ACTIVIDAD COLABORATIVA: CRIPTOGRAFÍA CUÁNTICA

Realizado por: **Grupo 2**

1. Raúl Manrubia Mateo (Responsable)
2. Marian Ares Alonso (Responsable)
3. Ricardo Adrián Ramos Rivero
4. Manuel Vidal Lozano
5. Sergio Jiménez Palacios
6. Hugo Díaz García
7. Javier García Cambronel
8. Melisa Duro Maneiro

1. Introducción

Actualmente existen algoritmos (Shor, Grover, Temple, etc…) que aplicados sobre computadores cuánticos de altas prestaciones serían capaces de romper los cifrados clásicos (pública y privada), mediante fuerza bruta, hallando su logaritmo discreto, etc. al igual que la seguridad de las funciones resumen. Dentro de la criptografía cuántica, existe una versión evolucionada del cifrado de Vernam, que sustituye la transmisión de la clave secreta a través de correo seguro por transmisión fotónica, a través de fibra óptica como B92 o BB84. Para llevar a cabo una transmisión segura estos sistemas necesitas unas condiciones físicas muy precisas para no generar error, que en el mundo real cuesta reproducir.

Cabe destacar que estos sistemas no son resistentes ataques por intromisión y por tanto necesitan un mecanismo de autenticación por clave secreta (WEG81).Por otra parte los algoritmos de cifrado que se están utilizando actualmente se idearon para los avances de los ordenadores cuánticos a base de utilizar claves mucho más largas de las requeridas para garantizar la seguridad frente a ataques con ordenadores clásicos como, Advanced Encryption Standard (AES) para cifrado en bloque resultaría hoy seguro con una clave de 100 bits de longitud, pero está diseñado para usar claves de hasta 256 bits.

2. Algoritmos cuánticos

El mayor riesgo de los algoritmos de clave pública más populares hoy en día es que se basan en tres problemas matemáticos: factorización de números enteros, el problema del logaritmo discreto y el problema de curvas-elípticas. Y estos tres problemas se pueden resolver por un computador cuántico que ejecute el Algoritmo de Shor. Sin embargo, la mayoría de algoritmos de cifrado simétrico y funciones de hash son considerados seguros ante la irrupción de la computación cuántica. Pese a que el Algoritmo de Grover acelere los ataques a los cifradores simétricos, se pueden considerar seguros doblando el tamaño de las claves. Por lo tanto, la criptografía simétrica post-cuántica no debe diferir mucho de la actual.

2.1 Algoritmo de Shor

El Algoritmo de Shor es un algoritmo propuesto por Peter Shor en 1994, el cual permite descomponer en factores primos un número N cualquiera, en tiempo O ((log N)3) y espacio O(log/V), por lo cual si se implementara en un ordenador cuántico, los sistemas criptográficos basados en procesos de factorización, como el sistema de clave pública RSA, quedarían obsoletos. Los algoritmos clásicos conocidos no pueden realizar la factorización en tiempo O ((log N)k) para ningún *k* , mientras que con el Algoritmo de Shor se podría realizar en tiempo super polinómico. Hasta el momento solo se han podido realizar pruebas en ordenadores cuánticos con un pequeño número de bits, por lo cual solo se ha probado a factorizar números pequeños. Es un algoritmo probabilístico: da la respuesta correcta con alta probabilidad, y la probabilidad de fallo puede ser disminuida repitiendo el algoritmo.

El Algoritmo de Shor consiste en dos partes:

1. Una reducción del problema de descomponer en factores al problema de encontrar el orden, que se puede hacer en una computadora clásica.

