# Are AG codes secure for code based PKC?

I. Márquez-Corbella [1] E. Martínez-Moro [2] R. Pellikaan [3]

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

[2] Department of Applied Mathematics, University of Valladolid.

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

EIDMA/DIAMANT Cryptography Working Group

# Overview



1 Introduction
- Introduction to Coding Theory
- Public-Key Cryptosystems
- McEliece cryptosystem
- Attacks on the McEliece PKC
- Niederreiter Cryptosystem
- Attacks on the Niederreiter PKC

2 Weak keys in the Berguer-Loidreau PKC

3 Cryptanalysis of PKC based on AG codes

4 Proofs

# Introduction to Coding Theory

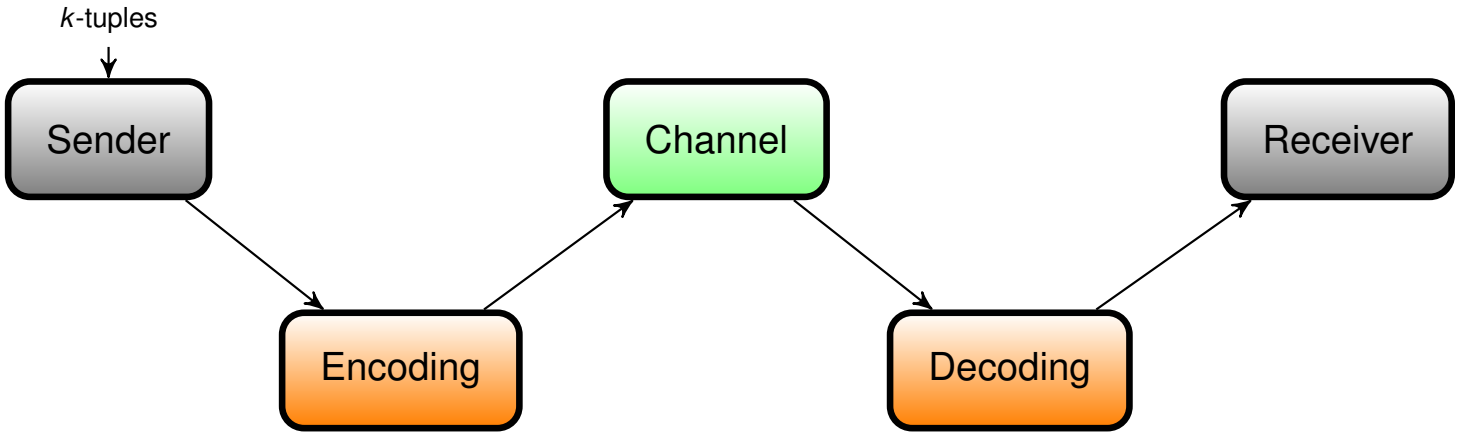


**Claude Shannon**
**(1916-2001)**

*A Mathematical Theory of Communication*
(Claude Shannon, 1948)

Information Theory

Coding Theory




$$c: \quad \mathcal{A}^k \longrightarrow \mathcal{A}^n$$

# INTRODUCTION TO CODING THEORY I

- A **linear code $\mathcal{C}$ of parameters [n,k]** over $\mathbb{F}_q$ is a $k$-dimensional subspace of $\mathbb{F}_q^n$.
- The **Hamming distance** between $\mathbf{x},\ \mathbf{y} \in \mathbb{F}_q^n$ is $d_H(\mathbf{x},\mathbf{y}) = |\{i \mid x_i \neq y_i\}|$.
- The **Hamming weight** of $\mathbf{x} \in \mathbb{F}_q^n$ is $w_H(\mathbf{x}) = |\mathrm{supp}(\mathbf{x})| = |\{i \mid x_i \neq 0\}|$.
- The **Minimum distance of a linear code $\mathcal{C}$** es

$$d = \min\{d_H(\mathbf{c}_1,\mathbf{c}_2) \mid \mathbf{c}_1,\ \mathbf{c}_2 \in \mathcal{C} \text{ y } \mathbf{c}_1 \neq \mathbf{c}_2\}.$$

