Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

## Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani<sup>1</sup> Hervé Talé Kalachi <sup>1,2</sup> Sélestin Ndjeya <sup>2</sup>

University of Rouen, France.

University of Yaounde 1, Cameroon.

February 3, 2017

Image: A matrix

< E.

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Linear code

Linear code = vector space over a finite field

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

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

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

**③** Decoding a word  $\vec{w} \in \mathbb{F}_a^n = \text{Closest Vector Problem (CVP)}$ .

э

• • • • • • • • • • • •

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work



▲□▶ ▲圖▶ ▲国▶ ▲国▶

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work



▲□▶ ▲圖▶ ▲国▶ ▲国▶

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work



• Decoding is NP-Hard for a random linear code (Berlekamp-McEliece-Van Tilborg '78)

イロン イロン イヨン イヨン

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

## McEliece Public-Key Encryption Scheme ('78)

• Use code in Hamming metric

Based on linear codes equipped with an efficient decoding algorithm

- Public key = random basis
- Private key = decoding algorithm
- McEliece proposed binary Goppa codes
  - No efficient attack on the system up to now
  - Problem of huge key size

### McEliece Variants

Use another family of code

Output State of Use another metric instead of Hamming metric

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

## McEliece Public-Key Encryption Scheme ('78)

• Use code in Hamming metric

Based on linear codes equipped with an efficient decoding algorithm

- Public key = random basis
- Private key = decoding algorithm
- McEliece proposed binary Goppa codes
  - No efficient attack on the system up to now
  - Problem of huge key size

### McEliece Variants

Use another family of code

<sup>2</sup> Use another metric instead of Hamming metric

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

#### Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

## GPT cryptosystem '91

Rank metric with Gabidulin codes

### But many attacks

- Gibson's attacks '95, '96
- Overbeck's attack '05

#### Some GPT Variants

- Gabidulin '08
- Rashwan-Gabidulin-Honary, '10

#### Purpose of this presentation

Polynomial attack against above reparations

3

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

#### Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

## GPT cryptosystem '91

Rank metric with Gabidulin codes

### But many attacks

- Gibson's attacks '95, '96
- Overbeck's attack '05

### Some GPT Variants

- Gabidulin '08
- Rashwan-Gabidulin-Honary, '10

### Purpose of this presentation

Polynomial attack against above reparations

イロト イヨト イヨト イヨ

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

#### Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

 ${\it Cryptanalysis}$ 

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

## GPT cryptosystem '91

Rank metric with Gabidulin codes

### But many attacks

- Gibson's attacks '95, '96
- Overbeck's attack '05

### Some GPT Variants

- Gabidulin '08
- Rashwan-Gabidulin-Honary, '10

### Purpose of this presentation

Polynomial attack against above reparations

э

## Outline

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis Gabidulin.

Rashwan and Honary Variant

Conclusion and Related Work

### Preliminaries

2 General GPT Cryptosystem

3 Overbeck's Attack

Gabidulin's General Reparation

5 Cryptanalysis

6 Gabidulin, Rashwan and Honary Variant



## Plan

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Preliminaries

General GPT Cryptosystem

3 Overbeck's Attack

Gabidulin's General Reparation

5 Cryptanalysis

🗿 Gabidulin, Rashwan and Honary Variant

### Conclusion and Related Work

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya (UniversiImproved Cryptanalysis of Rank Metric Schemes Based on Gabie

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Definition 1

• *n*, *m* and *q* are integers with  $n \leq m$ 

• 
$$\mathbb{F}_{q^m} = \mathbb{F}_q < w >$$

• 
$$\mathscr{B} = \{b_1, b_2, ..., b_m\}$$
 a  $\mathbb{F}_q$ -basis of  $\mathbb{F}_{q^m}$ 

We define the one to one application  $\phi$  by:

$$\phi: \qquad \mathbb{F}_{q^m} \longrightarrow \mathcal{M}_{m \times 1}(\mathbb{F}_q)$$
$$x = \sum_{i=1}^m x_i b_i \longmapsto \phi(x) \stackrel{\mathsf{def}}{=} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ x_m \end{pmatrix}$$

イロト イヨト イヨト イヨ

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Avoub Otmani. Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin. Rashwan and Honary Variant

Conclusion and Related Work

### Extension Of $\phi$

• For a vector 
$$\vec{x} = (x_1, x_2, ..., x_n) \in \mathbb{F}_{q^m}^n$$

$$\phi(\vec{x}) \stackrel{\text{def}}{=} (\phi(x_1), \phi(x_2), ..., \phi(x_n)) \in \mathcal{M}_{m \times n}(\mathbb{F}_q)$$

• And for a matrix  $\boldsymbol{M} = (m_{ii}) \in \mathcal{M}_{k \times \ell}(\mathbb{F}_{q^m})$ 

 $\phi(\boldsymbol{M}) \stackrel{\text{def}}{=} (\phi(m_{ij})) \in \mathcal{M}_{km \times \ell}(\mathbb{F}_q)$ 

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya (UniversiImproved Cryptanalysis of Rank Metric Schemes Based on Gabie

æ February 3, 2017 11 / 43

3

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Definition 2 (Rank Weight)

• 
$$\vec{x} = (x_1, x_2, ..., x_n) \in \mathbb{F}_{q^m}^n$$

The rank weight of  $\vec{x}$  is defined by

$$\left\|\vec{x}\right\|_{q} \stackrel{\text{def}}{=} \operatorname{Rank}\left(\phi\left(\vec{x}\right)\right)$$

#### Example

• So.

