New Direction for Rank-Based Cryptography

Hervé Talé Kalachi

LACGAA Seminar

Université Cheikh Anta Diop, Dakar

April 15, 2023

Outline

1. Code-Based Cryptography
2. Rank-Based Cryptography
3. New Direction for Rank-Based Cryptography

Linear code

1. $(\mathbb{F}^n, \|\cdot\|)$, $\mathbb{F}$ a finite field and $\|\cdot\|$ a norm
2. Linear code $\mathscr{C}$ = v.ss of $(\mathbb{F}^n, \|\cdot\|)$

$$\mathscr{C} = \bigoplus_{i=1}^{k} \mathbb{F}\, \vec{v}_i$$

where $\vec{v}_i$ are linearly independent.

3. The matrix $\boldsymbol{G} = \begin{pmatrix} \vec{v}_1 \\ . \\ . \\ . \\ \vec{v}_k \end{pmatrix}$ is called a generator matrix of $\mathscr{C}$
4. Any $k \times n$ matrix whose rows form a basis of $\mathscr{C}$ is also a generator matrix of $\mathscr{C}$

Linear code

1. $(\mathbb{F}^n, \|\cdot\|)$, $\mathbb{F}$ a finite field and $\|\cdot\|$ a norm
2. Linear code $\mathscr{C}$ = v.ss of $(\mathbb{F}^n, \|\cdot\|)$

$$\mathscr{C} = \bigoplus_{i=1}^{k} \mathbb{F}\, \vec{v}_i$$

   where $\vec{v}_i$ are linearly independent.
3. The matrix $\boldsymbol{G} = \begin{pmatrix} \vec{v}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{v}_k \end{pmatrix}$ is called a generator matrix of $\mathscr{C}$
4. Any $k \times n$ matrix whose rows form a basis of $\mathscr{C}$ is also a generator matrix of $\mathscr{C}$

Introduction

Linear code

1. $(\mathbb{F}^n, \|\cdot\|)$, $\mathbb{F}$ a finite field and $\|\cdot\|$ a norm

2. Linear code $\mathscr{C}$ = v.ss of $(\mathbb{F}^n, \|\cdot\|)$

$$\mathscr{C} = \bigoplus_{i=1}^{k} \mathbb{F}\,\vec{v}_i$$

where $\vec{v}_i$ are linearly independent.

3. The matrix $\boldsymbol{G} = \begin{pmatrix} \vec{v}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{v}_k \end{pmatrix}$ is called a generator matrix of $\mathscr{C}$

4. Any $k \times n$ matrix whose rows form a basis of $\mathscr{C}$ is also a generator matrix of $\mathscr{C}$

Introduction

Linear code

1. $(\mathbb{F}^n, \|\cdot\|)$, $\mathbb{F}$ a finite field and $\|\cdot\|$ a norm

2. Linear code $\mathscr{C}$ = v.ss of $(\mathbb{F}^n, \|\cdot\|)$

$$\mathscr{C} = \bigoplus_{i=1}^{k} \mathbb{F}\, \vec{v}_i$$

where $\vec{v}_i$ are linearly independent.

3. The matrix $\boldsymbol{G} = \begin{pmatrix} \vec{v}_1 \\ . \\ . \\ . \\ \vec{v}_k \end{pmatrix}$ is called a generator matrix of $\mathscr{C}$

4. Any $k \times n$ matrix whose rows form a basis of $\mathscr{C}$ is also a generator matrix of $\mathscr{C}$

Introduction

Linear code

1. $(\mathbb{F}^n, \|\cdot\|)$, $\mathbb{F}$ a finite field and $\|\cdot\|$ a norm

2. Linear code $\mathscr{C}$ = v.ss of $(\mathbb{F}^n, \|\cdot\|)$

$$\mathscr{C} = \bigoplus_{i=1}^{k} \mathbb{F}\, \vec{v}_i$$

where $\vec{v}_i$ are linearly independent.

3. The matrix $\boldsymbol{G} = \begin{pmatrix} \vec{v}_1 \\ . \\ . \\ . \\ \vec{v}_k \end{pmatrix}$ is called a generator matrix of $\mathscr{C}$

4. Any $k \times n$ matrix whose rows form a basis of $\mathscr{C}$ is also a generator matrix of $\mathscr{C}$

Introduction

Hamming metric

Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ and $\vec{x} = (x_1 \cdots x_n) \in \mathbb{F}_{q^m}^n$.

$$\|\vec{x}\|_h = \#\{\ i\ :\ x_i \neq 0\}$$

Example

- $\mathbb{F} = \mathbb{F}_{2^5} = \mathbb{F}_2 < w > = < 1, w, w^2, w^3, w^4 >_{\mathbb{F}_2}$
- $\vec{x} = (w, 0, 0, w)$
-

$$\|\vec{x}\|_h = 2$$

Hamming metric

Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ and $\vec{x} = (x_1 \cdots x_n) \in \mathbb{F}_{q^m}^n$.

$$\|\vec{x}\|_h = \#\{\ i\ :\ x_i \neq 0\}$$

Example

- $\mathbb{F} = \mathbb{F}_{2^5} = \mathbb{F}_2 < w >=< 1, w, w^2, w^3, w^4 >_{\mathbb{F}_2}$
- $\vec{x} = (w, 0, 0, w)$
-

$$\|\vec{x}\|_h = 2$$

Introduction

Hamming metric

Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ and $\vec{x} = (x_1 \cdots x_n) \in \mathbb{F}_{q^m}^n$.

$$\|\vec{x}\|_h = \#\{\ i\ :\ x_i \neq 0\}$$

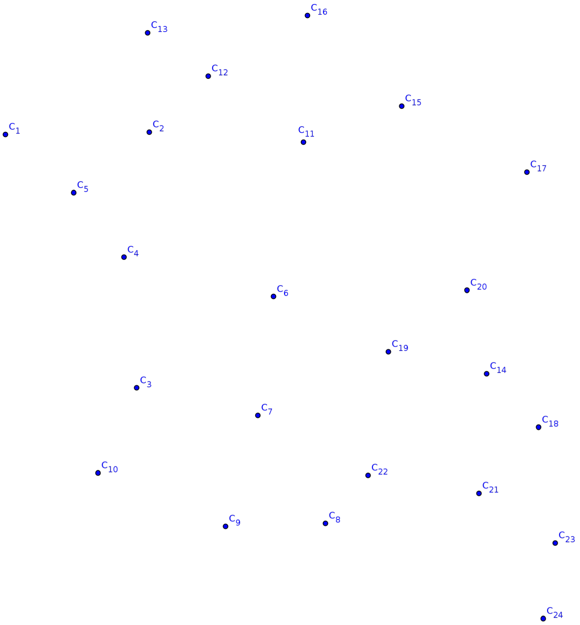
Example

- $\mathbb{F} = \mathbb{F}_{2^5} = \mathbb{F}_2 < w > = < 1, w, w^2, w^3, w^4 >_{\mathbb{F}_2}$
- $\vec{x} = (w, 0, 0, w)$
- $$\|\vec{x}\|_h = 2$$

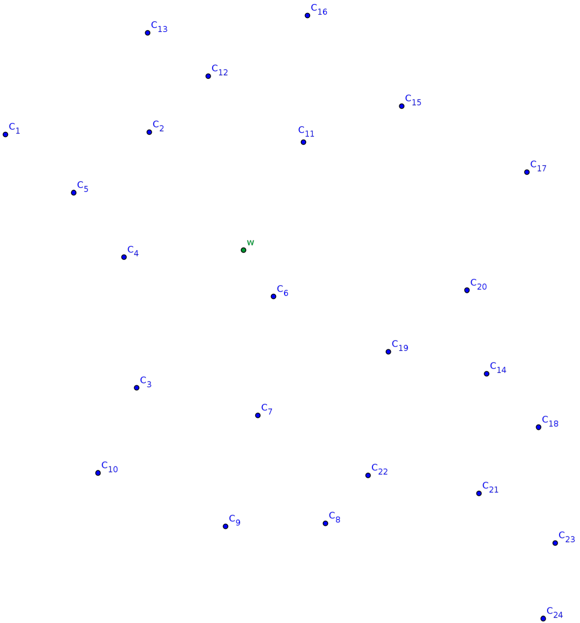
Introduction

Decoding $\vec{w} \in \mathbb{F}^n$ in $\mathscr{C}$ $=$ Closest Vector Problem (CVP)

