

# Public key cryptosystems based on algebraic geometry codes

Ruud Pellikaan  
[g.r.pellikaan@tue.nl](mailto:g.r.pellikaan@tue.nl)

joint work with

Alain Couvreur, Irene Márquez-Corbella  
Edgar Martínez-Moro and Diego Ruano

YACC, Porquerolles, 10 June 2014

- ▶ Error correcting pairs
- ▶ Codes on curves
- ▶ Error correcting pairs **for** codes on curves
- ▶ Majority coset decoding and error correcting arrays
- ▶ Error correcting arrays **for** codes on curves
- ▶ Code based public key cryptosystem
- ▶ Reverse engineering AG codes
- ▶ Error correcting pairs and arrays **from** codes on curves
- ▶ Questions

$C$  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  $C$

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

$t$  = error correcting capacity of  $C$

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

The **standard inner product** is defined by

$$\mathbf{a} \cdot \mathbf{b} = a_1 b_1 + \cdots + a_n b_n$$

For two subsets  $A$  and  $B$  of  $\mathbb{F}_q^n$

$A \perp B$  if and only if  $\mathbf{a} \cdot \mathbf{b} = 0$  for all  $\mathbf{a} \in A$  and  $\mathbf{b} \in B$

Let  $\mathbf{a}$  and  $\mathbf{b}$  in  $\mathbb{F}_q^n$

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

$$\mathbf{a} * \mathbf{b} = (a_1 b_1, \dots, a_n b_n)$$

For two subsets  $A$  and  $B$  of  $\mathbb{F}_q^n$

$$A * B = \langle \{\mathbf{a} * \mathbf{b} \mid \mathbf{a} \in A \text{ and } \mathbf{b} \in B\} \rangle \text{ and } A^{(2)} = A * A$$

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

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

**Evaluation map:**

$$\text{ev}_{\mathbf{a},\mathbf{b}}(f(X)) = (f(a_1)b_1, \dots, f(a_n)b_n)$$

$$GRS_k(\mathbf{a}, \mathbf{b}) = \{ \text{ev}_{\mathbf{a},\mathbf{b}}(f(X)) \mid f(X) \in \mathbb{F}_q[X], \deg(f(X)) < k \}$$

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

Furthermore

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

$$GRS_k(\mathbf{a}, \mathbf{b}) * GRS_l(\mathbf{a}, \mathbf{c}) = GRS_{k+l-1}(\mathbf{a}, \mathbf{b} * \mathbf{c})$$

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**  $(A * B) \perp C$

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

**E.3**  $d(B^\perp) > t$

**E.4**  $d(A) + d(C) > n$

Let  $C^\perp = GRS_{n-2t}(\mathbf{a}, \mathbf{b})$ , has parameters:  $[n, 2t, n - 2t + 1]$

Then  $C = GRS_{2t}(\mathbf{a}, \mathbf{c})$  for some  $\mathbf{c}$

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

Let  $A = GRS_{t+1}(\mathbf{a}, \mathbf{1})$  and  $B = GRS_t(\mathbf{a}, \mathbf{b})$

Then  $(A * B) \subseteq C^\perp$

$A$  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  $C$

Let  $A$  and  $B$  be linear subspaces of  $\mathbb{F}_q^n$

Let  $r \in \mathbb{F}_q^n$  be a **received word**

Define the **kernel of error locator vectors**

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

### 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  $A * B \subseteq C^\perp$ , then

$$K(r) = K(e)$$



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

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

**Set of zeros of error locator vectors contains the error positions:**

**Lemma**

Let  $(A * B) \perp C$

Let  $\mathbf{e}$  be an error vector of the received word  $\mathbf{r}$

If  $I = \text{supp}(\mathbf{e}) = \{ i \mid e_i \neq 0 \}$ , then

$$A(I) \subseteq K(\mathbf{r})$$

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

## 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  $\mathcal{O}((mn)^3)$

Let  $\mathcal{X}$  be an **algebraic curve** defined over  $\mathbb{F}_q$  of **genus**  $g$   
 $\mathcal{X}(\mathbb{F}_q)$  is the set of  $\mathbb{F}_q$ -**rational points** of  $\mathcal{X}$

Let  $\mathbb{F}_q(\mathcal{X})$  be the vector space of **rational functions** on  $\mathcal{X}$ .

