CRYPTANALYSIS OF PUBLIC-KEY CRYPTOSYSTEMS THAT USE SUBCODES OF ALGEBRAIC GEOMETRY CODES

A. COUVREUR [1] I. MÁRQUEZ-CORBELLA [1] R. PELLIKAAN [2]

[1] INRIA, Saclay & LIX, CNRS UMR 7161, École Polytechnique

[2] Dept. of Mathematics and Computing Science, Eindhoven University of Technology

4th International Castle Meeting on Coding Theory and Applications

4ICMCTA

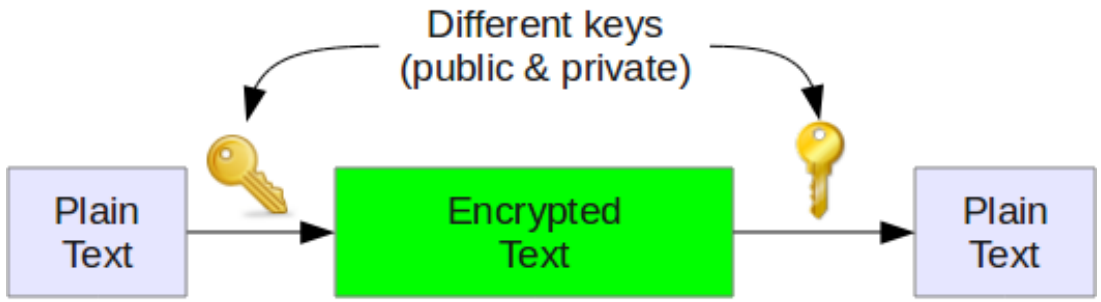
September 15-18, 2014

Public-Key Cryptosystems

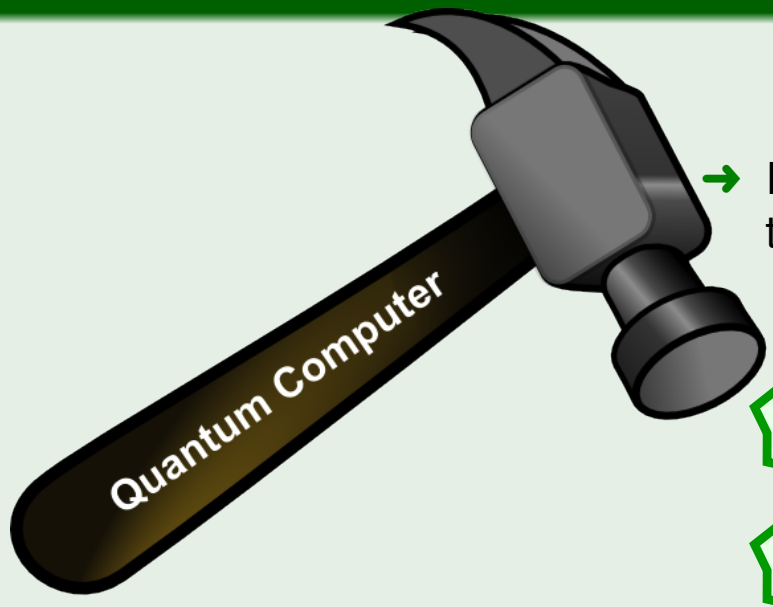
Most PKC are based on Number-theoretic problems

➜ It can be attacked in polynomial time using **Shor's algorithm**

Public-Key Cryptosystems



Most PKC are based on Number-theoretic problems



➜ It can be attacked in polynomial time using **Shor's algorithm**

RSA
DSA
ECDSA
HECC
ECC

McEliece cryptosystem

➜ McEliece introduced the first PKC based on Error-Correcting Codes in 1978.

Advantages:

1. Fast encryption (matrix-vector multiplication) and decryption functions.
2. Interesting candidate for post-quantum cryptography.

Drawback:

➢ Large key size.

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

McEliece cryptosystem

➜ McEliece introduced the first PKC based on Error-Correcting Codes in 1978.

Advantages:

1. Fast encryption (matrix-vector multiplication) and decryption functions.
2. Interesting candidate for post-quantum cryptography.

Drawback:

➢ Large key size.

R. J. McEliece.

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

McEliece cryptosystem

➜ McEliece introduced the first PKC based on Error-Correcting Codes in 1978.

Advantages:

1. Fast encryption (matrix-vector multiplication) and decryption functions.
2. Interesting candidate for post-quantum cryptography.

Drawback:

➢ Large key size.

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

McEliece cryptosystem

➜ McEliece introduced the first PKC based on Error-Correcting Codes in 1978.

Advantages:

1. Fast encryption (matrix-vector multiplication) and decryption functions.
2. Interesting candidate for post-quantum cryptography.

Drawback:

➢ Large key size.

R. J. McEliece.

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

McEliece Cryptosystem

➜ $t \in \mathbb{N}^* \implies$ **Error-correcting capacity** of $\mathcal{C}$

Consider any triplet:

$$\left(\mathcal{C}, \mathcal{A}_{\mathcal{C}}(t) \right)$$

➜ $[n,k]_q$ **linear code** with an efficient decoding algorithm

➠ Let G be a non structured generator matrix of $\mathcal{C}$.

➜ ***"Efficient"* decoding algorithm** for $\mathcal{C}$ which corrects up to t errors.

