Code-Based Cryptography

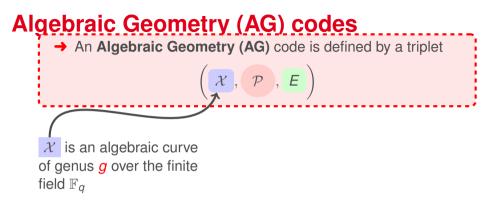
- 1. Error-Correcting Codes and Cryptography
- 2. McEliece Cryptosystem
- 3. Message Attacks (ISD)
- 4. Key Attacks
- 5. Other Cryptographic Constructions Relying on Coding Theory

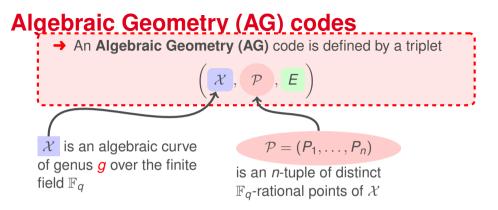
4. Key Attacks

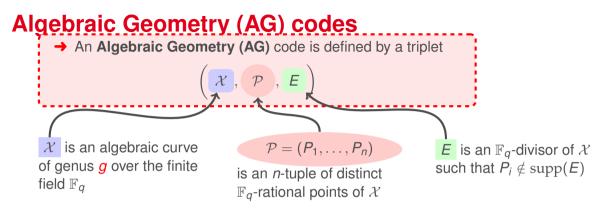
- 1. Introduction
- 2. Support Splitting Algorithm
- 3. Distinguisher for GRS codes
- 4. Attack against subcodes of GRS codes
- 5. Error-Correcting Pairs
- 6. Attack against GRS codes
- 7. Attack against Reed-Muller codes
- 8. Attack against Algebraic Geometry codes
- 9. Goppa codes still resist

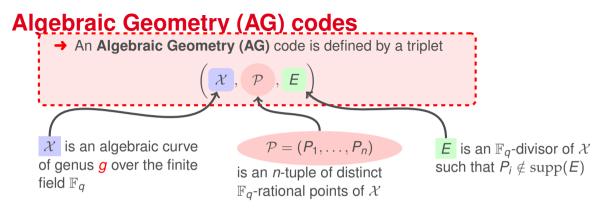
→ An Algebraic Geometry (AG) code is defined by a triplet

$\left(\mathcal{X}, \mathcal{P}, \mathcal{E} \right)$









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

$$\mathcal{C}_{L}(\mathcal{X},\mathcal{P},E) = \{ \operatorname{ev}_{\mathcal{P}}(f) = (f(P_{1}),\ldots,f(P_{n})) \mid f \in L(E) \}$$

AG codes are "almost" optimal codes

Let $C = C_L(\mathcal{X}, \mathcal{P}, E)$. Then,

$$d(\mathcal{C}) \geq n - K(\mathcal{C}) + 1 - g$$

where g is the genus of \mathcal{X}

AG codes are "almost" optimal codes

Let $C = C_L(\mathcal{X}, \mathcal{P}, E)$. Then,

$$d(\mathcal{C}) \geq n - K(\mathcal{C}) + 1 - g$$

where g is the genus of \mathcal{X}

The dual of an AG code is an AG code

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

AG codes for the McEliece scheme

Algebraic-Geometry codes



H. Janwa and O. Moreno.

McEliece public crypto system using algebraic-geometric codes. Designs, Codes and Cryptography, 1996.

Parameters	Key size	Security level
$[171, 109, 61]_{128}$	16 ko	2 ⁶⁶

AG codes for the McEliece scheme

Algebraic-Geometry codes



H Janwa and O Moreno

McEliece public crypto system using algebraic-geometric codes. Designs, Codes and Cryptography, 1996.

Parameters	Key size	Security level
$[171, 109, 61]_{128}$	16 ko	2 ⁶⁶

Attack against this proposal:



C. Faure and L. Minder.

Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes. Proceedings 11th Int, Workshop on Algebraic and Combinatorial Coding Theory, 2008.



