

CRYPTANALYSIS OF GRS-BASED CRYPTOSYSTEMS USING THE SQUARE-CODE DISTINGUISHER

APPLICATION TO THE XGRS SCHEME

ALAIN COUVREUR¹ AND MATTHIEU LEQUESNE²

¹ LIX, ÉCOLE POLYTECHNIQUE
INRIA SACLAY, TEAM GRACE



² SORBONNE UNIVERSITÉ
INRIA PARIS, TEAM COSMIQ



SÉMINAIRE DE CRYPTOGRAPHIE DE RENNES, FEBRUARY 7, 2020

ALL YOU EVER WANTED TO KNOW ABOUT CODE-BASED CRYPTO

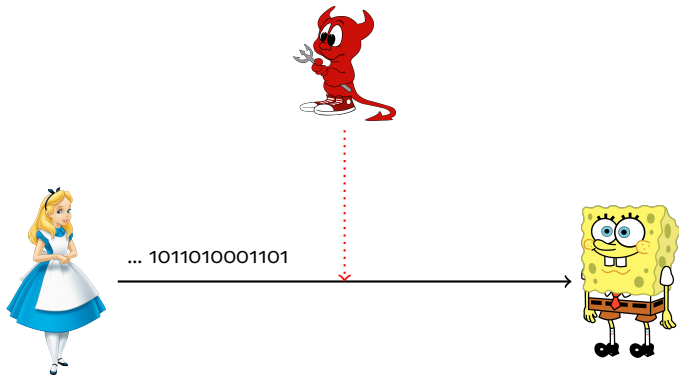
PUBLIC KEY CRYPTOGRAPHY



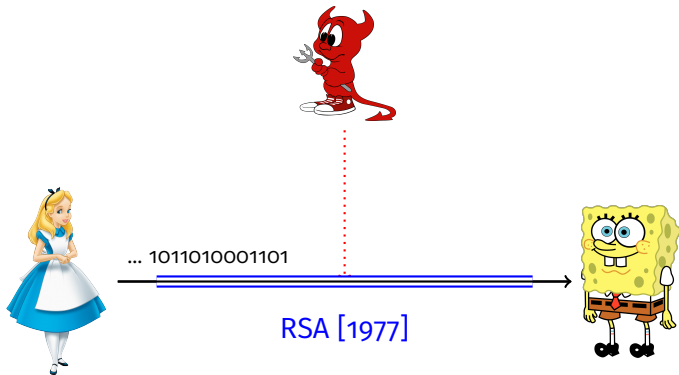
... 1011010001101



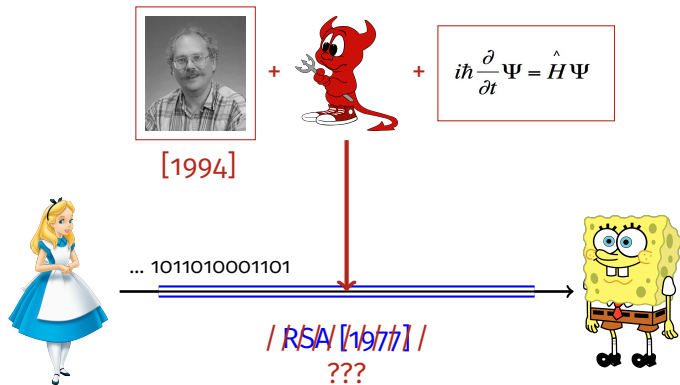
PUBLIC KEY CRYPTOGRAPHY



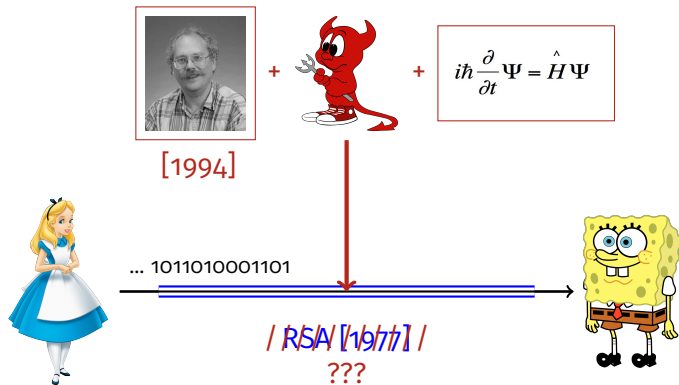
PUBLIC KEY CRYPTOGRAPHY



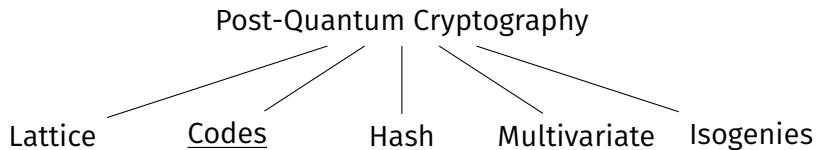
PUBLIC KEY CRYPTOGRAPHY

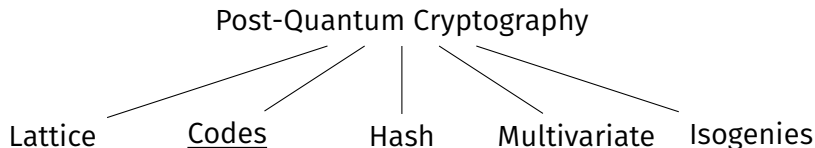


PUBLIC KEY CRYPTOGRAPHY



NIST





1978, Robert McEliece: [McE78]

A Public-Key Cryptosystem Based On Algebraic Coding Theory

R. J. McEliece
Communications Systems Research Section

Using the fact that a fast decoding algorithm exists for a general Goppa code, while no such exists for a general linear code, we construct a public-key cryptosystem which appears quite secure while at the same time allowing extremely rapid data rates. This kind of cryptosystem is ideal for use in multi-user communication networks, such as those envisioned by NASA for the distribution of space-acquired data



Definition (Code)

An $[n, k]_{\mathbb{F}_q}$ linear **code** \mathcal{C} is a linear subspace of \mathbb{F}_q^n of dimension k .

Definition (Decoder)

A **decoder** for the code \mathcal{C} is a function

$$\Phi_{\mathcal{C}} : \mathbb{F}_q^n \rightarrow \mathcal{C} \cup \{?\}.$$

We say that $\Phi_{\mathcal{C}}$ can decode up to t errors if

$$\forall \mathbf{c} \in \mathcal{C}, \forall \mathbf{e} \in \mathbb{F}_q^n, \quad |\mathbf{e}| \leq t \quad \Rightarrow \quad \Phi_{\mathcal{C}}(\mathbf{c} + \mathbf{e}) = \mathbf{c}.$$

Definition (Generator matrix)

A **generator matrix** of a code \mathcal{C} is a matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ such that:

$$\mathcal{C} = \{\mathbf{xG} \mid \mathbf{x} \in \mathbb{F}_q^k\}.$$

Definition (Parity-check matrix)

A **parity-check matrix** of a code \mathcal{C} is a matrix $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$ such that:

$$\mathcal{C} = \{\mathbf{y} \in \mathbb{F}_q^n \mid \mathbf{Hy}^T = \mathbf{0}\}.$$

Example (Repetition Code)

$$\begin{array}{lcl} \mathbb{F}_2 & \rightarrow & \mathbb{F}_2^3 \\ 0 & \mapsto & (0,0,0) \\ 1 & \mapsto & (1,1,1) \end{array}$$

Example (Decoder)

```
if |x| <= 1:
    return 0
else:
    return 1
```

Example (Repetition Code)

$$\begin{array}{lcl} \mathbb{F}_2 & \rightarrow & \mathbb{F}_2^3 \\ 0 & \mapsto & (0,0,0) \\ 1 & \mapsto & (1,1,1) \end{array}$$

$$G = (1 \ 1 \ 1)$$

Example (Decoder)

```
if |x| <= 1:
    return 0
else:
    return 1
```

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$


Main idea: how hard is it to decode up to t errors?

Main idea: how hard is it to decode up to t errors?


- For a random code



Main idea: how hard is it to decode up to t errors?

- For a random code 
- For some special families of structured codes 

Main idea: how hard is it to decode up to t errors?

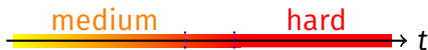
- For a random code 
- For some special families of structured codes 

easy = in polynomial time (with trap)

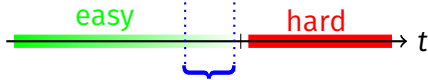
medium / **hard** = requires exponential time

Main idea: how hard is it to decode up to t errors?

- For a random code



- For some special families of structured codes



easy = in polynomial time (with trap)

medium / **hard** = requires exponential time

HOW TO DESIGN A CODE-BASED CRYPTOSYSTEM?

HOW TO DESIGN A CODE-BASED CRYPTOSYSTEM?

Ingredients:

- a family \mathcal{F} of structured codes;

HOW TO DESIGN A CODE-BASED CRYPTOSYSTEM?

Ingredients:

- a family \mathcal{F} of structured codes;
- a decoder $\Phi_{\mathcal{F}}$ that can correct efficiently up to t errors;

HOW TO DESIGN A CODE-BASED CRYPTOSYSTEM?

Ingredients:

- a family \mathcal{F} of structured codes;
- a decoder $\Phi_{\mathcal{F}}$ that can correct efficiently up to t errors;
- a shaker!



HOW TO DESIGN A CODE-BASED CRYPTOSYSTEM?