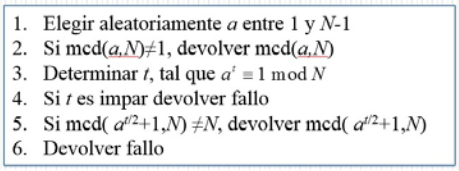

1. Elegir aleatoriamente a entre 1 y N-1
2. Si mcd(a,N)≠1, devolver mcd(a,N)
3. Determinar t, tal que $a^t \equiv 1 \bmod N$
4. Si t es impar devolver fallo
5. Si mcd($a^{t/2}$+1,N) ≠N, devolver mcd($a^{t/2}$+1,N)
6. Devolver fallo

Imagen tomada de documento del grupo GIEMATIC (UPM) (ver bibliografía)

2. Un algoritmo cuántico para solucionar el problema de encontrar el periodo, usando la transformada de Fourier cuántica, y es responsable de la aceleración cuántica.

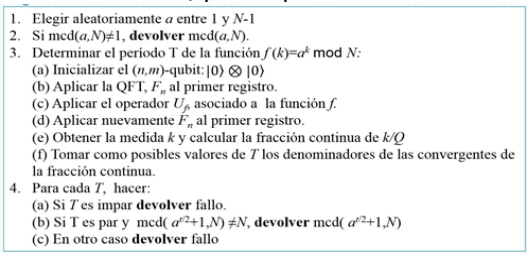

1. Elegir aleatoriamente a entre 1 y N-1
2. Si mcd(a,N)≠1, **devolver** mcd(a,N).
3. Determinar el período T de la función $f(k)=a^k \bmod N$:
   (a) Inicializar el (n,m)-qubit: $|0\rangle \otimes |0\rangle$
   (b) Aplicar la QFT, F_n al primer registro.
   (c) Aplicar el operador U_f, asociado a la función f.
   (d) Aplicar nuevamente F_n al primer registro.
   (e) Obtener la medida k y calcular la fracción continua de k/Q
   (f) Tomar como posibles valores de T los denominadores de las convergentes de la fracción continua.
4. Para cada T, hacer:
   (a) Si T es impar **devolver** fallo.
   (b) Si T es par y mcd($a^{t/2}$+1,N) ≠N, **devolver** mcd($a^{t/2}$+1,N)
   (c) En otro caso **devolver** fallo

Imagen tomada de documento del grupo GIEMATIC (UPM) (ver bibliografía)

2.2 Algoritmo de Grover

En computación cuántica, el algoritmo de Grover es un algoritmo cuántico para la búsqueda en una secuencia no ordenada de datos con N componentes en un tiempo O (N1/2), y con una necesidad adicional de espacio de almacenamiento de O(logN) (véase notación O). Fue enunciado por Lov K. Grover en 1996.

En una búsqueda normal de un dato, si tenemos una secuencia desordenada se debe realizar una inspección lineal, que necesita un tiempo de O (N), por lo que el algoritmo de Grover es una mejora bastante sustancial, evitando, además, la necesidad de la ordenación previa. La ganancia obtenida es "sólo" de la raíz cuadrada, lo que contrasta con otras mejoras de los algoritmos cuánticos que obtienen mejoras de orden exponencial sobre sus contrapartidas clásicas.

Al igual que otros algoritmos de naturaleza cuántica, el algoritmo de Grover es un algoritmo de carácter probabilístico, por lo que produce la respuesta correcta con una determinada probabilidad de error, que, no obstante, puede obtenerse tan baja como se desee por medio de iteraciones.

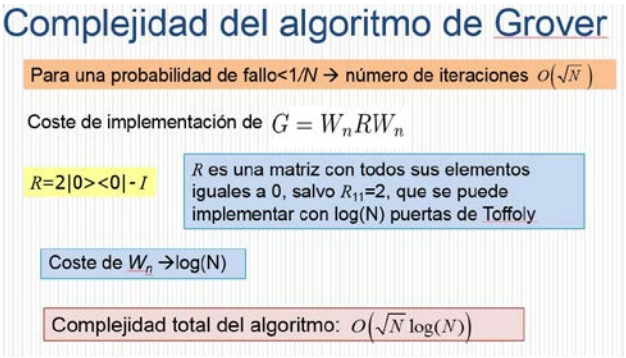


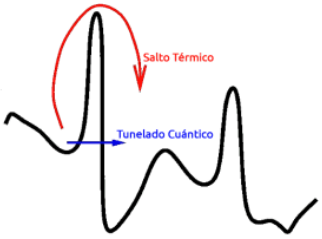
Imagen tomada de documento del grupo GIEMATIC (UPM) (ver bibliografía)

