Introduction
Signature schemes

Luis J. Dominguez Perez

CRYPTO-CO, Julio 1 de 2016

Contenido, sección 1

Shor's algorithm

- Factorise a non-prime integer number in polinomial time
- There are two principal parts:
  - Reduce the factorisation problem to a sorted search (classic computing)
  - Solve the problem of sorted search (quantum computing)

Consequences: RSA could be broken since its strength sits in the difficulty to find two prime factors from a very large integer number.

Attacks

- The Shor's quantum algorithm solves, in polynomial time, certain schemes based on the hidden subgroup problem for finite *abelian* groups.

- In particular, this algorithm could break the following schemes:
  - RSA
  - DSA
  - ECDSA

  in $\mathcal{O}(\log N)^3$

Shor's Algorithm

Algorithm 1 Shor's Algorithm

Require: $N \in \mathbb{N}$ non-prime
Ensure: a factor of N

1: Choose randomly $x \in [2..N]$
2: If CD$(x, N) \neq 1$ abort
3: Find order$r$ from $x \bmod N (x^r \equiv 1 \bmod N)$
4: **if** r is even, and $x^{r/2} \neq \pm 1 \bmod N$ **then**
5: GCD$(x^{r/2} + 1, N)$ is not a trivial factor of N
6: **else**
7: try with another x
8: **end if**

Scope

- The cryptographic algorithms based on the strength of a problem that cannot be broken by the Schor's algorithm, are known as **post-quantum cryptographic schemes**
- These schemes are based in problems which are computationally **NP**-complete o **NP**-hard:
  - Hash functions
  - Codes
  - Lattices
  - Multivariate quadratic equations
  - Secret Key
  - Isogenies over supersingular elliptic curves
  - Non-abelian groups
  - etc.

Contenido, sección 2

Postquantum

Criptografía basada en códigos

Funcionamiento

Ejemplos

Códigos lineares

Definiciones:

- El peso Hamming $w(u)$ de $u \in (\mathbb{F}_q)^n$ es el número de componentes de u que no están en cero.

- La distancia Hamming entre $u, v \in (\mathbb{F}_q)^n$ es $dist(u, v) = w(u - v)$.

- Un código linear $\mathcal{C}[n, k]$ sobre $\mathbb{F}_q$ es un vector de k dimensiones en el subespacio de $(\mathbb{F}_q)^n$.

- Un código puede ser definido por una matriz generadora $G \in (\mathbb{F}_q)^{k \times n}$ o por una matriz de verificación de paridad $H \in (\mathbb{F}_q)^{r \times n}$ with $r = n - k$:
  - $C = \{uG \in (\mathbb{F}_q)^n | u \in (\mathbb{F}_q)^n\}$
  - $C = \{v \in (\mathbb{F}_q)^n | Hv^T \in O^r\}$

  donde $HG^T = O$.

- Un vector s es llamado síndrome of v, si $Hv^T = s^T$.

Matriz generadora

- Las matrices generadores y de verificación de paridad no son únicas:
  - dada una matriz no singular $S \in (\mathbb{F}_q)^{k \times k}$ (resp. $S \in (\mathbb{F}_q)^{r \times r}$)
  - la matriz $G' = SG$ (resp. $H' = SH$) define el mismo código que G (resp. H) en otra base.

- Como consecuencia, la forma sistemática (escalonada) $G = [I_k|M]$, $H = [-M^T|I_r]$ donde $M \in (\mathbb{F}_q)^{k \times r}$ no es siempre posible.

Códigos equivalentes

- Dos códigos son equivalentes (aún permutados) si difieren por una permutación en las coordenadas de sus elementos.

- Formalmente, un código C' generado por G' es equivalente a un código C generado por G sí y solo sí $G' = SGP$ para alguna matriz de permutación $P \in (\mathbb{F}_q)^{n \times n}$, y una matriz no singular $S \in (\mathbb{F}_q)^{k \times k}$.

En esencia, se dice que $C' = CP$.

Contenido, sección 3

Funcionamiento

La decodificación funciona de la siguiente manera:

Decodificación General

- Dados unos enteros positivos (n, k, t), un campo finito $\mathbb{F}_q$, un código linear $\mathcal{C}[n, k] \in (\mathbb{F}_q)^n$ definido por una matrix generadora $G \in (\mathbb{F}_q)^{k \times n}$, y un vector $c \in (\mathbb{F}_q)^n$
- ¿existe un vector $m \in (\mathbb{F}_q)^k$ tal que $e = c - mG$ tiene peso $w(e) \leq t$?
- Encontrar tal vector e es un problema NP-completo.

