Cryptanalysis of a variant of the McEliece encryption scheme

Julien Lavauzelle

IRMAR, Université de Rennes 1

Journées Nationales de Calcul Formel 2020

03/03/2020

Outline

McEliece cryptosystem

McEliece cryptosystem (1978): a public-key encryption scheme.

McEliece cryptosystem

McEliece cryptosystem (1978): a public-key encryption scheme.

Summary:

- **private key:** an efficient decoding algorithm for a code $\mathcal{C}$,
- **public key:** a random description of the code (masks the decoding algorithm),
- **encryption:** encode the message and add an error,
- **decryption:** decode the error and retrieve the message.

McEliece cryptosystem

McEliece cryptosystem (1978): a public-key encryption scheme.

Summary:

- **private key:** an efficient decoding algorithm for a code $\mathcal{C}$,
- **public key:** a random description of the code (masks the decoding algorithm),
- **encryption:** encode the message and add an error,
- **decryption:** decode the error and retrieve the message.

Security relies on two problems:

1. hardness of decoding random codes
2. **hardness of recognizing the structure of a code** ($\simeq$ find an efficient decoding algorithm from a random description of a code)

General statement of the problem

Let $\mathcal{F}$ be a k-dimensional subspace of $\mathbb{F}_q[x]/(x^q - x)$.

Input.

$$\boldsymbol{G} = \begin{pmatrix} y_1 f_1(x_1) & \dots & \dots & y_n f_1(x_n) \\ \vdots & & & \vdots \\ y_1 f_k(x_1) & \dots & \dots & y_n f_k(x_n) \end{pmatrix} \in \mathbb{F}_q^{k \times n}$$

where: $\begin{cases} f_1(x), \dots, f_k(x) \text{ is a basis of } \mathcal{F}, \\ (x_1, \dots, x_n) \text{ are pairwise distinct in } \mathbb{F}_q, \\ (y_1, \dots, y_n) \text{ are non-zero elements of } \mathbb{F}_q. \end{cases}$

General statement of the problem

Let $\mathcal{F}$ be a k-dimensional subspace of $\mathbb{F}_q[x]/(x^q - x)$.

Input.

$$\boldsymbol{G} = \begin{pmatrix} y_1 f_1(x_1) & \dots & \dots & y_n f_1(x_n) \\ \vdots & & & \vdots \\ y_1 f_k(x_1) & \dots & \dots & y_n f_k(x_n) \end{pmatrix} \in \mathbb{F}_q^{k \times n}$$

where: $\begin{cases} f_1(x), \dots, f_k(x) \text{ is a basis of } \mathcal{F}, \\ (x_1, \dots, x_n) \text{ are pairwise distinct in } \mathbb{F}_q, \\ (y_1, \dots, y_n) \text{ are non-zero elements of } \mathbb{F}_q. \end{cases}$

Output. A basis $g_1(x), \dots, g_k(x)$ of $\mathcal{F}$, pairwise distinct elements $x'_1, \dots, x'_n \in \mathbb{F}_q$ and non-zero elements $y'_1, \dots, y'_n \in \mathbb{F}_q^\times$ such that

$$\boldsymbol{G} = \begin{pmatrix} y'_1 g_1(x'_1) & \dots & \dots & y'_n g_1(x'_n) \\ \vdots & & & \vdots \\ y'_1 g_k(x'_1) & \dots & \dots & y'_n g_k(x'_n) \end{pmatrix}.$$

Instances of the problem

A Public-Key Cryptosystem Based on Algebraic Coding Theory. McEliece. Jet Propulsion Laboratory DSN Progress Report. **1978**.

Original McEliece cryptosystem: binary Goppa codes, $q = 2^m$.

- $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ pairwise distinct,
- $\pi(x)$ the derivative of $\prod_{i=1}^{n}(x - x_i) \in \mathbb{F}_q[x]$,
- an irreducible $\Gamma(x) \in \mathbb{F}_q[x]$,
- $\boldsymbol{y} = \left(\frac{\Gamma(x_1)}{\pi(x_1)}, \ldots, \frac{\Gamma(x_1)}{\pi(x_1)}\right) \in (\mathbb{F}_q^{\times})^n$.

$$\mathcal{F}_{x,\Gamma,r} = \left\{ f(x) \in \mathbb{F}_q[x] \mid \deg(f) < r \text{ and } y_i f(x_i) \in \mathbb{F}_2, \forall i = 1, \ldots, n \right\}.$$

Instances of the problem

A Public-Key Cryptosystem Based on Algebraic Coding Theory. McEliece. Jet Propulsion Laboratory DSN Progress Report. **1978**.

Original McEliece cryptosystem: binary Goppa codes, $q = 2^m$.

- $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ pairwise distinct,
- $\pi(x)$ the derivative of $\prod_{i=1}^{n}(x - x_i) \in \mathbb{F}_q[x]$,
- an irreducible $\Gamma(x) \in \mathbb{F}_q[x]$,
- $\boldsymbol{y} = \left(\frac{\Gamma(x_1)}{\pi(x_1)}, \ldots, \frac{\Gamma(x_1)}{\pi(x_1)}\right) \in (\mathbb{F}_q^{\times})^n$.

$$\mathcal{F}_{x,\Gamma,r} = \left\{ f(x) \in \mathbb{F}_q[x] \mid \deg(f) < r \text{ and } y_i f(x_i) \in \mathbb{F}_2, \forall i = 1, \ldots, n \right\}.$$

- Still considered as **secure** (NIST competition).
- **Main drawback**: large key sizes.