Ingredients:

- a family \mathcal{F} of structured codes;
- a decoder $\Phi_{\mathcal{F}}$ that can correct efficiently up to t errors;
- a shaker!



Recipe:

KeyGen()

$$\mathbf{G}_{\text{sk}} \xleftarrow{\$} \mathcal{F}$$
$$\mathbf{G}_{\text{pk}} \leftarrow \text{Shake}(\mathbf{G}_{\text{sk}})$$

Enc(m)

$$e \xleftarrow{\$} \mathbb{F}_q^n, \text{ s.t. } |e| = t$$
$$c \leftarrow m\mathbf{G}_{\text{pk}} + e$$

Dec(c)

$$m \leftarrow \Phi_{\mathcal{F}}(\mathbf{G}_{\text{sk}}, c)$$

HOW TO DESIGN A CODE-BASED CRYPTOSYSTEM?

Ingredients:

- a family \mathcal{F} of structured codes;
- a decoder $\Phi_{\mathcal{F}}$ that can correct efficiently up to t errors;
- a shaker!



Recipe:

KeyGen()

$$\mathbf{G}_{\text{sk}} \xleftarrow{\$} \mathcal{F}$$
$$\mathbf{G}_{\text{pk}} \leftarrow \text{Shake}(\mathbf{G}_{\text{sk}})$$

Enc(m)

$$e \xleftarrow{\$} \mathbb{F}_q^n, \text{ s.t. } |e| = t$$
$$c \leftarrow m\mathbf{G}_{\text{pk}} + e$$

Dec(c)

$$m \leftarrow \Phi_{\mathcal{F}}(\mathbf{G}_{\text{sk}}, c)$$

The key to success:

- choose t s.t. it is **hard** to decode t errors for a random code;

HOW TO DESIGN A CODE-BASED CRYPTOSYSTEM?

Ingredients:

- a family \mathcal{F} of structured codes;
- a decoder $\Phi_{\mathcal{F}}$ that can correct efficiently up to t errors;
- a shaker!



Recipe:

KeyGen()

$$\mathbf{G}_{\text{sk}} \xleftarrow{\$} \mathcal{F}$$
$$\mathbf{G}_{\text{pk}} \leftarrow \text{Shake}(\mathbf{G}_{\text{sk}})$$

Enc(m)

$$e \xleftarrow{\$} \mathbb{F}_q^n, \text{ s.t. } |e| = t$$
$$c \leftarrow m\mathbf{G}_{\text{pk}} + e$$

Dec(c)

$$m \leftarrow \Phi_{\mathcal{F}}(\mathbf{G}_{\text{sk}}, c)$$

The key to success:

- choose t s.t. it is **hard** to decode t errors for a random code;
- $\Phi_{\mathcal{F}}$ needs the structured version of the code to be efficient;

HOW TO DESIGN A CODE-BASED CRYPTOSYSTEM?

Ingredients:

- a family \mathcal{F} of structured codes;
- a decoder $\Phi_{\mathcal{F}}$ that can correct efficiently up to t errors;
- a shaker!



Recipe:

KeyGen()

$$\mathbf{G}_{\text{sk}} \xleftarrow{\$} \mathcal{F}$$
$$\mathbf{G}_{\text{pk}} \leftarrow \text{Shake}(\mathbf{G}_{\text{sk}})$$

Enc(m)

$$e \xleftarrow{\$} \mathbb{F}_q^n, \text{ s.t. } |e| = t$$
$$c \leftarrow m\mathbf{G}_{\text{pk}} + e$$

Dec(c)

$$m \leftarrow \Phi_{\mathcal{F}}(\mathbf{G}_{\text{sk}}, c)$$

The key to success:

- choose t s.t. it is **hard** to decode t errors for a random code;
- $\Phi_{\mathcal{F}}$ needs the structured version of the code to be efficient;
- the shaker shakes well enough!

How could Eve break this scheme? 2 possibilities:

1. Reconstruct \mathbf{G}_{sk} from \mathbf{G}_{pk} and then use $\Phi_{\mathcal{F}}$ to decode.

How could Eve break this scheme? 2 possibilities:

1. Reconstruct \mathbf{G}_{sk} from \mathbf{G}_{pk} and then use $\Phi_{\mathcal{F}}$ to decode.

Security hypothesis 1

\mathbf{G}_{pk} is indistinguishable from a random $k \times n$ matrix.

How could Eve break this scheme? 2 possibilities:

1. Reconstruct \mathbf{G}_{sk} from \mathbf{G}_{pk} and then use $\Phi_{\mathcal{F}}$ to decode.

Security hypothesis 1

\mathbf{G}_{pk} is indistinguishable from a random $k \times n$ matrix.

2. Decode using \mathbf{G}_{pk} .

SECURITY HYPOTHESIS

How could Eve break this scheme? 2 possibilities:

1. Reconstruct \mathbf{G}_{sk} from \mathbf{G}_{pk} and then use $\Phi_{\mathcal{F}}$ to decode.

Security hypothesis 1

\mathbf{G}_{pk} is indistinguishable from a random $k \times n$ matrix.

2. Decode using \mathbf{G}_{pk} .

Security hypothesis 2

Decoding t errors in a random $[n, k]$ -code is hard.

How could Eve break this scheme? 2 possibilities:

1. Reconstruct \mathbf{G}_{sk} from \mathbf{G}_{pk} and then use $\Phi_{\mathcal{F}}$ to decode.

Security hypothesis 1

\mathbf{G}_{pk} is indistinguishable from a random $k \times n$ matrix.

2. Decode using \mathbf{G}_{pk} .

Security hypothesis 2

Decoding t errors in a random $[n, k]$ -code is hard.

Remark: Hypothesis 1 depends on the choice of the family of codes \mathcal{F} and the shaker, while Hypothesis 2 is generic!

- Examples of choices of \mathcal{F} :
 - ▶ Goppa codes [Original McEliece];
 - ▶ QC-MDPC codes [BIKE];
 - ▶ Rank-based codes [ROLLO];
 - ▶ Generalised Reed Solomon codes (GRS).

SOME EXAMPLES

■ Examples of choices of \mathcal{F} :

- ▶ Goppa codes [Original McEliece];
- ▶ QC-MDPC codes [BIKE];
- ▶ Rank-based codes [ROLLO];
- ▶ **Generalised Reed Solomon codes (GRS).**

■ Examples of shakers:

- ▶ row scrambler;
- ▶ columns isometry (permutation);
- ▶ subfield subcode;
- ▶ adding random columns...



- ▶ Niederreiter's proposal [Nie86],

- ▶ Niederreiter's proposal [Nie86],
 - ▶ attack by Sidelnikov and Shestakov [SS92];

- ▶ Niederreiter's proposal [Nie86],
 - ▶ attack by Sidelnikov and Shestakov [SS92];
- ▶ Berger-Loidreau's cryptosystem [BL05],

- ▶ Niederreiter's proposal [Nie86],
 - ▶ attack by Sidelnikov and Shestakov [SS92];
- ▶ Berger-Loidreau's cryptosystem [BL05],
 - ▶ attack by Wieschebrink [Wie06, Wie09];

- ▶ Niederreiter's proposal [Nie86],
 - ▶ attack by Sidelnikov and Shestakov [SS92];
- ▶ Berger-Loidreau's cryptosystem [BL05],
 - ▶ attack by Wieschebrink [Wie06, Wie09];
- ▶ Wang's RLCE cryptosystem [Wan17], submitted to the NIST,

- ▶ Niederreiter's proposal [Nie86],
 - ▶ attack by Sidelnikov and Shestakov [SS92];
- ▶ Berger-Loidreau's cryptosystem [BL05],
 - ▶ attack by Wieschebrink [Wie06, Wie09];
- ▶ Wang's RLCE cryptosystem [Wan17], submitted to the NIST,
 - ▶ partial attack by Couvreur, L., Tillich [CLT19];

- ▶ Niederreiter's proposal [Nie86],
 - ▶ attack by Sidelnikov and Shestakov [SS92];
- ▶ Berger-Loidreau's cryptosystem [BL05],
 - ▶ attack by Wieschebrink [Wie06, Wie09];
- ▶ Wang's RLCE cryptosystem [Wan17], submitted to the NIST,
 - ▶ partial attack by Couvreur, L., Tillich [CLT19];
- ▶ New proposal: *"Encryption Scheme Based on Expanded Reed-Solomon Codes"* by Khathuria, Rosenthal and Weger,

- ▶ Niederreiter's proposal [Nie86],
 - ▶ attack by Sidelnikov and Shestakov [SS92];
- ▶ Berger-Loidreau's cryptosystem [BL05],
 - ▶ attack by Wieschebrink [Wie06, Wie09];
- ▶ Wang's RLCE cryptosystem [Wan17], submitted to the NIST,
 - ▶ partial attack by Couvreur, L., Tillich [CLT19];
- ▶ New proposal: *"Encryption Scheme Based on Expanded Reed-Solomon Codes"* by Khathuria, Rosenthal and Weger,
 - ▶ partial attack in this work.

THE XGRS CRYPTOSYSTEM (V1)

Definition (Generalised Reed Solomon codes)

The generalised Reed–Solomon (GRS) code with support \mathbf{x} and multiplier \mathbf{y} of dimension k is defined as

$$\mathbf{GRS}_k(\mathbf{x}, \mathbf{y}) \triangleq \{(y_1 f(x_1), \dots, y_n f(x_n)) \mid f \in \mathbb{F}_q[X]_{<k}\}.$$

Definition (Generalised Reed Solomon codes)

The generalised Reed–Solomon (GRS) code with support \mathbf{x} and multiplier \mathbf{y} of dimension k is defined as

$$\mathbf{GRS}_k(\mathbf{x}, \mathbf{y}) \triangleq \{(y_1 f(x_1), \dots, y_n f(x_n)) \mid f \in \mathbb{F}_q[X]_{<k}\}.$$

Sidelnikov Shestakov [SS92]

Given a generator matrix of a GRS code \mathcal{C} , it is possible to find \mathbf{x} and \mathbf{y} such that $\mathcal{C} = \mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$.

