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

GRS codes for the McEliece scheme

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}

GRS codes for the McEliece scheme

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}

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.

Filtration Attack for GRS codes

Suppose that we know:

$$\mathcal{C}_k = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \quad \text{and} \quad \mathcal{C}_{k-1} = \mathrm{GRS}_{k-1}(\mathbf{a}, \mathbf{b})$$

Proposition: Assume that $2k - 1 \leq n - 2$

$\mathcal{C}_{k-2} = \mathrm{GRS}_{k-2}(\mathbf{a}, \mathbf{b})$ is the solution space of the following problem

$$\mathbf{c} \in \mathcal{C}_{k-1} \quad \text{and } \mathbf{c} * \mathcal{C}_k \subseteq (\mathcal{C}_{k-1})^2$$

Filtration Attack for GRS codes

Suppose that we know:

$$\mathcal{C}_k = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \quad \text{and} \quad \mathcal{C}_{k-1} = \mathrm{GRS}_{k-1}(\mathbf{a}, \mathbf{b})$$

Proposition: Assume that $2k - 1 \leq n - 2$

$\mathcal{C}_{k-2} = \mathrm{GRS}_{k-2}(\mathbf{a}, \mathbf{b})$ is the solution space of the following problem

$$\mathbf{c} \in \mathcal{C}_{k-1} \quad \text{and } \mathbf{c} * \mathcal{C}_k \subseteq (\mathcal{C}_{k-1})^2$$

Proof: **[Sketch of the Proof]**

Filtration Attack for GRS codes

Suppose that we know:

$$\mathcal{C}_k = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \quad \text{and} \quad \mathcal{C}_{k-1} = \mathrm{GRS}_{k-1}(\mathbf{a}, \mathbf{b})$$

Proposition: Assume that $2k - 1 \leq n - 2$

$\mathcal{C}_{k-2} = \mathrm{GRS}_{k-2}(\mathbf{a}, \mathbf{b})$ is the solution space of the following problem

$$\mathbf{c} \in \mathcal{C}_{k-1} \quad \text{and } \mathbf{c} * \mathcal{C}_k \subseteq (\mathcal{C}_{k-1})^2$$

Proof: [Sketch of the Proof]

$$\mathcal{C}_{k-1} * \mathcal{C}_k = (\mathcal{C}_{k-1})^2$$

Filtration Attack for GRS codes

Suppose that we know:

$$\mathcal{C}_k = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \quad \text{and} \quad \mathcal{C}_{k-1} = \mathrm{GRS}_{k-1}(\mathbf{a}, \mathbf{b})$$

Proposition: Assume that $2k - 1 \leq n - 2$

$\mathcal{C}_{k-2} = \mathrm{GRS}_{k-2}(\mathbf{a}, \mathbf{b})$ is the solution space of the following problem

$$\mathbf{c} \in \mathcal{C}_{k-1} \quad \text{and } \mathbf{c} * \mathcal{C}_k \subseteq (\mathcal{C}_{k-1})^2$$

Proof: [Sketch of the Proof]

$$\mathcal{C}_{k-1} \quad * \quad \mathcal{C}_k \quad = \quad (\mathcal{C}_{k-1})^2$$

$$(\mathbf{b} * f(\mathbf{a})) \quad * \quad (\mathbf{b} * g(\mathbf{a})) \quad = \quad (\mathbf{b} * \mathbf{b})\,(fg)(\mathbf{a})$$

with $\deg(f) < k - 1$, $\deg(g) < k \Rightarrow \deg(fg) < 2k - 2$

Filtration Attack for GRS codes

Suppose that we know:

$$\mathcal{C}_k = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \quad \text{and} \quad \mathcal{C}_{k-1} = \mathrm{GRS}_{k-1}(\mathbf{a}, \mathbf{b})$$