Intances of the problem

In order to **reduce key sizes**:

- Niederreiter (1986): generalized Reed–Solomon codes
  - $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ pairwise distinct
  - $\boldsymbol{y} = (y_1, \ldots, y_n) \in (\mathbb{F}_q^\times)^n$

$$\mathcal{F} = \left\{ f(x) \in \mathbb{F}_q[x] \mid \deg(f) < k \right\}$$

Intances of the problem

In order to **reduce key sizes**:

- Niederreiter (1986): generalized Reed–Solomon codes
  - $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ pairwise distinct
  - $\boldsymbol{y} = (y_1, \ldots, y_n) \in (\mathbb{F}_q^\times)^n$

$$\mathcal{F} = \left\{ f(x) \in \mathbb{F}_q[x] \mid \deg(f) < k \right\}$$

However, **broken** by Sidelnikov and Shestakov in 1992 (Part II).

On Insecurity of Cryptosystems Based on Generalized Reed-Solomon Codes. Sidelnikov, Shestakov. Discrete Math. Appl.. **1992**.

Intances of the problem

In order to **reduce key sizes**:

- Niederreiter (1986): generalized Reed–Solomon codes
  - $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ pairwise distinct
  - $\boldsymbol{y} = (y_1, \ldots, y_n) \in (\mathbb{F}_q^\times)^n$

$$\mathcal{F} = \left\{ f(x) \in \mathbb{F}_q[x] \mid \deg(f) < k \right\}$$

  However, **broken** by Sidelnikov and Shestakov in 1992 (Part II).
- A lot of propositions to replace Goppa codes
  $\rightarrow$ Reed–Muller codes, AG codes, QC-MDPC codes, etc.

On Insecurity of Cryptosystems Based on Generalized Reed-Solomon Codes. Sidelnikov, Shestakov. Discrete Math. Appl.. **1992**.

Intances of the problem

In order to **reduce key sizes**:

- Niederreiter (1986): generalized Reed–Solomon codes
  - $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ pairwise distinct
  - $\boldsymbol{y} = (y_1, \ldots, y_n) \in (\mathbb{F}_q^\times)^n$

$$\mathcal{F} = \left\{ f(x) \in \mathbb{F}_q[x] \mid \deg(f) < k \right\}$$

  However, **broken** by Sidelnikov and Shestakov in 1992 (Part II).
- A lot of propositions to replace Goppa codes
  $\rightarrow$ Reed–Muller codes, AG codes, QC-MDPC codes, etc.
- In 2018: Beelen, Bossert, Puchinger and Rosenkilde proposed **twisted Reed–Solomon codes**.
  $\rightarrow$ claimed key size reduction by a factor 7
  $\rightarrow$ also broken (Part III)

On Insecurity of Cryptosystems Based on Generalized Reed-Solomon Codes. Sidelnikov, Shestakov. Discrete Math. Appl.. **1992**.

Cryptanalysis of a System Based on Twisted Reed–Solomon Codes. **L.**, Renner. Designs, Codes and Cryptograhy. **2020**.

Outline

1. McEliece cryptosystem and variants

2. Attack on the Reed–Solomon variant

3. Attack on the *twisted* Reed–Solomon variant

The problem

Let $\mathcal{F} = \{ f(x) \in \mathbb{F}_q[x] \mid \deg(f) < k \}$.

Input. A matrix

$$\boldsymbol{G} = \begin{pmatrix} y_1 f_1(x_1) & \cdots & \cdots & y_n f_1(x_n) \\ \vdots & & & \vdots \\ y_1 f_k(x_1) & \cdots & \cdots & y_n f_k(x_n) \end{pmatrix} \in \mathbb{F}_q^{k \times n}, \quad \text{where}$$

- $f_1(x), \ldots, f_k(x)$ is a basis of $\mathcal{F}$,
- $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$ are pairwise distinct, and $(y_1, \ldots, y_n) \in (\mathbb{F}_q^\times)^n$.

Output. A basis $g_1(x), \ldots, g_k(x)$ of $\mathcal{F}$, pairwise distinct elements $(x'_1, \ldots, x'_n) \in \mathbb{F}_q^n$ and non-zero elements $(y'_1, \ldots, y'_n) \in (\mathbb{F}_q^\times)^n$ such that

$$\boldsymbol{G} = \begin{pmatrix} y'_1 g_1(x'_1) & \cdots & \cdots & y'_n g_1(x'_n) \\ \vdots & & & \vdots \\ y'_1 g_k(x'_1) & \cdots & \cdots & y'_n g_k(x'_n) \end{pmatrix}.$$

Remark. One can write G as:

$$S \cdot \begin{pmatrix} 1 & 1 & \dots & \dots & 1 & 1 \\ x_1 & x_2 & \dots & \dots & x_{n-1} & x_n \\ x_1^2 & x_2^2 & \dots & \dots & x_{n-1}^2 & x_n^2 \\ \vdots & & & & & \vdots \\ x_1^{k-1} & x_2^{k-1} & \dots & \dots & x_{n-1}^{k-1} & x_n^{k-1} \end{pmatrix} \cdot \mathbf{Diag}(y_1, \dots, y_n)$$

where $S \in \mathbb{F}_q^{k \times k}$ is invertible.

Structural properties

Notation.