Let  $\mathbb{K} = \mathbb{F}_{2^5} = \mathbb{F}_2 < w >$ ,  $\vec{x_1} = (w, w, w, w, w)$ ,  $\vec{x_2} = (1, w, w^2, 1 + w^3, w^4)$  and  $\mathscr{B} = \{1, w, w^2, w^3, w^4\}.$ 

.

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Definition 2 (Rank Weight)

• 
$$\vec{x} = (x_1, x_2, ..., x_n) \in \mathbb{F}_{q^m}^n$$

The rank weight of  $\vec{x}$  is defined by

$$\left\|\vec{x}\right\|_{q} \stackrel{\text{def}}{=} \operatorname{Rank}\left(\phi\left(\vec{x}\right)\right)$$

### Example

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Definition 2 (Rank Weight)

• 
$$\vec{x} = (x_1, x_2, ..., x_n) \in \mathbb{F}_{q^m}^n$$

The rank weight of  $\vec{x}$  is defined by

$$\left\|\vec{x}\right\|_{q} \stackrel{\text{def}}{=} \operatorname{Rank}\left(\phi\left(\vec{x}\right)\right)$$

### Example

Let $\mathbb{K} = \mathbb{F}_{2^5} = \mathbb{F}_2 < v$	v >	$\vec{x}_1$	= (	w, I	<i>N</i> , W	$, w, w), \ \vec{x}_2 = (1, w)$	w, i	$v^2,$	1 +	$w^3$ ,	$w^4$ ) and
$\mathscr{B} = \{1, w, w^2, w^3, w^3\}$	<sup>4</sup> }.										
٠	/0	0	0	0	0)		/1	0	0	1	0)
	$\begin{pmatrix} 0\\1 \end{pmatrix}$	1	1	1	$\begin{pmatrix} 0\\1 \end{pmatrix}$		0	1	0	0	0
$\phi(ec{x_1}) =$	0	0	0	0	0	and $\phi(ec{x_2}) =$	0	0	1	0	0
	0	0	0	0	0		0	0	0	1	0
	(0	0	0	0	0/	(	0)	0	0	0	1/
• So,											
$\ ec{x_1}\ _q = 1,  \ ec{x_2}\ _q = 5$											

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Definition 2 (Rank Weight)

• 
$$\vec{x} = (x_1, x_2, ..., x_n) \in \mathbb{F}_{q^m}^n$$

The rank weight of  $\vec{x}$  is defined by

$$\left\|\vec{x}\right\|_{q} \stackrel{\text{def}}{=} \operatorname{Rank}\left(\phi\left(\vec{x}\right)\right)$$

#### Example

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Lemma 3

•  $\vec{x} \in \mathbb{F}_{q^m}^n$ 

•  $\boldsymbol{T} \in \operatorname{GL}_n(\mathbb{F}_q)$ 

 $\|\vec{x}\boldsymbol{T}\|_q = \|\vec{x}\|_q$ 

イロト イヨト イヨト イヨ

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Definition 4

For  $\boldsymbol{M} \in \mathcal{M}_{k \times n}(\mathbb{F}_{q^m})$ , the rank of  $\boldsymbol{M}$  over  $\mathbb{F}_q$  will denotes:

 $\operatorname{Rank}_{\mathbb{F}_{q}}(\boldsymbol{M}) \stackrel{\operatorname{def}}{=} \operatorname{Rank}(\phi(\boldsymbol{M}))$ 

э

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Definition 5 (Gabidulin codes)

• 
$$\vec{g} \in \mathbb{F}_{q^m}^n$$
 with  $\|\vec{g}\|_q = n$ 

The (n, k)-Gabidulin code  $\mathscr{G}_k(\vec{g})$  is the code generated by:



Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Avoub Otmani. Hervé Talé Kalachi , Sélestin Ndjeya

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin. Rashwan and Honary Variant

Conclusion and Related Work

### **Proposition 1**

**1** The correction capability of a Gabidulin code  $\mathscr{G}_k(\vec{g})$  is  $|\frac{n-k}{2}|$ 

2  $\mathscr{G}_k(\vec{g})^{\perp}$  is also a Gabidulin code.

э

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Proposition 2

• Let  $\boldsymbol{G} \in \mathcal{M}_{k \times n}(\mathbb{F}_{q^m})$ , a generator matrix of  $\mathscr{G}_k(\vec{g})$ .

• 
$$\boldsymbol{T} \in \operatorname{GL}_n(\mathbb{F}_q)$$

Then **GT** is a generator matrix of  $\mathscr{G}_k(\vec{g} \mathbf{T})$ .

