COMPUTACIÓN CUÁNTICA: ATÁQUE 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 [5].

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 [5].

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, DES, AES; 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 [4]. 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 [2].

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 el problema de logaritmos discretos en tiempo polinomial [7]. 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 [8]:

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. 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 [6].

- 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 [8], [9].

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

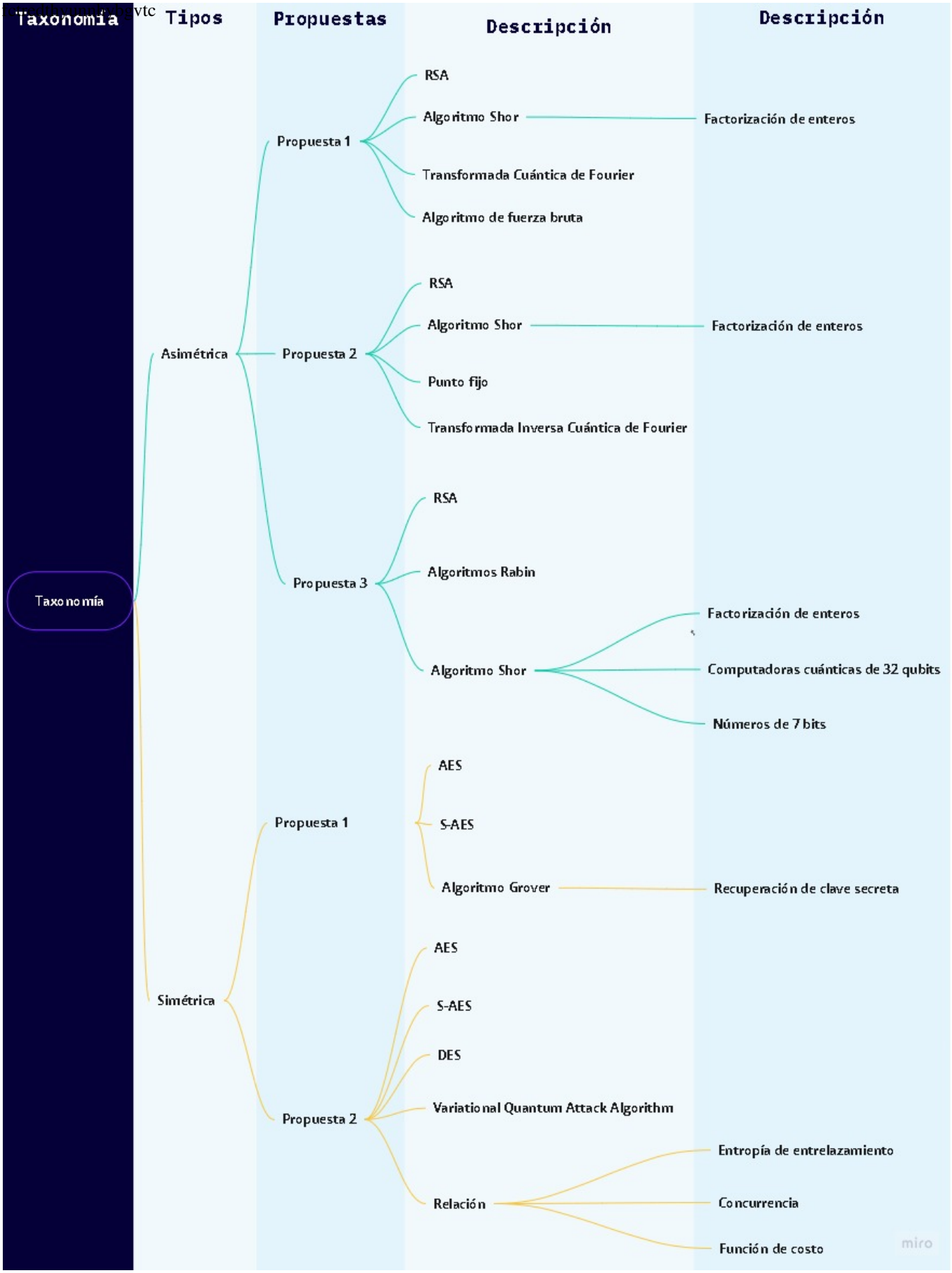
  Este survey propone, cómo el algoritmo de Shor puede romper los algoritmos de de criptografía que se basan en factorización como el RSA y los algoritmos de Rabin usando IBM Quantum Experience, pero dicho experimento se hará con no más de 7 bits, puesto que IBM ofrece solo 32 qubits. El enfoque de dicho 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 [3].

- 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 [7].


Taxonomía
Tipos
Propuestas
Descripción
Descripción
Taxonomía
Asimétrica
Propuesta 1
RSA
Algoritmo Shor
Factorización de enteros
Transformada Cuántica de Fourier
Algoritmo de fuerza bruta
Propuesta 2
RSA
Algoritmo Shor
Factorización de enteros
Punto fijo
Transformada Inversa Cuántica de Fourier
Propuesta 3
RSA
Algoritmos Rabin
Algoritmo Shor
Factorización de enteros
Computadoras cuánticas de 32 qubits
Números de 7 bits
Simétrica
Propuesta 1
AES
S-AES
Algoritmo Grover
Recuperación de clave secreta
Propuesta 2
AES
S-AES
DES
Variational Quantum Attack Algorithm
Relación
Entropía de entrelazamiento
Concurrencia
Función de costo
miro

fctredthyunnhybgvtc

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

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

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

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

[6] 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.

[7] 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.

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

[9] 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.