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
Distinguisher for Goppa codes

The generator matrix of a Goppa code looks random.
Distinguisher for Goppa codes

The generator matrix of a Goppa code looks random.

\[ \mathcal{K}_{\text{Goppa}} = \text{All generator matrices of a } [n, k]\text{-binary Goppa code} \]

**Goppa Code Distinguishing (GCD) problem**

**INPUT:** A matrix \( G \in \mathbb{F}_2^{k \times n} \)

**OUTPUT:** Is \( G \in \mathcal{K}_{\text{Goppa}} \)?

Difficult Problem
Distinguisher for Goppa codes

The generator matrix of a Goppa code looks random.

\[ \mathcal{K}_{\text{Goppa}} = \text{All generator matrices of a } [n, k]\text{-binary Goppa code} \]

**Goppa Code Distinguishing (GCD) problem**

**INPUT:** A matrix \( G \in \mathbb{F}_2^{k \times n} \)

**OUTPUT:** Is \( G \in \mathcal{K}_{\text{Goppa}} \)?

1. There exists an efficient distinguisher for **high-rate** codes.

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

*A Distinguisher for High-Rate McEliece Cryptosystems.*

The generator matrix of a Goppa code looks random.

\[ \mathcal{K}_{\text{Goppa}} = \text{All generator matrices of a } [n, k]\text{-binary Goppa code} \]

**Goppa Code Distinguishing (GCD) problem**

**INPUT:** A matrix \( G \in \mathbb{F}_2^{k \times n} \)

**OUTPUT:** Is \( G \in \mathcal{K}_{\text{Goppa}} \)?

1. There exists an efficient distinguisher for high-rate codes.
   
   J. . Faugère, V. Gauthier-Umana, A. Otmani, L. Perret and J. P. Tillich
   
   *A Distinguisher for High-Rate McEliece Cryptosystems.*
   

2. **General case:** best-known attacks are based on the support splitting algorithm and have exponential runtime.

   P. Loidreau, N. Sendrier
   
   *Weak keys in McEliece public-key cryptosystem.*

---

**Distinguisher for Goppa codes**
Distinguisher - Square Code - GRS codes

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

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

2. If $C$ is a GRS code

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

I. Márquez-Corbella, E. Martínez-Moro and R. Pellikaan.
*The non-gap sequence of a subcode of a generalized Reed-Solomon code.*

C. Wieschebrink.
*Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes.*
Proposition:

→ \( a \in \mathbb{F}_{q^m}^n \) with \( a_i \neq a_j \) for all \( i \neq j \)

→ \( b_1 \) and \( b_2 \) \( n \)-tuples of nonzero elements of \( \mathbb{F}_{q^m} \)

Then, there exists \( b_3 \in \mathbb{F}_{q^m}^n \) such that:

\[
\text{Alt}_r(a, b_1) \ast \text{Alt}_s(a, b_2) \subseteq \text{Alt}_{r+s-n+1}(a, b_3)
\]
Distinguisher - Square Code - Alternant codes

**Proposition:**

- \( a \in \mathbb{F}_{q^m}^n \) with \( a_i \neq a_j \) for all \( i \neq j \)
- \( b_1 \) and \( b_2 \) \( n \)-tuples of nonzero elements of \( \mathbb{F}_{q^m}^n \)

Then, there exists \( b_3 \in \mathbb{F}_{q^m}^n \) such that:

\[
\text{Alt}_r(a, b_1) \ast \text{Alt}_s(a, b_2) \subseteq \text{Alt}_{r+s-n+1}(a, b_3)
\]

**Proof:** Recall that \( \text{Alt}_r(a, b) \subseteq \text{GRS}_r(a, b) = \text{GRS}_{n-k}(a, b^\perp) \)

Let:

- \( c_1 \in \text{Alt}_r(a, b_1) \implies \exists f \in \mathbb{F}_q[X]_{<n-s} \) such that \( c_1 = b_1^\perp \ast f(a) \)
- \( c_2 \in \text{Alt}_r(a, b_2) \implies \exists g \in \mathbb{F}_q[X]_{<n-r} \) such that \( c_2 = b_2^\perp \ast g(a) \)

\[
c_1 \ast c_2 = b_1^\perp b_2^\perp \ast (fg)(a) \text{ with } \deg(fg) < 2n - (s + r) - 1
\]

Thus \( c_1 \ast c_2 \in \text{GRS}_{2n-(s+r)-1}(a, b_3^\perp) \cap \mathbb{F}_q^n = \text{Alt}_{s+r-n+1}(a, b_3^\perp) \)
Distinguisher - Square Code - Alternant codes

Thus, \((\text{Alt}_r(a, b))^{(2)} \subseteq \text{GRS}_{2(n-r)-1}(a, b^\perp)\)

To distinguish we need:

\[2(n - r) < n \implies r > \frac{n}{2}\]

However recall that

\[\dim(\text{Alt}_r(a, b)) = n - rm \geq 0 \implies r < \frac{n}{m} \leq \frac{n}{2} \text{ for all } m \geq 1\]

Distinguisher for Wild Goppa codes for \(m = 2\)

The square code of a shortened wild Goppa code of extension degree 2 has an abnormal dimension.

A. Couvreur, A. Otmani and J.P. Tillich
Polynomial Time Attack on Wild McEliece Over Quadratic Extensions.
Recent results against Wild Goppa codes

1. **Wild Goppa code with** $m = 2$
   
   A. Couvreur, A. Otmani and J.P. Tillich
   *Polynomial Time Attack on Wild McEliece Over Quadratic Extensions.*

2. **Some special cases of Wild McEliece Incognito.**
   
   J.C. Faugère, L. Perret and F. Portzamparc
   *Algebraic Attack against Variants of McEliece with Goppa Polynomial of a Special Form.*
Subcodes of GRS codes

New results in
Wild Goppa codes

(Broken)
Subcodes of AG codes

Subcodes of GRS codes

Reed Muller codes

Alternant codes

Goppa codes

GRS codes

Broken

Unbroken

Subcodes of GRS of small dimension (Unbroken)

New results in Wild Goppa codes (Broken)
Subcodes of AG codes

Subcodes of GRS codes

Goppa codes

GRS codes

Reed-Muller codes

Broken

Subcodes of GRS codes of small dimension (Unbroken)

New results in Wild Goppa codes (Broken)
Subcodes of GRS codes

Subcodes of AG codes

AG codes

GRS codes

Goppa codes

Alternant codes

Reed Muller codes

Broken

Unbroken

Subcodes of GRS codes of small dimension (Unbroken)

New results in Wild Goppa codes (Broken)
Subcodes of AG codes
Subcodes of GRS codes
Alternant codes
Goppa codes
Reed-Muller codes

New results in Wild Goppa codes (Broken)
Subcodes of GRS of small dimension (Unbroken)
Subcodes of AG codes
Subcodes of GRS codes
New results in Wild Goppa codes (Broken)
(Unbroken) Subcodes of GRS codes of small dimension
Reed-Muller codes
Goppa codes
Alternant codes
GRS codes
AG codes
Broken
Unbroken
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