

VULNERABILITIES OF CODE-BASED CRYPTOGRAPHY

I. MÁRQUEZ-CORBELLA¹ E. MARTÍNEZ-MORO² R. PELLIKAAN³

¹Department of Algebra, Geometry and Topology, University of Valladolid.
Supported by a FPU grant AP2008-01598 by Spanish MEC.

²Department of Applied Mathematics, University of Valladolid.

³Department of Mathematics and Computing Science, Eindhoven University of Technology.

Spanish Cryptography Days (SCD 2011)

PUBLIC-KEY CRYPTOSYSTEMS

VULNERABILITIES OF CODE-BASED CRYPTOGRAPHY

INTRODUCTION

McELIECE CRYPTOSYSTEM
ATTACKS ON THE McELIECE PKC
NIEDERREITER CRYPTOSYSTEM
PKC USING
ALGEBRAIC-GEOMETRY CODES

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

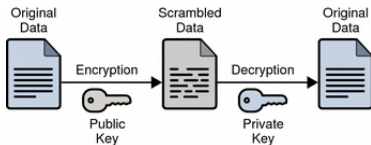
PROOFS

TWO KEYS:

- **Private Key:** Known only by the recipient.
- **Public Key:** Available to anyone.

MOST PKC ARE BASED ON NUMBER-THEORETIC PROBLEMS

→ Quantum computers will break the most popular PKCs: RSA, DSA, ECDSA, ECC, HECC, ... can be attacked in polynomial time using **Shor's algorithm**



GOOD NEWS: POST-QUANTUM CRYPTOGRAPHY

- Hash-based cryptography,
- Code-based cryptography,
- Lattice-based cryptography,
- Multivariate-quadratic-equation cryptography



D. J. Bernstein, J. Buchmann, E. Dahmen.
Post-Quantum Cryptography.
Springer, 2009.

McEliece CRYPTOSYSTEM

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

McEliece CRYPTOSYSTEM

ATTACKS ON THE McEliece PKC

NIEDERREITER CRYPTOSYSTEM

PKC USING
ALGEBRAIC-GEOMETRY CODES

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

KEY GENERATION

1 Given:

- \mathcal{C} an $[n, k, d]$ linear code over \mathbb{F}_q
- $G \in \mathbb{F}_q^{k \times n}$ a generator matrix of \mathcal{C} .
- $S \in \mathbb{F}_q^{k \times k}$ a nonsingular matrix.
- $P \in \mathbb{F}_q^{n \times n}$ a permutation matrix.

2 **McEliece Public Key** : $(G' = SGP, t)$.

3 **McEliece Private Key** : (G, S, P)

ENCRYPTION

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

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

where \mathbf{e} and $\mathbf{e}' = \mathbf{e}P$ in \mathbb{F}_q^n are random error vectors of weight t .

DECRYPTION

1 Compute $\mathbf{y} = \mathbf{y}'P^{-1} = \mathbf{m}G'P^{-1} + \mathbf{e}'P^{-1} = \mathbf{m}SG + \mathbf{e}$.

2 Apply the decoding algorithm for \mathcal{C} to find $\mathbf{m}S$.

3 $\mathbf{m} = \mathbf{m}S^{-1}$.

- McEliece introduced the first PKC based on **Error-Correcting Codes** in 1978.
- **Advantages**:
 - 1 Interesting candidate for post-quantum cryptography.
 - 2 Fast encryption (matrix-vector multiplication) and decryption functions.
- **Drawback**: Large key size.



R. J. McEliece.

A public-key cryptosystem based on algebraic coding theory.

DSN Progress Report, 42-44:114-116, 1978.

ATTACKS ON THE McELIECE PKC

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

McELIECE CRYPTOSYSTEM

ATTACKS ON THE McELIECE PKC

NIEDERREITER CRYPTOSYSTEM

PKC USING
ALGEBRAIC-GEOMETRY CODES

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

→ Most effective attack against the McEliece cryptosystem is **Information Set Decoding**. Many variants:

- 1 McEliece (1978)
- 2 Leon (1988)
- 3 Lee and Brickell (1988)
- 4 Stern (1989)
- 5 van Tilburg (1990)

- 6 Canteaut and Chabanne (1994)
- 7 Canteaut and Chabaud (1998)
- 8 Canteaut and Sendrier (1998)
- 9 Bernstein, Lange and Peters (2008)



A. Canteaut and H. Chabanne.

A further improvement of the work factor in an attempt at breaking McEliece's cryptosystem.
EUROCODE 94, 1994.



A. Canteaut and F. Chabaud.

A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511.
IEEE Transaction on Information Theory.



A. Canteaut and N. Sendrier.

Cryptanalysis of the original McEliece cryptosystem.
Advances in cryptology - ASIACRYPT'98.



P. J. Lee and E. F. Brickell.

An observation on the security of McEliece's public-key cryptosystem.
Advances in cryptology - EUROCRYPT'98.



D. J. Bernstein, T. Lange, C. Peters.

Attacking and defending the McEliece cryptosystem.
Post-Quantum Cryptography



J. S. Leon.

A probabilistic algorithm for computing minimum weights of large error-correcting codes.
IEEE Transaction on Information Theory.



R. J. McEliece.

A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report



J. Stern.

A method for finding codewords of small weight.
Coding theory and applications, Vol 388 of Lecture Notes in Computer Science, 106-113. Springer, New York, 1989.



J. van Tilburg.

On the McEliece public-key cryptosystem.
Advances in cryptology - CRYPTO'88.

NIEDERREITER CRYPTOSYSTEM

VULNERABILITIES OF CODE-BASED CRYPTOGRAPHY

INTRODUCTION

McELIECE CRYPTOSYSTEM

ATTACKS ON THE McELIECE PKC

NIEDERREITER CRYPTOSYSTEM

PKC USING ALGEBRAIC-GEOMETRY CODES

GAPS OF A CODE

GRS SUBCODES OF GRS CODES

THE SQUARE OF A CODE

PROOFS

→ Niederreiter presents a dual version of McEliece cryptosystem in 1986 which is equivalent in terms of security, with the same Goppa codes.

KEY GENERATION

1 Given:

- C an $[n, k, d]$ linear code over \mathbb{F}_q
- $H \in \mathbb{F}_q^{(n-k) \times n}$ a parity check matrix of C .
- $S \in \mathbb{F}_q^{(n-k) \times (n-k)}$ a nonsingular matrix.
- $P \in \mathbb{F}_q^{n \times n}$ a permutation matrix.

2 Niederreiter Public Key :
($H' = SHP, t$).

3 Niederreiter Private Key: (H, S, P)

ENCRYPTION

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

$$\mathbf{y}' = \mathbf{m}H'^T.$$

DECRYPTION

- 1 Compute $\mathbf{y} = \mathbf{y}' = (S^{-1})^T = \mathbf{m}P^T H^T = \mathbf{m}' H^T$. Syndrome of \mathbf{m}' by H .
- 2 Apply decoding algorithm for C to find $\mathbf{m}' = \mathbf{m}P^T$ and thereby \mathbf{m} .

→ In its original paper Niederreiter proposed the class of GRS codes over \mathbb{F}_{2^m} .



H. Niederreiter.

Knapsack-type crypto system and algebraic coding theory.

Problems of Control and Information Theory, 1986.



Y. Xing Li, R. H. Deng and X. Mei Wang.

On the equivalence of McEliece's and Niederreiter public-key cryptosystems.

IEEE Transaction on Information Theory, 1994.

PKC USING ALGEBRAIC-GEOMETRY CODES

VULNERABILITIES OF CODE-BASED CRYPTOGRAPHY

INTRODUCTION

McELIECE CRYPTOSYSTEM

ATTACKS ON THE McELIECE PKC

NIEDERREITER CRYPTOSYSTEM

PKC USING ALGEBRAIC-GEOMETRY CODES

GAPS OF A CODE

GRS SUBCODES OF GRS CODES

THE SQUARE OF A CODE

PROOFS

- **Sidelnikov and Shestakov** in 1992 introduced an algorithm that breaks the original Niederreiter cryptosystem in polynomial time.