McEliece Cryptosystem

➜ $t \in \mathbb{N}^* \implies$ **Error-correcting capacity** of $\mathcal{C}$

Consider any triplet:

$$\left(\mathcal{C}, \mathcal{A}_{\mathcal{C}}(t) \right)$$

➜ $[n,k]_q$ **linear code** with an efficient decoding algorithm

➠ Let G be a non structured generator matrix of $\mathcal{C}$.

➜ ***"Efficient"* decoding algorithm** for $\mathcal{C}$ which corrects up to t errors.

McEliece Cryptosystem

➜ $t \in \mathbb{N}^* \implies$ **Error-correcting capacity** of $\mathcal{C}$

Consider any triplet:

$$\left(\mathcal{C}, \mathcal{A}_{\mathcal{C}}(t) \right)$$

➜ $[n, k]_q$ **linear code** with an efficient decoding algorithm

➠ Let G be a non structured generator matrix of $\mathcal{C}$.

➜ ***"Efficient"* decoding algorithm** for $\mathcal{C}$ which corrects up to t errors.

McEliece Cryptosystem

➜ $t \in \mathbb{N}^* \implies$ **Error-correcting capacity** of $\mathcal{C}$

Consider any triplet:

$$\left(\mathcal{C}, \quad \mathcal{A}_{\mathcal{C}}(t) \right)$$

➜ $[n, k]_q$ **linear code** with an efficient decoding algorithm

➠ Let G be a non structured generator matrix of $\mathcal{C}$.

➜ ***"Efficient"* decoding algorithm** for $\mathcal{C}$ which corrects up to t errors.

McEliece Cryptosystem

Key Generation

Given:

1. **McEliece Public Key:** $\mathcal{K}_{pub} = (G, t)$
2. **McEliece Private Key:** $\mathcal{K}_{secret} = (\mathcal{A}_{\mathcal{C}})$

Encryption

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

$$\mathbf{y} = \mathbf{m}G + \mathbf{e}$$

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

Decryption

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

McEliece Cryptosystem

Key Generation

Given:

1. **McEliece Public Key:** $\mathcal{K}_{pub} = (G, t)$
2. **McEliece Private Key:** $\mathcal{K}_{secret} = (\mathcal{A}_{\mathcal{C}})$

Encryption

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

$$\mathbf{y} = \mathbf{m}G + \mathbf{e}$$

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

Decryption

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

McEliece Cryptosystem

Key Generation

Given:

1. **McEliece Public Key:** $\mathcal{K}_{pub} = (G, t)$
2. **McEliece Private Key:** $\mathcal{K}_{secret} = (\mathcal{A}_C)$

Encryption

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

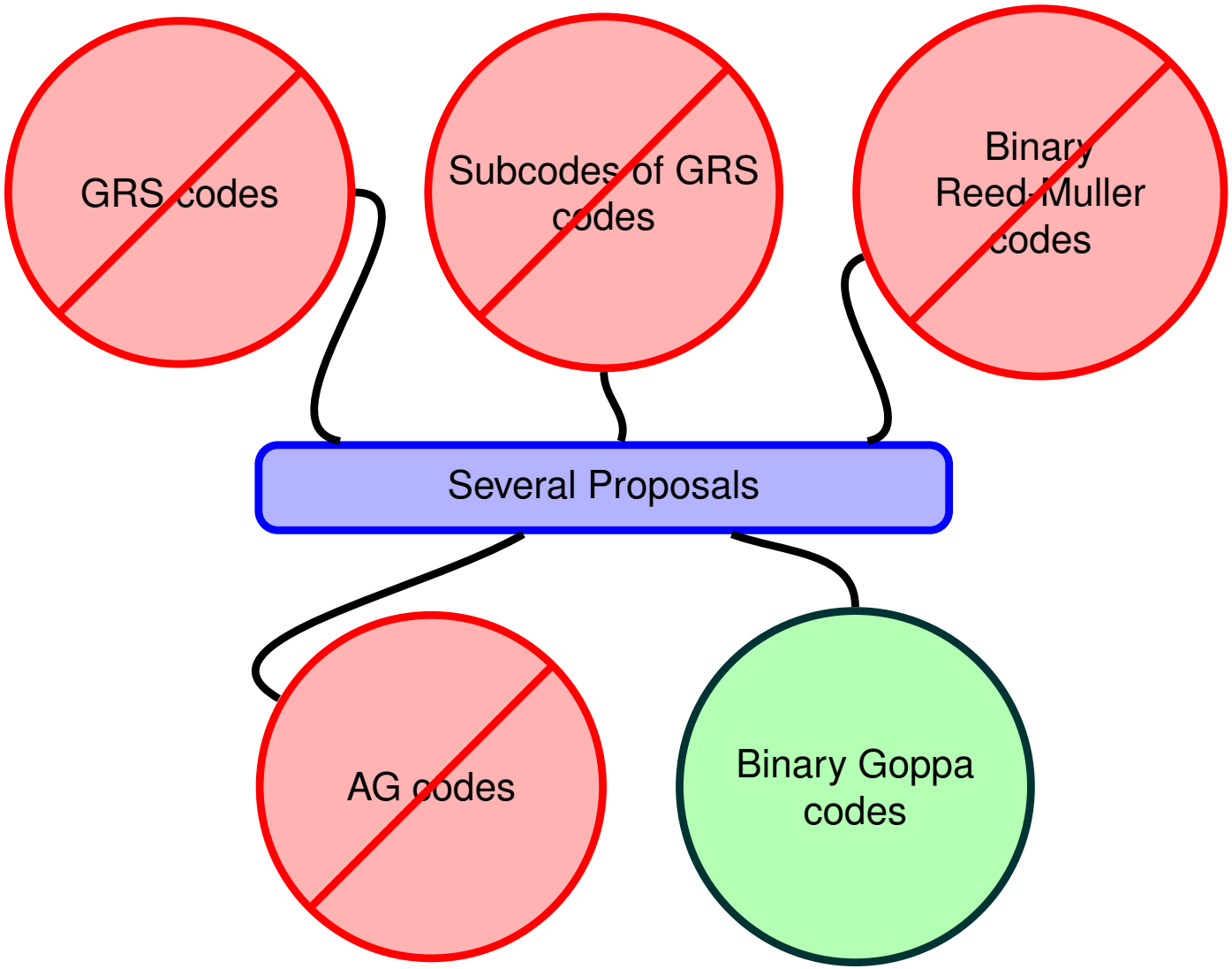
$$\mathbf{y} = \mathbf{m}G + \mathbf{e}$$

