Universidad de Alcalá

Resumen presentación
Criptografía postcuántica

Máster en ciberseguridad

Asignatura: Criptografía aplicada

Kevin van Liebergen

2021

RSA $\rightarrow$ Su seguridad radica en la dificultad de factorizar $N = p \cdot q$ en un ordenador clásico, es decir, es de clase NP (no resoluble en tiempo polinómico). Basta con probar 2 hasta $\sqrt{N}$ para saber si un número es primo o no.

Diffie-Hellman $\rightarrow$ Algoritmo de intercambio de claves. Problema de logaritmo discreto, sin embargo se han desarrollado varias investigaciones para factorizar este problema de logaritmos discretos [1].

Por lo que, los ordenadores cuánticos van a dejar obsoletos a este tipo de algoritmos, es más, ya se están desarrollando ordenadores cuánticos

Un bit puede tener el valor de 0 o 1, la criptografía cuántica se basa en que un qbit puede poseer ambos valores, es la probabilidad de que el sistema se encuentre en un estado.

- En 2001 IBM factoriza $15 = 3 \cdot 5$ en un 'ordenador' cuántico de 7 qbits (utilizando Shor)
- En 2019 IBM lanza QSystem1, el primer ordenador cuántico de 20 qbits
- En enero de 2020 IBM anuncia el lanzamiento de qSystem2, el segundo ordenador cuántico de 50 qbits
- Se prevee que en 25/30 años se encuentre roto

A raíz de eso se han desarrollado distintos tipos de criptografías post-cuántica (resistentes a la criptografía cuántica):

- PQC (Post Quantum Cryptography) basado en erro connecting codes (Criptosistema de McEliece) [1]
- PQC basado en polinomios multivariantes (Ding $\rightarrow$ Firmas digitales)
  - Ecuación lineal, de grado superior

$$f_1(X_1, ..., X_n) = 0$$

$$f_r(X_1, ..., X_n) = 0 \, , Si \, f \in \mathbb{F}_q[x_1, ..., x_r]$$

- PQC basado en curvas elípticas
  - Polinomio de grado 3
- PQC basado en retículos

[1] https://es.wikipedia.org/wiki/Complejidad_y_criptografia

Vamos a comentar la criptografía basada en retículos, los retículos son estructuras algebraicas similares a espacios vectoriales, generados con una base, estos retículos se utilizan como garantías.

Un retículo de rango k en $\mathbb{R}^n$ en (λ, ϕ), siendo λ un grupo abeliano finitamente generado de rango k y $\phi \to \mathbb{R}^n$ homomórficamente inyectivo.

$$\phi(a+b) = \phi(a) + \phi(b)$$
$$\phi(-a) = -\phi(a)$$

Por ejemplo:

$$\mathbb{Z}^n = \{(a_1, ..., a_n)(a_i \in \mathbb{Z})\} = a_1(1,0,...,0) + a_2(0,1,...,0) + ... + a_n(0,0,...,1)$$

$$\mathbb{Z}[i] \; = \; a + b \,||\, a, b \in \mathbb{Z} \to \mathbb{R}^2 \approx \mathbb{C}$$

Siendo $i = \sqrt{-1}$

SVP (Shortest Vector Problem)

El problema no es encontrar lambda 1, si no encontrar un vector que se a proxime a lambda 1.

El input $\wedge$ es un retículo full rank de rango n. El objetivo es determinar

$$V_0 \; \in \wedge\{0\},$$

El retículo de rango n, devolver vector que la la norma sea la mínima (norma mínima = λ_1)

Según una investigación de Micciano [2], si

$$\gamma(n) \leq \sqrt{2} \; \forall_n \; \Rightarrow \text{el } \gamma\text{-SUP es NP-hard}$$

Definición

Un problema es NP si existe un algoritmo (Turing computable) y determinista de manera que determinar un nº N es solución de problema (A) requiere una cantidad polinomial $O(P_A \log(N))$ de operaciones.

A = factorización

N = p * q

$$p = p_0 + p_1 \cdot 10 + ... + p_r \cdot 10^r$$
$$q = q_0 + q_1 \cdot 10 + ... + q_r \cdot 10^r$$

Por lo que hay que realizar r operacionaes durante r veces, $r \cdot r = r^2$

$$r^2 \; = \; \log_{10}(N)^2$$

Learning With Errors (LWE)

El criptosistema LWE [3], q primo, $\mathbb{F}_q$ cuerpo finito de q elementos,

$$\mathbb{F}_q^n = \{(a_1, ..., a_n) \mid a_i \in \mathbb{F}_q\}$$

$\mathbb{F}_q^n$ es un espacio vectorial sobre $\mathbb{F}_q$

Criptosistema LWE

Definición
Siendo q primo χ gaussiana discreta, $S \in \mathbb{F}_q^n$.
Un oráculo LWE es un algoritmo aleatorio

- Paso 1

  Toma $a \in \mathbb{F}_q^n$ uniformemente

- Paso 2

  Calcula $< a, s > \in \mathbb{F}_q$

- Paso 3

  Muestrea $e \hookleftarrow \chi$

- Output

  $(a < a, s > +e) \in \mathbb{F}_q^n \times \mathbb{F}_q$

Existe un algoritmo polinomial [3] en $\log(n)$ cuántico que reduce γ_SVP a LWE para el oráculo q,s,χ. Para resolver SVP hay que resolver LWE (NP-hard $\gamma(n) \leq \sqrt{2}$)

