Calificación: 100

Módulo 1 - Tarea Colaborativa 2 - Grupo 3
Algoritmos cuánticos como amenaza a los criptosistemas modernos

1. Estado del Arte

Algoritmos cuánticos

La computación cuántica supone una revolución en ell campo de la ciberseguridad, al permitir, en teoría, romper muchos de los algoritmos de cifrado actuales, en especial los de clave pública, ya que puede realizar operaciones de factorización a una velocidad muchísimo más rápida que los ordenadores actuales. La fortaleza de los sistemas de cifrado actuales se basa en que el esfuerzo computacional necesario para romper las claves de cifrado es demasiado elevado para llevar a cabo ataques. Con los ordenadores cuánticos, este tiempo se reduce drásticamente, haciendo posible romper las claves y comprometer los algoritmos de cifrado. Los algoritmos cuánticos codifican los bits de la clave como datos cuánticos, y estos, por el principio de incertidumbre de de Heisenberg que dice que el proceso de medir en un sistema cuántico perturba dicho sistema, aparecerán como modificados si son observados por un tercero, evidenciando que la comunicación ha sido comprometida.

Algoritmos cuánticos pioneros. El algoritmo de Deutsch y la máquina de Turing

El algoritmo de Deutsch, desarrollado David Elieser Deutsch, físico de la Universidad de Oxford, determina si una función es equilibrada o constante . Las funciones consideradas en el algoritmo son aquellas que asignan una entrada {0,1} a una salida {0,1}.
Una función se equilibra si f (0) es distinta de f (1), es decir, es una relación uno a uno. Por otro lado, una función es constante si f (0) es igual a f (1), es decir, una salida es siempre la misma independientemente de una entrada.
Una computadora clásica debe evaluar f dos veces para ver si está equilibrada o es constante, es decir, la función debe evaluarse para todas las entradas posibles; en ese caso, el dominio consta de dos elementos {0,1}.
Por otro lado, Alan Turing es considerado uno de los padres de la ciencia de la computación y precursor de la informática moderna. Proporcionó una influyente formalización de los conceptos de algoritmo y computación: la máquina de Turing.
Turing demostró que dicha máquina era capaz de resolver cualquier problema matemático que pudiera representarse mediante un algoritmo. Las máquinas de Turing siguen siendo el objeto central de estudio en la teoría de la computación. Llegó a probar que no había ninguna solución para el problema de decisión, Entscheidungsproblem, demostrando primero, que el problema de la parada para las máquinas de Turing es irresoluble: no es posible decidir algorítmicamente si una máquina de Turing dada llegará a pararse o no. Su estudio también introduce el concepto de números definibles.

2. ¿Que algoritmos cuánticos pueden romper criptosistemas modernos?

Algoritmo de Shor

En contraste con la búsqueda y multiplicación de grandes números primos, no se conoce ningún algoritmo clásico eficiente para la factorización de grandes números. Un algoritmo se llama eficiente si su tiempo de ejecución, es decir, el número de operaciones elementales, es asintóticamente polinomial en la longitud de su entrada medida en bits. El algoritmo clásico más conocido necesita.

$$O\left(\exp\left(\left(\tfrac{64}{9}\right)^{1/3} N^{1/3} (\ln N)^{2/3}\right.\right.$$

para factorizar un número binario de N bits, es decir, escalar exponencialmente con el tamaño de entrada.
La multiplicación de grandes números primos es, por lo tanto, una función unidireccional, es decir, una función que puede evaluarse fácilmente en una dirección, mientras que su inversión es prácticamente imposible. Las funciones unidireccionales juegan un papel importante en la criptografía y son esenciales para los sistemas criptográficos de clave pública, donde la clave para la codificación es pública y sólo la clave para la decodificación permanece secreta.
Aunque en general se cree (aunque no se ha demostrado formalmente) que la factorización primaria eficiente en un ordenador clásico es imposible. Un algoritmo eficiente para computadoras cuánticas fue propuesto en 1994 por P.W. Shor.
El algoritmo de Shor es probabilístico: da la respuesta correcta con alta probabilidad, y la probabilidad de fallo puede ser disminuida repitiendo el algoritmo. Como hasta ahora sólo se ha podido implementar en computadoras cuánticas con un pequeño número qubits, sólo se ha podido experimentar para factorizar números pequeños.
El algoritmo se compone de las siguientes partes: 1) **Determinar si un número es primo o no**, 2) **Encontrar el mínimo común denominador**, 3) **Determinar el periodo de una función**.
Los dos primeros se pueden resolver en tiempo polinómico con algoritmos clásicos y es en el tercero donde la transformada cuántica de Fourier marca la diferencia de complejidad asintótica utilizada en conjunción con el algoritmo clásico de expansión continua de fracciones.
Esto pone en riesgo principalmente los algoritmos asimétricos que se basan en llaves públicas como son RSA, DSA y ECDSA. Cualquier sistema que aplique cifrado asimétrico ve afectada su seguridad por el algoritmo de Shor. Sistemas como Blockchain, diversos tipos de VPNs, o navegación segura entre muchos otros, basan su seguridad en la criptografía asimétrica. Así que la criptografía moderna debe encontrar soluciones nuevas para protegerse contra el algoritmo de Shor en un momento en que los ordenadores cuánticos serán lo suficientemente poderosos.