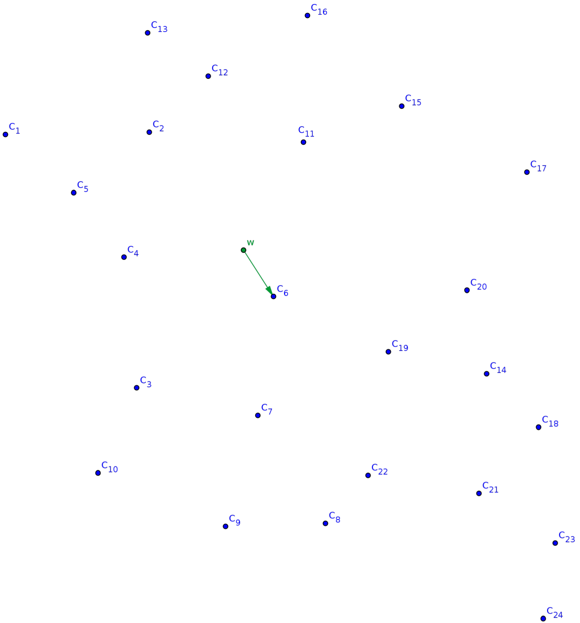
Introduction



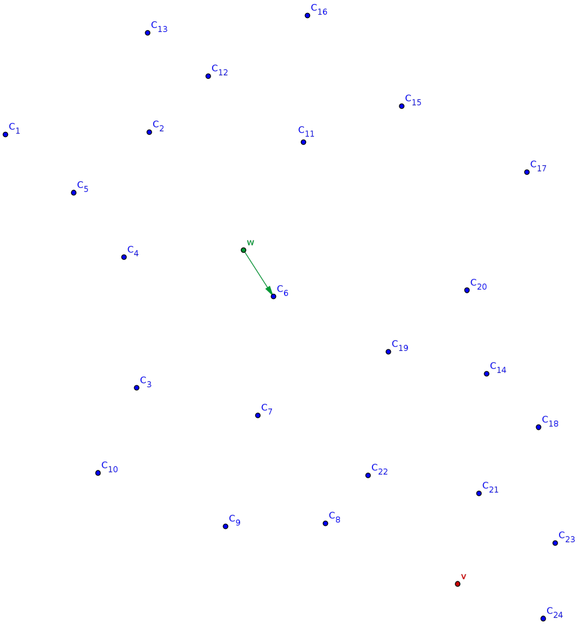
Introduction - Decoding



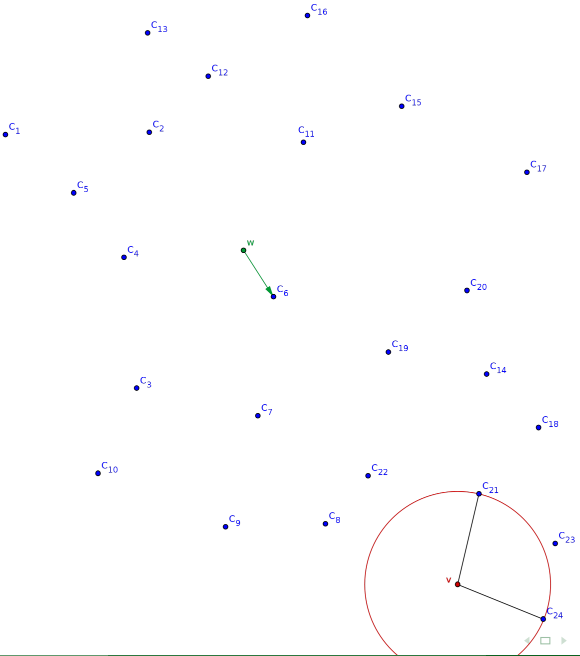
Introduction - Decoding



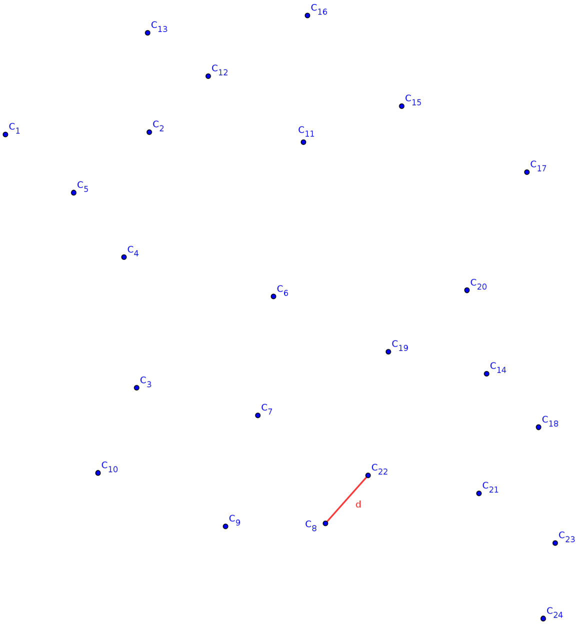
Introduction - Decoding



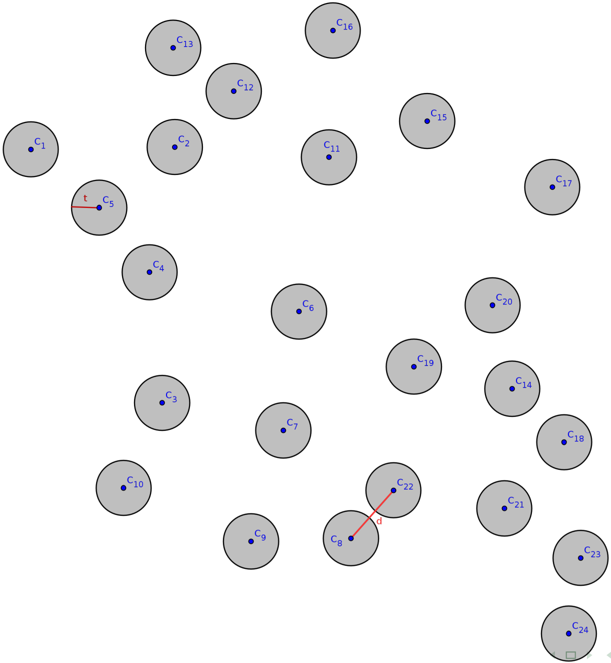
Introduction - Decoding



Introduction - Decoding



Introduction - Decoding



Introduction - Decoding

Hardness of decoding

- Decoding is NP-Hard for a "random" linear code
- For Hamming metric: Berlekamp-McEliece-Van Tilborg '78

Solving the decoding problem

- Information set decoding
- Introduced by Prange '62
- Complexity: $2^{at(1+o(1))}$

$$a = constante(\frac{k}{n}, \frac{t}{n})$$

Hardness of decoding

- Decoding is NP-Hard for a "random" linear code
- For Hamming metric: Berlekamp-McEliece-Van Tilborg '78

Solving the decoding problem

- Information set decoding
- Introduced by Prange '62
- Complexity: $2^{at(1+o(1))}$

$$a = constante(\frac{k}{n}, \frac{t}{n})$$

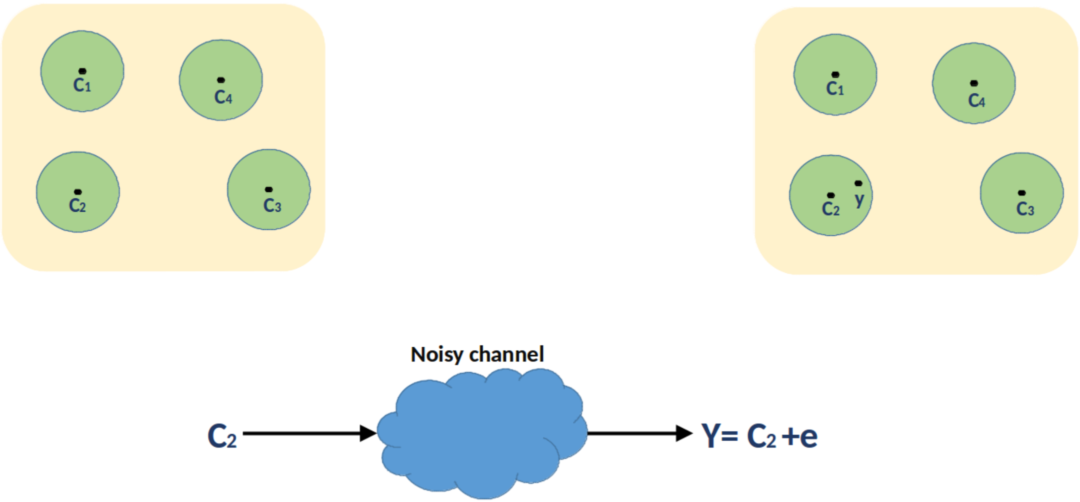
Some codes with efficient decoding algorithms

1. **GRS** codes '60 — One-variable polynomials
2. **Goppa** codes '70 — Sub-field sub-codes of GRS codes
3. **Reed-Muller** codes '54 — Multivariate polynomials

Some codes with efficient decoding algorithms

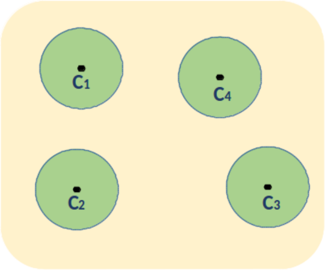
1. **GRS** codes '60 — One-variable polynomials
2. **Goppa** codes '70 — Sub-field sub-codes of GRS codes
3. **Reed-Muller** codes '54 — Multivariate polynomials

