Code-Based Cryptography

Key Attacks

I. Márquez-Corbella

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

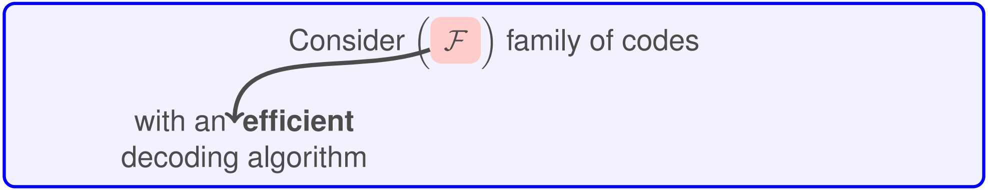
4. Key Attacks

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

The McEliece Cryptosystem

Consider $\left(\mathcal{F}\right)$ family of codes

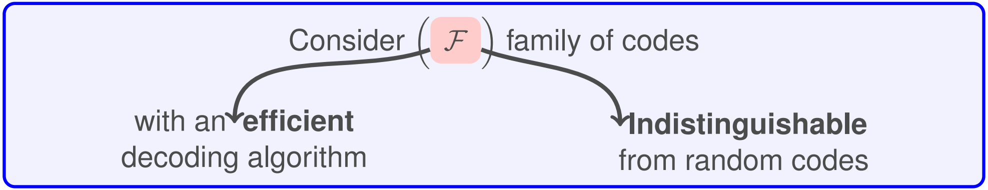
The McEliece Cryptosystem



Consider $\left(\mathcal{F}\right)$ family of codes

with an **efficient** decoding algorithm

The McEliece Cryptosystem

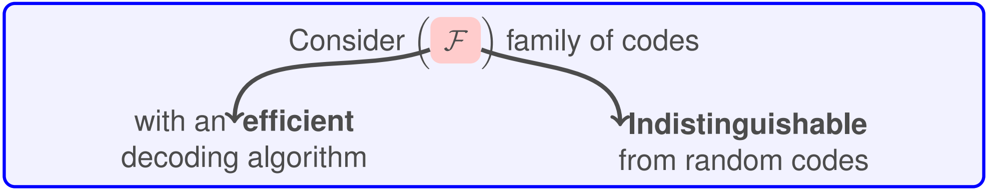


Consider $\left(\mathcal{F}\right)$ family of codes

with an **efficient** decoding algorithm

Indistinguishable from random codes

The McEliece Cryptosystem



Consider $(\mathcal{F})$ family of codes

with an **efficient** decoding algorithm

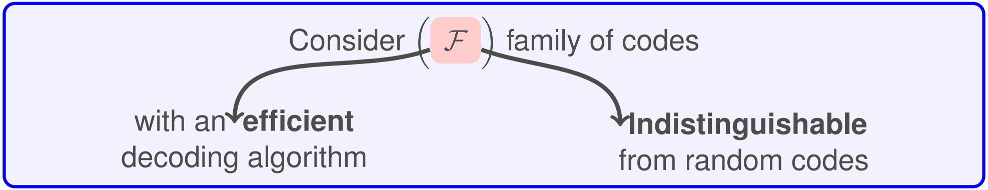
Indistinguishable from random codes

Key Generation Algorithm:

1. $G \in \mathbb{F}_q^{k \times n}$ a **generator matrix** for $\mathcal{C} \in \mathcal{F}$
2. $\mathcal{A}_{\mathcal{C}}$ an **“Efficient” decoding algorithm** for $\mathcal{C}$ which corrects up to t **errors**.

Public Key: $\mathcal{K}_{\text{pub}} = (G, t)$
Private Key: $\mathcal{K}_{\text{secret}} = (\mathcal{A}_{\mathcal{C}})$

The McEliece Cryptosystem



Consider $\mathcal{F}$ family of codes

with an **efficient** decoding algorithm

Indistinguishable from random codes

Key Generation Algorithm:

1. $G \in \mathbb{F}_q^{k \times n}$ a **generator matrix** for $\mathcal{C} \in \mathcal{F}$
2. $\mathcal{A}_{\mathcal{C}}$ an **“Efficient” decoding algorithm** for $\mathcal{C}$ which corrects up to t **errors**.

