EVALUATION OF PUBLIC-KEY CRYPTOSYSTEMS BASED ON ALGEBRAIC GEOMETRY CODES

INTRODUCTION

CURVES DEFINED BY QUADRATIC EQUATIONS

DETERMINATION OF $I_2(Q)$ VSAG CODES

CRYPTANALYSIS OF PKC PROOFS

EVALUATION OF PUBLIC-KEY CRYPTOSYSTEMS BASED ON ALGEBRAIC GEOMETRY CODES

I. MÁRQUEZ-CORBELLA ¹  E. MARTÍNEZ-MORO ²  R. PELLKAAN 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.

3ICMCTA

3rd International Castle Meeting on Coding Theory and Applications
EVALUATION OF PUBLIC-KEY CRYPTOSYSTEMS BASED ON ALGEBRAIC GEOMETRY CODES

OVERVIEW

1 INTRODUCTION

2 CURVES DEFINED BY QUADRATIC EQUATIONS

3 DETERMINATION OF $l_2(Q)$

4 VSAG CODES

5 CRYPTANALYSIS OF PKC

6 PROOFS
**Projective systems and linear codes**

**r-dimensional projective space over \( \mathbb{F}_q \):**

\[ \mathbb{P}^r(\mathbb{F}_q) = \left( \mathbb{F}_q^{r+1} \setminus \{(0, \ldots, 0)\} \right) \sim \]

where \((x_0, \ldots, x_r) \sim (y_0, \ldots, y_r) \iff \exists \alpha \in \mathbb{F}_q^\ast : x_i = \alpha y_i \text{ for all } i \in \{0, \ldots, r\}\]

→ We write \((x_0 : x_1 : \ldots : x_r)\) for the equivalence class of \((x_0, x_1, \ldots, x_r)\) in \(\mathbb{P}^r(\mathbb{F}_q)\).

**Projective system**

An \(n\)-tuple of points \((P_1, \ldots, P_n)\) in \(\mathbb{P}^r(\mathbb{F}_q)\) is a **projective system** if not all these points lie in a hyperplane.

1. Let \(P = (P_1, \ldots, P_n)\) be a projective system in \(\mathbb{P}^r(\mathbb{F}_q)\).
   → We define the matrix \(G_P \in \mathbb{F}_q^{(r+1) \times n}\) as the matrix with \(P_j^T\) as \(j\)-th column.
   → Then \(G_P\) is the generator matrix of a nondegenerate \([n, r + 1]\) code over \(\mathbb{F}_q\).

2. Let \(C\) be a nondegenerate \([n, k]\) code over \(\mathbb{F}_q\) with generator matrix \(G\).
   → Take the columns of \(G\) as homogeneous coordinates of points in \(\mathbb{P}^{k-1}(\mathbb{F}_q)\).
   → This gives the projective system \(P_G\) over \(\mathbb{F}_q\) of \(G\).
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

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

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 $\text{supp}(D) = \{Q \mid n_Q \neq 0\}$

**Divisors of Rational Functions**

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

$$(f) = (\text{zeros of } f) - (\text{poles of } f).$$
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 \( \text{supp}(E) \cap P = \emptyset \) and \( \deg(E) = m \).

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 \( \text{supp}(E) \cap P = \emptyset \) the following evaluation map is well defined:

\[
\text{ev}_P : \quad L(E) \longrightarrow \mathbb{F}_q^n
\]

\[
f \quad \longmapsto \quad \text{ev}_P(f) = (f(P_1), \ldots, f(P_n))
\]

\text{RIEMMAN-ROCH THEOREM}

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

Furthermore if \( m > 2g - 2 \) then \( \dim L(E) = m + 1 - g \).
valuation of public-key cryptosystems based on algebraic geometry codes

introduction

projective systems and linear codes

algebraic geometry codes

algebraic geometry representations of a code

dual codes on curves

curves defined by quadratic equations

determination of $I_2(Q)$

VSAG codes

cryptanalysis of PKC

proofs

algebraic geometry codes (AG codes)

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

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

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 $k = m + 1 - g$.