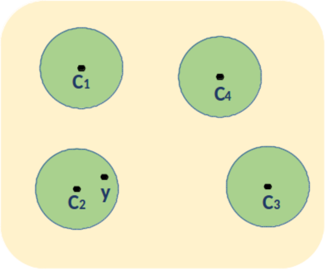
Theory of error correcting codes

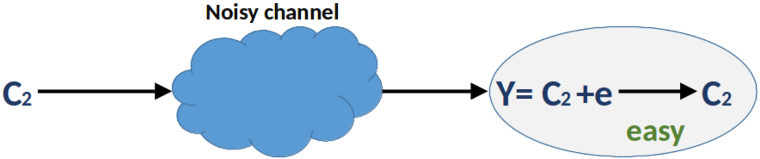


Theory of error correcting codes

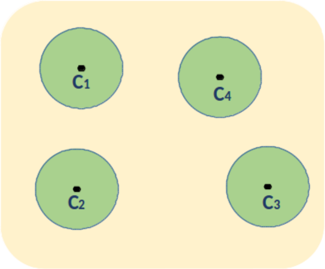
With the knowledge of a good basis

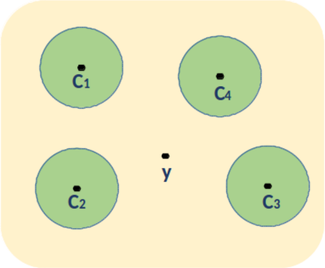


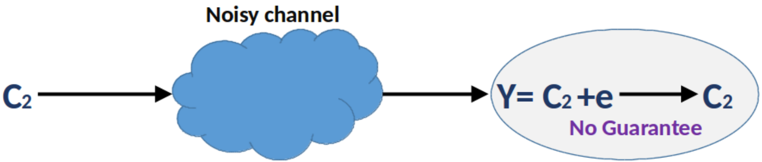


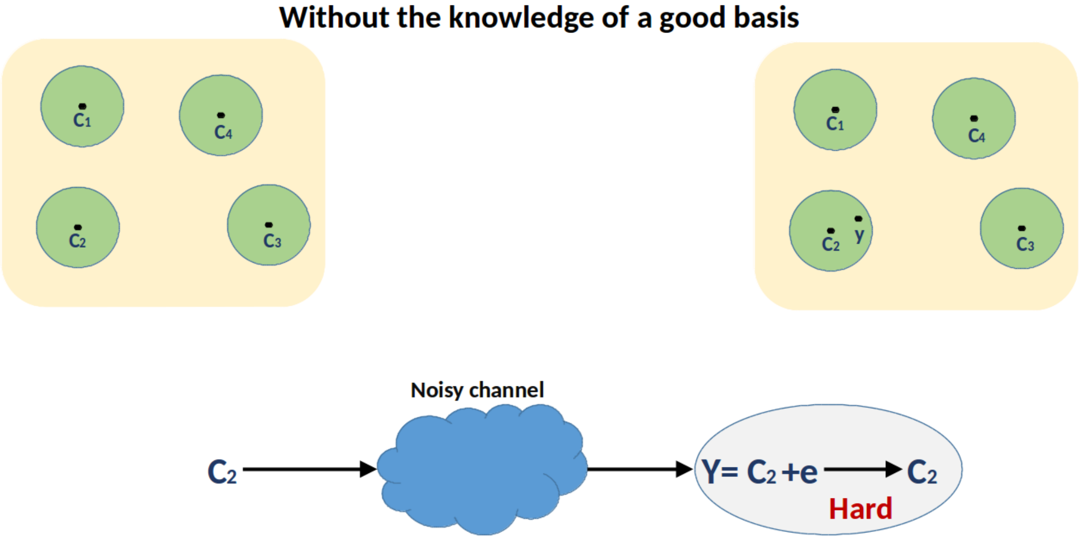


With the knowledge of a good basis








Without the knowledge of a good basis
C1
C4
C2
C3
C1
C4
C2
y
C3
Noisy channel
C2
Y= C2 +e
C2
Hard

Plan

1. Code-Based Cryptography
2. Rank-Based Cryptography
3. New Direction for Rank-Based Cryptography

McEliece Cryptosystem

McEliece Cryptosystem ('78)

1. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm (good basis)
2. McEliece proposed binary Goppa codes

Security assumptions

- Indistinguishability of Goppa codes **Courtois-Finiasz-Sendrier '01**
- Hardness of decoding a "random" linear code

McEliece Cryptosystem

McEliece Cryptosystem ('78)

1. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm (good basis)
2. McEliece proposed binary Goppa codes

Security assumptions

- Indistinguishability of Goppa codes **Courtois-Finiasz-Sendrier '01**
- Hardness of decoding a "random" linear code

McEliece Cryptosystem

McEliece Cryptosystem ('78)

1. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm (good basis)
2. McEliece proposed binary Goppa codes

Security assumptions

- Indistinguishability of Goppa codes **Courtois-Finiasz-Sendrier '01**
- Hardness of decoding a "random" linear code

McEliece Cryptosystem

McEliece Cryptosystem ('78)

1. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm (good basis)
2. McEliece proposed binary Goppa codes

Security assumptions

- Indistinguishability of Goppa codes **Courtois-Finiasz-Sendrier '01**
- Hardness of decoding a "random" linear code

McEliece Cryptosystem

McEliece Cryptosystem ('78)

1. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm (good basis)
2. McEliece proposed binary Goppa codes

Security assumptions

- Indistinguishability of Goppa codes **Courtois-Finiasz-Sendrier '01**
- Hardness of decoding a "random" linear code

McEliece Cryptosystem

McEliece Cryptosystem ('78)

1. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm (good basis)
2. McEliece proposed binary Goppa codes

Security assumptions

- Indistinguishability of Goppa codes **Courtois-Finiasz-Sendrier '01**
- Hardness of decoding a "random" linear code

McEliece Cryptosystem

McEliece Cryptosystem ('78)

1. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm (good basis)
2. McEliece proposed binary Goppa codes

Security assumptions

- Indistinguishability of Goppa codes **Courtois-Finiasz-Sendrier '01**
- Hardness of decoding a "random" linear code

McEliece Cryptosystem ('78)

Advantages

1. Encryption and decryption are very fast
2. No efficient attack
3. Candidate for Post-Quantum Cryptography

McEliece Cryptosystem ('78)

Advantages

1. Encryption and decryption are very fast
2. No efficient attack
3. Candidate for Post-Quantum Cryptography

McEliece Cryptosystem ('78)

Advantages

1. Encryption and decryption are very fast
2. No efficient attack
3. Candidate for Post-Quantum Cryptography

McEliece Cryptosystem ('78)

Advantages

1. Encryption and decryption are very fast
2. No efficient attack
3. Candidate for Post-Quantum Cryptography

McEliece Cryptosystem ('78)

NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PROJECTS | POST-QUANTUM CRYPTOGRAPHY

Post-Quantum Cryptography PQC

Round 4 Submissions

Official comments on the Fourth Round Candidate Algorithms should be submitted using the "Submit Comment" link for the appropriate algorithm. Comments from the pqc-forum Google group subscribers will also be forwarded to the pqc-forum Google group list. We will periodically post and update the comments received to the appropriate algorithm.

All relevant comments will be posted in their entirety and should not include PII information in the body of the email message.

Please refrain from using OFFICIAL COMMENT to ask administrative questions, which should be sent to pqc-comments@nist.gov

PROJECT LINKS

- Overview
- FAQs
- News & Updates
- Events
- Publications
- Presentations

ADDITIONAL PAGES

McEliece Cryptosystem ('78)

Classic McEliece *(merger of Classic McEliece and NTS-KEM*	GZ file (4MB) KAT files (GZ format) (93MB) Website	Daniel J. Bernstein Tung Chou Carlos Cid Jan Gilcher Tanja Lange Varun Maram Ingo von Maurich Rafael Misoczki Ruben Niederhagen Edoardo Persichetti Christiane Peters Nicolas Sendrier Jakub Szefer Cen Jung Tjhai Martin Tomlinson Wen Wang	Submit Comment View Comments

McEliece Cryptosystem ('78)

Advantages

1. Encryption and decryption are very fast
2. No efficient attack
3. Candidate for Post-Quantum Cryptography

Drawback

1. Enormous size of the Public Key

McEliece Cryptosystem ('78)

Advantages

1. Encryption and decryption are very fast
2. No efficient attack
3. Candidate for Post-Quantum Cryptography

Drawback

1. Enormous size of the Public Key

McEliece Cryptosystem - Reduction of key size

Use another family of codes

1. GRS codes by **Niederreiter '86**
2. Reed-Muller codes by **Sidelnikov '94**
3. Algebraic geometric codes by **Janwa-Moreno '96**
4. LDPC codes by **Monico-Rosenthal-Shokrollahi '00**
5. Wild Goppa (non-binary) by **Bernstein-Lange-Peters '10**
6. Polar codes by **Shrestha-Kim '14**

McEliece Cryptosystem - Reduction of key size

Use another family of codes

1. GRS codes by **Niederreiter '86**
2. Reed-Muller codes by **Sidelnikov '94**
3. Algebraic geometric codes by **Janwa-Moreno '96**
4. LDPC codes by **Monico-Rosenthal-Shokrollahi '00**
5. Wild Goppa (non-binary) by **Bernstein-Lange-Peters '10**
6. Polar codes by **Shrestha-Kim '14**

Use another family of codes

1. GRS codes by **Niederreiter '86**
2. Reed-Muller codes by **Sidelnikov '94**
3. Algebraic geometric codes by **Janwa-Moreno '96**
4. LDPC codes by **Monico-Rosenthal-Shokrollahi '00**
5. Wild Goppa (non-binary) by **Bernstein-Lange-Peters '10**
6. Polar codes by **Shrestha-Kim '14**

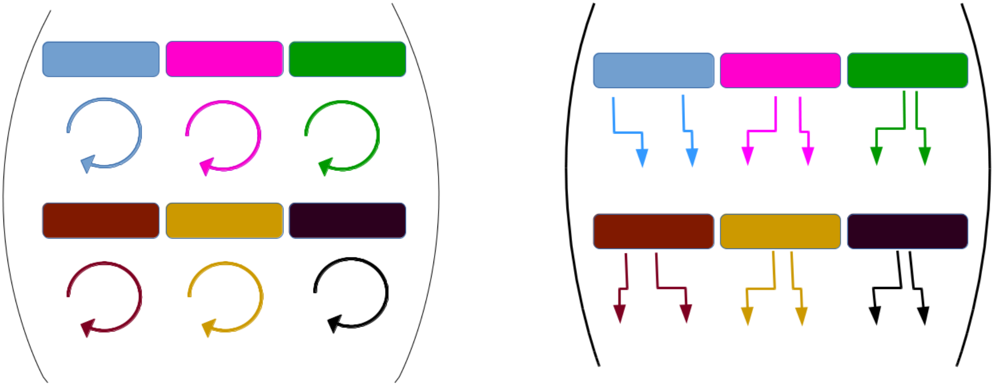
Use another family of codes

1. GRS codes by **Niederreiter '86**
2. Reed-Muller codes by **Sidelnikov '94**
3. Algebraic geometric codes by **Janwa-Moreno '96**
4. LDPC codes by **Monico-Rosenthal-Shokrollahi '00**
5. Wild Goppa (non-binary) by **Bernstein-Lange-Peters '10**
6. Polar codes by **Shrestha-Kim '14**