Proposition: Assume that $2k - 1 \leq n - 2$

$\mathcal{C}_{k-2} = \mathrm{GRS}_{k-2}(\mathbf{a}, \mathbf{b})$ is the solution space of the following problem

$$\mathbf{c} \in \mathcal{C}_{k-1} \quad \text{and } \mathbf{c} * \mathcal{C}_k \subseteq (\mathcal{C}_{k-1})^2$$

In this way we build the following filtration

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \supseteq \mathrm{GRS}_{k-1}(\mathbf{a}, \mathbf{b}) \supseteq \mathrm{GRS}_{k-2}(\mathbf{a}, \mathbf{b}) \supseteq \cdots \supseteq \mathrm{GRS}_1(\mathbf{a}, \mathbf{b})$$

Filtration Attack for GRS codes

Suppose that we know:

$$\mathcal{C}_k = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \quad \text{and} \quad \mathcal{C}_{k-1} = \mathrm{GRS}_{k-1}(\mathbf{a}, \mathbf{b})$$

Proposition: Assume that $2k - 1 \leq n - 2$

$\mathcal{C}_{k-2} = \mathrm{GRS}_{k-2}(\mathbf{a}, \mathbf{b})$ is the solution space of the following problem

$$\mathbf{c} \in \mathcal{C}_{k-1} \quad \text{and } \mathbf{c} * \mathcal{C}_k \subseteq (\mathcal{C}_{k-1})^2$$

In this way we build the following filtration

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \supseteq \mathrm{GRS}_{k-1}(\mathbf{a}, \mathbf{b}) \supseteq \mathrm{GRS}_{k-2}(\mathbf{a}, \mathbf{b}) \supseteq \cdots \supseteq \mathrm{GRS}_1(\mathbf{a}, \mathbf{b})$$

Note that: $\mathrm{GRS}_1(\mathbf{a}, \mathbf{b}) = \{\alpha \mathbf{b} \mid \alpha \in \mathbb{F}_q^*\}$

Filtration Attack for GRS codes

Suppose that we know:

$$\mathcal{C}_k = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \quad \text{and} \quad \mathcal{C}_{k-1} = \mathrm{GRS}_{k-1}(\mathbf{a}, \mathbf{b})$$

Proposition: Assume that $2k - 1 \leq n - 2$

$\mathcal{C}_{k-2} = \mathrm{GRS}_{k-2}(\mathbf{a}, \mathbf{b})$ is the solution space of the following problem

$$\mathbf{c} \in \mathcal{C}_{k-1} \quad \text{and } \mathbf{c} * \mathcal{C}_k \subseteq (\mathcal{C}_{k-1})^2$$

In this way we build the following filtration

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \supseteq \mathrm{GRS}_{k-1}(\mathbf{a}, \mathbf{b}) \supseteq \mathrm{GRS}_{k-2}(\mathbf{a}, \mathbf{b}) \supseteq \cdots \supseteq \mathrm{GRS}_1(\mathbf{a}, \mathbf{b})$$

Note that: $\mathrm{GRS}_1(\mathbf{a}, \mathbf{b}) = \{\alpha \mathbf{b} \mid \alpha \in \mathbb{F}_q^*\}$

So we get the **column multiplier b**.

Filtration Attack for GRS codes

Suppose that we know:

$$\mathcal{C}_k = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \quad \text{and} \quad \mathcal{C}_{k-1} = \mathrm{GRS}_{k-1}(\mathbf{a}, \mathbf{b})$$

Proposition: Assume that $2k - 1 \leq n - 2$

$\mathcal{C}_{k-2} = \mathrm{GRS}_{k-2}(\mathbf{a}, \mathbf{b})$ is the solution space of the following problem

$$\mathbf{c} \in \mathcal{C}_{k-1} \quad \text{and } \mathbf{c} * \mathcal{C}_k \subseteq (\mathcal{C}_{k-1})^2$$

In this way we build the following filtration

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \supseteq \mathrm{GRS}_{k-1}(\mathbf{a}, \mathbf{b}) \supseteq \mathrm{GRS}_{k-2}(\mathbf{a}, \mathbf{b}) \supseteq \cdots \supseteq \mathrm{GRS}_1(\mathbf{a}, \mathbf{b})$$

Note that: $\mathrm{GRS}_1(\mathbf{a}, \mathbf{b}) = \{\alpha \mathbf{b} \mid \alpha \in \mathbb{F}_q^*\}$

So we get the **column multiplier b**. If **b** is known, **a** can be computed by **solving a linear system**.

