Лекция № 12
Код Гоппы

Опр-ие 1 Зафикс. $m \geq 1$, $L = [\alpha_1 \ldots \alpha_n] \subseteq \mathbb{F}_{q^m}$, α_i — различны

$g(x) \in \mathbb{F}_{q^m}[x]$, $\deg g(x) = r$, т.ч. $g(\alpha_i) \neq 0 \ \forall i$

Код Гоппы длины n

(1) $$C = \Gamma(L, g) = \left\{ c \in \mathbb{F}_q^n : \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} \equiv 0 \bmod g(x) \right\}$$

Замечание 1. $\Gamma(L, g)$ — линейный (если $c_1, c_2 \in C$, то $c_1 + c_2 \in C$; если $c_1 \in C$, $\alpha \in \mathbb{F}_{q^m}$, то $\alpha \cdot c_1 \in C$)

2. $(x - \alpha_i)^{-1}$ существует в $\mathbb{F}_{q^m}[x] / g(x)$, т.к. α_i не являются корнями $g(x)$

В явном виде, $(x - \alpha_i)^{-1} = -\dfrac{g(x) - g(\alpha_i)}{x - \alpha_i} \cdot g^{-1}(\alpha_i)$

Проверим, $\cancel{(x - \alpha_i)} \cdot \left(-\dfrac{g(x) - g(\alpha_i)}{\cancel{x - \alpha_i}} \cdot g^{-1}(\alpha_i) \right) = -g(x) \cdot g^{-1}(\alpha_i) + 1$

$\equiv 1 \bmod g(x)$

из (1): $c \in \Gamma(L, g) \Leftrightarrow \overbrace{-\sum_{i=1}^{n} c_i \underbrace{\frac{g(x) - g(\alpha_i)}{x - \alpha_i}}_{\text{степень} < \deg(x)}}^{(2)} \cdot g^{-1}(\alpha_i) = 0$ в $\mathbb{F}_{q^m}[x]$

Т.к. сумма мн-в степени $< \deg g(x)$ есть мн-н степени $< \deg g(x)$, то "редукция по mod $g(x)$" ничего не меняет.

Построим проверочную матрицу кода Гоппы

Пусть $g(x) = \sum_{j=0}^{r} g_j \cdot x^j$, $g_j \in \mathbb{F}_{q^m}$, $g_r \neq 0$

$$\frac{g(x)-g(d_i)}{x-d_i} = \frac{\sum_{j=0}^{r} g_j (x^j - d_i^j)}{x-d_i} = \frac{g_r(x^r-d_i^r)+g_{r-1}(x^{r-1}-d_i^{r-1})+\dots+g_1(x-d_i)+g_0\overbrace{(1-1)}^{=0}}{x-d_i} =$$

$$\left\{ x^a - y^a = (x-y)(x^{a-1}+x^{a-2}\cdot y + \dots x\cdot y^{a-2}+y^{a-1}) \right\}$$

$$= g_r(x^{r-1}+d_i x^{r-2}+\dots+d_i^{r-1}) + g_{r-1}(x^{r-2}+d_i x^{r-3}+\dots+d_i^{r-2}) + \dots +$$
$$+ g_2(x+d_i)+g_1 .$$

В (2):

коэфф-ты при x^{r-1}: $g_r\cdot g^{-1}(d_1)\cdot c_1 + g_r\cdot g^{-1}(d_2)\cdot c_2 + \dots + g_r\, g^{-1}(d_n)\cdot c_n$

— // — x^{r-2}: $(g_{r-1}+g_r d_1)\cdot g^{-1}(d_1)\cdot c_1 + (g_{r-1}+g_r d_2)\, g^{-1}(d_2)\cdot c_2 + \dots + (g_{r-1}+g_r d_n)\, g^{-1}(d_n)\, c_n$

⋮

— // — x^0 $(g_1+g_2 d_1+\dots g_r d_1^{r-1})\cdot g^{-1}(d_1)\cdot c_1 + \dots + (g_1+g_2 d_n+\dots g_r d_n^{r-1})\cdot g^{-1}(d_n)\cdot c_n$