2.3 Algoritmo del temple cuántico

Es una analogía de cómo se ordenan las moléculas en los metales y/o cristales cuando se suceden procesos físicos que fuerzan a que estos se enfríen lentamente y a velocidad constante. El modelo resultante apenas tiene impurezas y se ordena con el menor gasto energético posible (minimización de energía en el sentido de Helmholtz).

El temple cuántico o “Quantum annealing” se trata de una aproximación de la computación cuántica orientada a hacia problemas de muestreo u optimización. Entiéndase optimización como la búsqueda de la mejor solución sobre una gran cantidad de posibles combinaciones debido a procesos multivariables. La versión clásica de este algoritmo, conocida

como temple simulado, lo que hace es provocar alteraciones térmicas en los estados para verificar si atraviesan una barrera de potencial. El temple cuántico aprovecha el efecto túnel, para cruzar barreras de potencial por lo que proporcionará más aceleración cuando el perfil de la función esté compuesto por mínimos en valles separados por crestas altas y estrechas. Una analogía ingeniosa del temple cuántico puede visualizarse en el vídeo de este enlace: https://www.youtube.com/watch?v=PqzLM3I9pcM.



Fluctuación cuántica: Puente Cuántico - Fuente: lapastillaroja.net

Al igual que el Temple Simulado, el Temple cuántico reduce en gran medida la complejidad del cómputo al aplicar el algoritmo de Montecarlo (gran repetición probabilística aleatoria)

3. Contramedidas

Existen varias clases de sistemas criptográficos que actualmente se cree que resisten la computación cuántica, como pueden ser:

- **Criptografía basada en enrejado (lattice based):** Incluye sistemas criptográficos que soportan firmas digitales e intercambio de claves. Algunos ejemplos son NTRU4, NTRU MLS (sin ataque conocido), LWE o ring-LWE, los cuales permiten tamaños de clave pequeños.
- **Criptografía de ecuaciones cuadráticas y multivariantes:** Normalmente sólo se admite en firmas. Ecuaciones de campo ocultas (HFE) son un ejemplo de esta clase de criptografía, al igual que el esquema Rainbow. Aunque varios sistemas de cifrado basado en ecuaciones multivariables han fracasado, Rainbow podría proporcionar las bases para firma digital a prueba de ataques cuánticos.
- **Criptografía basada en hash:** Se trata de firmas digitales construidas con funciones hash. Incluye sistemas criptográficos como las firmas Lamport y el esquema de firmas Merkle. La firma digital basada en funciones hash fue introducida en los 70 y ha sido estudiada desde entonces como una alternativa a los basados en números teóricos como RSA y DSA. en Entre las variantes modernas se incluyen SPHINCS y XMSS.
- **Criptografía basada en código:** Sistemas que se basan en códigos de corrección de errores y apoya el intercambio de claves, pero no es práctico en la actualidad para la firma. Ha sido mucho más exitosa en esquemas de cifrado que en firma. Como ejemplos de cifrado basado en código tenemos los criptosistemas McEliece y Niederreiter y sus variantes tales como PQGuard, Wild McEliece y McBits. La Comisión Europea ha recomendado el sistema de cifrado de clave pública McEliece como candidato para la protección a largo plazo frente a los computadores cuánticos.
- **Criptografía Isogenética de la Curva Elíptica Supersingular:** Por lo general sólo admite el cifrado. Funciona de forma parecida a las implementaciones Diffie-Hellman, por lo tanto, este sistema criptográfico crea un reemplazo potencial de tipo Diffie-Hellman con secreto.