### Proof.

For the proof, remark that

$$(\vec{g} \boldsymbol{T})^{q^{i}} = \vec{g}^{q^{i}} \boldsymbol{T}$$
 since  $\boldsymbol{T}^{q^{i}} = \boldsymbol{T}$ 

for any integer *i*.

æ

3

## Plan

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

#### Preliminaries

### 2 General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

5 Cryptanalysis

Gabidulin, Rashwan and Honary Variant

### 7 Conclusion and Related Work

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya (UniversiImproved Cryptanalysis of Rank Metric Schemes Based on Gabie

э

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Key generation.

- k,  $\ell$ , n and m are some integers such that  $k < n \leqslant m$  and  $\ell \ll n$ .
- $oldsymbol{G} \in \mathcal{M}_{k imes n}(\mathbb{F}_{q^m})$  is a generator matrix of  $\mathscr{G}_k\left(ec{g}
  ight)$
- Pick at random  $\boldsymbol{S} \in \mathrm{GL}_k(\mathbb{F}_{q^m}).$
- Pick a random matrix  $oldsymbol{X} \in \mathcal{M}_{k imes \ell}\left(\mathbb{F}_{q^m}
  ight)$
- Let  $P \in GL_{n+\ell}(\mathbb{F}_q)$  be a random non-singular matrix
- Compute

$$\boldsymbol{S}_{pub} \stackrel{\text{def}}{=} \boldsymbol{S}(\boldsymbol{X} \mid \boldsymbol{G})\boldsymbol{P} \tag{1}$$

The public key is  $(\boldsymbol{G}_{pub}, t)$  where  $t \stackrel{\text{def}}{=} \lfloor \frac{n-k}{2} \rfloor$ 

#### Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### **Encryption.**

To encrypt a message  $\vec{m} \in \mathbb{F}_{q^m}^k$ ,

- Generate  $\vec{e} \in \mathbb{F}_{q^m}^n$  such that  $\|\vec{e}\|_q \leqslant t$ .
- One ciphertext is the vector

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

Decryption.	
• Compute $\vec{z} = \vec{c} P^{-1}$	$ec{z} = ec{m} oldsymbol{S} \left( oldsymbol{X} \mid oldsymbol{G}  ight) + ec{e} oldsymbol{P}^{-1}$
• Let $\vec{z}'$ be the last <i>n</i> components of $\vec{z}$	$ec{z}'=ec{m}oldsymbol{S}oldsymbol{G}+ec{e}'$
• Compute $\vec{y} = Dec_{.G}(\vec{z}')$	$\vec{y} = \vec{m} \boldsymbol{S}$ since $\ \vec{e}'\ _q \leqslant \ \vec{e}\ _q \leqslant t$
• Return $\vec{m}' = \vec{y} S^{-1}$	$\vec{m}' = \vec{m}$

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

m	k	WF general decoding	
48	10	2 <sup>134</sup>	
48	16	2 <sup>124</sup>	
48	24	2 <sup>198</sup>	

#### Structural attack

Parameters

- Overbeck's attack '05 '08
- Polynomial:  $\mathcal{O}((n+\ell)^3)$

・ロト ・回ト ・ヨト

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

m	k	WF general decoding	
40	10	0134	
48	10	2154	
48	16	2 <sup>124</sup>	
48	24	2 <sup>198</sup>	

### Structural attack

Parameters

- Overbeck's attack '05 '08
- Polynomial:  $\mathcal{O}((n+\ell)^3)$

3

・ロト ・日下・ ・ ヨト・

## Plan

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

#### Preliminaries

General GPT Cryptosystem

### 3 Overbeck's Attack

Gabidulin's General Reparation

5 Cryptanalysis

🗿 Gabidulin, Rashwan and Honary Variant

### 7 Conclusion and Related Work

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya (UniversiImproved Cryptanalysis of Rank Metric Schemes Based on Gabie

February 3, 2017 22 / 43

æ

э

## Overbeck's attack - Preliminaries

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Definition 6 (Distinguisher)

• f is an integer such that  $f \leq n - k$ 

We define the application  $\Lambda_f$  by:

$$\begin{array}{cccc} \Lambda_{f} : & \mathcal{M}_{\ell \times n} \left( \mathbb{F}_{q^{m}} \right) & \longrightarrow & \mathcal{M}_{\left( (f+1)\ell \right) \times n} \left( \mathbb{F}_{q^{m}} \right) \\ & \mathbf{M} & & & \\ & \mathbf{M} & & & \\ & \mathbf{M}^{\left( 0 \right)} \stackrel{\text{def}}{=} \begin{pmatrix} \mathbf{M}^{\left[ 0 \right]} \\ \mathbf{M}^{\left[ 1 \right]} \\ \vdots \\ \vdots \\ \mathbf{M}^{\left[ f \right]} \end{pmatrix} = \begin{pmatrix} \mathbf{M}^{q^{0}} \\ \mathbf{M}^{q^{1}} \\ \vdots \\ \vdots \\ \mathbf{M}^{q^{f}} \end{pmatrix} \end{array}$$

## Remark 1

• for 
$$m{G} \in \mathcal{M}_{k imes n}(\mathbb{F}_{q^m})$$
 and  $m{P} \in \mathcal{M}_{n imes n}(\mathbb{F}_q)$ 