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

Decryption

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

Proposals



GRS codes

- The class of **GRS** codes was proposed by **Niederreiter** in 1986 for code-based PKC.
- **Sidelnikov-Shestakov** in 1992 introduced an algorithm that breaks this proposal in polynomial time.

Parameters	Key size	Security level
$[256, 128, 129]_{256}$	67 ko	2^{95}

Subcodes of GRS codes I

- **Berger and Loidreau** in 2005 propose another version of the Niederreiter scheme designed to resist the Sidelnikov-Shestakov attack.
  - **Main idea:** work with subcodes of the original GRS code.

- **Attacks:**
  - **Wieschebrink:** (2010)
    - Presents the first feasible attack to the Berger-Loidreau cryptosystem but is impractical for small subcodes.
    - Notes that if the square code of a subcode of a GRS code of parameters $[n, k]_q$ is itself a GRS code of dimension $2k - 1$ then we can apply Sidelnikov-Shestakov attack.
  - **M-Mártinez-Pellikaan:** (2012) Give a characterization of the possible parameters that should be used to avoid attacks on the Berger-Loidreau cryptosystem.

Subcodes of GRS codes II

- **Wieschebrick** (2010) and **Baldi et al.** (2011) proposed other variants of the Niederreiter scheme.

- **Attacks: Couvreur et al.** (2013) provide a cryptanalysis of these schemes.

Binary Reed-Muller codes

- The class of **Binary Reed-Muller** codes was proposed by **Sidelnikov** in 1994 for code-based PKC.
- **Minder-Shokrollahi** in 2007 presents a sub-exponential time attack.

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

AG codes

- In 1996 **Janwa and Moreno** propose to use AG codes for the McEliece cryptosystem.

- This system was broken for:

  1. Genus $g = 0$: by the **Sidelnikov-Shestakov** attack in 1992

     GRS codes are Algebraic Geometry codes on the projective line.

  2. Genus $g = 1$: by **Minder-Shokrollahi** in 2007.
  3. Genus $g \leq 2$: by **Faure-Minder** in 2008.
  4. Arbitrary genus by **Couvreur-M-Pellikaan** in 2014.
     We can retrieve the **model of the curve** (in polynomial time) by **M-Martínez-Pellikaan-Ruano** in 2013

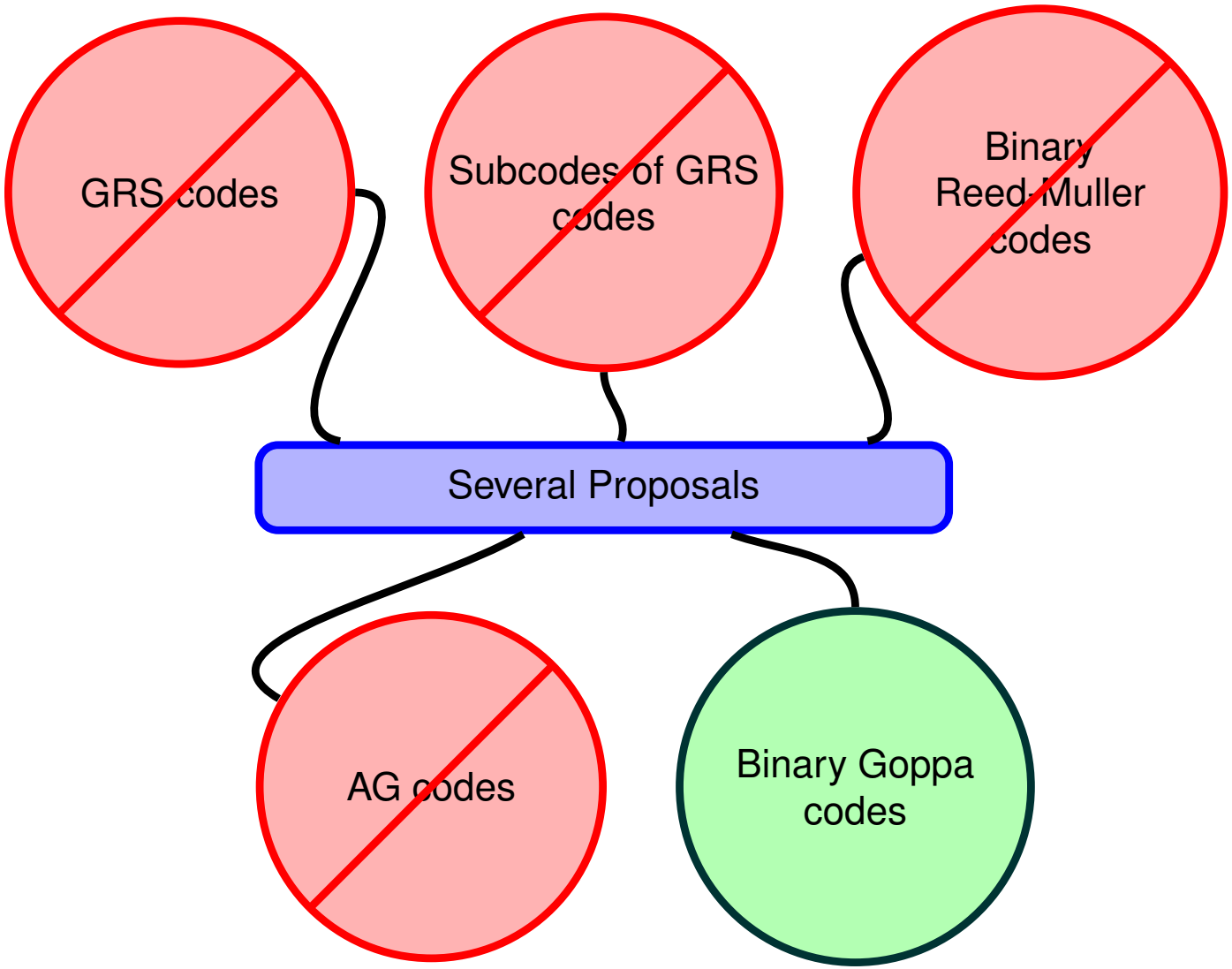
Parameters	Key size	Security level
$[171, 109, 61]_{128}$	16 ko	2^{66}

