Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Harold Alejandro Villanueva Borda
Título del ejercicio:	CS401 [Turnitin hasta domingo 11/Diciembre 23:59h] Evalua...
Título de la entrega:	Computacion cuantica ataque a la criptografia clasica
Nombre del archivo:	33702_Harold_Alejandro_Villanueva_Borda_Computacion_cu...
Tamaño del archivo:	311.48K
Total páginas:	11
Total de palabras:	7,333
Total de caracteres:	39,243
Fecha de entrega:	05-dic.-2022 05:05a. m. (UTC-0800)
Identificador de la entre...	1971983486

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*—Actualmente la criptografía clásica protege el intercambio de información, sin embargo los avances de la computación cuántica pone en peligro dicha protección,ya que, con los nuevos algoritmos cuánticos se ha demostrado que es posible vulnerar y romper muchos criptosistemas clásicos, ya sea asimétrico o simétrico. En este survey se mostrará diferentes técnicas que son usadas para resolver problemas como la factorización de número grandes, logaritmos discretos, y con un tiempo polinomial; con la finalidad de romper criptosistemas simétricos y asimétricos como DES (Data Encryption Standard) y RSA (Rivest, Shamir y Adleman).**

***Index Terms*—Criptografía, Seguridad y Privacidad, QFT, Algoritmo de Shor, Algorítmo Grover, RSA, DES, AES**

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