THE EXPANSION OPERATOR $\text{Exp}_{(\alpha,\beta)}$

Let (α, β) be an \mathbb{F}_q -base of \mathbb{F}_{q^2} . Denote $\phi_\alpha(\cdot)$, $\phi_\beta(\cdot)$ the projectors.

THE EXPANSION OPERATOR $\text{Exp}_{(\alpha,\beta)}$

Let (α, β) be an \mathbb{F}_q -base of \mathbb{F}_{q^2} . Denote $\phi_\alpha(\cdot)$, $\phi_\beta(\cdot)$ the projectors.

Definition

$$\begin{array}{ccc} & \mathbb{F}_{q^2}^{k \times n} & \rightarrow \\ & \begin{pmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,n} \\ \vdots & \vdots & & \vdots \\ m_{k,1} & m_{k,2} & \cdots & m_{k,n} \end{pmatrix} & \mapsto \\ & \mathbb{F}_q^{2k \times 2n} & \\ & \begin{pmatrix} \mathbf{M}_{1,1} & \mathbf{M}_{1,2} & \cdots & \mathbf{M}_{1,n} \\ \mathbf{M}_{2,1} & \mathbf{M}_{2,2} & \cdots & \mathbf{M}_{2,n} \\ \vdots & \vdots & & \vdots \\ \mathbf{M}_{k,1} & \mathbf{M}_{k,2} & \cdots & \mathbf{M}_{k,n} \end{pmatrix} & \end{array}$$

$$\text{where } \mathbf{M}_{i,j} \triangleq \begin{pmatrix} \phi_\alpha(\alpha m_{i,j}) & \phi_\alpha(\beta m_{i,j}) \\ \phi_\beta(\alpha m_{i,j}) & \phi_\beta(\beta m_{i,j}) \end{pmatrix} \in \mathbb{F}_q^{2 \times 2}.$$

Definition

For $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_{q^2}^n$, denote

$$\phi_{\alpha,\beta}^{(n)}(\mathbf{x}) \triangleq (\phi_{\alpha}(x_1), \phi_{\beta}(x_1), \dots, \phi_{\alpha}(x_n), \phi_{\beta}(x_n)) \in \mathbb{F}_q^{2n}.$$

PROPERTIES OF $\mathbf{Exp}_{(\alpha,\beta)}$

Definition

For $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_{q^2}^n$, denote

$$\phi_{\alpha,\beta}^{(n)}(\mathbf{x}) \triangleq (\phi_{\alpha}(x_1), \phi_{\beta}(x_1), \dots, \phi_{\alpha}(x_n), \phi_{\beta}(x_n)) \in \mathbb{F}_q^{2n}.$$

Proposition

Let \mathcal{C} be an $[n, k]$ -code over \mathbb{F}_{q^2} , \mathbf{G} a generator matrix and \mathbf{H} a parity-check matrix of \mathcal{C} . Then, for any \mathbb{F}_q -base (α, β) of \mathbb{F}_{q^2} :

- $\phi^{(n)}(\mathbf{x} \cdot \mathbf{G}) = \phi^{(k)}(\mathbf{x}) \cdot \mathbf{Exp}(\mathbf{G})$ for all $\mathbf{x} \in \mathbb{F}_{q^2}^k$;
- $\phi^{(n-k)}(\mathbf{H} \cdot \mathbf{y}^T) = \overline{\mathbf{Exp}(\mathbf{H})} \cdot \phi^{(n)}(\mathbf{y})^T$ for all $\mathbf{y} \in \mathbb{F}_{q^2}^n$,

where $\overline{\mathbf{Exp}(M)} \triangleq (\mathbf{Exp}(M^T))^T$.

PROPERTIES OF $\mathbf{Exp}_{(\alpha,\beta)}$

Let \mathcal{C} be an $[n, k]$ -code over \mathbb{F}_{q^2} .

Let $\hat{\mathcal{C}}$ be the code over \mathbb{F}_q defined by

$$\hat{\mathcal{C}} \triangleq \{\phi^{(n)}(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}\}.$$

Proposition

- $\mathbf{Exp}(\mathbf{G})$ is a generator matrix of $\hat{\mathcal{C}}$;
- $\overline{\mathbf{Exp}}(\mathbf{H})$ is a parity-check matrix of $\hat{\mathcal{C}}$,

where \mathbf{G} is a generator matrix and \mathbf{H} a parity-check matrix of \mathcal{C} .

KEY GENERATION

For parameters (q, n, k) :

- γ a primitive element of \mathbb{F}_{q^2} : $(\alpha, \beta) = (1, \gamma)$
- $\mathbf{G} \stackrel{\$}{\leftarrow} \mathbf{GRS}_{\mathbb{F}_{q^2}}(n, k) \in \mathbb{F}_{q^2}^{k \times n}$
- $t = \lfloor \frac{k}{2} \rfloor$ (error-correction capacity of \mathbf{G}^\perp)
- $\mathbf{S} \stackrel{\$}{\leftarrow} 2k \times 2k$ invertible matrix
- $\mathbf{P} \stackrel{\$}{\leftarrow} 2n \times 2n$ permutation matrix
- $\mathbf{G}_{pk} = \mathbf{S} \cdot (\mathbf{Exp}_{(1, \gamma)} \mathbf{G}) \cdot \mathbf{P}$

$$\begin{cases} \text{PublicKey} = & (\mathbf{G}_{pk}, t) \\ \text{SecretKey} = & (\gamma, \mathbf{G}, \mathbf{S}, \mathbf{P}). \end{cases}$$

KEY GENERATION

For parameters (q, n, k) :

- γ a primitive element of \mathbb{F}_{q^2} : $(\alpha, \beta) = (1, \gamma)$
- $\mathbf{G} \stackrel{\$}{\leftarrow} \mathbf{GRS}_{\mathbb{F}_{q^2}}(n, k) \in \mathbb{F}_{q^2}^{k \times n}$
- $t = \lfloor \frac{k}{2} \rfloor$ (error-correction capacity of \mathbf{G}^\perp)
- $\mathbf{S} \stackrel{\$}{\leftarrow} 2k \times 2k$ invertible matrix
- $\mathbf{P} \stackrel{\$}{\leftarrow} 2n \times 2n$ permutation matrix
- $\mathbf{G}_{pk} = \mathbf{S} \cdot (\mathbf{Exp}_{(1, \gamma)} \mathbf{G}) \cdot \mathbf{P}$

$$\begin{cases} \text{PublicKey} = (\mathbf{G}_{pk}, t) \\ \text{SecretKey} = (\gamma, \mathbf{G}, \mathbf{S}, \mathbf{P}). \end{cases}$$



ENCRYPTION / DECRYPTION (EASY VERSION)

Recall the generic recipe:

KeyGen()

$$\mathbf{G}_{\text{sk}} \xleftarrow{\$} \mathcal{F}$$

$$\mathbf{G}_{\text{pk}} \leftarrow \text{Shake}(\mathbf{G}_{\text{sk}})$$

Enc(m)

$$e \xleftarrow{\$} \mathbb{F}_q^n, \text{ s.t. } |e| = t$$

$$c \leftarrow m\mathbf{G}_{\text{pk}} + e$$

Dec(c)

$$m \leftarrow \Phi_{\mathcal{F}}(\mathbf{G}_{\text{sk}}, c)$$

ENCRYPTION / DECRYPTION (EASY VERSION)

Recall the generic recipe:

KeyGen()

$$\mathbf{G}_{\text{sk}} \xleftarrow{\$} \mathcal{F}$$

$$\mathbf{G}_{\text{pk}} \leftarrow \text{Shake}(\mathbf{G}_{\text{sk}})$$

Enc(m)

$$e \xleftarrow{\$} \mathbb{F}_q^n, \text{ s.t. } |e| = t$$

$$c \leftarrow m\mathbf{G}_{\text{pk}} + e$$

Dec(c)

$$m \leftarrow \Phi_{\mathcal{F}}(\mathbf{G}_{\text{sk}}, c)$$

XGRS:



=

expand matrix
+ scramble rows
+ permute columns.

ENCRYPTION / DECRYPTION (HARD VERSION)

Message space

$$\{\mathbf{m} \in \mathbb{F}_q^{2n}, |\mathbf{m}| \leq t\}.$$

ENCRYPTION / DECRYPTION (HARD VERSION)

Message space

$$\{\mathbf{m} \in \mathbb{F}_q^{2n}, |\mathbf{m}| \leq t\}.$$

Encryption

Enc($\mathbf{m}, \mathbf{G}_{pk}$):

- $\mathbf{c} = \mathbf{G}_{pk} \mathbf{m}^T$
- Return \mathbf{c} .

ENCRYPTION / DECRYPTION (HARD VERSION)

Message space

$$\{\mathbf{m} \in \mathbb{F}_q^{2n}, |\mathbf{m}| \leq t\}.$$

Encryption

Enc($\mathbf{m}, \mathbf{G}_{\text{pk}}$):

- $\mathbf{c} = \mathbf{G}_{\text{pk}} \mathbf{m}^T$
- Return \mathbf{c} .