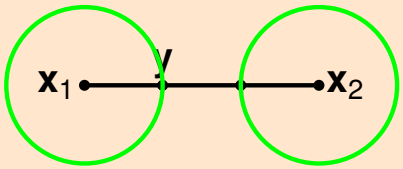



FIGURE: Code with $d = 3$

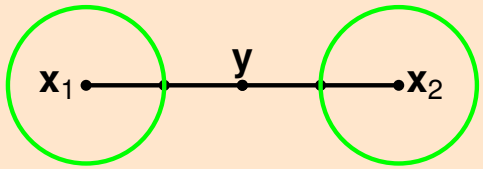



FIGURE: Code with $d = 4$

# Introduction to Coding Theory II



- The **Generator Matrix** of $\mathcal{C}$ is a matrix $G \in \mathbb{F}_q^{k \times n}$ whose rows form a basis of $\mathcal{C}$, i.e.

$$\mathcal{C} = \left\{ \mathbf{x}G \ : \ \mathbf{x} \in \mathbb{F}_q^k \right\}.$$

- The **Parity-Check Matrix** of $\mathcal{C}$ is a matrix $H \in \mathbb{F}_q^{(n-k) \times n}$ whose nullspace is generated by the codewords of $\mathcal{C}$, i.e.

$$\mathcal{C} = \left\{ \mathbf{y} \in \mathbb{F}_q^n \ : \ H\mathbf{y}^T = 0 \right\}.$$

## Properties of Linear Codes

For any linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ of parameters $[n, k]$:

1. **Singleton bound:** $d \leq n - k + 1$.
2. $H^T G = 0$.
3. We can detect up to $d - 1$ errors.
4. We can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors.

➜ The **rate information** is $R = \frac{k}{n}$

# Public-Key Cryptosystems



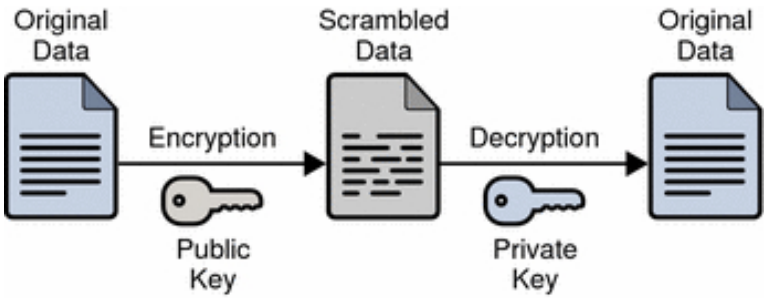
## Two keys:

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

## Most PKC are based on number-theoretic problems

➜ Quatum 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-quatum cryptography

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

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

# McEliece cryptosystem



## 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 $e' = eP$ 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. $\mathbf{m} = \mathbf{m}SS^{-1}$.

- 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

➜ 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.

*Crytanalysis 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

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

# Attacks on the Niederreiter PKC



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

V. M. Sidelnikov and S. O. Shestakov.

*On insecurity of cryptosystems based on generalized Reed-Solomon codes.*
Discrete Mathematics and Applications.

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

Let :

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

$$\begin{array}{rccc} \mathrm{ev}_{\mathbf{a},\mathbf{b}} : & L_k & \to & \mathbb{F}_q^n \\ & f & \mapsto & (f(a_1)b_1, \ldots, f(a_n)b_n) \end{array}$$

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

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

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

## REMARK

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

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



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

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

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

## $(\mathbf{a}, \mathbf{b})$-GAP OF THE CODE

$i \in \mathbb{Z}_{\geq 0}$ is called an **$(\mathbf{a}, \mathbf{b})$-gap** of the code $\mathcal{C}$ if $\mathcal{C}_i = \mathcal{C}_{i+1}$.
We define the **associated $(\mathbf{a}, \mathbf{b})$ 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 $(\mathbf{a}, \mathbf{b})$ non-gap of $\mathcal{C}$ $\iff$ $\exists f \in \mathbb{F}_q[X]$ with $\deg(f(X)) = i$ such that $\mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X)) \in \mathcal{C}$

## COROLLARY 1

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

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

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



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 $\mathcal{I} = \{i_1, \ldots, i_l\}$ and there are $l$ polynomials in unique normal form

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

such that

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

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

**PROPOSITION 3** ◂ Proof

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

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

where $i_0 = -1$. Then **the number of $l$-dimensional subcodes of the code** $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ 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

**REMARK**

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

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

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

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

# GRS SUBCODES OF GRS CODES I



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

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

**PROPOSITION 4** ◂ Proof

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

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

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

**PROPOSITION 5** ◂ Proof

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

Note that the converse is not true in general.

