, por supuesto (con una probabilidad bastante baja), el algoritmo de Shor puede fallar. Tales contraejemplos se construyen fácilmente. Pero representan casos bastante atípicos. Además, en lugar de utilizar la transformada clásica (rápida) de Fourier, también hay algoritmos cuánticos para la transformada de Fourier, que hacen que el algoritmo de Shor funcione aún más rápido en la práctica, pero no hasta el punto de mejorar el orden lineal de complejidad [27].

IV. Representación gráfica de la taxonomía



V. Trabajos Relacionados

- Cryptographic Attack Possibilities over RSA Algorithm through Classical and Quantum Computation

  El sistema criptográfico RSA es usado para el diseño de cifrado, su protocolo de seguridad funciona según el principio de factorización de enteros grandes que descompone el número compuesto en un producto de números primos. En dicho survey se describe un ataque por fuerza bruta, en la que tiene como objetivo encontrar la clave secreta consultando la función de cifrado sucesivamente con todas las posibles claves. Por otro lado, para vulnerar el algoritmo RSA es necesario la factorización de números enteros grandes, actualmente no existe un algoritmo en tiempo polinomial que pueda realizarlo en una computadora clásica, sin embargo en dicho survey se propone el Algoritmo Shor logra factorizar números enteros grandes en tiempo polinomial, pero este algoritmo sólo puede ejecutarse en una computadora cuántica [21].

- Quantum Algorithm for Attacking RSA Based on Fourier Transform and Fixed-Point

  Shor diseña un algoritmo cuántico de tiempo polinomial para encontrar el orden r de un elemento a en el grupo multiplicativo Z_n^* , que es usado para factorizar el entero positivo n y lograr así romper el famoso sistema criptográfico RSA, pero está sujeto a una condición, donde se requiere que r sea par, sin embargo dicho survey propone un ataque de punto fijo basado en la transformada inversa cuántica de Fourier y la estimación de fase, este algoritmo se ejecuta en tiempo polinomial cuántico y no necesita factorizar explícitamente el módulo n y además no requiere que r sea par, esta propuesta asegura que la probabilidad de éxito sea mayor frente al algoritmo Shor, pero la complejidad del tiempo es la misma para ambos [23], [26].

- Experimental Analysis of Attacks on RSA Rabin Cryptosystems using Quantum Shor's Algorithm

  Este survey propone, cómo el algoritmo de Shor puede romper los algoritmos de de criptografía que se basan en factorización como el RSA y los algoritmos de Rabin usando IBM Quantum Experience, pero dicho experimento se hará con no más de 7 bits, puesto que IBM ofrece solo 32 qubits. El enfoque de dicho survey está en demostrar que el algoritmo de Quantum Shor representa un peligro para los criptosistemas asimétricos que utilizan productos de números primos grandes para la generación de claves [7].

- Quantum Grover Attack on the Simplified-AES

  Este survey presenta la forma de atacar el algoritmo estándar de cifrado avanzado simplificado (S-AES) usando el algoritmo de Grover, donde se construyen circuitos cuánticos para los componentes principales de S-AES para luego juntarlos y formar una versión cuántica de dicho algoritmo; de esta forma el S-AES se integra en una caja negra que pasara por el algoritmo de Grover y así recuperar la clave secreta en aceleración cuadrática [1].

- Variational quantum attacks threaten advanced encryption standard based symmetric cryptography

  Este survey propone un Variational Quantum Attack Algorithm (VQAA) para la criptografía simétrica AES (Advanced Encryption Standard), a su vez muestra cómo en ocasiones el VQAA es mucho más rápido que

el algoritmo de Grover utilizando el mismo orden de consultas de espacio de búsqueda, así como también muestran la relación entre la entropía de entrelazamiento, la concurrencia y la función de costo [22].

