Error Correcting Pair: A New Approach to Code-based Cryptography

I. Márquez-Corbera 1 R. Pellikaan 2

1 INRIA Saclay & LIX
2 Department of Mathematics and Computing Science, TU/e.

20th Conference on Applications of Computer Algebra (ACA 2014)
CACTC Session - (Computer Algebra in Coding Theory and Cryptography)

July 9-12, 2014
Public-Key Cryptosystems

Error Correcting Pair: A New Approach to Code-based Cryptography

Introduction
Public-Key Cryptosystems
McEliece Cryptosystem

Proposals
GRS codes
Subcodes of GRS codes
Binary Reed-Muller codes
AG codes
Compact variants
Binary Goppa codes

Decoding by ECP
Examples of the Existence of ECP
ECP for GRS
ECP for subcodes of GRS
ECP for AG
ECP for alternant codes
ECP for Goppa codes
ECP for cyclic codes

Conclusions

Most PKC are based on number-theoretic problems

It can be attacked in polynomial time using Shor's algorithm

Quantum Computer

RSA
ECDSA
HECC

EC

DSA
McEliece introduced the first PKC based on Error-Correcting Codes in 1978.

**Advantages:**

1. Fast encryption (matrix-vector multiplication) and decryption functions.
2. Interesting candidate for post-quantum cryptography.

**Drawback:**

- Large key size.

R. J. McEliece.

*A public-key cryptosystem based on algebraic coding theory.*

Consider any triplet:

\[ t \in \mathbb{N}^* \implies \text{Error-correcting capacity of } C \]

\[ [n, k]_q \text{ linear code with an efficient decoding algorithm} \]

- Let \( G \) be a non structured generator matrix of \( C \).

- “Efficient” decoding algorithm for \( C \) which corrects up to \( t \) errors.
**McEliece Cryptosystem**

### Key Generation

Given:

1. **McEliece Public Key**: $\mathcal{K}_{\text{pub}} = (G, t)$
2. **McEliece Private Key**: $\mathcal{K}_{\text{secret}} = (A_C)$

### Encryption

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

$$y = mG + e$$

where $e$ is a random error vector of weight at most $t$.

### Decryption

Using $\mathcal{K}_{\text{secret}}$, the receiver obtain $m$. 
PROPOSALS

ERROR CORRECTING PAIR: A NEW APPROACH TO CODE-BASED CRYPTOGRAPHY

INTRODUCTION
PUBLIC-KEY CRYPTOSYSTEMS
MCEliece Cryptosystem

PROPOSALS
GRS codes
Subcodes of GRS codes
Binary Reed-Muller codes
AG codes
Compact variants
Binary Goppa codes

DECODING BY ECP
EXAMPLES OF THE EXISTENCE OF ECP
ECP for GRS
ECP for subcodes of GRS
ECP for AG
ECP for alternating codes
ECP for Goppa codes
ECP for cyclic codes

CONCLUSIONS
The class of **GRS** codes was proposed by **Niederreiter** in 1986 for code-based PKC.

**Sidelnikov-Shestakov** in 1992 introduced an algorithm that breaks this proposal in polynomial time.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Key size</th>
<th>Security level</th>
</tr>
</thead>
<tbody>
<tr>
<td>$[256, 128, 129]_{256}$</td>
<td>67 ko</td>
<td>$2^{95}$</td>
</tr>
</tbody>
</table>
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:**

- **Wieschebrink:** (2010)
  - 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 \([n, k]_q\) is itself a GRS code of dimension \(2k - 1\) then we can apply Sidelnikov-Shestakov attack.

- **M-Mártilnez-Pellikaan:** (2012) Give a characterization of the possible parameters that should be used to avoid attacks on the Berger-Loidreau cryptosystem.
Wieschebrick (2010) and Baldi et al. (2011) proposed other variants of the Niederreiter scheme.

 Attacks: Couvreur et al. (2013) provide a cryptanalysis of these schemes.
Binary Reed-Muller codes

The class of Binary Reed-Muller codes was proposed by Sidelnikov in 1994 for code-based PKC.

Minder-Shokrollahi in 2007 presents a sub-exponential time attack.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Key size</th>
<th>Security level</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1024, 176, 128]_2</td>
<td>22.5 ko</td>
<td>2^{12}</td>
</tr>
<tr>
<td>[2048, 232, 256]_2</td>
<td>59, 4 ko</td>
<td>2^{93}</td>
</tr>
</tbody>
</table>
AG codes

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

This system was broken for:

1. Genus \( g = 0 \): by the Sidelnikov-Shestakov attack in 1992.

   GRS codes are Algebraic Geometry codes on the projective line.

