Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes

Ayoub Otmani[1] Hervé Talé Kalachi [1,2] Sélestin Ndjeya [2]

University of Rouen, France.

University of Yaounde 1, Cameroon.

February 3, 2017

Linear code

1. Linear code = vector space over a finite field

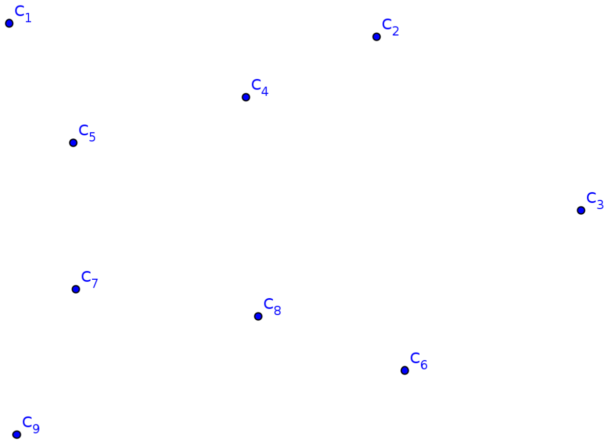
$$\mathscr{C} = \bigoplus_{i=1}^{k} \mathbb{F}_q \, \vec{v}_i$$

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

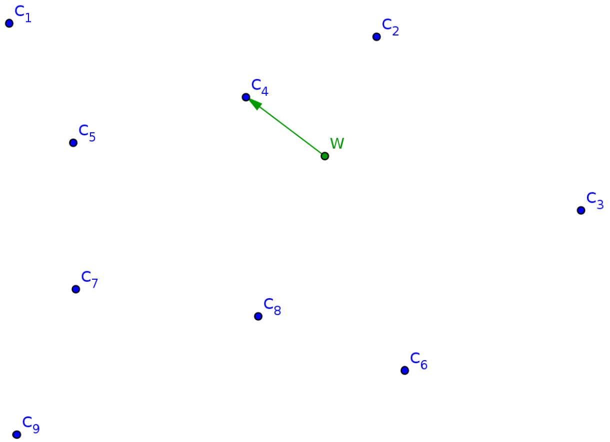
2. Any $k \times n$ matrix $\boldsymbol{G}$ whose rows form a basis of $\mathscr{C}$ is a generator matrix of $\mathscr{C}$.

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

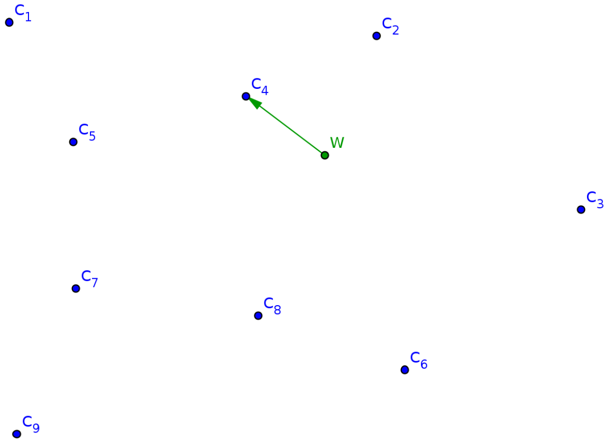
Introduction



Introduction



Introduction



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

McEliece Public-Key Encryption Scheme ('78)

1. Use code in Hamming metric
2. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm
3. McEliece proposed binary Goppa codes
   - No efficient attack on the system up to now
   - Problem of huge key size

McEliece Variants

1. Use another family of code
2. Use another metric instead of Hamming metric

Introduction

McEliece Public-Key Encryption Scheme ('78)

1. Use code in Hamming metric
2. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm
3. McEliece proposed binary Goppa codes
   - No efficient attack on the system up to now
   - Problem of huge key size

