CÓDIGOS Y CRIPTOGRAFÍA. INFORMÁTICA DIEGO RUANO 13/12 2022

CRIPTOGRAFIA POST-CUÁNTICA

LA SEGURIDAD DE RSA ESTA BASADA EN LA IMPOSIBILIDAD COMPUTACIONAL DE FACTORIZAR $N=pq$ PARA p Y q GRANDES (EN UN ORDENADOR CLÁSICO)

SIN EMBARGO EN 1994 SHOR INTRODUJO UN ALGORITMO QUE ES CAPAZ DE FACTORIZAR RÁPIDAMENTE UN NÚMERO GRANDE EN UN ORDENADOR CUÁNTICO.

n = TAMAÑO DE N

COMPLEJIDAD: $\mathcal{O}(n^3 \log n)$

$\mathcal{O}(n^{2+\mathcal{O}(1)})$ ⟸ MUCHOS MÁS Q-BITS

Y ADEMÁS, ¡ES PARALELIZABLE!

ADEMÁS EL ALGORITMO DE SHOR SE PUEDE MODIFICAR FÁCILMENTE PARA CALCULAR LOGARITMOS DISCRETOS

POR LO QUE LOS CRIPTOSISTEMAS DE CLAVE PÚBLICA USADOS ACTUALMENTE SERIAN INSEGUROS SI SE DISPUSIERA DE UN ORDENADOR CUÁNTICO CON UN NÚMERO SUFICIENTE DE Q-BITS.

CONCURSO NIST ← VER ENLACE EN CAMPUS VIRTUAL

EL SISTEMA CRIPTOGRÁFICO DE MCELIECE (1978)

LA DESCODIFICACIÓN DE UN CÓDIGO LINEAL GENERAL ES UN PROBLEMA COMPUTACIONAL MUY DIFÍCIL (NP-COMPLETO)

SI C ES UN CÓDIGO $[n,k,d]$ SOBRE UN CUERPO FINITO $\mathbb{F}_q$ Y $\vec{c} \in C$ ES UNA PALABRA ENVIADA QUE SE HA VISTO ALTERADA Y SE RECIBE $\vec{y} \in \mathbb{F}_q^{\,n}$, $\vec{y} = \vec{c} + \vec{e}$ CON $w_H(\vec{e}) \leq t = \left\lfloor \frac{d-1}{2} \right\rfloor$

LA ELIMINACIÓN DEL VECTOR $\vec{e}$ ES TEÓRICAMENTE FACTIBLE PUESTO QUE $\vec{c}$ ES EL ÚNICO ELEMENTO DE C A DISTANCIA MENOR

O IGUAL QUE t DE $\vec{y}$

SIN EMBARGO, HACERLO RESULTA COMPUTACIONALMENTE IMPOSIBLE PARA PARÁMETROS SUFICIENTEMENTE GRANDES DE C.

PERO, TAMBIÉN HEMOS VISTO, QUE PARA CIERTOS CÓDIGOS CORRECTORES PARTICULARES HAY ALGORITMOS RÁPIDOS Y EFICIENTES DE DECODIFICACIÓN QUE PERMITEN DECODIFICAR EN TIEMPO POLINÓMICO.

ESTOS SON LOS CÓDIGOS CORRECTORES USADOS EN LA PRÁCTICA PARA CORREGIR ERRORES

IDEA DE MCELIECE:

- USAR UN CÓDIGO GRANDE PERO FÁCILMENTE DECODIFICABLE COMO CLAVE PRIVADA
- "ENMASCARAR" EL CÓDIGO PARA QUE PAREZCA UN CÓDIGO GENERAL Y USARLO COMO CLAVE PÚBLICA. ASÍ EVE SE TIENE QUE ENFRENTAR A UN PROBLEMA COMPUTACIONALMENTE IMPOSIBLE

MATRIZ PERMUTACIÓN P

$$(x_1, x_2, x_3)\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (x_2, x_1, x_3)$$

$n \times n$

"PERMUTA" → CAMBIO DE ORDEN

$$(x_1, x_2, x_3)\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = (x_3, x_1, x_2)$$

UNA MATRIZ PERMUTACIONAL ES UNA FORMA DE REPRESENTAR UNA PERMUTACIÓN

MATRIZ "SCRAMBLE" S

S ← MATRIZ "SCRAMBLE"

UNA MATRIZ ALEATORIA INVERTIBLE DE TAMAÑO $k \times k$

NOTA: SG Y G SON MATRICES GENERADORAS DEL MISMO CÓDIGO.