Binary Goppa codes

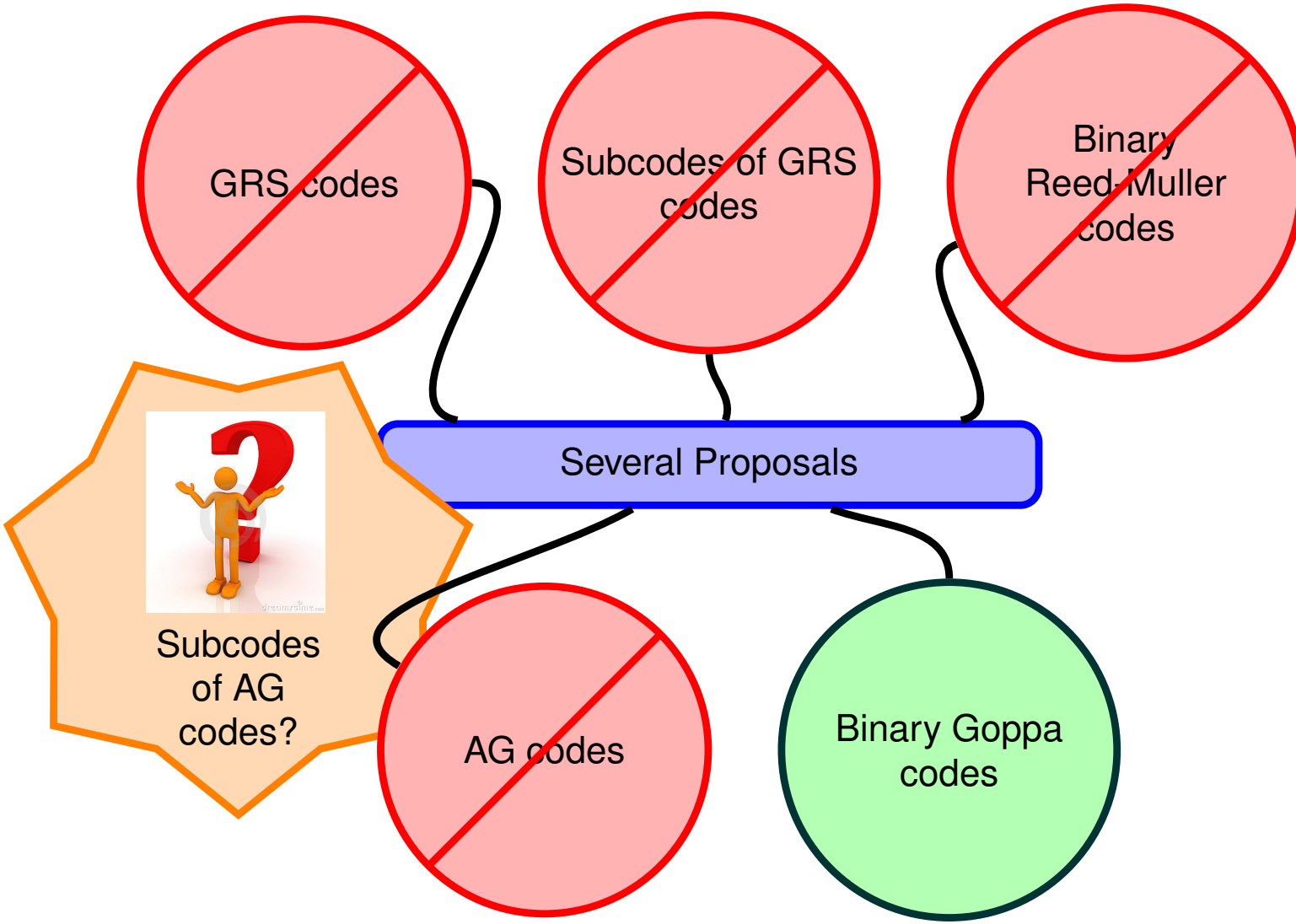
- The class of **binary goppa** codes was proposed by **McEliece** in 1977 for code-based PKC.
- ✔ McEliece with Goppa codes **has resisted cryptanalysis** so far!!