- A Variational Quantum Attack for AES-like Symmetric Cryptography

  En este artículo los autores usaron criptografía asimétrica como el RSA, para transmitir la clave secreta y criptografía simétrica, como Advanced Encryption Standard (AES), para cifrar datos. Con el desarrollo de las computadoras cuánticas, se ha dado más atención al análisis de seguridad de la criptografía clásica bajo ataques cuánticos. El algoritmo de Shor es capaz de descifrar la criptografía RSA en tiempo polinomial, lo que amenaza seriamente la seguridad de la criptografía asimétrica. Para la criptografía simétrica, el algoritmo de Grover puede encontrar la clave en un conjunto que tiene N entradas evaluando sólo el orden de $\sqrt{N}$ entradas. En dicho artículo los autores muestran las implementaciones cuánticas eficientes de AES y el Estándar de cifrado de datos (DES) se proponen basándose en menos recursos cuánticos, como qubits, puertas cuánticas y profundidades de circuitos. En la redacción de este artículo aún se encuentra en la era ruidosa de escala intermedia cuántica (NISQ), es decir, cuando los sistemas de computación cuántica se caracterizan por un bajo número de qubits, baja fidelidad y circuitos cuánticos poco profundos. Bajo estas restricciones, se han propuesto varios algoritmos híbridos cuánticos clásicos, incluido el algoritmo cuántico variacional (VQA) y el algoritmo de optimización aproximada cuántica (QAOA). Estos algoritmos híbridos tienen ventajas significativas para resolver problemas de optimización combinatoria y de estado fundamental hamiltoniano. En el diseño empleado por los autores, el circuito cuántico parametrizado (PQC) opera en el espacio clave y la función de costo está diseñada de acuerdo con el texto cifrado conocido, asi como también muestran mediante simulaciones que el VQAA, en promedio, utiliza el mismo orden de consultas de espacio de búsqueda que el algoritmo de Grover. Sin embargo, en algunos casos, es incluso más rápido que el algoritmo de Grover. También se investiga la relación entre la entropía de entrelazamiento, la concurrencia y la función de costo, y encontramos que la aceleración alcanzada está relacionada con la entropía, lo cual no es inesperado, porque la entropía por definición representa el grado específico de sorpresa al revelar un determinado solución del problema/resultado [25].

- Algebraic attacks on block ciphers using quantum annealing

  Este artículo presenta un método para la transformación de ecuaciones algebraicas de cifrado simétrico en el problema QUBO (Quadratic Unconstrained Binary Optimization). Después de dicha transformación, el problema QUBO obtenido puede resolverse utilizando el enfoque de recocido cuántico, especialmente en la computadora DWave. En primer lugar, se deben obtener ecuaciones algebraicas de cifrado. La idea aquí es la misma que en el caso de los ataques algebraicos. Después de obtener las ecuaciones booleanas del cifrado dado en forma algebraica normal, cada ecuación f debe transformarse en una ecuación de variables booleanas con coeficientes enteros. Después de la transformación de las ecuaciones dadas, se debe linealizar cada una, finalmente, uno puede obtener el problema en la forma QUBO. Los autores presentan los resultados de la transformación del cifrado AES-128 completo al problema QUBO, donde el número de variables del problema QUBO equivalente es igual a 237.915, lo que significa, al menos teóricamente, que el problema puede ser resuelto usando la computadora D-Wave Advantage. Desafortunadamente, es difícil estimar el tiempo que requeriría este proceso [4].

- Quantum Attack-Resistent Certificateless Multi-Receiver Signcryption Scheme

  Signcryption es una primitiva criptográfica que proporciona tanto la firma como el cifrado de forma simultánea a la información confidencial con una sobrecarga de cómputo y comunicación más baja que el enfoque tradicional de firma y luego cifrado, existen dos tipos de esquemas de cifrado de signos. Uno se basa en la infraestructura de clave pública tradicional, lo que provoca el costoso problema de gestión de certificados; el otro se basa en la criptografía de clave pública basada en la identidad, que evita la gestión de certificados, pero provoca el problema de custodia de claves. Hasta la fecha, las implementaciones de casi todos los esquemas de cifrado de firmas sin certificado se basan en criptosistemas de clave pública tradicionales, en los que la seguridad se basa principalmente en los problemas difíciles, como la descomposición de factores y el logaritmo discreto. Sin embargo, la computación cuántica ha supuesto un desafío potencial para estos difíciles problemas matemáticos. La criptografía de clave pública multivariante (MPKC), que puede resistir ataques cuánticos, es una de las soluciones alternativas para garantizar la seguridad de las comunicaciones en la era post cuántica. La seguridad de MPKC se basa en el problema Multivariante Cuadrático (MQ) y el problema de Isomorfismo de Polinomios (IP). En comparación con la criptografía basada en identidad, MPKC tiene una menor complejidad de cálculo y una mayor eficiencia, lo que hace que MPKC sea muy adecuado para implementar comunicaciones muy seguras para dispositivos de gama baja. Los esquemas basados en MPKC se han estudiado