2. Genus \( g = 1 \): by Minder-Shokrollahi in 2007.

3. Genus \( g \leq 2 \): by Faure-Minder in 2008.


   We can retrieve the model of the curve (in polynomial time) by
   M-Martínez-Pellikaan-Ruano in 2013.

---

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Key size</th>
<th>Security level</th>
</tr>
</thead>
<tbody>
<tr>
<td>([171, 109, 61]_{128})</td>
<td>16 ko</td>
<td>(2^{66})</td>
</tr>
</tbody>
</table>
In **2005** Gaborit propose to use BCH codes.  
**Size key:** $\sim 1.5 \text{ ko}$, **Security level:** $2^{80}$.

In **2009** Berger, Cayrel, Gaborit and Otmani propose to use alternate quasi-cyclic codes.  
**Size key:** $\sim 750 \text{ o}$, **Security level:** $2^{80}$.

In **2009** Misoczki and Baretto propose to use alternate quasi-dyadic codes.  
**Size key:** $\sim 2.5 \text{ ko}$, **Security level:** $2^{80}$.

**Algebraic Attacks:**

- Otmani, Tillich and Dallot in **2008**.
- Faugère, Otmani, Perret, Tillich in **2010**.
- F. de Portzamparck, Faugère, Otmani, Perret, Tillich in **2014**.

**Compact variants**
The class of **binary goppa** codes was proposed by **McEliece** in 1977 for code-based PKC.

**✓** McEliece with Goppa codes **has resisted cryptanalysis** so far!!

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Key size</th>
<th>Security level</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1024, 524, 101]_2</td>
<td>67 ko</td>
<td>$2^{62}$</td>
</tr>
<tr>
<td>[2048, 1608, 48]_2</td>
<td>412 ko</td>
<td>$2^{96}$</td>
</tr>
</tbody>
</table>
Notation

For all \( \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n \) we define:

- **Star Product:** \( \mathbf{a} \ast \mathbf{b} = (a_1 b_1, \ldots, a_n b_n) \in \mathbb{F}_q^n \)

- **Standard Inner Product:** \( \langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=1}^{n} a_i b_i \in \mathbb{F}_q \)

For all subsets \( A, B \subseteq \mathbb{F}_q^n \) we define:

- \( A \ast B = \langle \{\mathbf{a} \ast \mathbf{b} | \mathbf{a} \in A \text{ and } \mathbf{b} \in B \} \rangle \)

For \( B = A \implies A \ast A \) is denoted as \( A^{(2)} \)

- \( A \perp B \iff \langle \mathbf{a}, \mathbf{b} \rangle = 0 \ \forall \ \mathbf{a} \in A \text{ and } \mathbf{b} \in B \)
Let $C$ be a linear code. We denote by:

1. $k(C) = \text{dimension of } C$
2. $d(C) = \text{minimum distance of } C$

**Error-Correcting Pairs (ECP)**

Let $C$ be an $\mathbb{F}_q$ linear code of length $n$. The pair $(A, B)$ of $\mathbb{F}_{q^m}$-linear codes of length $n$ is a $t$-ECP for $C$ over $\mathbb{F}_{q^m}$ if the following properties hold:

1. $(A \ast B) \perp C$.
2. $k(A) > t$.
3. $d(B^\perp) > t$.
4. $d(A) + d(C) > n$.

An $[n, k]_q$ code which has a $t$-ECP over $\mathbb{F}_q$ has a decoding algorithm with complexity $O((nm)^w)$.
**Decoding by Error-Correcting Pairs (ECP)**

Let:
- \( C, A \) and \( B \) be linear subspaces of \( \mathbb{F}_q^n \)
- \( y \in \mathbb{F}_q^n \) be the received word with error vector \( e \)

Compute:
\[
K_y = \{ a \in A \mid \langle y, a \ast b \rangle = 0, \text{ for all } b \in B \}
\]

**Remark: Condition 1**

If \( A \ast B \subseteq C^\perp \) \( \implies \) \( K_y = K_e \)

Let \( J \) be a subset of \( \{1, \ldots, n\} \), define:
\[
A(J) = \{ a \in A \mid a_j = 0, \text{ for all } j \in J \}
\]

**Lemma 1: Condition 3**

Let \( I = \text{supp}(e) \) and \( A \ast B \subseteq C^\perp \). If \( d(B^\perp) > t \) \( \implies \) \( A(I) = K_y \)
**Decoding by Error-Correcting Pairs (ECP) II**

