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[A Variational Quantum Attack for AES-like Symmetric Cryptography].

cita del paper:
@article{AVariationalQuantumAttackforAESlikeSymmetricCryptography,
author = {Wang, ZeGuo and Wei, ShiJie and Long, Gui-Lu and Hanzo, L.},
year = {2022},
month = {05},
pages = {},
title = {A Variational Quantum Attack for AES-like Symmetric Cryptography}
}

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[Algebraic Attacks on Block Ciphers Using Quantum Annealing].

```
@ARTICLE{Algebraicattacksonblockciphersusingquantumannealing ,
  author={Burek, Elżbieta and Wroński, Michał and Mańk, Krzysztof and Misztal, Michał},
  journal={IEEE Transactions on Emerging Topics in Computing},
  title={Algebraic Attacks on Block Ciphers Using Quantum Annealing},
  year={2022},
  volume={10},
  number={2},
  pages={678-689}}
```

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[Quantum Attack-Resistent Certificateless Multi-Receiver Signcryption Scheme].

@article{QuantumAttackResistentCertificatelessMultiReceiverSigncryptionScheme,
author = {Li, Huixian and Chen, Xubao and Pang, Liaojun and Shi, Weisong},
year = {2013},
month = {06},
pages = {e49141},
title = {Quantum Attack-Resistent Certificateless Multi-Receiver Signcryption Scheme},
volume = {8},
journal = {PloS one}
}

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 $O(2^frac{n,2})$[Quantum Attacks on 1K-AES and PRINCE].

@article{QuantumAttackson1KAESandPRINCE,
author = {Cai, Binbin and Yusen, Wu and Dong, Jing and Qin, Su-Juan and Gao, Fei and Wen, Qiao-Yan},
year = {2022},
month = {02},
pages = {},
title = {Quantum Attacks on 1K-AES and PRINCE},
journal = {The Computer Journal}
}

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 O(exp log log log , (cn n ( )1/3 2/3)( )), donde mi C ≈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 O((log n) 2+ε). 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 n er−1 mod . 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[Quantum polynomial-time fixed-point attack for RSA].

@ARTICLE{QuantumPolynomialTimeFixedPointAttackforRSA,
 author={Wang, Yahui and Zhang, Huanguo and Wang, Houzhen},
 journal={China Communications},
 title={Quantum polynomial-time fixed-point attack for RSA},
 year={2018},
 volume={15},
 number={2},
 pages={25-32}}

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:
(i) un fenómeno no determinista
(ii) 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[Quantum attacks on pseudorandom generators].

@article{Quantumattacksonpseudorandomgenerators,
author = {Guedes, Elloá and de Assis, Francisco and LULA, BERNARDO},
year = {2013},
month = {06},
pages = {},
title = {Quantum attacks on pseudorandom generators},
volume = {23},
journal = {Mathematical Structures in Computer Science}
}

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)[Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research].

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[Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research].

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[Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research].