McEliece Variants

1. Use another family of code
2. Use another metric instead of Hamming metric

GPT 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**

Purpose of this presentation

Polynomial attack against above reparations

GPT 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**

Purpose of this presentation

Polynomial attack against above reparations

GPT 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**

Purpose of this presentation

Polynomial attack against above reparations

Outline

Plan

Definition 1

- n, m and q are integers with $n \leqslant m$
- $\mathbb{F}_{q^m} = \mathbb{F}_q < w >$
- $\mathscr{B} = \{b_1, b_2, \ldots, b_m\}$ a $\mathbb{F}_q-$basis of $\mathbb{F}_{q^m}$

We define the one to one application ϕ by:

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

Extension Of ϕ

- 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 $\boldsymbol{M} = (m_{ij}) \in \mathcal{M}_{k \times \ell}(\mathbb{F}_{q^m})$

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

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

$$\|\vec{x}\|_q \stackrel{\text{def}}{=} Rank\,(\phi\,(\vec{x}))$$

Example

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 $\mathscr{B} = \{1, w, w^2, w^3, w^4\}$.

- $$\phi(\vec{x}_1) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } \phi(\vec{x}_2) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- So,

$$\|\vec{x}_1\|_q = 1, \quad \|\vec{x}_2\|_q = 5$$

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

$$\|\vec{x}\|_q \stackrel{\text{def}}{=} Rank\,(\phi\,(\vec{x}))$$

Example

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 $\mathscr{B} = \{1, w, w^2, w^3, w^4\}$.

- $$\phi(\vec{x}_1) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \phi(\vec{x}_2) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- So,

$$\|\vec{x}_1\|_q = 1, \quad \|\vec{x}_2\|_q = 5$$

Definition 2 (Rank Weight)

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

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

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

Example

Let $\mathbb{K} = \mathbb{F}_{2^5} = \mathbb{F}_2 < w >$, $\vec{x}_1 = (w, w, w, w, w)$, $\vec{x}_2 = \left(1, w, w^2, 1 + w^3, w^4\right)$ and $\mathscr{B} = \{1, w, w^2, w^3, w^4\}$.

- $$\phi(\vec{x}_1) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } \phi(\vec{x}_2) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$
- So,

$$\|\vec{x}_1\|_q = 1, \quad \|\vec{x}_2\|_q = 5$$

Preliminaries

Definition 2 (Rank Weight)

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

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

$$\|\vec{x}\|_q \stackrel{\text{def}}{=} Rank\,(\phi\,(\vec{x}))$$

Example

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 $\mathscr{B} = \{1, w, w^2, w^3, w^4\}$.

- $$\phi(\vec{x}_1) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } \phi(\vec{x}_2) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$
- So,

$$\|\vec{x}_1\|_q = 1, \quad \|\vec{x}_2\|_q = 5$$

Lemma 3

- $\vec{x} \in \mathbb{F}_{q^m}^n$
- $\boldsymbol{T} \in \mathrm{GL}_n(\mathbb{F}_q)$

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

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:

$$\mathtt{Rank}_{\mathbb{F}_q}(\boldsymbol{M}) \stackrel{\text{def}}{=} Rank\,(\phi(\boldsymbol{M}))$$

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:

$$\boldsymbol{G} = \begin{pmatrix} g_1^{[0]} & g_2^{[0]} & \cdot & \cdot & \cdot & g_n^{[0]} \\ g_1^{[1]} & g_2^{[1]} & \cdot & \cdot & \cdot & g_n^{[1]} \\ \cdot & \cdot & \cdot & & & \cdot \\ \cdot & \cdot & & \cdot & & \cdot \\ \cdot & \cdot & & & \cdot & \cdot \\ g_1^{[k-1]} & g_2^{[k-1]} & \cdot & \cdot & \cdot & g_n^{[k-1]} \end{pmatrix} = \begin{pmatrix} g_1^{q^0} & g_2^{q^0} & \cdot & \cdot & \cdot & g_n^{q^0} \\ g_1^{q^1} & g_2^{q^1} & \cdot & \cdot & \cdot & g_n^{q^1} \\ \cdot & \cdot & \cdot & & & \cdot \\ \cdot & \cdot & & \cdot & & \cdot \\ \cdot & \cdot & & & \cdot & \cdot \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdot & \cdot & \cdot & g_n^{q^{k-1}} \end{pmatrix}$$

$\vec{g}$ is called generator vector of $\mathscr{G}_k(\vec{g})$.