McEliece Cryptosystem - Reduction of key size

Use another family of codes

1. GRS codes by **Niederreiter '86**
2. Reed-Muller codes by **Sidelnikov '94**
3. Algebraic geometric codes by **Janwa-Moreno '96**
4. LDPC codes by **Monico-Rosenthal-Shokrollahi '00**
5. Wild Goppa (non-binary) by **Bernstein-Lange-Peters '10**
6. Polar codes by **Shrestha-Kim '14**



Quasi-cyclique **Quasi-dyadique**

McEliece Cryptosystem (Use more structured codes)

csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions#

NIST

Search CSRC

CSRC MENU

BIKE	Zip File (77MB) IP Statements Website	Nicolas Aragon Paulo Barreto Slim Bettaieb Loic Bidoux Olivier Blazy Jean-Christophe Deneuville Phillipe Gaborit Shay Gueron Tim Guneysu Carlos Aguilar Melchor Rafael Misoczki Edoardo Persichetti Nicolas Sendrier Jean-Pierre Tillich Gilles Zemor Valentin Vasseur	Submit Comment View Comments

McEliece Cryptosystem (Use more structured codes)

DAGS	Zip File (1MB) KAT Files (18MB) IP Statements Website	Gustavo Banegas Paolo S. L. M. Barreto Brice Odilon Boidje Pierre-Louis Cayrel Gilbert Ndollane Dione Kris Gaj Cheikh Thiecoumba Gueye Richard Haeussler Jean Belo Klamti Ousmane N'diaye Duc Tri Nguyen Edoardo Persichetti Jefferson E. Ricardini	Submit Comment View Comments

McEliece Cryptosystem - Reduction of key size

Several families do not behave like random codes

Example: GRS Codes - Distinguisher based on code product

- Schur / Star product of $\vec{a} = (a_1, ..., a_n),\ \vec{b} = (b_1, ..., b_n) \in \mathbb{F}_q^n$

$$\vec{a} \star \vec{b} \overset{def}{=} (a_1 b_1, ..., a_n b_n)$$

- $\mathscr{A}$ and $\mathscr{B}$ are two codes of length n.
- $\mathscr{A} \star \mathscr{B} \overset{\text{def}}{=} \left\{ \vec{a} \star \vec{b} : \vec{a} \in \mathscr{A}, \vec{b} \in \mathscr{B} \right\}$
- $\mathscr{B} = \mathscr{A} \to \mathscr{A}^2$

- "Random" code $\mathscr{A}$

$$\dim(\mathscr{A}^2) = \binom{\dim(\mathscr{A}) + 1}{2}$$

- GRS code

$$\dim(GRS^2) = 2\dim(GRS) - 1$$

Several families do not behave like random codes

Example: GRS Codes - Distinguisher based on code product

- Schur / Star product of $\vec{a} = (a_1, \dots, a_n)$, $\vec{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$

$$\vec{a} \star \vec{b} \overset{def}{=} (a_1 b_1, \dots, a_n b_n)$$

- $\mathscr{A}$ and $\mathscr{B}$ are two codes of length n.
- $\mathscr{A} \star \mathscr{B} \overset{\text{def}}{=} \left\{ \vec{a} \star \vec{b} : \vec{a} \in \mathscr{A}, \vec{b} \in \mathscr{B} \right\}$
- $\mathscr{B} = \mathscr{A} \rightarrow \mathscr{A}^2$

- "Random" code $\mathscr{A}$

$$\dim(\mathscr{A}^2) = \binom{\dim(\mathscr{A}) + 1}{2}$$

- GRS code

$$\dim(GRS^2) = 2\dim(GRS) - 1$$

McEliece Cryptosystem - Reduction of key size

Several families do not behave like random codes

Example: GRS Codes - Distinguisher based on code product

- Schur / Star product of $\vec{a} = (a_1, \dots, a_n),\ \vec{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$

$$\vec{a} \star \vec{b} \overset{def}{=} (a_1 b_1, \dots, a_n b_n)$$

- $\mathscr{A}$ and $\mathscr{B}$ are two codes of length n.
- $\mathscr{A} \star \mathscr{B} \overset{\text{def}}{=} \left\{ \vec{a} \star \vec{b} : \vec{a} \in \mathscr{A}, \vec{b} \in \mathscr{B} \right\}$
- $\mathscr{B} = \mathscr{A} \to \mathscr{A}^2$

- "Random" code $\mathscr{A}$

$$\dim(\mathscr{A}^2) = \binom{\dim(\mathscr{A}) + 1}{2}$$

- GRS code

$$\dim(GRS^2) = 2\dim(GRS) - 1$$

Several families do not behave like random codes

Example: GRS Codes - Distinguisher based on code product

- Schur / Star product of $\vec{a} = (a_1, \dots, a_n),\ \vec{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$

$$\vec{a} \star \vec{b} \stackrel{def}{=} (a_1 b_1, \dots, a_n b_n)$$

- $\mathscr{A}$ and $\mathscr{B}$ are two codes of length n.
- $\mathscr{A} \star \mathscr{B} \stackrel{\text{def}}{=} \left\{ \vec{a} \star \vec{b} : \vec{a} \in \mathscr{A}, \vec{b} \in \mathscr{B} \right\}$

- $\mathscr{B} = \mathscr{A} \to \mathscr{A}^2$

- "Random" code $\mathscr{A}$

$$\dim(\mathscr{A}^2) = \binom{\dim(\mathscr{A}) + 1}{2}$$

- GRS code

$$\dim(GRS^2) = 2\dim(GRS) - 1$$

Several families do not behave like random codes

Example: GRS Codes - Distinguisher based on code product

- Schur / Star product of $\vec{a} = (a_1, \ldots, a_n),\ \vec{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$

$$\vec{a} \star \vec{b} \overset{def}{=} (a_1 b_1, \ldots, a_n b_n)$$

- $\mathscr{A}$ and $\mathscr{B}$ are two codes of length n.
- $\mathscr{A} \star \mathscr{B} \overset{\text{def}}{=} \left\{ \vec{a} \star \vec{b} : \vec{a} \in \mathscr{A}, \vec{b} \in \mathscr{B} \right\}$
- $\mathscr{B} = \mathscr{A} \to \mathscr{A}^2$

- "Random" code $\mathscr{A}$

$$\dim(\mathscr{A}^2) = \binom{\dim(\mathscr{A}) + 1}{2}$$

- GRS code

$$\dim(GRS^2) = 2\dim(GRS) - 1$$

McEliece Cryptosystem - Reduction of key size

Date	Scheme	Attack	Complexity
1994	GRS	Sidelnikov-Shestakov	polynomial
2007	Reed-Muller	Minder-Shokrollahi	Sub-exponential
2013	GRS	Couvreur-Gaborit-Gauthier-Otmani-Tillich	polynomial
2010	quasi-cyclic alternants	Faugère-Otmani-Tillich	polynomial
2013	Reed-Muller	Chizhov-Borodin	polynomial
2014	Wild Goppa (non-binary) $m = 2$	Couvreur-Otmani-Tillich	polynomial
2014	AG Codes	Couvreur-Màrquez Corbella-Pellikaan	polynomial
2014	quasi-dyadic Goppa	Faugère-Otmani-Perret-Portzamparc-Tillich	polynomial
2014	AG codes	Couvreur-Màrquez Corbella-Pellikaan	polynomial

Rank Metric Vs Hamming Metric

Example

- $\mathbb{F} = \mathbb{F}_{2^5} = \mathbb{F}_2 < w > = < 1, w, w^2, w^3, w^4 >_{\mathbb{F}_2}$
- $\vec{x} = (w, 0, 0, w)$

1. **Hamming metric:**
   - $\|\vec{x}\|_h = 2$
2. **Rank metric:**
   - $\|\vec{x}\|_2 = \dim\left(< w, w >_{\mathbb{F}_2}\right) = 1$

Rank Metric Vs Hamming Metric

Example

- $\mathbb{F} = \mathbb{F}_{2^5} = \mathbb{F}_2 < w >=< 1, w, w^2, w^3, w^4 >_{\mathbb{F}_2}$
- $\vec{x} = (w, 0, 0, w)$

1. **Hamming metric:**
   - $\|\vec{x}\|_h = 2$
2. **Rank metric:**
   - $\|\vec{x}\|_2 = \dim\left(< w, w >_{\mathbb{F}_2}\right) = 1$

Rank Metric Vs Hamming Metric

Hardness of decoding

- Decoding is NP-Hard for a "random" linear code
  - For Hamming metric: Berlekamp-McEliece-Van Tilborg '78
  - For Rank metric: Gaborit-Zémor '16

Solving the decoding problem

1. Hamming metric
   - Information set decoding
   - Complexity: $2^{at(1+o(1))}$

     $$a = constante(\frac{k}{n}, \frac{t}{n})$$

2. Rank metric :
   - Ourivski-Johannsson '02

     $$(tm)^3 2^{kt+f(k,t)}$$

   - Aragon-Gaborit-Hautville-Tillich '18 ($n \geqslant m$)

     $$(n-k)^3 m^3 2^{w\lceil \frac{(k+1)m}{n} \rceil - m}$$

Hardness of decoding

- Decoding is NP-Hard for a "random" linear code
  - For Hamming metric: Berlekamp-McEliece-Van Tilborg '78
  - For Rank metric: Gaborit-Zémor '16