Todos estos algoritmos y técnicas son teóricamente seguros frente a los algoritmos cuánticos existentes hoy en día. No obstante, surgió la necesidad de comenzar a pensar e implementar algoritmos post cuánticos para proteger, por ejemplo, todo el tráfico en Internet, vulnerable a posibles ataques cuánticos. Es por ello por lo que, a raíz de todo esto, surge el proyecto Open Quantum Safe (OQS), con el fin de apoyar el desarrollo y la creación de prototipos de criptografía resistentes a la cuántica.

4. Conclusiones.

Por último, decir que a la criptografía cuántica todavía le queda por hacer un gran trabajo de investigación, dado que actualmente es un híbrido entre mecanismos clásicos y cuánticos. El objetivo por tanto es conseguir algoritmos criptográficos seguros totalmente cuánticos que sean fiables. No obstante, todos los avances que se realicen en este campo estarán a disposición tanto de los criptoanalistas como los fabricantes de algoritmos de cifrado. El trabajo de un criptoanalista descifrando datos con algoritmos convencionales se vería drásticamente reducido, pero al mismo tiempo se empezarán a cifrar datos con potentísimos algoritmos de cifrado cuántico, por lo que el equilibrio entre el cifrado y el criptoanálisis estaría en la misma situación que hoy en día.

5. Bibliografía Y Webgrafía

INTRODUCCIÓN:

- La criptografía cuántica, ¿realidad o ficción?1. Disponible en: https://www.researchgate.net/publication/255601730_La_criptografia_cuantica_realidad_o_ficcion1
- ¿Hay criptografía después del gato? Disponible en https://www.incibe-cert.es/blog/hay-criptografia-despues-del-gato

ALGORITMOS CUÁNTICOS

- Algoritmo de Shor: Disponible en: https://es.wikipedia.org/wiki/Algoritmo_de_Shor#Teorema_1
- Imágenes Algoritmo Shor: Disponible en: http://www.giematic.eui.upm.es/images/pdf/Cuant/Leccion3_Algoritmos.pdf.
- Algoritmo de Grover: Dr. Grov K. Grover [2007] Quantum algorithms_8 Dr Lov. Grover. Disponible en: https://www.youtube.com/watch?v=rhSZLYB1ihs.
- Algoritmo de Grover: Disponible en: https://es.wikipedia.org/wiki/Algoritmo_de_Grover
- Imagen algoritmo de Grover: Disponible en: http://www.criptored.upm.es/crypt4you/temas/cuantica/leccion3/leccion03.html
- *The simulated annealing algorithm explained with an analogy to a toy*. Disponible en: https://www.youtube.com/watch?v=eBmU1ONJ-os.
- *How The Quantum Annealing Process Works*. Disponible en: https://www.youtube.com/watch?v=UV_RlCAc5Zs&index=2&list=PLPvKnT7dgEsvVQwGgrlUVXBa2J6PAW8a4.
- Quantum annealing, descripción del método algorítmico. Disponible en: https://es.scribd.com/document/75391263/Quantum-annealing-descripcion-del-metodo-algoritmico.
- Temple paralelo - Estado del arte. Disponible en: https://es.scribd.com/document/66288537/Temple-paralelo-Estado-del-arte.
- Computación cuántica para torpes. Disponible en: https://lapastillaroja.net/2016/09/computacion-cuantica/

CONTRAMEDIDAS y CONCLUSIÓN:

- El fin de la seguridad con las computadoras cuánticas. Disponible en: https://latam.kaspersky.com/blog/el-fin-de-la-seguridad-con-las-computadoras-cuanticas/1453/
- La criptografía post-quantum. Disponible en: https://ciberseguridad.blog/la-criptografia-post-quantum/
- Open Quantum Safe. Disponible en: https://openquantumsafe.org/