ampliamente y se han propuesto varios esquemas excelentes. Por ejemplo, SFLASH, un esquema de firma basado en MPKC, ha sido recomendado por el Consorcio Europeo NESSIE desde 2003 como la solución más conocida para su implementación en tarjetas inteligentes de bajo costo. Los autores emplearon MPKC para construir un esquema de cifrado de firmas multireceptor sin certificado resistente a ataques cuánticos eficiente, que combina el criptosistema sin certificado y MPKC. El nuevo esquema no solo tiene la ventaja del criptosistema sin certificado, que evita el problema de la gestión de claves, sino que también resiste el ataque cuántico solo con cómputo liviano como las operaciones polinómicas cuadráticas multivariadas. En el esquema, las operaciones polinómicas cuadráticas multivariantes, que tienen una complejidad de cálculo menor que las operaciones de emparejamiento bilineal, se emplean para encriptar un mensaje para un cierto número de receptores. Por lo tanto, el esquema presentado en el paper es más eficiente que los esquemas CLMSC existentes y es adecuado para terminales móviles con bajo poder de cómputo. El análisis de seguridad muestra que nuestro esquema es un esquema seguro de encriptación de firmas de múltiples receptores basado en MPKC, y también tiene importantes propiedades de seguridad, como la confidencialidad del mensaje, la imposibilidad de falsificar, el no repudio, el secreto perfecto hacia adelante, el secreto perfecto hacia atrás y la verificabilidad pública [11].

- Quantum Attacks on 1K-AES and PRINCE

  Evidentemente, la investigación del criptoanálisis cuántico es importante tanto en la teoría como en las aplicaciones, ya que estimula el desarrollo de la criptografía post cuántica. En este paper los autores estudiaron el ataque de deslizamiento cuántico en 1K-AES (1K-Advanced Encryption Standard) y el ataque de clave relacionada cuántica en PRINCE. Las principales contribuciones de este trabajo incluyen los siguientes dos aspectos. 1. Proponen el ataque deslizante cuántico en 1K-AES mediante la introducción del algoritmo BHT (Brassard-Høyer-Tapp). Implica que el ataque de deslizamiento cuántico también podría aplicarse en la construcción de la red de permutación de sustitución (SPN), además del cifrado de Even-Mansour iterado y las construcciones de Feistel. En el ataque cuántico propuesto, generalizan el algoritmo BHT a la situación en la que no se conoce de antemano el número de elementos marcados. Además, proporcionan un esquema de implementación del oráculo clasificador basado en el algoritmo de estimación de fase cuántica. El ataque cuántico que presentan los autores en este artículo puede lograr una aceleración sub-cuadrática con la misma probabilidad de éxito sin importar la complejidad de la consulta, la complejidad del tiempo o la complejidad de la memoria. Además, el ataque de deslizamiento cuántico propuesto en 1K-AES reduce la complejidad de la consulta en un factor de $2^{\frac{n}{6}}$ en comparación con la búsqueda de Grover en 1K-AES. 2. Los autores del artículo afirman que el algoritmo BHT generalizado también podría introducirse en el ataque de clave relacionada en PRINCE. Por lo tanto, este ataque también es propuesto, ya que, puede recuperar la primera subclave; la complejidad de la consulta, la complejidad del tiempo y la complejidad de la memoria son $O(2^{\frac{n}{3}})$ cuando la probabilidad de éxito es de alrededor del 63%. Después de recuperar la primera subclave, la otra subclave se puede recuperar mediante la búsqueda de Grover. Por lo tanto, la complejidad de la consulta aumenta a $O(2^{\frac{n}{2}})$ cuando consideramos todo el ataque cuántico a PRINCE. En comparación con la búsqueda de Grover en PRINCE, la complejidad de la consulta de todo el ataque cuántico se reduce de $O(2^n)$ a $O(2^{\frac{n}{2}})$. Cuando se compara con la combinación de los algoritmos de Grover y Simon en PRINCE, la complejidad de la consulta de este ataque se reduce de $O(n.2^{\frac{n}{2}})$ a $O(2^{\frac{n}{2}})$ [5].