Solving the decoding problem

1. Hamming metric
   - Information set decoding
   - Complexity: $2^{at(1+o(1))}$

$$a = constante(\frac{k}{n}, \frac{t}{n})$$

2. Rank metric :
   - Ourivski-Johannsson '02

$$(tm)^3 2^{kt+f(k,t)}$$

   - Aragon-Gaborit-Hautville-Tillich '18 ($n \geqslant m$)

$$(n-k)^3 m^3 2^{w\lceil \frac{(k+1)m}{n} \rceil - m}$$

Rank Metric Vs Hamming Metric

Hardness of decoding

- Decoding is NP-Hard for a "random" linear code
  - For Hamming metric: Berlekamp-McEliece-Van Tilborg '78
  - For Rank metric: Gaborit-Zémor '16

Solving the decoding problem

1. Hamming metric
   - Information set decoding
   - Complexity: $2^{at(1+o(1))}$

$$a = constante(\frac{k}{n}, \frac{t}{n})$$

2. Rank metric :
   - Ourivski-Johannsson '02

$$(tm)^3 2^{kt+f(k,t)}$$

   - Aragon-Gaborit-Hautville-Tillich '18 ($n \geqslant m$)

$$(n-k)^3 m^3 2^{w\lceil \frac{(k+1)m}{n} \rceil - m}$$

Plan

Rank metric cryptography

Gabidulin-Paramonov-Tretjakov cryptosystem '91

1. Rank metric with Gabidulin codes
2. But many attacks
   - Gibson's attacks '95, '96
   - Overbeck's attack '05

Some GPT Variants

- **Gabidulin '08**
- **Rashwan-Gabidulin-Honary '10**

Rank metric cryptography

Gabidulin-Paramonov-Tretjakov cryptosystem ’91

1. Rank metric with Gabidulin codes
2. But many attacks
   - Gibson’s attacks ’95, ’96
   - Overbeck’s attack ’05

Some GPT Variants

- **Gabidulin ’08**
- **Rashwan-Gabidulin-Honary ’10**

Rank metric cryptography

Gabidulin-Paramonov-Tretjakov cryptosystem '91

1. Rank metric with Gabidulin codes
2. But many attacks
    - Gibson's attacks '95, '96
    - Overbeck's attack '05

Some GPT Variants

- **Gabidulin '08**
- **Rashwan-Gabidulin-Honary '10**

Rank metric cryptography

Gabidulin-Paramonov-Tretjakov cryptosystem '91

1. Rank metric with Gabidulin codes
2. But many attacks
   - Gibson's attacks '95, '96
   - Overbeck's attack '05

Some GPT Variants

- **Gabidulin '08**
- **Rashwan-Gabidulin-Honary '10**

Rank metric cryptography

Gabidulin-Paramonov-Tretjakov cryptosystem ’91

1. Rank metric with Gabidulin codes
2. But many attacks
   - Gibson’s attacks ’95, ’96
   - Overbeck’s attack ’05

Some GPT Variants

- **Gabidulin ’08**
- **Rashwan-Gabidulin-Honary ’10**

Rank metric cryptography

Gabidulin-Paramonov-Tretjakov cryptosystem ’91

1. Rank metric with Gabidulin codes
2. But many attacks
   - Gibson’s attacks ’95, ’96
   - Overbeck’s attack ’05

Some GPT Variants

- **Gabidulin ’08**
- **Rashwan-Gabidulin-Honary ’10**

Gabidulin's codes do not behave like random codes

- Overbeck's distinguisher :

$$\begin{array}{cccc} \Lambda_f : & \mathbb{F}_{q^m}^n & \longrightarrow & \mathbb{F}_{q^m}^n \\ & \mathscr{U} & \longmapsto & \Lambda_f(\mathscr{U}) \stackrel{\text{def}}{=} \mathscr{U} + \mathscr{U}^q + \cdots + \mathscr{U}^{q^f} \end{array}$$

- "Random" code $\mathscr{A}$
- Gabidulin code

$\dim(\Lambda_f(\mathscr{A})) = \min\{n, k(f+1)\}$, $\dim(\Lambda_f(Gab)) = \dim(Gab) + f$

Gabidulin's codes do not behave like random codes

- Overbeck's distinguisher :

$$\begin{array}{rccl} \Lambda_f : & \mathbb{F}_{q^m}^n & \longrightarrow & \mathbb{F}_{q^m}^n \\ & \mathscr{U} & \longmapsto & \Lambda_f(\mathscr{U}) \stackrel{\text{def}}{=} \mathscr{U} + \mathscr{U}^q + \cdots + \mathscr{U}^{q^f} \end{array}$$

- "Random" code $\mathscr{A}$
- Gabidulin code

$\dim(\Lambda_f(\mathscr{A})) = \min\{n, k(f+1)\}$, $\dim(\Lambda_f(Gab)) = \dim(Gab) + f$

Gabidulin's codes do not behave like random codes

- Overbeck's distinguisher :

$$\begin{array}{rccl} \Lambda_f : & \mathbb{F}_{q^m}^n & \longrightarrow & \mathbb{F}_{q^m}^n \\ & \mathscr{U} & \longmapsto & \Lambda_f(\mathscr{U}) \stackrel{\text{def}}{=} \mathscr{U} + \mathscr{U}^q + \cdots + \mathscr{U}^{q^f} \end{array}$$

- "Random" code $\mathscr{A}$
- Gabidulin code

$\dim(\Lambda_f(\mathscr{A})) = \min\{n, k(f+1)\}$, $\dim(\Lambda_f(Gab)) = \dim(Gab) + f$

LRPC Codes with application to cryptography [1]

- $\mathscr{V} =< \vec{v}_1, \cdots, \vec{v}_d >_{\mathbb{F}_q} \subset \mathbb{F}_{q^m}$
- $\boldsymbol{H} \in \mathcal{M}_{n-k \times n}(\mathscr{V})$, $Rank(\boldsymbol{H}) = n - k$
- $\boldsymbol{G}_{pub} \in \mathcal{M}_{k \times n}(\mathbb{F}_{q^m})$ such that $\boldsymbol{H}\boldsymbol{G}_{pub}^t = \mathbf{0}$
- The public key is

$$(\boldsymbol{G}_{pub}, t) \text{ with } t \leqslant \frac{n-k}{d}$$

[1] Gaborit-Murat-Ruatta-Zémor '13

Encryption with LRPC Codes

- $\vec{m} \in \mathbb{F}_{q^m}^k$ a message to encrypt
- $\mathscr{E} =< \vec{b}_1, \cdots, \vec{b}_t >_{\mathbb{F}_q} \subset \mathbb{F}_{q^m}$
- $\vec{e} \xleftarrow{\$} \mathscr{E}^n$
- The ciphertext is

$$\vec{y} = \vec{m}\boldsymbol{G}_{pub} + \vec{e}$$

Decryption

- Compute the syndrome

$$\vec{s} = \boldsymbol{H}\vec{y}^T = \boldsymbol{H}\boldsymbol{G}_{pub}^T\vec{m}^T + \boldsymbol{H}\vec{e}^T = \boldsymbol{H}\vec{e}^T$$

- Remember that

$$\boldsymbol{H} = (h_{ij})_{i,j} = \left(\sum_{\ell=1}^{d} h_{ij\ell}\vec{v}_\ell\right)_{i,j}, \quad h_{ij\ell} \in \mathbb{F}_q$$

- And

$$\vec{e} = (e_1, \cdots, e_n) = \left(\sum_{r=1}^{t} e_{1r}\vec{b}_r, \cdots, \sum_{r=1}^{t} e_{nr}\vec{b}_r\right) = \left(\sum_{r=1}^{t} e_{\eta r}\vec{b}_r\right)_\eta, \quad e_{\eta r} \in \mathbb{F}_q$$

- Thus,

$$s_i \in \; < \vec{v}_1\vec{b}_1, \vec{v}_1\vec{b}_2, \cdots, \vec{v}_d\vec{b}_t >_{\mathbb{F}_q}$$

Decryption

- Compute the syndrome

$$\vec{s} = \boldsymbol{H}\vec{y}^T = \boldsymbol{H}\boldsymbol{G}_{pub}^T\vec{m}^T + \boldsymbol{H}\vec{e}^T = \boldsymbol{H}\vec{e}^T$$

- Remember that

$$\boldsymbol{H} = (h_{ij})_{i,j} = \left(\sum_{\ell=1}^{d} h_{ij\ell}\vec{v}_\ell\right)_{i,j}, \quad h_{ij\ell} \in \mathbb{F}_q$$

- And

$$\vec{e} = (e_1, \cdots, e_n) = \left(\sum_{r=1}^{t} e_{1r}\vec{b}_r, \cdots, \sum_{r=1}^{t} e_{nr}\vec{b}_r\right) = \left(\sum_{r=1}^{t} e_{\eta r}\vec{b}_r\right)_\eta, \quad e_{\eta r} \in \mathbb{F}_q$$

- Thus,

$$s_i \in \ < \vec{v}_1\vec{b}_1, \vec{v}_1\vec{b}_2, \cdots, \vec{v}_d\vec{b}_t >_{\mathbb{F}_q}$$

Decryption

- Compute the syndrome

$$\vec{s} = \boldsymbol{H}\vec{y}^T = \boldsymbol{H}\boldsymbol{G}_{pub}^T\vec{m}^T + \boldsymbol{H}\vec{e}^T = \boldsymbol{H}\vec{e}^T$$