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

What about using subcodes of AG codes?



What about using subcodes of AG codes?



Algebraic Geometry codes

➜ An AG code is defined by a triplet

$$\left(\mathcal{X}, \mathcal{P}, E\right)$$

➜ $\mathcal{X}$ is an algebraic curve of genus g over the finite field $\mathbb{F}_q$

Algebraic Curve = Smooth, Projective and Geometrically Connected Curve

Whose defining equations are polynomials with coefficients in $\mathbb{F}_q$.

➜ $\mathcal{P} = (P_1, \ldots, P_n)$ is an n-tuple of mutually distinct $\mathbb{F}_q$-rational points of $\mathcal{X}$

$D_{\mathcal{P}}$ denotes the divisor $D_{\mathcal{P}} = P_1 + \cdots + P_n$

Algebraic Geometry codes

➜ An AG code is defined by a triplet

$$\left(\mathcal{X}, \mathcal{P}, E\right)$$

➜ $\mathcal{X}$ is an algebraic curve of genus g over the finite field $\mathbb{F}_q$

Algebraic Curve = Smooth, Projective and Geometrically Connected Curve

Whose defining equations are polynomials with coefficients in $\mathbb{F}_q$.

➜ $\mathcal{P} = (P_1, \ldots, P_n)$ is an n-tuple of mutually distinct $\mathbb{F}_q$-rational points of $\mathcal{X}$

$D_{\mathcal{P}}$ denotes the divisor $D_{\mathcal{P}} = P_1 + \cdots + P_n$

Algebraic Geometry codes I

- An AG code is defined by a triplet

$$\left(\mathcal{X}, \mathcal{P}, E\right)$$

- E is an $\mathbb{F}_q$-divisor of $\mathcal{X}$ such that

$$\mathrm{supp}(E) \cap \mathrm{supp}(D_{\mathcal{P}}) = \emptyset$$

Algebraic Geometry codes II

➜ Let us consider the triplet:

$$\left(\mathcal{X}, \mathcal{P}, E\right)$$

➜ $\mathcal{X}$ is an algebraic curve of genus g over the finite field $\mathbb{F}_q$.

➜ $\mathcal{P}$ is an n-tuple of distinct $\mathbb{F}_q$-rational points of $\mathcal{X}$.

➜ E is an $\mathbb{F}_q$-divisor of $\mathcal{X}$ such that $\operatorname{supp}(E) \cap \operatorname{supp}(D_{\mathcal{P}}) = \emptyset$

Since $\operatorname{supp}(E) \cap \operatorname{supp}(D_{\mathcal{P}}) = \emptyset$ the following **evaluation map** is well defined:

$$\begin{array}{rccc} \mathrm{ev}_{\mathcal{P}}: & L(E) & \longrightarrow & \mathbb{F}_q^n \\ & f & \longmapsto & \mathrm{ev}_P(f) = (f(P_1), \ldots, f(P_n)) \end{array}$$

Algebraic Geometry Code (AG code)

The **AG code** associated to the triplet $(\mathcal{X}, \mathcal{P}, E)$ is:

$$\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E) = \{\mathrm{ev}_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n)) \mid f \in L(E)\}$$

Algebraic Geometry codes III

➜ If $\{f_1, \ldots, f_k\}$ is a basis of $L(E)$ then

$$G = \begin{pmatrix} f_1(P_1) & \cdots & f_1(P_n) \\ \vdots & \ddots & \vdots \\ f_k(P_1) & \cdots & f_k(P_n) \end{pmatrix} \in \mathbb{F}_q^{k \times n}$$

is a **generator** matrix of the code $\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$

Theorem [Parameters of an AG code]

Let $\mathcal{C} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$. If $\deg(E) < n$ then

$$k(\mathcal{C}) \geq \deg(E) + 1 - g \quad \text{and} \quad d(\mathcal{C}) \geq n - \deg(E)$$

Moreover, if $n > \deg(E) > 2g - 2$ then $k(\mathcal{C}) = \deg(E) - g + 1$.

Dual of an AG code

Let:

- ω be a **differential form** with a simple pole and residue 1 at P_j for all $j = 1, \ldots, n$.
- K be the **canonical divisor** of ω.

Then

$$\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)^\perp = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E^\perp)$$

with $E^\perp = D_\mathcal{P} - E + K$ and $\deg(E^\perp) = n - \deg(E) + 2g - 2$

Theorem [Parameters of the dual of an AG code]

Let $\mathcal{C} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$. If $\deg(E) > 2g - 2$ then

$$k(\mathcal{C}^\perp) \geq n - \deg(E) - 1 + g \quad \text{and} \quad d(\mathcal{C}^\perp) \geq \deg(E) - 2g + 2$$

Moreover, if $n > \deg(E) > 2g - 2$ then $k(\mathcal{C}^\perp) = n - \deg(E) - 1 + g$

Schur Product

- For all $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ we define:
  - **Star Product:** $\mathbf{a} * \mathbf{b} = (a_1 b_1, \ldots, a_n b_n) \in \mathbb{F}_q^n$
  - **Standard Inner Product:** $\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=1}^{n} a_i b_i \in \mathbb{F}_q$