**Lemma 2: Condition 2**

If \( l = \text{supp}(e) \) and \( k(A) > t \) \( \iff \exists a \in K_y \setminus \{0\} \)

**Lemma 3: Condition 4**

Let \( a \in K_y \setminus \{0\} \) and define \( J = \{ j \mid a_j = 0 \} \). Then:

1. If \( d(B^\perp) > t \) then \( l = \text{supp}(e) \subseteq J \)
2. If \( d(A) + d(C) > n \) then there exists a unique solution to:

\[
Hx^T = Hy^T \text{ such that } x_j \neq 0 \text{ for all } j \in J
\]
Decoding by Error-Correcting Pairs (ECP) III

1. Compute:

\[ K_y = \{ a \in A | \langle y, a \ast b \rangle = 0, \text{ for all } b \in B \} \]

Find the zero space of a set of linear equations over \( \mathbb{F}_q \)

2. If \( K_y = 0 \iff \text{The received word has more than } t \text{ errors} \)

   Else take a nonzero \( a \in K_y = A(I) \) and define \( J = \{ j | a_j = 0 \} \)

3. Find \( e \in \mathbb{F}_q^n \) by solving the following linear equation (which has a unique solution):

\[ Hx^T = Hy^T \quad \text{such that} \quad x_j \neq 0 \text{ for } j \in J \]

Solve linear equations over \( \mathbb{F}_q \)

**Complexity:** \( \sim \mathcal{O}(n^w) \)
Motivation

“*At the heart of any public-key cryptosystem is a one-way function - a function* \( y = f(x) \) *that is easy to evaluate but for which is computationally infeasible (one hopes) to find the inverse* \( x = f^{-1}(y) \).”

N. Koblitz, A. Menezes.

*The brave new world of bodacious assumptions in cryptography.*


Let \( C_t \) the class of linear codes over \( \mathbb{F}_q \) that have a \( t \)-ECP over an extension of \( \mathbb{F}_q \).

\[ \rightarrow \quad \text{This family have an efficient decoding algorithm} \quad \Rightarrow \quad \text{they are appropriate for code-based cryptography.} \]

\[ \rightarrow \quad \text{Most families of codes used in code-based cryptography belongs to} \quad C_t. \text{ (Like GRS codes, Goppa codes, AG codes ... )} \]

\[ \rightarrow \quad \text{We proposed to use the subclass of} \quad C_t \text{ formed by those linear codes} \quad C \text{ whose error correcting pair is not easily reconstructed from} \quad C, \text{ i.e. we consider the following one way function:} \]

\[ x = (A, B) \quad \mapsto \quad y = A \ast B, \]

where \( (A, B) \) is a \( t \)-ECP.
Examples of the Existence of ECP

- $t$-ECP for Generalized Reed-Solomon (GRS) codes
- $t$-ECP for Algebraic-Geometric (AG) codes.
- $t$-ECP for Alternate codes.
- $t$-ECP for Goppa codes.
- $t$-ECP for cyclic codes.

**Question:**

- If a code has a $t$-ECP how difficult / easy is to retrieve such a pair?
Let

- $a = (a_1, \ldots, a_n)$ be an $n$-tuple of mutually distinct elements of $\mathbb{F}_q$.
- $b = (b_1, \ldots, b_n)$ be an $n$-tuple of nonzero elements of $\mathbb{F}_q$.
- $k \in \mathbb{N} : k < n$

The **GRS code** $\text{GRS}_k(a, b)$ is defined by:

$$\text{GRS}_k(a, b) = \{b * f(a) = (b_1 f(a_1), \ldots, b_n f(a_n)) \mid f \in \mathbb{F}_q[X]_{<k}\}$$
The GRS$_k(a, b)$ is an MDS code with parameters $[n, k, n - k + 1]_q$.

A generator matrix of GRS$_k(a, b)$ is given by

$$G_{a,b} = \begin{pmatrix} b_1 & \cdots & b_n \\ b_1a_1 & \cdots & b_na_n \\ \vdots & \ddots & \vdots \\ b_1a_1^{k-1} & \cdots & b_na_n^{k-1} \end{pmatrix} \in \mathbb{F}_q^{k \times n}$$

The dual of a GRS code is again a GRS code. In particular:

$$\text{GRS}_k(a, b)^\perp = \text{GRS}_{n-k}(a, c)$$

for some $c$ explicitly known

The $\text{GRS}_k(a, b)^\perp$ is an MDS code with parameters $[n, n - k, k + 1]_q$. 

$$\text{GRS}_k(a, b)^\perp = \text{GRS}_{n-k}(a, c)$$

for some $c$ explicitly known.
$t$-ECP for GRS I

Note that: $\text{GRS}_k(a, b) \ast \text{GRS}_l(a, c) = \text{GRS}_{k+l-1}(a, b \ast c)$

Let

$$A = \text{GRS}_{t+1}(a, b_1), \quad B = \text{GRS}_t(a, b_2) \quad \text{and} \quad C = \text{GRS}_{2t}(a, b_1 \ast b_2)^\perp$$

then $(A, B)$ is a $t$-ECP for $C$.