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

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

is a generator matrix of the code $C_L(\mathcal{X}, P, E)$
## Algebraic Geometry Representations of a Code

### Weakly Algebraic-Geometric (WAG)

A code \( C \) over \( \mathbb{F}_q \) is **WAG** if \( C = C_L(\mathcal{X}, P, E) \) 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 \( \text{supp}(E) \cap P = \emptyset \) and \( \deg(E) = m \).  

\[ \implies \text{Then} \ (\mathcal{X}, P, E) \ \text{is called a WAG representation of} \ C. \]

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

**Introduction**

**Projective Systems and Linear Codes**

**Algebraic Geometry Codes**

**Algebraic Geometry Representations of a Code**

**Dual Codes on Curves**

**Curves Defined by Quadratic Equations**

**Determination of $I_2(\mathbb{Q})$**

**VSAG Codes**

**Cryptanalysis of PKC**

**Proofs**

---

**Equivalent Representations**

Two representations $(\mathcal{X}, P, E)$ and $(\mathcal{Y}, Q, F)$ are:

- **equivalent** if there exists an isomorphism of curves
  
  \[ \varphi: \mathcal{X} \rightarrow \mathcal{Y} \]

  such that \( \varphi(P) = Q \) and \( \varphi(E) \equiv F \)

  i.e. \( \exists f \in \mathbb{F}_q(\mathcal{Y}) \mid F = \varphi(E) + (f) \).

- **strict equivalent** if there exists an isomorphism of curves
  
  \[ \varphi: \mathcal{X} \rightarrow \mathcal{Y} \]

  such that \( \varphi(P) = Q \) and \( \varphi(E) \equiv_Q F \)

  i.e. \( \exists f \in \mathbb{F}_q(\mathcal{Y}) \) such that: \( f \) has no poles at the points of \( Q \), \( \varphi(E) = F + (f) \), \( f(Q_j) = 1 \) for all \( j \) and \( \text{supp}(\varphi(E)) \cap \text{supp}(F) = \emptyset \).

---

**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 $\mathcal{C} = \mathcal{D}$. 

**Proposition [Munuera - Pellikaan (1993)]**

Let:
- \( \mathcal{X} \) be a curve over \( \mathbb{F}_q \) of genus \( g \)
- \( P \) be an \( n \)-tuple of mutually distinct \( \mathbb{F}_q \)-rational points of \( \mathcal{X} \).

If \( E \) and \( F \) are divisors on \( \mathcal{X} \) of degree \( m \) with \( 2g - 1 < m < n - 1 \) then:

\[
C_L(\mathcal{X}, P, E) = C_L(\mathcal{X}, P, F) \iff E \equiv_P F
\]

**Proposition 6**

Let \((\mathcal{X}, P, E)\) be a representation of the code \( C \) where:
- \( \mathcal{X} \) 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 with \( \text{supp}(E) \cap P = \emptyset \) and \( \deg(E) = m > 2g \).

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

\[
\varphi_E : \mathcal{X} \times P \longrightarrow \mathbb{P}^r(\mathbb{F}_q) \\
(\mathcal{X}, P) \longmapsto \varphi_E(P) = (f_0(P), \ldots, f_r(P))
\]

If \( \mathcal{Y} = \varphi_E(\mathcal{X}), Q = \varphi_E(P) \) and \( F = \varphi_E(E) \) then \((\mathcal{Y}, Q, F)\) is a representation of \( C \) that is strict isomorphic with \((\mathcal{X}, P, E)\).
Let

- \( w \) be a differential form with a simple pole at \( P_j \) with residue 1 for all \( j = 1, \ldots, n \).
- \( K \) be the canonical divisor of \( w \).
- \( E \) be a divisor of \( \mathcal{X} \) of degree \( m \) and disjoint support from \( P \).

We define

\[
E^\perp = P - E + K \quad \text{and} \quad m^\perp = \deg(E^\perp) = 2g - 2 - m + n
\]

Then

\[
C_L(\mathcal{X}, P, E)^\perp = C_L(\mathcal{X}, P, E^\perp)
\]

See Proposition 2.2.10

H. Stichtenoth.

*Algebraic function fields and codes.*

Introduction

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.

$\rightarrow$ 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.

F. Enriques.

Sulle curve canoniche di genere $p$ dello spazio a $p - 1$ dimensioni.

K. Petri.

Über die invariante Darstellung algebraischer Funktionen einer Veränderlichen.

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.

D. Mumford.

Varieties defined by quadratic equations.