GRS codes are Algebraic Geometry codes on the projective line.

- This result was generalized to curves of genus 1 and 2 by **Faure and Minder** in 2008.
- In 1996 **Janwa and Moreno** propose to use AG code for the McEliece cryptosystem.
- For $g > 2$ the security status was not known.



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



V. M. Sidelnikov and S. O. Shestakov.
On insecurity of cryptosystems based on generalized Reed-Solomon codes.
Discrete mathematics and Applications.



H. Janwa and O. Moreno.
McEliece public crypto system using algebraic-geometric codes.
Designs, Codes and Cryptography, 8:293-307, 1996.

PKC USING ALGEBRAIC-GEOMETRY CODES

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

McELIECE CRYPTOSYSTEM

ATTACKS ON THE McELIECE PKC

NIEDERREITER CRYPTOSYSTEM

PKC USING
ALGEBRAIC-GEOMETRY CODES

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

WAG AND SAG CODES

A code \mathcal{C} over \mathbb{F}_q is called **WAG** if $\mathcal{C} = \mathcal{C}_L(\mathcal{X}, P, E)$ where:

- \mathcal{X} is an algebraic curve over \mathbb{F}_q with genus g ,
- $P = \{P_1, \dots, P_n\}$ is an n -tuple of mutually distinct points of $\mathcal{X}(\mathbb{F}_q)$,
- E is a divisor on \mathcal{X} with $\text{supp}(E) \cap P = \emptyset$ and $\text{deg}(E) = m$

→ If $2g - 2 < m < n$ then it is called **SAG**.

→ Let $R = \frac{k}{n}$ be the **information rate** and $\gamma = \frac{g}{n}$ the **relative genus** then:

SAG codes are **not secure** for code based PKC:

1 If $\frac{1}{6} \leq \gamma \leq \frac{1}{4}$ in the range:

$$\gamma \leq R \leq 1 - 3\gamma \quad \text{or} \quad 3\gamma \leq R \leq 1 - \gamma$$

2 If $\gamma \leq \frac{1}{6}$ in the range: $\gamma \leq R \leq 1 - \gamma$



I. Márquez-Corbella, E. Martínez-Moro and R. Pellikaan.

Evaluation of Public-Key Cryptosystems Based on Algebraic Geometry Codes.

Proceedings of the III International Castle Meeting on Coding Theory and Applications, September 11-15, Castell de Cardona, Spain, 2011.

PKC USING ALGEBRAIC-GEOMETRY CODES

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

McELIECE CRYPTOSYSTEM

ATTACKS ON THE McELIECE PKC

NIEDERREITER CRYPTOSYSTEM

PKC USING
ALGEBRAIC-GEOMETRY CODES

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

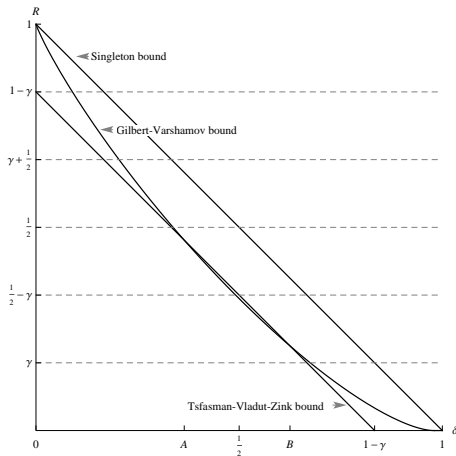


FIGURE: Bounds on R as a function of the relative minimum distance δ for $q = 49$ and $\gamma = \frac{1}{6}$.

PKC USING ALGEBRAIC-GEOMETRY CODES

VULNERABILITIES OF CODE-BASED CRYPTOGRAPHY

INTRODUCTION

McELIECE CRYPTOSYSTEM

ATTACKS ON THE McELIECE PKC

NIEDERREITER CRYPTOSYSTEM

PKC USING ALGEBRAIC-GEOMETRY CODES

GAPS OF A CODE

GRS SUBCODES OF GRS CODES

THE SQUARE OF A CODE

PROOFS

- **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:**

- 1 **Wieschebrink:**

- 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 $[n, k]$ is itself a GRS code of dimension $2k - 1$ then we can apply Sidelnikov-Shestakov attack.

- 2 **M-Mártinez-Pellikaan:** Give a characterization of the possible parameters that should be used to avoid attacks on the Berger-Loidreau cryptosystem.



T. Berger and P. Loidreau.

How to mask the structure of codes for a cryptographic use.

Designs, Codes and Cryptography, 35: 63–79, 2005.



I. Márquez-Corbella, E. Martínez-Moro and R. Pellikaan.

The non-gap sequence of a subcode of a generalized Reed-Solomon code.

Proceedings of the Seventh International Workshop on Coding and Cryptography, April 11-15, Paris, France, 183-193, 2011.



C. Wieschebrink.

An attack on the modified Niederreiter encryption scheme.

In PKC 2006, Lecture Notes in Computer Science, volume 3958, 14–26, Berlin, 2006. Springer.



C. Wieschebrink.

Cryptoanalysis of the Niederreiter public key scheme based on GRS subcodes.

In Post-Quantum Cryptography, Lecture Notes in Computer Science, volume 6061, 6–72, Berlin, 2010. Springer.

NOTATION

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

Let :

- \mathbb{F}_q be a finite field with q elements.
- $n, k, l \in \mathbb{N} : 1 \leq l \leq k \leq n \leq q$.
- $L_k := \{f \in \mathbb{F}_q[X] : \deg(f(X)) \leq k - 1\}$.
- $\text{ev}_{\mathbf{a}, \mathbf{b}}$ be the **evaluation map** at the elements $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ i.e.

$$\text{ev}_{\mathbf{a}, \mathbf{b}} : \begin{array}{l} L_k \rightarrow \\ f \mapsto \end{array} \begin{array}{l} \mathbb{F}_q^n \\ (f(a_1)b_1, \dots, f(a_n)b_n) \end{array}$$

GENERALIZED REED-SOLOMON CODES (OR GRS CODES)

Let $\mathbf{a} \in \mathbb{F}_q^n$ such that $a_i \neq a_j$ for $1 \leq i < j \leq n$ and $\mathbf{b} \in \mathbb{F}_q^n$ with non-zero entries. The **GRS** code $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ is defined by:

$$\text{GRS}_k(\mathbf{a}, \mathbf{b}) := \{\text{ev}_{\mathbf{a}, \mathbf{b}}(f(X)) : f \in L_k\}$$

We define the **star product** $\mathbf{a} * \mathbf{b} \in \mathbb{F}_q^n$ by $\mathbf{a} * \mathbf{b} = (a_1 \cdot b_1, \dots, a_n \cdot b_n)$.

REMARK

- $\text{GRS}_k(\mathbf{a}, \mathbf{b}) = \mathbf{b} * \text{GRS}_k(\mathbf{a}, \mathbf{1})$.
- $\text{ev}_{\mathbf{a}, \mathbf{b}}(f(X)g(X)) = \text{ev}_{\mathbf{a}, \mathbf{1}}(f(X)) * \text{ev}_{\mathbf{a}, \mathbf{b}}(g(X))$.

(a, b)-GAP OF A CODE

Let \mathcal{C} be an l -dimensional subcode of the code $\text{GRS}_k(\mathbf{a}, \mathbf{b})$, we denote by

$$\mathcal{C}_i := \mathcal{C} \cap \text{GRS}_i(\mathbf{a}, \mathbf{b}).$$

Then $\mathcal{C}_0 \subseteq \mathcal{C}_1 \subseteq \dots \subseteq \mathcal{C}_k = \mathcal{C} \cap \text{GRS}_k(\mathbf{a}, \mathbf{b}) = \mathcal{C}$.

(a, b)-GAP OF THE CODE

$i \in \mathbb{Z}_{\geq 0}$ is called an **(a, b)-gap** of the code \mathcal{C} if $\mathcal{C}_i = \mathcal{C}_{i+1}$.