Public Key: $\mathcal{K}_{\text{pub}} = (G, t)$

Private Key: $\mathcal{K}_{\text{secret}} = (\mathcal{A}_{\mathcal{C}})$

Parameters	Key size	Security level
$[1024, 524, 101]_2$	67 ko	2^{62}
$[2048, 1608, 48]_2$	412 ko	2^{96}

The McEliece Cryptosystem

Encryption Algorithm:

Encrypt a message $\mathbf{m} \in \mathbb{F}_q^k$ as

$$\textsc{Encrypt}(\mathbf{m}) = \mathbf{m}G + \mathbf{e} = \mathbf{y}$$

where $\mathbf{e}$ is a random error vector of weight at most t.

The McEliece Cryptosystem

Encryption Algorithm:

Encrypt a message $\mathbf{m} \in \mathbb{F}_q^k$ as

$$\textsc{Encrypt}(\mathbf{m}) = \mathbf{m}G + \mathbf{e} = \mathbf{y}$$

where $\mathbf{e}$ is a random error vector of weight at most t.

Decryption Algorithm:

Using $\mathcal{K}_{secret}$, the receiver obtain $\mathbf{m}$.

$$\textsc{Decrypt}(\mathbf{y}) = \mathcal{A}_{\mathcal{C}}(\mathbf{y}) = \mathbf{m}$$

Which code Family? - GRS codes

➢ 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}

Which code Family? - GRS codes

➢ 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.

Which code Family? - Subcodes of GRS codes

- **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.

Which code Family? - Subcodes of GRS codes

➢ 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.

Which code Family? - Reed-Muller codes

Reed-Muller codes

V. Sidelnikov.
A public-key cryptosytem based on Reed-Muller codes.
Discrete Math. Appl., 4(3):191—207, 1994.

Parameters	Key size	Security level
$[1024, 176, 128]_2$	22.5 ko	2^{72}
$[2048, 232, 256]_2$	$59, 4$ ko	2^{93}

Which code Family? - Reed-Muller codes

➢ Reed-Muller codes

V. Sidelnikov.
A public-key cryptosytem based on Reed-Muller codes.
Discrete Math. Appl., 4(3):191—207, 1994.

Parameters	Key size	Security level
$[1024, 176, 128]_2$	22.5 ko	2^{72}
$[2048, 232, 256]_2$	59, 4 ko	2^{93}

✗ Attacks against this proposal:

L. Minder and A. Shokrollahi.
Cryptanalysis of the Sidelnikov cryptosystem.
In EUROCRYPT 2007, pages 347—360, 2007.

I. V. Chizhov, and M. A. Borodin.
The failure of McEliece PKC based on Reed-Muller codes.
IACR Cryptology ePrint Archive, 287, 2013.

Which code Family? - AG codes

Algebraic Geometry codes

H. Janwa and O. Moreno.
McEliece public crypto system using algebraic-geometric codes.
Designs, Codes and Cryptography, 1996.

Parameters	Key size	Security level
$[171, 109, 61]_{128}$	16 ko	2^{66}

Which code Family? - AG codes

➢ Algebraic Geometry codes

H. Janwa and O. Moreno.
McEliece public crypto system using algebraic-geometric codes.
Designs, Codes and Cryptography, 1996.

Parameters	Key size	Security level
$[171, 109, 61]_{128}$	16 ko	2^{66}

✗ Attacks against this proposal:

C. Faure and L. Minder.
Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes.
Proceedings 11th Int. Workshop on Algebraic and Combinatorial Coding Theory, 2008.