**E.1** $A \ast B = \text{GRS}_{2t}(a, b_1 \ast b_2) = C^\perp \Rightarrow (A \ast B) \perp C$

**E.2** $k(A) > t$

**E.3** $B^\perp = \text{GRS}_{n-t}(a, c_2) \Rightarrow d(B^\perp) = t + 1 > t$

**E.4** $d(A) + d(C) = (n - t) + (2t + 1) > n$
Conversely, let \( C = \text{GRS}_{n-2t}(a, b) \) then

\[
A = \text{GRS}_{t+1}(a, c) \quad \text{and} \quad B = \text{GRS}_t(a, 1)
\]

is a \( t \)-ECP for \( C \) where \( c \in (\mathbb{F}_q \setminus \{0\})^n \) verifies that

\[
C^\perp = \text{GRS}_{n-2t}(a, b)^\perp = \text{GRS}_{2t}(a, c).
\]

Moreover an \([n, n - 2t, 2t + 1]_q\) code that has a \( t \)-ECP is a GRS code.
Let: $C \subseteq D$

$\Rightarrow D$ be a code that has $(A, B)$ as $t$-ECP

$\Rightarrow C$ be a subcode of $D$

Then $(A, B)$ is also a $t$-ECP for $C$. 
An AG code is defined by a triplet
\[ (\mathcal{X}, \mathcal{P}, \mathcal{E}) \]

\( \mathcal{X} \) is an algebraic curve of genus \( g \) over the finite field \( \mathbb{F}_q \)

**Algebraic Curve = Smooth, Projective and Geometrically Connected Curve**

Whose defining equations are polynomials with coefficients in \( \mathbb{F}_q \).

\( \mathcal{P} = (P_1, \ldots, P_n) \) is an \( n \)-tuple of mutually distinct \( \mathbb{F}_q \)-rational points of \( \mathcal{X} \)

\( D_\mathcal{P} \) denotes the divisor \( D_\mathcal{P} = P_1 + \cdots + P_n \)
An AG code is defined by a triplet \((\mathcal{X}, \mathcal{P}, E)\). 

- \(\mathcal{X}\) is an algebraic curve of genus \(g\) over the finite field \(\mathbb{F}_q\).

- \(\mathcal{P} = (P_1, \ldots, P_n)\) is an \(n\)-tuple of mutually distinct \(\mathbb{F}_q\)-rational points of \(\mathcal{X}\).

\(D_\mathcal{P}\) denotes the divisor \(D_\mathcal{P} = P_1 + \cdots + P_n\).
An AG code is defined by a triplet
\((\mathcal{X}, \mathcal{P}, E)\)

\(E\) is an \(\mathbb{F}_q\)-divisor of \(\mathcal{X}\) such that
\[ \text{supp}(E) \cap \text{supp}(D_P) = \emptyset \]
Let us consider the triplet:

$$\big(\mathcal{X}, \mathcal{P}, E\big)$$

- $\mathcal{X}$ is an algebraic curve of genus $g$ over the finite field $\mathbb{F}_q$.
- $\mathcal{P}$ is an $n$-tuple of distinct $\mathbb{F}_q$-rational points of $\mathcal{X}$.
- $E$ is an $\mathbb{F}_q$-divisor of $\mathcal{X}$ such that $\text{supp}(E) \cap \text{supp}(D_{\mathcal{P}}) = \emptyset$.