B. Saint-Donat.

Sur les équations définissant une courbe algébrique.
**Curves defined by quadratic equations**

\[ I_d(Y) \]

\[ I_d(Y) \] is the ideal generated by the homogeneous elements of degree \( d \) in \( I(Y) \).

**Proposition**

Let \( X \) be an absolutely irreducible and non-singular curve of genus \( g \) over the perfect field \( \mathbb{F} \) and \( E \) be a divisor on \( X \) of degree \( m \).

1. If \( m \geq 2g + 2 \) then \( \varphi_E(X) = Y \) is a normal curve in \( \mathbb{P}^{m-g} \) which is the intersection of quadrics.
   
   ➔ In particular \( I(Y) \) is generated by \( I_2(Y) \).

   - B. Saint-Donat.
   
   *Sur les équations définissant une courbe algébrique.*

2. If \( m \geq 2g + 1 \) then \( \varphi_E(X) = Y \) is a normal curve in \( \mathbb{P}^{m-g} \) which is the intersection of quadrics and cubics.
   
   ➔ In particular \( I(Y) \) is generated by \( I_2(Y) \) and \( I_3(Y) \).

- D. Mumford.
  
  *Varieties defined by quadratic equations.*

- B. Saint-Donat.
  
  *Sur les équations définissant une courbe algébrique.*
**Determination of } l_2(Q) \text{**}

Let:

- \( \mathcal{Y} \) be an absolutely irreducible curve in \( \mathbb{P}^r \) of degree \( m \) such that \( l(\mathcal{Y}) = l_2(\mathcal{Y}) \).
- \( Q \) be an \( n \)-tuples of points that lies on the curve \( \mathcal{Y} \) (i.e. \( l(\mathcal{Y}) \subseteq l(Q) \)).

**Questions treated on this section:**

1. Under which hypothesis is true that \( l_2(Q) = l_2(\mathcal{Y}) \)?
2. How we can compute \( l_2(Q) \) efficiently?

**Proposition 8**

Let

- \( m, \ r, \ n, \ d \in \mathbb{Z} \) such that \( r \geq 2 \) and \( n > dm \).
- \( \mathcal{Y} \) be an absolutely irreducible curve in \( \mathbb{P}^r \) of degree \( m \).
- \( Q \) be an \( n \)-tuple of points that lies on the curve \( \mathcal{Y} \).

Then \( l_{\leq q}(Q) = l_{\leq q}(\mathcal{Y}) \).
Determination of $l_2(Q)$

Let $C$ be a $k$-dimensional subspace of $\mathbb{F}^n$ with basis $\{g_1, \ldots, g_k\}$.

We denote:

1. **The second symmetric power of $C$ by $S^2(C)$**
   - $S^2(C)$ is the linear subspace in $\mathbb{F}^n$ with basis $\{g_ig_j \mid 1 \leq i \leq j \leq n\}$ and dimension $\binom{k}{2}$.

2. **The square code of $C$ by $\langle C \ast C \rangle$ or by $C^2$.**
   - $C^2$ is the linear subspace in $\mathbb{F}^n$ generated by $\{a \ast b \mid a, b \in C\}$.

We consider the linear map:

$$\sigma : S^2(C) \rightarrow C^2$$

$$g_ig_j \mapsto g_i \ast g_j$$

We denote by $K^2(C)$ the kernel of this map, then

$$0 \rightarrow K^2(C) \rightarrow S^2(C) \rightarrow C^2 \rightarrow 0$$

is an exact sequence.
**PROPOSITION 9**  

Let:
- $Q$ be an $n$-tuple of points in $\mathbb{P}^{k-1}$ over $\mathbb{F}$ not in a hyperplane.
- $G_Q \in \mathbb{F}^{k \times n}$ be the matrix associated to $Q$.
- $C$ the $k$-dimensional subspace of $\mathbb{F}^n$ generated by the rows of $G_Q$ with basis\{g_1, \ldots, g_k\}.

Then

$$l_2(Q) = \left\{ \sum_{1 \leq i \leq j \leq k} a_{ij} x_i x_j \mid \sum_{1 \leq i \leq j \leq k} a_{ij} g_i g_j \in K^2(C) \right\}.$$  

**COROLLARY 10**  

Let $Q$ be an $n$-tuple of points in $\mathbb{P}^r$ over $\mathbb{F}$ not in a hyperplane. Then the complexity of the computation of $l_2(Q)$ is at most $O\left(n^2 \binom{r}{2}\right)$.