funcionamiento

Decodificación Síndrome

- Dados unos enteros positivos (n, k, t), un campo finito $\mathbb{F}_q$, un código linear $\mathcal{C}[n, k] \in (\mathbb{F}_q)^n$ definido por una matrix de paridad $H \in (\mathbb{F}_q)^{r \times n}$ con $r = n - k$, y un vector $s \in (\mathbb{F}_q)^r$
- ¿existe un vector $e \in (\mathbb{F}_q)^n$ de peso $w(e) \leq t$ tal que $He^T = s^T$?
- Encontrar tal vector e también es un problema NP-completo.

funcionamiento

Decodificación Permutada

- Resolver el problema de decodificación general o el de decodificación síndrome para un código C que sea equivalente tras permutación a un código C' eficientemente decodificable, consiste en encontrar la permutación y cambio de bases entre los códigos, y utilizar el código C' como pasadillo secreto (trapdoor) para decodificar en C.
- Esto se cree que es lo *suficientemente difícil* para "ciertos códigos".

funcionamiento

Decodificación Recortada

- Resolver el problema de decodificación general o el de decodificación síndrome para un código C que sea equivalente tras permutación a algún subcódigo recortado (una proyección) de algún código C' eficientemente decodificable, consite en encontrar la permitación y cambio de bases entre los códigos, y usar el código C' como pasadillo secreto (trapdoor) para decodificar C.
- Decidir si el código es equivalente al código recortado es un problema NP-completo.

Contenido, sección 4

Ejemplos de sistemas

Existen varios esquemas criptográficos basados en códigos, por ejemplo: McEliece, Niederreiter, firmas CFS, entre otros.

Sistema McEliece

- Este criptosistema utiliza la matriz generadora para la clave pública, por lo que para el cifrado, el secreto se multiplica por ella y se le agrega la información de corrección de errores (ruido).
- Para el decifrado, se recupera la información del vector de errores y se elimina del mensaje recibido.

ejemplos de sistemas

Sistema Niederreiter

- A diferencia del anterior, en este caso se utiliza la matriz de permutación como clave pública, por lo que el transpuesto del vector de corrección de errores (que contiene el mensaje) se multiplica por esta matriz.
- Para el decifrado, el proceso es similar.

ejemplos de sistemas

Firmas CFS

- Para las firmas, la clave pública también utiliza la matriz de permutación.
- Dado un oráculo aleatorio, y hasta encontrar un síndrome decodificable con el mensaje.
- De igual manera, se extrae el vector de corrección (conteniendo el mensaje) y se utiliza como firma (junto con un valor del oráculo aleatorio).
- Para la verificación, se multiplica la firma con la matriz de permutación y se corrobora con una aplicación de la firma sobre el mensaje (y el valor del oráculo aleatorio).

Cifrado McEliece

- Generación de llaves:
  - Escoja aleatorios $[n, k]$, t-corrección de errores, un código eficientemente decodificable Γ, y una matriz aleatorio de permutación $P \in (\mathbb{F}_q)^{k \times k}$, y calcule una matriz generadora $G \in (\mathbb{F}_q)^{k \times k}$ para el código equivalente ΓP.
  - Kpriv $= (\Gamma, P)$, Kpub = (G, t).
- Cifrado de un texto plano $m \in (\mathbb{F}_q)^k$:
  - ☐ Escoja un elemento aleatorio e con error t $e \in (\mathbb{F}_q)^n$ y calcule $c = mG + e \in (\mathbb{F}_q)^n$.
- Descifrado de un texto cifrado $c \in (\mathbb{F}_q)^n$:
  - ☐Corrija los errores en $c' = cP^{-1}$, encuentre el vector e' con t-errores $e' = eP^1$ tal que $c' - e' \in \Gamma$, y recupere m directamente de $c - e \in \Gamma P$.

Ejemplo de Cifrado McEliece

- Sea $n = 8$, $t = 1$, $k = 4$, y un código con la siguiente matriz de paridad H, y matriz generadora G:

$$H = \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

$$G = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{array}\right]$$

- Cifre el mensaje $m = (1100)$ con vector de error de corrección $e = (00100000)$: $c = mG + e = (11100101)$
- El cálculo del síndrome $Hc^T = (1111)^T$, la corrección del error revela e, y nos da $mG = c - e = (11000101)$.

Retos

- La criptografía basada en códigos, presenta el problema de seleccionar un tipo de código que permita que la decodificación permutada sea fuerte.

- Adicionalmente, sufre del elevado espacio de almacenamiento y transmición requeridos para la llave pública.

- La tendencia actual en investigación para este tipo de criptografía se centra en reducir la llave pública, y en la elaboración de protocolos criptográficos que utilicen códigos como su primitiva.