- Quantum Polynomial-Time Fixed-Point Attack for RSA

  Es bien sabido que la seguridad de RSA depende esencialmente solo de la intratabilidad computacional del problema de factorización de enteros (IFP) y, en particular, solo se asegura si el IFP no tiene un algoritmo eficiente. Es decir, cualquiera que pueda resolver el IFP en tiempo polinomial puede romper el sistema criptográfico RSA en tiempo polinomial. Existen muchos métodos para atacar RSA, como los ataques de factorización de enteros, los ataques de logaritmos discretos, los ataques de exponente público, los ataques de exponente privado y los ataques de canal lateral. El método más poderoso para descifrar RSA en una computadora clásica es usar el NFS (Number Field Sieve) para factorizar n, que se ejecuta en tiempo subexponencial $\mathcal{O}(exp(c(n)^{\frac{1}{3}})(\log\log n)^{\frac{2}{3}})$, donde mi $C \approx 1.92$. Sin embargo, un algoritmo de factorización cuántica en tiempo polinomial, propuesto por Shor en 1994, puede resolver el IFP en un tiempo proporcional a $\mathcal{O}((\log n)^{2+\varepsilon})$. Investigaciones recientes han buscado reducir la cantidad de bits cuánticos y facilitar su ejecución en una computadora cuántica con menos bits cuánticos. Sin embargo, se sabe desde hace mucho tiempo que no hay necesidad de factorizar n si el único objetivo es atacar RSA. De hecho, para recuperar M de C, basta calcular el orden, r, del punto fijo C. Una vez que se ha encontrado el orden r, el texto sin formato M es simplemente el elemento $C^{e^{r-1}} \mod n$. En la computación clásica, este cálculo es equivalente a factorizar n, que se cree que es difícil. En este artículo, los autores presentaron un nuevo algoritmo cuántico de tiempo polinomial que se puede usar para atacar RSA

sin factorizar el módulo n [24].

- Quantum attacks on pseudorandom generators

  Un generador aleatorio es un sistema cuya salida consiste en secuencias numéricas totalmente impredecibles. Dichos generadores se componen de dos elementos:
  - Un fenómeno no determinista
  - Un post-procesador que comprime la secuencia previamente producida para minimizar defectos estadísticos.

  Los generadores pseudoaleatorios son algoritmos deterministas y recursivos y estos juegan un papel importante en la criptografía. Las claves de sesión, los vectores de inicialización, las sales que se codifican con contraseñas y los parámetros únicos en las firmas digitales son ejemplos de la aplicación criptográfica de los generadores pseudoaleatorios. Se han propuesto varios algoritmos de computación cuántica eficientes para problemas en los que no se conoce un algoritmo de computación clásica de tiempo polinomial. En este artículo, los autores presentan un ataque cuántico al generador de Blum-Micali, que es un generador pseudoaleatorio criptográficamente seguro que ha sido ampliamente adoptado en los criptosistemas. El ataque propuesto se compone de tres etapas: la segunda etapa es un procedimiento inspirado en Grover y la tercera etapa utiliza el algoritmo de logaritmo discreto de Shor. Como resultado de este ataque, la salida anterior y futura del generador se vuelve predecible, comprometiendo así por completo la seguridad del generador [6].

VI. Análisis de fortalezas y debilidades

Si bien la computación cuántica ha avanzado dramáticamente durante la última década, sus aplicaciones potenciales aún no se han demostrado a gran escala. Es probable que tales demostraciones requieran avances en física, informática e ingeniería, ya que, las computadoras cuánticas son propensas a errores debido a la coherencia cuántica y las condiciones ambientales [20].

