Kryptanalyse von McEliece

Bachelorarbeit

Alexander Kulpe

Ruhr-Universität Bochum

09.02.2022

Inhaltsverzeichnis

Inhaltsverzeichnis

Definition

Parameter:

- $\mathbb{F}_{p^m}$, wobei p prim und $m \geq 1$
- $L = \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_{p^m}$, unterschiedliche α_i, $n \leq p^m$
- $g(x) \in \mathbb{F}_{p^m}[x], \deg g(x) \leq t$, s.d. $g(\alpha_i) \neq 0 \forall i$

Definition

Parameter:

- $\mathbb{F}_{p^m}$, wobei p prim und $m \geq 1$
- $L = \{\alpha_1, \dots, \alpha_n\} \subset \mathbb{F}_{p^m}$, unterschiedliche α_i, $n \leq p^m$
- $g(x) \in \mathbb{F}_{p^m}[x], \deg g(x) \leq t$, s.d. $g(\alpha_i) \neq 0 \forall i$

Goppa-Code Γ der Länge n ist

$$\Gamma = \Gamma(L, g) = \left\{ c \in \mathbb{F}_p^n \mid \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} = 0 \mod g(x) \right\}$$

Parity-Check-Matrix

$$\mathfrak{A} = \begin{pmatrix} g^{-1}(\alpha_1) & \dots & g^{-1}(\alpha_n) \\ \alpha_1 g^{-1}(\alpha_1) & \dots & \alpha_n g^{-1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ \alpha_1^{t-1} g^{-1}(\alpha_1) & \dots & \alpha_n^{t-1} g^{-1}(\alpha_n) \end{pmatrix} \in \mathbb{F}_{p^m}^{t \times n}$$

Durch Wahl einer fixen Basis erhalten wir eine Matrix über $\mathbb{F}_p^{tm \times n}$ durch eine natürliche Bijektion $\mathbb{F}_{p^m}^{t \times n} \to \mathbb{F}_p^{tm \times n}$.

Beispiel

- $\mathbb{F}_{p^m} = \mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3 + x + 1)$
- $g(x) = x^2 + x + 1$ irreduzibel in $\mathbb{F}_2$
- $L = \mathbb{F}_{2^3} = \{0, 1, \alpha, \alpha^2, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^2 + 1\}$, wobei $\alpha^3 + \alpha + 1 = 0$

Beispiel

- $\mathbb{F}_{p^m} = \mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3 + x + 1)$
- $g(x) = x^2 + x + 1$ irreduzibel in $\mathbb{F}_2$
- $L = \mathbb{F}_{2^3} = \{0, 1, \alpha, \alpha^2, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^2 + 1\}$, wobei $\alpha^3 + \alpha + 1 = 0$

$$\mathfrak{A} = \begin{pmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 \end{pmatrix} \text{ über } \mathbb{F}_{2^3}$$

Beispiel

- $\mathbb{F}_{p^m} = \mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3+x+1)$
- $g(x) = x^2+x+1$ irreduzibel in $\mathbb{F}_2$
- $L = \mathbb{F}_{2^3} = \{0, 1, \alpha, \alpha^2, \alpha+1, \alpha^2+\alpha, \alpha^2+\alpha+1, \alpha^2+1\}$, wobei $\alpha^3+\alpha+1=0$

$$\mathfrak{A} = \begin{pmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 \end{pmatrix} \text{ über } \mathbb{F}_{2^3}$$

$$\mathfrak{A}' = \left(\begin{array}{cccccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ \hline 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right) \text{ über } \mathbb{F}_2$$

Dekodierung

- Minimale Distanz von $\Gamma(L, g)$ ist $d \geq t + 1$
- Chiffrat $y = (y_1, \ldots, y_n) = (c_1, \ldots, c_n) + (e_1, \ldots, e_n)$ mit $\omega(e) \leq \lfloor \frac{d-1}{2} \rfloor$
- Fehlerpositionen $\mathfrak{B} = \{i \mid e_i \neq 0\}$, $|\mathfrak{B}| = \omega(e)$