- For all subsets $A,\ B \subseteq \mathbb{F}_q^n$ we define:
  - $A * B = \langle \{ \mathbf{a} * \mathbf{b} \mid \mathbf{a} \in A \text{ and } \mathbf{b} \in B \} \rangle$
    For $B = A \Longrightarrow A * A$ is denoted as $A^{(2)}$
  - $A \perp B \iff \langle \mathbf{a}, \mathbf{b} \rangle = 0 \quad \forall\, \mathbf{a} \in A \text{ and } \mathbf{b} \in B$

Applications to Decoding - Decoding by Error Correcting Pairs

Let $\mathcal{C}$ be a linear code. We denote by:

- $k(\mathcal{C})$ = dimension of $\mathcal{C}$
- $d(\mathcal{C})$ = minimum distance of $\mathcal{C}$

Error-correcting pairs (ECP)

Let $\mathcal{C}$ be an $\mathbb{F}_q$ linear code of length n. The pair (A, B) of $\mathbb{F}_q$-linear codes of length n is a t-ECP for $\mathcal{C}$ over if the following properties hold:

- E.1 $(A * B) \perp \mathcal{C}$.
- E.2 $k(A) > t$.
- E.3 $d(B^{\perp}) > t$.
- E.4 $d(A) + d(\mathcal{C}) > n$.

An $[n, k]_q$ code which has a t-ECP over $\mathbb{F}_q$ has a decoding algorithm with complexity $\mathcal{O}\left(n^{\mathbf{w}}\right)$.

t-ECP for AG codes

➜ Consider the AG code

$$\mathcal{C} = \mathcal{C}_L\left(\mathcal{X}, \mathcal{P}, E\right)^{\perp}$$

Theorem [Pellikaan - 1992]

There always exists a t-ECP for $\mathcal{C}$ which correct up to

$$t^* = \underbrace{\left\lfloor \frac{d^*-1}{2} - \frac{g}{2} \right\rfloor}_{\substack{\text{half the} \\ \textbf{designed distance}} \; - \frac{g}{2}} \leq t = \underbrace{\left\lfloor \frac{d^*-1}{2} \right\rfloor}_{\substack{\text{Actual error-correction} \\ \text{capability of } \mathcal{C}}}$$

Using the concept of **Error-Correcting Arrays (ECA)** we can correct up to

$$t = \left\lfloor \frac{d^*-1}{2} \right\rfloor$$

Another application - Distinguisher and Cryptanalysis

Distinguisher: The square of an AG code is **very small** compared to that of a random code of the same dimension!

Recent Attacks:

"Take advantage of this distinguiser to compute a filtration of the public code"

- Alternative attack on GRS codes in 2014 by **Couvreur-Gaborit-GauthierUmaña-Otmani-Tillich**
- Key recovery attack on Wild Goppa codes over quadratic extensions in 2014 by **Couvreur-Otmani-Tillich**
- Attack on AG codes in 2014 by **Couvreur-M-Pellikaan**

GRS CODE

Let:

- $\mathbf{a} = (a_1, \ldots, a_n)$ be an n-tuple of **mutually distinct** elements of $\mathbb{F}_q$
- $\mathbf{b} = (b_1, \ldots, b_n)$ be an n-tuple of **nonzero** elements of $\mathbb{F}_q$
- $k \in \mathbb{N} \quad : \quad k < n$

The **GRS code** $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is defined by:

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) := \{\mathbf{b} * f(\mathbf{a}) = (b_1 f(a_1), \ldots, b_n f(a_n) \mid f \in \mathbb{F}_q[\mathbf{X}]_{<k})\}$$

THE CASE OF GRS CODES

- ➜ Using subcodes of GRS codes was proposed by **Berger-Loidreau** in 2005.
- ✖ This proposal was broken by **Wieschebrink** in 2010.

Public Key: $\mathcal{K}_{\text{pub}} := \mathcal{C} \subseteq \underbrace{\text{GRS}_k(\mathbf{a}, \mathbf{b})}_{\text{Secret}}$

The Algorithm:

STEP 1 Compute $\mathcal{C}^{(2)}$.

With **High Probability**:

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

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

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

THE t-CLOSURE OPERATION

Let:

- $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a code
- $t \geq 0$ be an integer

t-CLOSURE OF $\mathcal{C}$

$$\overline{\mathcal{C}}^t := \left\{ \mathbf{a} \in \mathbb{F}_q^n \mid a * \mathcal{C}^{(t-1)} \subseteq \mathcal{C}^{(t)} \right\}$$

$$\mathcal{C} \text{ is } t-\text{closed} \iff \overline{\mathcal{C}}^t = \mathcal{C}$$

THE t-CLOSURE OPERATION

PROPOSITION 2:

Let E be a divisor with $\deg(E) \geq 2g+1$

1. $\mathcal{C}_L(\mathcal{X},\mathcal{P},E)^{(t)} = \mathcal{C}_L(\mathcal{X},\mathcal{P},tE)$
2. If $\deg(E) \leq \dfrac{n-2}{t}$:

$$\overline{\mathcal{C}_L(\mathcal{X},\mathcal{P},E)}^{t} = \mathcal{C}_L(\mathcal{X},\mathcal{P},E)$$

COROLLARY 1:

Let E be a divisor such that $2g+1 \leq \deg(E) \leq \dfrac{n-2}{2}$

Then:

$$\overline{\mathcal{C}_L(\mathcal{X},\mathcal{P},E)}^{2} = \mathcal{C}_L(\mathcal{X},P,E)$$

The t-closure operation

Proposition 2:

Let E be a divisor with $\deg(E) \geq 2g+1$

1. $\mathcal{C}_L(\mathcal{X},\mathcal{P},E)^{(t)} = \mathcal{C}_L(\mathcal{X},\mathcal{P},tE)$
2. If $\deg(E) \leq \frac{n-2}{t}$:

$$\overline{\mathcal{C}_L(\mathcal{X},\mathcal{P},E)}^{t} = \mathcal{C}_L(\mathcal{X},\mathcal{P},E)$$

Corollary 1:

Let E be a divisor such that $2g+1 \leq \deg(E) \leq \frac{n-2}{2}$

Then:

$$\overline{\mathcal{C}_L(\mathcal{X},\mathcal{P},E)}^{2} = \mathcal{C}_L(\mathcal{X},P,E)$$

CONJECTURE:

Let $\mathcal{C}$ be a **subcode** of $\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$ such that:

$$\dim(\mathcal{C}) = l \quad \text{and} \quad \dim(\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)) = k = \deg(E) + 1 - g$$

If

$$2g + 1 \leq \deg(E) \leq \frac{n-2}{2} \quad \text{and} \quad 2k + 1 - g \leq \binom{l+1}{2}$$

Then:

$$\mathcal{C}^{(2)} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, 2E)$$

With High Probability!

COROLLARY 2:

Let $\mathcal{C}$ be a **subcode** of $\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$ such that:

$$\dim(\mathcal{C}) = l \quad \text{and} \quad \dim(\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)) = k = \deg(E) + 1 - g$$

If

$$2g + 1 \leq \deg(E) \leq \frac{n-2}{2} \quad \text{and} \quad 2k + 1 - g \leq \binom{l+1}{2}$$

Then:

$$\overline{\mathcal{C}}^2 = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$$

With High Probability!

Principle of the attack

Public Key:

$$\mathcal{K}_{\text{pub}} := \mathcal{C} \subseteq \underbrace{\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)}_{\text{Secret}} \quad \text{with } \dim(\mathcal{C}) = l \quad \text{and } t = \left\lfloor \frac{d^* - 1 - g}{2} \right\rfloor$$

The Algorithm: Assume that:

$$2g + 1 \leq \deg(E) \leq \frac{n-2}{2} \quad \text{and} \quad 2k + 1 - g \leq \binom{l+1}{2}$$

With **High Probability**: $\mathcal{C}^{(2)} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, 2E) \Longrightarrow \overline{\mathcal{C}}^2 = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$

Step 1: Compute $\overline{\mathcal{C}}^2$

Step 2: Appy the **Couvreur-M-Pellikaan** attack to recover an **Error-Correcting Pair** (A, B) for $\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$.

(A, B) is also an ECP for $\mathcal{C}$, thus:

➜**We obtain a decoding algorithm for $\mathcal{C}$.**

Example : Hermitian curves

Hermitian Curve

The **Hermitian curve** $\mathcal{H}_r$ over $\mathbb{F}_q$ with $q = r^2$ is defined by the affine equation

$$Y^r + Y = X^{r+1}$$

- This curve has $P_\infty = (0 : 1 : 0)$ as the only point at infinity.

Take:

- $E = mP_\infty$
- $\mathcal{P}$ be the $n = q\sqrt{q} = r^3$ affine $\mathbb{F}_q$-rational points of the curve.

The following tables consider different subcodes of type

$$\mathcal{C} \subseteq \mathcal{C}_L(\mathcal{H}_r, \mathcal{P}, E)^\perp \text{ with } n > \deg(E) > 2g - 2.$$

Example : Hermitian curves

q	n	k	t	Time	key size	**w**	l	L
7^2	343	193	54	80 s	83 ko	2^{30}	50	1000
					137 ko	2^{43}	100	1000
					163 ko	2^{62}	150	1000

q	n	k	t	Time	key size	**w**	l	L
9^2	729	521	19	30 min	216 ko	2^{32}	50	500
					670 ko	2^{121}	200	500
					835 ko	2^{178}	400	500

Table : Running times of the attack over Hermitian codes

w computed with Christiane Peters software

WHICH CODES ARE SUBJECT TO THIS ATTACK?

The subcode $\mathcal{C} \subseteq \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$ should satisfy:

$$\binom{\dim(\mathcal{C})+1}{2} \geq \dim \mathcal{C}_L(\mathcal{X}, \mathcal{P}, 2E) \quad \text{and} \quad 2g+1 \leq \leq \deg E \leq \frac{n-2}{2}$$

- ➜ In general is satisfied
- ➜ Can be relaxed by using **shortening** trick
- ➜ Otherwise $\mathcal{C}$ will behave like a **random code**

Let $\mathcal{C} \subseteq \underbrace{\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)}_{\dim(*)=k} : \binom{\dim \mathcal{C}+1}{2} \leq \dim \mathcal{C}_L(\mathcal{X}, \mathcal{P}, 2E)$

$$\Longrightarrow \dim \mathcal{C} \leq \sqrt{2k} \quad \textbf{(Small Subcodes)}$$

- ➜ Loss of efficiency
- ➜ Can be subject to **generic attacks** (like ISD)

WHICH CODES ARE SUBJECT TO THIS ATTACK?