Por otro lado, se dice que en el futuro, una computadora cuántica (QC) puede resolver algunos problemas mucho más rápido que una computadora clásica (CC), lo que se denomina ventaja cuántica, esto se debe a que la potencia de cómputo de QC está creciendo más rápido que la de CC. Una de las medidas del rendimiento de la Computadora Cuántica introducida por IBM es el Volumen Cuántico. Para lograr una ventaja cuántica en la próxima década, IBM declaró que "necesitan al menos duplicar el volumen cuántico de nuestros sistemas de computación cuántica cada año." En enero de 2020, Chow y Gambetta confirmaron que IBM está en camino de alcanzar este objetivo con una nueva computadora cuántica de 28 qubits que demuestra el volumen cuántico de 32 [28].

- *Ataque a la criptografía asimétrica*

  Todos los algoritmos asimétricos actuales (RSA, ECC, DH, DSA) se pueden descifrar mediante computadoras cuánticas. Se basan en el problema de factorización prima o el problema del logaritmo discreto, que son fáciles de resolver en computadoras cuánticas utilizando el algoritmo de Shor. Matemáticos y criptógrafos utilizaron estos problemas de teoría de números para fundamentar la seguridad de los algoritmos asimétricos. Ahora tienen que buscar nuevos problemas matemáticos que las computadoras cuánticas no puedan resolver fácilmente [2].

  Actualmente todos los algoritmos asimétricos se basan en problemas matemáticos para los que la gente ha buscado soluciones durante siglos. Sin embargo, la debilidad que tienen es que las computadoras cuánticas son buenas en tareas paralelas que requieren un resultado al final. Dado que los algoritmos requieren solo un resultado al final, se puede usar una superposición de qubits para paralelizar todos los cálculos y luego se puede medir el resultado. Para evitar aprovechar el paralelismo de las computadoras cuánticas se pueden utilizar algoritmos que requieren varios resultados. De esta manera, el paralelismo de las computadoras cuánticas no se puede utilizar en toda su extensión [2].

- *Ataque a la criptografía simétrica*

  Los algoritmos simétricos y las funciones hash son relativamente seguros en un mundo poscuántico. El algoritmo de Grover puede acelerar los ataques por complejidad de raíz cuadrada, sin embargo, la mayoría de los algoritmos se pueden volver a asegurar duplicando el tamaño de la clave [2]. Cuando se consideran aplicaciones del algoritmo de Grover, se debe enfatizar que la base de datos no se representa explícitamente. En cambio, se invoca un oráculo para evaluar un elemento por su índice. Leer una base de datos completa elemento por elemento y convertirlo en una representación de este tipo puede llevar mucho más tiempo que la búsqueda de Grover. Para tener en cuenta tales efectos, el algoritmo de Grover se puede considerar como una solución a una ecuación o una restricción. En tales aplicaciones, el oráculo es una forma de verificar la restricción y no está relacionado con el algoritmo de búsqueda. Esta separación generalmente evita las optimizaciones algorítmicas, mientras que los algoritmos de búsqueda convencionales a menudo se basan en tales optimizaciones y evitan la búsqueda exhaustiva [20].

Algunas limitaciones importantes de la computadora cuántica de IBM [20]:

- Problemas de coherencia:

  El dispositivo debe luchar constantemente contra el

entorno que actúa para degradar la coherencia del sistema. Y, por lo tanto, la delicada información cuántica almacenada en una computadora cuántica es extremadamente susceptible al ruido. Los qubits deben mantenerse fríos o de lo contrario colapsarán fácilmente. El error debido al entrelazamiento de qubits es alto. Los errores de puerta multiqubit fueron mucho más altos que los errores de puerta de un solo qubit.

- La conectividad limitada entre los qubits:

  Esta es otra de las limitaciones más importante, por lo tanto, existe la necesidad de emplear un gran número. de compuertas de intercambio que aumenta el conteo de compuertas (lo que se suma a los errores de compuerta) especialmente los cnots que tienen errores bastante altos y, por lo tanto, reducen en gran medida la fidelidad de estado esperada y también los circuitos se vuelven complejos y difíciles de comprender y depurar.

Los simuladores de IBM ya tienen una longitud de código limitada (comparativamente, LIQ$Ui|\rangle$ y Quirk Quantum Simulator tienen longitudes de código relajadas), por lo que se vuelve difícil implementar circuitos grandes o ampliar los circuitos para agregar puertas de corrección de errores o resolver el problema de la conectividad limitada agregando más intercambio. puertas. La implementación de la puerta tofolli para 16 qubits requirió muchos qubits adicionales o una gran cantidad de etapas, las cuales no son posibles en los dispositivos IBM actuales y, por lo tanto, implementar la búsqueda de Grover de 16 qubits en los simuladores de IBM y los dispositivos reales no era realista [20].