$c\in\Gamma(L,g) \iff$ коэфф-ты при x^j в (2) $=0\ \forall j \iff \overline{H}\cdot c = 0$, где

$$\overline{H} = \begin{array}{c} \\ r \end{array} \overbrace{\begin{bmatrix} g_r\cdot g^{-1}(d_1) & g_r\, g^{-1}(d_2) & \dots & g_r g^{-1}(d_n) \\ (g_{r-1}+g_r d_1) g^{-1}(d_1) & (g_{r-1}+g_r d_2) g^{-1}(d_2) & \dots & (g_{r-1}+g_r d_n) g^{-1}(d_n) \\ \vdots & & & \\ (g_1+\dots+g_r d_1^{r-1}) g^{-1}(d_1) & \dots & \dots & (g_1+\dots+g_r d_n^{r-1}) g^{-1}(d_n) \end{bmatrix}}^{n}$$

$$= \underbrace{\begin{bmatrix} g_r & 0 & 0 & \dots & 0 \\ g_{r-1} & g_r & 0 & \dots & 0 \\ g_{r-2} & g_{r-1} & g_r & \dots & 0 \\ g_1 & g_2 & g_3 & \dots & g_r \end{bmatrix}}_{G} \cdot \underbrace{\begin{bmatrix} 1 & \dots & 1 \\ d_1 & \dots & d_n \\ \vdots & & \\ d_1^{r-1} & \dots & d_n^{r-1} \end{bmatrix}}_{X} \cdot \underbrace{\begin{bmatrix} g^{-1}(d_1) & & & 0 \\ & g^{-1}(d_2) & & \\ & & \ddots & \\ 0 & & & g^{-1}(d_n) \end{bmatrix}}_{Y}$$

(G: $r\times r$; X: $r\times n$; Y: $n\times n$)

$\overline{H} = G X \cdot Y$

Т.к. G – обратима, часто $\overline{H}$ умножают на G^{-1} слева, получаем

$$\overline{H}' := G^{-1} \cdot \overline{H} = \begin{array}{c} \uparrow \\ r \\ \downarrow \end{array} \overbrace{\begin{bmatrix} g^{-1}(\alpha_1) & \dots & g^{-1}(\alpha_n) \\ \alpha_1 g^{-1}(\alpha_1) & \dots & \alpha_n g^{-1}(\alpha_n) \\ \vdots & & \\ \alpha_1^{r-1} g^{-1}(\alpha_1) & \dots & g_n^{r-1} g^{-1}(\alpha_n) \end{bmatrix}}^{n} \in \mathbb{F}_{q^m}^{r\times n}$$

Проверочная матрица с эл-тами из $\mathbb{F}_q$ получается из $\overline{H}'$ заменой каждого эл-та матрицы соответствующим вектором-столбцом длины m над $\mathbb{F}_q$. При такой замене кол-во строк новой матрицы (назовём её $\underset{\in \mathbb{F}_q^{n-k\times n}}{H}$) есть $r.m$ $\Rightarrow$ $\mathrm{rank}(H) \leq r.m$ $\Rightarrow$ размерность кода Гоппы

$k = n - \mathrm{rank}(H) \geq n - r.m$.

Пример $q=2$, $g(x) = x^2+x+1$, $m=3$ $\mathbb{F}_{2^m} = \mathbb{F}_2[x]/(x^3+x+1)$

$L = \mathbb{F}_2^3 = \{0, 1, \alpha, \alpha^2, \alpha^3 = \alpha+1, \alpha^4 = \alpha^2+\alpha, \alpha^5 = \alpha^2+\alpha+1, \alpha^6 = \alpha^2+1\}$

Построим $\Gamma(L, g)$. $n = |L| = 8$

$k \geq 8 - r.m = 8 - 2\cdot 3 = 2$

$d \geq 4$

$$\overline{H}' = \begin{bmatrix} \frac{1}{g(0)} & \frac{1}{g(1)} & \frac{1}{g(\alpha)} & \dots & \frac{1}{g(\alpha^2+1)} \\ \frac{0}{g(0)} & \frac{1}{g(1)} & \frac{\alpha}{g(\alpha)} & \dots & \frac{\alpha^2+1}{g(\alpha^2+1)} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 \end{bmatrix}$$

$$\Rightarrow \begin{array}{c} 1 \\ \alpha \\ \alpha^2 \\ 1 \\ \alpha \\ \alpha^2 \end{array} \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \leftarrow \text{проверочная матрица для } \Gamma(L, g)$$