Proposition 1

1. *The correction capability of a Gabidulin code* $\mathscr{G}_k(\vec{g})$ *is* $\lfloor \frac{n-k}{2} \rfloor$
2. $\mathscr{G}_k(\vec{g})^{\perp}$ *is also a Gabidulin code.*

Proposition 2

- *Let $\boldsymbol{G} \in \mathcal{M}_{k\times n}\left(\mathbb{F}_{q^m}\right)$, a generator matrix of $\mathscr{G}_k\left(\vec{g}\right)$.*
- $\boldsymbol{T} \in \mathrm{GL}_n(\mathbb{F}_q)$

Then $\boldsymbol{G}\boldsymbol{T}$ is a generator matrix of $\mathscr{G}_k\left(\vec{g}\boldsymbol{T}\right)$.

Proof.

For the proof, remark that

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

for any integer i. □ □

Plan

Key generation.

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

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

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

General GPT Cryptosystem

Encryption.

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

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

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

Decryption.

1. Compute $\vec{z} = \vec{c}\boldsymbol{P}^{-1}$ $\qquad \vec{z} = \vec{m}\boldsymbol{S}(\boldsymbol{X} \mid \boldsymbol{G}) + \vec{e}\boldsymbol{P}^{-1}$
2. Let $\vec{z}'$ be the last n components of $\vec{z}$ $\qquad \vec{z}' = \vec{m}\boldsymbol{S}\boldsymbol{G} + \vec{e}'$
3. Compute $\vec{y} = Dec_{.\boldsymbol{G}}(\vec{z}')$ $\qquad \vec{y} = \vec{m}\boldsymbol{S}$ since $\|\vec{e}'\|_q \leqslant \|\vec{e}\|_q \leqslant t$
4. Return $\vec{m}' = \vec{y}\boldsymbol{S}^{-1}$ $\qquad \vec{m}' = \vec{m}$

General GPT Cryptosystem

Parameters

m	k	WF general decoding
48	10	2^{134}
48	16	2^{124}
48	24	2^{198}

Structural attack

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

Parameters

m	k	WF general decoding
48	10	2^{134}
48	16	2^{124}
48	24	2^{198}

Structural attack

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

Plan

Definition 6 (Distinguisher)

- f is an integer such that $f \leqslant n-k$

We define the application Λ_f by:

$$\begin{array}{rccc} \Lambda_f : & \mathcal{M}_{\ell\times n}(\mathbb{F}_{q^m}) & \longrightarrow & \mathcal{M}_{((f+1)\ell)\times n}(\mathbb{F}_{q^m}) \\ & \boldsymbol{M} & \longmapsto & \Lambda_f(\boldsymbol{M}) \stackrel{\text{def}}{=} \begin{pmatrix} \boldsymbol{M}^{[0]} \\ \boldsymbol{M}^{[1]} \\ \vdots \\ \boldsymbol{M}^{[f]} \end{pmatrix} = \begin{pmatrix} \boldsymbol{M}^{q^0} \\ \boldsymbol{M}^{q^1} \\ \vdots \\ \boldsymbol{M}^{q^f} \end{pmatrix} \end{array}$$

Remark 1

- *for* $\boldsymbol{G} \in \mathcal{M}_{k\times n}(\mathbb{F}_{q^m})$ *and* $\boldsymbol{P} \in \mathcal{M}_{n\times n}(\mathbb{F}_q)$

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

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

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

Overbeck's attack

Proposition 3

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

$$< \Lambda_f(\boldsymbol{G}) >= \mathscr{G}_{k+f}(\vec{g})$$

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.

Overbeck's attack

Proposition 3

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

$$< \Lambda_f(\boldsymbol{G}) >= \mathscr{G}_{k+f}(\vec{g})$$

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.