We define the **associated (a, b) non-gap sequence** of \mathcal{C} by

$$\mathcal{I}(\mathbf{a}, \mathbf{b}, \mathcal{C}) = \mathcal{I}(\mathcal{C}) = \{i \in \mathbb{Z}_{\geq 0} : i \text{ is a non-gap of } \mathcal{C}\}$$

PROPOSITION 1 ◀ Proof

$i \in \mathbb{Z}_{\geq 0}$ is an **(a, b) non-gap** of \mathcal{C} $\iff \exists f \in \mathbb{F}_q[X]$ with $\deg(f(X)) = i$
such that $\text{ev}_{\mathbf{a}, \mathbf{b}}(f(X)) \in \mathcal{C}$

COROLLARY 1

Let \mathcal{C} be an l -dimensional subcode of the code $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ with associated non-gap sequence $\mathcal{I}(\mathcal{C})$. Then:

- 1 $\mathcal{I}(\mathcal{C}) = \{i \mid \exists f \in \mathbb{F}_q[X]$ with $\deg(f(X)) = i < k : \text{ev}_{\mathbf{a}, \mathbf{b}}(f(X)) \in \mathcal{C}\}$
- 2 $\mathcal{C} = \{\text{ev}_{\mathbf{a}, \mathbf{b}}(f(X)) \mid f = 0 \text{ or } f \in \mathbb{F}_q[X] \text{ and } \deg(f(x)) \in \mathcal{I}(\mathcal{C})\}$

(a, b)-GAP OF A CODE

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

We can obtain a basis of \mathcal{C} by studying the associated (\mathbf{a}, \mathbf{b}) non-gap sequence of \mathcal{C} .

PROPOSITION 2 ◀ Proof

There is a set $\mathcal{I} = \{i_1, \dots, i_l\}$ and there are l polynomials in unique normal form

$$f_j(X) = X^{i_j} + \sum_{\substack{s < i_j \\ s \notin \mathcal{I}}} f_{j,s} X^s \in \mathbb{F}_q[X], \text{ for all } j = 1, \dots, l,$$

such that

$$\mathcal{C} = \langle \text{ev}_{\mathbf{a}, \mathbf{b}}(f_j(X)) \mid j = 1, \dots, l \rangle.$$

Furthermore $\mathcal{I}(\mathcal{C}) = \mathcal{I}$ and $\dim(\mathcal{C}) = |\mathcal{I}(\mathcal{C})|$.

PROPOSITION 3 ◀ Proof

Let $\mathcal{I} = \{i_1, \dots, i_l\}$ and

$$e(\mathcal{I}) = i_1 l + (i_2 - i_1 - 1)(l - 1) + \dots + (i_l - i_{l-1} - 1) = \sum_{s=1}^l (i_s - i_{s-1} - 1)(l - s + 1)$$

where $i_0 = -1$. Then **the number of l -dimensional subcodes of the code $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ over \mathbb{F}_q with a given non-gap sequence \mathcal{I} is equal to $q^{e(\mathcal{I})}$.**

(\mathbf{a}, \mathbf{b}) -GAP OF A CODE

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

REMARK

- $e(\mathcal{I})$ is minimal and equal to 0 for $\mathcal{I} = \{0, 1, \dots, l-1\}$.
- $e(\mathcal{I})$ is maximal and equal to $l(k-l)$ for $\mathcal{I} = \{k-l, \dots, k-1\}$.

→ The number of l -dimensional subcodes of the code $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ over \mathbb{F}_q is equal to the Gaussian binomial:

$$\frac{(q^k - 1)(q^k - q) \cdots (q^k - q^{l-1})}{(q^l - 1)(q^l - q) \cdots (q^l - q^{l-1})} := \begin{bmatrix} k \\ l \end{bmatrix}_q = \sum_{\substack{\mathcal{I} \subseteq \{0, \dots, k-1\} \\ |\mathcal{I}|=l}} q^{e(\mathcal{I})}.$$

→ This number is polynomial in q with non-negative integers as coefficients.

GRS SUBCODES OF GRS CODES I

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

We study the l -dimensional subcodes \mathcal{C} of the code $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ that are themselves GRS codes.

$$\mathbf{1} \quad \mathcal{C} = \text{GRS}_l(\mathbf{a}, \mathbf{b}) \text{ with } 2 \leq l \leq k.$$

PROPOSITION 4 ◀ Proof

$$\mathcal{C} = \text{GRS}_l(\mathbf{a}, \mathbf{b}) \iff \mathcal{I}(\mathcal{C}) = \{0, \dots, l-1\}$$

There is exactly **ONE** l -dimensional subcode \mathcal{C} with $\mathcal{I}(\mathcal{C}) = \{0, \dots, l-1\}$ which is $\text{GRS}_l(\mathbf{a}, \mathbf{b})$.

$$\mathbf{2} \quad \mathcal{C} = \text{GRS}_l(\mathbf{a}, \mathbf{a}^i * \mathbf{b}) \text{ with } i + l \leq k.$$

PROPOSITION 5 ◀ Proof

Let $\mathcal{I}(\mathcal{C}) = \{i_1, \dots, i_l\}$ and $\mathbf{c} = \text{ev}_{\mathbf{a}}(f(X))$ with $f \in \mathbb{F}_q[X]$ and $\deg(f(X)) = i$. If $i + i_j < k$ then $\mathcal{I}(\mathbf{c} * \mathcal{C}) = i + \mathcal{I}(\mathcal{C})$.

Note that the converse is not true in general.

COROLLARY 3

If $i + l \leq k$ then $\mathcal{I}(\text{GRS}_l(\mathbf{a}, \mathbf{a}^i * \mathbf{b})) = \{i, i+1, \dots, i+l-1\}$.

GRS SUBCODES OF GRS CODES II

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

$$\mathbf{3} \quad \mathcal{C} = \text{GRS}_l(\mathbf{c}, \mathbf{d}).$$

PROPOSITION 6 ◀ Proof

Let $l \geq 2$, $\mathbf{a} \in \mathbb{F}_q^n : a_i \neq a_j \text{ with } 1 \leq i < j \leq n$, $\mathbf{b} \in \mathbb{F}_q^n : b_i \neq 0 \text{ with } 1 \leq i \leq n$,
 $g_0, h_1 \in \mathbb{F}_q[X]$, $d_0 = \deg(g_0(X))$, $d_1 = d_0 + \deg(h_1(X))$

If $\mathbf{1} \quad \text{ev}_{\mathbf{a}}(h_1(X)) = \mathbf{c} : c_i \neq c_j \text{ with } 1 \leq i < j \leq n$, $\mathbf{3} \quad d_0 < d_1$
 $\mathbf{2} \quad \text{ev}_{\mathbf{a}, \mathbf{b}}(g_0(X)) = \mathbf{d} : d_i \neq 0 \text{ with } 1 \leq i \leq n$, $\mathbf{4} \quad d_0 + (l-1)(d_1 - d_0) < k$.

Then the code $\mathcal{C} = \text{GRS}_l(\mathbf{c}, \mathbf{d})$ is an l -dimensional subcode of $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ with :

$$\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{d_0, d_1, \dots, d_0 + j(d_1 - d_0), \dots, d_0 + (l-1)(d_1 - d_0)\}$$

PROPOSITION 7 ◀ Proof

If $2k - 2 < n$ and $l \geq 2$.

Assume that $\mathcal{C} = \text{GRS}_l(\mathbf{c}, \mathbf{d}) \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{b})$ and let $d_0 < d_1$ be the first two elements of $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b})$. Then $\exists g_0, h_1 \in \mathbb{F}_q[X]$ such that:

$\mathbf{1} \quad \text{ev}_{\mathbf{a}, \mathbf{b}}(g_0(X)) = \mathbf{d}$. $\mathbf{3} \quad d_0 = \deg(g_0(X))$.
 $\mathbf{2} \quad \text{ev}_{\mathbf{a}}(h_1(X)) = \mathbf{c}$. $\mathbf{4} \quad d_1 = d_0 + \deg(h_1(X))$.