- Remember that

$$\boldsymbol{H} = (h_{ij})_{i,j} = \left(\sum_{\ell=1}^{d} h_{ij\ell}\vec{v}_\ell\right)_{i,j}, \quad h_{ij\ell} \in \mathbb{F}_q$$

- And

$$\vec{e} = (e_1, \cdots, e_n) = \left(\sum_{r=1}^{t} e_{1r}\vec{b}_r, \cdots, \sum_{r=1}^{t} e_{nr}\vec{b}_r\right) = \left(\sum_{r=1}^{t} e_{\eta r}\vec{b}_r\right)_\eta, \quad e_{\eta r} \in \mathbb{F}_q$$

- Thus,

$$s_i \in \; < \vec{v}_1\vec{b}_1, \vec{v}_1\vec{b}_2, \cdots, \vec{v}_d\vec{b}_t >_{\mathbb{F}_q}$$

Decryption

- We have $s_i \in < \vec{v}_1\vec{b}_1, \vec{v}_1\vec{b}_2, \cdots, \vec{v}_d\vec{b}_t >_{\mathbb{F}_q}$
- That is to say

$$S =< s_1, \cdots s_{n-k} >_{\mathbb{F}_q} \quad \subseteq \quad < \vec{v}_1\vec{b}_1, \vec{v}_1\vec{b}_2, \cdots, \vec{v}_d\vec{b}_t >_{\mathbb{F}_q}$$

- For $d, t, dt \lll n-k$, w.h.p we have $\dim S = dt$
- i.e,

$$S =< s_1, \cdots s_{n-k} >_{\mathbb{F}_q} \quad = \quad < \vec{v}_1\vec{b}_1, \vec{v}_1\vec{b}_2, \cdots, \vec{v}_d\vec{b}_t >_{\mathbb{F}_q}$$

- For $\ell = 1, \cdots, d$ compute $S_\ell = \vec{v}_\ell^{\,-1} S$ and

$$\bigcap_{\ell=1}^{d} S_\ell \overset{\text{w.h.p}}{=} < \vec{b}_1, \cdots, \vec{b}_t >_{\mathbb{F}_q} = \mathscr{E}$$

Decryption

- We have $s_i \in <\vec{v}_1\vec{b}_1, \vec{v}_1\vec{b}_2, \cdots, \vec{v}_d\vec{b}_t>_{\mathbb{F}_q}$
- That is to say

$$S =< s_1, \cdots s_{n-k} >_{\mathbb{F}_q} \quad \subseteq \quad < \vec{v}_1\vec{b}_1, \vec{v}_1\vec{b}_2, \cdots, \vec{v}_d\vec{b}_t >_{\mathbb{F}_q}$$

- For $d, t, dt \lll n-k$, w.h.p we have $\dim S = dt$
- i.e,

$$S =< s_1, \cdots s_{n-k} >_{\mathbb{F}_q} \quad = \quad < \vec{v}_1\vec{b}_1, \vec{v}_1\vec{b}_2, \cdots, \vec{v}_d\vec{b}_t >_{\mathbb{F}_q}$$

- For $\ell = 1, \cdots, d$ compute $S_\ell = \vec{v}_\ell^{-1} S$ and

$$\bigcap_{\ell=1}^{d} S_\ell \overset{\text{w.h.p}}{=} < \vec{b}_1, \cdots, \vec{b}_t >_{\mathbb{F}_q} = \mathscr{E}$$

Decryption

- We have $s_i \in < \vec{v}_1\vec{b}_1, \vec{v}_1\vec{b}_2, \cdots, \vec{v}_d\vec{b}_t >_{\mathbb{F}_q}$
- That is to say

$$S =< s_1, \cdots s_{n-k} >_{\mathbb{F}_q} \quad \subseteq \quad < \vec{v}_1\vec{b}_1, \vec{v}_1\vec{b}_2, \cdots, \vec{v}_d\vec{b}_t >_{\mathbb{F}_q}$$

- For $d, t, dt \lll n-k$, w.h.p we have $\dim S = dt$
- i.e,

$$S =< s_1, \cdots s_{n-k} >_{\mathbb{F}_q} \quad = \quad < \vec{v}_1\vec{b}_1, \vec{v}_1\vec{b}_2, \cdots, \vec{v}_d\vec{b}_t >_{\mathbb{F}_q}$$

- For $\ell = 1, \cdots, d$ compute $S_\ell = \vec{v}_\ell^{-1} S$ and

$$\bigcap_{\ell=1}^{d} S_\ell \overset{\text{w.h.p}}{=} < \vec{b}_1, \cdots, \vec{b}_t >_{\mathbb{F}_q} = \mathscr{E}$$

Decryption

- We have $s_i \in < \vec{v}_1\vec{b}_1, \vec{v}_1\vec{b}_2, \cdots, \vec{v}_d\vec{b}_t >_{\mathbb{F}_q}$
- That is to say

$$S =< s_1, \cdots s_{n-k} >_{\mathbb{F}_q} \quad \subseteq \quad < \vec{v}_1\vec{b}_1, \vec{v}_1\vec{b}_2, \cdots, \vec{v}_d\vec{b}_t >_{\mathbb{F}_q}$$

- For $d, t, dt \lll n-k$, w.h.p we have $\dim S = dt$
- i.e,

$$S =< s_1, \cdots s_{n-k} >_{\mathbb{F}_q} \quad = \quad < \vec{v}_1\vec{b}_1, \vec{v}_1\vec{b}_2, \cdots, \vec{v}_d\vec{b}_t >_{\mathbb{F}_q}$$

- For $\ell = 1, \cdots, d$ compute $S_\ell = \vec{v}_\ell^{-1} S$ and

$$\bigcap_{\ell=1}^{d} S_\ell \overset{\text{w.h.p}}{=} < \vec{b}_1, \cdots, \vec{b}_t >_{\mathbb{F}_q} = \mathscr{E}$$

Security assumptions

- Indistinguishability of LRPC codes : **Gaborit-Murat-Ruatta-Zémor ’13**
- Hardness of decoding a "random" rank-metric code

Rank-Based Cryptography in the NIST competition

csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions#

NIST

Search CSRC

CSRC MENU

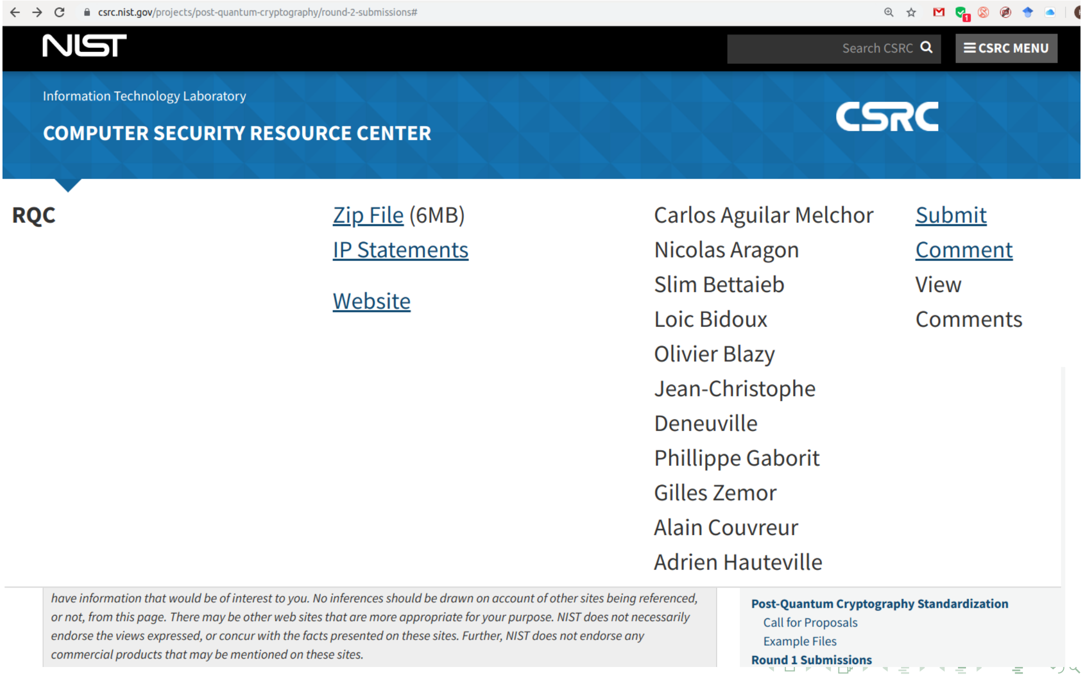
Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

CSRC

ROLLO *(merger of LAKE, LOCKER and Ouroboros-R)*	Zip File (8MB) IP Statements Website	Nicolas Aragon Olivier Blazy Jean-Christophe Deneuville Philippe Gaborit Adrien Hauteville Olivier Ruatta Jean-Pierre Tillich Gilles Zemor Carlos Aguilar Melchor Slim Bettaieb Loic Bidoux Magali Bardet Ayoub Otmani	Submit Comment View Comments

Rank-Based Cryptography in the NIST competition



Rank-Based Cryptography in the NIST competition

Annual International Conference on the Theory and Applications of Cryptographic Techniques

↳ EUROCRYPT 2020: **Advances in Cryptology – EUROCRYPT 2020** pp 64–93 | Cite as

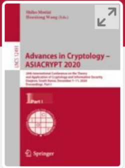
Home › Advances in Cryptology – EUROCRYPT 2020 › Conference paper

An Algebraic Attack on Rank Metric Code-Based Cryptosystems

Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, Vincent Neiger ✉, Olivier Ruatta & Jean-Pierre Tillich ✉

Conference paper | First Online: 01 May 2020

Rank-Based Cryptography in the NIST competition



International Conference on the Theory and Application of Cryptology and Information Security