Proposition 4

- Let $\boldsymbol{G}_{pub} = \boldsymbol{S}\left(\boldsymbol{X} \mid \boldsymbol{G}\right)\boldsymbol{P}$
- $f = n - k - 1$

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

$$\boldsymbol{G}'_{pub} = \begin{pmatrix} \boldsymbol{X}_1 & \boldsymbol{G}_{n-1} \\ \boldsymbol{X}_2 & \boldsymbol{0} \end{pmatrix}\boldsymbol{P}$$

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

Overbeck's attack

Remark 2

$$Rank\left(\Lambda_f(\boldsymbol{G}_{pub})\right) = Rank\left(\boldsymbol{G}'_{pub}\right) = n - 1 + Rank\left(\boldsymbol{X}_2\right)$$

Theorem 8

If $Rank\left(\boldsymbol{X}_2\right) = \ell$ then,

- $$\dim < \Lambda_f(\boldsymbol{G}_{pub}) >^{\perp} = 1$$
- $$< \Lambda_f(\boldsymbol{G}_{pub}) >^{\perp} = \left\{ \left(0 \mid \alpha \vec{h}\right) \left(\boldsymbol{P}^{-1}\right)^{T} \ : \ \alpha \in \mathbb{F}_{q^m} \right\}$$

$\vec{h} \in \mathbb{F}_{q^m}^{n}$ *such that* $\left\| \vec{h} \right\|_q = n$ *and* $\boldsymbol{G}\vec{h}^T = \boldsymbol{0}$

Overbeck's attack

Remark 2

$$Rank\left(\Lambda_f(\boldsymbol{G}_{pub})\right) = Rank\left(\boldsymbol{G}'_{pub}\right) = n - 1 + Rank\left(\boldsymbol{X}_2\right)$$

Theorem 8

If $Rank\left(\boldsymbol{X}_2\right) = \ell$ *then,*

- $$\dim < \Lambda_f(\boldsymbol{G}_{pub}) >^{\perp} = 1$$
- $$< \Lambda_f(\boldsymbol{G}_{pub}) >^{\perp} = \left\{ \left(0 \mid \alpha \vec{h}\right) \left(\boldsymbol{P}^{-1}\right)^{T} \ : \ \alpha \in \mathbb{F}_{q^m} \right\}$$

$\vec{h} \in \mathbb{F}_{q^m}^n$ *such that* $\left\|\vec{h}\right\|_q = n$ *and* $\boldsymbol{G}\vec{h}^T = \boldsymbol{0}$

Overbeck's attack

Summary

- $f = n - k - 1$
- Compute

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

- If

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

- Choose $\vec{h} \in < \Lambda_f(\boldsymbol{G}_{pub}) >^{\perp}$ with $\vec{h} \neq \mathbf{0}$
- Find $\boldsymbol{T} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$ with $\vec{h} = (\mathbf{0} \mid \vec{h}')\boldsymbol{T}$

Remark 3

The success of this attack is:

1. *Linked to the fact that the matrix* $\boldsymbol{P} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$ *is defined on the based field* $\mathbb{F}_q$
2. *Also based on the supposition that* $\boldsymbol{X}_2$ *is of full rank* $Rank\,(\boldsymbol{X}_2) = \ell$

GPT Reparations

Reparation ideas linked to $\boldsymbol{X}$

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

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

GPT Reparations

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 $\boldsymbol{X}$ such that $Rank\,(\Lambda_f(\boldsymbol{G}_{pub})) < n + \ell - 1$ or such that $Rank\,(\boldsymbol{X}_2) < \ell$

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

GPT Reparations

Reparation ideas linked to P

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

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

Plan

Gabidulin's Variant

Key generation.