GRS SUBCODES OF GRS CODES III

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

COROLLARY 5 ◀ Proof

If $2k - 2 < n$ and $2 \leq l \leq k$. Then the number of l -dimensional subcodes of the code $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ over \mathbb{F}_q that are GRS code is at most q^{k-l+3} .

The probability that an arbitrary l -dimensional subcode of the code $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ is a GRS code is at most

$$\frac{q^{k-l+3}}{\begin{bmatrix} k \\ l \end{bmatrix}_q} \leq \frac{q^{k-l+3}}{q^{l(k-l)}} = q^{-(l-1)(k-l)+3}$$

This fraction tends to zero for $k \rightarrow \infty$ or $(k-l) \rightarrow \infty$.

THE SQUARE OF A CODE

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

THE SQUARE CODE

The **square code** of a $[n, k]$ code \mathcal{C} over \mathbb{F}_q , $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle$, is the code generated by

$$\{\mathbf{r}_i * \mathbf{r}_j : 1 \leq i \leq j \leq k\}$$

where $\mathbf{r}_1, \dots, \mathbf{r}_k$ denotes the rows of a generator matrix of \mathcal{C} .

Let:

- \mathcal{C} be an l -dimensional subcode of $\text{GRS}_k(\mathbf{a}, \mathbf{b})$.
- $\mathbf{r}_1, \dots, \mathbf{r}_l$ be the rows of a generator matrix of \mathcal{C} .
- f_1, \dots, f_l be the polynomials associated to those rows.

Then

$$\mathbf{r}_i * \mathbf{r}_j = (b_1^2 f_i(a_1) f_j(a_1), \dots, b_n^2 f_i(a_n) f_j(a_n)) = \text{ev}_{\mathbf{a}, \mathbf{b} * \mathbf{b}}(f_i(X) f_j(X))$$

and $\deg(f_i(X) f_j(X)) = \deg(f_i(X)) + \deg(f_j(X)) \leq 2k - 2$ for $1 \leq i \leq j \leq l$

REMARK

The code $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle = \langle \mathbf{r}_i * \mathbf{r}_j : 1 \leq i \leq j \leq l \rangle$ is a subcode of the code $\text{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$.

$(\mathbf{a}, \mathbf{b} * \mathbf{b})$ GAP OF $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle$

We denote by $\mathcal{D}_i = \mathcal{D} \cap \text{GRS}_i(\mathbf{a}, \mathbf{b} * \mathbf{b})$.

Then:

- $i \in \mathbb{Z}_{\geq 0}$ is an $(\mathbf{a}, \mathbf{b} * \mathbf{b})$ gap of \mathcal{D} if $\mathcal{D}_i = \mathcal{D}_{i+1}$.
- $\mathcal{J}(\mathcal{D}, \mathbf{a}, \mathbf{b} * \mathbf{b}) = \{j \in \mathbb{Z}_{\geq 0} : j \text{ is an } (\mathbf{a}, \mathbf{b} * \mathbf{b})\text{-non gap of } \mathcal{D}\}$ is the $(\mathbf{a}, \mathbf{b} * \mathbf{b})$ non-gap sequence associated to the square code.

REMARK

$$j \in \mathcal{J}(\mathcal{D}, \mathbf{a}, \mathbf{b} * \mathbf{b}) \iff \exists g \in \mathbb{F}_q[X] \text{ with } \deg(g(X)) = j : \text{ev}_{\mathbf{a}, \mathbf{b} * \mathbf{b}}(g(X)) \in \mathcal{D}$$

PROPOSITION 8 ◀ Proof

$$\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) + \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{i + j : i, j \in \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b})\} \subseteq \mathcal{J}(\mathcal{D}, \mathbf{a}, \mathbf{b} * \mathbf{b})$$

Furthermore:

- 1 If $0 \in \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b})$ then $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) \subseteq \mathcal{J}(\mathcal{D}, \mathbf{a}, \mathbf{b} * \mathbf{b})$
- 2 Let $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{i_1, \dots, i_l\}$ with $i_1 + i_l < 2k - 1$ and $\mathbf{c} = \text{ev}_{\mathbf{a}, \mathbf{b}}(f(X)) \in \mathcal{C}$ for $f \in \mathbb{F}_q[X]$ with $\deg(f(X)) = i_1$ then

$$\mathcal{I}(\mathbf{c} * \mathcal{C}, \mathbf{a}, \mathbf{b}) = i_1 + \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) \subseteq \mathcal{J}(\mathcal{D}).$$

THE SQUARE CODE

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

PROPOSITION 9 ◀ Proof

$$\dim(\mathcal{D}) \leq \min \left\{ 2k - 1, \binom{l+1}{2} \right\}$$

Furthermore:

- 1 If $\mathcal{D} = \text{GRS}_r(\mathbf{a}, \mathbf{b} * \mathbf{b})$ then $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) \subseteq \{0, \dots, \lfloor \frac{r-1}{2} \rfloor\}$.
- 2 If $\mathcal{D} = \text{GRS}_r(\mathbf{a}, \mathbf{a}^i * \mathbf{b} * \mathbf{b})$ then $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) \subseteq \{\lfloor \frac{i}{2} \rfloor, \dots, \lfloor \frac{i+r-1}{2} \rfloor\}$.
- 3 If $\mathcal{D} = \text{GRS}_r(\mathbf{c}, \mathbf{d})$ then $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) \subseteq \{\lfloor \frac{d_0}{2} \rfloor, \dots, \lfloor \frac{d_0 + (r-1)(d_1 - d_0)}{2} \rfloor\}$ where $d_0 < d_1$ and $d_0 + (r-1)(d_1 - d_0) < 2k - 1$

THE SQUARE CODE OF A GRS CODE

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

Let \mathcal{C} be a GRS code then:

PROPOSITION 10 ◀ Proof

$$\langle \text{GRS}_k(\mathbf{a}, \mathbf{b}) * \text{GRS}_l(\mathbf{a}, \mathbf{c}) \rangle = \text{GRS}_{k+l-1}(\mathbf{a}, \mathbf{b} * \mathbf{c})$$

In particular $\text{GRS}_{2l-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$ is the square code of $\text{GRS}_l(\mathbf{a}, \mathbf{b})$.

COROLLARY 6

If $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{0, \dots, l-1\}$ then $\mathcal{J}(\mathcal{D}, \mathbf{a}, \mathbf{b} * \mathbf{b}) = \{0, \dots, 2l-2\}$ i.e.
 $\mathcal{D} = \text{GRS}_{2l-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$.

The converse is NOT true in general

WHEN $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle = \text{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$?

PROPOSITION 11 ◀ Proof

Let $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{i_1, \dots, i_l\}$. If $\mathcal{D} = \text{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$, then

$$|\{(u, v) : i_u + i_v \geq t \text{ and } 1 \leq u \leq v \leq l\}| \geq 2k - t - 1$$

for all $t = 0, \dots, 2k - 2$.

REMARK

Let \mathcal{C} be an l -dimensional subcode of $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ with $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{i_1, \dots, i_l\}$. If $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle = \text{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$ then:

- 1 $2k - 1 \leq \binom{l+1}{2}$ (Particular case $t = 0$ of [Proposition 11](#)).
- 2 $i_l = k - 1$ (Case $t = 2k - 2$ of [Proposition 11](#)).
- 3 $i_{l-1} = k - 2$ (Case $t = 2k - 3$ of [Proposition 11](#)).
- 4 $i_{l-2} \geq k - 4$ (Case $t = 2k - 5$ of [Proposition 11](#)).

REMARK

$\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{k - l, \dots, k - 1\}$ satisfies the conditions of [Proposition 11](#) for all t . However this not imply that $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle$ is exactly $\text{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$.

WHEN $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle = \text{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$?