Dekodierung

- Syndrom $s(y) = \sum_i \frac{y_i}{x-\alpha_i} = \sum_i \frac{e_i}{x-\alpha_i} \mod g(x)$
- Zwei Hilfspolynome:

$$\sigma(x) = \prod_{i \in \mathfrak{B}} (x - \alpha_i) \text{ Polynom zur Fehlerlokalisierung}$$

$$w(x) = \sum_{i \in \mathfrak{B}} e_i \prod_{j \in \mathfrak{B}, j \neq i} (x - \alpha_j)$$

- Identitäten:

$$e_k = \frac{w(\alpha_k)}{\sigma'(\alpha_k)} \quad \forall k \in \mathfrak{B}$$

$$\sigma(x)s(x) = w(x) \mod g(x)$$

- $\deg \sigma(x) = |\mathfrak{B}| = \omega(e), \deg w(x) = \omega(e) - 1$
- $\deg g = t$ Gleichungen mit $2\omega(e) - 1$ Unbekannten. Da $\omega(e) < \frac{t-1}{2}$ können e_k bestimmt werden.

Inhaltsverzeichnis

Definition

Parameter:

- $[n, k, d]$-Code
- $1 \leq k < n$; endlicher Körper $\mathbb{F}_q$ mit $q > n$.
- $\alpha = (\alpha_1, \ldots, \alpha_n), \alpha_i \in \mathbb{F}_q$, alle α_i verschieden
- $z = (z_1, \ldots, z_n), z_i \in \mathbb{F}_q \setminus \{0\}$

Definition

Parameter:

- $[n, k, d]$-Code
- $1 \leq k < n$; endlicher Körper $\mathbb{F}_q$ mit $q > n$.
- $\alpha = (\alpha_1, \ldots, \alpha_n), \alpha_i \in \mathbb{F}_q$, alle α_i verschieden
- $z = (z_1, \ldots, z_n), z_i \in \mathbb{F}_q \setminus \{0\}$

GRS-Code der Länge n ist

$$GRS_k(\alpha, z) = \{(z_1 f(\alpha_1), \ldots, z_n f(\alpha_n)) \in \mathbb{F}_q^n \mid f \in \mathbb{F}_q[x], \deg f(x) \leq k - 1\}$$

Parity-Check-Matrix

$$\mathfrak{A} = \begin{pmatrix} z_1 & \dots & z_n \\ z_1\alpha_1 & \dots & z_n\alpha_n \\ \vdots & \ddots & \vdots \\ z_1\alpha_1^{n-k-1} & \dots & z_n\alpha_n^{n-k-1} \end{pmatrix} \in \mathbb{F}_q^{(n-k)\times n}$$

Kenntnis von α, z erlaubt effizientes Dekodieren.

McEliece mit GRS-Codes

- $sk = (H, \mathfrak{A})$, wobei $H \in \mathrm{GL}(n-k, \mathbb{F}_q), \mathfrak{A} \in \mathbb{F}_q^{(n-k)\times n}$ Parity-Check-Matrix
- $pk = \mathfrak{B} = H\mathfrak{A} \in \mathbb{F}_q^{(n-k)\times(n-k)}$
- Unter Kenntnis von sk ist effizientes Dekodieren für bis zu $\lfloor \frac{n-k}{2} \rfloor$ Fehlern möglich.

Inhaltsverzeichnis

Vorbereitung: Allgemeines

- Angriff auf McEliece mit GRS-Codes
- Input: Matrix $\mathfrak{B}$
- Output: Matrizen $H, \mathfrak{A}$, s.d. $\mathfrak{B} = H\mathfrak{A}$
- Betrachte $\mathbb{F} = \mathbb{F}_q \cup \{\infty\}$ mit $\frac{1}{\infty} = 0, \frac{1}{0} = \infty, f(\infty) = f_{\deg f}$