- $\mathbf{1} = (1, \ldots, 1) \in \mathbb{F}_q^n$
- $\boldsymbol{a} \star \boldsymbol{b} = (a_1 b_1, \ldots, a_n b_n)$
- $\lambda \boldsymbol{a} = (\lambda a_1, \ldots, \lambda a_n)$

$$\mathcal{F} = \{ f(x) \in \mathbb{F}_q[x] \mid \deg(f) < k \}$$

Structural properties

Notation.

- $\mathbf{1} = (1, \ldots, 1) \in \mathbb{F}_q^n$
- $\boldsymbol{a} \star \boldsymbol{b} = (a_1 b_1, \ldots, a_n b_n)$
- $\lambda \boldsymbol{a} = (\lambda a_1, \ldots, \lambda a_n)$

$$\mathcal{F} = \{ f(x) \in \mathbb{F}_q[x] \mid \deg(f) < k \}$$

Definition. Generalized Reed–Solomon code:

$$\mathrm{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) := \{ \boldsymbol{y} \star \mathrm{ev}_{\boldsymbol{x}}(f) := (y_1 f(x_1), \ldots, y_n f(x_n)) \mid f(x) \in \mathcal{F} \} \subseteq \mathbb{F}_q^n$$

Notation.

- $\mathbf{1} = (1, \ldots, 1) \in \mathbb{F}_q^n$
- $\boldsymbol{a} \star \boldsymbol{b} = (a_1 b_1, \ldots, a_n b_n)$
- $\lambda \boldsymbol{a} = (\lambda a_1, \ldots, \lambda a_n)$

$$\mathcal{F} = \{ f(x) \in \mathbb{F}_q[x] \mid \deg(f) < k \}$$

Definition. Generalized Reed–Solomon code:

$$\mathrm{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) := \{ \boldsymbol{y} \star \mathrm{ev}_{\boldsymbol{x}}(f) := (y_1 f(x_1), \ldots, y_n f(x_n)) \mid f(x) \in \mathcal{F} \} \subseteq \mathbb{F}_q^n$$

$\mathcal{F}$ is invariant under the action of the general affine group $\{x \mapsto ax + b\}$.

Proposition. Let $a, b \in \mathbb{F}_q$. We have

$$\mathrm{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{GRS}_k(a\boldsymbol{x} + b\mathbf{1}, \boldsymbol{y}) .$$

Structural properties

Actually, one can "extend" the evaluation of elements in $\mathcal{F}$, at a point at infinity:

$$X^{k-1}(\infty) = 1 \quad \text{and} \quad X^j(\infty) = 0 \ \text{ for } j < k-1.$$

Structural properties

Actually, one can "extend" the evaluation of elements in $\mathcal{F}$, at a point at infinity:

$$X^{k-1}(\infty) = 1 \quad \text{and} \quad X^j(\infty) = 0 \ \text{ for } j < k-1.$$

Can be formally written as **evaluating rational functions** at points of the **projective line** $\mathbb{P}^1(\mathbb{F}_q) \simeq \mathbb{F}_q \cup \{\infty\}$.

Structural properties

Actually, one can "extend" the evaluation of elements in $\mathcal{F}$, at a point at infinity:

$$X^{k-1}(\infty) = 1 \quad \text{and} \quad X^j(\infty) = 0 \ \text{ for } j < k-1.$$

Can be formally written as **evaluating rational functions** at points of the **projective line** $\mathbb{P}^1(\mathbb{F}_q) \simeq \mathbb{F}_q \cup \{\infty\}$.

Invariance under the projective linear group $\{(t:s) \mapsto (at+bs : ct+ds)\}$.

Proposition. Let $a, b, c, d \in \mathbb{F}_q$, $ad - bc = 1$. Then we have

$$\mathrm{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{GRS}_k\left(\frac{a\boldsymbol{x} + b\mathbf{1}}{c\boldsymbol{x} + d\mathbf{1}}, \boldsymbol{y}\right).$$

Structural properties

Actually, one can "extend" the evaluation of elements in $\mathcal{F}$, at a point at infinity:

$$X^{k-1}(\infty) = 1 \quad \text{and} \quad X^j(\infty) = 0 \ \text{ for } j < k-1.$$

Can be formally written as **evaluating rational functions** at points of the **projective line** $\mathbb{P}^1(\mathbb{F}_q) \simeq \mathbb{F}_q \cup \{\infty\}$.

Invariance under the projective linear group $\{(t:s) \mapsto (at+bs : ct+ds)\}$.

Proposition. Let $a, b, c, d \in \mathbb{F}_q$, $ad - bc = 1$. Then we have

$$\mathrm{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{GRS}_k\left(\frac{a\boldsymbol{x} + b\mathbf{1}}{c\boldsymbol{x} + d\mathbf{1}}, \boldsymbol{y}\right).$$

Remark. The group of homographies $t \mapsto \frac{at+b}{ct+d}$ is 3-transitive over $\mathbb{F}_q \cup \{\infty\}$.

In our search for $\boldsymbol{x}$, one can arbitrarily fix 3 points, say
$x_{n-2} = 1, x_{n-1} = 0, x_n = \infty$.