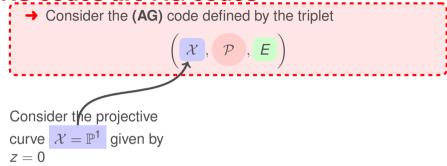
A. Couvreur, I. Márguez-Corbella and R. Pellikaan.

A Polvnomial Time Attack against Algebraic Geometry Code Based Public Key Cryptosystems. IEEE Information Theory, ISIT 2014, 1446-1450, 2014.

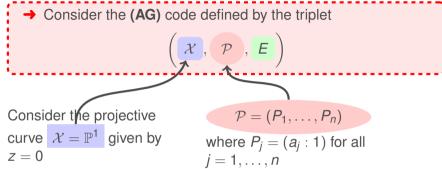
GRS codes are AG codes

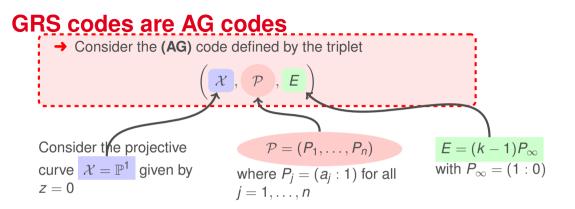
→ Consider the (AG) code defined by the triplet $\begin{pmatrix} \mathcal{X}, \mathcal{P}, \mathcal{E} \end{pmatrix}$

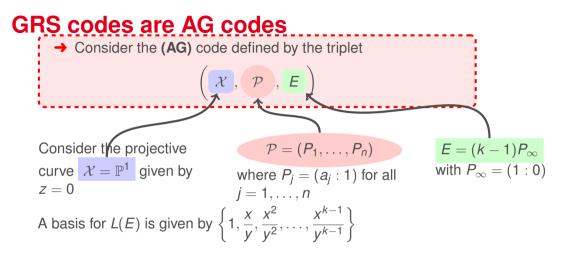
GRS codes are AG codes

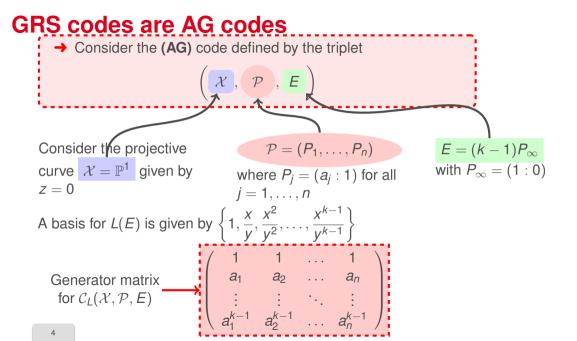


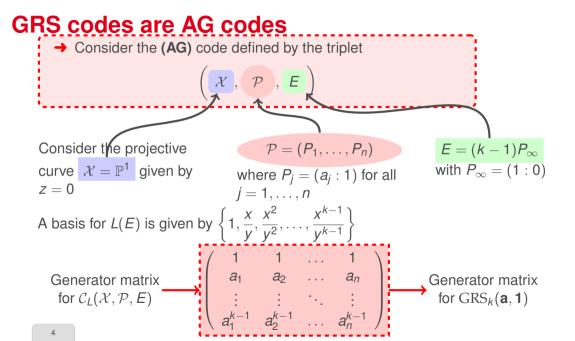
GRS codes are AG codes











Suppose that we know:

$$C_k = GRS_k(\mathbf{a}, \mathbf{b})$$
 and $C_{k-1} = GRS_{k-1}(\mathbf{a}, \mathbf{b})$

Proposition: Assume that $2k - 1 \le n - 2$

 $C_{k-2} = \text{GRS}_{k-2}(\mathbf{a}, \mathbf{b})$ is the solution space of the following problem

$$\mathbf{c} \in \mathcal{C}_{k-1}$$
 and $\mathbf{c} * \mathcal{C}_k \subseteq (\mathcal{C}_{k-1})^2$

Suppose that we know:

$$C_k = GRS_k(\mathbf{a}, \mathbf{b})$$
 and $C_{k-1} = GRS_{k-1}(\mathbf{a}, \mathbf{b})$

