Error-correcting pairs
and majority coset decoding
for public-key cryptosystems

Ruud Pellikaan
g.r.pellikaan@tue.nl
joint work with
Irene Márquez-Corbella

Crypto Working Group
Utrecht, 14 June 2013
Introduction and content

- Error-correcting pairs
  - Generalized Reed-Solomon codes
  - Alternant codes
  - Goppa codes
- $t$-Error-correcting pair corrects $t$-errors
- Algebraic geometry codes
- Majority coset decoding
- Code-based cryptography
Error-correcting codes

A linear block code: $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$

Parameters $[n, k, d]$:

- $n =$ length
- $k =$ dimension of $C$
- $d =$ minimum distance of $C$

$$d = \min \{|d(x, y) | x, y \in C, x \neq y\}|$$

$t =$ error-correcting capacity of $C$

$$t = \left\lfloor \frac{d - 1}{2} \right\rfloor$$
The **standard inner product** is defined by

\[ a \cdot b = a_1 b_1 + \cdots + a_n b_n \]

For two subsets \(A\) and \(B\) of \(\mathbb{F}_q^n\), \(A \perp B\) if and only if \(a \cdot b = 0\) for all \(a \in A\) and \(b \in B\).

Let \(a\) and \(b\) in \(\mathbb{F}_q^n\),

The **star product** is defined by coordinatewise multiplication:

\[ a \star b = (a_1 b_1, \ldots, a_n b_n) \]

For two subsets \(A\) and \(B\) of \(\mathbb{F}_q^n\),

\[ A \star B = \{ a \star b \mid a \in A \text{ and } b \in B \} \]
Let $C$ be a linear code in $\mathbb{F}_q^n$

The pair $(A, B)$ of linear subcodes of $\mathbb{F}_{q^m}^n$ is called a $t$-error correcting pair (ECP) over $\mathbb{F}_{q^m}$ for $C$ if

E.1 \quad (A \ast B) \perp C
E.2 \quad k(A) > t
E.3 \quad d(B^\perp) > t
E.4 \quad d(A) + d(C) > n
Generalized Reed-Solomon codes

Let \( a = (a_1, \ldots, a_n) \) be an \( n \)-tuple of mutually distinct elements of \( \mathbb{F}_q \)

Let \( b = (b_1, \ldots, b_n) \) be an \( n \)-tuple of nonzero elements of \( \mathbb{F}_q \)

Evaluation map:

\[
ev_{a,b}(f(X)) = (f(a_1)b_1, \ldots, f(a_n)b_n)
\]

\( \text{GRS}_k(a, b) = \{ \ev_{a,b}(f(X)) \mid f(X) \in \mathbb{F}_q[X], \deg(f(X)) < k \} \)

Parameters: \([n, k, n - k + 1]\) if \( k \leq n \)

Furthermore

\[
ev_{a,b}(f(X)) \ast \ev_{a,c}(g(X)) = \ev_{a,b}(f(X)g(X)) \ast c
\]

\[
\langle \text{GRS}_k(a, b) \ast \text{GRS}_l(a, c) \rangle = \text{GRS}_{k+l-1}(a, b \ast c)
\]
Let $C = \text{GRS}_{n-2t}(a, b)$

Then $C$ has parameters: $[n, n - 2t, 2t + 1]$

and $C^\perp = \text{GRS}_{2t}(a, c)$ for some $c$

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

Then $A \ast B \subseteq C^\perp$

$A$ has parameters $[n, t + 1, n - t]$

$B$ has parameters $[n, t, n - t + 1]$

So $B^\perp$ has parameters $[n, n - t, t + 1]$

Hence $(A, B)$ is a $t$-error-correcting pair for $C$

Conversely an $[n, n - 2t, 2t + 1]$ code that has a $t$-ECP is a GRS code
Alternant codes

Let \( a \) be an \( n \)-tuple of mutually distinct elements of \( \mathbb{F}_{q^m} \).
Let \( b \) be an \( n \)-tuple of nonzero elements of \( \mathbb{F}_{q^m} \).