Let \mathcal{C} be an l -dimensional subcode of $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ with $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{i_1, \dots, i_l\}$ then:

→ By **Proposition 2** there are l polynomials in normal form such that

$$\mathcal{C} = \langle \text{ev}_{\mathbf{a}, \mathbf{b}}(f_1(X)), \dots, \text{ev}_{\mathbf{a}, \mathbf{b}}(f_l(X)) \rangle \text{ with } \deg(f_j(X)) = i_j \forall j = 1, \dots, l$$

→ Furthermore

$$\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle = \langle \text{ev}_{\mathbf{a}, \mathbf{b}}(f_u(X)f_v(X)) \mid 1 \leq u \leq v \leq l \rangle$$

We denote $f_u(X)f_v(X) = g_{uv}(X) = g_{uv,0} + g_{uv,1}X + \dots + g_{uv,(2k-2)}X^{2k-2}$ for $1 \leq u \leq v \leq l$.

→ Then the following matrix form a generating set of the code \mathcal{D} :

$$G_{\mathcal{D}} = \begin{pmatrix} g_{11,0} & g_{11,1} & \dots & g_{11,2k-2} \\ \vdots & \vdots & \ddots & \vdots \\ g_{1l,0} & g_{1l,1} & \dots & g_{1l,2k-2} \\ g_{22,0} & g_{22,1} & \dots & g_{22,2k-2} \\ \vdots & \vdots & \ddots & \vdots \\ g_{2l,0} & g_{2l,1} & \dots & g_{2l,2k-2} \\ \vdots & \vdots & \ddots & \vdots \\ g_{ll,0} & g_{ll,1} & \dots & g_{ll,2k-2} \end{pmatrix} \in \mathbb{F}_q^{\binom{l+1}{2} \times (2k-1)}$$

NECESSARY CONDITIONS TO HAVE:

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

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

FINAL REMARK

The following properties are necessary conditions to have that

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

- 1 $\mathcal{I}(\mathcal{C}) = \{i_1, \dots, i_l\} \subseteq \{0, \dots, k-1\}$.
- 2 $i_l = k-1$, $i_{l-1} = k-2$ and $i_{l-2} \geq k-4$.
- 3 $\text{rank}(G_{\mathcal{D}}) = 2k-1$.

WHEN $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle = \text{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$?

If $2k - 1 \leq n$ then:

$$\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle = \text{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b}) \iff \text{rank}(G_{\mathcal{D}}) = 2k - 1$$

- Almost all l dimensional subcodes \mathcal{C} of $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ have the property that:

$$\mathcal{I}(\mathcal{C}) = \{k - l, \dots, k - 1\} \quad \text{for } q \gg k.$$

PROPOSITION 12 ◀ Proof

If $4k - 3l - 1 < q$ then the number of l -dimensional subcodes \mathcal{C} of $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ over \mathbb{F}_q such that

$$2k - 1 \leq n, \quad 2k - 1 \leq \binom{l+1}{2} \quad \text{and} \quad \mathcal{I}(\mathcal{C}) = \{k - l, \dots, k - 1\}$$

is at most $(4k - 3l - 2)q^{l(k-l)-1}$.

If $4k - 3l - 1 < q$, $2k - 1 \leq n$ and $2k - 1 \leq \binom{l+1}{2}$ then the **sought probability** is at least:

$$1 - \frac{(4k - 3l - 2)q^{l(k-l)-1}}{q^{l(k-l)}} = 1 - \frac{4k - 3l - 2}{q}$$

This fraction tends to one for $q \rightarrow \infty$.

THANK FOR YOUR ATTENTION

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS



PROPOSITION 1

VULNERABILITIES OF CODE-BASED CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS CODES

THE SQUARE OF A CODE

PROOFS

PROPOSITION 1

PROPOSITION 2

PROPOSITION 3

PROPOSITION 4

PROPOSITION 5

PROPOSITION 6

PROPOSITION 7

PROPOSITION 8

PROPOSITION 9

PROPOSITION 10

PROPOSITION 11

PROPOSITION 12

COROLLARY 5

PROPOSITION 1 ◀ Return

$i \in \mathbb{Z}_{\geq 0}$ is an (\mathbf{a}, \mathbf{b}) non-gap of \mathcal{C} \iff $\exists f \in \mathbb{F}_q[X]$ with $\deg(f(X)) = i$
such that $\text{ev}_{\mathbf{a}, \mathbf{b}}(f(X)) \in \mathcal{C}$

\Rightarrow Suppose that $i \in \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b})$ then by definition $\mathcal{C}_i \neq \mathcal{C}_{i+1}$. That is

$$\exists \mathbf{c} \in \mathcal{C}_{i+1} \setminus \mathcal{C}_i \Rightarrow \begin{cases} \mathbf{c} \in \mathcal{C} \\ \mathbf{c} \in \text{GRS}_{i+1}(\mathbf{a}, \mathbf{b}) \setminus \text{GRS}_i(\mathbf{a}, \mathbf{b}) \end{cases}$$

i.e. there exists a unique polynomial $f \in L_{i+1} : \mathbf{c} = \text{ev}_{\mathbf{a}, \mathbf{b}}(f(X))$

But if $\deg(f(X)) < i$ then $\mathbf{c} \in \mathcal{C}_i$, thus $\deg(f(X)) = i$.

\Leftarrow If $\exists f \in \mathbb{F}_q[X]$ with $\deg(f(X)) = i$ such that $\mathbf{c} = \text{ev}_{\mathbf{a}, \mathbf{b}}(f(X))$ then $\mathbf{c} \in \mathcal{C}_{i+1} \setminus \mathcal{C}_i$.
Hence $i \in \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b})$.

PROPOSITION 2 [Return](#)

- By Corollary 1, $\forall \mathbf{c} \in \mathcal{C}$, $\exists f \in \mathbb{F}_q[X]$ with $\deg(f(X)) \in \mathcal{I}(\mathcal{C})$: $\mathbf{c} = \text{ev}_{\mathbf{a},\mathbf{b}}(f(X))$.
- Furthermore the code \mathcal{C} has dimension l ,
i.e. $\exists f_1, \dots, f_l \in \mathbb{F}_q[X]$ with $\deg(f_i(X)) \in \mathcal{I}(\mathcal{C})$ for $i \in \{1, \dots, l\}$ such that
$$\mathcal{C} = \langle \text{ev}_{\mathbf{a},\mathbf{b}}(f_i(X)) \text{ with } i \in \{1, \dots, l\} \rangle.$$

To make the notation easier we can assume that:

- 1 $\deg(f_j(X)) = i_j$ for $j \in \{1, \dots, l\}$.
- 2 $\deg(f_1(X)) \leq \dots \leq \deg(f_l(X))$, i.e. $\mathcal{I} = \{i_1, \dots, i_l\}$.
- 3 The polynomials f_1, \dots, f_l are monics.

Thus each polynomial f_j can be written as

$$f_j(X) = \sum_{s=0}^{i_j-1} f_{j,s} X^s + X^{i_j} \text{ for } j = 1, \dots, l.$$

Let us define the matrix $M(f_1, \dots, f_l) = (f_{j,s}) \in \mathbb{F}_q^{l \times k}$ as the matrix whose i -th row represent the coefficients with respect to the monomials $\{1, X, \dots, X^{k-1}\}$ of the polynomial f_j for $j \in \{1, \dots, l\}$. After applying Gaussian elimination on the previous matrix we obtain a matrix with the following form:

$$\begin{pmatrix} *1,0 & \cdots & *1,i_1-1 & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ *2,0 & \cdots & *2,i_1-1 & 0 & *2,i_1+1 & \cdots & *2,i_2-1 & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ *l,0 & \cdots & *l,i_1-1 & 0 & *l,i_1+1 & \cdots & *l,i_2-1 & 0 & \cdots & 0 \end{pmatrix}. \quad (1)$$

From the above matrix we can conclude the result of the [Theorem](#).