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

$$\boldsymbol{P}^{-1} = \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix} \tag{2}$$

with

- $\boldsymbol{Q}_{11} \in \mathcal{M}_{\ell\times\ell}(\mathbb{F}_{q^m})$
- $\boldsymbol{Q}_{21} \in \mathcal{M}_{n\times\ell}(\mathbb{F}_{q^m})$
- $\boldsymbol{Q}_{12} \in \mathcal{M}_{\ell\times n}(\mathbb{F}_{q^m})$ so that $\mathtt{Rank}_{\mathbb{F}_q}(\boldsymbol{Q}_{12}) = s$
- $\boldsymbol{Q}_{22} \in \mathcal{M}_{n\times n}(\mathbb{F}_q)$

Compute

$$\boldsymbol{G}_{pub} \stackrel{\text{def}}{=} \boldsymbol{S}(\boldsymbol{X} \mid \boldsymbol{G})\boldsymbol{P} \tag{3}$$

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

Plan

Lemma 9

There exist

- $\boldsymbol{P}_{11} \in \mathrm{GL}_{\ell+s}(\mathbb{F}_{q^m})$
- $\boldsymbol{P}_{22} \in \mathrm{GL}_{n-s}(\mathbb{F}_q)$
- $\boldsymbol{P}_{21} \in \mathcal{M}_{(n-s)\times(\ell+s)}(\mathbb{F}_{q^m})$
- $\boldsymbol{L}$ *and* $\boldsymbol{R}$ *belonging to* $\mathrm{GL}_n(\mathbb{F}_q)$

Such that

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

Theorem 10

There exist

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

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

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

$$t^* = t - \frac{1}{2}s > t - s = t_{\mathrm{pub}}$$

Corollary 11

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

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

Plan

Gabidulin, Rashwan and Honary Variant

Key generation

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

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

where

- $\boldsymbol{Q}_1 \in \mathcal{M}_{n \times a}(\mathbb{F}_{q^m})$
- while $\boldsymbol{Q}_2 \in \mathcal{M}_{n \times (n-a)}(\mathbb{F}_q)$

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

Remark 4

$$(\boldsymbol{Q}_1 \mid \boldsymbol{Q}_2) \Longrightarrow \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix} \Longrightarrow \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix} \quad \textit{with} \quad s = a$$

Corollary 12

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

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

Experimental Results

m	k	t	t_{pub}	Time (second)
20	10	5	4	$\leqslant 1$
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.

Plan

Conclusion and Related Work

1. **Overbeck's attack**: Principal threat of Gabidulin-based Schemes
2. Taking $\boldsymbol{P} \in \mathrm{GL}(\mathbb{F}_{q^m})$ might protect against it
3. In practice,

$$\boldsymbol{P}^{-1} = \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix} \quad \text{with} \quad \boldsymbol{Q}_{22} \in \mathrm{GL}(\mathbb{F}_q) \quad \text{and} \quad \mathrm{Rank}_{\mathbb{F}_q}(\boldsymbol{Q}_{12}) = s$$

$\rightsquigarrow$ **Our works give a polynomial attack**

	Matrix	Code generated	Length	Correction capability
Secret	$\boldsymbol{G}$	$\mathscr{G}_k(\vec{g})$	n	t
Attack	$\boldsymbol{G}^*$	$\mathscr{G}_k(\vec{g}^*)$	$n - s$	$t - \frac{s}{2}$
Public	$\boldsymbol{G}_{\text{pub}}$	$(n+\ell, k)$−code	$n + \ell$	$t - s$

Conclusion and Related Work

1. **Overbeck's attack**: Principal threat of Gabidulin-based Schemes
2. Taking $\boldsymbol{P} \in \mathrm{GL}(\mathbb{F}_{q^m})$ might protect against it
3. In practice,

$$\boldsymbol{P}^{-1} = \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix} \quad \text{with} \quad \boldsymbol{Q}_{22} \in \mathrm{GL}(\mathbb{F}_q) \quad \text{and} \quad \mathtt{Rank}_{\mathbb{F}_q}(\boldsymbol{Q}_{12}) = s$$

$\rightsquigarrow$ **Our works give a polynomial attack**

	Matrix	Code generated	Length	Correction capability
Secret	$\boldsymbol{G}$	$\mathscr{G}_k(\vec{g})$	n	t
Attack	$\boldsymbol{G}^*$	$\mathscr{G}_k(\vec{g}^*)$	$n-s$	$t-\frac{s}{2}$
Public	$\boldsymbol{G}_{\mathrm{pub}}$	$(n+\ell,k)$−code	$n+\ell$	$t-s$

