Структурные Атаки

SD: Найти e : $He = y$; $\underbrace{mG}+\underbrace{e} = y$

1. Атаки декод. (ISD)
2. Структур. атаки (восст. секрет. ключа → эффек. декод.)
   - Общ. идеи схожи

(ISD — дек. по инф. множ-вам)

$\Gamma(g, L)$ g - многочлен степени t $\quad L \subseteq \mathbb{F}_q^n$ $\quad$ Задача: Найти g', L'

$$H = \begin{pmatrix} \frac{1}{g(\alpha_1)} & \cdots & \frac{1}{g(\alpha_n)} \\ \frac{\alpha_1}{g(\alpha_1)} & \cdots & \frac{\alpha_n}{g(\alpha_n)} \\ \vdots & & \vdots \\ \frac{\alpha_1^{t-1}}{g(\alpha_1)} & \cdots & \frac{\alpha_n^{t-1}}{g(\alpha_n)} \end{pmatrix}$$

Подполе $\Rightarrow$ H_{GOPPA}

$$\mathcal{A} = GRS^{\perp} \cap F_p$$

$Goppa \subset \mathcal{A}$

Легко восстановить

L, g GRS-код

$G_{\text{рид}} = SGP$

"Хорошие" коды:

1. Подполевые $C_1, C_2 \quad C_1 \otimes C_2$
2. Сплет. + MDPC
3. Модификации кодов (Тензор. произвед.; $(U|U+V)$ - плоткина)

Виды структурных атак:

1. Различители (алг., отличающие код от случ.)
2. Перебор g', L' (с оптимизацией SSA)

$L' = (\alpha_1, \dots \alpha_n) \to set(L')$

алг. расщепления носителя

$\exists$ ли σ : $\sigma(C') = C$

(ex) $L' = (\alpha_4, \alpha_2, \alpha_1, \alpha_3) \xrightarrow{SSA} (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$

3. Алгебраич. криптоанализ (дано: $G, H \to$ сист. уравнений $\to$ решаем)

$$G H^T_{изв.} = 0$$

Перебор:

$g(x)$ – Неприв. унитар. многочлен над $\mathbb{F}_{p^m} = \mathbb{F}_{2^m}$

$$M_t(\mathbb{F}_{2^m}) = \frac{1}{t}\sum_{d \mid t} \mu(d) \cdot 2^{\frac{mt}{d}} \simeq \frac{2^{mt}}{t}$$ – кол-во многочленов

$h \in \mathbb{F}_{2^m}^n \Rightarrow \binom{2^m}{n}$ (ex) $\mathbb{F}_{2^{12}}$; $n \simeq 3400$, $t \simeq 64$

$t = \deg g(x)$

Сложность: $\binom{2^m}{n} \cdot \frac{2^{mt}}{t}$

$|L| = 2^m$

Пример:

$\exists\, \mathbb{F}_{2^m}$, $n = 2^m$; $\deg(g(x)) = t$

Алгоритм:

Вход: матрица G кода $\Gamma(g, L)$

Выход: g', L' : $\Gamma(g, L) = \Gamma(g', L')$

1. $\exists L' = (0, \alpha, \alpha^2, \dots \alpha^{2^m-1})$
2. Повторить
3. Выбрать $g'(x)$: $\deg(g') = t$ и g' - унитар. неприв.
4. $SSA(\Gamma(g, L), \Gamma(g', L'))$
5. Пока $\Gamma(g, L) \not\cong \Gamma(g', L')$

Вернуть g', L'

Зная g', L' можем декод. $\Gamma(g, L)$

$G \cdot H^T = 0$

Сложность: $\frac{n^3 \cdot 2^{m(t-3)}}{mt}$

CFS - ЦП

$n \approx K$, $t \approx 11$

Различители:

Явл. ли код случ. или $\in$ семейству (знаем G или H)

1. Алгебраический различитель (2011)
   - Знаем G или H → сост. сист. уравнений $\boxed{G}\,\underset{\text{числ.}}{H'}{}^{T} = 0$ → Линеаризация →
   - → Выделяют подсистему лин. уравнений → rank, dim(ker) — отлич. от случ. кода
   - Работает, когда $R \approx 1$ $(R > 0{,}95)$ ~~СТБ~~ $R = \frac{k}{n}$ McEliece $R \in [0.7, 0.85]$
   - Атака 2024
     - $R \geq 1 - \sqrt{\frac{2m \log q}{q^m \log m}}\,(1 + o(1))$ при $n = q^m$

2. Разделитель на произведении Шура (Адамара) (2023)

- Альтернативное описание (2011)
- Доказана корректность
- Улучшена граница на R ($0{,}95$)
- Идея: $\dim\left(\left(\Gamma(g,\lambda)^{\perp}\right)^{(2)}\right)$

Произв. Шура

$(x_1, x_2, \ldots, x_n) * (y_1, y_2 \ldots y_n) = (x_1 \cdot y_1, \ldots, x_n y_n)$

$C_1 * C_2 = \{ c_1 * c_2 \mid c_1 \in C_1,\ c_2 \in C_2 \}$

$C^{(2)} = C * C$

Случ. код: $\dim = n$ $[n, n]$

Гоппа: $\dim < n$