A. Couvreur, I. Márquez-Corbella and R. Pellikaan.
A polynomial time attack against Algebraic Geometry code based Public-Key Cryptosystems.
ISIT 2014, 1446—1450, 2014.

Which code Family? - Concatenated codes

➢ Concatenated codes

H. Niederreiter.
Knapsack-type cryptosystems and algebraic coding theory.
Problems of Control and Information Theory, 15(2):159—166, 1986.

Which code Family? - Concatenated codes

➢ Concatenated codes

H. Niederreiter.
Knapsack-type cryptosystems and algebraic coding theory.
Problems of Control and Information Theory, 15(2):159—166, 1986.

✗ Attack against this proposal:

N. Sendrier.
On the concatenated structure of a linear code.
AAECC, 9(3):221—242, 1998

Which code Family? - Convolutional codes

Convolutional codes

C. Löndahl and T. Johansson.
A new version of McEliece PKC based on convolutional codes.
ICICS, 15(2): 461-470, 2012.

Which code Family? - Convolutional codes

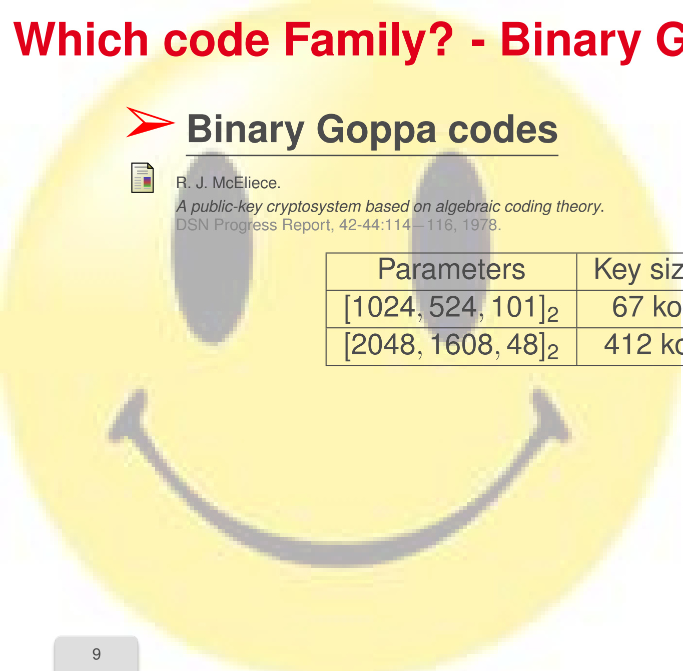
➢ Convolutional codes

C. Löndahl and T. Johansson.
A new version of McEliece PKC based on convolutional codes.
ICICS, 15(2): 461-470, 2012.

✗ Attack against this proposal:

G. Landais and J.P. Tillich
An efficient attack of a McEliece cryptosystem variant based on convolutional codes.
Post-Quantum Cryptography, LNCS, vol. 7932, 102-117, 2013.

Which code Family? - Binary Goppa codes



Binary Goppa codes

R. J. McEliece.
A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114—116, 1978.

Parameters	Key size	Security level
$[1024, 524, 101]_2$	67 ko	2^{62}
$[2048, 1608, 48]_2$	412 ko	2^{96}

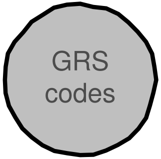
Which code Family? - Binary Goppa codes

➢ Binary Goppa codes

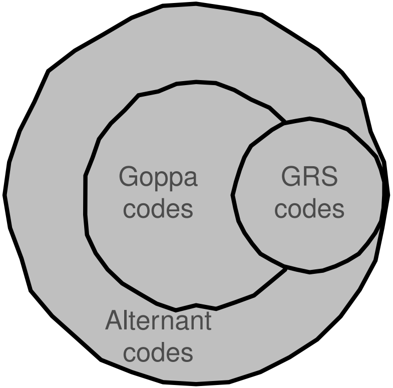
R. J. McEliece.
A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114—116, 1978.