Decryption

Dec($\mathbf{c}, \gamma, \mathbf{G}, \mathbf{S}, \mathbf{P}$):

- $\mathbf{c}' = \mathbf{S}^{-1} \mathbf{c}$
 $\mathbf{c}' = (\mathbf{Exp}_{(1,\gamma)} \mathbf{G}) \cdot (\mathbf{P} \cdot \mathbf{m}^T)$
- $\mathbf{c}'' = \phi_{(1,\gamma)}^{(-n)}(\mathbf{c}')$
 $\mathbf{c}'' = \mathbf{G} \cdot (\phi_{(1,\gamma)}^{(n)}(\mathbf{P} \cdot \mathbf{m}^T))^T$
- Find \mathbf{m}' (correcting t errors)
- Return $\mathbf{m} = \mathbf{P}^{-1} \cdot \phi_{(1,\gamma)}^{(n)}(\mathbf{m}')$.

- q a prime power ;
- n, k such that $0 \leq k \leq n \leq q^2$.

q	n	k	key size (Mb)
31	925	232	3.18

Figure: Parameters proposed for the scheme
(Classical McEliece key size = 8.37 Mb)



Definition (Schur product)

Schur product of vectors: $\mathbf{a} \star \mathbf{b} \triangleq (a_1 b_1, \dots, a_n b_n).$

Definition (Schur product)

Schur product of vectors: $\mathbf{a} \star \mathbf{b} \triangleq (a_1 b_1, \dots, a_n b_n)$.

Schur product of codes:

$$\mathcal{A} \star \mathcal{B} \triangleq \text{Span}_{\mathbb{F}_q} \{ \mathbf{a} \star \mathbf{b} \mid \mathbf{a} \in \mathcal{A}, \mathbf{b} \in \mathcal{B} \}.$$

Definition (Schur product)

Schur product of vectors: $\mathbf{a} \star \mathbf{b} \triangleq (a_1 b_1, \dots, a_n b_n)$.

Schur product of codes:

$$\mathcal{A} \star \mathcal{B} \triangleq \text{Span}_{\mathbb{F}_q} \{ \mathbf{a} \star \mathbf{b} \mid \mathbf{a} \in \mathcal{A}, \mathbf{b} \in \mathcal{B} \}.$$

Notation: $\mathcal{C}^{\star 2} \triangleq \mathcal{C} \star \mathcal{C}$.

Question

Given a code \mathcal{C} of dimension k , what is the value of $\dim \mathcal{C}^{*2}$?

Question

Given a code \mathcal{C} of dimension k , what is the value of $\dim \mathcal{C}^{*2}$?

Square-code Distinguisher

$$\mathcal{C} \text{ random} \quad \Rightarrow \quad \dim \mathcal{C}^{*2} = \binom{k+1}{2} = \frac{k(k+1)}{2}.$$

Question

Given a code \mathcal{C} of dimension k , what is the value of $\dim \mathcal{C}^{*2}$?

Square-code Distinguisher

$$\mathcal{C} \text{ random} \quad \Rightarrow \quad \dim \mathcal{C}^{*2} = \binom{k+1}{2} = \frac{k(k+1)}{2}.$$

$$\mathcal{C} = \mathbf{GRS}_k(\mathbf{x}, \mathbf{y}) \quad \Rightarrow \quad \dim \mathcal{C}^{*2} = 2k - 1.$$

Proof.

Let \mathbf{c} and $\mathbf{c}' \in \mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$.

$$\mathbf{c} = (y_1 p(x_1), \dots, y_n p(x_n)), \quad \mathbf{c}' = (y_1 q(x_1), \dots, y_n q(x_n))$$

where p and q are two **polynomials** of degree at most $k - 1$.

Proof.

Let \mathbf{c} and $\mathbf{c}' \in \mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$.

$$\mathbf{c} = (y_1 p(x_1), \dots, y_n p(x_n)), \quad \mathbf{c}' = (y_1 q(x_1), \dots, y_n q(x_n))$$

where p and q are two **polynomials** of degree at most $k - 1$.

$$\begin{aligned} \mathbf{c} \star \mathbf{c}' &= y_1^2 p(x_1) q(x_1), \dots, y_n^2 p(x_n) q(x_n) \\ &= y_1^2 r(x_1), \dots, y_n^2 r(x_n). \end{aligned}$$

where r is a **polynomial** of degree at most $2k - 2$.

THE TOOLS: SQUARE-CODE DISTINGUISHER

Proof.

Let \mathbf{c} and $\mathbf{c}' \in \mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$.

$$\mathbf{c} = (y_1 p(x_1), \dots, y_n p(x_n)), \quad \mathbf{c}' = (y_1 q(x_1), \dots, y_n q(x_n))$$

where p and q are two **polynomials** of degree at most $k - 1$.

$$\begin{aligned} \mathbf{c} \star \mathbf{c}' &= y_1^2 p(x_1) q(x_1), \dots, y_n^2 p(x_n) q(x_n) \\ &= y_1^2 r(x_1), \dots, y_n^2 r(x_n). \end{aligned}$$

where r is a **polynomial** of degree at most $2k - 2$.

Hence,

$$(\mathbf{GRS}_k(\mathbf{x}, \mathbf{y}))^{*2} = \mathbf{GRS}_{2k-1}(\mathbf{x}, \mathbf{y} \star \mathbf{y}).$$

□

Square-code Distinguisher

\mathcal{C} a code of length n and dimension k .

$$\mathcal{C} \text{ random} \quad \Rightarrow \quad \dim \mathcal{C}^{*2} = \frac{k(k+1)}{2}.$$

$$\mathcal{C} = \mathbf{GRS}_k(\mathbf{x}, \mathbf{y}) \quad \Rightarrow \quad \dim \mathcal{C}^{*2} = 2k - 1.$$

Square-code Distinguisher

\mathcal{C} a code of length n and dimension k . **DIMENSION \leq LENGTH.**

$$\mathcal{C} \text{ random} \quad \Rightarrow \quad \dim \mathcal{C}^{*2} = \min \left(\frac{k(k+1)}{2}, n \right).$$

$$\mathcal{C} = \mathbf{GRS}_k(\mathbf{x}, \mathbf{y}) \quad \Rightarrow \quad \dim \mathcal{C}^{*2} = \min(2k - 1, n).$$

Square-code Distinguisher

\mathcal{C} a code of length n and dimension k . **DIMENSION \leq LENGTH.**

$$\mathcal{C} \text{ random} \quad \Rightarrow \quad \dim \mathcal{C}^{*2} = \min\left(\frac{k(k+1)}{2}, n\right).$$

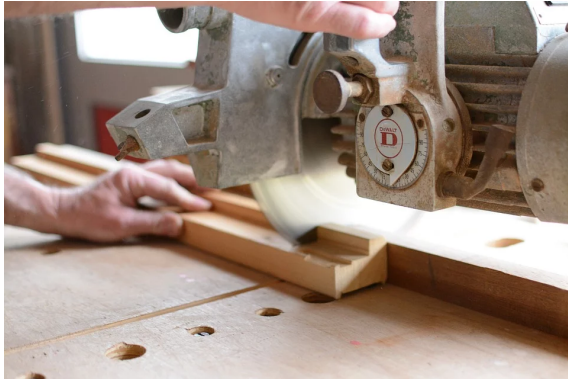
$$\mathcal{C} = \mathbf{GRS}_k(\mathbf{x}, \mathbf{y}) \quad \Rightarrow \quad \dim \mathcal{C}^{*2} = \min(2k - 1, n).$$

$$\text{Distinguisher works if: } \begin{cases} \dim \mathcal{C}^{*2} < \frac{k(k+1)}{2}, \\ \dim \mathcal{C}^{*2} < n. \end{cases}$$

How to reach the parameter range where the distinguisher works?

THE TOOLS: SQUARE-CODE DISTINGUISHER

How to reach the parameter range where the distinguisher works?



Definition (punctured code)

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ and $j \in \llbracket 1, n \rrbracket$.

$$\mathcal{P}_{\{j\}}(\mathcal{C}) \triangleq \{(\mathbf{c}_i)_{i \in \llbracket 1, n \rrbracket, i \neq j} \text{ s.t. } \mathbf{c} \in \mathcal{C}\}.$$

Definition (punctured code)

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ and $j \in \llbracket 1, n \rrbracket$.

$$\mathcal{P}_{\{j\}}(\mathcal{C}) \triangleq \{(\mathbf{c}_i)_{i \in \llbracket 1, n \rrbracket, i \neq j} \text{ s.t. } \mathbf{c} \in \mathcal{C}\}.$$

Definition (shortened code)

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ and $j \in \llbracket 1, n \rrbracket$.

$$\mathcal{S}_{\{j\}}(\mathcal{C}) \triangleq \mathcal{P}_{\{j\}}(\{\mathbf{c} \in \mathcal{C} \text{ s.t. } c_j = 0\}).$$

THE TOOLS: PUNCTURED AND SHORTENED CODES

For \mathcal{C} a **random** code of dimension k and length n :

\mathcal{C} **random**
length = n
dimension = k



$\mathcal{C}' = \mathcal{S}(\mathcal{C})$
length $n' = n - 1$
dimension $k' = k - 1$

$$\dim \mathcal{C}^{*2} = \min \left(\frac{k(k+1)}{2}, n \right).$$

THE TOOLS: PUNCTURED AND SHORTENED CODES

For $\mathcal{C} = \mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$:

\mathcal{C}
length = n
dimension = k



$\mathcal{C}' = \mathcal{S}(\mathcal{C})$
length $n' = n - 1$
dimension $k' = k - 1$

$$\dim \mathcal{C}^{*2} = \min(2k - 1, n).$$

THE TOOLS: PUNCTURED AND SHORTENED CODES

For $\mathcal{C} = \mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$:

\mathcal{C}
length = n
dimension = k



$\mathcal{C}' = \mathcal{S}(\mathcal{C})$
length $n' = n - 1$
dimension $k' = k - 1$

$$\dim \mathcal{C}^{*2} = \min(2k - 1, n).$$

Repeat until $\dim \mathcal{C}^{*2} < n$.