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

$$\text{ev}_{\mathcal{P}} : L(E) \rightarrow \mathbb{F}_q^n$$

$$f \mapsto \text{ev}_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$$

**Algebraic Geometry Code (AG code)**

The AG code associated to the triplet $(\mathcal{X}, \mathcal{P}, E)$ is:

$$C_L(\mathcal{X}, \mathcal{P}, E) = \{\text{ev}_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n)) | f \in L(E)\}$$
Error correcting pair: A new approach to code-based cryptography

Introduction
Public-key cryptosystems
McEliece cryptosystem

Proposals
GRS codes
Subcodes of GRS codes
Binary Reed-Muller codes
AG codes
Compact variants
Binary Goppa codes

Decoding by ECP
Examples of the existence of ECP
ECP for GRS
ECP for subcodes of GRS
ECP for AG
ECP for alternant codes
ECP for Goppa codes
ECP for cyclic codes

Conclusions

Algebraic Geometry codes III

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 \( C_L(\mathcal{X}, \mathcal{P}, E) \)

**Theorem I** [Parameters of an AG code]

Let \( C = C_L(\mathcal{X}, \mathcal{P}, E) \). If \( \deg(E) < n \) then

\[
k(C) \geq \deg(E) + 1 - g \quad \text{and} \quad d(C) \geq n - \deg(E)
\]

Moreover, if \( n > \deg(E) > 2g - 2 \) then \( k(C) = \deg(E) - g + 1 \).
**Algebraic Geometry codes IV**

**Dual of an AG code**

Let:

- \( \omega \) be a **differential form** with a simple pole and residue 1 at \( P_j \) for all \( j = 1, \ldots, n \).
- \( K \) be the **canonical divisor** of \( \omega \).

Then

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

with

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

**Theorem II [Parameters of the Dual of an AG code]**

Let \( C = C_L(\mathcal{X}, \mathcal{P}, E) \). If \( \deg(E) > 2g - 2 \) then

\[
k(C^\perp) \geq n - \deg(E) - 1 + g \quad \text{and} \quad d(C^\perp) \geq \deg(E) - 2g + 2
\]

Moreover, if \( n > \deg(E) > 2g - 2 \) then \( k(C^\perp) = n - \deg(E) - 1 + g \)
Consider the AG code

\[ C = C_L \left( \mathcal{X}, \mathcal{P}, E \right) \perp \]

**Theorem [Pellikaan - 1992]**

The pair of codes \((A, B)\) defined by

\[ A = C_L(\mathcal{X}, \mathcal{P}, F) \quad \text{and} \quad B = C_L(\mathcal{X}, \mathcal{P}, E - F) \]

with \(\deg(E) > \deg(F) \geq t + g\) is a \(t\)-ECP for \(C\).

Such a pair **always exists** whenever

\[ \deg(E) > 2g - 2 \quad \text{and} \quad t = t^* = \left\lfloor \frac{d^* - 1 - g}{2} \right\rfloor. \]

where \(d^* = \deg(E) - 2g + 2\) is the designed minimum distance of \(C\).
**Corollary [MAIN COROLLARY]**

Let \( C = C_L(\mathcal{X}, \mathcal{P}, E) \bot \) and \( B = C_L(\mathcal{X}, \mathcal{P}, E - F) \) with \( \deg(F) \geq t + g \).

And let us define \( A_0 = (B \ast C) \bot \). Then \((A_0, B)\) is a \( t\)-ECP for \( C \).

In order to compute a \( t\)-ECP for \( C = C_L(\mathcal{X}, \mathcal{P}, E) \), it suffices to compute a code of type

\[
C_L(\mathcal{X}, \mathcal{P}, E - F)
\]

for some divisor \( F \) with

\[
\deg(F) \geq t + g
\]
**Public Key:**

\[ K_{\text{pub}} = G \quad \text{and} \quad t^* = \left\lfloor \frac{d^* - g - 1}{2} \right\rfloor \]

where:

- \( G \) is a generator matrix of the public code:

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

- \( d^* = \deg(E) - 2g + 2 \) is the designed minimum distance of \( C_{\text{pub}} \)

→ **Our** \( t^* \) **seems reasonable if** \( K_{\text{secret}} \) **is based on ECP.**

\[ t^* = \left\lfloor \frac{d^* - g - 1}{2} \right\rfloor \leq t = \left\lfloor \frac{d^* - 1}{2} \right\rfloor = \text{actual error-correction capability of } C \]

→ **Future work!!!**
**THE P-FILTRATION**

Let $P = P_1$ be a point of the $n$-tuple $\mathcal{P}$.

We focus on the sequence of codes:

$$\mathcal{B}_i := (C_L(\mathcal{X}, \mathcal{P}, E - iP_1))_{i \in \mathbb{N}}$$

**Which Elements of the Sequence do We know?**

1. From a generator matrix of $C_{pub} = C_L(\mathcal{X}, \mathcal{P}, E)^\perp$ one can compute $C_L(\mathcal{X}, \mathcal{P}, E)$.

   ➔ Computed by **Gaussian elimination**.

