Code-Based Cryptography

4. Key Attacks

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.

Attack - If $2k - 1 \leq n - 2$

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

Attack - If $2k - 1 \leq n - 2$

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

The Algorithm:

STEP 1 Compute $\mathcal{C}^{(2)}$.
With **High Probability**:

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

Attack - If $2k - 1 \leq n - 2$

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

The Algorithm:

STEP 1 Compute $\mathcal{C}^{(2)}$.
With **High Probability**:

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

STEP 2 Apply the **Sidelnikov-Shestakov** attack to recover

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

Shortened code

Let:

- ➜ $\mathcal{C}$ be an $[n, k]_q$ code

Shortened code

Let:

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

Shortened code

Let:

- ➜ $\mathcal{C}$ be an $[n, k]_q$ code
- ➜ $(J, \overline{J})$ 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

Let:

- ➜ $\mathcal{C}$ be an $[n, k]_q$ code
- ➜ $(J, \overline{J})$ 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 $S_J(\mathcal{C})$

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

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

Shortened code

Let:

- ➜ $\mathcal{C}$ be an $[n, k]_q$ code
- ➜ $(J, \overline{J})$ 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

$$\begin{array}{ccc}
 & \begin{array}{cc} \overset{|J|}{\longleftrightarrow} & \overset{n-|J|}{\longleftrightarrow} \end{array} & \\
G = & \left[\begin{array}{c|c} \begin{matrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{matrix} & \phantom{\begin{matrix} 0 & 0 & 0 \end{matrix}} \\ \hline \begin{matrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{matrix} & \end{array}\right] & \begin{matrix} |J| \\ \\ k-|J| \end{matrix}
\end{array}$$

Shortened code $S_J(\mathcal{C})$

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

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

Shortened code

$$G = \begin{array}{cc} \begin{array}{cc} \quad |J| \quad & \quad\quad n-|J| \quad\quad \end{array} & \\ \left[\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & \\ 0 & & 1 & \\ \hline 0 & \dots & 0 & \\ \vdots & \ddots & \vdots & \text{Generator matrix} \\ & & & \text{for } S_J(\mathcal{C}) \\ 0 & \dots & 0 & \end{array}\right] & \begin{array}{c} |J| \\ \\ \\ \\ k-|J| \end{array} \end{array}$$

Let:

- ➜ $\mathcal{C}$ be an $[n,k]_q$ code
- ➜ $(J, \overline{J})$ 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 $S_J(\mathcal{C})$

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

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

Shortening a GRS code

The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J\left(\mathrm{GRS}_k(\mathbf{a},\mathbf{b})\right) = \mathrm{GRS}_{n-|J|}(\mathbf{a}_{\overline{J}},\mathbf{b}') \text{ with } b_i' = b_i \prod_{j\in J}(a_i - a_j)$$

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

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

Shortening a GRS code

The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J\left(\mathrm{GRS}_k(\mathbf{a},\mathbf{b})\right) = \mathrm{GRS}_{n-|J|}(\mathbf{a}_{\overline{J}},\mathbf{b}') \text{ with } b'_i = b_i \prod_{j\in J}(a_i - a_j)$$

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

$$G = \begin{array}{l} \boxed{\begin{matrix} b_1 & b_2 & \dots & b_n \end{matrix}} \xrightarrow{\quad} \mathbf{g}_1 \\ \begin{matrix} b_1 a_1 & b_2 a_2 & \dots & b_n a_n \\ \vdots & \vdots & \ddots & \vdots \\ b_1 a_1^{k-1} & b_2 a_2^{k-1} & \dots & b_n a_n^{k-1} \end{matrix} \end{array}$$

Shortening a GRS code

The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J\left(\mathrm{GRS}_k(\mathbf{a},\mathbf{b})\right) = \mathrm{GRS}_{n-|J|}(\mathbf{a}_{\overline{J}},\mathbf{b}') \text{ with } b_i' = b_i \prod_{j \in J}(a_i - a_j)$$

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

$$G = \begin{matrix} b_1 & b_2 & \dots & b_n \\ b_1 a_1 & b_2 a_2 & \dots & b_n a_n \\ \vdots & \vdots & \ddots & \vdots \\ b_1 a_1^{k-1} & b_2 a_2^{k-1} & \dots & b_n a_n^{k-1} \end{matrix} \begin{array}{l} \\ \longrightarrow \mathbf{g}_2 \\ \\ \\ \end{array}$$

Shortening a GRS code

The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J\left(\mathrm{GRS}_k(\mathbf{a},\mathbf{b})\right) = \mathrm{GRS}_{n-|J|}(\mathbf{a}_{\overline{J}},\mathbf{b}') \text{ with } b'_i = b_i \prod_{j\in J}(a_i - a_j)$$