Proposition: Assume that $2k - 1 \le n - 2$

 $C_{k-2} = \text{GRS}_{k-2}(\mathbf{a}, \mathbf{b})$ is the solution space of the following problem

$$\mathbf{c} \in \mathcal{C}_{k-1}$$
 and $\mathbf{c} * \mathcal{C}_k \subseteq (\mathcal{C}_{k-1})^2$

In this way we build a filtration

 $\operatorname{GRS}_k(\mathbf{a},\mathbf{b}) \supseteq \operatorname{GRS}_{k-1}(\mathbf{a},\mathbf{b}) \supseteq \operatorname{GRS}_{k-2}(\mathbf{a},\mathbf{b}) \supseteq \cdots$

Proposition 1:

Let
$$\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d}) \implies \mathcal{C}^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp})$$

Proposition 1:

Let
$$\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d}) \implies \mathcal{C}^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp})$$

Then,
$$\mathcal{A} = \text{GRS}_{t+1}(\mathbf{c}, \mathbf{1})$$
 and $\mathcal{B} = \text{GRS}_t(\mathbf{c}, \mathbf{d}^{\perp})$
is a *t*-ECP for \mathcal{C} over \mathbb{F}_q

Proposition 1:

Let
$$\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d}) \implies \mathcal{C}^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp})$$

Then,
$$\mathcal{A} = \text{GRS}_{t+1}(\mathbf{c}, \mathbf{1})$$
 and $\mathcal{B} = \text{GRS}_t(\mathbf{c}, \mathbf{d}^{\perp})$
is a *t*-ECP for \mathcal{C} over \mathbb{F}_q

Proposition 2: To compute a *t*-ECP for $C = \text{GRS}_k(\mathbf{a}, \mathbf{b})$ it suffise to compute a code of type $\mathcal{B} = \text{GRS}_t(\mathbf{c}, \mathbf{d}^{\perp})$

If we know
$$\mathcal{C} = \text{GRS}_k(\mathbf{c}, \mathbf{d})$$
 and $\mathcal{B} = \text{GRS}_t(\mathbf{c}, \mathbf{d})$

Proposition 1:

Let
$$\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d}) \implies \mathcal{C}^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp})$$

Then,
$$\mathcal{A} = \text{GRS}_{t+1}(\mathbf{c}, \mathbf{1})$$
 and $\mathcal{B} = \text{GRS}_t(\mathbf{c}, \mathbf{d}^{\perp})$
is a *t*-ECP for \mathcal{C} over \mathbb{F}_q

Proposition 2: To compute a *t*-ECP for $C = \text{GRS}_k(\mathbf{a}, \mathbf{b})$ it suffise to compute a code of type $\mathcal{B} = \text{GRS}_t(\mathbf{c}, \mathbf{d}^{\perp})$

If we know
$$C = GRS_k(\mathbf{c}, \mathbf{d})$$
 and $\mathcal{B} = GRS_t(\mathbf{c}, \mathbf{d}^{\perp})$

Then,
$$\mathcal{A} = \text{GRS}_{t+1}(\mathbf{a}, \mathbf{1}) = (\mathcal{B} * \mathcal{C})^{\perp}$$

Public Key:
$$\mathcal{K}_{\text{pub}} = \begin{cases} \text{ a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{ and } t = \left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor \end{cases}$$

The Algorithm: Assume that $2k - 1 \le n - 2$

Public Key:
$$\mathcal{K}_{\text{pub}} = \begin{cases} \text{ a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{ and } t = \left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor \end{cases}$$

The Algorithm: Assume that $2k - 1 \le n - 2$

1. Determine the codes

$$C_{pub}^{\perp} = \text{GRS}_{2t}(\mathbf{a}, \mathbf{b}^{\perp}) \text{ and } S_1(C_{pub}^{\perp}) = \text{GRS}_{2t-1}(\mathbf{a}', \sim \mathbf{b}^{\perp})$$

Public Key:
$$\mathcal{K}_{\text{pub}} = \begin{cases} \text{ a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{ and } t = \left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor \end{cases}$$