 $\Lambda_f(\boldsymbol{GP}) = \Lambda_f(\boldsymbol{G})\boldsymbol{P}$ 

• If  $\boldsymbol{S} \in \mathcal{M}_{k \times k}(\mathbb{F}_{q^m})$  is a non singular matrix,

$$< \Lambda_f(\boldsymbol{S}\boldsymbol{G}) > = < \Lambda_f(\boldsymbol{G}) >$$

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Avoub Otmani. Hervé Talé Kalachi, Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Gabidulin's General Reparation

Cryptanalysis

Gabidulin. Rashwan and Honary Variant

Conclusion and Related Work

### **Proposition 3**

- **G** is a generator matrix of  $\mathscr{G}_k(\vec{g})$
- $f \leq n-k-1$

$$<\Lambda_{f}(\boldsymbol{G})>=\mathscr{G}_{k+\boldsymbol{f}}\left(ec{g}
ight)$$

For a random  $\mathbf{M} \in \mathcal{M}_{k \times n}(\mathbb{F}_{q^m})$ , we have

æ

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### **Proposition 3**

- **G** is a generator matrix of  $\mathscr{G}_k(\vec{g})$
- $f \leq n-k-1$

$$<\Lambda_{f}(\boldsymbol{G})>=\mathscr{G}_{k+\boldsymbol{f}}\left(ec{g}
ight)$$

### Theorem 7

For a random  $\boldsymbol{M} \in \mathcal{M}_{k \times n}(\mathbb{F}_{q^m})$ , we have

 $Rank(\Lambda_f(\boldsymbol{M})) = min\{n, k(f+1)\}$ 

with a high probability.

æ

3

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Avoub Otmani. Hervé Talé Kalachi, Sélestin Ndjeya

Preliminaries

General GPT Cryptosystem

Gabidulin's General Reparation

Cryptanalysis

Gabidulin. Rashwan and Honary Variant

Conclusion and Related Work

### **Proposition 4**

• Let 
$$\boldsymbol{G}_{pub} = \boldsymbol{S}(\boldsymbol{X} \mid \boldsymbol{G}) \boldsymbol{P}$$

• f = n - k - 1

By some additional transformations on the rows of  $\Lambda_f(\mathbf{G}_{pub})$ , we can get:

$$m{G}_{m{
houb}}^{\prime}=egin{pmatrix}m{X}_1&m{G}_{n-1}\m{X}_2&m{0}\end{pmatrix}m{P}$$

Where  $\mathbf{G}_{n-1}$  is a generator matrix of  $\mathscr{G}_{n-1}(\vec{g})$ .

э

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Remark 2

$$\mathsf{Rank}\left(\mathsf{\Lambda}_{\mathsf{f}}(oldsymbol{G}_{\mathsf{pub}})
ight)=\mathsf{Rank}\left(oldsymbol{G}_{\mathsf{pub}}'
ight)=\mathsf{n}-1+\mathsf{Rank}\left(oldsymbol{X}_{2}
ight)$$

#### heorem 8

If Rank  $(\mathbf{X}_2) = \ell$  then,

$$\mathsf{dim} < \Lambda_f(\boldsymbol{G}_{pub}) >^\perp = 1$$

$$< \Lambda_f(\boldsymbol{G}_{pub}) >^{\perp} = \left\{ \left( 0 \mid lpha ec{h} 
ight) \left( \boldsymbol{P^{-1}} 
ight)^{\mathsf{T}} : lpha \in \mathbb{R} 
ight\}$$
 , such that  $\left\| ec{h} 
ight\|_q = n$  and  $\boldsymbol{G} ec{h}^{\mathsf{T}} = \boldsymbol{0}$ 

æ

3

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin. Rashwan and Honary Variant

Conclusion and Related Work

### Remark 2

$$\mathsf{Rank}\left(\mathsf{\Lambda}_{\mathsf{f}}(oldsymbol{G}_{\mathsf{pub}})
ight)=\mathsf{Rank}\left(oldsymbol{G}_{\mathsf{pub}}
ight)=\mathsf{n}-1+\mathsf{Rank}\left(oldsymbol{X}_{2}
ight)$$

Theorem 8  
If Rank 
$$(\mathbf{X}_2) = \ell$$
 then,  
 $\mathbf{dim} < \Lambda_f(\mathbf{G}_{pub}) >^{\perp} = 1$   
 $\mathbf{dim} < \Lambda_f(\mathbf{G}_{pub}) >^{\perp} = \left\{ \left( 0 \mid \alpha \vec{h} \right) \left( \mathbf{P}^{-1} \right)^T : \alpha \in \mathbb{F}_{q^m} \right\}$   
 $\vec{h} \in \mathbb{F}_{q^m}^n$  such that  $\left\| \vec{h} \right\|_q = n$  and  $\mathbf{G} \vec{h}^T = \mathbf{0}$ 

3

・ロト ・ 日 ・ ・ ヨ ・ ・

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Avoub Otmani. Hervé Talé Kalachi, Sélestin Ndjeya