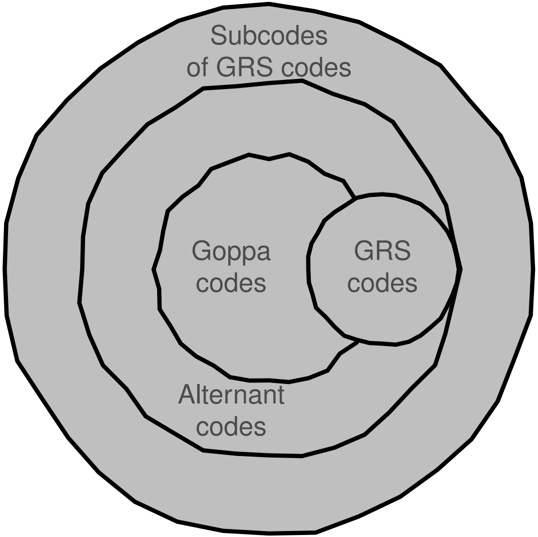
Parameters	Key size	Security level
$[1024, 524, 101]_2$	67 ko	2^{62}
$[2048, 1608, 48]_2$	412 ko	2^{96}

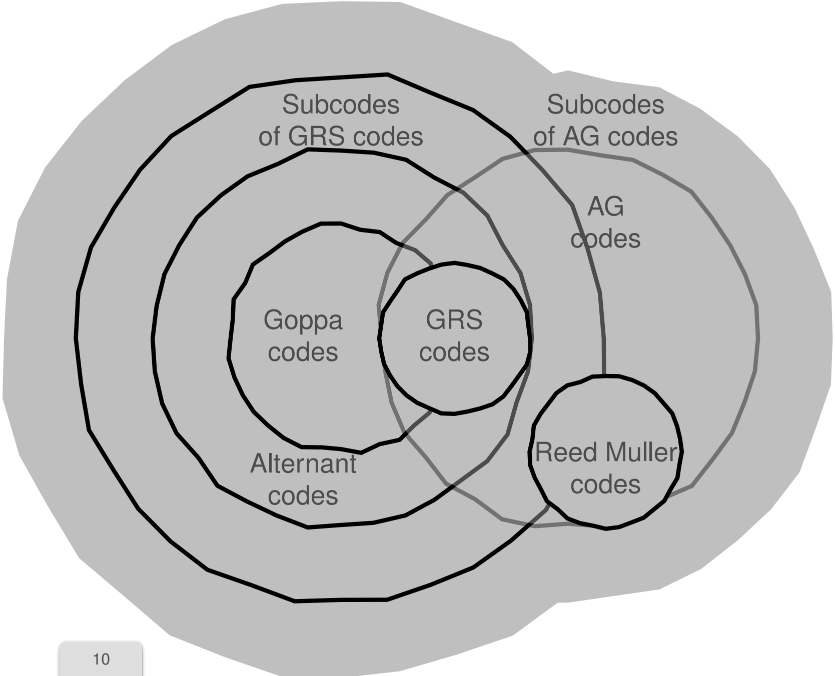
✔ **McEliece scheme with Goppa codes has resisted cryptanalysis so far!**