The Algorithm: Assume that $2k - 1 \le n - 2$

1. Determine the codes

$$\mathcal{C}_{pub}^{\perp} = \mathrm{GRS}_{2t}(\mathbf{a}, \mathbf{b}^{\perp}) \text{ and } S_1(\mathcal{C}_{pub}^{\perp}) = \mathrm{GRS}_{2t-1}(\mathbf{a}', \sim \mathbf{b}^{\perp})$$

$$\underbrace{\operatorname{GRS}_{2t}(\mathbf{a},\mathbf{b})}_{\mathcal{C}_{pub}^{\perp}} \supseteq \underbrace{\operatorname{GRS}_{2t-1}(\mathbf{a}',\sim\mathbf{b}^{\perp})}_{S_{1}(\mathcal{C}_{pub}^{\perp})} \supseteq \ldots \supseteq \underbrace{\operatorname{GRS}_{t}(\mathbf{a}',\sim\mathbf{b}^{\perp})}_{\mathcal{B}}$$

Public Key:
$$\mathcal{K}_{\text{pub}} = \begin{cases} \text{ a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{ and } t = \left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor \end{cases}$$

The Algorithm: Assume that $2k - 1 \le n - 2$

1. Determine the codes

$$\mathcal{C}_{pub}^{\perp} = \mathrm{GRS}_{2t}(\mathbf{a}, \mathbf{b}^{\perp}) \quad \text{and} \quad S_1(\mathcal{C}_{pub}^{\perp}) = \mathrm{GRS}_{2t-1}(\mathbf{a}', \sim \mathbf{b}^{\perp})$$

$$\underbrace{\operatorname{GRS}_{2t}(\mathbf{a}, \mathbf{b})}_{\mathcal{C}_{pub}^{\perp}} \supseteq \underbrace{\operatorname{GRS}_{2t-1}(\mathbf{a}', \sim \mathbf{b}^{\perp})}_{S_1(\mathcal{C}_{pub}^{\perp})} \supseteq \ldots \supseteq \underbrace{\operatorname{GRS}_t(\mathbf{a}', \sim \mathbf{b}^{\perp})}_{\mathcal{B}}$$
Generator matrix
for \mathcal{C}_k , $\mathcal{G} = \begin{pmatrix} 1 & a_{12} & \ldots & a_{1n} \\ 0 & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{k2} & \ldots & a_{kn} \end{pmatrix}$

Public Key:
$$\mathcal{K}_{\text{pub}} = \begin{cases} \text{ a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{ and } t = \left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor \end{cases}$$

The Algorithm: Assume that $2k - 1 \le n - 2$

1. Determine the codes

$$\mathcal{C}_{pub}^{\perp} = \mathrm{GRS}_{2t}(\mathbf{a}, \mathbf{b}^{\perp}) \quad \text{and} \quad S_1(\mathcal{C}_{pub}^{\perp}) = \mathrm{GRS}_{2t-1}(\mathbf{a}', \sim \mathbf{b}^{\perp})$$

$$\underbrace{\operatorname{GRS}_{2t}(\mathbf{a}, \mathbf{b})}_{\mathcal{C}_{pub}^{\perp}} \supseteq \underbrace{\operatorname{GRS}_{2t-1}(\mathbf{a}', \sim \mathbf{b}^{\perp})}_{\mathcal{C}_{pub}^{\perp}} \supseteq \ldots \supseteq \underbrace{\operatorname{GRS}_{t}(\mathbf{a}', \sim \mathbf{b}^{\perp})}_{\mathcal{B}}$$
Generator matrix
for \mathcal{C}_{k} $\mathcal{G} = \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2t} \\ \vdots & \ddots & \vdots \\ 0 & a_{k2} & \cdots & a_{kn} \end{pmatrix}$ Generator matrix
for $S_{1}(\mathcal{C}_{k})$

Public Key:
$$\mathcal{K}_{\text{pub}} = \begin{cases} \text{ a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{ and } t = \left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor \end{cases}$$

