Code-Based Cryptography

- 1. Error-Correcting Codes and Cryptography
- 2. McEliece Cryptosystem
- 3. Message Attacks (ISD)
- 4. Key Attacks
- 5. Other Cryptographic Constructions Relying on Coding Theory

4. Key Attacks

- 1. Introduction
- 2. Support Splitting Algorithm
- 3. Distinguisher for GRS codes
- 4. Attack against subcodes of GRS codes
- 5. Error-Correcting Pairs
- 6. Attack against GRS codes
- 7. Attack against Reed-Muller codes
- 8. Attack against Algebraic Geometry codes
- 9. Goppa codes still resist

→ *n*, *k* nonnegative integers such that $1 \le k \le n \le q$.

- → *n*, *k* nonnegative integers such that $1 \le k \le n \le q$.
- → $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.

- → *n*, *k* nonnegative integers such that 1 < k < n < q.
- → $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$. → $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all *i*.

- → *n*, *k* nonnegative integers such that 1 < k < n < q.
- → $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$. → $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all *i*.

Polynomial Vector Space:

$$L_k = \mathbb{F}_q[X]_{< k} = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) < k\}$$

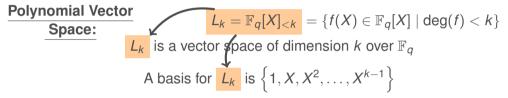
- → *n*, *k* nonnegative integers such that 1 < k < n < q.
- → $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$. → $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all *i*.

Polynomial Vector Space:

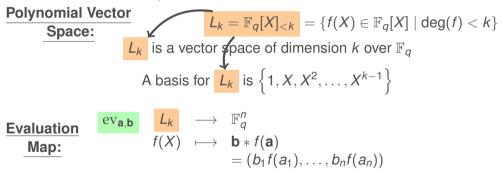
$$\boxed{\textbf{L}_k = \mathbb{F}_q[X]_{< k}} = \{f(X) \in \mathbb{F}_q[X] \mid \mathsf{deg}(f) < k\}$$

 L_k is a vector space of dimension k over \mathbb{F}_q

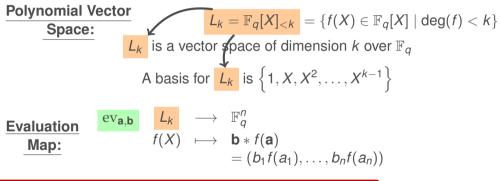
- → *n*, *k* nonnegative integers such that $1 \le k \le n \le q$.
- → $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.
- → **b** = $(b_1, \ldots, b_n) \in \mathbb{F}_q^{\hat{n}}$ with $b_i \neq 0$ for all *i*.



- → *n*, *k* nonnegative integers such that $1 \le k \le n \le q$.
- → $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.
- → **b** = $(b_1, \ldots, b_n) \in \mathbb{F}_q^{\hat{n}}$ with $b_i \neq 0$ for all *i*.



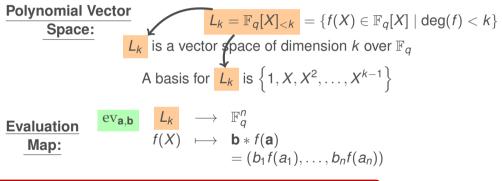
- → *n*, *k* nonnegative integers such that $1 \le k \le n \le q$.
- → $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.
- → **b** = $(b_1, \ldots, b_n) \in \mathbb{F}_q^{\hat{n}}$ with $b_i \neq 0$ for all *i*.



The Generalized Reed-Solomon code (GRS)

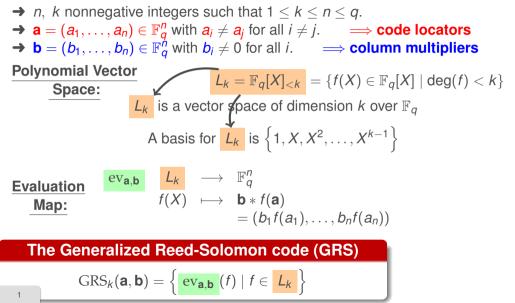
$$\operatorname{GRS}_k(\mathbf{a}, \mathbf{b}) = \left\{ \operatorname{ev}_{\mathbf{a}, \mathbf{b}}(f) \mid f \in L_k \right\}$$

- → *n*, *k* nonnegative integers such that $1 \le k \le n \le q$.
- → $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$. \implies code locators → $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all *i*.