Definición

- Generación de claves

  Tomamos $a, \in \mathbb{F}_q^n$ (unif)

  Tomamos $e_i \leftarrow \chi$

  La clave pública P_k es $P_k = \{(a_i, < a_i, s > +e_i)\}$ para $1 \leq i \leq m$

  La clave privada $S_k = S$

- Cifrado

  $0 \in \mathbb{F}_2 \rightarrow 0 \in \mathbb{F}_q$

  $1 \in \mathbb{F}_2 \rightarrow 1 \in \mathbb{F}_q$

Quiero cifrar $Z \in \{0,1\} \leq \mathbb{F}_q$

Tomo $S \leq \{1,\ldots,m\}$ (un subconjunto cogido uniformemente)

$E(s,z) \ = \ (\sum_{i\in S} \ a_i, \sum_{i\in S} \ < a_{i,s} > \ + e_i \ + \ z|\frac{q}{2}|)$

- Descifrado

  Se tiene que:

  $v - < u, s > = \ \sum e_i + Z|\frac{q}{2}|$

  La probabilidad $p(\sum e_i \ \leq \ |\frac{q}{4}|) \approx 1$ (muy grande)

  Si $Z \ = \ 0$ con probabilidad cercana a 1 $\quad |v - < u, s > | \ \leq \ |\frac{q}{4}|$

  Si $Z \ = \ 1$ esto no pasa

  $q \in \{n^2, ..., 2n\}$ se demuestra que el criptosistema es seguro

Durante las diez primeras páginas de [4] se realiza un criptoanálisis de Ring-LWE, el inconveniente de la clave pública P_k

Criptosistema de PLWE

$$n \ = \ 2^{k+1}$$

$$m \ = \ \phi(n) = 2^k$$

$$\phi_n(x) \ = \ X^m + 1$$

$$R_q = \mathbb{F}_q[X]_{\leq m-1} = \{a_0 + a_1 \cdot X + \cdots + a_{m-1} \cdot X^{m-1}, a_i \in \mathbb{F}_q\}$$

Y en R_q

$$X^m \ := \ -1$$

$$X \cdot (a_0 + a_1 + \cdots + a_{m-1} \cdot X^{m-1})$$

$$X = a_0 \cdot X + a_1 \cdot X^2 + \cdots + a_{m-2} \cdot X^{m-2} - a_{m-1}$$

R_q, t, es un anillo (cuerpo sin inversos)

1 Valoración personal

No cabe duda que la computación cuántica traerá grandes cambios a nuestra sociedad, más positivos que negativos, y es innegable pensar que la criptografía de hoy en día perdurará con la misma fortaleza en 15 años, y más teniendo en cuenta la llegada de ordenadores cuánticos que romperán con los problemas sobre los que se sustenta la mayor pare de protocolos criptográficos de clave pública.

Por ello actualmente se encuentran desarollándose algoritmos de cifrado resistentes a la criptografía cuántica, es decir, para un mundo post-cuántico. Dentro de los algoritmos post-cuánticos la charla se ha centrado en los algoritmos basados en retículos, estructuras algebraicas similar a espacios vectoriales generados con una base.

Este tipo de criptografía (criptografía homomórfica), permite realizar operaciones algebraicas mediante datos cifrados, de tal manera que al descifrar equivalga a realizar las mismas operaciones algebraicas sobre datos en texto plano.

Dentro de la criptografía basada en retículos (Lattice-based cryptography) tenemos los problema SVP, encontrar un vector que se aproxime a lambda 1, un vector cercano al origen del espacio dada una base larga.

Uno de los algoritmos que más se están desarrollando son los LWE (Learn With Errors), sin embargo computacionalmente son difíciles de implementar, además LWE introduce un problema y es la dificultad de determinar qué variables se han introducido si se inserta un error aleatorio.

Es una gran noticia de que existen este tipo de algoritmos orientados a reforzar la criptografía cuando existan los ordenadores cuánticos, debido a que la privacidad no se verá violada por ningun tercero. Este tipo de algoritmos LWE resultan bastante novedoso y es normal que aún no se encuentren totalmente implementado, además es necesario realizar una valoración de eficacia para conocer si es posible implementarlo en algún sistema, al ser sistemas tan complejos no se puede implementar en cualquier dispositivo.

Bibliografía

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," vol. 41, no. 2, pp. 303–332, publisher: Society for Industrial and Applied Mathematics. [Online]. Available: https://www.jstor.org/stable/2653075

[2] D. Micciancio, "On the inapproximability of the shortest vector in a lattice within some constant factor preliminary version," p. 11.

[3] D. Aharonov, "Lattice problems in NP coNP," p. 17.

[4] C. Peikert, "How (not) to instantiate ring-LWE," in *Security and Cryptography for Networks*, V. Zikas and R. De Prisco, Eds. Springer International Publishing, vol. 9841, pp. 411–430, series Title: Lecture Notes in Computer Science. [Online]. Available: http://link.springer.com/10.1007/978-3-319-44618-9_22