Sidelnikov–Shestakov's attack

(Trivial) lemma. For every subset $S \subset \{x_1, \ldots, x_n\}$ of cardinality $k-1$, there exists a unique monic $f \in \mathcal{F}$ such that $f(S) = \{0\}$.

$$f(x) = \prod_{i=1}^{k-1} (x - s_i)$$

Sidelnikov–Shestakov's attack

(Trivial) lemma. For every subset $S \subset \{x_1, \ldots, x_n\}$ of cardinality $k-1$, there exists a unique monic $f \in \mathcal{F}$ such that $f(S) = \{0\}$.

$$f(x) = \prod_{i=1}^{k-1} (x - s_i)$$

$$\boldsymbol{G} = \begin{pmatrix} y_1 f_1(x_1) & y_2 f_1(x_2) & \ldots & \ldots & \ldots & y_n f_1(x_n) \\ \vdots & & & & & \vdots \\ \vdots & & & & & \vdots \\ y_1 f_k(x_1) & y_2 f_k(x_2) & \ldots & \ldots & \ldots & y_n f_k(x_n) \end{pmatrix}$$

By Gaussian elimination:

$$\begin{array}{rcccccccc} \boldsymbol{u} = & (0 & \ldots & 0 & 0 & 1 & u_{k+1} & \ldots & u_n) \quad \rightarrow \quad f(x) \\ \boldsymbol{v} = & (0 & \ldots & 0 & 1 & 0 & v_{k+1} & \ldots & v_n) \quad \rightarrow \quad g(x) \end{array}$$

where u_i's, v_i's are non-zero.

Sidelnikov–Shestakov's attack

$$\begin{aligned} \boldsymbol{u} &= \begin{pmatrix} 0 & \dots & 0 & 0 & 1 & u_{k+1} & \dots & u_n \end{pmatrix} & \to \quad f(x) \\ \boldsymbol{v} &= \begin{pmatrix} 0 & \dots & 0 & 1 & 0 & v_{k+1} & \dots & v_n \end{pmatrix} & \to \quad g(x) \end{aligned}$$

Lemma. If two elements $f, g \in \mathcal{F}$ share $k-2$ zeroes, then

$$\frac{f(x)}{g(x)} = \frac{\alpha x + \beta}{\gamma x + \delta}\,.$$

Sidelnikov–Shestakov's attack

$$\begin{array}{lllllllll} \boldsymbol{u} = \begin{pmatrix} 0 & \dots & 0 & 0 & 1 & u_{k+1} & \dots & u_n \end{pmatrix} & \to & f(x) \\ \boldsymbol{v} = \begin{pmatrix} 0 & \dots & 0 & 1 & 0 & v_{k+1} & \dots & v_n \end{pmatrix} & \to & g(x) \end{array}$$

Lemma. If two elements $f, g \in \mathcal{F}$ share $k-2$ zeroes, then

$$\frac{f(x)}{g(x)} = \frac{\alpha x + \beta}{\gamma x + \delta}\,.$$

$$\boldsymbol{u} \star \boldsymbol{v}^{-1} = \begin{pmatrix} \perp & \perp & \dots & \perp & \frac{u_{k+1}}{v_{k+1}} & \dots & \frac{u_n}{v_n} \end{pmatrix} \quad \to \quad \phi(x) = \frac{f(x)}{g(x)} = \frac{\alpha x + \beta}{\gamma x + \delta}$$

Sidelnikov–Shestakov's attack

$$\begin{array}{lllllllll} \boldsymbol{u} = (0 & \dots & 0 & 0 & 1 & u_{k+1} & \dots & u_n) & \to \quad f(x) \\ \boldsymbol{v} = (0 & \dots & 0 & 1 & 0 & v_{k+1} & \dots & v_n) & \to \quad g(x) \end{array}$$

Lemma. If two elements $f, g \in \mathcal{F}$ share $k-2$ zeroes, then

$$\frac{f(x)}{g(x)} = \frac{\alpha x + \beta}{\gamma x + \delta}\,.$$

$$\boldsymbol{u} \star \boldsymbol{v}^{-1} = \left(\perp \quad \perp \quad \dots \quad \perp \quad \frac{u_{k+1}}{v_{k+1}} \quad \dots \quad \frac{u_n}{v_n}\right) \quad \to \quad \phi(x) = \frac{f(x)}{g(x)} = \frac{\alpha x+\beta}{\gamma x+\delta}$$

Solve (in $\alpha, \beta, \gamma, \delta$) the system $\phi(x_i) = \frac{u_i}{v_i}$, where $i \in \{n-2, n-1, n\}$

$$\Longrightarrow \text{ find } \phi$$

Sidelnikov–Shestakov's attack

$$\begin{array}{lllllllll} \boldsymbol{u} = (0 & \dots & 0 & 0 & 1 & u_{k+1} & \dots & u_n) & \to \quad f(x) \\ \boldsymbol{v} = (0 & \dots & 0 & 1 & 0 & v_{k+1} & \dots & v_n) & \to \quad g(x) \end{array}$$

Lemma. If two elements $f, g \in \mathcal{F}$ share $k-2$ zeroes, then

$$\frac{f(x)}{g(x)} = \frac{\alpha x + \beta}{\gamma x + \delta}\,.$$

$$\boldsymbol{u} \star \boldsymbol{v}^{-1} = \left(\perp \quad \perp \quad \dots \quad \perp \quad \frac{u_{k+1}}{v_{k+1}} \quad \dots \quad \frac{u_n}{v_n}\right) \quad \to \quad \phi(x) = \frac{f(x)}{g(x)} = \frac{\alpha x+\beta}{\gamma x+\delta}$$

Solve (in $\alpha, \beta, \gamma, \delta$) the system $\phi(x_i) = \frac{u_i}{v_i}$, where $i \in \{n-2, n-1, n\}$

$$\Longrightarrow \text{ find } \phi$$

Solve the equation $\quad \phi(x_i) = \frac{u_i}{v_i} \quad$ for each $i \in [k+1, n-3]$

$$\Longrightarrow \text{ find } x_{k+1}, \dots, x_{n-3}$$

Sidelnikov–Shestakov's attack

Once $\boldsymbol{x}$ is known, one can easily find a valid $\boldsymbol{y}'$ by solving a linear system.