VII. Conclusiones

La criptografía cuántica es un campo que recientemente está emergiendo y de manera rápida. Muchas compañías alrededor del mundo están invirtiendo recursos para aumentar el conocimiento y las prácticas que se tiene actualmente con respecto a la seguridad post cuántica. Dado los múltiples intereses y estudios, es necesario comprender el énfasis actual en la seguridad cuántica y los avances actuales en este campo. Los algoritmos de clave simétrica son tanto clásicos como resistentes a la cuántica (se ha utilizado AES-256 para caracterizar el nivel más alto de seguridad para todos los algoritmos nuevos), pero son difíciles de implementar en circuitos cuánticos, especialmente considerando que la maquinaria cuántica se ha desarrollado solo para un tamaño de mensaje muy pequeño (aproximadamente 20 bits) [2].

Los avances adicionales en la tecnología basada en la mecánica cuántica podrían conducir a una expansión de estas capacidades, lo que daría como resultado formas mejores y más eficientes de implementar criptosistemas simétricos como AES. Para los criptosistemas simétricos, las formas cuánticas de descifrar el algoritmo requieren un oráculo cuántico. Siempre que la criptografía simétrica no se implemente con oráculos cuánticos, están a salvo de los ataques cuánticos. Todos nuestros datos clásicos actuales están seguros. Sin embargo, las implicaciones de la computación cuántica en el criptosistema de clave pública son mucho más serias, ya que, no se requiere una implementación cuántica de los algoritmos para descifrarlo. Un adversario con recursos cuánticos locales puede explotar y descifrar los algoritmos de cifrado. Esto hace que todos los datos cifrados asimétricos sean inseguros y susceptibles a ataques cuando se construyen computadoras cuánticas eficientes. A partir de ahora, los algoritmos cuánticos ya existen para todos los principales criptosistemas de clave pública y es solo cuestión de tiempo antes de que se rompan por completo. Los investigadores han estado tratando de encontrar formas de aumentar la dureza de los problemas que se están utilizando actualmente (RSA, Elliptic Curve Cryptography) o generar nuevos problemas que sean lo suficientemente difíciles incluso para una computadora cuántica. Sin embargo, muchos algoritmos que se proponen, son difíciles de implementar y su rendimiento debe optimizarse para un uso público generalizado [2].

En 2017, NIST (National Institute of Standards and Technology) emitió una convocatoria de algoritmos en todo el mundo para poder determinar un estándar para la criptografía de clave pública en el futuro. Identificó que la necesidad de definir un sistema se acercaba rápidamente, con base en el criterio de que el tiempo de implementación junto con el desarrollo de los algoritmos no debe exceder al de desarrollo de sistemas que puedan romper los criptosistemas actualmente en uso [2].

References

[1] Mishal Almazrooie et al. “Quantum Grover Attack on the Simplified-AES”. In: *Proceedings of the 2018 7th International Conference on Software and Computer Applications*. ICSCA 2018. Kuantan, Malaysia: Association for Computing Machinery, 2018, pp. 204–211.

[2] Ritik Bavdekar et al. “Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research”. In: *CoRR* abs/2202.02826 (2022). arXiv: 2202.02826.

[3] Dagmar Bruss et al. “Quantum Cryptography: A Survey”. In: *ACM Comput. Surv.* 39.2 (2007), 6–es.

[4] Elżbieta Burek et al. “Algebraic Attacks on Block Ciphers Using Quantum Annealing”. In: *IEEE Transactions on Emerging Topics in Computing* 10.2 (2022), pp. 678–689.

[5] Binbin Cai et al. “Quantum Attacks on 1K-AES and PRINCE”. In: *The Computer Journal* (Feb. 2022).

[6] Elloá Guedes, Francisco de Assis, and BERNARDO LULA. “Quantum attacks on pseudorandom generators”. In: *Mathematical Structures in Computer Science* 23 (June 2013).

