Criptosistema de McEliece

Mario Muñoz Adrián Rodríguez Carlota Valdivia

Seguridad y Protección de Sistemas Informáticos

Índice de contenidos

- Publicado en 1978 por Robert McEliece como un criptosistema de clave pública basado en códigos correctores de errores.
- No vulnerable al Algoritmo de Shor.
- Criptografía post-quántica, NIST.

Índice de contenidos

Un alfabeto $\mathcal{A}$ no es más que un conjunto finito no vacío de símbolos, y llamamos palabra a cada expresión construida con símbolos del alfabeto.

Definition

Llamamos bloque de código a un conjunto de palabras de longitud n. Esto es, se dice que C es un bloque de código de longitud n si es un subconjunto de $\mathcal{A}^n$. A cada elemento del bloque se le llamará palabra de código.

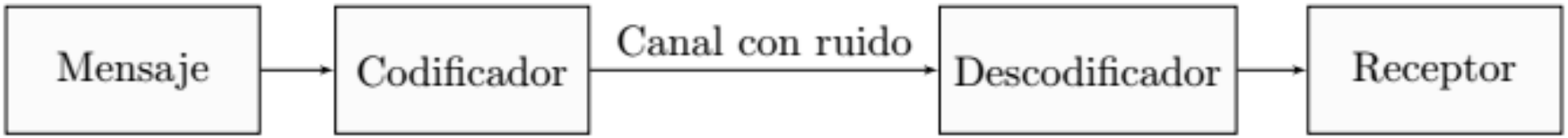

Figura: Transmisión a través de un canal con ruido.

En adelante trabajaremos con el alfabeto $\mathbb{F}_q$

Definition

Diremos que un bloque de código C es corrector de t errores si cuando tomamos una palabra de código del mismo y cambiamos hasta un máximo de t símbolos, no alcanzamos una palabra de código diferente y tampoco alcanzamos una palabra que pueda ser obtenida a partir de una palabra de código cambiando un máximo de t símbolos.

Definition

La distancia de Hamming entre dos vectores de $\mathbb{F}_q^n$ se denota por $d_H(x,y) := |\{i \in \{1,\ldots,n\} \ : \ x_i \neq y_i\}|$. El peso de Hamming $wt(x)$ de $x \in \mathbb{F}_q^n$ es el número de coordenadas distintas de 0. La relación entre distancia y peso es $wt(x) = d_H(x,0)$. La distancia de Hamming de un bloque de código C de longitud n se define como $d_H(C) := \min\{d_H(x,y)\ \forall x,y \in C \text{ con } x \neq y\}$

Nos centramos en los bloques de código $C \subseteq \mathbb{F}_q^n$.
$\mathbb{F}_q^n$ es un $\mathbb{F}_q$-espacio vectorial

Definition

Sea $C \subseteq \mathbb{F}_q^n$, se dice que C es un código lineal si C es un subespacio vectorial de $\mathbb{F}_q^n$.
Si C es un subespacio k-dimensional de $\mathbb{F}_q^n$ también nos referimos a C como un código $[n, k]$. Si además la distancia mínima de Hamming $d_H(C) = d$, nos referiremos como un código $[n, k, d]$

Valery Denisovich Goppa, matemático ruso, presenta en 1970 los códigos Goppa.

Definition

Sea $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_t x^t \in \mathbb{F}_{p^m}[x]$ con p primo, y sea $L = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{p^m}^n$ tal que $g(\alpha_i) \neq 0 \quad \forall \alpha_i \in L$. Llamaremos código de Goppa correspondiente a L y $g(x)$, denotado por $\Gamma(L, g)$, al código corrector de errores formado por

$$\left\{ \mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}_p^n \ : \ \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} \equiv 0 \text{ mód } g(x) \right\}$$

Cuando $p = 2$ decimos que se trata de un código Goppa binario y lo denotamos por $\Gamma_2(L, g)$.

Proposición

Sea $\Gamma(L, g)$ un código Goppa, entonces $\Gamma(L, g)$ es un código lineal.

Que sea un código lineal implica que como subespacio vectorial tiene una base, y podremos codificar de forma eficiente.

Definition

Sea C un código lineal $[n, k]$ sobre $\mathbb{F}_q$. Se llama matriz generadora de C a la matriz $k \times n$ formada por los elementos de la base de C como filas.

Veamos cómo podríamos codificar y descodificar con códigos Goppa:

- **Codificación.** Codificar un mensaje de longitud k, $\mathbf{m} = (m_1, \ldots, m_k) \in \mathbb{F}_q^k$, simplemente consiste en multiplicar por la matriz generadora G, la codificación del mensaje será $\mathbf{m} \cdot G$.
- **Descodificación.** Sea $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ el vector recibido con r errores

$$\mathbf{y} = (y_1, y_2, \ldots, y_n) = \underbrace{(c_1, c_2, \ldots, c_n)}_{\text{palabra de código}} + \underbrace{(e_1, e_2, \ldots, e_n)}_{\text{vector error}}$$

con $e_i \neq 0$ en exactamente r posiciones. Para descodificar, si el código Goppa es binario, podemos aplicar el algoritmo de Patterson, que dado $\mathbf{y}$ nos devolverá el vector de error. Por lo que ya podemos recuperar el mensaje enviado por la relación:
$(m_1, m_2, \ldots, m_k) \cdot G = (c_1, c_2, \ldots, c_n)$

Índice de contenidos

Intercambio de mensajes.