Vorbereitung: Struktur Matrizen

- $H = \begin{pmatrix} f_0^{(1)} & \dots & f_{n-k-1}^{(1)} \\ f_0^{(2)} & \dots & f_{n-k-1}^{(2)} \\ \vdots & \ddots & \vdots \\ f_0^{(n-k)} & \dots & f_{n-k-1}^{(n-k)} \end{pmatrix}$, $\mathfrak{A} = \begin{pmatrix} z_1 & \dots & z_n \\ z_1\alpha_1 & \dots & z_n\alpha_n \\ \vdots & \ddots & \vdots \\ z_1\alpha_1^{n-k-1} & \dots & z_n\alpha_n^{n-k-1} \end{pmatrix}$
- $\mathfrak{B} = \begin{pmatrix} z_1 f^{(1)}(\alpha_1) & \dots & z_n f^{(1)}(\alpha_n) \\ z_1 f^{(2)}(\alpha_1) & \dots & z_n f^{(2)}(\alpha_n) \\ \vdots & \ddots & \vdots \\ z_1 f^{(n-k)}(\alpha_1) & \dots & z_n f^{(n-k)}(\alpha_n) \end{pmatrix}$
- $\mathfrak{A}$ bestimmt durch x, z.
- Einträge von $\mathfrak{B}$ sind Auswertungen von Polynomen in α.

Vorbereitung: Lösungen

Sei (H, x, z) Lösung für $\mathfrak{B} = H\mathfrak{A}$

- Dann $\exists H', z'$, s.d. $H', z', x' = (\phi(x_1), \ldots, \phi(x_n))$ Lösung $\forall \phi(x) = \frac{ax+b}{cx+d}, ad - bc \neq 0$
- $\forall x_1, x_2, x_3 \in \mathbb{F}\, \exists \phi$ s.d. $\phi(x_1) = 1, \phi(x_2) = 0, \phi(x_3) = \infty$ $\Rightarrow$ Es existiert eine Lösung mit $x'_1 = 1, x'_2 = 0, x'_3 = \infty$.
- Dann $\exists H' = z_1 H, z' = (1, z'_2, \ldots, z'_n) = (1, \frac{z_2}{z_1}, \ldots, \frac{z_n}{z_1})$

Idee

- Setze $x_1 = 1, x_2 = 0, x_3 = \infty$.
- Finde passende $x_4, \ldots, x_n$.
- Wende geeignetes ϕ auf $x \in \mathbb{F}^n$ an, um $x' \in \mathbb{F}_q^n$ zu erhalten.
- Setze $z_1 = 1$.
- Finde passende $z_2, \ldots, z_{n-k+1}$.
- Finde passendes H.
- Finde passende $z_{n-k+2}, \ldots, z_n$

Finde passende $x_4, \ldots, x_n$

$$\mathfrak{B} = \begin{pmatrix} z_1 f^{(1)}(x_1) & \cdots & z_n f^{(1)}(x_n) \\ \vdots & \cdots & \vdots \\ z_1 f^{(n-k)}(x_1) & \cdots & z_n f^{(n-k)}(x_n) \end{pmatrix}$$

- Betrachte Spalten indiziert mit $I = \{1, n-k+1, \ldots, 2(n-k-1)\}$
- Finde $c_1 = (c_{11}, \ldots, c_{1(n-k)}) \in \mathbb{F}_q^{n-k}$, s.d. $\sum_{i=1}^{n-k} c_{1i} b_{ij} = 0$ für $j \in I$
- $F_1(x) := \sum_{i=1}^{n-k} c_{1i} f^{(i)}(x_j)$

Finde passende $x_4, \ldots, x_n$

$$\mathfrak{B} = \begin{pmatrix} z_1 f^{(1)}(x_1) & \ldots & z_n f^{(1)}(x_n) \\ \vdots & \ldots & \vdots \\ z_1 f^{(n-k)}(x_1) & \ldots & z_n f^{(n-k)}(x_n) \end{pmatrix}$$

- Betrachte Spalten indiziert mit $I = \{1, n-k+1, \ldots, 2(n-k-1)\}$
- Finde $c_1 = (c_{11}, \ldots, c_{1(n-k)}) \in \mathbb{F}_q^{n-k}$, s.d. $\sum_{i=1}^{n-k} c_{1i} b_{ij} = 0$ für $j \in I$
- $F_1(x) := \sum_{i=1}^{n-k} c_{1i} f^{(i)}(x_j)$
- $\sum_{i=1}^{n-k} c_{1i} b_{ij} = \sum_{i=1}^{n-k} c_{1i} z_j f^{(i)}(x_j) = z_j F_1(x)$
- Nst. von F_1: $x_i, i \in I \Rightarrow F_1(x) = a_1 \prod_{i \in I}(x - x_i)$
  $a_1 = F_1(\infty) = F_1(x_3) = \sum_{i=1}^{n-k} c_{1i} f^{(i)}(x_3) = \sum_{i=1}^{n-k} c_{1i} b_{i3}$

