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.

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

Goppa Code Distinguishing (GCD) problem Difficult Problem

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

OUTPUT: Is $G \in \mathcal{K}_{\text{Goppa}}$?

Distinguisher for Goppa codes

The generator matrix of a Goppa code looks random.

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

Goppa Code Distinguishing (GCD) problem Difficult 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.
IEEE Trans. Inf. Theory. 59(10), pp. 6830-6844, 2013.

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 Difficult 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.
   IEEE Trans. Inf. Theory. 59(10), pp. 6830-6844, 2013.

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 - Square Code - GRS codes

1. If $\mathcal{C}$ 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 $\mathcal{C}$ is a **GRS** code

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

I. Márquez-Corbella, E. Martínez-Moro and R. Pellikaan.
The non-gap sequence of a subcode of a generalized Reed-Solomon code.
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.
PQCrypto 2010, LNCS, volume 6061, 61-72, 2010.

Distinguisher - Square Code - Alternant codes

Proposition:

- $\mathbf{a} \in \mathbb{F}_{q^m}^n$ with $a_i \neq a_j$ for all $i \neq j$
- $\mathbf{b}_1$ and $\mathbf{b}_2$ n-tuples of nonzero elements of $\mathbb{F}_{q^m}$

Then, there exists $\mathbf{b}_3 \in \mathbb{F}_{q^m}^n$ such that:

$$\mathrm{Alt}_r(\mathbf{a}, \mathbf{b}_1) * \mathrm{Alt}_s(\mathbf{a}, \mathbf{b}_2) \subseteq \mathrm{Alt}_{r+s-n+1}(\mathbf{a}, \mathbf{b}_3)$$

Distinguisher - Square Code - Alternant codes

Proposition:

- $\mathbf{a} \in \mathbb{F}_{q^m}^n$ with $a_i \neq a_j$ for all $i \neq j$
- $\mathbf{b}_1$ and $\mathbf{b}_2$ n-tuples of nonzero elements of $\mathbb{F}_{q^m}$

Then, there exists $\mathbf{b}_3 \in \mathbb{F}_{q^m}^n$ such that:

$$\mathrm{Alt}_r(\mathbf{a}, \mathbf{b}_1) * \mathrm{Alt}_s(\mathbf{a}, \mathbf{b}_2) \subseteq \mathrm{Alt}_{r+s-n+1}(\mathbf{a}, \mathbf{b}_3)$$

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

Let:

$$\mathbf{c}_1 \in \mathrm{Alt}_r(\mathbf{a}, \mathbf{b}_1) \implies \exists f \in \mathbb{F}_q[X]_{<n-s} \text{ such that } \mathbf{c}_1 = \mathbf{b}_1^{\perp} * f(\mathbf{a})$$

$$\mathbf{c}_2 \in \mathrm{Alt}_r(\mathbf{a}, \mathbf{b}_2) \implies \exists g \in \mathbb{F}_q[X]_{<n-r} \text{ such that } \mathbf{c}_2 = \mathbf{b}_2^{\perp} * g(\mathbf{a})$$

$$\mathbf{c}_1 * \mathbf{c}_2 = \mathbf{b}_1^{\perp}\mathbf{b}_2^{\perp} * (fg)(\mathbf{a}) \text{ with } \deg(fg) < 2n - (s+r) - 1$$

Thus $\mathbf{c}_1 * \mathbf{c}_2 \in \mathrm{GRS}_{2n-(s+r)-1}(\mathbf{a}, \mathbf{b}_3^{\perp}) \cap \mathbb{F}_q^n = \mathrm{Alt}_{s+r-n+1}(\mathbf{a}, \mathbf{b}_3^{\perp})$

Distinguisher - Square Code - Alternant codes

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

To distinguish we need:

$$2(n-r) < n \Longrightarrow r > \frac{n}{2}$$

However recall that

$$\dim\left(\mathrm{Alt}_r(\mathbf{a}, \mathbf{b})\right) = n - rm \geq 0 \Longrightarrow r < \frac{n}{m} \leq \frac{n}{2} \text{ for all } m \geq 1$$

Distinguisher for Wild Goppa codes for $m = 2$

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

A. Couvreur, A. Otmani and J.P. Tillich
Polynomial Time Attack on Wild McEliece Over Quadratic Extensions.
EUROCRYPT 2014, 17—39.

