Evaluation of public-key cryptosystems based on algebraic geometry codes

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.

3ICMCTA
3rd International Castle Meeting on Coding Theory and Applications

Overview

Projective systems and linear codes

r-dimensional projective space over $\mathbb{F}_q$: $\mathbb{P}^r(\mathbb{F}_q)$

The $\mathbb{P}^r(\mathbb{F}_q)$ is defined by

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

where $(x_0,\ldots,x_r) \sim (y_0,\ldots,y_r) \iff \exists \alpha \in \mathbb{F}_q^* \ : \ x_i = \alpha y_i$ 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 $\mathcal{C}$ 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.

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

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

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

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

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

Theorem: Parameters of an AG code

If $n > m$ then $\mathcal{C}_L(\mathcal{X}, P, E)$ 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 $\mathcal{C}_L(\mathcal{X}, P, E)$

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.

Algebraic geometry representations of a code

Equivalent representations

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

- **equivalent** if there exists an isomorphism of curves

$$\varphi : \quad \mathcal{X} \quad \longrightarrow \quad \mathcal{Y}$$

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

$$\varphi : \quad \mathcal{X} \quad \longrightarrow \quad \mathcal{Y}$$

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 $\mathrm{supp}(\varphi(E)) \cap \mathrm{supp}(F) = \emptyset$.

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

Algebraic geometry representations of a code

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:

$$\mathcal{C}_L(\mathcal{X}, P, E) = \mathcal{C}_L(\mathcal{X}, P, F) \iff E \equiv_P F$$

Proposition 6

Let $(\mathcal{X}, P, E)$ be a representation of the code $\mathcal{C}$ 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 $\mathrm{supp}(E) \cap P = \emptyset$ 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:

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

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** $\mathcal{C}$ **that is strict isomorphic with** $(\mathcal{X}, P, E)$.

Dual codes on curves

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

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

Then

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

See Proposition 2.2.10

H. Stichtenoth.
Algebraic function fields and codes.
Springer, Berlin, 1993.

Curves defined by quadratic equations

The canonical model of a non-singular non-hyperelliptic projective curve of genus ≥ 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.

Curves defined by quadratic equations

$I_d(\mathcal{Y})$

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

Proposition

Let $\mathcal{X}$ be an absolutely irreducible and non-singular curve of genus g over the perfect field $\mathbb{F}$ 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. $I(\mathcal{Y}) \subseteq I(Q)$)

Questions treated on this section:

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

Proposition 8 Proof

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

Determination of $I_2(Q)$

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

  We denote:

1. **The second symmetric power of $\mathcal{C}$** by $S^2(\mathcal{C})$
   - $S^2(\mathcal{C})$ is the linear subspace in $\mathbb{F}^n$ with basis $\{g_i g_j \mid 1 \leq i \leq j \leq n\}$ and dimension $\binom{k}{2}$.
2. **The square code of $\mathcal{C}$** by $\langle \mathcal{C} * \mathcal{C} \rangle$ or by $\mathcal{C}^2$.
   - $\mathcal{C}^2$ is the linear subspace in $\mathbb{F}^n$ generated by $\{\mathbf{a} * \mathbf{b} \mid \mathbf{a}, \mathbf{b} \in \mathcal{C}\}$.

- We consider the linear map:

$$\begin{array}{rccc} \sigma : & S^2(\mathcal{C}) & \longrightarrow & \mathcal{C}^2 \\ & g_i g_j & \longmapsto & g_i * g_j \end{array}$$

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

$$0 \longrightarrow K^2(\mathcal{C}) \longrightarrow S^2(\mathcal{C}) \longrightarrow \mathcal{C}^2 \longrightarrow 0$$

  is an **exact sequence**.

Determination of $I_2(Q)$

Proposition 9 ◂ Proof

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.
- $\mathcal{C}$ the k-dimensional subspace of $\mathbb{F}^n$ generated by the rows of G_Q with basis

$$\{g_1, \ldots, g_k\}.$$

Then

$$I_2(Q) = \left\{ \sum_{1\le i\le j\le k} a_{ij}x_ix_j \mid \sum_{1\le i\le j\le k} a_{ij}g_ig_j \in K^2(\mathcal{C}) \right\}.$$

Corollary 10 ◂ Proof

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 $\mathcal{O}\left(n^2\binom{r}{2}\right)$.

