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

Subcodes of GRS codes for the McEliece scheme



Subcodes of GRS codes



T. Berger and P. Loidreau.

How to mask the structure of codes for a cryptographic use. Des. Codes Cryptogr., 35:63-79, 2005.

Subcodes of GRS codes for the McEliece scheme



Subcodes of GRS codes



T. Berger and P. Loidreau.

How to mask the structure of codes for a cryptographic use. Des. Codes Cryptogr., 35:63-79, 2005.



Attack against this proposal:



C. Wieschebrink.

Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. In Post-Quantum Cryptography, volume 6061 of Lecture Notes in Comput. Sci., pages 61–72, 2010.

Public Key:
$$\mathcal{K}_{\text{pub}} = \begin{cases} \text{a gen. matrix of } \mathcal{C} \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{n-k}{2} \right\rfloor \end{cases}$$

Public Key:
$$\mathcal{K}_{\text{pub}} = \left\{ \begin{array}{l} \text{a gen. matrix of } \mathcal{C} \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{n-k}{2} \right\rfloor \end{array} \right.$$

The Algorithm:

STEP 1 Compute $C^{(2)}$.

With High Probability:

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

Public Key:
$$\mathcal{K}_{\text{pub}} = \left\{ \begin{array}{l} \text{a gen. matrix of } \mathcal{C} \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{n-k}{2} \right\rfloor \end{array} \right.$$

The Algorithm:

STEP 1 Compute $C^{(2)}$.

With **High Probability**:

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

STEP 2 Apply the Sidelnikov-Shestakov attack to recover

a and $\mathbf{b} * \mathbf{b}$

Let:

 \rightarrow C be an $[n, k]_q$ code

Let:

- \rightarrow C be an $[n, k]_q$ code
- \rightarrow (J, \overline{J}) be a partition of $\{1, \dots, n\}$

Let:

- \rightarrow C be an $[n, k]_q$ code
- \rightarrow (J, \overline{J}) be a partition of $\{1, \dots, n\}$
- → \mathbf{x}_J the **restriction** of $\mathbf{x} \in \mathbb{F}_q^n$ to the coordinates indexed by J

Let:

- \rightarrow C be an $[n, k]_q$ code
- \rightarrow (J, \overline{J}) be a partition of $\{1, \dots, n\}$
- → \mathbf{x}_J the **restriction** of $\mathbf{x} \in \mathbb{F}_q^n$ to the coordinates indexed by J

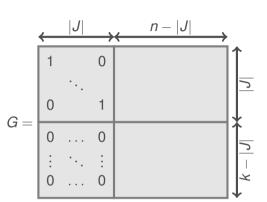
Shortened code $S_J(C)$

The words of $S_J(\mathcal{C})$ are codewords of \mathcal{C} that have a zero in the J-locations, i.e.

$$S_J(\mathcal{C}) = \{ \mathbf{c}_{\overline{J}} \mid \mathbf{c} \in \mathcal{C} \text{ and } c_j = 0 \text{ for all } j \in J \}$$

Let:

- \rightarrow C be an $[n, k]_q$ code
- \rightarrow (J, \overline{J}) be a partition of $\{1, \dots, n\}$
- → \mathbf{x}_J the **restriction** of $\mathbf{x} \in \mathbb{F}_q^n$ to the coordinates indexed by J



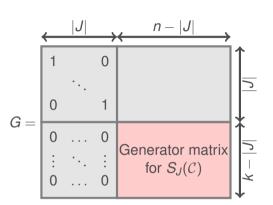
Shortened code $S_J(C)$

The words of $S_J(\mathcal{C})$ are codewords of \mathcal{C} that have a zero in the J-locations, i.e.

$$\mathcal{S}_J(\mathcal{C}) = \left\{ \mathbf{c}_{\overline{J}} \mid \mathbf{c} \in \mathcal{C} \text{ and } c_j = 0 \text{ for all } j \in J \right\}$$

Let:

- \rightarrow C be an $[n, k]_q$ code
- \rightarrow (J, \overline{J}) be a partition of $\{1, \ldots, n\}$
- → \mathbf{x}_J the **restriction** of $\mathbf{x} \in \mathbb{F}_q^n$ to the coordinates indexed by J



Shortened code $S_J(C)$

The words of $S_J(\mathcal{C})$ are codewords of \mathcal{C} that have a zero in the J-locations, i.e.

$$\mathcal{S}_J(\mathcal{C}) = \left\{ \mathbf{c}_{\overline{J}} \mid \mathbf{c} \in \mathcal{C} \text{ and } c_j = 0 \text{ for all } j \in J \right\}$$

The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J(GRS_k(\mathbf{a},\mathbf{b})) = GRS_{n-|J|}(\mathbf{a}_{\overline{J}},\mathbf{b}') \text{ with } b_i' = b_i \prod_{j \in J} (a_i - a_j)$$

<u>Proof:</u> Assume $J = \{1\}$. Let G be a gen. matrix for $GRS_k(\mathbf{a}, \mathbf{b})$.

$$G = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ b_1 a_1 & b_2 a_2 & \dots & b_n a_n \\ \vdots & \vdots & \ddots & \vdots \\ b_1 a_1^{k-1} & b_2 a_2^{k-1} & \dots & b_n a_n^{k-1} \end{pmatrix}$$

The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J(GRS_k(\mathbf{a},\mathbf{b})) = GRS_{n-|J|}(\mathbf{a}_{\overline{J}},\mathbf{b}') \text{ with } b_i' = b_i \prod_{j \in J} (a_i - a_j)$$

Proof: Assume $J = \{1\}$. Let G be a gen. matrix for $GRS_k(\mathbf{a}, \mathbf{b})$.

The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J(GRS_k(\mathbf{a},\mathbf{b})) = GRS_{n-|J|}(\mathbf{a}_{\overline{J}},\mathbf{b}') \text{ with } b_i' = b_i \prod_{j \in J} (a_i - a_j)$$

<u>Proof:</u> Assume $J = \{1\}$. Let G be a gen. matrix for $GRS_k(\mathbf{a}, \mathbf{b})$.

$$G = \begin{bmatrix} b_1 & b_2 & \dots & b_n \\ \hline b_1a_1 & b_2a_2 & \dots & b_na_n \\ \vdots & \vdots & \ddots & \vdots \\ b_1a_1^{k-1} & b_2a_2^{k-1} & \dots & b_na_n^{k-1} \end{bmatrix} \longrightarrow \mathbf{g}_2$$

The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J(GRS_k(\mathbf{a},\mathbf{b})) = GRS_{n-|J|}(\mathbf{a}_{\overline{J}},\mathbf{b}') \text{ with } b_i' = b_i \prod_{j \in J} (a_i - a_j)$$

<u>Proof:</u> Assume $J = \{1\}$. Let G be a gen. matrix for $GRS_k(\mathbf{a}, \mathbf{b})$.

The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J(GRS_k(\mathbf{a},\mathbf{b})) = GRS_{n-|J|}(\mathbf{a}_{\overline{J}},\mathbf{b}') \text{ with } b_i' = b_i \prod_{j \in J} (a_i - a_j)$$

Proof: Assume $J = \{1\}$. Let G be a gen. matrix for $GRS_k(\mathbf{a}, \mathbf{b})$.

The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J(GRS_k(\mathbf{a},\mathbf{b})) = GRS_{n-|J|}(\mathbf{a}_{\overline{J}},\mathbf{b}') \text{ with } b_i' = b_i \prod_{j \in J} (a_i - a_j)$$

<u>Proof:</u> Assume $J = \{1\}$. Let G be a gen. matrix for $GRS_k(\mathbf{a}, \mathbf{b})$.



The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J(GRS_k(\mathbf{a},\mathbf{b})) = GRS_{n-|J|}(\mathbf{a}_{\overline{J}},\mathbf{b}') \text{ with } b_i' = b_i \prod_{i \in J} (a_i - a_j)$$

<u>Proof:</u> Assume $J = \{1\}$. Let G be a gen. matrix for $GRS_k(\mathbf{a}, \mathbf{b})$.