Sidelnikov–Shestakov's attack

Once $\boldsymbol{x}$ is known, one can easily find a valid $\boldsymbol{y}'$ by solving a linear system.

Theorem. [Sidelnikov–Shestakov] Given as input any matrix $\boldsymbol{G}$ generating the code $\mathrm{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$, there exists an algorithm running in time $\mathcal{O}(n^4)$ that outputs $\boldsymbol{x}', \boldsymbol{y}'$ such that

$$\mathrm{GRS}_k(\boldsymbol{x}', \boldsymbol{y}') = \mathrm{GRS}_k(\boldsymbol{x}, \boldsymbol{y})\,.$$

$$\text{Moreover, } \boldsymbol{x}' = \frac{a\boldsymbol{x}+b\boldsymbol{1}}{c\boldsymbol{x}+d\boldsymbol{1}} \text{ and } \boldsymbol{y}' = \lambda \boldsymbol{y}.$$

Outline

1. McEliece cryptosystem and variants

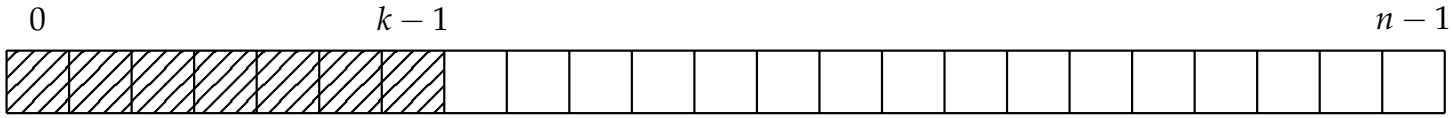
2. Attack on the Reed–Solomon variant

3. Attack on the *twisted* Reed–Solomon variant

Twisted Reed–Solomon codes

Reed–Solomon codes:

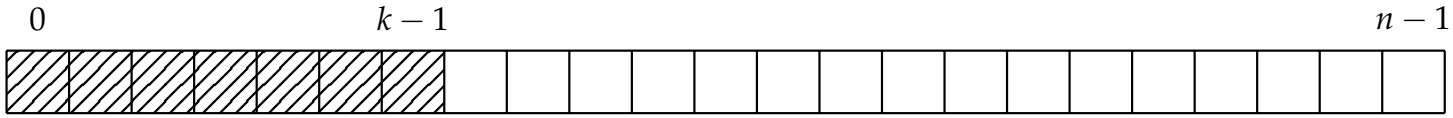
$$\mathcal{F}_{\mathrm{RS}} = \langle 1, x, \ldots, x^{h-1}, x^h, x^{h+1}, \ldots, x^{k-1} \rangle_{\mathbb{F}_q}$$



Twisted Reed–Solomon codes

Reed–Solomon codes:

$$\mathcal{F}_{\mathrm{RS}} = \langle 1, x, \ldots, x^{h-1}, x^h, x^{h+1}, \ldots, x^{k-1} \rangle_{\mathbb{F}_q}$$



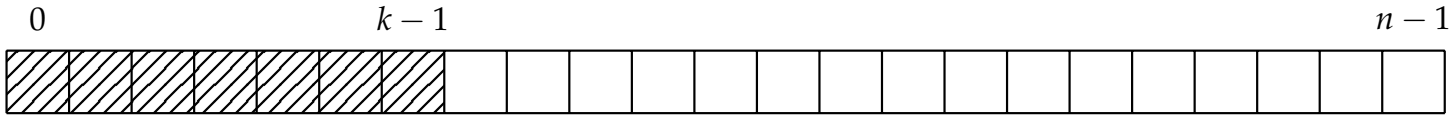
Definition. *Twisted* Reed–Solomon codes (with one twist):

$$\mathcal{F}_{\mathrm{TRS}} = \langle 1, x, \ldots, x^{h-1}, x^h + \underbrace{\eta}_{\in \mathbb{F}_{q^2}} x^{k-1+t}, x^{h+1}, \ldots, x^{k-1} \rangle_{\mathbb{F}_{q^2}}$$

Twisted Reed–Solomon codes

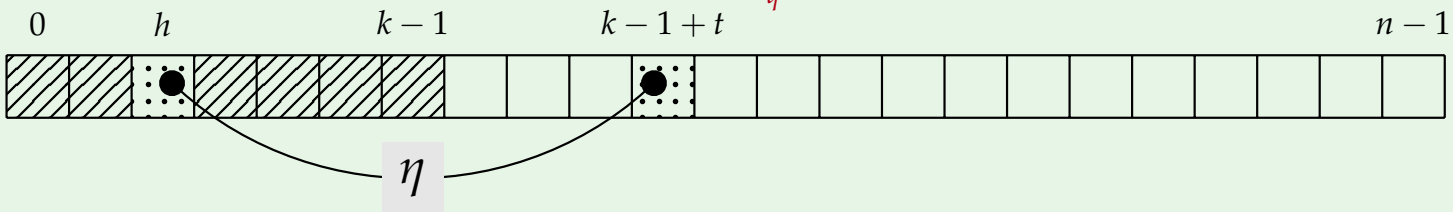
Reed–Solomon codes:

$$\mathcal{F}_{\mathrm{RS}} = \langle 1, x, \ldots, x^{h-1}, x^h, x^{h+1}, \ldots, x^{k-1} \rangle_{\mathbb{F}_q}$$