II Минимальное расстояние $\Gamma(L, g)$

Лемма 1 $d(\Gamma(L,g)) \geq r+1$ $(\deg g(x) = r)$

Δ Пусть $c \in \Gamma(L,g)$, $wt(c) = w \Rightarrow c_i = 0$, $i \in \{i_1, \dots i_w\}$ – индексы ненулевых позиций в c

$$\sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} \equiv 0 \mod g(x)$$

$$\frac{1}{x-\alpha_{i_j}} = \frac{\prod_{k=1, k\neq j}^{w} (x - \alpha_{i_k})}{\prod_{j=1}^{w} (x - \alpha_{i_j})}$$

$$\frac{\sum_{j=1}^{w} c_{i_j} \prod_{k=1, k\neq j}^{w} (x - \alpha_{i_k})}{\prod_{j=1}^{w} (x - \alpha_{i_j})} \equiv 0 \mod g(x)$$

числитель $=: f(x)$
знаменатель $=: h(x)$

Т.к. α_{i_j} – не корни $g(x)$, то $g(x)$ делит $f(x)$.

$$\deg f(x) \leq w - 1 \Rightarrow \underbrace{\deg g(x)}_{r} \leq \deg f(x) \leq w - 1$$

$$r \leq w - 1 \Rightarrow w \geq r+1 \quad \blacktriangleright$$

Лемма 2 Для $q = 2$ и g – сепарабельного (т.е. в g нет корней кратности >1), справедливо

$$d(\Gamma(L, g)) \geq 2r + 1.$$

III Декодирование кода Гоппы

$$y = (y_1 \dots y_n) = (c_1 \dots c_n) + (e_1 \dots e_n), \quad wt(e) = t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$$

Пусть $B = \{ i : e_i \neq 0 \}$ – позиции ошибок, $|B| = t$

$$\sigma(x) = \prod_{i \in B} (x - \alpha_i) \text{ – полином-локатор}, \quad \deg \sigma(x) = t$$

$$\omega(x) = \sum_{i \in B} e_i \cdot \prod_{j \in B, j \neq i} (x - \alpha_j), \quad \deg \omega(x) = t - 1$$

НОД $(\sigma(x), w(x)) = 1$ (т.к. d_i не являются корнями $w(x)$)

синдром полученного y - многочлен $S(x) \in \mathbb{F}_{q^m}[x]/g(x)$ вида:

$$S(x) = \sum_{i=1}^{n} \frac{y_i}{x-d_i} = \underbrace{\sum_{i=1}^{n} \frac{c_i}{x-d_i}}_{\equiv 0 \bmod g(x)} + \sum_{i=1}^{n} \frac{e_i}{x-d_i} = \sum_{i=1}^{n} \frac{e_i}{x-d_i} \bmod g(x)$$

Для $q=2$, синдром $S(x)$ считается по модулю $g^2(x)$ $(\Gamma(L,g)=\Gamma(L,g^2))$

Лемма 3

1) $e_k = \dfrac{w(d_k)}{\sigma'(d_k)} \quad \forall k \in B$

2) $\sigma(x) \cdot S(x) = w(x) \bmod g(x)$ (замечание: для $q=2$: $\sigma(x) \cdot S(x) \equiv w(x) \bmod g^2(x)$)

◁ 1) $\sigma'(x) = \dfrac{\partial \prod_{i\in B}(x-d_i)}{\partial x} = \sum_{i\in B} \prod_{\substack{j\in B \\ j\neq i}} (x-d_j)$

$$\left.\begin{aligned} \sigma'(d_k) &= \prod_{\substack{j\in B \\ j\neq k}} (d_k - d_j) \\ w(d_k) &= \sum_{i\in B} e_i \prod_{\substack{j\in B \\ j\neq i}} (d_k-d_j) = e_k \prod_{\substack{j\in B \\ j\neq k}} (d_k-d_j) \end{aligned}\right\} \Rightarrow \frac{w(d_k)}{\sigma'(d_k)} = e_k$$

2) $\sigma(x) \cdot S(x) = \prod_{i\in B} (x-d_i) \cdot \sum_{i\in B} \dfrac{e_i}{x-d_i} = \sum_{i\in B} e_i \cdot \prod_{\substack{j\in B \\ j\neq i}} (x-d_j) \equiv w(x)$ ▶

Декодирование

$$\underbrace{\sigma(x)}_{\sigma_0+\sigma_1 x+\ldots+\sigma_{t-1}x^{t-1}+x^t} \cdot \overbrace{S(x)}^{\text{известен}} \equiv \underbrace{w(x)}_{w_0+w_1x+\ldots+w_{t-1}x^{t-1}} \bmod g(x)$$