Finde passende $x_4, \ldots, x_n$

- $I = \{1, n-k+1, \ldots, 2(n-k-1)\}$
- Betrachte Spalten indiziert mit $J = \{2, n-k+1, \ldots, 2(n-k-1)\}$
- Analog $F_2(x) = a_2 \prod_{j \in J}(x - x_j)$

$$\frac{z_l F_1(x_l)}{z_l F_2(x_l)} = \frac{a_1 \prod_{i \in I}(x_l - x_i)}{a_2 \prod_{j \in J}(x_l - x_j)} = \frac{a_1}{a_2} \frac{x_l - x_1}{x_l - x_2}$$

$$\Rightarrow x_l = \frac{a_1/a_2}{a_1/a_2 - F_1(x_l)/F_2(x_l)} \quad 4 \leq l \leq n-k$$

Finde passende $x_4, \ldots, x_n$

$x_1, \ldots, x_{n-k}$ bekannt.

- $I = \{1, 3, \ldots, n-k\}, J = \{2, 3, \ldots, n-k\}$
- Finde c_3 und F_3 mit Nullstellen in $x_i, i \in I$
- Finde c_4 und F_4 mit Nullstellen in $x_j, j \in J$

$$\frac{z_l F_3(x_j)}{z_l F_4(x_j)} = \frac{a_3(x_l - x_1)}{a_4(x_l - x_2)} \Rightarrow x_l = \frac{a_3/a_4}{a_3/a_4 - F_3(x_l)/F_4(x_l)} \quad n-k+1 \leq l \leq n$$

Ersetze x durch $\phi(x)$

- $x = (1, 0, \infty, x_4, \dots x_n) \in \mathbb{F}^n = (\mathbb{F}_q \cup \{\infty\})^n$
- $x' = (\phi(1), \phi(0), \phi(\infty), \phi(x_4), \dots, \phi(x_n))$ für $\phi(x) = \frac{ax+b}{cx+d}$, $ad - bc \neq 0$ ist auch eine Lösung.
- Wähle $a = 0, b = 1, c = -1$ und $d \in \mathbb{F}_q \setminus \{x_1, \dots, x_n\}$.
- $\Rightarrow x' \in \mathbb{F}_q^n$

Finde passende $z_2, \ldots, z_{n-k+1}$

Betrachte die ersten $n-k+1$ Spalten von $\mathfrak{B}$.

$$\begin{pmatrix} z_1 f^{(1)}(x_1) & \ldots & z_{n-k+1} f^{(1)}(x_{n-k+1}) \\ \vdots & \ldots & \vdots \\ z_1 f^{(n-k)}(x_1) & \ldots & z_{n-k+1} f^{(n-k)}(x_{n-k+1}) \end{pmatrix}$$

Finde $c \in \mathbb{F}_q^{n-k+1} \setminus \{0\}$, s.d.

$$\sum_{j=1}^{n-k+1} c_j b_{ij} = 0, \quad 1 \leq i \leq n-k$$

Finde passende $z_2, \ldots, z_{n-k+1}$

$$\sum_{j=1}^{n-k+1} c_j b_{ij} = \sum_{j=1}^{n-k+1} c_j z_j f^{(i)}(x_j) = 0, \quad 1 \leq i \leq n-k$$

Als Matrizen:

$$\underbrace{\begin{pmatrix} f^{(1)}(x_1) & \ldots & f^{(1)}(x_{n-k+1}) \\ \vdots & \ldots & \vdots \\ f^{(n-k+1)}(x_1) & \ldots & f^{(n-k+1)}(x_{n-k+1}) \end{pmatrix}}_{H\begin{pmatrix} x_1 & \ldots & x_{n-k+1} \\ \vdots & \ddots & \vdots \\ x_1^{n-k+1} & \ldots & x_{n-k+1}^{n-k+1} \end{pmatrix}} \begin{pmatrix} c_1 & & \\ & \ddots & \\ & & c_{n-k+1} \end{pmatrix} \begin{pmatrix} z_1 \\ \vdots \\ z_{n-k+1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Finde passende $z_2, \ldots, z_{n-k+1}$

$$\begin{pmatrix} x_1 & \cdots & x_{n-k+1} \\ \vdots & \ddots & \vdots \\ x_1^{n-k+1} & \cdots & x_{n-k+1}^{n-k+1} \end{pmatrix} \begin{pmatrix} c_1 & & \\ & \ddots & \\ & & c_{n-k+1} \end{pmatrix} \begin{pmatrix} z_1 \\ \vdots \\ z_{n-k+1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