**COROLLARY 3**

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

# GRS subcodes of GRS codes II



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

**Proposition 6** ◂ Proof

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

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

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

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

**Proposition 7** ◂ Proof

If $2k - 2 < n$ and $l \geq 2$.
Assume that $\mathcal{C} = \mathrm{GRS}_l(\mathbf{c}, \mathbf{d}) \subseteq \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ 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:

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

# GRS subcodes of GRS codes III



**Corollary 5** ◂ Proof

If $2k - 2 < n$ and $2 \leq l \leq k$. Then the number of $l$-dimensional subcodes of the code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ 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 $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ 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 $k \to \infty$ or $(k - l) \to \infty$.

# THE SQUARE OF A CODE

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

Let:

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

Then

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

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 $\mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$.

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



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

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

**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 $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{i_1, \ldots, i_l\}$ with $i_1 + i_l < 2k - 1$ and $\mathbf{c} = \mathrm{ev}_{\mathbf{a}, \mathbf{b}}(f(X)) \in \mathcal{C}$ for $f \in \mathbb{F}_q[X]$ with $\deg(f(X)) = i_1$ then

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

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



**Proposition 11** ◂ Proof

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

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

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

**Remark**

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

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

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



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

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

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

- Furthermore

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

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

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

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

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

# Necessary conditions to have:

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



## Final Remark

The following properties are necessary conditions to have that

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

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

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



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

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

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

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

**Proposition 12** ◂ Proof

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

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

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 $q \to \infty$.

# Overview



1 Introduction

2 Weak keys in the Berguer-Loidreau PKC

3 Cryptanalysis of PKC based on AG codes
- AG Codes
- AG representations of a code
- Curves defined by quadratic equations
- Determination of $I_2(\mathcal{Q})$
- VSAG codes

4 Proofs

# Cryptanalysis of PKC based on AG codes



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

- **Faure and Minder** in 2008 generalized this result to curves of genus 1 and 2.

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.

H. Janwa and O. Moreno.

McEliece public cryptosystem using algebraic-geometric codes.
Designs, Codes and Cryptography, 8:293-307, 1996.

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.

V. M. Sidelnikov and S. O. Shestakov.

On insecurity of cryptosystems based on generalized Reed-Solomon codes.
Discrete mathematics and Applications.

# ALGEBRAIC GEOMETRY CODES

- Let $\mathcal{X}$ be an **algebraic curve** over $\mathbb{F}_q$ defined by the polynomial $F(X) \in \mathbb{F}_q[X]$.

## RATIONAL FUNCTIONS

The **function field** or the **field of rational functions** on $\mathcal{X}$ is

$$\mathbb{F}_q(\mathcal{X}) = \left( \left\{ \frac{g(X)}{h(X)} \mid g,\ h \in \mathbb{F}_q[X] \quad \begin{array}{c} \text{are homogeneous} \\ \text{of the same degree} \end{array} \right\} \cup \{0\} \right) \setminus \sim$$

where $\frac{g}{h} \sim \frac{g'}{h'} \iff gh' - g'h \in \langle F \rangle$.

## DIVISORS ON CURVES

Every divisor $D$ on $\mathcal{X}$ over $\mathbb{F}_q$ is of the form $D = \sum n_Q Q$ where $n_Q \in \mathbb{Z}$ and $Q$ is a point on $\mathcal{X}$.

- The **degree** of $D$ is $\deg D = \sum n_Q \deg(Q)$.
- The **support** of $D$ is $\operatorname{supp}(D) = \{Q \mid n_Q \neq 0\}$

## DIVISORS OF RATIONAL FUNCTIONS

The divisor of $f \in \mathbb{F}_q(\mathcal{X})$ is defined to be:

$$(f) = (\text{zeros of } f) - (\text{poles of } f).$$

# ALGEBRAIC GEOMETRY CODES

➜ Let:

- $\mathcal{X}$ be an algebraic curve of genus $g$ defined over the finite field $\mathbb{F}_q$,
- $P = (P_1, \ldots, P_n)$ be an $n$-tuple of distinct $\mathbb{F}_q$-rational points on $\mathcal{X}$
- $E$ be a divisor of $\mathcal{X}$ with $\mathrm{supp}(E) \cap P = \emptyset$ and $\deg(E) = m$.