2. $\mathcal{B}_0 = C_L(\mathcal{X}, \mathcal{P}, E)$.

3. $\mathcal{B}_1$ is the set of codewords of the code $\mathcal{B}_0$ which are zero at position $P_1$.

   ➔ Computed by **Gaussian elimination**.

The codes $\mathcal{B}_0$ and $\mathcal{B}_1$ are known.
**Effective Computation - Algorithm I**

**Proposition**

Let $F$, $G$ be two divisors on $\mathcal{X}$ such that

\[
\text{deg}(F) \geq 2g \quad \text{and} \quad \text{deg}(G) \geq 2g + 1
\]

Then,

\[
\mathcal{C}_L(\mathcal{X}, \mathcal{P}, F) \ast \mathcal{C}_L(\mathcal{X}, \mathcal{P}, G) = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, F + G)
\]

**How to compute $\mathcal{B}_2$?**

$\mathcal{B}_2$ is the solution space of the following problem

\[
\mathbf{z} \in \mathcal{B}_1 \quad \text{and} \quad \mathbf{z} \ast \mathcal{B}_0 \subseteq (\mathcal{B}_1)^{(2)}
\]  

\[
\mathcal{C}_L(\mathcal{X}, \mathcal{P}, E - 2\mathcal{P}_1) \ast \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E - \mathcal{P}_1) \subseteq \mathcal{C}_L(\mathcal{X}, \mathcal{P}, 2E - 2\mathcal{P}_1)
\]
**Effective Computation - Algorithm I**

**Theorem I:** If we know $B_{s-1}$ and $B_s$ we can compute $B_{s+1}$

$B_{s+1}$ is the solution space of the following problem

$$z \in B_s \quad \text{and} \quad z \ast B_{s-1} \subseteq (B_s)^{(2)} \quad \text{(2)}$$

$$\left( C_L(\mathcal{X}, \mathcal{P}, E - (s + 1)P_1) \ast C_L(\mathcal{X}, \mathcal{P}, E - (s - 1)P_1) \right) \subseteq C_L(\mathcal{X}, \mathcal{P}, 2E - 2sP_1)$$

If $s \geq 1$ and $\frac{n}{2} > \deg(E) \geq 2g + s + 1$.

$(t^* + g)$ repeated applications of **Theorem I** determines the code $B_{t^* + g}$. 

**Construct** $C_L(\mathcal{X}, \mathcal{P}, E - F)$ with $\deg(F) \geq t^* + g$ from $C = C_L(\mathcal{X}, \mathcal{P}, E)^{\perp}$. 

---

**Error Correcting Pair:** A new approach to code-based cryptography

**Introduction**

Public-Key Cryptosystems
MCELiece Cryptosystem

**Proposals**

GRS codes
Subcodes of GRS codes
Binary Reed-Muller codes
AG codes
Compact variants
Binary Goppa codes

Decoding by ECP

Examples of the Existence of ECP
ECP for GRS
ECP for subcodes of GRS
ECP for AG
ECP for Alternant codes
ECP for Goppa codes
ECP for cyclic codes

Conclusions
**Effective Computation - Algorithm II**

We can do **better** by **decreasing** the number of iterations and **relaxing** the parameters conditions ⇒ **Algorithm II**

→ **Algorithm I:**

\[ B_0 \supseteq B_1 \supseteq B_2 \supseteq B_3 \supseteq \ldots \supseteq B_{t^*+g-1} \supseteq B_{t^*+g} \]

Solve \((t^* + g)\) systems of linear equations

→ **Algorithm II:**

\[ B_0 \supseteq B_1 \supseteq B_2 \supseteq B_4 \supseteq \ldots \supseteq B_{\frac{t^*+g}{2}} \supseteq B_{t^*+g} \]

Solve \(2 \left\lceil \log_2 (t^* + g) \right\rceil + 2\) systems of linear equations
**Error correcting pair: a new approach to code-based cryptography**

**Introduction**

**Public-Key Cryptosystems**

**McEliece Cryptosystem**

**Proposals**

GRS codes

Subcodes of GRS codes

Binary Reed-Muller codes

AG codes

Compact variants

Binary Goppa codes

**Decoding by ECP**

**Examples of the existence of ECP**

ECP for GRS

ECP for subcodes of GRS

ECP for AG

ECP for alternant codes

ECP for Goppa codes

ECP for cyclic codes

**Conclusions**

---

**Polynomial time attack against McEliece based in AG codes - Retrieving an ECP**

**Public Key:**  \( \mathcal{K}_{pub} = C_{pub} = C_L(\mathcal{X}, \mathcal{P}, E)\perp \) and  \( t = \left\lfloor \frac{d^* - g - 1}{2} \right\rfloor \)

**The Algorithm:** Suppose that  \( \frac{n}{2} \geq \deg(E) \).

**STEP 1.** Determine the values  \( g \) and  \( \deg(E) \) using the following Proposition.

**Proposition**

If  \( 2g + 1 \leq \deg(E) < \frac{1}{2}n \).