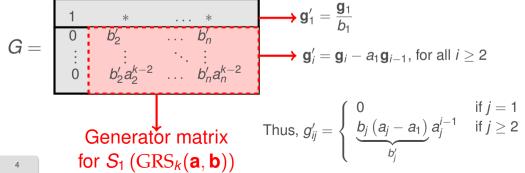
Thus,
$$g'_{ij} = \left\{ \begin{array}{ll} 0 & \text{if } j = 1 \\ \underbrace{b_j \left(a_j - a_1 \right)}_{b'_i} a_j^{i-1} & \text{if } j \geq 2 \end{array} \right.$$

The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J(GRS_k(\mathbf{a},\mathbf{b})) = GRS_{n-|J|}(\mathbf{a}_{\overline{J}},\mathbf{b}') \text{ with } b_i' = b_i \prod_{i \in J} (a_i - a_j)$$

Proof: Assume $J = \{1\}$. Let G be a gen. matrix for $GRS_k(\mathbf{a}, \mathbf{b})$.



Public Key:
$$\mathcal{K}_{\text{pub}} = \left\{ \begin{array}{l} \text{a gen. matrix of } \mathcal{C} \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{n-k}{2} \right\rfloor \end{array} \right.$$

Public Key:
$$\mathcal{K}_{\text{pub}} = \left\{ \begin{array}{l} \text{a gen. matrix of } \mathcal{C} \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{n-k}{2} \right\rfloor \end{array} \right.$$

The Algorithm:

STEP 1 Chose a set of indices

$$J = \{i_1, ..., i_N\} \subseteq \{1, ..., n\}$$
 such that $2(k - N) \le n - 2$

Public Key:
$$\mathcal{K}_{\text{pub}} = \begin{cases} \text{a gen. matrix of } \mathcal{C} \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{n-k}{2} \right\rfloor \end{cases}$$

The Algorithm:

STEP 1 Chose a set of indices

$$J = \{i_1, \dots, i_N\} \subseteq \{1, \dots, n\}$$
 such that $2(k - N) \le n - 2$

STEP 2 Compute a generator matrix of the shortened code $S_J(\mathcal{C})$

$$S_J(\mathcal{C}) \subseteq GRS_{k-N}(\mathbf{a}_J, \mathbf{b}')$$

Recall that

with
$$b_i' = b_i \prod_{i \in I} (a_i - a_j)$$
 for all $j \notin J$

The Algorithm:

STEP 1 Chose a set of indices

$$J = \{i_1, ..., i_N\} \subseteq \{1, ..., n\}$$
 such that $2(k - N) \le n - 2$

STEP 2 Compute a generator matrix of the shortened code $S_J(\mathcal{C}) \subseteq GRS_{k-N}(\mathbf{a}_J, \mathbf{b}')$

STEP 3 Apply the previous algorithm to retrieve \mathbf{a}_J and \mathbf{b}' .

Note that
$$2(k - N) \le n - 2$$
.

Public Key:
$$\mathcal{K}_{\text{pub}} = \left\{ \begin{array}{l} \text{a gen. matrix of } \mathcal{C} \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{n-k}{2} \right\rfloor \end{array} \right.$$

The Algorithm:

STEP 1 Chose a set of indices

$$J = \{i_1, \dots, i_N\} \subseteq \{1, \dots, n\}$$
 such that $2(k - N) \le n - 2$

STEP 2 Compute a generator matrix of the shortened code $S_J(\mathcal{C}) \subseteq GRS_{k-N}(\mathbf{a}_J, \mathbf{b}')$

STEP 3 Apply the previous algorithm to retrieve \mathbf{a}_J and \mathbf{b}' .

Note that $2(k - N) \le n - 2$.

STEP 4 Return to STEP 1 until a is completely retrieved.

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
- Attack against Reed-Muller codes
- 8. Attack against Algebraic Geometry codes
- 9. Goppa codes still resist