PERMUTING THE GENERATOR MATRIX

Let (α, β) be an \mathbb{F}_q -base of \mathbb{F}_{q^2} . Denote $\phi_\alpha(\cdot)$, $\phi_\beta(\cdot)$ the projectors.

Definition

Exp $_{(\alpha, \beta)}$

$$\begin{array}{ccc} \mathbb{F}_{q^2}^{k \times n} & \rightarrow & \mathbb{F}_q^{2k \times 2n} \\ \left(\begin{array}{cccc} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,n} \\ \vdots & \vdots & & \vdots \\ m_{k,1} & m_{k,2} & \cdots & m_{k,n} \end{array} \right) & \mapsto & \left(\begin{array}{cccc} \mathbf{M}_{1,1} & \mathbf{M}_{1,2} & \cdots & \mathbf{M}_{1,n} \\ \mathbf{M}_{2,1} & \mathbf{M}_{2,2} & \cdots & \mathbf{M}_{2,n} \\ \vdots & \vdots & & \vdots \\ \mathbf{M}_{k,1} & \mathbf{M}_{k,2} & \cdots & \mathbf{M}_{k,n} \end{array} \right) \end{array}$$

$$\text{where } \mathbf{M}_{i,j} \triangleq \begin{pmatrix} \phi_\alpha(\alpha m_{i,j}) & \phi_\alpha(\beta m_{i,j}) \\ \phi_\beta(\alpha m_{i,j}) & \phi_\beta(\beta m_{i,j}) \end{pmatrix} \in \mathbb{F}_q^{2 \times 2}.$$

PERMUTING THE GENERATOR MATRIX

Let (α, β) be an \mathbb{F}_q -base of \mathbb{F}_{q^2} . Denote $\phi_\alpha(\cdot)$, $\phi_\beta(\cdot)$ the projectors.

Definition

$\text{Exp}_{(\alpha, \beta)}$

$$\begin{array}{ccc} \mathbb{F}_{q^2}^{k \times n} & \rightarrow & \mathbb{F}_q^{2k \times 2n} \\ \left(\begin{array}{cccc} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,n} \\ \vdots & \vdots & & \vdots \\ m_{k,1} & m_{k,2} & \cdots & m_{k,n} \end{array} \right) & \mapsto & \left(\begin{array}{cccc} \mathbf{M}_{1,1} & \mathbf{M}_{1,2} & \cdots & \mathbf{M}_{1,n} \\ \mathbf{M}_{2,1} & \mathbf{M}_{2,2} & \cdots & \mathbf{M}_{2,n} \\ \vdots & \vdots & & \vdots \\ \mathbf{M}_{k,1} & \mathbf{M}_{k,2} & \cdots & \mathbf{M}_{k,n} \end{array} \right) \end{array}$$

$$\text{where } \mathbf{M}_{i,j} \triangleq \begin{pmatrix} \phi_\alpha(\alpha m_{i,j}) & \phi_\alpha(\beta m_{i,j}) \\ \phi_\beta(\alpha m_{i,j}) & \phi_\beta(\beta m_{i,j}) \end{pmatrix} \in \mathbb{F}_q^{2 \times 2}.$$

PERMUTING THE GENERATOR MATRIX

Property

Up to permutation of the rows and columns, we have:

$$\mathbf{Exp}_{(\alpha, \beta)} : \begin{cases} \mathbb{F}_{q^2}^{k \times n} & \rightarrow \\ \mathbf{M} & \mapsto \end{cases} \left(\begin{array}{c|c} \mathbb{F}_q^{2k \times 2n} & \\ \hline \phi_\alpha(\alpha \mathbf{M}) & \phi_\alpha(\beta \mathbf{M}) \\ \hline \phi_\beta(\alpha \mathbf{M}) & \phi_\beta(\beta \mathbf{M}) \end{array} \right).$$

Property

Up to permutation of the rows and columns, we have:

$$\mathbf{Exp}_{(1,\gamma)} : \begin{cases} \mathbb{F}_{q^2}^{k \times n} & \rightarrow \\ \mathbf{M} & \mapsto \end{cases} \left(\begin{array}{c|c} \mathbb{F}_q^{2k \times 2n} & \\ \hline \phi_1(\mathbf{M}) & \phi_1(\gamma\mathbf{M}) \\ \hline \phi_\gamma(\mathbf{M}) & \phi_\gamma(\gamma\mathbf{M}) \end{array} \right).$$

Definition

$$\begin{aligned} \mathbf{Tr}_q : \quad \mathbb{F}_{q^2} &\rightarrow \mathbb{F}_q \\ x &\mapsto x + x^q \end{aligned}$$

Definition

$$\mathbf{Tr}_q : \begin{array}{ccc} \mathbb{F}_{q^2} & \rightarrow & \mathbb{F}_q \\ x & \mapsto & x + x^q \end{array}$$

Hypothesis: we will choose γ such that $\gamma^2 = -1$, i.e. $\mathbf{Tr}_q(\gamma) = 0$.

Let $x = \phi_1(x) + \gamma\phi_\gamma(x)$.

$$\mathbf{Tr}_q(x) = 2\phi_1(x),$$

$$\mathbf{Tr}_q(-\gamma x) = 2\phi_\gamma(x).$$

Property

Up to permutation of the rows and columns, we have:

$$\mathbf{Exp}_{(1,\gamma)} : \begin{cases} \mathbb{F}_{q^2}^{k \times n} & \rightarrow \\ \mathbf{M} & \mapsto \end{cases} \left(\begin{array}{c|c} \mathbb{F}_q^{2k \times 2n} & \\ \hline \phi_1(\mathbf{M}) & \phi_1(\gamma\mathbf{M}) \\ \hline \phi_\gamma(\mathbf{M}) & \phi_\gamma(\gamma\mathbf{M}) \end{array} \right).$$

PERMUTING THE GENERATOR MATRIX

Property

Up to permutation of the rows and columns, we have:

$$\mathbf{Exp}_{(1,\gamma)} : \begin{cases} \mathbb{F}_{q^2}^{k \times n} & \rightarrow \\ \mathbf{M} & \mapsto 2 \left(\begin{array}{c|c} \mathbb{F}_q^{2k \times 2n} & \\ \hline \text{Tr}_q(\mathbf{M}) & \text{Tr}_q(\gamma\mathbf{M}) \\ \hline \text{Tr}_q(-\gamma\mathbf{M}) & \text{Tr}_q(\mathbf{M}) \end{array} \right).$$

To use the square code distinguisher, we need to compute

$$\dim \langle \mathbf{G}_{pk} \rangle^{*2} = ???$$

To use the square code distinguisher, we need to compute

$$\dim \langle \mathbf{G}_{pk} \rangle^{*2} = ???$$

Theorem

Let $\mathbf{G} \in \mathbb{F}_{q^2}^{k \times n}$ be the generator matrix of a **GRS** $_{\mathbb{F}_{q^2}}(n, k)$ code,

$$\mathcal{C} \triangleq \langle \mathbf{Exp}_{1,\gamma}(\mathbf{G}) \rangle_{\mathbb{F}_q},$$

$$\dim \mathcal{C}^{*2} = k^2 + 4k - 2.$$

SQUARE CODE DIMENSION (PROOF)

$$\mathcal{C} \triangleq \langle \mathbf{G} \rangle \quad ; \quad \widehat{\mathcal{C}}_1 \triangleq \langle \mathbf{Exp}_{1,\gamma}(\mathbf{G}) \rangle_{\mathbb{F}_q} \quad ; \quad \widehat{\mathcal{C}}_2 \triangleq \langle \mathbf{Exp}_{1,\gamma}(\mathbf{G}) \rangle_{\mathbb{F}_{q^2}}$$

SQUARE CODE DIMENSION (PROOF)

$$\mathcal{C} \triangleq \langle \mathbf{G} \rangle \quad ; \quad \widehat{\mathcal{C}}_1 \triangleq \langle \mathbf{Exp}_{1,\gamma}(\mathbf{G}) \rangle_{\mathbb{F}_q} \quad ; \quad \widehat{\mathcal{C}}_2 \triangleq \langle \mathbf{Exp}_{1,\gamma}(\mathbf{G}) \rangle_{\mathbb{F}_{q^2}}$$

Property 1

$$\dim_{\mathbb{F}_q} \widehat{\mathcal{C}}_1^{*2} = \dim_{\mathbb{F}_{q^2}} \widehat{\mathcal{C}}_2^{*2}$$

SQUARE CODE DIMENSION (PROOF)

$$\mathcal{C} \triangleq \langle \mathbf{G} \rangle \quad ; \quad \widehat{\mathcal{C}}_1 \triangleq \langle \mathbf{Exp}_{1,\gamma}(\mathbf{G}) \rangle_{\mathbb{F}_q} \quad ; \quad \widehat{\mathcal{C}}_2 \triangleq \langle \mathbf{Exp}_{1,\gamma}(\mathbf{G}) \rangle_{\mathbb{F}_{q^2}}$$