Then,  \( \deg(E) = k(C^{(2)}) - k(C) \) and  \( g = k(C^{(2)}) - 2k(C) + 1 \)

**STEP 2.** Compute the code  \( B_{t^* + g} = C_L(\mathcal{X}, \mathcal{P}, E - (t^* + g)P_1) \), using one of the algorithms described in §5.1

**STEP 3.** Deduce an ECP from  \( B \).

**Corollary:** Let  \( B \) of type  \( C_L(\mathcal{X}, \mathcal{P}, E - F) \) with  \( \deg(F) \geq t^* + g \).

Let us define  \( A_0 = (B \ast C)\perp \). Then  \( (A_0, B) \) is a  \( t \)-ECP for  \( C = C_L(\mathcal{X}, \mathcal{P}, E)\perp \).
Complexity of the Attack:

The costly part of the attack is the computation of the code $B$

We can apply one of the algorithms of §5.1

Computing:

1. a generator matrix of $C^{(2)}$
2. and then apply Gaussian elimination to such matrix

costs

$$O \left( \binom{k}{2} n + \binom{k}{2} n^2 \right) \sim O \left( k^2 n^2 \right)$$ operations in $\mathbb{F}_q$.

Roughly speaking the cost of our attack is about $O \left( (\lambda + 1)n^4 \right)$

where:

1. $\lambda =$ Linear systems to solve depending on the chosen algorithm from §5.1
2. The term $(\lambda + 1)$ is the cost of computing a non-degenerated code.
Example:

We summarize in the following tables the average running times of our algorithm for several codes.

The attack has been implemented with MAGMA.

The work factor $w$ of and ISD attack is given. These work factors have been computed thanks to Christiane Peter’s Software.

Remark: ISD’s average complexity is

$$O \left( k^2 \frac{n}{t} \frac{\binom{n}{t}}{\binom{n-k}{t}} \right)$$ operations in $\mathbb{F}_q$
**Example I: Hermitian Curves**

The **Hermitian curve** $\mathcal{H}_r$ over $\mathbb{F}_q$ with $q = r^2$ is defined by the affine equation

$$Y^r + Y = X^{r+1}$$

→ This curve has $P_\infty = (0 : 1 : 0)$ as the only point at infinity.

Take:

→ $E = mP_\infty$

→ $\mathcal{P}$ be the $n = q\sqrt{q} = r^3$ affine $\mathbb{F}_q$-rational points of the curve.

The following table considers different codes of type $C_L(\mathcal{H}_r, \mathcal{P}, E)\perp$ with $n > \deg(E) > 2g - 2$.

<table>
<thead>
<tr>
<th>$q$</th>
<th>$g$</th>
<th>$n$</th>
<th>$k$</th>
<th>$t$</th>
<th>$w$</th>
<th>key size</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>$7^2$</td>
<td>21</td>
<td>343</td>
<td>193</td>
<td>54</td>
<td>$2^{84}$</td>
<td>163 ko</td>
<td>74 s</td>
</tr>
<tr>
<td>$9^2$</td>
<td>36</td>
<td>729</td>
<td>404</td>
<td>126</td>
<td>$2^{182}$</td>
<td>833 ko</td>
<td>21 min</td>
</tr>
<tr>
<td>$11^2$</td>
<td>55</td>
<td>1331</td>
<td>885</td>
<td>168</td>
<td>$2^{311}$</td>
<td>2730 ko</td>
<td>67 min</td>
</tr>
</tbody>
</table>

**Table:** Comparison with Hermitian codes

$w$ computed with Christiane Peters software
**Error Correcting Pair:** A new approach to code-based cryptography

**Introduction**

Public-Key Cryptosystems
MCElience Cryptosystem

Proposals
GRS codes
Subcodes of GRS codes
Binary Reed-Muller codes
AG codes
Compact variants
Binary Goppa codes

Decoding by ECP
Examples of the Existence of ECP
ECP for GRS
ECP for subcodes of GRS
ECP for AG
ECP for alternative codes
ECP for Goppa codes
ECP for cyclic codes

Conclusions

---

**Alternant codes**

Let

- \( \mathbf{a} = (a_1, \ldots, a_n) \) be an \( n \)-tuple of **mutually distinct** elements of \( \mathbb{F}_{q^m} \).
- \( \mathbf{b} = (b_1, \ldots, b_n) \) be an \( n \)-tuple of **nonzero** elements of \( \mathbb{F}_{q^m} \).