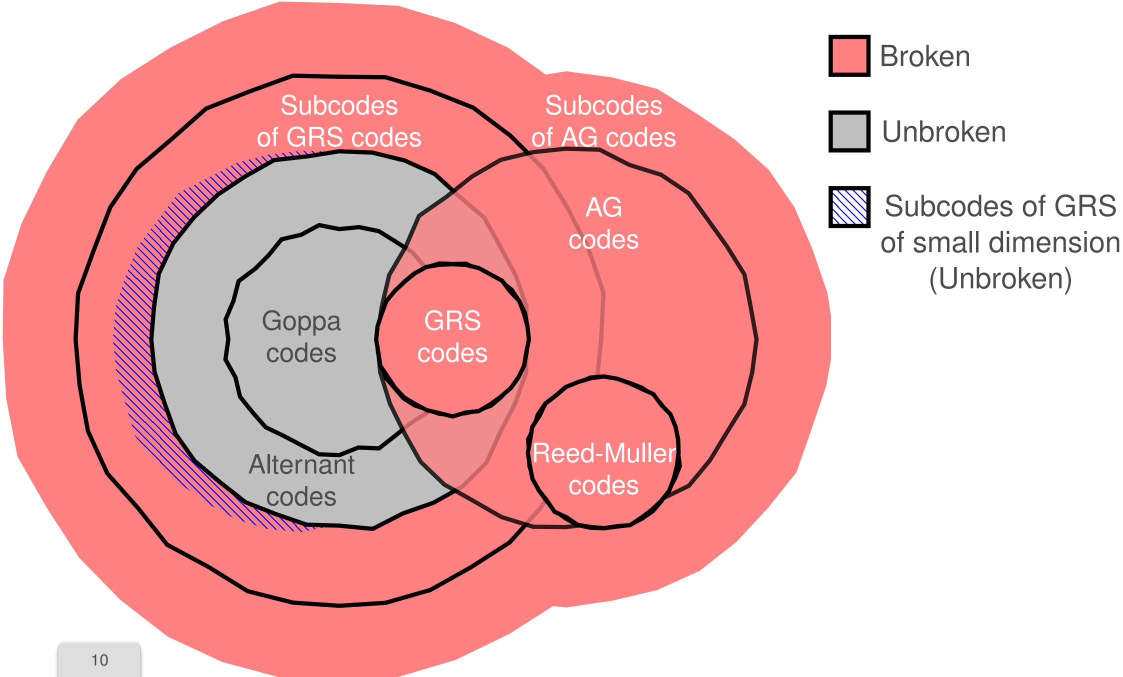


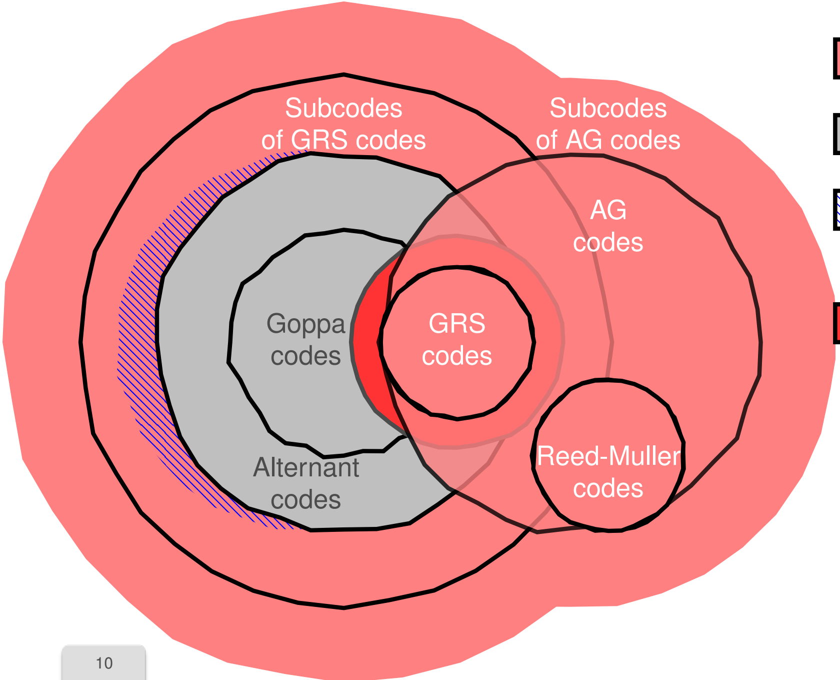
GRS codes


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
Alternant codes
Reed Muller 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)

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