↳ ASIACRYPT 2020: **Advances in Cryptology – ASIACRYPT 2020** pp 507–536 | Cite as

Home › Advances in Cryptology – ASIACRYPT 2020 › Conference paper

Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank Problems

Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich & Javier Verbel

Conference paper | First Online: 06 December 2020

Excerpt from the NIST Report on the Second Round of the PQCS

"... Despite the development of algebraic attacks, NIST believes rank-based cryptography should continue to be researched. The rank metric cryptosystems offer a nice alternative to traditional hamming metric codes with comparable bandwidth... " [2]

[2] Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, **July 2020**

Plan

1. Code-Based Cryptography
2. Rank-Based Cryptography
3. New Direction for Rank-Based Cryptography

Starting Point of Recent Algebraic Attacks

- $\mathscr{C}$ is a $(n,k)_{\mathbb{F}_{q^m}}$−code generated by $\boldsymbol{G}$
- $\vec{y} = \vec{c} + \vec{e} = \vec{m}\boldsymbol{G} + \vec{e}$ is the received word with $\mathtt{Rank}_{\mathbb{F}_q}(\vec{e}) = r$
- The problem is to find $\vec{e}$

Ourivski-Johansson's Modelling

- $\mathscr{C}_{ext}$ the $(n, k+1)$−code generated by

$$\mathscr{C}_{ext} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{y} \end{pmatrix} >_{\mathbb{F}_{q^m}} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{e} \end{pmatrix} >_{\mathbb{F}_{q^m}} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{m}\boldsymbol{G} + \vec{e} \end{pmatrix} >_{\mathbb{F}_{q^m}}$$

$$\Longrightarrow \exists \vec{c}' \in \mathscr{C}_{ext} \text{ s.t } \mathtt{Rank}_{\mathbb{F}_q}(\vec{c}') = r$$

- Each solution is of the form $\vec{c}' = \lambda\vec{e},\ \lambda \in \mathbb{F}_{q^m}^*$
- There is exactly one solution of the form $\vec{c}' = (1, c_2', \cdots, c_n')$

Starting Point of Recent Algebraic Attacks

- $\mathscr{C}$ is a $(n,k)_{\mathbb{F}_{q^m}}-$code generated by $\boldsymbol{G}$
- $\vec{y} = \vec{c} + \vec{e} = \vec{m}\boldsymbol{G} + \vec{e}$ is the received word with $\mathtt{Rank}_{\mathbb{F}_q}(\vec{e}) = r$
- The problem is to find $\vec{e}$

Ourivski-Johansson's Modelling

- $\mathscr{C}_{ext}$ the $(n, k+1)-$code generated by

$$\mathscr{C}_{ext} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{y} \end{pmatrix} >_{\mathbb{F}_{q^m}} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{e} \end{pmatrix} >_{\mathbb{F}_{q^m}} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{m}\boldsymbol{G} + \vec{e} \end{pmatrix} >_{\mathbb{F}_{q^m}}$$

$$\Longrightarrow \exists \vec{c}' \in \mathscr{C}_{ext} \text{ s.t } \mathtt{Rank}_{\mathbb{F}_q}(\vec{c}') = r$$

- Each solution is of the form $\vec{c}' = \lambda\vec{e}$, $\lambda \in \mathbb{F}_{q^m}^*$
- There is exactly one solution of the form $\vec{c}' = (1, c_2', \cdots, c_n')$

- $\mathscr{C}$ is a $(n,k)_{\mathbb{F}_{q^m}}-$code generated by $\boldsymbol{G}$
- $\vec{y} = \vec{c} + \vec{e} = \vec{m}\boldsymbol{G} + \vec{e}$ is the received word with $\mathtt{Rank}_{\mathbb{F}_q}(\vec{e}) = r$
- The problem is to find $\vec{e}$

Ourivski-Johansson's Modelling

- $\mathscr{C}_{ext}$ the $(n,k+1)-$code generated by

$$\mathscr{C}_{ext} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{y} \end{pmatrix} >_{\mathbb{F}_{q^m}} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{e} \end{pmatrix} >_{\mathbb{F}_{q^m}} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{m}\boldsymbol{G} + \vec{e} \end{pmatrix} >_{\mathbb{F}_{q^m}}$$

$$\Longrightarrow \exists \vec{c}' \in \mathscr{C}_{ext} \text{ s.t } \mathtt{Rank}_{\mathbb{F}_q}(\vec{c}') = r$$

- Each solution is of the form $\vec{c}' = \lambda\vec{e},\ \lambda \in \mathbb{F}_{q^m}^*$
- There is exactly one solution of the form $\vec{c}' = (1, c_2', \cdots, c_n')$

- $\mathscr{C}$ is a $(n,k)_{\mathbb{F}_{q^m}}-$code generated by $\boldsymbol{G}$
- $\vec{y} = \vec{c} + \vec{e} = \vec{m}\boldsymbol{G} + \vec{e}$ is the received word with $\texttt{Rank}_{\mathbb{F}_q}(\vec{e}) = r$
- The problem is to find $\vec{e}$

Ourivski-Johansson's Modelling

- $\mathscr{C}_{ext}$ the $(n, k+1)-$code generated by

$$\mathscr{C}_{ext} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{y} \end{pmatrix} >_{\mathbb{F}_{q^m}} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{e} \end{pmatrix} >_{\mathbb{F}_{q^m}} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{m}\boldsymbol{G} + \vec{e} \end{pmatrix} >_{\mathbb{F}_{q^m}}$$

$$\Longrightarrow \exists \vec{c}' \in \mathscr{C}_{ext} \text{ s.t } \texttt{Rank}_{\mathbb{F}_q}(\vec{c}') = r$$

- Each solution is of the form $\vec{c}' = \lambda\vec{e}$, $\lambda \in \mathbb{F}_{q^m}^*$
- There is exactly one solution of the form $\vec{c}' = (1, c_2', \cdots, c_n')$

Starting Point of Recent Algebraic Attacks

- $\mathscr{C}$ is a $(n,k)_{\mathbb{F}_{q^m}}$−code generated by $\boldsymbol{G}$
- $\vec{y} = \vec{c} + \vec{e} = \vec{m}\boldsymbol{G} + \vec{e}$ is the received word with $\texttt{Rank}_{\mathbb{F}_q}(\vec{e}) = r$
- The problem is to find $\vec{e}$

Ourivski-Johansson's Modelling

- $\mathscr{C}_{ext}$ the $(n, k+1)$−code generated by

$$\mathscr{C}_{ext} = <\begin{pmatrix} \boldsymbol{G} \\ \vec{y} \end{pmatrix}>_{\mathbb{F}_{q^m}} = <\begin{pmatrix} \boldsymbol{G} \\ \vec{e} \end{pmatrix}>_{\mathbb{F}_{q^m}} = <\begin{pmatrix} \boldsymbol{G} \\ \vec{m}\boldsymbol{G} + \vec{e} \end{pmatrix}>_{\mathbb{F}_{q^m}}$$

$$\Longrightarrow \exists \vec{c}' \in \mathscr{C}_{ext} \text{ s.t } \texttt{Rank}_{\mathbb{F}_q}(\vec{c}') = r$$

- Each solution is of the form $\vec{c}' = \lambda\vec{e}$, $\lambda \in \mathbb{F}_{q^m}^*$
- There is exactly one solution of the form $\vec{c}' = (1, c_2', \cdots, c_n')$

Starting Point of Recent Algebraic Attacks

- $\mathscr{C}$ is a $(n, k)_{\mathbb{F}_{q^m}}$−code generated by $\boldsymbol{G}$
- $\vec{y} = \vec{c} + \vec{e}$ is the received word with $\mathtt{Rank}_{\mathbb{F}_q}(\vec{e}) = r$
- The problem is to find $\vec{e}$

Ourivski-Johansson's Modelling

- $\mathscr{C}_{ext}$ the $(n, k+1)$−code generated by

$$\mathscr{C}_{ext} = < \begin{pmatrix} \boldsymbol{G} \\ \vec{y} \end{pmatrix} >_{\mathbb{F}_{q^m}} = < \begin{pmatrix} \boldsymbol{G} \\ \vec{e} \end{pmatrix} >_{\mathbb{F}_{q^m}} = < (\boldsymbol{I}_{k+1} \mid \boldsymbol{R}) >_{\mathbb{F}_{q^m}}$$

$$\implies \exists \vec{c}' \in \mathscr{C}_{ext} \text{ s.t } \mathtt{Rank}_{\mathbb{F}_q}(\vec{c}') = r$$

- Each solution is of the form $\vec{c}' = \lambda \vec{e}$, $\lambda \in \mathbb{F}_{q^m}^*$
- There is exactly one solution of the form $\vec{c}' = (1, c_2', \cdots, c_n')$

- $\mathscr{C}$ is a $(n,k)_s-$code generated by $\boldsymbol{G}$
- $\vec{y} = \vec{c} + \vec{e}$ is the received word with $\texttt{Rank}_R(\vec{e}) = r$
- The problem is to find $\vec{e}$

Ourivski-Johansson's Modelling

- $\mathscr{C}_{ext}$ the $(n,k+1)-$code generated by

$$\mathscr{C}_{ext} = < \begin{pmatrix} \boldsymbol{G} \\ \vec{y} \end{pmatrix} >_s = < \begin{pmatrix} \boldsymbol{G} \\ \vec{e} \end{pmatrix} >_s = < (\boldsymbol{I}_{k+1} \mid \boldsymbol{R}) >_s$$

$$\Longrightarrow \exists \vec{c}' \in \mathscr{C}_{ext} \text{ s.t } \texttt{Rank}_{\mathbb{F}_q}(\vec{c}') = r$$

- Each solution is of the form $\vec{c}' = \lambda \vec{e}$, $\lambda \in S^*$
- There is exactly one solution of the form $\vec{c}' = (1, c_2', \cdots, c_n')$??