Preliminaries

General GPT Cryptosystem

Gabidulin's General Reparation

Cryptanalysis

Gabidulin. Rashwan and Honary Variant

Conclusion and Related Work

### Summary

• f = n - k - 1

• Compute

$$< \Lambda_f(oldsymbol{G}_{pub}) >^\perp$$

• If

$$\dim < \Lambda_f(\boldsymbol{G}_{pub}) >^{\perp} = 1$$

• Choose  $\vec{h} \in < \Lambda_f(\boldsymbol{G}_{pub}) >^{\perp}$  with  $\vec{h} \neq \boldsymbol{0}$ 

• Find  $\mathbf{T} \in \operatorname{GL}_{n+\ell}(\mathbb{F}_q)$  with  $\vec{h} = (\mathbf{0} \mid \vec{h}')\mathbf{T}$ 

(

э

・ロン ・日ン ・ヨン・

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

#### Remark 3

The success of this attack is:

- Linked to the fact that the matrix  $P \in GL_{n+\ell}(\mathbb{F}_q)$  is defined on the based field  $\mathbb{F}_q$
- **2** Also based on the supposition that  $X_2$  is of full rank  $Rank(X_2) = \ell$

## **GPT** Reparations

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Reparation ideas linked to $\boldsymbol{X}$

- Loidreau '10 : Proposition of parameters for  $\boldsymbol{X}$  such that Rank  $(\Lambda_f(\boldsymbol{G}_{pub})) < n + \ell - 1$ .
- Rashwan-Gabidulin-Honary '10 : Smart approach of the GPT Cryptosystem. The authors propose a design of **X** such that  $Rank(\Lambda_f(\mathbf{G}_{pub})) < n + \ell - 1$  or such that  $Rank(\mathbf{X}_2) < \ell$

 $\rightarrow$  Attack of **[Horlemann-Trautmann, Marshall, Rosenthal]**: Extension of Overbeck's Attack for Gabidulin-based Cryptosystems, November 2015

## **GPT** Reparations

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Reparation ideas linked to X

- Loidreau '10 : Proposition of parameters for  $\boldsymbol{X}$  such that Rank  $(\Lambda_f(\boldsymbol{G}_{pub})) < n + \ell - 1$ .
- Rashwan-Gabidulin-Honary '10 : Smart approach of the GPT Cryptosystem. The authors propose a design of X such that  $Rank(\Lambda_f(G_{pub})) < n + \ell - 1$  or such that  $Rank(X_2) < \ell$

 $\rightarrow$  Attack of [Horlemann-Trautmann, Marshall, Rosenthal]: Extension of Overbeck's Attack for Gabidulin-based Cryptosystems, November 2015

• • • • • • • • • • • •

## **GPT** Reparations

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Avoub Otmani. Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin. Rashwan and Honary Variant

Conclusion and Related Work

#### Reparation ideas linked to **P**

These variants consist to select  $P \in GL_{n+\ell}(\mathbb{F}_{q^m})$ 

#### • Gabidulin '08

Rashwan-Gabidulin-Honary '10

э

## Plan

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

### 4 Gabidulin's General Reparation

**5** Cryptanalysis

Gabidulin, Rashwan and Honary Variant

### 7 Conclusion and Related Work

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya (UniversiImproved Cryptanalysis of Rank Metric Schemes Based on Gabie

February 3, 2017 31 / 43

## Gabidulin's Variant

### Key generation.

Choose  $P \in GL_{n+\ell}(\mathbb{F}_{q^m})$  such that

•  $\boldsymbol{Q}_{11} \in \mathcal{M}_{\ell \times \ell} \left( \mathbb{F}_{q^m} \right)$ 

•  $\boldsymbol{Q}_{21} \in \mathcal{M}_{n \times \ell} (\mathbb{F}_{q^m})$ 

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

Improved Cryptanalysis of Rank Metric Schemes Based

> on Gabidulin Codes

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis Gabidulin,

Rashwan and Honary Variant

Conclusion and Related Work

## $\operatorname{GL}_{n+\ell}(\mathbb{F}_{q^m})$ such that

$$\boldsymbol{P}^{-1} = \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix}$$

• 
$$oldsymbol{Q}_{12} \in \mathcal{M}_{\ell imes n}(\mathbb{F}_{q^m})$$
 so that  
 $\operatorname{Rank}_{\mathbb{F}_q}(oldsymbol{Q}_{12}) = s$ 

• • • • • • • • • • • •

• 
$$\boldsymbol{Q}_{22} \in \mathcal{M}_{n \times n}(\mathbb{F}_q)$$

Compute

with

$$oldsymbol{\mathcal{S}}_{pub} \stackrel{ ext{def}}{=} oldsymbol{\mathcal{S}}(oldsymbol{X} \mid oldsymbol{\mathcal{G}})oldsymbol{\mathcal{P}})$$

The public key is  $(m{G}_{ ext{pub}},t_{ ext{pub}})$  where  $t_{ ext{pub}} \stackrel{ ext{def}}{=} t-s$ 

(2)

(3)