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

$$G = \begin{array}{cccc} b_1 & b_2 & \dots & b_n \\ b_1 a_1 & b_2 a_2 & \dots & b_n a_n \\ \vdots & \vdots & \ddots & \vdots \\ \boxed{b_1 a_1^{k-1} \quad b_2 a_2^{k-1} \quad \dots \quad b_n a_n^{k-1}} \end{array} \longrightarrow \mathbf{g}_k$$

Shortening a GRS code

The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J\left(\mathrm{GRS}_k(\mathbf{a},\mathbf{b})\right) = \mathrm{GRS}_{n-|J|}(\mathbf{a}_{\overline{J}}, \mathbf{b}') \text{ with } b_i' = b_i \prod_{j\in J}(a_i - a_j)$$

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

$$G = \begin{array}{l} \boxed{\begin{matrix} 1 & * & \dots & * \end{matrix}} \longrightarrow \mathbf{g}_1' = \dfrac{\mathbf{g}_1}{b_1} \\ \begin{matrix} b_1 a_1 & b_2 a_2 & \dots & b_n a_n \\ \vdots & \vdots & \ddots & \vdots \\ b_1 a_1^{k-1} & b_2 a_2^{k-1} & \dots & b_n a_n^{k-1} \end{matrix} \end{array}$$

Shortening a GRS code

The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J\left(\mathrm{GRS}_k(\mathbf{a},\mathbf{b})\right) = \mathrm{GRS}_{n-|J|}(\mathbf{a}_{\overline{J}}, \mathbf{b}') \text{ with } b_i' = b_i \prod_{j\in J}(a_i - a_j)$$

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

$$G = \left[\begin{array}{cccc} 1 & * & \dots & * \\ \hline & & & \\ & & & \\ \end{array}\right] \begin{array}{l} \longrightarrow \mathbf{g}_1' = \dfrac{\mathbf{g}_1}{b_1} \\ \longrightarrow \mathbf{g}_i' = \mathbf{g}_i - a_1\mathbf{g}_{i-1}, \text{ for all } i \geq 2 \end{array}$$

Shortening a GRS code

The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J\left(\mathrm{GRS}_k(\mathbf{a},\mathbf{b})\right) = \mathrm{GRS}_{n-|J|}(\mathbf{a}_{\overline{J}}, \mathbf{b}') \text{ with } b'_i = b_i \prod_{j\in J}(a_i - a_j)$$

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

$$G = \begin{bmatrix} 1 & * & \dots & * \\ \hline 0 & b'_2 & \dots & b'_n \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b'_2 a_2^{k-2} & \dots & b'_n a_n^{k-2} \end{bmatrix}$$

$\longrightarrow \mathbf{g}'_1 = \dfrac{\mathbf{g}_1}{b_1}$

$\longrightarrow \mathbf{g}'_i = \mathbf{g}_i - a_1\mathbf{g}_{i-1}$, for all $i \geq 2$

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

Shortening a GRS code

The shortened code of a GRS code is GRS code

For GRS code we always have:

$$S_J\left(\mathrm{GRS}_k(\mathbf{a},\mathbf{b})\right) = \mathrm{GRS}_{n-|J|}(\mathbf{a}_{\bar{J}}, \mathbf{b}') \text{ with } b'_i = b_i \prod_{j\in J}(a_i - a_j)$$

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

$$G = \left[\begin{array}{c|ccc} 1 & * & \dots & * \\ \hline 0 & b'_2 & \dots & b'_n \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b'_2 a_2^{k-2} & \dots & b'_n a_n^{k-2} \end{array}\right]$$

$$\mathbf{g}'_1 = \frac{\mathbf{g}_1}{b_1}$$

$$\mathbf{g}'_i = \mathbf{g}_i - a_1\mathbf{g}_{i-1}, \text{ for all } i \geq 2$$

Generator matrix for $S_1\left(\mathrm{GRS}_k(\mathbf{a},\mathbf{b})\right)$

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

Attack - If $2k - 1 > n - 2$

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

Attack - If $2k - 1 > n - 2$

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

The Algorithm:

STEP 1 Chose a set of indices

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

Attack - If $2k - 1 > n - 2$

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

The Algorithm:

STEP 1 Chose a set of indices

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

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

Recall that

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

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

Attack - If $2k - 1 > n - 2$

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

The Algorithm:

STEP 1 Chose a set of indices

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

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

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

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

Attack - If $2k - 1 > n - 2$

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

The Algorithm:

STEP 1 Chose a set of indices

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

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

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

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

STEP 4 Return to STEP 1 until $\mathbf{a}$ 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
7. Attack against Reed-Muller codes
8. Attack against Algebraic Geometry codes
9. Goppa codes still resist