**\( \text{GRS}_k(\mathbf{a}, \mathbf{b}) \)** be the GRS code over \( \mathbb{F}_{q^m} \) of dimension \( k \).

The **alternant code** \( \text{Alt}_r(\mathbf{a}, \mathbf{b}) \) is the \( \mathbb{F}_q \)-linear restriction:

\[
\text{Alt}_r(\mathbf{a}, \mathbf{b}) = \mathbb{F}_q^n \cap (\text{GRS}_r(\mathbf{a}, \mathbf{b}))^\perp
\]

**Parameters of \( \text{Alt}_r(\mathbf{a}, \mathbf{b}) \)**

The \( \text{Alt}_r(\mathbf{a}, \mathbf{b}) \) has parameters \([n, k, d]_q \) with:

\[
k \geq n - mr \quad \text{and} \quad d \geq r + 1
\]

Every \([n, k, d] \) linear code with \( d \geq 2 \) is an **alternant code**!
t-ECP for Alternant codes

Let $C = \text{Alt}_{2t}(a, b)$. Then:

$$d(C) \geq 2t + 1 \quad \text{and} \quad C \subseteq (\text{GRS}_{2t+1}(a, b))^\perp$$

Let

$$A = \text{GRS}_{t+1}(a, 1), \quad \text{and} \quad B = \text{GRS}_t(a, b)$$

then $(A, B)$ is a $t$-ECP over $\mathbb{F}_{q^m}$ for $C$.

No known structural attacks against code-base PKC using Alternant codes
Goppa codes

Let

- \( \mathbf{a} = (a_1, \ldots, a_n) \) be an \( n \)-tuple of mutually distinct elements of \( \mathbb{F}_{q^m} \).
- \( g \) be a polynomial with coefficients in \( \mathbb{F}_{q^m} \) such that
  \[ g(a_j) \neq 0 \quad \text{for all} \quad j = 1, \ldots, n \]

The **Goppa code** \( \Gamma(\mathbf{a}, g) \) is the \( \mathbb{F}_q \)-linear code defined by:

\[
\Gamma(\mathbf{a}, g) = \left\{ \mathbf{c} \in \mathbb{F}_q^n \mid \sum_{j=1}^n \frac{c_j}{\mathbf{X} - a_j} \equiv 0 \mod g(\mathbf{X}) \right\}
\]
**Goppa Codes are Alternant Codes**

Let

- \( a = (a_1, \ldots, a_n) \) be an \( n \)-tuple of mutually distinct elements of \( \mathbb{F}_{q^m} \).
- \( g \) be a Goppa polynomial of degree \( r \).
- \( b = (b_1, \ldots, b_n) \) be an \( n \)-tuple of nonzero elements of \( \mathbb{F}_{q^m} \) such that
  \[ b_j = \frac{1}{g(a_j)} \]

Then: \( \Gamma(a, g) = \text{Alt}_r(a, b) \implies \text{it has an } \left\lfloor \frac{r}{2} \right\rfloor \text{-ECP} \)

No known structural attacks against code-base PKC using Binary Goppa codes
\textbf{t-ECP for cyclic codes}

\begin{itemize}
  \item \textbf{ECP} for cyclic codes were found \textbf{beyond half the BCH bound} by Duursma (1993) and Kötter (1996).
\end{itemize}

\begin{itemize}
  \item I. Duursma
    \textit{Decoding codes from curves and cyclic codes.}
  \item I. Duursma, R. Kötter.
    \textit{Error-locating pairs for cyclic codes.}
  \item R. Kötter.
    \textit{On algebraic decoding of algebraic-geometric and cyclic codes.}
\end{itemize}
Conclusions

We propose for the McEliece cryptosystem the class of codes $C_t$
- with a $t$-ECP
- but whose error-correcting pair is not easily reconstructed from a given generator matrix.

That is: the security of the McEliece cryptosystem is not only based on the inherent intractability of bounded distance decoding but on the one-way function:

$$x = (A, B) \quad \mapsto \quad y = A \ast B$$

First Question: If a code has a $t$-ECP, how difficult/easy is to retrieve such a pair?

Second Question: It is possible to distinguish a random code from one having a $t$-ECP?
THANK YOU FOR YOUR ATTENTION!