## Plan

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

#### Preliminaries

General GPT Cryptosystem

3 Overbeck's Attack

Gabidulin's General Reparation

### 5 Cryptanalysis

Gabidulin, Rashwan and Honary Variant

### 7 Conclusion and Related Work

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya (UniversiImproved Cryptanalysis of Rank Metric Schemes Based on Gabie

February 3, 2017 33 / 43

Avoub Otmani. Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Gabidulin. Rashwan and Honary Variant

Conclusion and Related Work

### Lemma 9

There exist

- $\boldsymbol{P}_{11} \in \operatorname{GL}_{\ell+s}(\mathbb{F}_{q^m})$
- $\boldsymbol{P}_{21} \in \mathcal{M}_{(n-s) imes (\ell+s)}(\mathbb{F}_{q^m})$

- $P_{22} \in \operatorname{GL}_{n-s}(\mathbb{F}_q)$
- **L** and **R** belonging to  $GL_n(\mathbb{F}_q)$

Such that

$$\boldsymbol{P} = \begin{pmatrix} \boldsymbol{I}_{\ell} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{L} \end{pmatrix} \begin{pmatrix} \boldsymbol{P}_{11} & \boldsymbol{0} \\ \boldsymbol{P}_{21} & \boldsymbol{P}_{22} \end{pmatrix} \begin{pmatrix} \boldsymbol{I}_{\ell} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{R} \end{pmatrix}$$
(4)

#### Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

- General GPT Cryptosystem
- Overbeck's Attack

Gabidulin's General Reparation

#### Cryptanalysi

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Theorem 10

#### There exist

- $X^* \in \mathcal{M}_{k imes (\ell+s)}(\mathbb{F}_{q^m})$
- $\boldsymbol{P}^{*} \in \operatorname{GL}_{n+\ell}\left(\mathbb{F}_{q}
  ight)$
- $G^*$  that defines an (n s, k)-Gabidulin code  $\mathscr{G}_k(\vec{g}^*)$  such that

$$\boldsymbol{G}_{\mathrm{pub}} = \boldsymbol{S} \left( \boldsymbol{X}^* \mid \boldsymbol{G}^* \right) \boldsymbol{P}^*.$$
 (5)

Furthermore, the error correction capability of  $\mathscr{G}_k(\vec{g}^*)$  is

$$t^*=t-rac{1}{2}s>t-s=t_{
m pub}$$

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya (UniversiImproved Cryptanalysis of Rank Metric Schemes Based on Gabie

э

э

Image: A math the second se

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

#### Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Corollary 11

The system can be broken by applying Overbeck's attack on  $\boldsymbol{G}_{\mathrm{pub}}$  with

$$f=n-s-k-1$$

## Plan

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

#### Preliminaries

General GPT Cryptosystem

3 Overbeck's Attack

Gabidulin's General Reparation

5 Cryptanalysis

6 Gabidulin, Rashwan and Honary Variant

#### Conclusion and Related Work

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya (UniversiImproved Cryptanalysis of Rank Metric Schemes Based on Gabie

## Gabidulin, Rashwan and Honary Variant

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### Key generation

Choose  $\boldsymbol{P} \in \operatorname{\mathsf{GL}}_n(\mathbb{F}_{q^m})$  such that

$$\boldsymbol{P}^{-1} = (\boldsymbol{Q}_1 \mid \boldsymbol{Q}_2) \tag{6}$$

where

$$oldsymbol{Q}_{1}\in\mathcal{M}_{n imes a}\left(\mathbb{F}_{q^{m}}
ight)$$

• while 
$$oldsymbol{Q}_{2}\in\mathcal{M}_{n imes(n-a)}\left(\mathbb{F}_{q}
ight)$$

• 
$$a \stackrel{\text{def}}{=} t - t_{\text{pub}} \implies t_{\text{pub}} = t - a$$

## Cryptanalysis

Remark 4

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

# $(\mathbf{Q}_1 \mid \mathbf{Q}_2) \implies \begin{pmatrix} \mathbf{Q}_{11} & \mathbf{Q}_{12} \\ \mathbf{Q}_{21} & \mathbf{Q}_{22} \end{pmatrix} \implies \begin{pmatrix} \mathbf{Q}_{11} & \mathbf{Q}_{12} \\ \mathbf{Q}_{21} & \mathbf{Q}_{22} \end{pmatrix}$ with s = a

### Corollary 12

One can recover an alternative secret key by applying Overbeck's attack with

$$f=n-a-k-1$$

3

## **Experimental Results**

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin. Rashwan and Honary Variant

Conclusion and Related Work

т	k	t	$t_{ m pub}$	Time (second)
20	10	5	4	≤ 1
28	14	7	3	$\leqslant 1$
28	14	7	4	$\leqslant 1$
28	14	7	5	$\leqslant 1$
28	14	7	6	$\leqslant 1$
20	10	5	4	$\leqslant 1$

Table : Parameters where n = m and at least 80-bit security.