$G' = SGP$ ES UNA MATRIZ GENERADORA DE UN CÓDIGO EQUIVALENTE AL QUE GENERAN G Y SG, PUESTO QUE P CAMBIA EL ORDEN DE LAS COLUMNAS. EN PARTICULAR LOS PARÁMETROS (Y CAPACIDAD CORRECTORA) SON LOS MISMOS.

NOTA: LA CLAVE PÚBLICA, ADEMÁS DE LA MATRIZ G', INCLUYE SU CAPACIDAD CORRECTORA.

NOTA: LA CLAVE PRIVADA, ADEMÁS DE LAS MATRICES G, S, P, INCLUYE UN ALGORITMO DE DECODIFICACIÓN DEL CÓDIGO GENERADO POR G

CIFRADO:

- SE OBTIENE LA CLAVE PÚBLICA DEL DESTINATARIO G' UNA MATRIZ $k \times n$ SOBRE $\mathbb{F}_q$ QUE GENERA UN CÓDIGO CON CAPACIDAD CORRECTORA t.
- SE DIVIDE EL MENSAJE A ENVIAR EN BLOQUES DE TAMAÑO k. (MENSAJE SOBRE $\mathbb{F}_q$)

PARA CIFRAR UN BLOQUE $\vec{m}$

1) SE MULTIPLICA $\vec{m}$ POR G': $\vec{x} = \vec{m}G'$

   Y SE OBTIENE $\vec{x}$, VECTOR LONGITUD n.

2) SE GENERA AL AZAR UN VECTOR $\vec{e} \in \mathbb{F}_q^n$

   TAL QUE $\omega_H(\vec{e}) \leq t$ (TIENE AL MENOS $n-t$ COORDENADAS IGUAL A 0)

   ↑ PESO DE HAMMING

3) SE SUMA $\vec{x}$ Y $\vec{e}$: $\vec{c} = \vec{x} + \vec{e}$

EL MENSAJE CIFRADO A ENVIAR ES $\vec{c}$

DESCIFRADO:

EL RECEPTOR RECIBE EL MENSAJE CIFRADO $\vec{c}$

$$\vec{c} = \vec{x} + \vec{e} = \vec{m} G' + \vec{e}$$

PARA DESCIFRAR $\vec{c}$

1) SE MULTIPLICA $\vec{c}$ POR P^{-1}, LA PERMUTACIÓN INVERSA

$$\vec{c}' = \vec{c} P^{-1} = (\vec{m} G' + \vec{e}) P^{-1} = (\vec{m} S G P + \vec{e}) P^{-1}$$

$$= \vec{m} S G + \vec{e} P^{-1} = \vec{m}' G + \vec{e}'$$

$\vec{m}' = \vec{m} S$

$\vec{e}' = \vec{e} P^{-1}$

MISMO PESO QUE $\vec{e}$

2) OBTENEMOS $\vec{m}'G$ A PARTIR DE $\vec{c}'$
ES DECIR USAMOS EL ALGORITMO DE DECODIFICACIÓN DEL CÓDIGO GENERADO POR G PARA CORREGIR EL ERROR $\vec{e}'$ DE PESO MENOR O IGUAL QUE t.

3) OBTENEMOS $\vec{m}'$ A PARTIR DE $\vec{m}'G$
ESTO ES RESOLVER UN SISTEMA DE ECUACIONES.

S INVERTIBLE

4) $\vec{m}' = \vec{m}S \Longrightarrow \vec{m} = \vec{m}'S^{-1}$

FINALMENTE MULTIPLICAMOS $\vec{m}'$ POR LA INVERSA DE LA MATRIZ SCRAMBLE

VENTAJAS

- VELOCIDAD DE CIFRADO Y DESCIFRADO MÁS RÁPIDO QUE RSA Y ELGAMAL
- RESISTENTE A ATAQUES REALIZADOS CON EL ALGORITMO DE SHOR IMPLEMENTADO EN UN ORDENADOR CUÁNTICO.