$t + t = 2t$ неизвестных

$\deg g = r$ - число уравнений

$2t \le r$

$t \le \dfrac{r}{2}$

$$\left\{ \begin{aligned} & d \geq r+1 \\ & t \leq \frac{d-1}{2} \leq \frac{r}{2} \end{aligned} \right\}$$

Пример

$q=3$, $m=2$; $\mathbb{F}_{3^2}[x]/(x^2+2x+2)$ α – примитивный

$g = x^2+\alpha x+2\alpha$, $\deg g(x) = 2$ $\Rightarrow$ min. расстояние $\geq 3 \Rightarrow$ исправляем ≥ 1 ошибку

$L = \{1, 2, 2\alpha+2, \alpha, 2\alpha, \alpha+1, 2\alpha+1\}$, $|L| = 7$ $\Rightarrow$ длина кода $= 7$

$$\overline{H}' = \begin{bmatrix} 1 & 2\alpha+2 & 1 & \alpha & 2\alpha+1 & \alpha+2 & 2\alpha+2 \\ 1 & \alpha+1 & 2\alpha+2 & \alpha+1 & 1 & \alpha & \alpha \end{bmatrix}$$

$$\downarrow$$

$$\begin{bmatrix} 1 & 2 & 1 & 0 & 1 & 2 & 2 \\ 0 & 2 & 0 & 1 & 2 & 1 & 2 \\ 1 & 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 1 & 1 \end{bmatrix} \in \mathbb{F}_3^{\,n-k \times n}, \quad k=3$$

$y = [0\ 0\ 2\ 2\ 1\ 0\ 1]$

$\frac{1}{x-1} = 2x+2\alpha+2 \mod g(x)$

$\frac{1}{x-2\alpha} = (\alpha+2)x \mod g(x)$

$\frac{1}{x-2} = (\alpha+1)x+\alpha \mod g(x)$

$\frac{1}{x-(\alpha+1)} = (2\alpha+1)x + 2\alpha+2 \mod g(x)$

$\frac{1}{x-(2\alpha+2)} = 2x+1 \mod g(x)$

$\frac{1}{x-(2\alpha+1)} = (\alpha+1)x + (\alpha+1) \mod g(x)$

$\frac{1}{x-\alpha} = 2\alpha\cdot x + \alpha+1 \mod g(x)$

$$S(x) = \sum_{i=1}^{7} \frac{y_i}{x-\alpha_i} = 0\cdot(2x+2\alpha+2) + 0\cdot((\alpha+1)x+\alpha) + 2(2x+1) + \dots$$

$$\dots 1\cdot((\alpha+1)x+(\alpha+1)) = x+2 \mod g(x)$$

$\deg \sigma(x) = 1 \Rightarrow \sigma(x) = \underset{i\text{-поз. ошибки}}{\prod (x-\alpha_i)} = x - \sigma_0$

$\deg \omega(x) = 0 \Rightarrow \omega = \omega_0$

$$(x-\sigma_0)\cdot(x+2) \equiv \omega_0 \mod x^2+\alpha x+2\alpha$$

$$x^2+(2-\sigma_0)x-2\sigma_0 \equiv \omega_0 \mod x^2+\alpha x+2\alpha$$

$$\text{|||}$$

$$-\alpha x-2\alpha = 2\alpha x+\alpha$$

$$(2-\sigma_0+2\alpha)x-2\sigma_0+\alpha = \omega_0 \mod x^2+\alpha x+2\alpha$$

$$\Rightarrow \begin{cases} 2-\sigma_0+2\alpha = 0 \\ -2\sigma_0+\alpha = \omega_0 \end{cases} \Rightarrow \begin{cases} \sigma_0 = 2\alpha+2 \\ \omega_0 = \alpha+2\alpha+2 = 2 \end{cases}$$

$$\sigma(x) = x-\underbrace{(2\alpha+2)}_{}, \quad \omega_0 = 2$$

$\| \; L[3] \Rightarrow$ ошибка в третьей позиции (считая с 1)

$$e_3 = \frac{\omega(\alpha_3)}{\sigma'(\alpha_3)} = \frac{2}{1} = 2 \Rightarrow c = y-[0,0,2,0,0,0,0]$$

$$= [0,0,0,2,1,0,1].$$