PROPOSITION 4

Return

VULNERABILITIES OF CODE-BASED CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

PROPOSITION 1

PROPOSITION 2

PROPOSITION 3

PROPOSITION 4

PROPOSITION 5

PROPOSITION 6

PROPOSITION 7

PROPOSITION 8

PROPOSITION 9

PROPOSITION 10

PROPOSITION 11

PROPOSITION 12

COROLLARY 5

\Rightarrow If $\mathcal{C} = \text{GRS}_l(\mathbf{a}, \mathbf{b})$ by definition $\mathcal{I}(\mathcal{C}) = \{0, \dots, l-1\}$

\Leftarrow Suppose that the associated non-gap sequence of \mathcal{C} is $\mathcal{I}(\mathcal{C}) = \{0, \dots, l-1\}$
i.e. by Proposition 2 $\{e_{\mathbf{a}, \mathbf{b}}(X^i) \text{ with } i \in \{0, \dots, l-1\}\}$ form a basis of \mathcal{C}
which is also a basis of $\text{GRS}_l(\mathbf{a}, \mathbf{b})$.
Thus $\mathcal{C} = \text{GRS}_l(\mathbf{a}, \mathbf{b})$.

REMARK

If $\mathcal{I} = \{0, \dots, l-1\}$ then $e(\mathcal{I}) = 0$, thus there exists exactly **ONE** l -dimensional subcode \mathcal{C} of the code $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ with $\mathcal{I}(\mathcal{C}) = \{0, \dots, l-1\}$.
And by Proposition 4 we have that $\mathcal{C} = \text{GRS}_l(\mathbf{a}, \mathbf{b})$.

PROPOSITION 5 [Return](#)

VULNERABILITIES OF CODE-BASED CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

PROPOSITION 1

PROPOSITION 2

PROPOSITION 3

PROPOSITION 4

PROPOSITION 5

PROPOSITION 6

PROPOSITION 7

PROPOSITION 8

PROPOSITION 9

PROPOSITION 10

PROPOSITION 11

PROPOSITION 12

COROLLARY 5

Suppose that $\mathcal{I}(\mathcal{C}) = \{i_1, \dots, i_l\}$, then there are l polynomials in normal form

$$f_j(X) = \sum_{\substack{s < i_j \\ s \notin \mathcal{I}}}^{i_j-1} f_{j,s} X^s + X^{i_j} \text{ for } j = 1, \dots, l.$$

such that

$$\mathcal{C} = \langle \text{ev}_{\mathbf{a}, \mathbf{b}}(f_i(X)) \text{ with } i \in \{1, \dots, l\} \rangle.$$

Since $\mathbf{c} = \text{ev}_{\mathbf{a}}(f(X))$ with $f \in \mathbb{F}_q[X]$ and $\deg(f(X)) = i$. Then:

$$\mathbf{c} * \text{ev}_{\mathbf{a}, \mathbf{b}}(f_j(X)) = \text{ev}_{\mathbf{a}, \mathbf{b}}(f(X)f_j(X))$$

with $\deg(f(X)f_j(X)) = i + i_j \leq i + i_l < k$ for all $j \in \{1, \dots, l\}$.

Hence

$$\mathbf{c} * \mathcal{C} = \langle \text{ev}_{\mathbf{a}, \mathbf{b}}(f(X)f_j(X)) \text{ with } j \in \{1, \dots, l\} \rangle \subseteq \text{GRS}_{i+i_l+1}(\mathbf{a}, \mathbf{b})$$

That is $\{i + i_1, \dots, i + i_l\} = i + \mathcal{I}(\mathcal{C}) \subseteq \mathcal{I}(\mathbf{c} * \mathcal{C})$.

Since $\mathbf{c} * \mathcal{C}$ has dimension l then $|\mathcal{I}(\mathbf{c} * \mathcal{C})| = l$, thus

$$\mathcal{I}(\mathbf{c} * \mathcal{C}) = i + \mathcal{I}(\mathcal{C}).$$

PROPOSITION 6

[Return](#)

VULNERABILITIES OF CODE-BASED CRYPTOGRAPHY

[INTRODUCTION](#)[GAPS OF A CODE](#)[GRS SUBCODES OF GRS
CODES](#)[THE SQUARE OF A CODE](#)[PROOFS](#)[PROPOSITION 1](#)[PROPOSITION 2](#)[PROPOSITION 3](#)[PROPOSITION 4](#)[PROPOSITION 5](#)[PROPOSITION 6](#)[PROPOSITION 7](#)[PROPOSITION 8](#)[PROPOSITION 9](#)[PROPOSITION 10](#)[PROPOSITION 11](#)[PROPOSITION 12](#)[COROLLARY 5](#)

Let us define $g_j(X) = g_0(X) (h_1(X))^j$ with $j \in \{0, \dots, l-1\}$.

Then $0 \leq \deg(g_j(X)) = d_0 + j(d_1 - d_0) < k$ for all $j \in \{0, \dots, l-1\}$.

Thus the degree of $g_j(X)$ is strictly increasing with j , (since $d_0 < d_1$).

Furthermore

$$\text{ev}_{\mathbf{a}, \mathbf{b}}(g_j(X)) = \text{ev}_{\mathbf{a}, \mathbf{b}}(g_0(X)) * (\text{ev}_{\mathbf{a}}(h_1(X)))^j = \mathbf{d} * \mathbf{c}^j$$

i.e. the code $\text{GRS}_l(\mathbf{c}, \mathbf{d})$ has $\text{ev}_{\mathbf{a}, \mathbf{b}}(g_j(X))$ with $j \in \{0, \dots, l-1\}$ as a basis.

That is $\text{GRS}_l(\mathbf{c}, \mathbf{d})$ is an l -dimensional subcode of the code $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ and

$$\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{d_0, d_1, d_0 + 2(d_1 - d_0), \dots, d_0 + (l-1)(d_1 - d_0)\}$$

PROPOSITION 7

[Return](#)

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

PROPOSITION 1

PROPOSITION 2

PROPOSITION 3

PROPOSITION 4

PROPOSITION 5

PROPOSITION 6

PROPOSITION 7

PROPOSITION 8

PROPOSITION 9

PROPOSITION 10

PROPOSITION 11

PROPOSITION 12

COROLLARY 5

Let us assume that $\mathcal{C} = \text{GRS}_k(\mathbf{c}, \mathbf{d})$ is an l -dimensional subcode of $\text{GRS}_k(\mathbf{a}, \mathbf{b})$, i.e. $\exists g_j \in \mathbb{F}_q[X] : \text{ev}_{\mathbf{a}, \mathbf{b}}(g_j(X)) = \text{ev}_{\mathbf{c}, \mathbf{d}}(X^j)$ with $j \in \{0, \dots, l-1\}$.
Hence:

$$\begin{aligned} \mathbf{b} * \text{ev}_{\mathbf{a}, \mathbf{b}}(g_i(X)g_j(X)) &= \text{ev}_{\mathbf{a}, \mathbf{b}}(g_i(X)) * \text{ev}_{\mathbf{a}, \mathbf{b}}(g_j(X)) \\ &= \text{ev}_{\mathbf{c}, \mathbf{d}}(X^i) * \text{ev}_{\mathbf{c}, \mathbf{d}}(X^j) = \mathbf{d} * \text{ev}_{\mathbf{c}, \mathbf{d}}(X^{i+j}) \end{aligned}$$

So $\text{ev}_{\mathbf{a}, \mathbf{b}}(g_i(X)g_j(X)) = \text{ev}_{\mathbf{a}, \mathbf{b}}(g_u(X)g_v(X))$, i.e. $g_i(X)g_j(X) = g_u(X)g_v(X)$ with $0 \leq i, j, u, v \leq l$ such that $i+j = u+v$.
In particular we have that

$$g_0^{j-1}(X)g_j(X) = g_1^j(X) \quad (2)$$

$$g_0(X)g_2(X) = g_1(X)g_1(X) \quad (3)$$

From Equation 3 we can deduce that $\exists h_1 \in \mathbb{F}_q[X]$ such that $g_1(X) = g_0(X)h_1(X)$.

That is $g_j(X) = g_0(X)h_1^j(X)$.