Let  $f$  be a rational function and  $P$  a **place**

$v_P(f)$  is the **valuation** of  $f$  at  $P$

$(f) = \sum_P v_P(f)P$  is the **principal divisor**  $f$

Let  $E = \sum m_P P$  be a **divisor**, a finite formal sum of places

$\deg(E) = \sum m_P \deg(P)$  is the **degree** of  $E$

$$L(E) = \{f \in \mathbb{F}_q(\mathcal{X}) \mid (f) \geq -E, f \neq 0\} \cup \{0\}$$

**Riemann-Roch:**  $\dim L(E) \geq \deg(E) + 1 - g$

equality holds if  $\deg(E) > 2g - 2$

Let  $\mathcal{X}$  be an algebraic curve defined over  $\mathbb{F}_q$  of genus  $g$

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

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

$n - m$  is called the **designed minimum distance** of  $C_L(\mathcal{X}, \mathcal{P}, E)$

**Embedding** of  $\mathcal{X}$  in **linear system** of  $E$  of degree  $m$

Let  $f_1, f_2, \dots, f_k$  be a basis of  $L(E)$

$$\varphi_E : \mathcal{X} \longrightarrow \mathbb{P}^{k-1}$$

$$P \mapsto (f_1(P) : f_2(P) : \dots : f_k(P))$$

$\mathcal{Y} = \varphi_E(\mathcal{X})$  is a curve of degree  $m$  in  $\mathbb{P}^{k-1}$

$\mathcal{Q} = (\varphi_E(P_1), \dots, \varphi_E(P_n))$  **projective system**

$$G_{\mathcal{Q}} = \begin{pmatrix} f_1(P_1) & \cdots & f_1(P_j) & \cdots & f_1(P_n) \\ f_2(P_1) & \cdots & f_2(P_j) & \cdots & f_2(P_n) \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ f_k(P_1) & \cdots & f_k(P_j) & \cdots & f_k(P_n) \end{pmatrix} \text{generator matrix}$$

**minimum distance**  $\geq n - m$

Let  $\omega$  be a differential form  
with a simple pole and residue 1 at  $P_j$  for all  $j = 1, \dots, n$   
Let  $K$  be the canonical divisor of  $\omega$

Then

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

where  $E^\perp = P_1 + \dots + P_n - E + K$   
and  $\deg(E^\perp) = n - m + 2g - 2$

minimum distance is at least

$$d^* = m - 2g + 2$$

the designed minimum distance

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

$$C_L(\mathcal{X}, \mathcal{P}, F) * C_L(\mathcal{X}, \mathcal{P}, G) \subseteq C_L(\mathcal{X}, \mathcal{P}, F + G)$$

**Equality holds** if  $\deg(F) \geq 2g$  and  $\deg(G) \geq 2g + 1$

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

–  $A * B \subseteq C^\perp$

– If  $t + g \leq \deg(F) < n$ , then  $k(A) > t$

– If  $\deg(E - F) > t + 2g - 2$ , then  $d(B^\perp) > t$

– If  $\deg(E - F) > 2g - 2$ , 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

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

## 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

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

**Not constructive!**

Majority coset decoding gives a constructive and efficient approach

## Feng-Rao, Duursma

Let  $C$  be a code for which we **need** a decoding algorithm

Let  $D$  be a subcode for which we **have** a decoding algorithm

**Coset decoding** is an algorithm

Input:  $x$  such that  $x = e + c$  and  $c \in C$

Output:  $y$  such that  $y = e + d$  and  $d \in D$

Solution:

- Majority voting of unknown syndromes
- Majority coset decoding
- Error correcting array

An **array** of codes is a triple  $(\mathcal{A}, \mathcal{B}, \mathcal{C})$  of sequences of linear codes in  $\mathbb{F}_q^n$   
 $\mathcal{A} = (A_i | 1 \leq i \leq u)$ ,  $\mathcal{B} = (B_j | 1 \leq j \leq v)$  and  $\mathcal{C} = (C_r | w \leq r \leq l)$   
such that:

- $\dim(A_i) = i$ ,  $\dim(B_j) = j$  and  $\dim(C_r) = n - r$
- $A_i \subseteq A_{i+1}$ ,  $B_j \subseteq B_{j+1}$  and  $C_{r+1} \subseteq C_r$
- For every  $i$  and  $j$  there exists an  $r$  such that  $A_i * B_j \subseteq (C_r)^\perp$   
Let  $r(i, j)$  be the smallest index  $r$  such that  $A_i * B_j \subseteq (C_r)^\perp$
- If  $w < r(i, j)$  then  $r(i, j)$  is strictly increasing in both arguments:  
if  $1 < i$  then  $r(i-1, j) < r(i, j)$ , and if  $1 < j$  then  $r(i, j-1) < r(i, j)$ .
- If  $\mathbf{a} \in A_i \setminus A_{i-1}$  and  $\mathbf{b} \in B_j \setminus B_{j-1}$  and  $r = r(i, j) \geq w + 1$   
then  $\mathbf{a} * \mathbf{b}$  is an element of  $(C_r)^\perp \setminus (C_{r-1})^\perp$

Define the following set

$$N_r = \{(i, j) | 1 \leq i \leq u, 1 \leq j \leq v, r(i, j) = r + 1\}$$

Let  $v_r$  be the number of elements of  $N_r$ . Define **order bound**

$$d_r = \min\{v_{r'} | r \leq r' < l\} \cup \{d(C_l)\}.$$

## Theorem

For an array of codes we have that  $d_r \leq d(C_r)$ , for all  $w \leq r \leq l$ .

## Proposition

Let  $C$  be code with a subcode  $D$  of codimension one

Let  $\mathbf{a}_1, \dots, \mathbf{a}_w$  and  $\mathbf{b}_1, \dots, \mathbf{b}_w$  such that

$$\begin{cases} \mathbf{a}_i * \mathbf{b}_j \in C^\perp & \text{if } i + j \leq w, \\ \mathbf{a}_i * \mathbf{b}_j \in D^\perp \setminus C^\perp & \text{if } i + j = w + 1. \end{cases}$$

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  $s_{i,j} = a_i * b_j \cdot c$

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  $w = 2t + 1$

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & S_{1,w} \\ 0 & 0 & \cdots & 0 & 0 & \cdots & S_{2,w-1} & S_{2,w-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & S_{t,t+1} & \cdots & S_{t,w-1} & S_{t,w} \\ 0 & 0 & \cdots & S_{t+1,t} & S_{t+1,t+1} & \cdots & S_{t+1,w-1} & S_{t+1,w} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & S_{w-1,2} & \cdots & S_{w-1,t} & S_{w-1,t+1} & \cdots & S_{w-1,w-1} & S_{w-1,w} \\ S_{w,1} & S_{w,2} & \cdots & S_{w,t} & S_{w,t+1} & \cdots & S_{w,w-1} & S_{w,w} \end{pmatrix}$$



An array of codes  $(\mathcal{A}, \mathcal{B}, \mathcal{C})$  is called a  **$t$ -error correcting array** for a code  $C$  if  $C = C_w$  and  $t \leq (d_w - 1)/2$

And  $C_l = 0$  or there exists  $i$  and  $j$  such that  $(A_i, B_j)$  is a  $t$ -error correcting pair for  $C_r$ , where  $r = r(i, j)$

## Theorem

If a code has a  $t$ -error correcting array then it has a decoding algorithm which corrects  $t$  errors of complexity  $\mathcal{O}(n^3)$

**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  $s_{i,j}(r) = a_i * b_j \cdot r$

Then

$$s_{i,j}(r) = s_{i,j}(e) \quad \text{if } i + j \leq w$$

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

$$a_i * b_j \equiv \lambda_{ij} d \quad \text{mod } C^\perp$$

Hence the **unknown syndromes** are related to  $d \cdot r$  by:

$$s_{i,j}(r) = \lambda_{ij} d \cdot r \quad \text{if } i + j = w + 1$$

Let  $w = 2t + 1$

$$\begin{pmatrix} s_{1,1} & s_{1,2} & \cdots & s_{1,t} & s_{1,t+1} & \cdots & s_{1,w-1} & s_{1,w} \\ s_{2,1} & s_{2,2} & \cdots & s_{2,t} & s_{2,t+1} & \cdots & s_{2,w-1} & \\ \vdots & \vdots & \ddots & \vdots & \vdots & & & \\ s_{t,1} & s_{t,2} & \cdots & s_{t,t} & s_{t,t+1} & & & \\ s_{t+1,1} & s_{t+1,2} & \cdots & s_{t+1,t} & & & & \\ \vdots & \vdots & & & & & & \\ s_{w-1,1} & s_{w-1,2} & & & & & & \\ s_{w,1} & & & & & & & \end{pmatrix}$$