Algoritmo de Grover

Desarrollado por Lov K. Grover, fue publicado en 1996. Es un algoritmo explota al máximo el principio fundamental de superposición, capaz de agilizar las búsquedas en secuencias de datos no ordenadas de n elementos. Este algoritmo permitiría encontrar un dato en una base de datos no indexada en un tiempo proporcional a la raíz cuadrada del número de datos a revisar.
Clásicamente, la búsqueda en una base de datos sin clasificar requiere una búsqueda lineal, que es O(N) en el tiempo. El algoritmo de Grover, que toma tiempo O(N1/2), es el algoritmo cuántico más rápido posible para buscar en una base de datos sin clasificar. Proporciona "sólo" una aceleración cuadrática, a diferencia de otros algoritmos cuánticos, que pueden proporcionar una aceleración exponencial sobre sus contrapartes clásicas. Sin embargo, incluso la aceleración cuadrática es considerable cuando N es grande.

Ell algoritmo de Grover es probabilístico, en el sentido de que da la respuesta correcta con alta probabilidad. La probabilidad de fallo puede reducirse repitiendo el algoritmo.

No es tan rápido como el algoritmo de Shor por lo que no supone una amenaza tan seria, ya que se puede contrarrestar sin más que doblar la longitud de la clave, pero sí debe tenerse en cuenta. Por ello, este algoritmo reducirá a la mitad la seguridad de los algoritmos simétricos, como AES.

El algoritmo de Grover es un claro síntoma de la ventaja de que el ordenador cuántico tiene a veces sobre las computadoras clásicas. Grover derrota a la fuerza de cifrado simétrico y funciones de hash criptográfico por un factor de dos. Además, el algoritmo de Grover puede ser usado para encontrar colisiones en funciones hash en $O(\sqrt[3]{N})$. Cuando se trata de Grover, estos ataques pueden ser

fácilmente mitigados duplicando la seguridad de nuestros primitivos criptográficos simétricos. Esto hará que todos los protocolos sean un poco más lentos y usarán un poco de más ancho de banda. Con la criptografía asimétrica, realmente tenemos un problema. La mayoría de los criptos asimétricos utilizan la dureza del registro discreto o problemas de factorización para su seguridad. Actualmente, el método más popular para construir un ordenador cuántico es un ordenador cuántico con trampa de iones, que funciona utilizando láseres para manipular iones en un campo magnético. Otras implementaciones incluyen el uso de resonancia magnética nuclear o polarización de la luz. Hasta ahora, ningún grupo de investigación se ha acercado a la construcción de un ordenador cuántico con suficientes bits para romper cualquier criptograma del mundo real.

Criptosistema	Categoría	Tamaño de clave	Parámetro de seguridad	Algoritmo cuántico estimado que rompa el criptosistema	Nº de qubits lógicos necesarios	Nº de qubits físicos necesarios	Tiempo necesario para romper el sistema	Estrategias de reemplazo cuántico-resilientes
AES-GCM	Cifrado simétrico	128 192 256	128 192 256	Algoritmo de Grover	2.953 4.449 6.681	$4{,}61 \times 10^6$ $1{,}68 \times 10^7$ $3{,}36 \times 10^7$	$2{,}61 \times 10^{12}$ años $1{,}97 \times 10^{22}$ años $2{,}29 \times 10^{32}$ años	
RSA	Cifrado asimétrico	1024 2048 4096	80 112 128	Algoritmo de Shor	2.290 4.338 8.434	$2{,}56 \times 10^6$ $6{,}2 \times 10^6$ $1{,}47 \times 10^7$	3,58 horas 28,63 horas 229 horas	Migrar a un algoritmo PQC seleccionado por el NIST
ECC Problema del logaritmo discreto	Cifrado asimétrico	256 386 512	128 192 256	Algoritmo de Shor	2.330 3.484 4.719	$3{,}21 \times 10^6$ $5{,}01 \times 10^6$ $7{,}81 \times 10^6$	10,5 horas 37,67 horas 95 horas	Migrar a un algoritmo PQC seleccionado por el NIST
SHA256	Minado de Bitcoin	N/A	72	Algoritmo de Grover	2.403	2.23×10^6	$1{,}8 \times 10^4$ años	
PBKDF2 con 10.000 iteraciones	Hashing de contraseñas	N/A	66	Algoritmo de Grover	2.403	2.23×10^6	2.3×10^7 años	Abandonar la autenticación basada en contraseñas

Tabla 1: Tiempo estimado para romper criptografía clásica por medio de algoritmos cuánticos, así como contramedidas posibles (tomada de Quantum Computing: Progress and Prospects)

Presente y futuro de la computación cuántica

Hay dos enfoques principales para implementar físicamente una computadora cuántica actualmente, analógica y digital. Enfoques analógicas se dividen en simulación cuántica , recocido cuántica y la computación cuántica adiabática . Las computadoras cuánticas digitales utilizan compuertas de lógica cuántica para realizar el cálculo. Ambos enfoques utilizan bits cuánticos o qubits .

Las computadoras físicas cuánticas de hoy son muy ruidosas y la corrección de errores cuánticos es un campo de investigación en expansión. La supremacía cuántica es, con suerte, el próximo hito que la computación cuántica logrará pronto. Si bien hay mucha esperanza, dinero e investigación en el campo de la computación cuántica, a partir de marzo de 2019 no se han publicado algoritmos comercialmente útiles para las computadoras cuánticas de hoy.

3. Bibliografía

https://blog.elevenpaths.com/2019/01/futuro-post-cuantico-ciberseguridad.html
http://www.criptored.upm.es/crypt4you/temas/cuantica/leccion3/leccion03.html
http://dkopczyk.quantee.co.uk/deutschs-algorithm/
https://en.wikipedia.org/wiki/Deutsch%E2%80%93Jozsa_algorithm
https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf
https://www.nist.gov/publications/quantum-cryptanalysis-shor-grover-and-beyond
https://dsprenkels.com/files/grover.pdf