Definition. *Twisted* Reed–Solomon codes (with one twist):

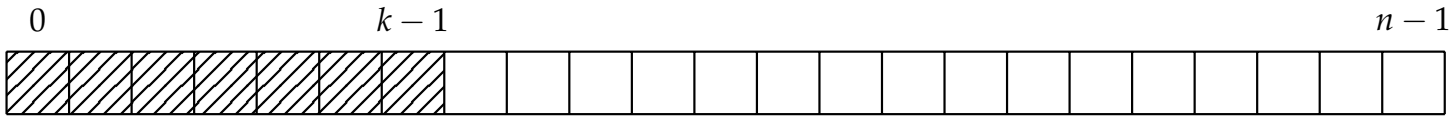
$$\mathcal{F}_{\mathrm{TRS}} = \langle 1, x, \ldots, x^{h-1}, x^h + \underbrace{\eta}_{\in \mathbb{F}_{q^2}} x^{k-1+t}, x^{h+1}, \ldots, x^{k-1} \rangle_{\mathbb{F}_{q^2}}$$



Twisted Reed–Solomon codes

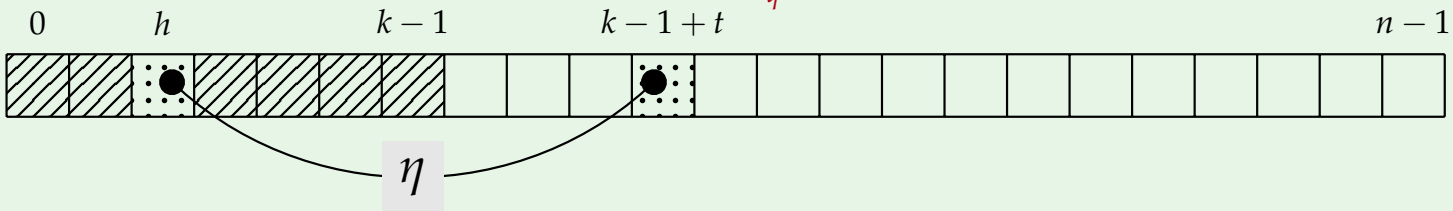
Reed–Solomon codes:

$$\mathcal{F}_{\mathrm{RS}} = \langle 1, x, \ldots, x^{h-1}, x^h, x^{h+1}, \ldots, x^{k-1} \rangle_{\mathbb{F}_q}$$



Definition. *Twisted* Reed–Solomon codes (with one twist):

$$\mathcal{F}_{\mathrm{TRS}} = \langle 1, x, \ldots, x^{h-1}, x^h + \underbrace{\eta}_{\in \mathbb{F}_{q^2}} x^{k-1+t}, x^{h+1}, \ldots, x^{k-1} \rangle_{\mathbb{F}_{q^2}}$$



Set $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ pairwise distinct, and $\boldsymbol{y} = \mathbf{1}$.

$$\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta] := \{(f(x_1), \ldots, f(x_n)) \mid f \in \mathcal{F}_{\mathrm{TRS}}\} \subseteq \mathbb{F}_{q^2}^n$$

Input

$$\underbrace{S}_{\in \mathrm{GL}_k(\mathbb{F}_{q^2})} \cdot \begin{pmatrix} 1 & 1 & \dots & \dots & 1 & 1 \\ x_1 & x_2 & \dots & \dots & x_{n-1} & x_n \\ x_1^2 & x_2^2 & \dots & \dots & x_{n-1}^2 & x_n^2 \\ \vdots & & & & & \vdots \\ x_1^h + \eta x_1^{k-1+t} & x_2^h + \eta x_2^{k-1+t} & \dots & \dots & x_{n-1}^h + \eta x_{n-1}^{k-1+t} & x_n^h + \eta x_n^{k-1+t} \\ \vdots & & & & & \vdots \\ x_1^{k-1} & x_2^{k-1} & \dots & \dots & x_{n-1}^{k-1} & x_n^{k-1} \end{pmatrix}$$

Structural properties

Structural Properties of Twisted Reed–Solomon Codes with Applications to Cryptography. Beelen, Bossert, Puchinger, Rosenkilde. ISIT. **2018**.

Can we apply the same technique?

Structural properties

Structural Properties of Twisted Reed–Solomon Codes with Applications to Cryptography. Beelen, Bossert, Puchinger, Rosenkilde. ISIT. **2018**.

Can we apply the same technique?

$\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta]$ is also MDS:

$$\forall I \subset [1,n], |I| = k-1, \quad \exists \text{ monic } f(x) \in \mathcal{F}_{\mathrm{TRS}}, \quad \forall i \in I, f(x_i) = 0$$

Structural properties

Structural Properties of Twisted Reed–Solomon Codes with Applications to Cryptography. Beelen, Bossert, Puchinger, Rosenkilde. ISIT. **2018**.

Can we apply the same technique?

$\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta]$ is also MDS:

$$\forall I \subset [1,n], |I| = k-1, \quad \exists \text{ monic } f(x) \in \mathcal{F}_{\mathrm{TRS}}, \quad \forall i \in I, f(x_i) = 0$$

However, if $f, g \in \mathcal{F}_{\mathrm{TRS}}$ share $k-2$ zeroes, then generally f/g is **not** a rational function of degree 1.

Structural properties

Structural Properties of Twisted Reed–Solomon Codes with Applications to Cryptography. Beelen, Bossert, Puchinger, Rosenkilde. ISIT. **2018**.