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

with designed minimum distance  $d^* = m - 2g + 2$

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

Choose a point  $P$  disjoint from  $\mathcal{P}$

Let  $A_i = C_L(\mathcal{X}, \mathcal{P}, \alpha_i P)$

with  $(\alpha_i)$  the **Weierstrass non-gap** sequence at  $P$

Let  $B_j = C_L(\mathcal{X}, \mathcal{P}, E + \beta_j P)$

with  $(\beta_j)$  the non-gap sequence of  $E$  at  $P$

Let  $C_r = C_L(\mathcal{X}, \mathcal{P}, E + \beta_r P)^\perp$

Let  $\mathcal{A} = (A_i | 1 \leq i \leq u)$ ,  $\mathcal{B} = (B_j | 1 \leq j \leq v)$ ,  $\mathcal{C} = (C_r | w \leq r \leq l)$

Then  $(\mathcal{A}, \mathcal{B}, \mathcal{C})$  is an  $t^*$ -error correcting array of codes

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)

Let  $\mathcal{X}$  be an absolutely irreducible and nonsingular curve of genus  $g$  over the perfect field  $\mathbb{F}$

Let  $E$  be a divisor on  $\mathcal{X}$  of degree  $m$

If  $m \geq 2g + 1$

then  $\varphi_E$  gives an embedding of  $\mathcal{X}$  onto  $\mathcal{Y} = \varphi_E(\mathcal{X})$   
which is a normal curve in the linear system  $|E| = \mathbb{P}^{m-g}$

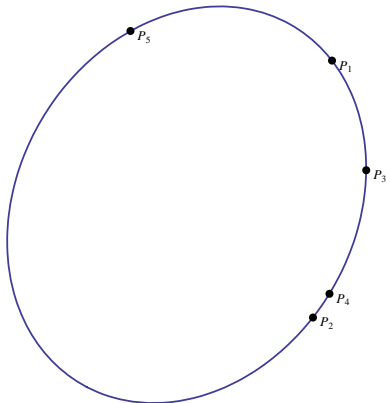
If  $m \geq 2g + 2$ , then  $\mathcal{Y}$  is an intersection of quadrics

More precisely:

$I(\mathcal{Y})$  is generated by  $I_2(\mathcal{Y})$

the set of homogeneous elements of degree two in  $I(\mathcal{Y})$

Conic determined by 5 points



Let  $\mathcal{Y}$  be a curve embedded in projective  $r$ -space of degree  $m$

Let  $I(\mathcal{Y})$  be the vanishing ideal of  $\mathcal{Y}$

Let  $\mathcal{Q}$  be a subset of  $\mathcal{Y}$  of  $n$  points

Then

$$I(\mathcal{Y}) \subseteq I(\mathcal{Q})$$

Hence

$$I_2(\mathcal{Y}) \subseteq I_2(\mathcal{Q})$$

Suppose  $I(\mathcal{Y})$  is generated by  $I_2(\mathcal{Y})$

$$\text{If } n > 2m, \text{ then } I_2(\mathcal{Y}) = I_2(\mathcal{Q})$$

By Bézout's Theorem



$\mathbf{g}_1, \dots, \mathbf{g}_k$  a basis of  $C$

$S^2(C)$  is the **second symmetric power** of  $C$

$S^2(C)$  has basis  $\{X_i X_j \mid 1 \leq i \leq j \leq n\}$  and dimension  $\binom{k+1}{2}$   
with  $X_i = \mathbf{g}_i$

$C^{(2)} = C * C$  the **square** of  $C$

Consider the linear map

$$\begin{aligned} \sigma : S^2(C) &\longrightarrow C^{(2)} \\ X_i X_j &\longmapsto \mathbf{g}_i * \mathbf{g}_j \end{aligned}$$