**SPACE OF RATIONAL FUNCTIONS ASSOCIATED TO $E$**

The space of rational functions associated to $E$ is

$$L(E) = \{f \in \mathbb{F}_q(\mathcal{X}) \mid f = 0 \text{ or } (f) + E \geq 0\}$$

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

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

**RIEMMAN-ROCH THEOREM**

$$\dim L(E) \geq m + 1 - g.$$

Furthermore if $m > 2g - 2$ then $\dim L(E) = m + 1 - g$.

# ALGEBRAIC GEOMETRY CODES

## ALGEBRAIC GEOMETRY CODES (AG CODES)

The AG code associated to $\mathcal{X}$, $P = (P_1, \ldots, P_n)$ and $E$ is

$$C_L(\mathcal{X}, P, E) = \{\mathrm{ev}_P(f) \mid f \in L(E)\}$$

## THEOREM: PARAMETERS OF AN AG CODE

If $n > m$ then $C_L(\mathcal{X}, P, E)$ is an $[n, k, d]$ code over $\mathbb{F}_q$ where

$$k \geq m + 1 - g \quad \text{and} \quad d \geq n - m$$

Moreover, if $m > 2g - 2$ then $k = m + 1 - g$.

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

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

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

# ALGEBRAIC GEOMETRY REPRESENTATIONS OF A CODE

## WEAKLY ALGEBRAIC-GEOMETRIC (WAG)

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

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

➜ Then $(\mathcal{X}, P, E)$ is called a **WAG representation** of $\mathcal{C}$.

## THEOREM [PELLIKAAN-SHEN-VAN WEE (1991)]

Every code has a WAG representation.

A **WAG** representation $(\mathcal{X}, P, E)$ is called:

➜ **Algebraic-geometric (AG)** if $\deg(E) < n$.

➜ **t-strong algebraic-geometric (t-SAG)** if $2g - 2 + t < m < n - t$.

➜ A 0-SAG representation is a **SAG** representation.

**PROPOSITION**

Let $(\mathcal{X}, P, E)$ and $(\mathcal{Y}, Q, F)$ be WAG representations of the codes $\mathcal{C}$ and $\mathcal{D}$, respectively. Then:

1. If $(\mathcal{X}, P, E)$ and $(\mathcal{Y}, Q, F)$ are **equivalent** then $\mathcal{C} \equiv \mathcal{D}$.
2. If $(\mathcal{X}, P, E)$ and $(\mathcal{Y}, Q, F)$ are **strict equivalent** then $\mathcal{C} = \mathcal{D}$.

Let $r = dim(L(E)) - 1$ and $\{f_0, \ldots, f_r\}$ be a basis of $L(E)$. We consider the following map:

$$\begin{array}{rccc} \varphi_E : & \mathcal{X} & \longrightarrow & \mathbb{P}^r(\mathbb{F}_q) \\ & P & \longmapsto & \varphi_E(P) = (f_0(P), \ldots, f_r(P)) \end{array}$$

**PROPOSITION 6**

Let $(\mathcal{X}, P, E)$ be WAG representation of the code $\mathcal{C}$ such that $\deg(E) = m > 2g$. Let $\mathcal{Y} = \varphi_E(\mathcal{X})$, $Q = \varphi_E(P)$ and $F = \varphi_E(E)$. Then $(\mathcal{Y}, Q, F)$ **is a representation of** $\mathcal{C}$ **that is strict isomorphic with** $(\mathcal{X}, P, E)$.

# Curves defined by quadratic equations

The canonical model of a non-singular non-hyperelliptic projective curve of genus $\geq 3$ is the intersection of quadrics and cubics.

➜ And of quadrics only except in case of a trigonal curve and a plane quintic.

See:

D. W. Babbage.

*A note on the quadrics through a canonical curve.*
Journ. London Math. Soc., volume 14, pp. 310–315, 1939.

F. Enriques.

*Sulle cuve canoniche di genere p dello spazio a p − 1 dimensioni.*
Rend. Accad. Sci. Ist. Bologna, volume 23, pp. 80–82, 1919.