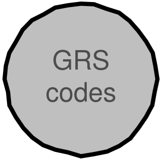
Recent results against Wild Goppa codes

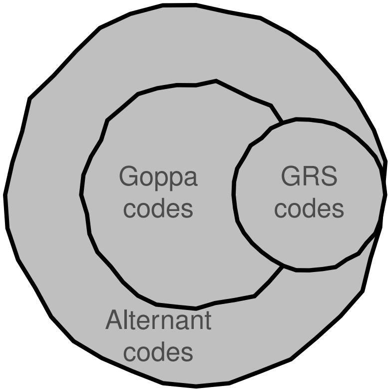
1. **Wild Goppa code** with $m = 2$

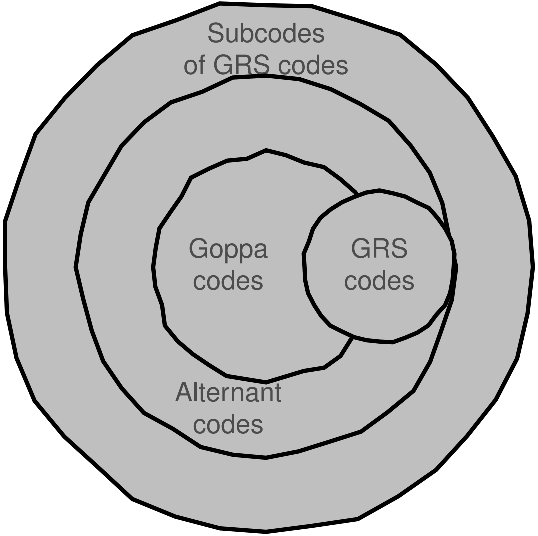
   A. Couvreur, A. Otmani and J.P. Tillich
   Polynomial Time Attack on Wild McEliece Over Quadratic Extensions.
   EUROCRYPT 2014, 17—39.

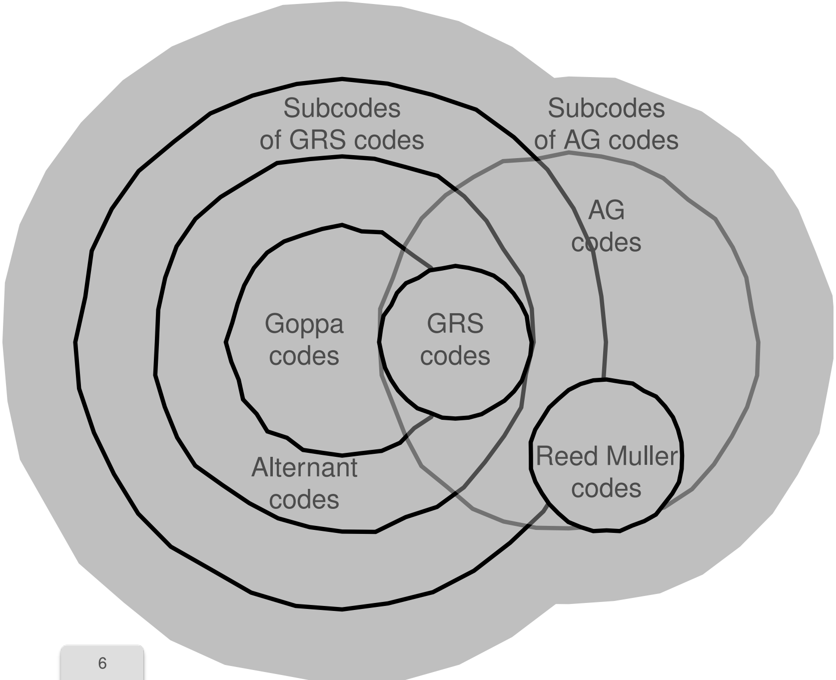
2. **Some special cases of Wild McEliece Incognito.**