$K_2(C)$  is the **kernel** of this map

Then

$$0 \longrightarrow K_2(C) \longrightarrow S^2(C) \longrightarrow C^{(2)} \longrightarrow 0$$

is an exact sequence and

$$I_2(Q) = K_2(C) := \left\{ \sum_{1 \leq i < j \leq k} a_{ij} X_i X_j \mid \sum_{1 \leq i < j \leq k} a_{ij} g_i * g_j = 0 \right\}$$

## Proposition

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  $\mathcal{O}(n^4)$

$C$  is called **very strong algebraic-geometric (VSAG)**

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

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

The dual of a VSAG code is again VSAG

## Main Theorem

Let  $C$  be a VSAG code

Then a VSAG representation of  $C$  can be obtained efficiently from its generator matrix

Moreover all VSAG representations of  $C$  are strict isomorphic

**Shortcut** via  $t$ -ECP pair  $(A, B)$  in  $\mathbb{F}_q^n$

Bypassing computation of triple  $(\mathcal{X}, \mathcal{P}, E)$  and Riemann–Roch spaces

	$\mathbb{F}_q(\mathcal{X})$	$\mathbb{F}_q^n$
		$C = C_L(\mathcal{X}, \mathcal{P}, E)^\perp$
$(\mathcal{X}, \mathcal{P}, E)$	$L(E)$	$C_L(\mathcal{X}, \mathcal{P}, E)$
$(\mathcal{X}, \mathcal{P}, iP_1)$	$L(iP_1)$	$A_i = C_L(\mathcal{X}, \mathcal{P}, iP_1)$
$(\mathcal{X}, \mathcal{P}, E - jP_1)$	$L(E - jP_1)$	$D_j = C_L(\mathcal{X}, \mathcal{P}, E - jP_1)$

In fact,  $D_j$  is the space of those code words in  $C^\perp$

that are **zero** with **multiplicity**  $j$  at  $P_1$

This multiplicity can be controlled  
since we computed  $I_2(Q)$  efficiently

## Proposition

Let  $A_i := \langle D_i * C \rangle^\perp$ , then

$(A_{t+g}, D_{t+g})$  is a  $t$ -ECP for  $C$  with  $t = \lfloor (d^* - 1 - g)/2 \rfloor$

Still reference to multiplicities

## Circumventing multiplicities altogether :

Let  $A_i = C_L(\mathcal{X}, \mathcal{P}, iP_1)$  and  $D_j = C_L(\mathcal{X}, \mathcal{P}, E - jP_1)$

Then  $D_0 = C_L(\mathcal{X}, \mathcal{P}, E) = C^\perp$

And  $D_1 = C_L(\mathcal{X}, \mathcal{P}, E - P_1)$ ,

the space of code words in  $C^\perp$  that are zero at the first position

So  $D_0$  and  $D_1$  are easily computed for given  $C$

The  $D_j$  are obtained as follows by induction

## Proposition

$$D_{j+1} = \{ z \in D_j \mid z * D_{j-1} \subseteq D_j^{(2)} \}$$

$$A_i = \langle D_i * C \rangle^\perp$$

$(A_{t+g}, D_{t+g})$  is a  $t$  - ECP for  $C$  with  $t = \lfloor (d^* - 1 - g)/2 \rfloor$

## Proposition

If  $\frac{n}{2} + i - 2 \geq m \geq 2g + i + 1$ , then

$$D_{j+1} = \{ \mathbf{z} \in D_j \mid \mathbf{z} * D_{j-1} \subseteq D_j^{(2)} \}$$

$$A_i = \langle D_i * C \rangle^\perp$$

If  $i \geq 2g + 1$ , then

$$A_{i+1} = \{ \mathbf{z} \in \mathbb{F}_q^n \mid \mathbf{z} * A_{i-1} \subseteq (A_i)^{(2)} \}$$



- Algebraic geometry codes on curves are not suitable for a McEliece PKC
- What about (subfield) subcodes of AG codes?
- What about codes from varieties of dimension larger than 1?
- What about Reed-Muller and order domain codes?