**REMARK**

- We define the spaces $S^d(C)$, $C^d$ and $K^d(C)$ for any $d \in \mathbb{Z}_{\geq 0}$.
- We can show the relation between $l_d(Q)$ and $K^d(C)$.
- **Complexity of the computation of** $l_d(Q) \sim O\left(n^2 \binom{k+d-1}{d}\right)$.
Introduction
Curves defined by quadratic equations
Determination of $I_2(\mathbb{Q})$
VSAG codes
Cryptanalysis of PKC
Proofs

Very Strong Algebraic-Geometric codes

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

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

The dual of a VSAG code is again VSAG.

$\Rightarrow$ The dimension of such a code is $k = m + 1 - g$. Thus the dimension satisfies the following bound:

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

Theorem 12

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

$\Rightarrow$ Moreover all VSAG representations of $C$ are strict isomorphic.
Special Issue of Mathematics in Computer Science on Matroids in Coding Theory and Related Topics

Guest Editors:

Ilias S. Kotsireas
Wilfrid Laurier University
Department of Physics and Computer Science
75 University Avenue West
Waterloo, Ontario N2L 3C5, CANADA
e-mail: ikotsire@wlu.ca
http://www.wlu.ca/science/physcomp/kotsireas/

Irene Márquez-Corbella
Universidad de Valladolid
Department of Algebra, Geometry & Topology
Facultad de Ciencias
Valladolid 47005, Castilla, SPAIN
e-mail: imarquez@agt.uva.es

Edgar Martínez-Moro
Universidad de Valladolid
Department of Applied Mathematics
Campus "Duques de Soria"
Soria 42004, Castilla, SPAIN
e-mail: edgar@mff.uva.es
http://www.singacom.uva.es/~edgar

This MCS Special Issue aims at bringing together high quality papers from all fields related to the applications of matroid theory in coding theory and other related areas such as cryptography. Since much of the work on the subject is still ongoing, the Special Issue encourages authors not only to present recent results, but also to propose new guidelines and insights of research as well as potential applications.

Submitted papers should fall within the scope of MCS: foundational research at the interface between mathematics and computer and information sciences. Theoretical investigations, experimental and case studies, scientific and engineering computations, and applications of mathematical methods and tools to outstanding or emerging problems are all welcome. All the submitted papers will be refereed according to the high standards of MCS.

This Special Issue will include selected contributions of the Minisymposium on Applications of Matroid Theory in Coding Theory held at the 3rd Biennial Canadian Discrete and Algorithmic Mathematics Conference (CanaDAM), from May 31 to June 3, 2011, at the University of Victoria, Canada

http://canadam.math.ca/2011/
**Public-Key Cryptosystems**

- **EVALUATION OF PUBLIC-KEY CRYPTO SYSTEMS BASED ON ALGEBRAIC GEOMETRY CODES**

**INTRODUCTION**

- CURVES DEFINED BY QUADRATIC EQUATIONS
- DETERMINATION OF $I_2(Q)$
- VSAG codes

**CRYPTANALYSIS OF PKC**

- McEliece Cryptosystem
- Attacks on the McEliece PKC
- Niederreiter Cryptosystem
- Attacks on the Niederreiter PKC
- PKC USING ALGEBRAIC-GEOMETRY CODES
- CRYPTOANALYSIS OF PKC USING VSAG CODES

**PROOFS**

- **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

---

**McEliece cryptosystem**

### Key Generation

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

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

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

### Encryption

Encrypt a message $m \in \mathbb{F}^k_q$ as

$$y' = mG' + e'$$

where $e$ and $e' = eP$ in $\mathbb{F}^n_q$ are random error vectors of weight $t$.

### Decryption

1. Compute $y = y'P^{-1} = mG'P^{-1} + e'P^{-1} = mSG + e$.

2. Apply the decoding algorithm for $C$ to find $mS$.

3. $m = mSS^{-1}$.

