CODIGOS Y CRIPTOGRAFIA. INFORMÁTICA. DIEGO RUANO 29/9 2022

DESCODIFICACIÓN CÓDIGOS RS

$C \; RS_{n,k} \; [n, k, d = n-k+1]_q \qquad (q \geq n)$

CAPACIDAD CORRECTORA: $t = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{n-k}{2} \right\rfloor$

PARA UNA PALABRA RECIBIDA $\vec{r} = \vec{c} + \vec{e}$, CON $w(\vec{e}) \leq t$

QUEREMOS DETERMINAR $Q(X,Y) \in \mathbb{F}_q[X,Y] \setminus \{0\}$

$$Q(X,Y) = Q_0(X) + Y Q_1(X) \qquad (\neq 0)$$

↖ POLINOMIO INTERPOLADOR DE LA PALABRA RECIBIDA

TAL QUE

1) $Q(x_i, r_i) = 0 \quad \forall i = 1, \ldots, n$
2) $\deg Q_0 \leq n-1-t$
3) $\deg Q_1 \leq n-1-t-(k-1)$

Th: EXISTE UN POLINOMIO INTERPOLADOR $\neq 0$ QUE VERIFICA 1, 2, Y 3)

DEM

$$Q = Q(x_1, z_1) = Q_0(x_1) + z_1 Q_1(x_1) = \underbrace{Q_{00}}_{\text{DESCONOCIDO}} + \underbrace{Q_{01}}_{\text{CONOCIDO}} x_1 + Q_{02} x_1^2 + \dots + Q_{0n} x_1^n + z_1 Q_{10} + z_1 Q_{11} x_1 + z_1 Q_{12} x_1^2 + \dots + z_1 Q_{1n} x_1^n$$

1) IMPONE n ECUACIONES SOBRE LOS COEFICIENTES DE Q_0 Y Q_1

EL SISTEMA TIENE SOLUCIÓN NO NULA SI TENEMOS MÁS VARIABLES (POSIBLES COEFICIENTES) QUE ECUACIONES

PARA Q_0 TENEMOS $n-1-t+1$ COEFICIENTES $\Big\} \Rightarrow$

" Q_1 " $n-1-t-(k-1)+1$ "

$$n-1-t+1+n-1-t-(k-1)+1 = 2n-2t-(k-1)$$

$$= 2n-2\left[\frac{n-k}{2}\right]-(k-1) \geq 2n-2\,\frac{n-k}{2}-(k-1) =$$

$$= n+1 \Rightarrow \#\text{COEFICIENTES} > n$$

t ↑

$\#\text{COEFICIENTES} \geq n+1$

TENEMOS MÁS VARIABLES QUE ECUACIONES $\Rightarrow \exists\, Q$

Th SI LA PALABRA ENVIADA FUE GENERADA POR $f(x)$ Y EL NÚMERO DE ERRORES ES MENOR QUE $d/2$ ENTONCES

$$f(x) = \frac{-Q_0(x)}{Q_1(x)}$$

DEM

$\vec{c} = (f(x_1), \dots, f(x_n))$ $\quad \vec{r} = \vec{c} + \vec{e}$, CON $w(\vec{e}) \leq t$

CALCULAMOS $Q(x, y) \neq 0$ QUE VERIFICA 1, 2 Y 3)

1) $\Rightarrow 0 = Q(x_i, r_i) = Q(x_i, c_i + e_i) = Q(x_i, f(x_i) + e_i) = 0$

$\forall\ i = 1, 2, \dots, n$

$e_i = 0$ SI NO HAY ERROR EN LA COORDENADA i-ESIMA

$e_i = 0$ EN AL MENOS $n - t$ POSICIONES DE $\vec{e} \Rightarrow$

$\Rightarrow Q(x_i, f(x_i)) = 0$ PARA AL MENOS $n - t$ VALORES DE i

(EXACTAMENTE CUANDO $c_i = e_i$ Y NO HAY ERROR)

$Q(X, f(X))$ POLINOMIO EN X $(\in \mathbb{F}_q[X])$

$\| $

$Q_0(X) + f(X)\, Q_1(X)$ TIENE GRADO COMO MUCHO $n-t-1$

deg: $n-1-t$ $\quad k-1 \quad n-1-t \quad (k-1)$

$n-1-t$

Y TIENE AL MENOS $n-t$ RAICES

#RAICES > GRADO

$Q(X, f(X)) = 0$ COMO POLINOMIO

$\Rightarrow Q_0(X) + f(X)\, Q_1(X) = 0$

$$\Rightarrow \quad f(x) = \frac{-Q_0(x)}{Q_1(x)}$$ □

$$\vec{c} = (f(x_1), \dots, f(x_n))$$

$$f = f_0 + f_1 x + \dots + f_{k-1} x^{k-1}$$

$(f_0, \dots, f_{k-1})$ ← VECTOR INFORMACIÓN

$$(f_0, \dots, f_{k-1})\, G = \vec{c}$$

$$Q(X,Y) = Q_0(X) + Y\,Q_1(X)$$

$$= Q_1(X)\left(Y + \frac{Q_0(X)}{Q_1(X)}\right) = Q_1(X)\,(Y - f(X))$$

x_i (ERROR) c_i $\neq 0$ SI ERROR

x_i DONDE HAY UN ERROR $\rightarrow$ ES UN CERO DE Q_1

(PORQUE $Y - f(x) \neq 0$ EN ESE CASO)

$Q_1(X)$ SE LE CONOCE COMO POLINOMIO LOCALIZADOR DE ERRORES

NOTACIÓN: $l_0 = n - 1 - t$ GRADO Q_0

$l_1 = n - 1 - t - (k-1)$ GRADO Q_1

ALGORITMO DECODIFICACIÓN

INPUT $\vec{r}=(r_1,\dots,r_n)$

1) ENCUENTRA UNA SOLUCIÓN NO NULA DE

$$M=\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{l_0} & r_1 & r_1x_1 & \cdots & r_1x_1^{l_1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{l_0} & r_2 & r_2x_2 & \cdots & r_2x_2^{l_1} \\ & & & & & & & & \\ 1 & x_n & x_n^2 & \cdots & x_n^{l_0} & r_n & r_nx_n & \cdots & r_nx_n^{l_1} \end{pmatrix}$$

$$M\begin{pmatrix} Q_{00} \\ Q_{01} \\ \vdots \\ Q_{0l_0} \\ Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,l_1} \end{pmatrix}=\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

VARIABLES

$Q(x_i,r_i)=0$ (FILA i)

$Q_0(x_i)+r_iQ_1(x_i)$

FILA i x VECTOR =

1 CONDICIÓN i-ESIMA

2) DEFINE

$$Q_0(X) = \sum_{j=0}^{l_0} Q_{0,j} X^j \quad , \quad Q_1(X) = \sum_{j=1}^{l_1} Q_{1,j} X^j$$

$$g(X) = - \frac{Q_0(X)}{Q_1(X)}$$

3) SI $g(X) \in P_K$ Y $d(\vec{r}, (g(\alpha_1), \ldots, g(\alpha_n))) \leq t$

OUTPUT $(g(\alpha_1), \ldots, g(\alpha_n))$

SI NO

OUTPUT ERROR

EJ 4.2.1 LIBRO JUSTESEN - HØHOLDT