Property 2

$$\widehat{\mathcal{C}}_2 = \underbrace{\langle (\mathbf{c}, \gamma \mathbf{c}) \mid \mathbf{c} \in \mathcal{C} \rangle_{\mathbb{F}_{q^2}}}_{(1)} + \underbrace{\langle (\mathbf{c}^q, -\gamma \mathbf{c}^q) \mid \mathbf{c} \in \mathcal{C} \rangle_{\mathbb{F}_{q^2}}}_{(2)}.$$

SQUARE CODE DIMENSION (PROOF)

$$\mathcal{C} \triangleq \langle \mathbf{G} \rangle \quad ; \quad \widehat{\mathcal{C}}_1 \triangleq \langle \mathbf{Exp}_{1,\gamma}(\mathbf{G}) \rangle_{\mathbb{F}_q} \quad ; \quad \widehat{\mathcal{C}}_2 \triangleq \langle \mathbf{Exp}_{1,\gamma}(\mathbf{G}) \rangle_{\mathbb{F}_{q^2}}$$

Property 2

$$\widehat{\mathcal{C}}_2 = \underbrace{\langle (\mathbf{c}, \gamma \mathbf{c}) \mid \mathbf{c} \in \mathcal{C} \rangle_{\mathbb{F}_{q^2}}}_{(1)} + \underbrace{\langle (\mathbf{c}^q, -\gamma \mathbf{c}^q) \mid \mathbf{c} \in \mathcal{C} \rangle_{\mathbb{F}_{q^2}}}_{(2)}.$$

Corrolary

$$\widehat{\mathcal{C}}_2^{\star 2} = \left\langle \begin{pmatrix} \mathbf{c}_1 \star \mathbf{c}_2 & , & -\mathbf{c}_1 \star \mathbf{c}_2 \\ \mathbf{c}_1^q \star \mathbf{c}_2^q & , & -\mathbf{c}_1^q \star \mathbf{c}_2^q \\ \mathbf{c}_1 \star \mathbf{c}_2^q & , & \mathbf{c}_1 \star \mathbf{c}_2^q \end{pmatrix}, \begin{matrix} (1) \star (1) \\ (2) \star (2) \\ (1) \star (2) \end{matrix} \mid (\mathbf{c}_1, \mathbf{c}_2) \in \mathcal{C}^2 \right\rangle_{\mathbb{F}_{q^2}}.$$

SQUARE CODE DIMENSION (PROOF)

$$\mathcal{C} \triangleq \langle \mathbf{G} \rangle \quad ; \quad \widehat{\mathcal{C}}_1 \triangleq \langle \mathbf{Exp}_{1,\gamma}(\mathbf{G}) \rangle_{\mathbb{F}_q} \quad ; \quad \widehat{\mathcal{C}}_2 \triangleq \langle \mathbf{Exp}_{1,\gamma}(\mathbf{G}) \rangle_{\mathbb{F}_{q^2}}$$

Property 2

$$\widehat{\mathcal{C}}_2 = \underbrace{\langle (\mathbf{c}, \gamma \mathbf{c}) \mid \mathbf{c} \in \mathcal{C} \rangle_{\mathbb{F}_{q^2}}}_{(1)} + \underbrace{\langle (\mathbf{c}^q, -\gamma \mathbf{c}^q) \mid \mathbf{c} \in \mathcal{C} \rangle_{\mathbb{F}_{q^2}}}_{(2)}$$

Corrolary

$$\widehat{\mathcal{C}}_2^{\star 2} = \left\langle \begin{pmatrix} \mathbf{c}_1 \star \mathbf{c}_2 & , & -\mathbf{c}_1 \star \mathbf{c}_2 \\ \mathbf{c}_1^q \star \mathbf{c}_2^q & , & -\mathbf{c}_1^q \star \mathbf{c}_2^q \\ \mathbf{c}_1 \star \mathbf{c}_2^q & , & \mathbf{c}_1 \star \mathbf{c}_2^q \end{pmatrix}, \begin{matrix} (1) \star (1) \\ (2) \star (2) \\ (1) \star (2) \end{matrix} \mid (\mathbf{c}_1, \mathbf{c}_2) \in \mathcal{C}^2 \right\rangle_{\mathbb{F}_{q^2}}$$

$$\dim \widehat{\mathcal{C}}_2^{\star 2} = (2k + 1) + (2k + 1) + \binom{k + 1}{2}$$

SQUARE CODE DIMENSION (PROOF)

$$\mathcal{C} \triangleq \langle \mathbf{G} \rangle \quad ; \quad \widehat{\mathcal{C}}_1 \triangleq \langle \mathbf{Exp}_{1,\gamma}(\mathbf{G}) \rangle_{\mathbb{F}_q} \quad ; \quad \widehat{\mathcal{C}}_2 \triangleq \langle \mathbf{Exp}_{1,\gamma}(\mathbf{G}) \rangle_{\mathbb{F}_{q^2}}$$

Property 2

$$\widehat{\mathcal{C}}_2 = \underbrace{\langle (\mathbf{c}, \gamma \mathbf{c}) \mid \mathbf{c} \in \mathcal{C} \rangle_{\mathbb{F}_{q^2}}}_{(1)} + \underbrace{\langle (\mathbf{c}^q, -\gamma \mathbf{c}^q) \mid \mathbf{c} \in \mathcal{C} \rangle_{\mathbb{F}_{q^2}}}_{(2)}.$$

Corrolary

$$\widehat{\mathcal{C}}_2^{\star 2} = \left\langle \begin{pmatrix} \mathbf{c}_1 \star \mathbf{c}_2 & , & -\mathbf{c}_1 \star \mathbf{c}_2 \\ \mathbf{c}_1^q \star \mathbf{c}_2^q & , & -\mathbf{c}_1^q \star \mathbf{c}_2^q \\ \mathbf{c}_1 \star \mathbf{c}_2^q & , & \mathbf{c}_1 \star \mathbf{c}_2^q \end{pmatrix}, \begin{matrix} (1) \star (1) \\ (2) \star (2) \\ (1) \star (2) \end{matrix} \mid (\mathbf{c}_1, \mathbf{c}_2) \in \mathcal{C}^2 \right\rangle_{\mathbb{F}_{q^2}}.$$

$$\dim \widehat{\mathcal{C}}_2^{\star 2} = (2k + 1) + (2k + 1) + \binom{k + 1}{2} = k^2 + 4k - 2. \quad \square$$

SQUARE OF A SHORTENED CODE

$$\dim\langle \mathbf{G}_{pk} \rangle^{*2} = k^2 + 4k - 2 \quad .$$

SQUARE OF A SHORTENED CODE

$$\dim\langle \mathbf{G}_{pk} \rangle^{*2} = \min(k^2 + 4k - 2, 2n).$$

SQUARE OF A SHORTENED CODE

$$\dim\langle \mathbf{G}_{pk} \rangle^{*2} = \min(k^2 + 4k - 2, 2n).$$

- What if we shorten some columns?

SQUARE OF A SHORTENED CODE

$$\dim\langle \mathbf{G}_{pk} \rangle^{*2} = \min(k^2 + 4k - 2, 2n).$$

- What if we shorten some columns?
 - ▶ If we shorten **two twin** columns?

SQUARE OF A SHORTENED CODE

$$\dim\langle \mathbf{G}_{pk} \rangle^{*2} = \min(k^2 + 4k - 2, 2n).$$

- What if we shorten some columns?
 - ▶ If we shorten **two twin** columns?

Equivalent to shortening the original GRS code.

$$\mathcal{S}_{\{j, \tau(j)\}}(\mathbf{Exp}(\mathbf{G})) = \mathbf{Exp}(\mathcal{S}_{\{j\}}(\mathbf{G})).$$

SQUARE OF A SHORTENED CODE

$$\dim \langle \mathbf{G}_{pk} \rangle^{*2} = \min(k^2 + 4k - 2, 2n).$$

- What if we shorten some columns?
 - ▶ If we shorten **two twin** columns?

Equivalent to shortening the original GRS code.

$$\mathcal{S}_{\{j, \tau(j)\}}(\mathbf{Exp}(\mathbf{G})) = \mathbf{Exp}(\mathcal{S}_{\{j\}}(\mathbf{G})).$$

$$\dim \mathcal{S}_{\{j, \tau(j)\}}(\mathbf{Exp}(\mathbf{G}))^{*2} = (k-1)^2 + 4(k-1) - 2.$$

SQUARE OF A SHORTENED CODE

$$\dim \langle \mathbf{G}_{pk} \rangle^{*2} = \min(k^2 + 4k - 2, 2n).$$

- What if we shorten some columns?
 - ▶ If we shorten **two twin** columns?

Equivalent to shortening the original GRS code.

$$\mathcal{S}_{\{j, \tau(j)\}}(\mathbf{Exp}(\mathbf{G})) = \mathbf{Exp}(\mathcal{S}_{\{j\}}(\mathbf{G})).$$

$$\dim \mathcal{S}_{\{j, \tau(j)\}}(\mathbf{Exp}(\mathbf{G}))^{*2} = (k-1)^2 + 4(k-1) - 2.$$

- ▶ If we shorten **one** column?

SQUARE OF A SHORTENED CODE

$$\dim \langle \mathbf{G}_{pk} \rangle^{*2} = \min(k^2 + 4k - 2, 2n).$$

■ What if we shorten some columns?