The Algorithm: Assume that $2k - 1 \le n - 2$

1. Determine the codes

$$\mathcal{C}_{pub}^{\perp} = \mathrm{GRS}_{2t}(\mathbf{a}, \mathbf{b}^{\perp}) \quad \text{and} \quad S_1(\mathcal{C}_{pub}^{\perp}) = \mathrm{GRS}_{2t-1}(\mathbf{a}', \sim \mathbf{b}^{\perp})$$

2. Build the filtration:

$$\underbrace{\operatorname{GRS}_{2t}(\mathbf{a},\mathbf{b})}_{\mathcal{C}_{pub}^{\perp}} \supseteq \underbrace{\operatorname{GRS}_{2t-1}(\mathbf{a}',\sim\mathbf{b}^{\perp})}_{S_{1}(\mathcal{C}_{pub}^{\perp})} \supseteq \ldots \supseteq \underbrace{\operatorname{GRS}_{t}(\mathbf{a}',\sim\mathbf{b}^{\perp})}_{\mathcal{B}}$$

3. Return $(\mathcal{A}, \mathcal{B})$ which is an *ECP* for $S_1(\mathcal{C})$ where: $\mathcal{A} = (\mathcal{B} * S_1(\mathcal{C}))^{\perp}$

Public Key:
$$\mathcal{K}_{\text{pub}} = \begin{cases} \text{ a generator matrix of } \mathcal{C}_{\text{pub}} = \text{GRS}_k(\mathbf{a}, \mathbf{b}) \\ \text{ and } t = \left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor \end{cases}$$

The Algorithm: Assume that $2k - 1 \le n - 2$

1. Determine the codes

$$\mathcal{C}_{pub}^{\perp} = \mathrm{GRS}_{2t}(\mathbf{a}, \mathbf{b}^{\perp}) \quad \text{and} \quad S_1(\mathcal{C}_{pub}^{\perp}) = \mathrm{GRS}_{2t-1}(\mathbf{a}', \sim \mathbf{b}^{\perp})$$

$$\underbrace{\operatorname{GRS}_{2t}(\mathbf{a},\mathbf{b})}_{\mathcal{C}_{pub}^{\perp}} \supseteq \underbrace{\operatorname{GRS}_{2t-1}(\mathbf{a}',\sim\mathbf{b}^{\perp})}_{S_{1}(\mathcal{C}_{pub}^{\perp})} \supseteq \ldots \supseteq \underbrace{\operatorname{GRS}_{t}(\mathbf{a}',\sim\mathbf{b}^{\perp})}_{\mathcal{B}}$$

- **3**. Return $(\mathcal{A}, \mathcal{B})$ which is an *ECP* for $S_1(\mathcal{C})$ where: $\mathcal{A} = (\mathcal{B} * S_1(\mathcal{C}))^{\perp}$
- Note that: Correcting an error in the first position is not a difficult problem.

Suppose that we know:

$$C_0 = C_L(\mathcal{X}, \mathcal{P}, E)$$
 and $C_1 = C_L(\mathcal{X}, \mathcal{P}, E - P)$

Proposition: Assume that $\frac{n}{2} - 2 \ge \deg(E)$

 $C_2 = C_L(\mathcal{X}, \mathcal{P}, E - 2P)$ is the solution space of the following problem

$$\mathbf{c} \in \mathcal{C}_1$$
 and $\mathbf{c} * \mathcal{C}_0 \subseteq (\mathcal{C}_1)^2$

Suppose that we know:

$$C_0 = C_L(\mathcal{X}, \mathcal{P}, E)$$
 and $C_1 = C_L(\mathcal{X}, \mathcal{P}, E - P)$

Proposition: Assume that $\frac{n}{2} - 2 \ge \deg(E)$

 $C_2 = C_L(\mathcal{X}, \mathcal{P}, E - 2P)$ is the solution space of the following problem

$$\mathbf{c} \in \mathcal{C}_1$$
 and $\mathbf{c} * \mathcal{C}_0 \subseteq (\mathcal{C}_1)^2$