And this imply that

$$\mathbf{d} * \mathbf{c}^j = \text{ev}_{\mathbf{c}, \mathbf{d}}(X^j) = \text{ev}_{\mathbf{a}, \mathbf{b}}(g_j(X)) = \text{ev}_{\mathbf{a}, \mathbf{b}}(g_0(X)) * \text{ev}_{\mathbf{a}}(h_1(X))^j$$

1 If $j = 0$ we deduce that $\mathbf{d} = \text{ev}_{\mathbf{a}, \mathbf{b}}(g_0(X))$.

2 If $j = 1$ we deduce that $\mathbf{c} = \text{ev}_{\mathbf{a}}(h_1(X))$.

Let $\hat{d}_0 = \deg(g_0(X))$ and $\hat{d}_1 = \hat{d}_0 + \deg(h_1(X))$. Then the (\mathbf{a}, \mathbf{b}) non-gap sequence of \mathcal{C} is

$$\hat{d}_0, \hat{d}_1, \hat{d}_0 + 2(\hat{d}_1 - \hat{d}_0), \dots, \hat{d}_0 + (l-1)(\hat{d}_1 - \hat{d}_0).$$

Therefore $\hat{d}_0 = d_0$ and $\hat{d}_1 = d_1$.

PROPOSITION 8 ◀ Return

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

PROPOSITION 1

PROPOSITION 2

PROPOSITION 3

PROPOSITION 4

PROPOSITION 5

PROPOSITION 6

PROPOSITION 7

PROPOSITION 8

PROPOSITION 9

PROPOSITION 10

PROPOSITION 11

PROPOSITION 12

COROLLARY 5

If $i_1 + i_2 \in \mathcal{I}(\mathcal{C}) + \mathcal{I}(\mathcal{C}) \Rightarrow$

$$\begin{cases} i_1 \in \mathcal{I}(\mathcal{C}) & \xRightarrow{\text{Prop.1}} \exists f_1 \in \mathbb{F}_q[X] \text{ with } \deg(f_1(X)) = i_1 : \text{ev}_{\mathbf{a},\mathbf{b}}(f_1(X)) \in \mathcal{C} \\ i_2 \in \mathcal{I}(\mathcal{C}) & \xRightarrow{\text{Prop.1}} \exists f_2 \in \mathbb{F}_q[X] \text{ with } \deg(f_2(X)) = i_2 : \text{ev}_{\mathbf{a},\mathbf{b}}(f_2(X)) \in \mathcal{C} \end{cases}$$

Therefore:

$$\text{ev}_{\mathbf{a},\mathbf{b}}(f_1(X)) * \text{ev}_{\mathbf{a},\mathbf{b}}(f_2(X)) = \text{ev}_{\mathbf{a},\mathbf{b}*\mathbf{b}}(f_1(X)f_2(X)) \in \mathcal{D}$$

with $\deg(f_1(X)f_2(X)) = \deg(f_1(X)) + \deg(f_2(X)) = i_1 + i_2$

Thus $i_1 + i_2 \in \mathcal{J}(\mathcal{D})$.

COUNTEREXAMPLE: THE EQUALITY DOES NOT HOLD IN GENERAL

Consider $\mathcal{C} = \langle \text{ev}_{\mathbf{a},\mathbf{b}}(f_1), \dots, \text{ev}_{\mathbf{a},\mathbf{b}}(f_4) \rangle \subseteq \text{GRS}_5(\mathbf{a}, \mathbf{b})$ where

$$f_1 = 1, \quad f_2 = X^2 + X, \quad f_3 = X^3 \quad \text{and} \quad f_4 = X^4$$

Then:

$$\mathbf{1} \quad \mathcal{I}(\mathcal{C}) = \{0, 2, 3, 4\} \Rightarrow \mathcal{I}(\mathcal{C}) + \mathcal{I}(\mathcal{C}) = \{0, 2, 3, 4, 5, 6, 7, 8\}.$$

$$\mathbf{2} \quad 1 \in \mathcal{J}(\mathcal{D}) \text{ since}$$

$$X = f_1(X)f_2(X) - f_2^2(X) + f_1(X)f_4(X) + 2f_1(X)f_3(X) \in \langle \mathcal{C} * \mathcal{C} \rangle = \mathcal{D}.$$

But $1 \notin \mathcal{I}(\mathcal{C}) + \mathcal{I}(\mathcal{C})$.

In fact $\mathcal{J}(\mathcal{D}) = \{0, 1, \dots, 8\} \Rightarrow \mathcal{D} = \text{GRS}_9(\mathbf{a}, \mathbf{b})$.

PROPOSITION 9

Return

- Let g_1, \dots, g_l be a basis of \mathcal{C} . Then the elements $g_i * g_j$ with $1 \leq i \leq j \leq l$ generate \mathcal{D} . Therefore

$$\dim \mathcal{D} \leq \sum_{i=1}^l i = \binom{l+1}{2}.$$

- Since $\mathcal{D} \subseteq \text{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$ then $\dim \mathcal{D} \leq 2k - 1$

Furthermore:

- If $\mathcal{D} = \text{GRS}_r(\mathbf{a}, \mathbf{b}) \Rightarrow \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) \subseteq \{0, \dots, \lfloor \frac{r-1}{2} \rfloor\}$.
In fact since $\mathcal{D} = \text{GRS}_r(\mathbf{a}, \mathbf{b})$ then by Proposition 4:

$$\mathcal{J}(\mathcal{D}) = \{0, \dots, r-1\}$$

and by Proposition 8:

$$\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) + \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) \subseteq \mathcal{J}(\mathcal{D}, \mathbf{a}, \mathbf{b} * \mathbf{b}).$$

i.e. if $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{i_1, \dots, i_l\}$ then:

- $2i_1 = i_1 + i_1 \geq 0 \Rightarrow i_1 \geq 0$.
 - If $2i_l \leq 2k - 1$ then $2i_l = i_l + i_l \in \mathcal{J}(\mathcal{D}) \Rightarrow i_l \leq \lfloor \frac{r-1}{2} \rfloor$.
- Similarly to the previous procedure we can conclude 2 and 3.

PROPOSITION 10

[◀ Return](#)

VULNERABILITIES OF CODE-BASED CRYPTOGRAPHY

[INTRODUCTION](#)[GAPS OF A CODE](#)[GRS SUBCODES OF GRS
CODES](#)[THE SQUARE OF A CODE](#)[PROOFS](#)[PROPOSITION 1](#)[PROPOSITION 2](#)[PROPOSITION 3](#)[PROPOSITION 4](#)[PROPOSITION 5](#)[PROPOSITION 6](#)[PROPOSITION 7](#)[PROPOSITION 8](#)[PROPOSITION 9](#)[PROPOSITION 10](#)[PROPOSITION 11](#)[PROPOSITION 12](#)[COROLLARY 5](#)

Recall that the code $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ is generated by the elements $\text{ev}_{\mathbf{a}, \mathbf{b}}(X^i)$ with $i \in \{0, \dots, k-1\}$.

Thus the code $\langle \text{GRS}_k(\mathbf{a}, \mathbf{b}) * \text{GRS}_l(\mathbf{a}, \mathbf{c}) \rangle$ is generated by the elements:

$$\text{ev}_{\mathbf{a}, \mathbf{b}}(X^i) * \text{ev}_{\mathbf{a}, \mathbf{c}}(X^j) = \text{ev}_{\mathbf{a}, \mathbf{b} * \mathbf{c}}(X^{i+j})$$

with $i \in \{0, \dots, k-1\}$ and $j \in \{0, \dots, l-1\}$ i.e. $0 \leq i+j \leq k+l-2$.

Therefore the right hand side of the previous equality is a complete set of generators of the code $\text{GRS}_{k+l-1}(\mathbf{a}, \mathbf{b} * \mathbf{c})$.