En esta sección se va a explicar el procedimiento de comunicación entre dos personas mediante el criptosistema de McEliece. Se explicará tanto el cifrado de un mensaje por parte de un emisor, como su correspondiente descifrado por parte de un receptor.

Generación de las claves públicas y privadas

Matrices necesarias

Para obtener las claves privadas y públicas es necesaria la generación de tres matrices:

- Una matriz G en $\mathbb{F}_2^{k \times n}$, que va a ser la **matriz generadora** de un código de Goppa binario [n,k] elegido.
- Una **matriz invertible aleatoria S** en $\mathbb{F}_2^{k \times k}$.
- Una **matriz de permutaciones aleatoria P** en $\mathbb{F}_2^{n \times n}$.

Generación las claves públicas y privadas

A partir de estas tres matrices se puede obtener la clave pública y privada de un usuario de la siguiente manera:

- **Clave privada.** La clave privada se corresponde con la terna formada por las tres matrices definidas anteriormente: $k_s = (G, S, P)$.
- **Clave pública.** La clave pública es el par formado por el producto resultante de los elementos de la terna de la clave privada $G' = S \cdot G \cdot P$ y el parámetro t: $k_p = (G', t)$.

- **Cifrado de un mensaje:** Para llevar a cabo el cifrado de un mensaje $\mathbf{m} = (m_1, \ldots, m_k) \in \mathbb{F}_2^k$ dirigido a un receptor con clave pública $k_p = (G', t)$, el emisor necesita:
  1. Elegir un vector aleatorio de errores $\mathbf{e} = (e_1, \ldots, e_k) \in \mathbb{F}_2^n$ con peso $wt(e) = t$.
  2. Multiplicar el mensaje m por la matriz G' y obtener un vector de tamaño n: $c = m \cdot G'$
  3. Añadir el vector de errores e al vector c: $c' = m \cdot G' + e$.

- **Descifrado de un mensaje:** Para llevar a cabo el descifrado de un mensaje $c' = mG' + e$ recibido por un receptor con clave pública $k_p = (G', t)$, dicho receptor necesita:
  1. En primer lugar, multiplicar dicho vector c' por la matriz inversa de la matriz de permutación, P^{-1}:
  $\hat{c} = c'P^{-1} = mSGPP^{-1} + eP^{-1} = mSG + eP^{-1}$.

Comunicación entre el emisor y el receptor

Descifrado de un mensaje:

2. A continuación, usar el algoritmo eficiente de descodificación de t errores para obtener mSG. Dicho algoritmo se puede usar ya que la matriz SG es una matriz generadora del código Goppa, y $wt(e) = wt(eP^{-1}) = t$.
3. Una vez se ha obtenido mSG, puede obtener mS resolviendo el sistema de ecuaciones correspondiente a llevar a cabo el descifrado del código de Goppa.
4. Finalmente, obtener el código descifrado m a partir de la inversa de la matriz aleatoria S, $m = mSS^{-1}$.

Índice de contenidos

Seguridad

La seguridad del criptosistema de McEliece es consecuencia de los siguientes problemas de decisión de la teoría de códigos:

- Sea C un $[n, k]$ código lineal sobre $\mathbb{F}_q$ y $\alpha \in \mathbb{F}_q^n$. Encontrar una palabra de código $c \in C$ tal que la distancia de Hamming $d(\alpha, c)$ sea mínima.
- Sea C un $[n, k]$ código lineal sobre un cuerpo $\mathbb{F}_q$ y $w \in \mathbb{N}$. Encontrar una palabra de código $c \in C$ tal que su peso $wt(c) = w$.

Ambos problemas son NP-Completos por tanto el problema de romper el criptosistema de McEliece también es NP-Completo.

Índice de contenidos

Ventajas

- Rápido proceso de codificación y descodificación.
- Criptosistema Post-Cuántico.

Desventajas

- Tamaño de las claves públicas y privadas.
- No se puede emplear para producir firmas digitales. El problema ha sido solucionado mediante Niederreiter.

Índice de contenidos

Ataques genéricos de descodificación

- **Ataques genéricos de descodificación**: consisten en intentar recuperar el mensaje original, $\mathbf{m}$, que ha sido cifrado obteniendo el vector $\mathbf{c}'$ considerando la matriz pública del criptosistema G', como matriz generatriz para dicho código. Los mejores resultados se obtienen utilizando algoritmos que mejoran la descodificación del conjunto de información.

Ataques contra la estructura del código

- **Ataques contra la estructura del código**: este tipo de ataques consisten en intentar recuperar las matrices G, S y P a partir de las cuales se ha construido el criptosistema de McEliece. Aquellos criptosistemas de McEliece que emplean códigos Goppa son los que presentan una mayor seguridad.

Índice de contenidos

Conclusiones

- Los sistemas criptográficos más populares de la actualidad serán muy vulnerables y dejarán de ser seguros cuando aparezcan en el mercado los ordenadores cuánticos.
- McEliece es un criptosistema resistente a los ataques actuales y a los ataques realizados por ordenadores cuánticos, es un criptosistema post-cuántico.
- Presenta algunas desventajas con respecto a otros criptosistemas debido al gran tamaño de sus claves, al ser matrices de elevadas dimensiones.
- Es necesario ir pensando en desarrollar nuevos algoritmos criptográficos más resistentes que los actuales para poder hacer frente a los ordenadores cuánticos.