In this way we build a filtration

$$\underbrace{\mathcal{C}_{L}(\mathcal{X},\mathcal{P},E)}_{\mathcal{C}_{0}} \supseteq \underbrace{\mathcal{C}_{L}(\mathcal{X},\mathcal{P},E-P)}_{\mathcal{C}_{1}} \supseteq \underbrace{\mathcal{C}_{L}(\mathcal{X},\mathcal{P},E-2P)}_{\mathcal{C}_{2}} \supseteq \cdots$$

Proposition 1: [Pellikaan 1992]

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

Proposition 1: [Pellikaan 1992]

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

Then,
$$\mathcal{A} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, F)$$
 and $\mathcal{B} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E - F)$ with
 $\deg(E) > \deg(F) = t + g$ is a *t*-ECP for \mathcal{C}

Proposition 1: [Pellikaan 1992]

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

Then,
$$\mathcal{A} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, F)$$
 and $\mathcal{B} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E - F)$ with
 $\deg(E) > \deg(F) = t + g$ is a *t*-ECP for \mathcal{C}

Proposition 2: To compute a *t*-ECP for $C = C_L(\mathcal{X}, \mathcal{P}, E)$ it suffise to compute a code of type $\mathcal{B} = C_L(\mathcal{X}, \mathcal{P}, E - (t+g)P)$

If we know

$$\mathcal{C} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)^{\perp}$$
 and $\mathcal{B} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E - (t+g)P)$

Proposition 1: [Pellikaan 1992]

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

Then,
$$\mathcal{A} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, F)$$
 and $\mathcal{B} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E - F)$ with
 $\deg(E) > \deg(F) = t + g$ is a *t*-ECP for \mathcal{C}

Proposition 2: To compute a *t*-ECP for $C = C_L(\mathcal{X}, \mathcal{P}, E)$ it suffise to compute a code of type $\mathcal{B} = C_L(\mathcal{X}, \mathcal{P}, E - (t+g)P)$

If we know

$$\mathcal{C} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)^{\perp}$$
 and $\mathcal{B} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E - (t+g)P)$

Let, $\mathcal{A} = (\mathcal{B} * \mathcal{C})^{\perp}$. Then the pair $(\mathcal{A}, \mathcal{B})$ is a *t*-ECP for \mathcal{C}

Public Key:
$$\mathcal{K}_{\text{pub}} = \begin{cases} \text{ a generator matrix of } \mathcal{C}_{\text{pub}} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)^{\perp} \\ \text{ and } t = \left\lfloor \frac{d(\mathcal{C}) - g - 1}{2} \right\rfloor \end{cases}$$

The Algorithm: Assume that
$$\frac{n}{2} - 1 \ge \deg(E)$$

Public Key:
$$\mathcal{K}_{\text{pub}} = \begin{cases} \text{ a generator matrix of } \mathcal{C}_{\text{pub}} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)^{\perp} \\ \text{ and } t = \left\lfloor \frac{d(\mathcal{C}) - g - 1}{2} \right\rfloor \end{cases}$$

The Algorithm: Assume that $\frac{n}{2} - 1 \ge \deg(E)$

1. Determine the codes

$$\mathcal{C}_0 = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E) = \mathcal{C}_{pub}^{\perp}$$
 and $\mathcal{C}_1 = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E - P_1)$

Note that C_1 is the set of codewords of C_0 which are zero at position P_1

Public Key:
$$\mathcal{K}_{\text{pub}} = \begin{cases} \text{ a generator matrix of } \mathcal{C}_{\text{pub}} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)^{\perp} \\ \text{ and } t = \left\lfloor \frac{d(\mathcal{C}) - g - 1}{2} \right\rfloor \end{cases}$$

The Algorithm: Assume that $\frac{n}{2} - 1 \ge \deg(E)$

1. Determine the codes

$$\mathcal{C}_0 = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E) = \mathcal{C}_{pub}^{\perp}$$
 and $\mathcal{C}_1 = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E - P_1)$

Note that C_1 is the set of codewords of C_0 which are zero at position P_1

Generator matrix
for
$$C_0$$
 $G = \begin{pmatrix} 1 & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{k2} & \dots & a_{kn} \end{pmatrix}$