K. Petri.

*Über die invariante Darstellung algebraischer Funktionen einer Veränderlichen.*
Math. Ann., volume 88, 1923.

This result for the **canonical divisor** was generalized for arbitrary divisors under certain constraints on the degree.

See:

E. Arbarello and E. Sernesi.

*Petri's approach to the study of the ideal associated to a special divisor.*
Invent. Math., volume 49, pp. 99–119, 1978.

D. Mumford.

*Varieties defined by quadratic equations.*
Questions on algebraic varieties, C.I.M.E, III Ciclo, Varenna, 1969, pp. 29–100, Edizioni Cremonese, Rome, 1970.

B. Saint-Donat.

*Sur les équatons définissant une courbe algébrique.*
C. R. Acad. Sci. Paris Sr. A, volume 274, pp. 487–489, 1972.

## $I_d(\mathcal{Y})$

$I_d(\mathcal{Y})$ is the ideal generated by the homogeneous elements of degree $d$ in $I(\mathcal{Y})$.

## Proposition 7

Let $\mathcal{X}$ be an algebraic curve of genus $g$ over $\mathbb{F}$ and $E$ be a divisor on $\mathcal{X}$ of degree $m$.

1. If $m \geq 2g+2$ then $\varphi_E(\mathcal{X}) = \mathcal{Y}$ is a normal curve in $\mathbb{P}^{m-g}$ which is the intersection of quadrics.

➜ In particular $I(\mathcal{Y})$ is generated by $I_2(\mathcal{Y})$.

B. Saint-Donat.

*Sur les équatons définissant une courbe algébrique.*
C. R. Acad. Sci. Paris Sr. A, volume 274, pp. 487–489, 1972.

2. If $m \geq 2g+1$ then $\varphi_E(\mathcal{X}) = \mathcal{Y}$ is a normal curve in $\mathbb{P}^{m-g}$ which is the intersection of quadrics and cubics.

➜ In particular $I(\mathcal{Y})$ is generated by $I_2(\mathcal{Y})$ and $I_3(\mathcal{Y})$.

D. Mumford.

*Varieties defined by quadratic equations.*
Questions on algebraic varieties, C.I.M.E, III Ciclo, Varenna, 1969, pp. 29–100, Edizioni Cremonese, Rome, 1970.

B. Saint-Donat.

*Sur les équatons définissant une courbe algébrique.*
C. R. Acad. Sci. Paris Sr. A, volume 274, pp. 487–489, 1972.

# DETERMINATION OF $I_2(\mathcal{Q})$

Let:

- $\mathcal{Y}$ be an absolutely irreducible curve in $\mathbb{P}^r$ of degree $m$ such that $I(\mathcal{Y}) = I_2(\mathcal{Y})$.
- $Q$ be an $n$-tuples of points that lies on the curve $\mathcal{Y}$ (i.e. $I(\mathcal{Y}) \subseteq I(Q)$)

**WE CAN ANSWER THE FOLLOWING QUESTIONS:**

1. Under which hypothesis is true that $I_2(Q) = I_2(\mathcal{Y})$?
2. How we can compute $I_2(Q)$ efficiently?

# Very Strong Algebraic-Geometric codes



## Very Strong Algebraic-Geometric (VSAG) codes

A code $\mathcal{C}$ has a VSAG representation if $\mathcal{C} = \mathcal{C}_L(\mathcal{X}, P, E)$ where the curve $\mathcal{X}$ has genus $g$, $P$ consists of $n$ points and $E$ has degree $m$ such that

$$2g + 2 < m < \tfrac{1}{2}n \quad \text{or} \quad \tfrac{1}{2}n + 2g - 2 < m < n - 4$$

- The **dual** of a VSAG code is again VSAG.
- The dimension of such a code is $k = m + 1 - g$. Thus the dimension satisfies the following bound:

$$g + 3 < k < \tfrac{1}{2}n - g + 1 \quad \text{or} \quad \tfrac{1}{2}n + g - 1 < k < n - g - 2$$

## Theorem 12

◂ Proof

Let $\mathcal{C}$ be a VSAG code then a VSAG representation can be obtained from its generator matrix.

- Moreover all VSAG representations of $\mathcal{C}$ are strict isomorphic.