- ▶ If we shorten **two twin** columns?

Equivalent to shortening the original GRS code.

$$\mathcal{S}_{\{j, \tau(j)\}}(\mathbf{Exp}(\mathbf{G})) = \mathbf{Exp}(\mathcal{S}_{\{j\}}(\mathbf{G})).$$

$$\dim \mathcal{S}_{\{j, \tau(j)\}}(\mathbf{Exp}(\mathbf{G}))^{*2} = (k-1)^2 + 4(k-1) - 2.$$

- ▶ If we shorten **one** column?

Equivalent to shortening two twin columns and adding a random column.

$$\mathcal{S}_{\{j\}}(\mathbf{Exp}(\mathbf{G})) = \mathcal{S}_{\{j, \tau(j)\}}(\mathbf{Exp}(\mathbf{G})) + \langle r \rangle.$$

SQUARE OF A SHORTENED CODE

$$\dim \langle \mathbf{G}_{pk} \rangle^{*2} = \min(k^2 + 4k - 2, 2n).$$

■ What if we shorten some columns?

- ▶ If we shorten **two twin** columns?

Equivalent to shortening the original GRS code.

$$\mathcal{S}_{\{j, \tau(j)\}}(\mathbf{Exp}(\mathbf{G})) = \mathbf{Exp}(\mathcal{S}_{\{j\}}(\mathbf{G})).$$

$$\dim \mathcal{S}_{\{j, \tau(j)\}}(\mathbf{Exp}(\mathbf{G}))^{*2} = (k-1)^2 + 4(k-1) - 2.$$

- ▶ If we shorten **one** column?

Equivalent to shortening two twin columns and adding a random column.

$$\mathcal{S}_{\{j\}}(\mathbf{Exp}(\mathbf{G})) = \mathcal{S}_{\{j, \tau(j)\}}(\mathbf{Exp}(\mathbf{G})) + \langle r \rangle.$$

$$\dim \mathcal{S}_{\{j, \tau(j)\}}(\mathbf{Exp}(\mathbf{G}))^{*2} = ((k-1)^2 + 4(k-1) - 2) + 2(k-1) + 1.$$

SQUARE OF A SHORTENED CODE

Let $\mathbf{G} \in \mathbb{F}_{q^2}^{k \times n}$ be the generator matrix of a $\mathbf{GRS}_{\mathbb{F}_{q^2}}(n, k)$ code.
Let \mathcal{L} be a subset of $\llbracket 1, 2n \rrbracket$ containing:

- l_1 isolated columns;
- l_2 pairs of twin columns, (i.e. $|\mathcal{L}| = l_1 + 2l_2$)

then

Theorem

$$\dim \mathcal{S}_{\mathcal{L}}(\mathbf{Exp}(\mathbf{G}))^{*2} = (d^2 + 4d - 2) + 2dl_1 + \binom{l_1 + 1}{2},$$

$$\text{where } d \triangleq k - l_1 - l_2.$$

Previous theorem (simplified)

$$\dim \mathcal{S}_{\mathcal{L}}(\mathbf{G}_{\text{pk}})^{\star 2} = f(l_1, l_2).$$

USING THE DISTINGUISHER

- Pick \mathcal{L} a random subset of $\llbracket 1, 2n \rrbracket$;
- For $i \notin \mathcal{L}$, compute $\dim \mathcal{S}_{\mathcal{L} \cup \{i\}}(\mathbf{G}_{\text{pk}})^{\star 2}$:
 - ▶ $\dim \mathcal{S}_{\mathcal{L} \cup \{i\}}(\mathbf{G}_{\text{pk}})^{\star 2} = f(l_1 + 1, l_2) \Leftrightarrow \tau(i) \notin \mathcal{L}$,
 - ▶ $\dim \mathcal{S}_{\mathcal{L} \cup \{i\}}(\mathbf{G}_{\text{pk}})^{\star 2} = f(l_1 - 1, l_2 + 1) \Leftrightarrow \tau(i) \in \mathcal{L}$;

USING THE DISTINGUISHER

- Pick \mathcal{L} a random subset of $\llbracket 1, 2n \rrbracket$;
- For $i \notin \mathcal{L}$, compute $\dim \mathcal{S}_{\mathcal{L} \cup \{i\}}(\mathbf{G}_{\text{pk}})^{\star 2}$:
 - ▶ $\dim \mathcal{S}_{\mathcal{L} \cup \{i\}}(\mathbf{G}_{\text{pk}})^{\star 2} = f(l_1 + 1, l_2) \Leftrightarrow \tau(i) \notin \mathcal{L}$,
 - ▶ $\dim \mathcal{S}_{\mathcal{L} \cup \{i\}}(\mathbf{G}_{\text{pk}})^{\star 2} = f(l_1 - 1, l_2 + 1) \Leftrightarrow \tau(i) \in \mathcal{L}$;
- For $j \in \mathcal{L}$, compute $\dim \mathcal{S}_{\mathcal{L} \setminus \{j\}}(\mathbf{G}_{\text{pk}})^{\star 2}$:
 - ▶ $\dim \mathcal{S}_{\mathcal{L} \setminus \{j\}}(\mathbf{G}_{\text{pk}})^{\star 2} = f(l_1 - 1, l_2) \Leftrightarrow \tau(j) \notin \mathcal{L}$,
 - ▶ $\dim \mathcal{S}_{\mathcal{L} \setminus \{j\}}(\mathbf{G}_{\text{pk}})^{\star 2} = f(l_1 + 1, l_2 - 1) \Leftrightarrow \tau(j) \in \mathcal{L}$;

USING THE DISTINGUISHER

- Pick \mathcal{L} a random subset of $\llbracket 1, 2n \rrbracket$;
- For $i \notin \mathcal{L}$, compute $\dim \mathcal{S}_{\mathcal{L} \cup \{i\}}(\mathbf{G}_{\text{pk}})^{\star 2}$:
 - ▶ $\dim \mathcal{S}_{\mathcal{L} \cup \{i\}}(\mathbf{G}_{\text{pk}})^{\star 2} = f(l_1 + 1, l_2) \Leftrightarrow \tau(i) \notin \mathcal{L}$,
 - ▶ $\dim \mathcal{S}_{\mathcal{L} \cup \{i\}}(\mathbf{G}_{\text{pk}})^{\star 2} = f(l_1 - 1, l_2 + 1) \Leftrightarrow \tau(i) \in \mathcal{L}$;
- For $j \in \mathcal{L}$, compute $\dim \mathcal{S}_{\mathcal{L} \setminus \{j\}}(\mathbf{G}_{\text{pk}})^{\star 2}$:
 - ▶ $\dim \mathcal{S}_{\mathcal{L} \setminus \{j\}}(\mathbf{G}_{\text{pk}})^{\star 2} = f(l_1 - 1, l_2) \Leftrightarrow \tau(j) \notin \mathcal{L}$,
 - ▶ $\dim \mathcal{S}_{\mathcal{L} \setminus \{j\}}(\mathbf{G}_{\text{pk}})^{\star 2} = f(l_1 + 1, l_2 - 1) \Leftrightarrow \tau(j) \in \mathcal{L}$;
- For $j \in \mathcal{L}$ s.t. $\tau(j) \notin \mathcal{L}$, for $i \notin \mathcal{L}$ s.t. $\tau(i) \in \mathcal{L}$, compute $\dim \mathcal{S}_{(\mathcal{L} \setminus \{i\}) \cup \{j\}}(\mathbf{G}_{\text{pk}})^{\star 2}$:
 - ▶ $\dim \mathcal{S}_{(\mathcal{L} \setminus \{i\}) \cup \{j\}}(\mathbf{G}_{\text{pk}})^{\star 2} = f(l_1, l_2) \Leftrightarrow i = \tau(j)$.
 - ▶ $\dim \mathcal{S}_{(\mathcal{L} \setminus \{i\}) \cup \{j\}}(\mathbf{G}_{\text{pk}})^{\star 2} = f(l_1 - 2, l_2 + 1) \Leftrightarrow i \neq \tau(j)$.

1. Find which pairs of columns are twins;
2. In each pair, distinguish the left column from the right column (**work in progress...**);
3. Reconstruct the code over \mathbb{F}_{q^2} ;
4. Use Sidelnikov-Shestakov's attack to find the structure of the GRS code;
5. Correct the errors to find the message.

KEY GENERATION

For parameters (m, q, n, k) :

- γ a primitive element of \mathbb{F}_{q^m}
- $\mathbf{G} \stackrel{\$}{\leftarrow} \mathbf{GRS}_{\mathbb{F}_{q^m}}(n, k) \in \mathbb{F}_{q^m}^{k \times n}$
- $\hat{\mathbf{G}} = \mathbf{Exp}_{(1, \gamma, \dots, \gamma^m)}(\mathbf{G}) \in \mathbb{F}_q^{mk \times mn}$
- $\mathcal{P}(\hat{\mathbf{G}}) \in \mathbb{F}_q^{mk \times 2n} \leftarrow$ keep only two columns per block of \mathbf{G} , puncture the $(m - 2)$ other columns.
- $t = \lfloor \frac{k}{2} \rfloor$ (error-correction capacity of \mathbf{G}^\perp)
- $\mathbf{T}_i \stackrel{\$}{\leftarrow} 2 \times 2$ invertible matrices for $i \in \llbracket 1, n \rrbracket$
- \mathbf{T} the block-diagonal matrix of diagonal blocks $\mathbf{T}_1, \dots, \mathbf{T}_n$
- $\mathbf{G}_{pk} = \mathcal{P}(\hat{\mathbf{G}}) \cdot \mathbf{T}$

$$\begin{cases} \text{PublicKey} = & (\mathbf{G}_{pk}, t) \\ \text{SecretKey} = & (\gamma, \mathbf{G}, \mathbf{T}). \end{cases}$$

How does puncturing columns affect the structure of an expanded GRS code?