Filtration Attack for GRS codes

1. Suppose that $\mathcal{C}_k = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is known.

Filtration Attack for GRS codes

1. Suppose that $\mathcal{C}_k = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is known.
2. **Shortening** at the **first position** (i.e. $S_1(\mathcal{C}_k)$) we get $\mathcal{C}'_{k-1} = \mathrm{GRS}_{k-1}(\mathbf{a}', \mathbf{b}')$ where

$$\mathbf{a}' = (a_2, \ldots, a_n) \quad \text{and} \quad \mathbf{b}' = (b'_2, \ldots, b'_n) \quad \text{with } b'_j = b_j(a_j - a_1)$$

Filtration Attack for GRS codes

1. Suppose that $\mathcal{C}_k = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is known.
2. **Shortening** at the **first position** (i.e. $S_1(\mathcal{C}_k)$) we get $\mathcal{C}'_{k-1} = \mathrm{GRS}_{k-1}(\mathbf{a}', \mathbf{b}')$ where

$$\mathbf{a}' = (a_2, \ldots, a_n) \quad \text{and} \quad \mathbf{b}' = (b'_2, \ldots, b'_n) \quad \text{with } b'_j = b_j(a_j - a_1)$$

It's easy to get a generator matrix of $S_1(\mathcal{C}_k)$

$$G = \begin{pmatrix} 1 & a_{12} & \ldots & a_{1n} \\ 0 & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{k2} & \ldots & a_{kn} \end{pmatrix}$$

Generator matrix for $\mathcal{C}_k$

Filtration Attack for GRS codes

1. Suppose that $\mathcal{C}_k = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is known.
2. **Shortening** at the **first position** (i.e. $S_1(\mathcal{C}_k)$) we get $\mathcal{C}'_{k-1} = \mathrm{GRS}_{k-1}(\mathbf{a}', \mathbf{b}')$ where

$$\mathbf{a}' = (a_2, \ldots, a_n) \quad \text{and} \quad \mathbf{b}' = (b'_2, \ldots, b'_n) \quad \text{with } b'_j = b_j(a_j - a_1)$$

It's easy to get a generator matrix of $S_1(\mathcal{C}_k)$

$$G = \begin{pmatrix} 1 & a_{12} & \ldots & a_{1n} \\ 0 & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{k2} & \ldots & a_{kn} \end{pmatrix}$$

Generator matrix for $S_1(\mathcal{C}_k)$

Generator matrix for $\mathcal{C}_k$

Filtration Attack for GRS codes

1. Suppose that $\mathcal{C}_k = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is known.
2. **Shortening** at the **first position** (i.e. $S_1(\mathcal{C}_k)$) we get $\mathcal{C}'_{k-1} = \mathrm{GRS}_{k-1}(\mathbf{a}', \mathbf{b}')$ where

$$\mathbf{a}' = (a_2, \ldots, a_n) \quad \text{and} \quad \mathbf{b}' = (b'_2, \ldots, b'_n) \quad \text{with } b'_j = b_j(a_j - a_1)$$

3. We can build the filtration:

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \supseteq \mathrm{GRS}_{k-1}(\mathbf{a}', \mathbf{b}') \supseteq \mathrm{GRS}_{k-2}(\mathbf{a}', \mathbf{b}') \supseteq \mathrm{GRS}_1(\mathbf{a}', \mathbf{b}')$$