Conclusion and Related Work

1. **Overbeck's attack**: Principal threat of Gabidulin-based Schemes
2. Taking $\boldsymbol{P} \in \mathrm{GL}(\mathbb{F}_{q^m})$ might protect against it
3. In practice,

$$\boldsymbol{P}^{-1} = \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix} \text{ with } \boldsymbol{Q}_{22} \in \mathrm{GL}(\mathbb{F}_q) \text{ and } \mathtt{Rank}_{\mathbb{F}_q}(\boldsymbol{Q}_{12}) = s$$

$\rightsquigarrow$ **Our works give a polynomial attack**

	Matrix	Code generated	Length	Correction capability
Secret	$\boldsymbol{G}$	$\mathscr{G}_k(\vec{g})$	n	t
Attack	$\boldsymbol{G}^*$	$\mathscr{G}_k(\vec{g}^*)$	$n-s$	$t-\frac{s}{2}$
Public	$\boldsymbol{G}_{\mathrm{pub}}$	$(n+\ell, k)$−code	$n+\ell$	$t-s$

Conclusion and Related Work

1. **Overbeck's attack**: Principal threat of Gabidulin-based Schemes
2. Taking $\boldsymbol{P} \in \mathrm{GL}(\mathbb{F}_{q^m})$ might protect against it
3. In practice,

$$\boldsymbol{P}^{-1} = \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix} \quad \text{with} \quad \boldsymbol{Q}_{22} \in \mathrm{GL}(\mathbb{F}_q) \quad \text{and} \quad \mathtt{Rank}_{\mathbb{F}_q}(\boldsymbol{Q}_{12}) = s$$

$\rightsquigarrow$ **Our works give a polynomial attack**

	Matrix	Code generated	Length	Correction capability
Secret	$\boldsymbol{G}$	$\mathscr{G}_k(\vec{g})$	n	t
Attack	$\boldsymbol{G}^*$	$\mathscr{G}_k(\vec{g}^*)$	$n-s$	$t-\frac{s}{2}$
Public	$\boldsymbol{G}_{\mathrm{pub}}$	$(n+\ell,k)$−code	$n+\ell$	$t-s$

Conclusion and Related Work

1. **Overbeck's attack**: Principal threat of Gabidulin-based Schemes
2. Taking $\boldsymbol{P} \in \mathrm{GL}(\mathbb{F}_{q^m})$ might protect against it
3. In practice,

$$\boldsymbol{P}^{-1} = \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix} \quad \text{with} \quad \boldsymbol{Q}_{22} \in \mathrm{GL}(\mathbb{F}_q) \quad \text{and} \quad \mathtt{Rank}_{\mathbb{F}_q}(\boldsymbol{Q}_{12}) = s$$

$\rightsquigarrow$ **Our works give a polynomial attack**

	Matrix	Code generated	Length	Correction capability
Secret	$\boldsymbol{G}$	$\mathscr{G}_k(\vec{g})$	n	t
Attack	$\boldsymbol{G}^*$	$\mathscr{G}_k(\vec{g}^*)$	$n-s$	$t-\frac{s}{2}$
Public	$\boldsymbol{G}_{\mathrm{pub}}$	$(n+\ell, k)$−code	$n+\ell$	$t-\frac{s}{2}$

Conclusion and Related Work

1. **Overbeck's attack**: Principal threat of Gabidulin-based Schemes
2. Taking $\boldsymbol{P} \in \mathrm{GL}(\mathbb{F}_{q^m})$ might protect against it
3. In practice,

$$\boldsymbol{P}^{-1} = \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix} \quad \text{with} \quad \boldsymbol{Q}_{22} \in \mathrm{GL}(\mathbb{F}_q) \quad \text{and} \quad \mathtt{Rank}_{\mathbb{F}_q}(\boldsymbol{Q}_{12}) = s$$

$\rightsquigarrow$ **Our works give a polynomial attack**

	Matrix	Code generated	Length	Correction capability
Secret	$\boldsymbol{G}$	$\mathscr{G}_k(\vec{g})$	n	t
Attack	$\boldsymbol{G}^*$	$\mathscr{G}_k(\vec{g}^*)$	$n-s$	$t-\frac{s}{2}$
Public	$\boldsymbol{G}_{\mathrm{pub}}$	$(n+\ell, k)-$code	$n+\ell$	$t-s$