The Generalized Reed-Solomon code (GRS)

$$\operatorname{GRS}_k(\mathbf{a}, \mathbf{b}) = \left\{ \operatorname{ev}_{\mathbf{a}, \mathbf{b}}(f) \mid f \in L_k \right\}$$



Some Properties - GRS codes

Parameters - GRS are optimal codes

The $GRS_k(\mathbf{a}, \mathbf{b})$ is an $[n, k]_q$ code with minimum distance d = n - k + 1

Some Properties - GRS codes

Parameters - GRS are optimal codes

The $GRS_k(\mathbf{a}, \mathbf{b})$ is an $[n, k]_q$ code with minimum distance d = n - k + 1

The dual code of a GRS code is a GRS code

 $\operatorname{GRS}_k(\mathbf{a},\mathbf{b})^{\perp} = \operatorname{GRS}_{n-k}(\mathbf{a},\mathbf{b}^{\perp})$

Some Properties - GRS codes

Parameters - GRS are optimal codes

The $GRS_k(\mathbf{a}, \mathbf{b})$ is an $[n, k]_q$ code with minimum distance d = n - k + 1

The dual code of a GRS code is a GRS code

 $\operatorname{GRS}_k(\mathbf{a},\mathbf{b})^{\perp} = \operatorname{GRS}_{n-k}(\mathbf{a},\mathbf{b}^{\perp})$

GRS codes under transformations

There exists

→
$$\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$$
 with $c_i \neq c_j$ for all $i \neq j$ such that $c_1 = 0$ and $c_2 = 1$

→ $\mathbf{d} = (d_1, \ldots, d_n) \in \mathbb{F}_q^n$ with $d_i \neq 0$ for all *i*.

such that: $GRS_k(\mathbf{a}, \mathbf{b}) = GRS_k(\mathbf{c}, \mathbf{d})$

McEliece based on GRS codes



Generalized Reed-Solomon codes



H. Niederreiter.

Knapsack-type cryptosystems and algebraic coding theory. Problems of Control and Information Theory, 15(2):159-166, 1986.

Parameters	Key size	Security level
$[256, 128, 129]_{256}$	67 ko	2 ⁹⁵

McEliece based on GRS codes



Generalized Reed-Solomon codes



H. Niederreiter.

Knapsack-type cryptosystems and algebraic coding theory. Problems of Control and Information Theory, 15(2):159-166, 1986.

Parameters	Key size	Security level
$[256, 128, 129]_{256}$	67 ko	2 ⁹⁵

X Attack against this proposal:

V. M. Sidelnikov and S. O. Shestakov.

On the insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Math. Appl., 2:439-444, 1992.

Star Product

Given two vectors $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ and $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ we denote by

a * **b** the componentwise product:

 $\mathbf{a} * \mathbf{b} = (a_1 b_1, \dots, a_n b_n)$

Star Product

Given two vectors $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ and $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ we denote by

a * **b** the componentwise product:

 $\mathbf{a} * \mathbf{b} = (a_1 b_1, \dots, a_n b_n)$

Star Product of Codes

Let *A* and *B* be \mathbb{F}_q -codes of length *n*.

The **star product code** denoted by **A** * **B** is:

 $A * B = \langle \{ a * b \mid a \in A \text{ and } b \in B \} \rangle$

When B = A, then A * A is called the **square** of A and is denoted by A^2

Proposition: Dimension of the Square Code

Let *A* and *B* be \mathbb{F}_q -codes of length *n* with $(\mathbf{a}_i)_{i \in I}$ and $(\mathbf{b}_j)_{j \in J}$ as bases, respectively. Then:

1. $K(\boldsymbol{A} \ast \boldsymbol{B}) \leq K(\boldsymbol{A})K(\boldsymbol{B})$

2.
$$K(\mathbf{A}^2) \leq \binom{K(\mathbf{A}) + 1}{2}$$

Proposition: Dimension of the Square Code

Let *A* and *B* be \mathbb{F}_q -codes of length *n* with $(\mathbf{a}_i)_{i \in I}$ and $(\mathbf{b}_j)_{j \in J}$ as bases, respectively. Then:

1. $K(\mathbf{A} * \mathbf{B}) \leq K(\mathbf{A})K(\mathbf{B})$

$$\mathbf{2.} \ \mathbf{K}(\mathbf{A}^2) \leq \binom{\mathbf{K}(\mathbf{A}) + 1}{2}$$

Proof:

Note that:

- 1. A * B is generated by the $\mathbf{a}_i * \mathbf{b}_j' s$ with $i \in I$ and $j \in J$
- **2**. A^2 is generated by the $\mathbf{a}_i * \mathbf{a}_j$ with $i \le j$

Proposition: Dimension of the Square Code

Let *A* and *B* be \mathbb{F}_q -codes of length *n* with $(\mathbf{a}_i)_{i \in I}$ and $(\mathbf{b}_j)_{j \in J}$ as bases, respectively. Then:

1. $K(\boldsymbol{A} \ast \boldsymbol{B}) \leq K(\boldsymbol{A})K(\boldsymbol{B})$

$$2. \ \mathcal{K}(\mathbf{A}^2) \leq \binom{\mathcal{K}(\mathbf{A}) + 1}{2}$$

Complexity of computing A^2 is $O\left(K(A)^2 n^2\right)$ operations in \mathbb{F}_q .

Proof:

Note that:

- 1. A * B is generated by the $\mathbf{a}_i * \mathbf{b}_j' s$ with $i \in I$ and $j \in J$
- **2**. A^2 is generated by the $\mathbf{a}_i * \mathbf{a}_j$ with $i \le j$

Proposition:

Let A be an $[n, k]_q$ code.