Filtration Attack for GRS codes

1. Suppose that $\mathcal{C}_k = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is known.
2. **Shortening** at the **first position** (i.e. $S_1(\mathcal{C}_k)$) we get $\mathcal{C}'_{k-1} = \mathrm{GRS}_{k-1}(\mathbf{a}', \mathbf{b}')$ where

$$\mathbf{a}' = (a_2, \ldots, a_n) \quad \text{and} \quad \mathbf{b}' = (b'_2, \ldots, b'_n) \quad \text{with } b'_j = b_j(a_j - a_1)$$

3. We can build the filtration:

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \supseteq \mathrm{GRS}_{k-1}(\mathbf{a}', \mathbf{b}') \supseteq \mathrm{GRS}_{k-2}(\mathbf{a}', \mathbf{b}') \supseteq \mathrm{GRS}_1(\mathbf{a}', \mathbf{b}')$$

4. Se we get the column **multiplier** $\mathbf{b}'$ and the **support** $\mathbf{a}'$.

Filtration Attack for GRS codes

1. Suppose that $\mathcal{C}_k = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is known.
2. **Shortening** at the **first position** (i.e. $S_1(\mathcal{C}_k)$) we get $\mathcal{C}'_{k-1} = \mathrm{GRS}_{k-1}(\mathbf{a}', \mathbf{b}')$ where

$$\mathbf{a}' = (a_2, \ldots, a_n) \quad \text{and} \quad \mathbf{b}' = (b'_2, \ldots, b'_n) \quad \text{with } b'_j = b_j(a_j - a_1)$$

3. We can build the filtration:

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \supseteq \mathrm{GRS}_{k-1}(\mathbf{a}', \mathbf{b}') \supseteq \mathrm{GRS}_{k-2}(\mathbf{a}', \mathbf{b}') \supseteq \mathrm{GRS}_1(\mathbf{a}', \mathbf{b}')$$

4. Se we get the column **multiplier** $\mathbf{b}'$ and the **support** $\mathbf{a}'$.
5. Repeat the process **shortening** in another position to recover $\mathbf{a}$ completely.

Filtration Attack for GRS codes

Public Key: $\mathcal{K}_{\text{pub}} = \begin{cases} \text{a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \end{cases}$

The Algorithm: Assume that $2k - 1 \leq n - 2$

Filtration Attack for GRS codes

Public Key: $\mathcal{K}_{\text{pub}} = \begin{cases} \text{a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \end{cases}$

The Algorithm: Assume that $2k - 1 \leq n - 2$

1. Determine the code

$$S_1(\mathcal{C}_{pub}) = \text{GRS}_{k-1}(\mathbf{a}', \mathbf{b}')$$

Filtration Attack for GRS codes

Public Key: $\mathcal{K}_{\text{pub}} = \begin{cases} \text{a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \end{cases}$

The Algorithm: Assume that $2k - 1 \leq n - 2$

1. Determine the code

$$S_1(\mathcal{C}_{pub}) = \text{GRS}_{k-1}(\mathbf{a}', \mathbf{b}')$$

2. Build the filtration:

$$\underbrace{\text{GRS}_k(\mathbf{a}, \mathbf{b})}_{\mathcal{C}_{pub}} \supseteq \underbrace{\text{GRS}_{k-1}(\mathbf{a}', \mathbf{b}')}_{S_1(\mathcal{C}_{pub})} \supseteq \ldots \supseteq \text{GRS}_1(\mathbf{a}', \mathbf{b}')$$

Filtration Attack for GRS codes

Public Key: $\mathcal{K}_{\text{pub}} = \begin{cases} \text{a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \end{cases}$