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

If $\gamma \leq \frac{1}{4}$, **VSAG** codes are **not secure** for code based PKC in the range:

$$\gamma \leq R \leq \tfrac{1}{2} - \gamma \quad \text{or} \quad \tfrac{1}{2} + \gamma \leq R \leq 1 - \gamma$$

**Proposition 16**

If $\gamma \leq \frac{1}{4}$ and $\mathcal{C}$ is a **SAG** code in the range

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

then by shortening $\mathcal{C}$ sufficiently many times one gets a **VSAG** code.

**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: $\gamma \leq R \leq 1 - \gamma$

# PKC using Algebraic-Geometry codes



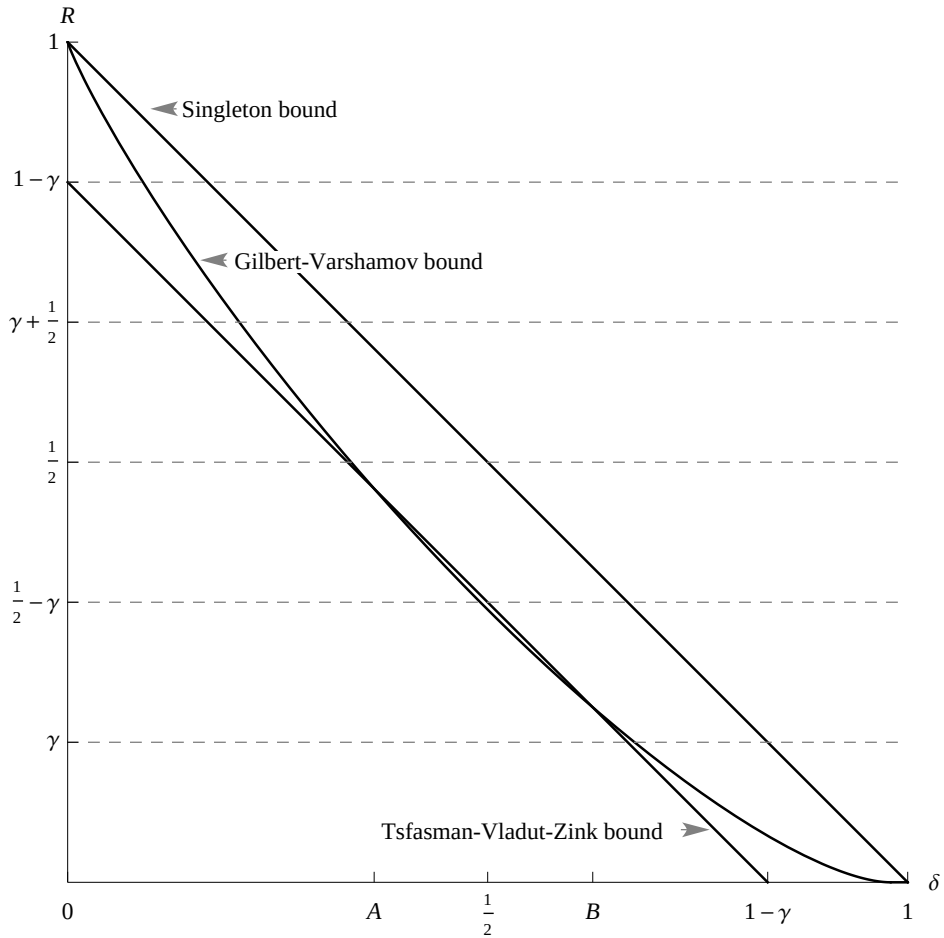



Figure: Bounds on $R$ as a function of the relative minimum distance $\delta$ for $q = 49$ and $\gamma = \frac{1}{6}$.