The complexity of computing the code A^2 is $\mathcal{O}\left(k^2n^2\right)$ operations in \mathbb{F}_q .

Proposition:

Let A be an $[n, k]_q$ code.

The complexity of computing the code A^2 is $\mathcal{O}\left(k^2n^2\right)$ operations in \mathbb{F}_q .

Proof:

1. Computing all of the $\binom{k(A) + 1}{2}$ generators of A^2 , i.e. $\mathbf{a}_i * \mathbf{a}_j$ with $i \le j$ → Cost: $\mathcal{O}(k^2n)$ operations in \mathbb{F}_q

Proposition:

Let A be an $[n, k]_q$ code.

The complexity of computing the code A^2 is $\mathcal{O}\left(k^2n^2\right)$ operations in \mathbb{F}_q .

Proof:

Computing all of the ^{k(A) + 1}/₂ generators of A², i.e. a_i * a_j with i ≤ j
 → Cost: O(k²n) operations in F_q
 Apply Gaussian elimination to a ^{k + 1}/₂ × n matrix
 → Cost: O(k²n²) operations in F_q

Distinguisher - Square Code

Let *A* be an $[n, k]_q$ random linear code. We expect that the dimension of A^2 should be of order:

$$K(A^2) \sim \min\left\{\binom{k+1}{2}, n\right\}$$

Theorem:

Let *A* be a random linear code of dimension *k* such that $k = O(\sqrt{n})$. Then,

$$\Pr\left(K(A^2) < \binom{k+1}{2}\right) \xrightarrow[n \to \infty]{} 0$$



J.C. Faugère, V. Gauthier-Umaña, A. Otmani, L. Perret and J.P. Tillich.

A distinguisher for high-rate McEliece cryptosystems. IEEE Transactions on Information Theory, 59(10):6830-8644, 2013.

Distinguisher - Square Code - GRS codes

Proposition:

If
$$k \leq \frac{n+1}{2}$$
. Then,

$$\operatorname{GRS}_k(\mathbf{a},\mathbf{b})^2 = \operatorname{GRS}_{2k-1}(\mathbf{a},\mathbf{b}*\mathbf{b})$$

Proof:

"⇒" Let
$$\mathbf{c}_1, \mathbf{c}_2 \in \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$$
.
Then, there exists $f, g \in \mathbb{F}_q[X]_{ such that
 $\mathbf{c}_1 * \mathbf{c}_2 = \mathrm{ev}_{\mathbf{a}, \mathbf{b}}(f) * \mathrm{ev}_{\mathbf{a}, \mathbf{b}}(g) = (\mathbf{b} * f(\mathbf{a})) * (\mathbf{b} * g(\mathbf{a})) = (\mathbf{b} * \mathbf{b}) * (fg)(\mathbf{a})$
with deg $(fg) \le 2k - 2$
Thus, $\mathbf{c}_1 * \mathbf{c}_2 \in \mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$$

"—" The converse is proved **similarly**.

Distinguisher - Square Code - GRS codes

Proposition:

If $k > \frac{n+1}{2}$, then we can apply the previous property to the dual of $\text{GRS}_k(\mathbf{a}, \mathbf{b})$

Proof:

1. Recall that, the dual of a GRS code is a GRS code:

$$\underbrace{\operatorname{GRS}_{k}(\mathbf{a}, \mathbf{b})^{\perp}}_{A} = \operatorname{GRS}_{n-k}(\mathbf{a}, \mathbf{c})$$
2. Moreover, if $k > \frac{n+1}{2}$, then:

$$K(A) = n - k < n - \frac{n+1}{2} < \frac{n+1}{2}$$

3. Applying the previous Proposition:

$$\left(\mathrm{GRS}_{k}(\mathbf{a},\mathbf{b})^{\perp}\right)^{2} = \mathrm{GRS}_{2K(\mathcal{A})-1}(\mathbf{a},\mathbf{c}*\mathbf{c})$$

Distinguisher - Square Code - GRS codes

1. If C is a **random** linear code of length n, with high probability:

$$K(\mathcal{C}^2) = \min\left\{\binom{K(\mathcal{C})+1}{2}, n\right\}$$

2. If C is a **GRS** code

$$K(\mathcal{C}^2) = \min \left\{ 2K(\mathcal{C}) - 1, n \right\}$$



I. Márguez-Corbella, E. Martínez-Moro and R. Pellikaan.

The non-gap sequence of a subcode of a generalized Reed-Solomon code. Designs, Codes and Cryptography, volume 66, Issue 1-3, 317-333, 2013.

C. Wieschebrink.

Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes. POCrypto 2010, LNCS, volume 6061, 61-72, 2010,

4. Key Attacks

- 1. Introduction
- 2. Support Splitting Algorithm
- 3. Distinguisher for GRS codes
- 4. Attack against subcodes of GRS codes
- 5. Error-Correcting Pairs
- 6. Attack against GRS codes
- 7. Attack against Reed-Muller codes
- 8. Attack against Algebraic Geometry codes
- 9. Goppa codes still resist