The Algorithm: Assume that $2k - 1 \leq n - 2$

1. Determine the code

$$S_1(\mathcal{C}_{pub}) = \text{GRS}_{k-1}(\mathbf{a}', \mathbf{b}')$$

2. Build the filtration:

$$\underbrace{\text{GRS}_k(\mathbf{a}, \mathbf{b})}_{\mathcal{C}_{pub}} \supseteq \underbrace{\text{GRS}_{k-1}(\mathbf{a}', \mathbf{b}')}_{S_1(\mathcal{C}_{pub})} \supseteq \ldots \supseteq \text{GRS}_1(\mathbf{a}', \mathbf{b}')$$

3. Return $\mathbf{b}'$ and $\mathbf{a}'$

Another (Filtration) Attack - Retrieving an ECP

Proposition 1:

Let $\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d}) \implies \mathcal{C}^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp})$

Another (Filtration) Attack - Retrieving an ECP

Proposition 1:

Let $\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d}) \implies \mathcal{C}^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp})$

Then, $\mathcal{A} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{1})$ and $\mathcal{B} = \mathrm{GRS}_t(\mathbf{c}, \mathbf{d}^{\perp})$

is a t-ECP for $\mathcal{C}$ over $\mathbb{F}_q$

Another (Filtration) Attack - Retrieving an ECP

Proposition 1:

Let $\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d}) \implies \mathcal{C}^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp})$

Then, $\mathcal{A} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{1})$ and $\mathcal{B} = \mathrm{GRS}_t(\mathbf{c}, \mathbf{d}^{\perp})$

is a t-ECP for $\mathcal{C}$ over $\mathbb{F}_q$

Proposition 2: To compute a t-ECP for $\mathcal{C} = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ it suffise to compute a code of type $\mathcal{B} = \mathrm{GRS}_t(\mathbf{c}, \mathbf{d}^{\perp})$

If we know $\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d})$ and $\mathcal{B} = \mathrm{GRS}_t(\mathbf{c}, \mathbf{d}^{\perp})$

Another (Filtration) Attack - Retrieving an ECP

Proposition 1:

Let $\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d}) \implies \mathcal{C}^\perp = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^\perp)$

Then, $\mathcal{A} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{1})$ and $\mathcal{B} = \mathrm{GRS}_t(\mathbf{c}, \mathbf{d}^\perp)$

is a t-ECP for $\mathcal{C}$ over $\mathbb{F}_q$

Proposition 2: To compute a t-ECP for $\mathcal{C} = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ it suffise to compute a code of type $\mathcal{B} = \mathrm{GRS}_t(\mathbf{c}, \mathbf{d}^\perp)$

If we know $\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d})$ and $\mathcal{B} = \mathrm{GRS}_t(\mathbf{c}, \mathbf{d}^\perp)$

Then, $\mathcal{A} = \mathrm{GRS}_{t+1}(\mathbf{a}, \mathbf{1}) = \left(\mathcal{B} * \mathcal{C}\right)^\perp$

Another (Filtration) Attack - Retrieving an ECP

Public Key: $\mathcal{K}_{\text{pub}} = \begin{cases} \text{a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \end{cases}$

The Algorithm: Assume that $2k - 1 \leq n - 2$

Another (Filtration) Attack - Retrieving an ECP

Public Key: $\mathcal{K}_{\text{pub}} = \begin{cases} \text{a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \end{cases}$

The Algorithm: Assume that $2k - 1 \leq n - 2$

1. Determine the codes

$$\mathcal{C}_{pub}^{\perp} = \text{GRS}_{2t}(\mathbf{a}, \mathbf{b}^{\perp}) \quad \text{and} \quad S_1(\mathcal{C}_{pub}^{\perp}) = \text{GRS}_{2t-1}(\mathbf{a}', \sim \mathbf{b}^{\perp})$$

Another (Filtration) Attack - Retrieving an ECP

Public Key: $\mathcal{K}_{\text{pub}} = \begin{cases} \text{a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \end{cases}$