# Thank for your attention



# PROPOSITION 1

## 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 $\mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X)) \in \mathcal{C}$

$\Rightarrow$ 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

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

i.e. there exists a unique polynomial $f \in L_{i+1}$ : $\mathbf{c} = \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X))$
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 $\mathbf{c} = \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X))$ 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 $\deg(f(X)) \in \mathcal{I}(\mathcal{C}) \ : \ \mathbf{c} = \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X))$.
- Furthermore the code $\mathcal{C}$ has dimension $l$, i.e. $\exists f_1, \ldots, f_l \in \mathbb{F}_q[X]$ with $\deg(f_i(X)) \in \mathcal{I}(\mathcal{C}))$ for $i \in \{1, \ldots, l\}$ such that

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

To make the notation easier we can assume that:

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

Thus each polynomial $f_j$ can be written as

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

Let us define the matrix $M(f_1, \ldots, f_l) = (f_{j,s}) \in \mathbb{F}_q^{l \times k}$ as the matrix whose $i$-th row represent the coefficients with respect to the monomials $\{1, X, \ldots, X^{k-1}\}$ of the polynomial $f_j$ for $j \in \{1, \ldots, l\}$. 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 3

Return



Let $\mathcal{C}$ be an $l$-dimensional subcode of $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ with non-gap sequence $\mathcal{I}(\mathcal{C}) = \{i_1, \ldots, i_l\}$.
By Proposition 2 there are $l$ polynomials in normal form

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

such that

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

If we fix the set $\mathcal{I}$ there are $q^{e(\mathcal{I})}$ $l$-dimensional subcodes of $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ with associated non-gap sequence $\mathcal{I}$.

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

Note that $e(\mathcal{I})$ is equal to the number of elements of the matrix $M(f_1, \ldots, f_l)$ which are free to be chosen in $\mathbb{F}_q$ as long as the form of $M$ is not changed.

# Proposition 4

Return



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

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

**Remark**

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

# Proposition 5

Return



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

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

such that

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

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

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

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

Hence

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

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



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

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

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

Furthermore

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

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

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

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

# PROPOSITION 7

Return

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

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

So $\mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_i(X))g_j(X)) = \mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_u(X)g_v(X))$, 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 $i + j = u + j$.
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

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

1. If $j = 0$ we deduce that $\mathbf{d} = \mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_0(X))$.
2. If $j = 1$ we deduce that $\mathbf{c} = \mathrm{ev}_{\mathbf{a}}(h_1(X))$.

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

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

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

# PROPOSITION 8

Return

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

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

Therefore:

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

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 $\mathcal{C} = \langle \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_1), \ldots, mathrmev_{\mathbf{a},\mathbf{b}}(f_l) \rangle \subseteq \mathrm{GRS}_5(\mathbf{a}, \mathbf{b})$ where

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

Then:

1. $\mathcal{I}(\mathcal{C}) = \{0, 2, 3, 4\} \Rightarrow \mathcal{I}(\mathcal{C}) + \mathcal{I}(\mathcal{C}) = \{0, 2, 3, 4, 5, 6, 7, 8\}$.
2. $1 \in \mathcal{J}(\mathcal{D})$ 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 $\mathcal{J}(\mathcal{D}) = \{0, 1, \ldots, 8\} \Rightarrow \mathcal{D} = \mathrm{GRS}_9(\mathbf{a}, \mathbf{b})$.

# PROPOSITION 11

Return

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

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

with $j \in \{1, \ldots, l\}$ such that $\mathcal{C} = \langle \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_1(X)), \ldots, \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_l(X))\rangle$.
Then the elements $\mathrm{ev}_{\mathbf{a},\mathbf{b}*\mathbf{b}}(f_u(X)f_v(X))$ with $1 \le u \le v \le l$ 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 $\mathcal{D} = \mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$ i.e. the elements $\mathrm{ev}_{\mathbf{a},\mathbf{b}*\mathbf{b}}(X^j)$ with $0 \le j \le 2k-2$ form a basis of $\mathcal{D}$.
Hence $\forall t \in \{0, \ldots, 2k-2\}, \exists (u, v) \ : \ i_u + i_v \ge t$ and $1 \le u \le v \le l$.
Since $\mathrm{ev}_{\mathbf{a},\mathbf{b}*\mathbf{b}}(f_u(X)f_v(X)) \in \mathrm{GRS}_t(\mathbf{a}, \mathbf{b} * \mathbf{b}) \Rightarrow i_u + i_v < t$ and $1 \le u \le v \le l$.
Then the vector space $V_t = \mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b}) \setminus \mathrm{GRS}_t(\mathbf{a}, \mathbf{b} * \mathbf{b})$ is generated by the elements $\mathrm{ev}_{\mathbf{a},\mathbf{b}*\mathbf{b}}(f_u(X)f_v(X))$ with $i_u + i_v \ge t$ and $1 \le u \le v \le l$, 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