- 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._

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

1. McEliece (1978)
2. Leon (1988)
3. Lee and Brickell (1988)
5. van Tilburg (1990)

A. Canteaut and H. Chabanne.

A. Canteaut and F. Chabaud.

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
Evaluation of public-key cryptosystems based on algebraic geometry codes

Introduction

Curves defined by quadratic equations

Determination of $l_2(\mathbb{Q})$

VSAG codes

Cryptanalysis of PKC

McEliece Cryptosystem

Attacks on the McEliece PKC

Niederreiter Cryptosystem

Attacks on the Niederreiter PKC

PKC using Algebraic-Geometry codes

Cryptanalysis of PKC using VSAG codes

Proofs

---

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:
   - $C$ 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 $m \in \mathbb{F}_q^k$ as

$$y' = mH'^T.$$ 

**Decryption**

1. Compute $y = y' = (S^{-1})^T = mP^TH^T = m'H^T$. Syndrome of $m'$ by $H$.

2. Apply decoding algorithm for $C$ to find $m' = mP^T$ and thereby $m$.

---

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.
ATTACKS ON THE NIEDERREITER PKC

- 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.

A GRS code of parameters \([n, k = r + 1]\) gives a projective system of \(n\) points in general position on a Rational Normal Curve of degree \(r\) in \(\mathbb{P}^r\).

SPECIAL CASE \(k = 3\)

- A Rational Normal Curve of degree 2 is a conic.
- Given 5 points of a conic in general position we can construct a parametrization of the conic.

PROPOSITION [PRINCIPLES OF ALGEBRAIC GEOMETRY BY GRIFFITHS AND HARRIS]

Through any \(r + 3\) points in \(\mathbb{P}^r\) in general position there passes a unique rational normal curve.

C. Faure and L. Minder. 

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

- **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.

---

**Proofs**

- T. Berger and P. Loidreau.
  *How to mask the structure of codes for a cryptographic use.*

- I. Máquez-Corbella, E. Martínez-Moro and R. Pellikaan.
  *The non-gap sequence of a subcode of a generalized Reed-Solomon code.*

- C. Wieschebrink.
  *An attack on the modified Niederreiter encryption scheme.*

- C. Wieschebrink.
  *Cryptoanalysis of the Niederreiter public key scheme based on GRS subcodes.*
PKC using Algebraic-Geometry codes

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

This system was broken for codes on curves of genus $g \leq 2$ by Faure and Minder in 2008.

C. Faure and L. Minder.  
*Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes.*  

H. Janwa and O. Moreno.  
*McEliece public crypto system using algebraic-geometric codes.*  
Designs, Codes and Cryptography, 8:293-307, 1996.
Let \((\mathcal{X}, P, E)\) be a VSAG representation of a code \(C\)

\(\rightarrow\) The dimension of \(C\) satisfies the following bound:

\[ g + 3 < k < \frac{1}{2}n - g + 1 \quad \text{or} \quad \frac{1}{2}n + g - 1 < k < n - g - 3 \]

\(\rightarrow\) Let \(R = \frac{k}{n}\) be the information rate and \(\gamma = \frac{g}{n}\) the relative genus then:

**VSAG** codes are **not secure** for code based PKC in the range:

\[ \gamma \leq R \leq \frac{1}{2} - \gamma \quad \text{or} \quad \frac{1}{2} + \gamma \leq R \leq 1 - \gamma \]
Thank for your attention
PROPOSITION 8

Let

- \( m, r, n, d \in \mathbb{Z} \) such that \( r \geq 2 \) and \( n > dm \).
- \( \mathcal{Y} \) be an absolutely irreducible curve in \( \mathbb{F}^r \) of degree \( m \).
- \( Q \) be an \( n \)-tuple of points that lies on the curve \( \mathcal{Y} \).

Then \( I_{\leq q}(Q) = I_{\leq q}(\mathcal{Y}) \).

**Proof:**

\( \supseteq \) Q lies on \( \mathcal{Y} \) so \( I(\mathcal{Y}) \subseteq I(Q) \). Hence \( I_{\leq d}(\mathcal{Y}) \subseteq I_{\leq d}(\mathcal{Y}) \).

\( \subseteq \) Let :

- \( f \) be an homogeneous polynomial in \( I_{\leq d}(Q) \) of degree \( e \leq d \)
- \( \mathcal{Z} \) be an hypersurface of degree \( e \) defined by \( f = 0 \).