The Algorithm: Assume that $2k - 1 \leq n - 2$

1. Determine the codes

$$\mathcal{C}_{pub}^{\perp} = \text{GRS}_{2t}(\mathbf{a}, \mathbf{b}^{\perp}) \quad \text{and} \quad S_1(\mathcal{C}_{pub}^{\perp}) = \text{GRS}_{2t-1}(\mathbf{a}', \sim \mathbf{b}^{\perp})$$

2. Build the filtration:

$$\underbrace{\text{GRS}_{2t}(\mathbf{a}, \mathbf{b}^{\perp})}_{\mathcal{C}_{pub}^{\perp}} \supseteq \underbrace{\text{GRS}_{2t-1}(\mathbf{a}', \sim \mathbf{b}^{\perp})}_{S_1(\mathcal{C}_{pub}^{\perp})} \supseteq \ldots \supseteq \underbrace{\text{GRS}_{t}(\mathbf{a}', \sim \mathbf{b}^{\perp})}_{\mathcal{B}}$$

Another (Filtration) Attack - Retrieving an ECP

Public Key: $\mathcal{K}_{\text{pub}} = \begin{cases} \text{a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \end{cases}$

The Algorithm: Assume that $2k - 1 \leq n - 2$

1. Determine the codes

$$\mathcal{C}_{pub}^{\perp} = \text{GRS}_{2t}(\mathbf{a}, \mathbf{b}^{\perp}) \quad \text{and} \quad S_1(\mathcal{C}_{pub}^{\perp}) = \text{GRS}_{2t-1}(\mathbf{a}', \sim \mathbf{b}^{\perp})$$

2. Build the filtration:

$$\underbrace{\text{GRS}_{2t}(\mathbf{a}, \mathbf{b}^{\perp})}_{\mathcal{C}_{pub}^{\perp}} \supseteq \underbrace{\text{GRS}_{2t-1}(\mathbf{a}', \sim \mathbf{b}^{\perp})}_{S_1(\mathcal{C}_{pub}^{\perp})} \supseteq \ldots \supseteq \underbrace{\text{GRS}_{t}(\mathbf{a}', \sim \mathbf{b}^{\perp})}_{\mathcal{B}}$$

3. Return $(\mathcal{A}, \mathcal{B})$ which is an *ECP* for $S_1(\mathcal{C})$ where: $\mathcal{A} = (\mathcal{B} * S_1(\mathcal{C}))^{\perp}$

Another (Filtration) Attack - Retrieving an ECP

Public Key: $\mathcal{K}_{\text{pub}} = \begin{cases} \text{a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{and } t = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \end{cases}$

The Algorithm: Assume that $2k - 1 \leq n - 2$

1. Determine the codes

$$\mathcal{C}_{pub}^{\perp} = \text{GRS}_{2t}(\mathbf{a}, \mathbf{b}^{\perp}) \quad \text{and} \quad S_1(\mathcal{C}_{pub}^{\perp}) = \text{GRS}_{2t-1}(\mathbf{a}', \sim \mathbf{b}^{\perp})$$

2. Build the filtration:

$$\underbrace{\text{GRS}_{2t}(\mathbf{a}, \mathbf{b}^{\perp})}_{\mathcal{C}_{pub}^{\perp}} \supseteq \underbrace{\text{GRS}_{2t-1}(\mathbf{a}', \sim \mathbf{b}^{\perp})}_{S_1(\mathcal{C}_{pub}^{\perp})} \supseteq \ldots \supseteq \underbrace{\text{GRS}_{t}(\mathbf{a}', \sim \mathbf{b}^{\perp})}_{\mathcal{B}}$$

3. Return $(\mathcal{A}, \mathcal{B})$ which is an *ECP* for $S_1(\mathcal{C})$ where: $\mathcal{A} = (\mathcal{B} * S_1(\mathcal{C}))^{\perp}$
4. **Note that:** Correcting an error in the first position is not a difficult problem.

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