э

## Plan

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

#### Preliminaries

General GPT Cryptosystem

3 Overbeck's Attack

Gabidulin's General Reparation

5 Cryptanalysis

Gabidulin, Rashwan and Honary Variant



Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### **Overbeck's attack**: Principal threat of Gabidulin-based Schemes

) Taking  $oldsymbol{P}\in {
m GL}({\mathbb F}_{q^m})$  might protect against it

In practice,

$$oldsymbol{P}^{-1} = egin{pmatrix} oldsymbol{Q}_{11} & oldsymbol{Q}_{12} \ oldsymbol{Q}_{21} & oldsymbol{Q}_{22} \end{pmatrix}$$
 with  $oldsymbol{Q}_{22} \in \operatorname{GL}(\mathbb{F}_q)$  and  $\operatorname{Rank}_{\mathbb{F}_q}(oldsymbol{Q}_{12}) = oldsymbol{s}$ 

→ Our works give a polynomial attack

Image: A mathematical states and a mathem

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### **Overbeck's attack**: Principal threat of Gabidulin-based Schemes

**②** Taking  $\boldsymbol{P} \in \mathsf{GL}(\mathbb{F}_{q^m})$  might protect against it

In practice,

$$oldsymbol{P}^{-1} = egin{pmatrix} oldsymbol{Q}_{11} & oldsymbol{Q}_{12} \ oldsymbol{Q}_{21} & oldsymbol{Q}_{22} \end{pmatrix}$$
 with  $oldsymbol{Q}_{22} \in \operatorname{GL}(\mathbb{F}_q)$  and  $\operatorname{Rank}_{\mathbb{F}_q}(oldsymbol{Q}_{12}) = s$ 

→ Our works give a polynomial attack

Image: A math the second se

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

**Overbeck's attack**: Principal threat of Gabidulin-based Schemes

- **②** Taking  $\boldsymbol{P} \in \mathsf{GL}(\mathbb{F}_{q^m})$  might protect against it
- In practice,

$$oldsymbol{P}^{-1} = egin{pmatrix} oldsymbol{Q}_{11} & oldsymbol{Q}_{12} \ oldsymbol{Q}_{21} & oldsymbol{Q}_{22} \end{pmatrix}$$
 with  $oldsymbol{Q}_{22} \in \mathsf{GL}(\mathbb{F}_q)$  and  $ext{Rank}_{\mathbb{F}_q}\left(oldsymbol{Q}_{12}
ight) = s$ 

~ Our works give a polynomial attack

э

Image: A math a math

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

**Overbeck's attack**: Principal threat of Gabidulin-based Schemes

- **②** Taking  $\boldsymbol{P} \in \mathsf{GL}(\mathbb{F}_{q^m})$  might protect against it
- In practice,

$$oldsymbol{P}^{-1} = egin{pmatrix} oldsymbol{Q}_{11} & oldsymbol{Q}_{12} \ oldsymbol{Q}_{21} & oldsymbol{Q}_{22} \end{pmatrix}$$
 with  $oldsymbol{Q}_{22} \in \operatorname{GL}(\mathbb{F}_q)$  and  $\operatorname{Rank}_{\mathbb{F}_q}(oldsymbol{Q}_{12}) = s$ 

### ~ Our works give a polynomial attack

	Matrix	Code generated	Length	Correction capability
Secret	G	$\mathscr{G}_k\left(\vec{g}\right)$	п	t
Public	$oldsymbol{G}_{ ext{pub}}$	$(n+\ell,k)-\operatorname{code}$	$n + \ell$	t-s

Image: A mathematical states and a mathem

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

**Overbeck's attack**: Principal threat of Gabidulin-based Schemes

- **②** Taking  $\boldsymbol{P} \in \mathsf{GL}(\mathbb{F}_{q^m})$  might protect against it
- In practice,

\_

$$oldsymbol{P}^{-1} = egin{pmatrix} oldsymbol{Q}_{11} & oldsymbol{Q}_{12} \ oldsymbol{Q}_{21} & oldsymbol{Q}_{22} \end{pmatrix}$$
 with  $oldsymbol{Q}_{22} \in \operatorname{GL}(\mathbb{F}_q)$  and  $\operatorname{Rank}_{\mathbb{F}_q}(oldsymbol{Q}_{12}) = s$ 

### ~ Our works give a polynomial attack

	Matrix	Code generated	Length	Correction capability
Secret	G	$\mathscr{G}_{k}\left(ec{g} ight)$	п	t
Attack	G*	$\mathscr{G}_k\left(ec{g}^* ight)$	n — s	$t-rac{s}{2}$
Public	$oldsymbol{\mathcal{G}}_{ ext{pub}}$	$(n+\ell,k)-code$	$n + \ell$	t-s

< □ > < 同 >

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

**Overbeck's attack**: Principal threat of Gabidulin-based Schemes

- **②** Taking  $\boldsymbol{P} \in \mathsf{GL}(\mathbb{F}_{q^m})$  might protect against it
- In practice,

-

$$oldsymbol{P}^{-1} = egin{pmatrix} oldsymbol{Q}_{11} & oldsymbol{Q}_{12} \ oldsymbol{Q}_{21} & oldsymbol{Q}_{22} \end{pmatrix}$$
 with  $oldsymbol{Q}_{22} \in \operatorname{GL}(\mathbb{F}_q)$  and  $\operatorname{Rank}_{\mathbb{F}_q}(oldsymbol{Q}_{12}) = s$ 