The subcode $\mathcal{C} \subseteq \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$ should satisfy:

$$\binom{\dim(\mathcal{C})+1}{2} \geq \dim \mathcal{C}_L(\mathcal{X}, \mathcal{P}, 2E) \quad \text{and} \quad 2g+1 \leq \leq \deg E \leq \frac{n-2}{2}$$

- ➜ In general is satisfied
- ➜ Can be relaxed by using **shortening** trick
- ➜ Otherwise $\mathcal{C}$ will behave like a **random code**

Let $\mathcal{C} \subseteq \underbrace{\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)}_{\dim(*)=k} : \binom{\dim \mathcal{C}+1}{2} \leq \dim \mathcal{C}_L(\mathcal{X}, \mathcal{P}, 2E)$

$$\Longrightarrow \dim \mathcal{C} \leq \sqrt{2k} \quad \textbf{(Small Subcodes)}$$

- ➜ Loss of efficiency
- ➜ Can be subject to **generic attacks** (like ISD)

Which codes are subject to this attack?

The subcode $\mathcal{C} \subseteq \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$ should satisfy:

$$\binom{\dim(\mathcal{C})+1}{2} \geq \dim \mathcal{C}_L(\mathcal{X}, \mathcal{P}, 2E) \quad \text{and} \quad 2g+1 \leq \leq \deg E \leq \frac{n-2}{2}$$

- ➜ In general is satisfied
- ➜ Can be relaxed by using **shortening** trick
- ➜ Otherwise $\mathcal{C}$ will behave like a **random code**

Let $\mathcal{C} \subseteq \underbrace{\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)}_{\dim(*)=k} : \binom{\dim \mathcal{C}+1}{2} \leq \dim \mathcal{C}_L(\mathcal{X}, \mathcal{P}, 2E)$

$$\Longrightarrow \dim \mathcal{C} \leq \sqrt{2k} \quad \text{(Small Subcodes)}$$

- ➜ Loss of efficiency
- ➜ Can be subject to **generic attacks** (like ISD)

Which codes are subject to this attack?

The subcode $\mathcal{C} \subseteq \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$ should satisfy:

$$\binom{\dim(\mathcal{C})+1}{2} \geq \dim \mathcal{C}_L(\mathcal{X}, \mathcal{P}, 2E) \quad \text{and} \quad 2g+1 \leq \leq \deg E \leq \frac{n-2}{2}$$

- ➜ In general is satisfied
- ➜ Can be relaxed by using **shortening** trick
- ➜ Otherwise $\mathcal{C}$ will behave like a **random code**

Let $\mathcal{C} \subseteq \underbrace{\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)}_{\dim(*)=k}$: $\binom{\dim \mathcal{C}+1}{2} \leq \dim \mathcal{C}_L(\mathcal{X}, \mathcal{P}, 2E)$

$$\Longrightarrow \dim \mathcal{C} \leq \sqrt{2k} \quad \textbf{(Small Subcodes)}$$

- ➜ Loss of efficiency
- ➜ Can be subject to **generic attacks** (like ISD)

Which codes are subject to this attack?

The subcode $\mathcal{C} \subseteq \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$ should satisfy:

$$\binom{\dim(\mathcal{C})+1}{2} \geq \dim \mathcal{C}_L(\mathcal{X}, \mathcal{P}, 2E) \quad \text{and} \quad 2g+1 \leq \leq \deg E \leq \frac{n-2}{2}$$

- ➜ In general is satisfied
- ➜ Can be relaxed by using **shortening** trick
- ➜ Otherwise $\mathcal{C}$ will behave like a **random code**

Let $\mathcal{C} \subseteq \underbrace{\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)}_{\dim(*)=k} : \binom{\dim \mathcal{C}+1}{2} \leq \dim \mathcal{C}_L(\mathcal{X}, \mathcal{P}, 2E)$

$$\Longrightarrow \dim \mathcal{C} \leq \sqrt{2k} \quad \textbf{(Small Subcodes)}$$

- ➜ Loss of efficiency
- ➜ Can be subject to **generic attacks** (like ISD)

WHICH CODES ARE SUBJECT TO THIS ATTACK?

The subcode $\mathcal{C} \subseteq \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$ should satisfy:

$$\binom{\dim(\mathcal{C})+1}{2} \geq \dim \mathcal{C}_L(\mathcal{X}, \mathcal{P}, 2E) \quad \text{and} \quad 2g-1 \leq \leq \deg E \leq \frac{n-2}{2}$$

- ➜ In general is satisfied
- ➜ Can be relaxed by using **shortening** trick
- ➜ Otherwise $\mathcal{C}$ will behave like a **random code**

Let $\mathcal{C} \subseteq \underbrace{\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)}_{\dim(*)=k} : \binom{\dim \mathcal{C}+1}{2} \leq \dim \mathcal{C}_L(\mathcal{X}, \mathcal{P}, 2E)$

$$\Longrightarrow \dim \mathcal{C} \leq \sqrt{2k} \quad \textbf{(Small Subcodes)}$$

- ➜ Loss of efficiency
- ➜ Can be subject to **generic attacks** (like ISD)

Conclusions: Subfield subcodes still resist!

Let

- ➜ $\mathbb{F}$ be a **proper subfield** of $\mathbb{F}_q$
  (assume q to be non prime)
- ➜ $\mathcal{C} := \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E) \cap \mathbb{F}^n$
  (apply a base field extension to have an $\mathbb{F}_q$-extension)

- ✖ $\mathcal{C}^{(2)} \subseteq \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)^{(2)} \cap \mathbb{F}_q^n$. Hence, **in general:** $\overline{\mathcal{C}}^2 \subsetneq \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)$

For this reason, **subfield subcodes** resist to this kind of attaks.

➜ **Genus zero case:** Subcodes of GRS resist to this attack.
Except Wild Goppa Codes over Quadratic Extensions.
(**Couvreur-Otmani-Tillich** - 2014.)

Thank you for your attention!