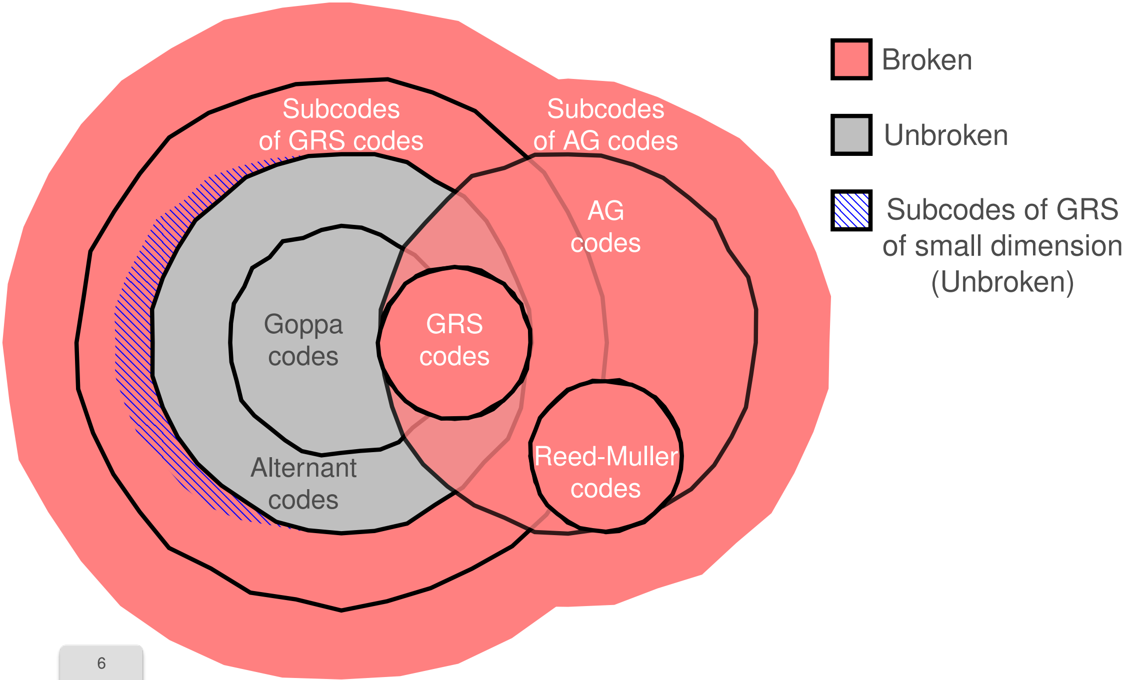
   J.C. Faugère, L. Perret and F. Portzamparc
   Algebraic Attack against Variants of McEliece with Goppa Polynomial of a Special Form.
   Asiacrypt 2014, LNCS, vol 8873, 21-41. 2014.

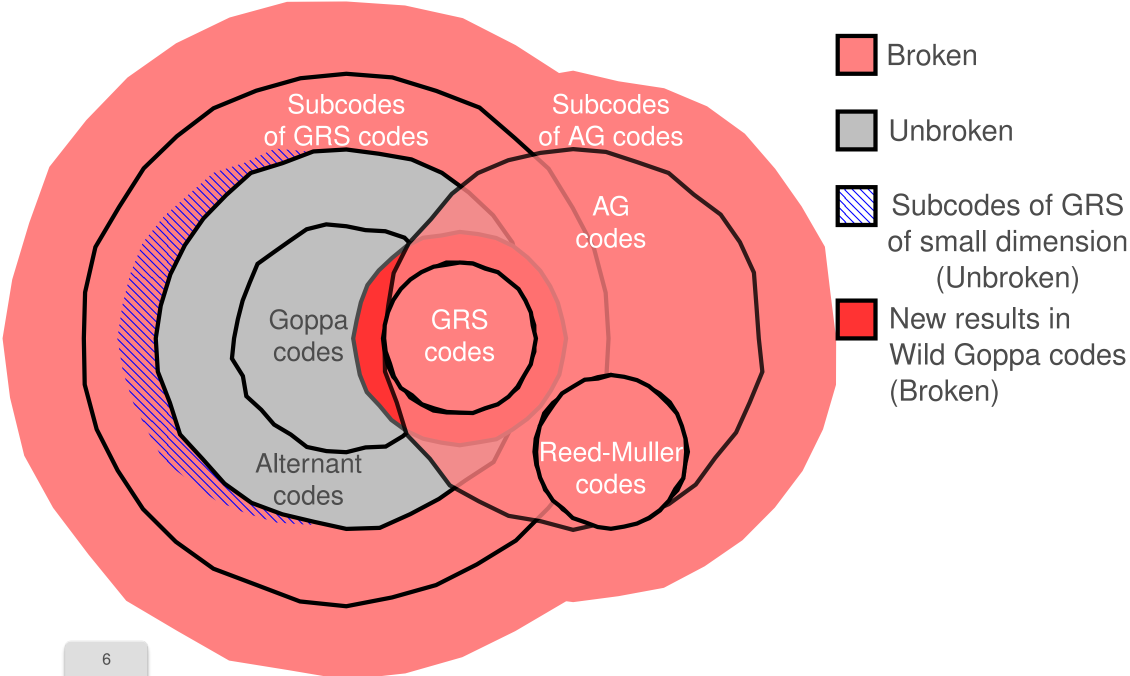

GRS
codes


Goppa
codes
GRS
codes
Alternant
codes


Subcodes
of GRS codes
Goppa
codes
GRS
codes
Alternant
codes


Subcodes
of GRS codes
Subcodes
of AG codes
AG
codes
Goppa
codes
GRS
codes
Reed Muller
codes
Alternant
codes


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


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

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**