### ~ Our works give a polynomial attack

	Matrix	Code generated	Length	Correction capability
Secret	G	$\mathscr{G}_k\left(ec{g} ight)$	п	t
Attack	<b>G</b> *	$\mathscr{G}_k\left(ec{g}^* ight)$	n — s	$t-rac{s}{2}$
Public	$oldsymbol{\mathcal{G}}_{ ext{pub}}$	$(n+\ell,k)-code$	$n + \ell$	t — s

< □ > < 同 >

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

**Overbeck's attack**: Principal threat of Gabidulin-based Schemes

- **②** Taking  $\boldsymbol{P} \in \mathsf{GL}(\mathbb{F}_{q^m})$  might protect against it
- In practice,

-

\_

-

$$oldsymbol{P}^{-1} = egin{pmatrix} oldsymbol{Q}_{11} & oldsymbol{Q}_{12} \ oldsymbol{Q}_{21} & oldsymbol{Q}_{22} \end{pmatrix}$$
 with  $oldsymbol{Q}_{22} \in \operatorname{GL}(\mathbb{F}_q)$  and  $\operatorname{Rank}_{\mathbb{F}_q}(oldsymbol{Q}_{12}) = s$ 

### ~ Our works give a polynomial attack

	Matrix	Code generated	Length	Correction capability
Secret	G	$\mathscr{G}_k\left(ec{g} ight)$	п	t
Attack	<b>G</b> *	$\mathscr{G}_k\left(ec{g}^* ight)$	n — s	$t-rac{s}{2}$
Public	$oldsymbol{\mathcal{G}}_{ ext{pub}}$	$(n+\ell,k)-code$	$n + \ell$	t – s

Image: A matrix

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

**Overbeck's attack**: Principal threat of Gabidulin-based Schemes

- **②** Taking  $\boldsymbol{P} \in \mathsf{GL}(\mathbb{F}_{q^m})$  might protect against it
- In practice,

$$oldsymbol{P}^{-1} = egin{pmatrix} oldsymbol{Q}_{11} & oldsymbol{Q}_{12} \ oldsymbol{Q}_{21} & oldsymbol{Q}_{22} \end{pmatrix}$$
 with  $oldsymbol{Q}_{22} \in \operatorname{GL}(\mathbb{F}_q)$  and  $\operatorname{Rank}_{\mathbb{F}_q}(oldsymbol{Q}_{12}) = s$ 

### ~ Our works give a polynomial attack

	Matrix	Code generated	Length	Correction capability
Secret	G	$\mathscr{G}_k\left(ec{g} ight)$	п	t
Attack	<b>G</b> *	$\mathscr{G}_k\left(ec{g}^* ight)$	n — s	$t-\frac{s}{2}$
Public	$oldsymbol{\mathcal{G}}_{ ext{pub}}$	$(n+\ell,k)-code$	$n + \ell$	t – s

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

**Overbeck's attack**: Principal threat of Gabidulin-based Schemes

- **②** Taking  $\boldsymbol{P} \in \mathsf{GL}(\mathbb{F}_{q^m})$  might protect against it
- In practice,

-

\_

-

$$oldsymbol{P}^{-1} = egin{pmatrix} oldsymbol{Q}_{11} & oldsymbol{Q}_{12} \ oldsymbol{Q}_{21} & oldsymbol{Q}_{22} \end{pmatrix}$$
 with  $oldsymbol{Q}_{22} \in \operatorname{GL}(\mathbb{F}_q)$  and  $\operatorname{Rank}_{\mathbb{F}_q}(oldsymbol{Q}_{12}) = s$ 

### ~ Our works give a polynomial attack

	Matrix	Code generated	Length	Correction capability
Secret	G	$\mathscr{G}_{k}\left(ec{g} ight)$	п	t
Attack	<b>G</b> *	$\mathscr{G}_k\left(ec{g}^* ight)$	n — s	$t-rac{s}{2}$
Public	$oldsymbol{\mathcal{G}}_{ ext{pub}}$	$(n+\ell,k)-code$	$n + \ell$	t – s

Image: A matrix

Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya

#### Preliminaries

General GPT Cryptosystem

Overbeck's Attack

Gabidulin's General Reparation

Cryptanalysis

Gabidulin, Rashwan and Honary Variant

Conclusion and Related Work

### New variant from **P. Loidreau** '16

•  $\mathscr{V} \subset \mathbb{F}_{q^m}$  a  $\mathbb{F}_q$ -vector space

• 
$$d = \dim_{\mathbb{F}_q} (\mathscr{V}) \geqslant 3$$

$$\mathbf{P}^{-1}\in\mathsf{GL}_{\textit{n}}(\mathscr{V})$$
 and  $oldsymbol{G}_{ ext{pub}}=oldsymbol{SGF}$ 

$$ightarrow t_{
m pub} = rac{n-k}{2d}$$

Ayoub Otmani, Hervé Talé Kalachi , Sélestin Ndjeya (UniversiImproved Cryptanalysis of Rank Metric Schemes Based on Gabie

æ

э