Can we apply the same technique?

$\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta]$ is also MDS:

$$\forall I \subset [1,n], |I| = k-1, \quad \exists \text{ monic } f(x) \in \mathcal{F}_{\mathrm{TRS}}, \quad \forall i \in I, f(x_i) = 0$$

However, if $f, g \in \mathcal{F}_{\mathrm{TRS}}$ share $k-2$ zeroes, then generally f/g is **not** a rational function of degree 1.

Moreover,

Proposition. Let $a \in \mathbb{F}_q$. We have

$$\mathrm{TRS}_k[a\boldsymbol{x}, h, t, \eta] = \mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta a^{k-1+t-h}]$$

But we cannot hope better.

Main idea

Our idea:

Starting from any generator matrix $\boldsymbol{G}$ for $\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta]$, build a **new** code:

- whose description involves $\boldsymbol{x}$,
- which can be attacked.

Two tools:

1. subfield subcode,
2. code squaring.

Subfield subcode

Subfield subcode of $\mathcal{C} \subseteq \mathbb{F}_{q^2}^n$:

$$\mathcal{C} \cap \mathbb{F}_q^n = \{\boldsymbol{c} \in \mathcal{C} \mid \forall i \in [1, n],\, c_i \in \mathbb{F}_q\}$$

Subfield subcode

Subfield subcode of $\mathcal{C} \subseteq \mathbb{F}_{q^2}^n$:

$$\mathcal{C} \cap \mathbb{F}_q^n = \{\boldsymbol{c} \in \mathcal{C} \mid \forall i \in [1, n],\, c_i \in \mathbb{F}_q\}$$

... efficiently computable from $\boldsymbol{G}$.

Subfield subcode

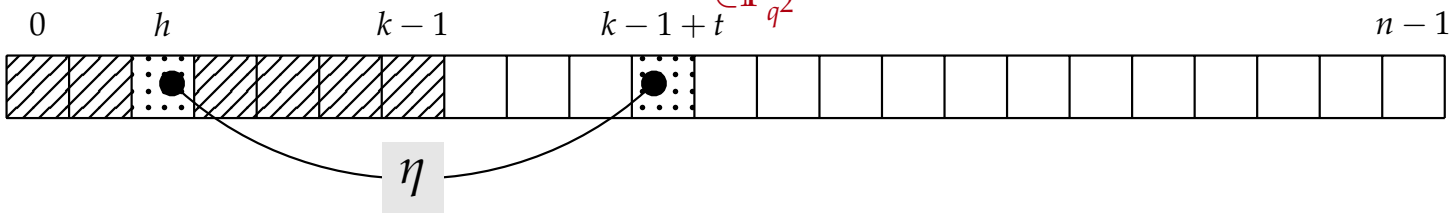
Subfield subcode of $\mathcal{C} \subseteq \mathbb{F}_{q^2}^n$:

$$\mathcal{C} \cap \mathbb{F}_q^n = \{\boldsymbol{c} \in \mathcal{C} \mid \forall i \in [1, n],\, c_i \in \mathbb{F}_q\}$$

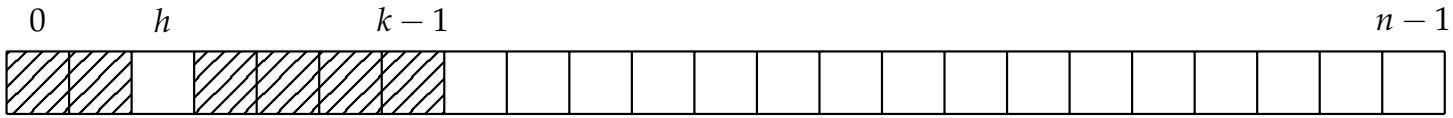
... efficiently computable from $\boldsymbol{G}$.

Here:

$$\mathcal{F}_{\mathrm{TRS}} = \langle 1, x, \ldots, x^{h-1}, x^h + \underbrace{\eta}_{\in \mathbb{F}_{q^2}} x^{k-1+t}, x^{h+1}, \ldots, x^{k-1} \rangle_{\mathbb{F}_{q^2}}$$



$$\mathcal{F}_{\mathrm{TRS}} \cap \mathbb{F}_q[x] = \langle 1, x, \ldots, x^{h-1}, 0, x^{h+1}, \ldots, x^{k-1} \rangle_{\mathbb{F}_q}$$



Close to a Reed–Solomon code!!

Squaring

Filling the gap by the **squaring method**.

Square code of $\mathcal{C}$:

$$\mathcal{C}^{\star 2} = \langle \boldsymbol{c} \star \boldsymbol{c}' \mid \boldsymbol{c} \in \mathcal{C}, \boldsymbol{c}' \in \mathcal{C} \rangle \subseteq \mathbb{F}_q^n$$

... efficiently computable from $\boldsymbol{G}$.

Squaring

Filling the gap by the **squaring method**.