How does puncturing columns affect the structure of an expanded GRS code?

- Puncturing = shortening the dual.

How does puncturing columns affect the structure of an expanded GRS code?

- Puncturing = shortening the dual.
- We know how shortening affects the structure.

How does puncturing columns affect the structure of an expanded GRS code?

- Puncturing = shortening the dual.
- We know how shortening affects the structure.

What is the dual of an expanded GRS code?

Definition

For an \mathbb{F}_q -base (b_1, \dots, b_m) of \mathbb{F}_{q^m} , we define the **dual base** (b_1^*, \dots, b_m^*) such that

$$\forall i \in \llbracket 1, m \rrbracket, \forall j \in \llbracket 1, m \rrbracket, \quad \langle b_i, b_j^* \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{elsewhere.} \end{cases}$$

Definition

For an \mathbb{F}_q -base (b_1, \dots, b_m) of \mathbb{F}_{q^m} , we define the **dual base** (b_1^*, \dots, b_m^*) such that

$$\forall i \in \llbracket 1, m \rrbracket, \forall j \in \llbracket 1, m \rrbracket, \quad \langle b_i, b_j^* \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{elsewhere.} \end{cases}$$

Property

Let (b_1, \dots, b_m) be a base and (b_1^*, \dots, b_m^*) its dual base. Then

$$\forall j \in \llbracket 1, m \rrbracket, \quad \phi_{b_j}(\cdot) = \mathbf{Tr}_q(b_j^* \cdot).$$

BETTER TOOLS FOR HIGHER DIMENSION

$$\mathbf{Exp}_{(b_1, \dots, b_m)} \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{pmatrix} =$$

$$\begin{pmatrix} \mathbf{Tr}_q(b_1^* b_1 g_{1,1}) & \cdots & \mathbf{Tr}_q(b_1^* b_m g_{1,1}) & \cdots & \mathbf{Tr}_q(b_1^* b_1 g_{1,n}) & \cdots & \mathbf{Tr}_q(b_1^* b_m g_{1,n}) \\ \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\ \mathbf{Tr}_q(b_m^* b_1 g_{1,1}) & \cdots & \mathbf{Tr}_q(b_m^* b_m g_{1,1}) & \cdots & \mathbf{Tr}_q(b_m^* b_1 g_{1,n}) & \cdots & \mathbf{Tr}_q(b_m^* b_m g_{1,n}) \\ \hline \vdots & & \vdots & & \vdots & & \vdots \\ \mathbf{Tr}_q(b_1^* b_1 g_{k,1}) & \cdots & \mathbf{Tr}_q(b_1^* b_m g_{k,1}) & \cdots & \mathbf{Tr}_q(b_1^* b_1 g_{k,n}) & \cdots & \mathbf{Tr}_q(b_1^* b_m g_{k,n}) \\ \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\ \mathbf{Tr}_q(b_m^* b_1 g_{k,1}) & \cdots & \mathbf{Tr}_q(b_m^* b_m g_{k,1}) & \cdots & \mathbf{Tr}_q(b_m^* b_1 g_{k,n}) & \cdots & \mathbf{Tr}_q(b_m^* b_m g_{k,n}) \end{pmatrix}$$

Theorem

Let $\mathbf{G} \in \mathbb{F}_{q^m}^{k \times n}$ and denote (b_1, \dots, b_m) an \mathbb{F}_q -base of \mathbb{F}_{q^m} . Then

$$\langle (\mathbf{Exp}_{(b_1, \dots, b_m)}(\mathbf{G}))^\top \rangle = \langle \mathbf{Exp}_{(\bar{b}_1, \dots, \bar{b}_m)}(\mathbf{G}^\top) \rangle,$$

where $(\bar{b}_1, \dots, \bar{b}_m)$ is such that

$$\forall i \in \llbracket 1, m-1 \rrbracket, \quad \sum_{j=1}^m b_j \bar{b}_j^{q^i} = 0.$$

We call $(\bar{b}_1, \dots, \bar{b}_m)$ the **exp-dual** base of (b_1, \dots, b_m) .

Remark

The **exp-dual** base $(\bar{b}_1, \dots, \bar{b}_m)$ is such that

$$\forall i \in \llbracket 1, m-1 \rrbracket, \quad (\bar{b}_1^{q^i}, \dots, \bar{b}_m^{q^i}) \in \langle (\bar{b}_1, \dots, \bar{b}_m) \rangle^\perp.$$

Denote (b'_1, \dots, b'_m) the basis such that

$$\mathbf{Gab}_1(b_1, \dots, b_m)^\perp = \mathbf{Gab}_{m-1}(b'_1, \dots, b'_m)$$

where $\mathbf{Gab}_k(x_1, \dots, x_n)$ is the Gabidulin code of dimension k evaluated in points (x_1, \dots, x_n) .

Then $\bar{b}_i = (b'_i)^{1/q}$. [Loio7]

CONCLUSION

- Square code distinguisher can be adapted to various schemes using GRS codes (BL, RLCE, XGRS, ...).

CONCLUSION

- Square code distinguisher can be adapted to various schemes using GRS codes (BL, RLCE, XGRS, ...).
- Structure of expanded codes much richer than expected.

CONCLUSION

- Square code distinguisher can be adapted to various schemes using GRS codes (BL, RLCE, XGRS, ...).
- Structure of expanded codes much richer than expected.
 - ▶ Links with trace code;

CONCLUSION

- Square code distinguisher can be adapted to various schemes using GRS codes (BL, RLCE, XGRS, ...).
- Structure of expanded codes much richer than expected.
 - ▶ Links with trace code;
 - ▶ Links with Gabidulin codes;

CONCLUSION

- Square code distinguisher can be adapted to various schemes using GRS codes (BL, RLCE, XGRS, ...).
- Structure of expanded codes much richer than expected.
 - ▶ Links with trace code;
 - ▶ Links with Gabidulin codes;
 - ▶ Attacks on XGRS still not complete;







- Square code distinguisher can be adapted to various schemes using GRS codes (BL, RLCE, XGRS, ...).
- Structure of expanded codes much richer than expected.
 - ▶ Links with trace code;
 - ▶ Links with Gabidulin codes;
 - ▶ Attacks on XGRS still not complete;
 - ▶ Requires further study.

CONCLUSION

- Square code distinguisher can be adapted to various schemes using GRS codes (BL, RLCE, XGRS, ...).
- Structure of expanded codes much richer than expected.
 - ▶ Links with trace code;
 - ▶ Links with Gabidulin codes;
 - ▶ Attacks on XGRS still not complete;
 - ▶ Requires further study.
- Be careful when designing schemes using GRS codes!

- Square code distinguisher can be adapted to various schemes using GRS codes (BL, RLCE, XGRS, ...).
- Structure of expanded codes much richer than expected.
 - ▶ Links with trace code;
 - ▶ Links with Gabidulin codes;
 - ▶ Attacks on XGRS still not complete;
 - ▶ Requires further study.
- Be careful when designing schemes using GRS codes!

Thank you for your attention!
Questions?

-  THIERRY P. BERGER AND PIERRE LOIDREAU.
HOW TO MASK THE STRUCTURE OF CODES FOR A CRYPTOGRAPHIC USE.
Des. Codes Cryptogr., 35(1):63–79, 2005.
-  ALAIN COUVREUR, MATTHIEU LEQUESNE, AND JEAN-PIERRE TILLICH.
RECOVERING SHORT SECRET KEYS OF RLCE IN POLYNOMIAL TIME.
In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography 2019*, volume 11505 of *LNCS*, pages 133–152, Chongqing, China, May 2019. Springer.
-  PIERRE LOIDREAU.
RANK METRIC AND CRYPTOGRAPHY.
Accreditation to supervise research, Université Pierre et Marie Curie - Paris VI, January 2007.
-  ROBERT J. McELIECE.
A PUBLIC-KEY SYSTEM BASED ON ALGEBRAIC CODING THEORY, PAGES 114–116.
Jet Propulsion Lab, 1978.
DSN Progress Report 44.
-  HARALD NIEDERREITER.
KNAPSACK-TYPE CRYPTOSYSTEMS AND ALGEBRAIC CODING THEORY.
Problems of Control and Information Theory, 15(2):159–166, 1986.
-  VLADIMIR MICHILOVICH SIDELNIKOV AND S.O. SHESTAKOV.

ON THE INSECURITY OF CRYPTOSYSTEMS BASED ON GENERALIZED REED-SOLOMON CODES.

Discrete Math. Appl., 1(4):439–444, 1992.



YONGGE WANG.

RLCE-KEM.

<http://quantumca.org>, 2017.

First round submission to the NIST post-quantum cryptography call.



CHRISTIAN WIESCHEBRINK.

AN ATTACK ON A MODIFIED NIEDERREITER ENCRYPTION SCHEME.

In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malk, editors, *Public-Key Cryptography - PKC 2006*, volume 3958 of LNCS, pages 14–26. Springer, 2006.



CHRISTIAN WIESCHEBRINK.

CRYPTANALYSIS OF THE NIEDERREITER PUBLIC KEY SCHEME BASED ON GRS SUBCODES.

IACR Cryptology ePrint Archive, Report 2009/452, 2009.