Let \( GRS_k(a, b) \) be the GRS code over \( \mathbb{F}_{q^m} \) of dimension \( k \).

The alternate code \( ALT_r(a, b) \) is the \( \mathbb{F}_q \)-linear restriction

\[
ALT_r(a, b) = \mathbb{F}_q^n \cap (GRS_r(a, b))^\perp
\]

Then \( ALT_r(a, b) \) has parameters \([n, k, d]_q\) with

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

Every linear code of minimum distance at least 2 is an alternant code!
$t$-ECP for $\text{ALT}_{2t}(a, b)$

Let $C = \text{ALT}_{2t}(a, b)$
Then $C$ has minimum distance $d \geq 2t + 1$
and $C \subseteq (\text{GRS}_{2t+1}(a, b))^\perp$

Let $A = \text{GRS}_{t+1}(a, 1)$ and $B = \text{GRS}_t(a, b)$
Then $A \ast B \subseteq \text{GRS}_{2t+1}(a, b)$
Then $(A \ast B) \perp C$

A has parameters $[n, t + 1, n - t]$
B has parameters $[n, t, n - t + 1]$
So $B^\perp$ has parameters $[n, n - t, t + 1]$

Hence $(A, B)$ is a $t$-error-correcting pair over $\mathbb{F}_{q^m}$ for $C$
Goppa codes

Let \( L = (a_1, \ldots, a_n) \) be an \( n \)-tuple of \( n \) distinct elements of \( \mathbb{F}_{q^m} \)

Let \( g \) be a polynomial with coefficients in \( \mathbb{F}_{q^m} \) such that

\[
g(a_j) \neq 0 \quad \text{for all } j
\]

Then \( g \) is called **Goppa polynomial** with respect to \( L \)

Define the \( \mathbb{F}_q \)-linear **Goppa code** \( \Gamma(L, g) \) by

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

Let $L = a = (a_1, \ldots, a_n)$
Let $g$ be a Goppa polynomial of degree $r$

Let $b_j = 1/g(a_j)$
Then

$$\Gamma(L, g) = ALT_r(a, b)$$

Hence $\Gamma(L, g)$ has parameters $[n, k, d]_q$ with

$$k \geq n - mr \text{ and } d \geq r + 1$$

and has an $\left\lfloor r/2 \right\rfloor$-error-correcting pair
Binary Goppa codes

Let \( L = a = (a_1, \ldots, a_n) \)

Let \( g \) be a Goppa polynomial with coefficients in \( \mathbb{F}_{2^m} \) of degree \( r \)

Suppose moreover that \( g \) has no square factor

Then

\[ \Gamma(L, g) = \Gamma(L, g^2) \]

Hence \( \Gamma(L, g) \) has parameters \([n, k, d]_q\) with

\[ k \geq n - mr \quad \text{and} \quad d \geq 2r + 1 \]

and has an \( r \)-error-correcting pair
Theory of error-correcting pairs

Let $C$ be a linear code in $\mathbb{F}_q^n$

The pair $(A, B)$ of linear subcodes of $\mathbb{F}_{q^m}^n$ is called a t-error correcting pair (ECP) over $\mathbb{F}_{q^m}$ for $C$ if

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

Let $(A, B)$ be linear subcodes of $\mathbb{F}_{q^m}^n$ that satisfy E.1, E.2, E.3 and

E.5 $d(A^\perp) > 1$
E.6 $d(A) + 2t > n$

Then $d(C) \geq 2t + 1$ and $(A, B)$ is a t-ECP for $C$
Kernel of a received word