PROPOSITION 11

[◀ Return](#)

VULNERABILITIES OF
CODE-BASED
CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS
CODES

THE SQUARE OF A CODE

PROOFS

PROPOSITION 1

PROPOSITION 2

PROPOSITION 3

PROPOSITION 4

PROPOSITION 5

PROPOSITION 6

PROPOSITION 7

PROPOSITION 8

PROPOSITION 9

PROPOSITION 10

PROPOSITION 11

PROPOSITION 12

COROLLARY 5

Let \mathcal{C} be an l -dimensional subcode of $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ with $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{i_1, \dots, i_l\}$. Then by Proposition 2 there are l polynomials in normal form

$$f_j(X) = X^{i_j} + \sum_{\substack{s < i_j \\ s \notin \mathcal{I}}} f_{j,s} X^s \in \mathbb{F}_q[X], \text{ for all } j = 1, \dots, l,$$

with $j \in \{1, \dots, l\}$ such that $\mathcal{C} = \langle \text{ev}_{\mathbf{a}, \mathbf{b}}(f_1(X)), \dots, \text{ev}_{\mathbf{a}, \mathbf{b}}(f_l(X)) \rangle$. Then the elements $\text{ev}_{\mathbf{a}, \mathbf{b} * \mathbf{b}}(f_u(X)f_v(X))$ with $1 \leq u \leq v \leq l$ generate the square code $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle$ where

$$\deg(f_u(X)f_v(X)) = \deg(f_u(X)) + \deg(f_v(X)) = i_u + i_v$$

Assume that $\mathcal{D} = \text{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$ i.e. the elements $\text{ev}_{\mathbf{a}, \mathbf{b} * \mathbf{b}}(X^j)$ with $0 \leq j \leq 2k - 2$ form a basis of \mathcal{D} .

Hence $\forall t \in \{0, \dots, 2k - 2\}, \exists (u, v) : i_u + i_v \geq t$ and $1 \leq u \leq v \leq l$.

Since $\text{ev}_{\mathbf{a}, \mathbf{b} * \mathbf{b}}(f_u(X)f_v(X)) \in \text{GRS}_t(\mathbf{a}, \mathbf{b} * \mathbf{b}) \Rightarrow i_u + i_v < t$ and $1 \leq u \leq v \leq l$.

Then the vector space $V_t = \text{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b}) \setminus \text{GRS}_t(\mathbf{a}, \mathbf{b} * \mathbf{b})$ is generated by the elements $\text{ev}_{\mathbf{a}, \mathbf{b} * \mathbf{b}}(f_u(X)f_v(X))$ with $i_u + i_v \geq t$ and $1 \leq u \leq v \leq l$, i.e.

$$\dim V_t = 2k - 1 - t.$$

Thus this is a lower bound of the number of elements that generates V_t .

PROPOSITION 12 ◀ Return I

VULNERABILITIES OF CODE-BASED CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS CODES

THE SQUARE OF A CODE

PROOFS

PROPOSITION 1

PROPOSITION 2

PROPOSITION 3

PROPOSITION 4

PROPOSITION 5

PROPOSITION 6

PROPOSITION 7

PROPOSITION 8

PROPOSITION 9

PROPOSITION 10

PROPOSITION 11

PROPOSITION 12

COROLLARY 5

Let \mathcal{C} be an l -dimensional subcode of $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ such that

$$2k - 1 \leq n, \quad 2k - 1 \leq \binom{l+1}{2} \quad \text{and} \quad \mathcal{I}(\mathcal{C}) = \{k - l, \dots, k - 1\}$$

By **Proposition 2** there are l polynomials $f_j \in L_k$ in normal form that generates \mathcal{C} such that:

$$f_u(X) = X^{k-l-1+u} + \bar{f}_u(X) \quad \text{with} \quad \deg(\bar{f}_u(X)) \leq k - l - 1 \quad \text{for} \quad u = 1, \dots, l$$

Then

$$g_{uv}(X) = f_u(X)f_v(X) = X^{2l-2l-2+u+v} + \bar{f}_u(X)X^{k-l-1+v} + \bar{f}_v(X)X^{k-l-1+u} + \bar{f}_u(X)\bar{f}_v(X)$$

Where:

- $\deg(\bar{f}_u(X)\bar{f}_v(X)) \leq 2k - 2l - 2.$
- $\deg(\bar{f}_v(X)X^{k-l-1+u}), \deg(\bar{f}_u(X)X^{k-l-1+v}) \leq 2k - l - 2.$
- $2k - 2l \leq \deg(f_u(X)f_v(X)) \leq 2k - 2$ and $LC(f_u(X)f_v(X)) = 1$

That is to say:

- 1 The first $2k - 2l - 1$ columns of $G_{\mathcal{D}}$ are quadratics in the $l(k - l)$ coefficients of the polynomials $\bar{f}_u(X)$ with $1 \leq u \leq l.$
- 2 The following l columns are linear in those coefficients.
- 3 The last l columns are the constant 0 or 1.

PROPOSITION 12 ◀ Return II

VULNERABILITIES OF CODE-BASED CRYPTOGRAPHY

INTRODUCTION

GAPS OF A CODE

GRS SUBCODES OF GRS CODES

THE SQUARE OF A CODE

PROOFS

PROPOSITION 1

PROPOSITION 2

PROPOSITION 3

PROPOSITION 4

PROPOSITION 5

PROPOSITION 6

PROPOSITION 7

PROPOSITION 8

PROPOSITION 9

PROPOSITION 10

PROPOSITION 11

PROPOSITION 12

COROLLARY 5

Suppose that $\text{rank}(G_{\mathcal{D}}) \leq 2k - 1$ then

- All square submatrices of $G_{\mathcal{D}}$ of size $2k - 1$ are singular.
- The determinant of such square submatrices is **CERO**.
- The determinant is a polynomial of degree $\leq 2(2k - 2l - 1) + l = 4k - 3l - 2$ whose variables are the coefficients of the polynomials $\bar{f}_u(X)$ with $1 \leq u \leq l$.

A polynomial $\Delta(Y) \in \mathbb{F}_q[Y_1, \dots, Y_N]$ of degree d has at most dq^{N-1} in \mathbb{F}_{q^N} if $d < q - 1$.

Hence the number of roots in $\mathbb{F}_{q^{l(k-l)}}$ of one of these determinants is at most $(4k - 3l - 2)q^{l(k-l)-1}$ if $4k - 3l - 2 < q - 1$.

COROLLARY 5

[Return](#)

VULNERABILITIES OF CODE-BASED CRYPTOGRAPHY

[INTRODUCTION](#)[GAPS OF A CODE](#)[GRS SUBCODES OF GRS
CODES](#)[THE SQUARE OF A CODE](#)[PROOFS](#)[PROPOSITION 1](#)[PROPOSITION 2](#)[PROPOSITION 3](#)[PROPOSITION 4](#)[PROPOSITION 5](#)[PROPOSITION 6](#)[PROPOSITION 7](#)[PROPOSITION 8](#)[PROPOSITION 9](#)[PROPOSITION 10](#)[PROPOSITION 11](#)[PROPOSITION 12](#)[COROLLARY 5](#)

Let \mathcal{C} be an l -dimensional GRS subcode of $\text{GRS}_k(\mathbf{a}, \mathbf{b})$, i.e. $\mathcal{C} = \text{GRS}_l(\mathbf{c}, \mathbf{d})$ and $d_0 < d_1$ be the first two elements of $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b})$.

By [Proposition 7](#) there exists $g_0, h_1 \in \mathbb{F}_q[X]$ such that:

$$\mathbf{1} \quad \text{ev}_{\mathbf{a}, \mathbf{b}}(g_0(X)) = \mathbf{d}.$$

$$\mathbf{3} \quad d_0 = \deg(g_0(X)).$$

$$\mathbf{2} \quad \text{ev}_{\mathbf{a}}(h_1(X)) = \mathbf{c}.$$

$$\mathbf{4} \quad d_1 = d_0 + \deg(h_1(X)).$$

Note that

- The number of possible polynomials $g_0 \in \mathbb{F}_q[X]$ is at most $(q-1)q^{d_0}$.
- The number of possible polynomials $h_1 \in \mathbb{F}_1[X]$ is at most $(q-1)q^{d_1-d_0}$.

Since the pair (g_0, h_1) determines the code \mathcal{C} uniquely and the number of possible pairs of given degree d_0 and d_1 is at most $(q-1)^2 q^{d_1}$, then the number of l -dimensional subcodes of $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ that are GRS is at most

$$\sum_{d_1=1}^{k-l+1} (q-1)^2 q^{d_1} \leq q^{k-l+3}.$$