[7] Babita Jajodia and Ritu Thombre. “Experimental Analysis of Attacks on RSA Rabin Cryptosystems using Quantum Shor’s Algorithm”. In: Apr. 2021.

[8] Phillip Kaye, Raymond Laflamme, and Michele Mosca. “ALGORITHMS BASED ON AMPLITUDE AMPLIFICATION”. In: (Nov. 2006), pp. 152–163.

[9] Phillip Kaye, Raymond Laflamme, and Michele Mosca. “INTRODUCTION AND BACKGROUND and LINEAR ALGEBRA AND THE DIRAC NOTATION”. In: (Nov. 2006), pp. 01–37.

[10] Phillip Kaye, Raymond Laflamme, and Michele Mosca. “Introductory Quantum Algorithms”. In: (Nov. 2006), pp. 94–99.

[11] Huixian Li et al. “Quantum Attack-Resistent Certificateless Multi-Receiver Signcryption Scheme”. In: *PloS one* 8 (June 2013), e49141.

[12] Richard J. Lipton and Kenneth W. Regan. “Grover’s Algorithm”. In: *Quantum Algorithms via Linear Algebra: A Primer*. 2014, pp. 115–128.

[13] Daniel Neuenschwander. “3 Factorization with Quantum Computers: Shor’s Algorithm”. In: *Probabilistic and Statistical Methods in Cryptology: An Introduction by Selected Topics*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 37–45.

[14] Nick Papanikolaou. “An Introduction to Quantum Cryptography”. In: *XRDS* 11.3 (2005), p. 3.

[15] Renato Portugal. “Deutsch’s Algorithm”. In: (Sept. 2022), pp. 26–31.

[16] Renato Portugal. “Quantum Circuits ”. In: (Sept. 2022), pp. 03–24.

[17] Renato Portugal. “Shor’s Algorithm for Factoring Integers ”. In: (Sept. 2022), pp. 56–74.

[18] Eleanor Rieffel and Wolfgang Polak. “An Introduction to Quantum Computing for Non-Physicists”. In: *ACM Comput. Surv.* 32.3 (2000), pp. 300–335.

[19] Jacob Hammond Shlomo Kashani Maryam Alqasemi. “A quantum Fourier transform (QFT) based note detection algorithm”. In: (Apr. 2022), pp. 4–8.

[20] Akanksha Singhal and Arko Chatterjee. *Grover’s Algorithm*. July 2018. DOI: 10.13140/RG.2.2.30860.95366.

[21] Kapil Kumar Soni and Akhtar Rasool. “Cryptographic Attack Possibilities over RSA Algorithm through Classical and Quantum Computation”. In: *2018 International Conference on Smart Systems and Inventive Technology (ICSSIT)*. 2018, pp. 11–15.

[22] Y. Wang, H. Zhang, and H. Wang. “Quantum Algorithm for Attacking RSA Based on the eth Root”. In: *Gongcheng Kexue Yu Jishu/Advanced Engineering Science* 50 (2018), pp. 163–169.

[23] Yahui Wang, Huanguo Zhang, and Houzhen Wang. “Quantum polynomial-time fixed-point attack for RSA”. In: *China Communications* 15.2 (2018), pp. 25–32.

[24] Yahui Wang, Huanguo Zhang, and Houzhen Wang. “Quantum polynomial-time fixed-point attack for RSA”. In: *China Communications* 15.2 (2018), pp. 25–32.

[25] ZeGuo Wang et al. “A Variational Quantum Attack for AES-like Symmetric Cryptography”. In: (May 2022).

[26] WANG, Yahui and ZHANG, Huanguo. “Quantum Algorithm for Attacking RSA Based on Fourier Transform and Fixed-Point”. In: *Wuhan Univ. J. Nat. Sci.* 26.6 (2021), pp. 489–494.

[27] Guoliang Xu et al. “Improving the Success Probability for Shor’s Factorization Algorithm”. In: *Reversibility and Universality: Essays Presented to Kenichi Morita on the Occasion of his 70th Birthday*. Ed. by Andrew Adamatzky. Cham: Springer International Publishing, 2018, pp. 447–462.

[28] Lei Zhang, Andriy Miranskyy, and Walid Rjaibi. *Quantum Advantage and Y2K Bug: Comparison*. July 2019.