Let $A$ and $B$ be linear subspaces of $\mathbb{F}_{q^m}^n$
Let $r \in \mathbb{F}_q^n$ be a received word
Define the kernel

$$K(r) = \{ a \in A \mid (a \ast b) \cdot r = 0 \text{ for all } b \in B \}$$

Lemma
Let $C$ be an $\mathbb{F}_q$-linear code of length $n$
Let $r$ be a received word with error vector $e$
So $r = c + e$ for some $c \in C$
If $A \ast B \subseteq C^\perp$, then

$$K(r) = K(e)$$
Kernel for a GRS code

Let $A = \text{GRS}_{t+1}(a, 1)$ and $B = \text{GRS}_t(a, 1)$ and $C = \langle A \ast B \rangle^\perp$

Let
\[ a_i = \text{ev}_{a,1}(X^{i-1}) \text{ for } i = 1, \ldots, t + 1 \]
\[ b_j = \text{ev}_{a,1}(X^j) \text{ for } j = 1, \ldots, t \]
\[ h_l = \text{ev}_{a,1}(X^l) \text{ for } l = 1, \ldots, 2t \]

Then
\( a_1, \ldots, a_{t+1} \) is a basis of $A$
\( b_1, \ldots, b_t \) is a basis of $B$
\( h_1, \ldots, h_{2t} \) is a basis of $C^\perp$

Furthermore
\[ a_i \ast b_j = \text{ev}_{a,1}(X^{i+j-1}) = h_{i+j-1} \]
Matrix of syndromes for a GRS code

Let $r$ be a received word and $s = rH^T$ its syndrome.

Then

$$(b_j \ast a_i) \cdot r = s_{i+j-1}.$$ 

To compute the kernel $K(r)$ we have to compute the null space of the matrix of syndromes

$$
\begin{pmatrix}
  s_1 & s_2 & \cdots & s_t & s_{t+1} \\
  s_2 & s_3 & \cdots & s_{t+1} & s_{t+2} \\
  \vdots & \vdots & \ddots & \vdots & \vdots \\
  s_t & s_{t+1} & \cdots & s_{2t-1} & s_{2t}
\end{pmatrix}
$$
Error location

Let \((A, B)\) be a \(t\)-ECP for \(C\)
Let \(J\) be a subset of \(\{1, \ldots, n\}\)
Define the subspace of \(A\)

\[
A(J) = \{ a \in A \mid a_j = 0 \text{ for all } j \in J \}
\]

Lemma
Let \((A \ast B) \perp C\)
Let \(e\) be an error vector of the received word \(r\)
If \(I = \text{supp}(e) = \{ i \mid e_i \neq 0 \}\), then

\[
A(I) \subseteq K(r)
\]

If moreover \(d(B^\perp) > \text{wt}(e)\), then \(A(I) = K(r)\)
Basic algorithm

Let \((A, B)\) be a \(t\)-ECP for \(C\) with \(d(C) \geq 2t + 1\)

Suppose that \(c \in C\) is the code word sent and \(r = c + e\) is the received word for some error vector \(e\) with \(\text{wt}(e) \leq t\)

The basic algorithm for the code \(C\):
- Compute the kernel \(K(r)\)
  
  This kernel is nonzero since \(k(A) > t\)
- Take a nonzero element \(a\) of \(K(r)\)
  
  \(K(r) = K(e)\) since \((A \ast B) \perp C\)
- Determine the set \(J\) of zero positions of \(a\)
  
  \(\text{supp}(e) \subseteq J\) since \(d(B^\perp) > t\)
  
  \(|J| < d(C)\) since \(d(A) + d(C) > n\)
- Compute the error values by erasure decoding
Theorem

Let $C$ be an $\mathbb{F}_q$-linear code of length $n$
Let $(A, B)$ be a $t$-error-correcting pair over $\mathbb{F}_{q^m}$ for $C$

Then the basic algorithm corrects $t$ errors for the code $C$ with complexity $\Theta((mn)^3)$
Codes on curves

Let $\mathcal{P} = (P_1, \ldots, P_n)$ an $n$-tuple of mutual distinct points of $\mathcal{X}(\mathbb{F}_q)$

(If the support of $E$ is disjoint from $\mathcal{P}$), then the evaluation map

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

where $\text{ev}_\mathcal{P}(f) = (f(P_1), \ldots, f(P_n))$, is well defined.