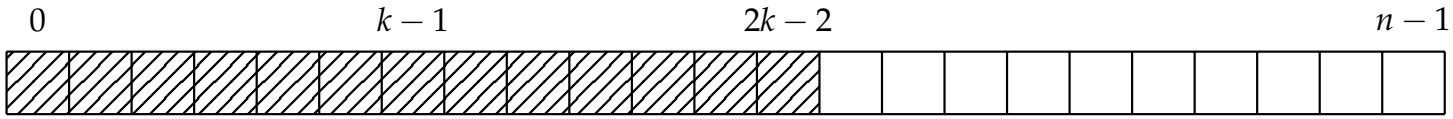
Square code of $\mathcal{C}$:

$$\mathcal{C}^{\star 2} = \langle \boldsymbol{c} \star \boldsymbol{c}' \mid \boldsymbol{c} \in \mathcal{C}, \boldsymbol{c}' \in \mathcal{C} \rangle \subseteq \mathbb{F}_q^n$$

... efficiently computable from $\boldsymbol{G}$.

$$\mathcal{F}_{\mathrm{TRS}} \cap \mathbb{F}_q[x] = \langle 1, x, \ldots, x^{h-1}, 0, x^{h+1}, \ldots, x^{k-1} \rangle_{\mathbb{F}_q}$$

$$(\mathcal{F}_{\mathrm{TRS}} \cap \mathbb{F}_q[x])^{\star 2} = \langle 1, x, \ldots, \ldots, x^{2k-2} \rangle_{\mathbb{F}_q}$$



Proposition.

$$(\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta] \cap \mathbb{F}_q^n)^{\star 2} = \mathrm{GRS}_{2k-1}(\boldsymbol{x}, \boldsymbol{1})$$

Using elder's techniques

Apply **Sidelnikov–Shestakov**'s attack on

$$(\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta] \cap \mathbb{F}_q^n)^{\star 2} = \mathrm{GRS}_{2k-1}(\boldsymbol{x}, \mathbf{1})$$

We also know that $\infty \notin \boldsymbol{x}$ and $\boldsymbol{y} = \mathbf{1}$.

$$\Longrightarrow \text{ the algorithm outputs } \boldsymbol{x}' = a\boldsymbol{x} + b\mathbf{1} \text{ for some } a, b \in \mathbb{F}_q$$

Using elder's techniques

Apply **Sidelnikov–Shestakov**'s attack on

$$(\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta] \cap \mathbb{F}_q^n)^{\star 2} = \mathrm{GRS}_{2k-1}(\boldsymbol{x}, \mathbf{1})$$

We also know that $\infty \notin \boldsymbol{x}$ and $\boldsymbol{y} = \mathbf{1}$.

$$\Longrightarrow \text{ the algorithm outputs } \boldsymbol{x}' = a\boldsymbol{x} + b\mathbf{1} \text{ for some } a, b \in \mathbb{F}_q$$

But... we only have

$$\mathrm{TRS}_k[a\boldsymbol{x}, h, t, \eta] = \mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta a^{k-1+t-h}]$$

Last steps:

- Exhaustive search over $b \Longrightarrow$ recover $a\boldsymbol{x}$
- Find η by interpolation of random codewords.

Summary of the attack

Input. a matrix $\boldsymbol{G} \in \mathbb{F}_{q^2}^{k \times n}$ generating $\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta] \subseteq \mathbb{F}_{q^2}^n$.

Output. a pair $(a\boldsymbol{x}, \eta a^{k-1+t-h})$ equivalent to $(\boldsymbol{x}, \eta)$.

1. Compute a generator matrix $\boldsymbol{G}_{\mathrm{sub}}$ of the subfield subcode
$$\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta] \cap \mathbb{F}_q^n \,.$$
2. Compute a generator matrix $\boldsymbol{G}_{\mathrm{sub}}^{\star 2}$ of the square code
$$(\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta] \cap \mathbb{F}_q^n)^{\star 2} \,.$$
3. Apply Sidelnikov–Shestakov attack on $\boldsymbol{G}_{\mathrm{sub}}^{\star 2}$ and recover $\boldsymbol{x}' = a\boldsymbol{x} + b\mathbf{1}$.
4. Find $b \in \mathbb{F}_q$ such that $\mathrm{ev}_{\boldsymbol{x}' - b\mathbf{1}}(x^j) \in \mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta]$ for all $j < h - 1$.
5. Find η by interpolation of random words in $\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta]$.

Summary of the attack

Input. a matrix $\boldsymbol{G} \in \mathbb{F}_{q^2}^{k\times n}$ generating $\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta] \subseteq \mathbb{F}_{q^2}^n$.

Output. a pair $(a\boldsymbol{x}, \eta a^{k-1+t-h})$ equivalent to $(\boldsymbol{x}, \eta)$.

1. Compute a generator matrix $\boldsymbol{G}_{\mathrm{sub}}$ of the subfield subcode
$$\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta] \cap \mathbb{F}_q^n \,.$$
2. Compute a generator matrix $\boldsymbol{G}_{\mathrm{sub}}^{\star 2}$ of the square code
$$(\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta] \cap \mathbb{F}_q^n)^{\star 2} \,.$$
3. Apply Sidelnikov–Shestakov attack on $\boldsymbol{G}_{\mathrm{sub}}^{\star 2}$ and recover $\boldsymbol{x}' = a\boldsymbol{x} + b\mathbf{1}$.
4. Find $b \in \mathbb{F}_q$ such that $\mathrm{ev}_{\boldsymbol{x}'-b\mathbf{1}}(x^j) \in \mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta]$ for all $j < h - 1$.
5. Find η by interpolation of random words in $\mathrm{TRS}_k[\boldsymbol{x}, h, t, \eta]$.

Theorem. [L., Renner] There is a key-recovery attack over the twisted Reed–Solomon variant of McEliece cryptosystem running in $\mathcal{O}(\max\{q, n\}n^3)$ operations over $\mathbb{F}_q$.

Questions?