- If \( \mathcal{Y} \cap \mathcal{Z} \) is a finite set over the algebraic closure of the field \( \mathbb{F} \) then the intersection divisor \( \mathcal{Y} \cdot \mathcal{Z} \) is well defined and has degree \( me \) by **Bézout Theorem**.
  Since \( n > dm \geq em \), this contradicts the fact that \( Q \) are in \( \mathcal{Y} \cap \mathcal{Z} \).
- So \( \mathcal{Y} \cap \mathcal{Z} \) is not finite.
  Since \( \mathcal{Y} \) is absolutely irreducible, we have that \( \mathcal{Y} \) must be contained in \( \mathcal{Z} \).
  i.e. \( f \) vanished on \( \mathcal{Y} \), therefore \( f \in I_{\leq d}(\mathcal{Y}) \).
Let:
- $Q$ be an $n$-tuple of points in $\mathbb{P}^{k-1}$ over $\mathbb{F}$ not in a hyperplane.
- $G_Q \in \mathbb{F}^{k \times n}$ be the matrix associated to $Q$.
- $C$ the $k$-dimensional subspace of $\mathbb{F}^n$ generated by the rows of $G_Q$ with basis
  $$\{g_1, \ldots, g_k\}.$$  

Then
$$l_2(Q) = \left\{ \sum_{1 \leq i \leq j \leq k} a_{ij} x_i x_j \mid \sum_{1 \leq i \leq j \leq k} a_{ij} g_i g_j \in K^2(C) \right\}.$$  

**Proof:**
Let $g_{ij}$ be the element of $G_Q$ in the $i$-th row and the $j$-th column.

Let $\sum_{1 \leq i \leq j \leq k} a_{ij} g_i g_j \in K^2(C)$ then:
$$0 = \sigma \left( \sum_{1 \leq i \leq j \leq k} g_i g_j \right) = \sum_{1 \leq i \leq j \leq k} a_{ij} g_i * g_j = \sum_{1 \leq i \leq j \leq k} a_{ij} \left( g_{i1} g_{j1}, \ldots, g_{in} g_{jn} \right)$$

$$\iff \sum_{1 \leq i \leq j \leq k} a_{ij} g_{it} g_{jt} = 0 \ \forall t = 1, \ldots, n$$  

Hence the equation $\sum_{1 \leq i \leq j \leq k} a_{ij} x_i x_j$ at $Q_t = (g_{1t} : \ldots : g_{kt})$ is zero for all $t = 1, \ldots, n$. Therefore $\sum_{1 \leq i \leq j \leq k} a_{ij} x_i x_j \in l_2(Q)$.
Corollary 10

Let $Q$ be an $n$-tuple of points in $\mathbb{P}^r$ over $\mathbb{F}$ not in a hyperplane. Then the complexity of the computation of $I_2(Q)$ is at most $O\left(n^2 \binom{r}{2}\right)$.

Proof:

By Proposition 9 a basis of $K^2(C)$ gives directly a generating set of $I_2(Q)$.

1. $C^2$ is generated by the elements $\{g_i * g_j \mid 1 \leq i \leq j \leq k = r - 1\}$.
2. All these elements form a matrix of size $\binom{k+1}{2} \times n$.
3. We compute gaussian elimination on the previous matrix to obtain a matrix $R$ in reduced row echelon form.

$\Rightarrow$ This can be done in $O\left(n^2 \binom{k+1}{2}\right)$ elementary operations.

4. A basis of $K^2(C)$ is the left kernel of $R$. 
Let $C$ be a VSAG code then a VSAG representation can be obtained from its generator matrix.

Moreover all VSAG representations of $C$ are strict isomorphic.

**Proof:**

Let $(\mathcal{X}, P, E)$ be a VSAG representation of $C$, 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 $\text{supp}(E) \cap P = \emptyset$ and $\text{deg}(E) = m$ such that

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

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 $C$ and $Q = PG$ the associated projective system of $G$.  

**Theorem 12**
Theorem 12 II

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

$$\varphi_E : \mathcal{X} \rightarrow \mathbb{P}^r
\quad P \mapsto \varphi_E(P) = (f_0(P), \ldots, f_r(P))$$

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 $l(\mathcal{Y})$ is generated by $l_2(\mathcal{Y})$.
- By Proposition 9, since $n > 2m$ then $l_2(\mathcal{Y}) = l_2(Q)$.
- 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.