The algebraic geometry code $C_L(\mathcal{X}, \mathcal{P}, E)$
is the image of $L(E)$ under the evaluation map $\text{ev}_\mathcal{P}$

If $m < n$, then $C_L(\mathcal{X}, \mathcal{P}, E)$ is an $[n, k, d]$ code with

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

$n - m$ is called the designed minimum distance of $C_L(\mathcal{X}, \mathcal{P}, E)$
Let $F$ and $G$ be divisors. Then there is a well defined linear map

$$L(F) \otimes L(G) \longrightarrow L(F + G)$$

given on generators by

$$f \otimes g \mapsto fg$$

Hence

$$CL(X, \mathcal{P}, F) \ast CL(X, \mathcal{P}, G) \subseteq CL(X, \mathcal{P}, F + G)$$
Let $C = C_L(\mathcal{X}, \mathcal{P}, E)^\perp$

Choose a divisor $F$ with support disjoint from $\mathcal{P}$
Let $A = C_L(\mathcal{X}, \mathcal{P}, F)$
Let $B = C_L(\mathcal{X}, \mathcal{P}, E - F)$

Then
- $A \ast B \subseteq C^\perp$
- If $t + g \leq \deg(F) < n$, then $k(A) > t$
- If $\deg(G - F) > t + 2g - 2$, then $d(B^\perp) > t$
- If $\deg(G - F) > 2g - 2$, then $d(A) + d(C) > n$
Proposition

An algebraic geometry code of designed minimum distance $d$ from a curve over $\mathbb{F}_q$ of genus $g$ has a $t$-error-correcting pair over $\mathbb{F}_q$ where

$$t = \left\lfloor \frac{d-1-g}{2} \right\rfloor$$
Proposition

An algebraic geometry code of designed minimum distance $d$ from a curve over $\mathbb{F}_q$ of genus $g$ has a $t$-error-correcting pair over $\mathbb{F}_{q^m}$ where

$$ t = \lfloor \frac{d-1}{2} \rfloor $$

if

$$ m > \log_q \left( 2 \binom{n}{t} + 2 \binom{n}{t+1} + 1 \right) $$

Not constructive!
Majority coset decoding gives a constructive and efficient approach
Proposition (Feng-Rao, Duursma)

Let $C$ be code with a subcode $D$ of codimension one.
Let $a_1, \ldots, a_w$ and $b_1, \ldots, b_w$ such that

$$
\begin{cases}
    a_i \ast b_j \in C^\perp & \text{if } i + j \leq w, \\
    a_i \ast b_j \in D^\perp \setminus C^\perp & \text{if } i + j = w + 1.
\end{cases}
$$

Then all words of $C \setminus D$ have weight at least $w$. 
**Proof:** Let \( c \in C \setminus D \)

Let \( A \) be the \( w \times n \) matrix with the \( a_i \)'s as rows

Let \( B \) be the \( w \times n \) matrix with the \( b_j \)'s as rows

Let \( D(c) \) be the diagonal matrix with \( c \) on the diagonal

Let \( S(c) \) be the \( w \times w \) matrix with entries \( s_{i,j} = a_i \ast b_j \cdot c \)

Then

\[
AD(c) B^T = S(c)
\]

and

\[
\begin{cases}
  s_{i,j} = 0 & \text{if } i + j \leq w, \\
  s_{i,j} \neq 0 & \text{if } i + j = w + 1.
\end{cases}
\]