Conclusion and Related Work

1. **Overbeck's attack**: Principal threat of Gabidulin-based Schemes
2. Taking $\boldsymbol{P} \in \mathrm{GL}(\mathbb{F}_{q^m})$ might protect against it
3. In practice,

$$\boldsymbol{P}^{-1} = \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix} \quad \text{with} \quad \boldsymbol{Q}_{22} \in \mathrm{GL}(\mathbb{F}_q) \quad \text{and} \quad \mathtt{Rank}_{\mathbb{F}_q}(\boldsymbol{Q}_{12}) = s$$

$\rightsquigarrow$ **Our works give a polynomial attack**

	Matrix	Code generated	Length	Correction capability
Secret	$\boldsymbol{G}$	$\mathscr{G}_k(\vec{g})$	n	t
Attack	$\boldsymbol{G}^*$	$\mathscr{G}_k(\vec{g}^*)$	$n-s$	$t-\frac{s}{2}$
Public	$\boldsymbol{G}_{\mathrm{pub}}$	$(n+\ell, k)-$code	$n+\ell$	$t-s$

Conclusion and Related Work

1. **Overbeck's attack**: Principal threat of Gabidulin-based Schemes
2. Taking $\boldsymbol{P} \in \mathrm{GL}(\mathbb{F}_{q^m})$ might protect against it
3. In practice,

$$\boldsymbol{P}^{-1} = \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix} \text{ with } \boldsymbol{Q}_{22} \in \mathrm{GL}(\mathbb{F}_q) \text{ and } \mathtt{Rank}_{\mathbb{F}_q}(\boldsymbol{Q}_{12}) = s$$

$\rightsquigarrow$ **Our works give a polynomial attack**

	Matrix	Code generated	Length	Correction capability
Secret	$\boldsymbol{G}$	$\mathscr{G}_k(\vec{g})$	n	t
Attack	$\boldsymbol{G}^*$	$\mathscr{G}_k(\vec{g}^*)$	$n-s$	$t-\frac{s}{2}$
Public	$\boldsymbol{G}_{\text{pub}}$	$(n+\ell, k)$−code	$n+\ell$	$t-s$

Conclusion and Related Work

1. **Overbeck's attack**: Principal threat of Gabidulin-based Schemes
2. Taking $\boldsymbol{P} \in \mathrm{GL}(\mathbb{F}_{q^m})$ might protect against it
3. In practice,

$$\boldsymbol{P}^{-1} = \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix} \quad \text{with} \quad \boldsymbol{Q}_{22} \in \mathrm{GL}(\mathbb{F}_q) \quad \text{and} \quad \mathtt{Rank}_{\mathbb{F}_q}(\boldsymbol{Q}_{12}) = s$$

$\rightsquigarrow$ **Our works give a polynomial attack**

	Matrix	Code generated	Length	Correction capability
Secret	$\boldsymbol{G}$	$\mathscr{G}_k(\vec{g})$	n	t
Attack	$\boldsymbol{G}^*$	$\mathscr{G}_k(\vec{g}^*)$	$n-s$	$t - \frac{s}{2}$
Public	$\boldsymbol{G}_{\mathrm{pub}}$	$(n+\ell, k)$−code	$n+\ell$	$t-s$

Conclusion and Related Work

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

- $\mathscr{V} \subset \mathbb{F}_{q^m}$ a $\mathbb{F}_q$−vector space
- $d = \dim_{\mathbb{F}_q}(\mathscr{V}) \geqslant 3$
- Choose

$$\boldsymbol{P}^{-1} \in \mathrm{GL}_n(\mathscr{V}) \quad \text{and} \quad \boldsymbol{G}_{\mathrm{pub}} = \boldsymbol{SGP}$$

$$\rightarrow \color{red}{t_{\mathrm{pub}}} = \frac{n-k}{2\color{red}{d}}$$