- $x_1, \ldots, x_{n-k+1}, c_1, \ldots, c_{n-k+1}, z_1$ sind bekannt

$$\begin{pmatrix} x_2 & \cdots & x_{n-k+1} \\ \vdots & \ddots & \vdots \\ x_2^{n-k+1} & \cdots & x_{n-k+1}^{n-k+1} \end{pmatrix} \begin{pmatrix} c_2 & & \\ & \ddots & \\ & & c_{n-k+1} \end{pmatrix} \begin{pmatrix} z_2 \\ \vdots \\ z_{n-k+1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

- $\det \neq 0 \Rightarrow$ eindeutige $z_2, \ldots, z_{n-k+1}$

Finde passendes H

- $\mathfrak{B} = H\mathfrak{A}$

$$\begin{pmatrix} b_{01} & \dots & b_{0,n-k} \\ \vdots & \ddots & \vdots \\ b_{n-k-1,0} & \dots & b_{n-k-1,n-k} \end{pmatrix} = H \begin{pmatrix} z_1 & \dots & z_{n-k-1} \\ \vdots & \ddots & \vdots \\ z_1 x_1^{n-k-1} & \dots & z_{n-k-1} x_{n-k-1}^{n-k-1} \end{pmatrix}$$

- Für festes i gilt: $\sum_{k=0}^{n-k-1} h_{ik} x_j^k = \frac{b_{ij}}{z_j} \quad 1 \leq j \leq n-k \Rightarrow h_{i0}, \dots, h_{i,n-k-1}$
- Löse lineares Gleichungssystem für $0 \leq i \leq n-k-1 \Rightarrow H$

Finde passende $z_{n-k+2}, \ldots, z_n$

- $\mathfrak{B} = H\mathfrak{A} \Rightarrow \mathfrak{A} = H^{-1}\mathfrak{B}$
- Betrachte erste Zeile von $H^{-1}, \mathfrak{A}$

$$\begin{pmatrix} z_1 & \ldots & z_n \end{pmatrix} = \begin{pmatrix} h'_{00} & \ldots & h'_{0,n-k-1} \end{pmatrix} \mathfrak{B}$$

- $z_j = \sum_{i=0}^{n-k-1} h'_{0i} b_{ij} \quad n-k+2 \leq j \leq n$

Inhaltsverzeichnis

Allgemeines

- Goppa-Codes über $\mathbb{F}_p$, p prim
- Sidelnikov-Shestakov-Angriff auf GRS-Codes über endliche Körper $\mathbb{F}_q$

Vorgehen:

- Betrachte Goppa-Codes über $\mathbb{F}_q = \mathbb{F}_{p^m}$
- Betrachte Goppa-Codes über $\mathbb{F}_q = \mathbb{F}_p$

Goppa-Codes über $\mathbb{F}_{p^m}$

Parity-Check-Matrix von Goppa-Code $\Gamma(L, g)$ identisch zu GRS-Codes

$$\begin{pmatrix} g(\alpha_1)^{-1} & \dots & g(\alpha_n)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \dots & \alpha_n g(\alpha_n)^{-1} \\ \vdots & \ddots & \vdots \\ \alpha_1^{\deg g-1} g(\alpha_1)^{-1} & \dots & \alpha_n^{\deg g-1} g(\alpha_n)^{-1} \end{pmatrix} = \mathfrak{A}(x, z)$$

mit $x = (\alpha_1, \dots, \alpha_n), z = (g^{-1}(\alpha_1), \dots, g^{-1}(\alpha_n))$
$\Rightarrow$ Angriff auf $\mathbb{F}_{p^m}$ anwendbar.