Hence \( \text{wt}(c) = \text{rk}(D(c)) \geq \text{rk}(S(c)) = w \)
Let \( w = 2t + 1 \)

\[
\begin{pmatrix}
0 & 0 & \cdots & 0 & 0 & \cdots & 0 & S_{1,w} \\
0 & 0 & \cdots & 0 & 0 & \cdots & S_{2,w-1} & S_{2,w-1} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 0 & S_{t,t+1} & \cdots & S_{t,w-1} & S_{t,w} \\
0 & 0 & \cdots & S_{t+1,t} & S_{t+1,t+1} & \cdots & S_{t+1,w-1} & S_{t+1,w} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & S_{w-1,2} & \cdots & S_{w-1,t} & S_{w-1,t+1} & \cdots & S_{w-1,w-1} & S_{w-1,w} \\
S_{w,1} & S_{w,2} & \cdots & S_{w,t} & S_{w,t+1} & \cdots & S_{w,w-1} & S_{w,w}
\end{pmatrix}
\]
Decoding: Let \( r \) be a received word with \( r = c + e \) and \( c \in C \setminus D \) and error vector \( e \)
Let \( S(r) \) be the \( t \times t \) syndrome matrix with entries \( s_{i,j}(r) = a_i \ast b_j \cdot r \)
Then
\[
s_{i,j}(r) = s_{i,j}(e) \quad \text{if} \quad i + j \leq w
\]
are called the known syndromes
Now \( D \) has codimension one in \( C \), so there exists a \( d \in D^\perp \setminus C^\perp \) and \( \lambda_{ij} \in \mathbb{F}_q^* \) for \( i + j = w + 1 \) such that
\[
a_i \ast b_j \equiv \lambda_{ij} d \mod C^\perp
\]
Hence the unknown syndromes are related to \( d \cdot r \) by:
\[
s_{i,j}(r) = \lambda_{ij} d \cdot r \quad \text{if} \quad i + j = w + 1
\]
Let \( w = 2t + 1 \)

\[
\begin{pmatrix}
    s_{1,1} & s_{1,2} & \cdots & s_{1,t} & s_{1,t+1} & \cdots & s_{1,w-1} & s_{1,w} \\
    s_{2,1} & s_{2,2} & \cdots & s_{2,t} & s_{2,t+1} & \cdots & s_{2,w-1} & \\
    \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \\
    s_{t,1} & s_{t,2} & \cdots & s_{t,t} & & s_{t,t+1} & & \\
    s_{t+1,1} & s_{t+1,2} & \cdots & & s_{t+1,t} & & & \\
    \vdots & \vdots & \cdots & & & & & \\
    s_{w-1,1} & s_{w-1,2} & & & & & & \\
    s_{w,1} & & & & & & &
\end{pmatrix}
\]
At the heart of any public-key cryptosystem is a one-way function
\[ y = f(x) \]
that is easy to evaluate but for which it is computationally infeasible (one hopes) to find an inverse
\[ x \in f^{-1}(y) \]
PKC systems use trapdoor one-way functions

by mathematical problems that are (supposedly) hard

– RSA, factoring integers
– Diffie-Hellman, discrete-log problem in finite field
– Elliptic curve PKC, addition on elliptic curve
– Lattice-based PKC systems closest vector problem
– Code-based PKC systems, decoding of codes
Code based PKC systems
Take a class of codes that have an efficient decoding algorithm:
Scramble a generator matrix such that it looks like a random code

- Goppa codes (McEliece)
- with parity check matrix instead of generator matrix (Niederreiter)
- Algebraic geometry codes (Janwa-Moreno)
- subcodes of GRS codes (Berger-Loidreau)
- subfield subcodes of algebraic geometry codes (Janwa-Moreno)
Code based PKC systems - 2

Generic attack – decoding algorithms:
- McEliece 1978
- Finiasz-Sendrier 2009
- Bernstein-Lange-Peters 2008-2011
- Becker-Joux-May-Meurer Eurocrypt 2012

Structural attack:
- GRS codes (Sidelnikov-Shestakov)
- subcodes of GRS codes (Wieschebrink, Márquez-Martínez-P)
- Alternant codes: open
- Goppa codes: open
- AG codels: (Faure-Minder, $g \leq 2$)
- VSAG codes: (Márquez-Martínez-P-Ruano, arbitrary $g$)
Most (all) classes of codes used in PKC systems have an ECP

From a structural point of view we pose the question:

Is the the map

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

a one-way function?