Remark

- ➜ We define the spaces $S^d(\mathcal{C})$, $\mathcal{C}^d$ and $K^d(\mathcal{C})$ for any $d \in \mathbb{Z}_{\ge 0}$.
- ➜ We can show the relation between $I_d(Q)$ and $K^d(\mathcal{C})$.
- ➜ **Complexity of the computation of** $I_d(Q) \sim \mathcal{O}\left(n^2\binom{k+d-1}{d}\right)$.

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.

Mathematics in Computer Science

Managing editor: D. Wang
ISSN: 1661-8270
Birkhäuser Basel

http://www.springer.com/birkhauser/mathematics/journal/11786

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@maf.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

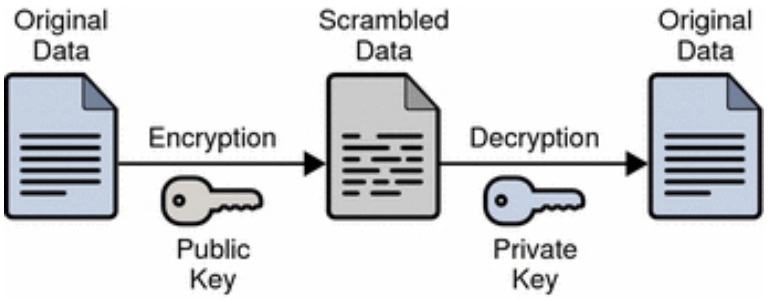
Two keys:

- 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 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.
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.

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.

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.

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.
Proceedings 11th Int. Workshop on Algebraic and Combinatorial Coding Theory, 2008.

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

Cryptanalysis of PKC using VSAG codes

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

- The dimension of $\mathcal{C}$ satisfies the following bound:

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

- 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:

$$\gamma \leq R \leq \frac{1}{2} - \gamma \qquad \text{or} \qquad \frac{1}{2} + \gamma \leq R \leq 1 - \gamma$$

Thank for your attention

Proposition 8

Proposition 8 Return

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 $\mathcal{Y}$.

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

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 $f \in I_{\leq d}(\mathcal{Y})$.

Proposition 9

Proposition 9

Return

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.
- $\mathcal{C}$ the k-dimensional subspace of $\mathbb{F}^n$ generated by the rows of G_Q with basis

$$\{g_1, \ldots, g_k\}.$$

Then

$$I_2(Q) = \left\{ \sum_{1\le i\le j\le k} a_{ij}x_ix_j \mid \sum_{1\le i\le j\le k} a_{ij}g_ig_j \in K^2(\mathcal{C}) \right\}.$$

Proof:

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

$\supseteq$ Let $\sum_{1\le i\le j\le k} a_{ij}g_ig_j \in K^2(\mathcal{C})$ then:

$$0 = \sigma\left(\sum_{1\le i\le j\le k} g_ig_j\right) = \sum_{1\le i\le j\le k} a_{ij}g_i * g_j = \sum_{1\le i\le j\le k} a_{ij}\left(g_{i1}g_{j1}, \ldots, g_{in}g_{jn}\right)$$

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

Hence the equation $\sum_{1\le i\le j\le k} a_{ij}x_ix_j$ at $Q_t = (g_{1t} : \ldots : g_{kt})$ is zero for all $t = 1, \ldots, n$. Therefore $\sum_{1\le i\le j\le k} a_{ij}x_ix_j \in I_2(Q)$.

Corollary 10

Corollary 10 Return

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 $\mathcal{O}\left(n^2\binom{r}{2}\right)$.

Proof:

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

1. $\mathcal{C}^2$ 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.

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

4. A basis of $K^2(\mathcal{C})$ is the left kernel of R.

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

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

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.