Beispiel: Goppa-Codes über $\mathbb{F}_{p^m}$

$$H = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \mathfrak{A} = \begin{pmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 \end{pmatrix}$$

$$\Rightarrow \mathfrak{B} = \begin{pmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 1 & 0 & \alpha^5 & \alpha^3 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^6 \end{pmatrix}$$

Angriff liefert Lösung $(c_{10} = c_{11} = c_{21} = 1, c_{20} = 0, c_{30} = c_{31} = c_{41} = 1, c_{40} = 0, d = \alpha, c_1 = \alpha^5, c_2 = \alpha^3, c_3 = 1)$

$$H' = \begin{pmatrix} 1 & 0 \\ \alpha^3 & \alpha^4 \end{pmatrix}, \mathfrak{A}' = \begin{pmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ \alpha^4 & \alpha^6 & 0 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^3 & \alpha^5 \end{pmatrix}$$

Goppa-Codes über $\mathbb{F}_p$

- Struktur von GRS-Codes geht verloren!
- Beispiel:

$$\mathfrak{A} = \begin{pmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 \end{pmatrix} \Rightarrow \mathfrak{A}' = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

- Angriff für $\mathbb{F}_{p^m} = \mathbb{F}_p \Leftrightarrow m = 1$ ist möglich.
- Was gilt für $m \neq 1$?

Idee: Transformiere Matrizen über $\mathbb{F}_p$ zu $\mathbb{F}_{p^m}$

Parity-Check-Matrix lässt sich transformieren:

$$\mathfrak{A}' \in \mathbb{F}_p^{m(n-k)\times n} \longrightarrow \mathfrak{A} \in \mathbb{F}_{p^m}^{(n-k)\times n}$$

Maskierungsmatrix lässt sich nicht transformieren:

$$\begin{tikzcd}
H' \in \mathbb{F}_p^{m(n-k)\times m(n-k)} \arrow[r, leftrightarrow, "/" marking] \arrow[d, leftrightarrow, "-" marking] \arrow[dr] & H \in \mathbb{F}_{p^m}^{(n-k)\times(n-k)} \arrow[d, leftrightarrow, "-" marking] \arrow[dl] \\
\bar{H} \in \mathbb{F}_p^{m(n-k)\times(n-k)} \arrow[r, leftrightarrow, "/" marking] & \bar{H}' \in \mathbb{F}_{p^m}^{(n-k)\times m(n-k)}
\end{tikzcd}$$

Liefern $H', \mathfrak{A}'$ Informationen über H?

Parity-Check-Matrix und Matrixprodukt lassen sich transformieren.

$$\begin{tikzcd}
\mathfrak{A}' \arrow[r, blue] \arrow[d, "H'"] & \mathfrak{A} \arrow[d, dotted, "H"] \\
\mathfrak{B}' \arrow[r, blue] & \mathfrak{B}
\end{tikzcd}$$

Lässt sich aus $\mathfrak{A}', H, H\mathfrak{A}'$ die Maskierungsmatrix H rekonstruieren?
$\rightarrow$ Im Allgemeinen nicht!

Beispiel

$$H' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \mathfrak{A}' = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$$\mathfrak{B}' := H' \cdot \mathfrak{A}' = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Beispiel

$$\mathfrak{A} = \begin{pmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 \end{pmatrix}, \mathfrak{B} = \begin{pmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ \alpha^2 & \alpha^6 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 \end{pmatrix}$$

Die ersten drei Spalten liefern für h_{10}, h_{11} :

$$\begin{cases} h_{10} & = \alpha^2 \\ h_{10} + \quad h_{11} & = \alpha^6 \\ \alpha^2 h_{10} + \alpha^3 h_{11} & = \alpha^3 \end{cases} \Rightarrow \begin{cases} h_{10} & = \alpha^2 \\ h_{11} & = 1 \\ \alpha^2 h_{10} + \alpha^3 h_{11} & = \alpha^3 \end{cases}$$

Es existiert kein H!

Conclusio

- Sidelnikov-Shestakov-Angriff für $m = 1$ anwendbar
- Goppa-Code über $\mathbb{F}_p$ i.A. nicht transformierbar in Goppa-Code über $\mathbb{F}_{p^m}$
- Goppa-Code über $\mathbb{F}_p$ liefert i.A. keine Informationen über Goppa-Code über $\mathbb{F}_{p^m}$