DESVENTAJA

- EL TAMAÑO DE LAS CLAVES
  $n = 2048$, $k = 1750$, $t = 27$
  2^{80} OPERACIONES PARA ROMPERLO

PERO PARA UN ORDENADOR CUÁNTICO

$n = 6960$, $k = 5400$, $t = 119$

$\Rightarrow 2^{23}$ BITS DE CLAVE PÚBLICA

- NO SE PUEDE EMPLEAR PARA FIRMAS DIGITALES, AUNQUE CON LA MODIFICACIÓN DE NIEDERREITER SE PUEDE

EJ DE MCELIECE EN SAGE

CRIPTOSISTEMA DE NIEDERREITER

PROPONE USAR LA MATRIZ DE CONTROL EN LUGAR DE LA MATRIZ GENERADORA (1986)

SU SEGURIDAD ES EQUIVALENTE A LA DEL SISTEMA DE MCELIECE (XING 1994)

CLAVE PRIVADA

MATRIZ DE CONTROL H DE UN CÓDIGO DE TAMAÑO $(n-k) \times n$

ENMASCARAMOS LA MATRIZ

$$H' = SHP$$

CON S MATRIZ NO SINGULAR TAMAÑO $n-k \times n-k$

P MATRIZ PERMUTACIÓN $n \times n$

CLAVE PÚBLICA: (H', t) CAPACIDAD CORRECTORA

CLAVE PRIVADA: $(H, S, P,$ ALGORITMO DECODIFICACIÓN$)$

CIFRADO:

EL PROCESO ES ANÁLOGO AL DE MCELIECE PERO SE EMPLEA LA MATRIZ H' EN LUGAR DE G' Y ÚNICAMENTE SE PUEDEN CIFRAR LAS PALABRAS DE PESO MENOR O IGUAL QUE t QUE VAN A SER LOS LÍDERES DE LOS

COGRUPOS EN LA DECODIFICACIÓN POR SÍNDROMES.

DESCIFRADO:

IGUAL QUE EN MCELIECE PERO APLICAMOS PRIMERO S^{-1} Y LUEGO P^{-1} (AL REVÉS QUE EN MCELIECE)

ATAQUES FRENTE A MCELIECE (O NIEDERREITER)

- ATAQUES GENÉRICOS DE DESCODIFICACIÓN

INTENTAR RECUPERAR $\vec{m}$ A PARTIR DE $\vec{c}$ USANDO EL CÓDIGO GENERADO POR G'

ALGORITMOS QUE MEJORAN LA DESCODIFICACIÓN DEL CONJUNTO DE INFORMACIÓN: TRATA DE ENCONTRAR k COORDENADAS DEL VECTOR $\vec{c}$ QUE NO TENGAN NINGÚN ERROR.
TOMANDO ESAS COORDENADAS DE $\vec{c}$ Y LA MATRIZ INVERSA FORMADA POR LAS k COLUMNAS SELECCIONADAS DE LA MATRIZ G', PODEMOS RECUPERAR $\vec{m}$.

ESTE ES EL MÉTODO EXPLICADO EN LA PÁGINA 246 DE MUNUERA-TENA

$$\vec{c} = \vec{m}\,G' + \vec{e}$$

COMO $\vec{m}$ TIENE k COORDENADAS NECESITAMOS k ECUACIONES

$$\vec{c}_k = \vec{m}\,G'_k + \vec{e}_k$$

MATRIZ $k \times k$ FILAS Y COLUMNAS $i_1, \ldots, i_k$

VECTOR CON k COMPONENTES $i_1, \ldots, i_k$

SI HAY SUERTE Y $\vec{e} = \vec{0} \Rightarrow \vec{c}_k = \vec{m}\,G'_k$

$$\Rightarrow \vec{m} = \vec{c}_k\,(G'_k)^{-1}$$

- ATAQUES CONTRA LA ESTRUCTURA DEL CÓDIGO

SE TRATA DE INTENTAR RECUPERAR G, S Y P A PARTIR DE G'

¿QUÉ CÓDIGOS SON SEGUROS?

MCELIECE EN SU PROPUESTA ORIGINAL PROPUSO USAR LOS CÓDIGOS DE GOPPA.

SE HAN PROPUESTO POSTERIORMENTE MUCHAS FAMILIAS DE CÓDIGOS COMO REED-SOLOMON GENERALIZADO, REED-MULLER, CUASI-CÍCLICOS, ...

SORPRENDENTEMENTE, LA MAYORIA DE ESTAS FAMILIAS DE CÓDIGOS SE HA DEMOSTRADO QUE SON

INSEGURAS, PERO LA PROPUESTA ORIGINAL DE MCELIECE (CÓDIGOS DE GOPPA) SIGUE SIENDO SEGURA Y ERA/ES UN FIRME CANDIDATO PARA LA COMPETICIÓN DE ESTANDARIZACIÓN DEL NIST.

OTROS MÉTODOS

RETÍCULOS (LATTICE)

ECUACIONES CUADRÁTICAS MULTIVARIABLE

FUNCIONES HASH