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

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

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

$$f_u(X) = X^{k-l-1+u} + \overline{f_u}(X) \text{ with } \deg(\overline{f_u}(X)) \leq k - l - 1 \text{ for } u = 1, \ldots, l$$

Then

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

Where:

- $\deg(\overline{f_u}(X)\overline{f_v}(X)) \leq 2k - 2l - 2$.
- $\deg(\overline{f_v}(X)X^{k-l-1+u}), \deg(\overline{f_u}(X)X^{k-l-1+v}) \leq 2k - l - 2$.
- $2k - 2l \leq \deg(f_u(X)f_v(X)) \leq 2k - 2$ 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 $\overline{f_u}(X)$ 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



Suppose that $\mathrm{rank}(G_{\mathcal{D}}) \leq 2k-1$ 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 $\overline{f_u}(X)$ with $1 \leq u \leq l$.

A polynomial $\Delta(Y) \in \mathbb{F}_q[Y1,\ldots,Y_N]$ 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

Let $\mathcal{C}$ be an $l$-dimensional GRS subcode of $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$, i.e. $\mathcal{C} = \mathrm{GRS}_l(\mathbf{c}, \mathbf{d})$ 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:

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

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 $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ that are GRS is at most

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

# Theorem 12 I



**Theorem 12** ◂ Return

Let $\mathcal{C}$ be a VSAG code then a VSAG representation can be obtained from its generator matrix.

➜ Moreover all VSAG representations of $\mathcal{C}$ are strict isomorphic.

**Proof:**

Let $(\mathcal{X}, P, E)$ be a VSAG representation of $\mathcal{C}$, i.e.

- $\mathcal{X}$ is an algebraic curve over $\mathbb{F}_q$ of genus $g$.
- $P$ is an $n$-tuple of mutually distinct $\mathbb{F}_q$-rational points of $\mathcal{X}$.
- $E$ is a divisor of $\mathcal{X}$ with $\mathrm{supp}(E) \cap P = \emptyset$ and $\deg(E) = m$ such that

$$2g + 2 < m < \tfrac{1}{2}n \quad \text{or} \quad \tfrac{1}{2}n + 2g - 2 < m < n - 4.$$

By duality we may assume that $2g + 2 < m < \frac{1}{2}n$.

Let $G \in \mathbb{F}_q^{k \times n}$ be a generator matrix of $\mathcal{C}$ and $Q = P_G$ the associated projective system of $G$.

# Theorem 12 II



- By **Proposition 6** there exists an embedding of the curve $\mathcal{X}$ in $\mathbb{P}^r$ of degree $m$:

$$\begin{array}{rccc} \varphi_E : & \mathcal{X} & \longrightarrow & \mathbb{P}^r \\ & P & \longmapsto & \varphi_E(P) = (f_0(P), \ldots, f_r(P)) \end{array}$$

  where $\{f_0, \ldots, f_r\}$ is a basis of $L(E)$ and $r = \dim(L(E)) - 1 = m - g$ (Since $m > 2g$) satisfying that:

  - The points $Q$ lies on the curve $\mathcal{Y} = \varphi_E(\mathcal{X})$.
  - $F = \varphi_E(E) = \mathcal{Y} \cdot H$ for some hyperplane $H$ of $\mathbb{P}^{m-g}$ that is disjoint from $Q$.

  such that $(\mathcal{Y}, Q, F)$ is a representation of $\mathcal{C}$ that is strict isomorphic with $(\mathcal{X}, P, E)$.

- By **Proposition 7**, since $m > 2g + 2$ then $I(\mathcal{Y})$ is generated by $I_2(\mathcal{Y})$.
- By **Proposition 9**, since $n > 2m$ then $I_2(\mathcal{Y}) = I_2(Q)$.
- So the curve $\mathcal{Y}$ is determined by the $n$-tuple of points $Q$.
- Let $(\mathcal{X}', P', E')$ be another VSAG representation of $\mathcal{C}$ then $(\mathcal{Y}, Q, F)$ is strict isomorphic with $(\mathcal{X}', P', E')$, i.e. $(\mathcal{X}, P, E)$ and $(\mathcal{X}', P', E')$ are strict isomorphic.