Another Fact : zero divisors

- Let $R = \mathbb{Z}_6$ and $\boldsymbol{A} = \begin{pmatrix} 5 & 0 \\ 0 & 3 \end{pmatrix}$. $2\boldsymbol{A} = \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}$.
- We have

$$\mathtt{Rank}_R(\boldsymbol{A}) = 2, \text{ while } \mathtt{Rank}_R(2\boldsymbol{A}) = 1$$

Rank Decoding Problem over Finite Rings

- Hardness ? [a]
- Combinatorial algorithms ?
- Algebraic Algorithms ?

[a] Hervé Talé Kalachi, Hermann Tchatchiem Kamche. On the rank decoding problem over finite principal ideal rings. *Advances in Mathematics of Communications*

- Existence of structured rank metric codes over finite rings ?

Rank Metric Codes-Based Cryptography over Finite Rings

Another Fact : zero divisors

- Let $R = \mathbb{Z}_6$ and $\boldsymbol{A} = \begin{pmatrix} 5 & 0 \\ 0 & 3 \end{pmatrix}$. $2\boldsymbol{A} = \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}$.
- We have

$$\mathtt{Rank}_{R}(\boldsymbol{A}) = 2, \text{ while } \mathtt{Rank}_{R}(2\boldsymbol{A}) = 1$$

Rank Decoding Problem over Finite Rings

- Hardness ? [a]
- Combinatorial algorithms ?
- Algebraic Algorithms ?

[a] Hervé Talé Kalachi, Hermann Tchatchiem Kamche. On the rank decoding problem over finite principal ideal rings. *Advances in Mathematics of Communications*

- Existence of structured rank metric codes over finite rings ?

Another Fact : zero divisors

- Let $R = \mathbb{Z}_6$ and $\boldsymbol{A} = \begin{pmatrix} 5 & 0 \\ 0 & 3 \end{pmatrix}$. $2\boldsymbol{A} = \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}$.
- We have

$$\mathtt{Rank}_R(\boldsymbol{A}) = 2, \text{ while } \mathtt{Rank}_R(2\boldsymbol{A}) = 1$$

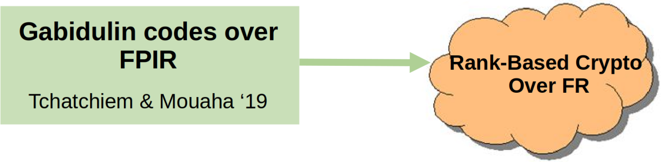
Rank Decoding Problem over Finite Rings

- Hardness ? [a]
- Combinatorial algorithms ?
- Algebraic Algorithms ?

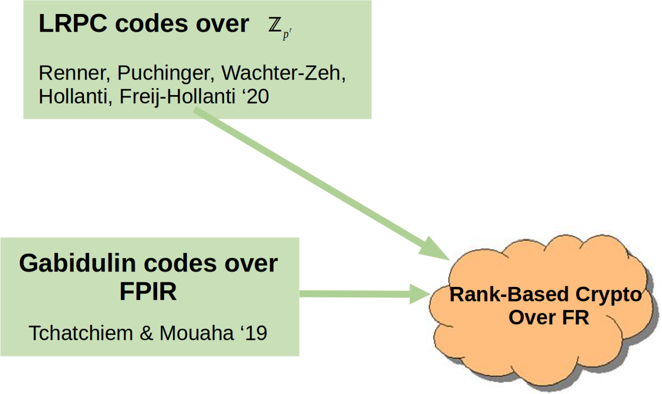
[a] Hervé Talé Kalachi, Hermann Tchatchiem Kamche. On the rank decoding problem over finite principal ideal rings. *Advances in Mathematics of Communications*

- Existence of structured rank metric codes over finite rings ?

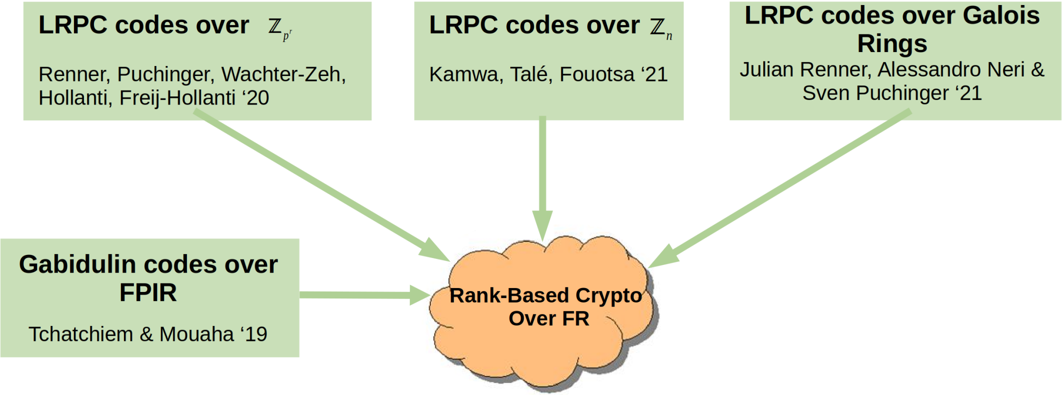
Some Progress for Rank Based Crypto over FR



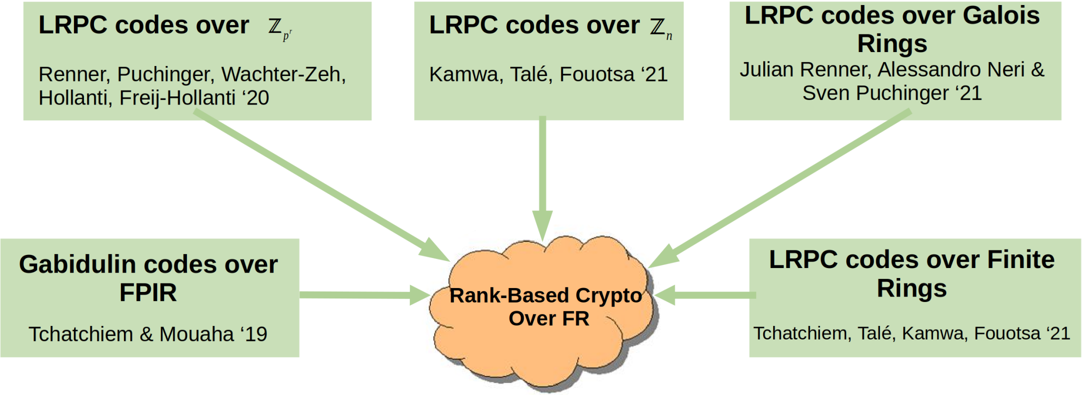
Some Progress for Rank Based Crypto over FR



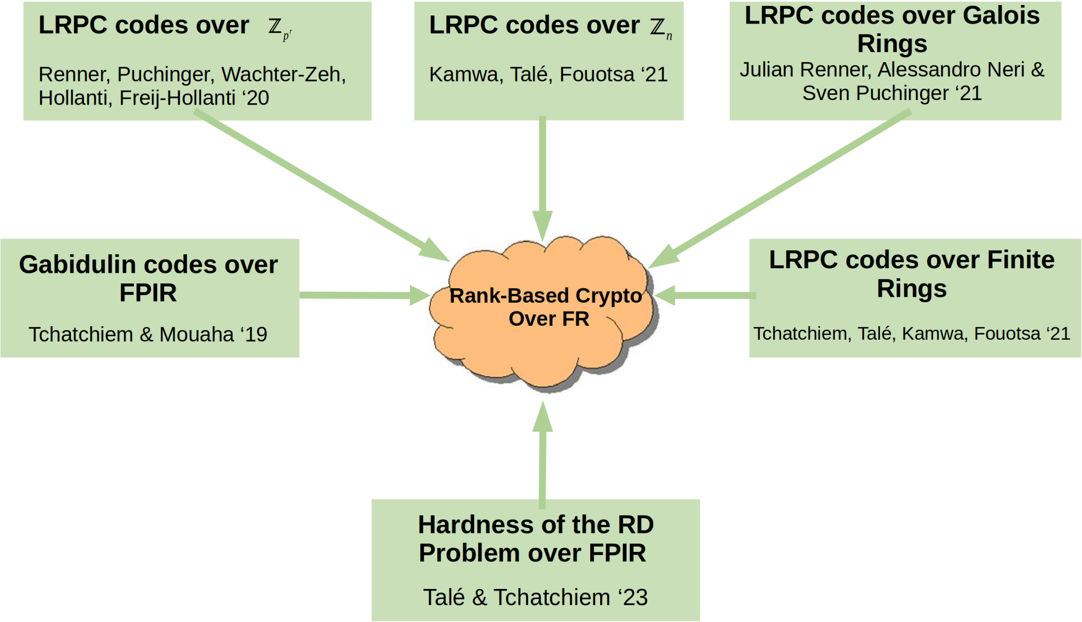
Some Progress for Rank Based Crypto over FR



Some Progress for Rank Based Crypto over FR

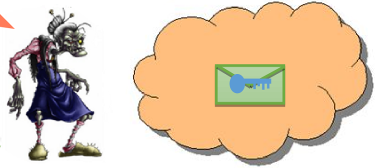


Some Progress for Rank Based Crypto over FR



Security and Parameters

Algebraic Attacks ?



Combinatorial Attacks over Finite Rings

Talé & Tchatchiem ‘23