Public Key:
$$\mathcal{K}_{\text{pub}} = \begin{cases} \text{ a generator matrix of } \mathcal{C}_{\text{pub}} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)^{\perp} \\ \text{ and } t = \left\lfloor \frac{d(\mathcal{C}) - g - 1}{2} \right\rfloor \end{cases}$$

The Algorithm: Assume that $\frac{n}{2} - 1 \ge \deg(E)$

1. Determine the codes

$$\mathcal{C}_0 = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E) = \mathcal{C}_{pub}^{\perp}$$
 and $\mathcal{C}_1 = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E - P_1)$

Note that C_1 is the set of codewords of C_0 which are zero at position P_1

Generator matrix
for
$$\mathcal{C}_0$$
 $\mathcal{G} = \begin{pmatrix} 1 & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{k2} & \dots & a_{kn} \end{pmatrix}$ Generator matrix
for \mathcal{C}_1

Public Key:
$$\mathcal{K}_{\text{pub}} = \begin{cases} \text{ a generator matrix of } \mathcal{C}_{\text{pub}} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)^{\perp} \\ \text{ and } t = \left\lfloor \frac{d(\mathcal{C}) - g - 1}{2} \right\rfloor \end{cases}$$

The Algorithm: Assume that $\frac{n}{2} - 1 \ge \deg(E)$

1. Determine the codes

$$\mathcal{C}_0 = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E) = \mathcal{C}_{pub}^{\perp}$$
 and $\mathcal{C}_1 = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E - P_1)$

Note that C_1 is the set of codewords of C_0 which are zero at position P_1 2. Build the filtration:

$$\underbrace{\mathcal{C}_{L}(\mathcal{X},\mathcal{P},E)}_{\mathcal{C}_{pub}^{\perp}=\mathcal{C}_{0}}\supseteq\underbrace{\mathcal{C}_{L}(\mathcal{X},\mathcal{P},E-P_{1})}_{\mathcal{C}_{1}}\supseteq\ldots\supseteq\underbrace{\mathcal{C}_{L}(\mathcal{X},\mathcal{P},E-(t+g)P_{1})}_{\mathcal{C}_{t+g}}$$

Public Key:
$$\mathcal{K}_{\text{pub}} = \begin{cases} \text{ a generator matrix of } \mathcal{C}_{\text{pub}} = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E)^{\perp} \\ \text{ and } t = \left\lfloor \frac{d(\mathcal{C}) - g - 1}{2} \right\rfloor \end{cases}$$

The Algorithm: Assume that $\frac{n}{2} - 1 \ge \deg(E)$

1. Determine the codes

$$\mathcal{C}_0 = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E) = \mathcal{C}_{pub}^{\perp}$$
 and $\mathcal{C}_1 = \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E - P_1)$

Note that C_1 is the set of codewords of C_0 which are zero at position P_1 2. Build the filtration:

$$\underbrace{\mathcal{C}_{L}(\mathcal{X},\mathcal{P},E)}_{\mathcal{C}_{pub}^{\perp}=\mathcal{C}_{0}}\supseteq\underbrace{\mathcal{C}_{L}(\mathcal{X},\mathcal{P},E-P_{1})}_{\mathcal{C}_{1}}\supseteq\ldots\supseteq\underbrace{\mathcal{C}_{L}(\mathcal{X},\mathcal{P},E-(t+g)P_{1})}_{\mathcal{C}_{t+g}}$$

3. Return $(\mathcal{A}, \mathcal{B})$ which is an *ECP* for \mathcal{C} where:

$$\mathcal{B} = \mathcal{C}_{t+g}$$
 and $\mathcal{A} = (\mathcal{B} * \mathcal{C})^{\perp}$

4. Key Attacks

- 1. Introduction
- 2. Support Splitting Algorithm
- 3. Distinguisher for GRS codes
- 4. Attack against subcodes of GRS codes
- 5. Error-Correcting Pairs
- 6. Attack against GRS codes
- 7. Attack against Reed-Muller codes
- 8. Attack against Algebraic Geometry codes
- 9. Goppa codes still resist