On the Failure of the Smart Approach of the GPT Cryptosystem

Hervé Talé Kalachi

AFRIMath Seminar

June 25, 2021

AFRIMath

Afrique France Réseau International en Mathématiques

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 : Column Scrambler in the Extension Field**
- **Rashwan-Gabidulin-Honary '10 : Smart Approach**

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 : Column Scrambler in the Extension Field**
- **Rashwan-Gabidulin-Honary '10 : Smart Approach**

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 : Column Scrambler in the Extension Field**
- **Rashwan-Gabidulin-Honary '10 : Smart Approach**

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 : Column Scrambler in the Extension Field**
- **Rashwan-Gabidulin-Honary '10 : Smart Approach**

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 : Column Scrambler in the Extension Field
- Rashwan-Gabidulin-Honary '10 : Smart Approach

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 : Column Scrambler in the Extension Field**
- **Rashwan-Gabidulin-Honary '10 : Smart Approach**

Outline

Example of isometry for rank metric

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

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

Gabidulin codes

Definition 1 (Gabidulin code)

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

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

$$\boldsymbol{G} = \begin{pmatrix} g_1^{q^0} & g_2^{q^0} & \cdots & g_n^{q^0} \\ g_1^{q^1} & g_2^{q^1} & \cdots & g_n^{q^1} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_n^{q^{k-1}} \end{pmatrix}$$

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

Gabidulin codes

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.*

The dual $\mathscr{C}^{\perp}$ of a code $\mathscr{C}$ is the v.s.s

$$\mathscr{C}^{\perp} = \{\vec{y} \in \mathbb{F}^n \ : \ \forall \ \vec{c} \in \mathscr{C}, \ \langle \vec{c}, \vec{y} \rangle = 0\} \text{ with } \langle \vec{c}, \vec{y} \rangle = \sum_{i=1}^{n} c_i y_i$$

Gabidulin codes

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.*

The dual $\mathscr{C}^\perp$ of a code $\mathscr{C}$ is the v.s.s

$$\mathscr{C}^\perp = \{\vec{y} \in \mathbb{F}^n \ : \ \forall\ \vec{c} \in \mathscr{C},\ \langle \vec{c}, \vec{y} \rangle = 0\} \text{ with } \langle \vec{c}, \vec{y} \rangle = \sum_{i=1}^{n} c_i y_i$$

Gabidulin codes

Proposition 2

- $\mathscr{G}_k(\vec{g})$ *a* $(n,k)-$*Gabidulin code on* $\mathbb{F}_{q^m}$
- $\boldsymbol{T} \in \mathrm{GL}_n(\mathbb{F}_q)$

$$\mathscr{G}_k(\vec{g})\,\boldsymbol{T} = \mathscr{G}_k(\vec{g}\,\boldsymbol{T})$$

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. □ □

Gabidulin codes

Proposition 2

- *$\mathscr{G}_k(\vec{g})$ a $(n, k)-$Gabidulin code on $\mathbb{F}_{q^m}$*
- $\boldsymbol{T} \in \mathrm{GL}_n(\mathbb{F}_q)$

$$\mathscr{G}_k(\vec{g})\,\boldsymbol{T} = \mathscr{G}_k(\vec{g}\,\boldsymbol{T})$$

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

GPT Cryptosystem

Key generation.

- $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ 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 $\boldsymbol{X} \in \mathbb{F}_{q^m}^{k \times \ell}$
- $\boldsymbol{P} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$ be a random non-singular matrix
- Compute

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

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

GPT Cryptosystem

Key generation.

- $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ 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 $\boldsymbol{X} \in \mathbb{F}_{q^m}^{k \times \ell}$
- $\boldsymbol{P} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$ be a random non-singular matrix
- Compute

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

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

Key generation.

- $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ 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 $\boldsymbol{X} \in \mathbb{F}_{q^m}^{k \times \ell}$
- $\boldsymbol{P} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$ be a random non-singular matrix
- Compute

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

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

Key generation.

- $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ 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 $\boldsymbol{X} \in \mathbb{F}_{q^m}^{k \times \ell}$
- $\boldsymbol{P} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$ be a random non-singular matrix
- Compute

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

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

Key generation.

- $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ 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 $\boldsymbol{X} \in \mathbb{F}_{q^m}^{k \times \ell}$
- $\boldsymbol{P} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$ be a random non-singular matrix
- Compute

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

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

Key generation.

- $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ a generator matrix of $\mathscr{G}_k\left(\vec{g}\right)$
- Pick at random $\boldsymbol{S} \in \mathrm{GL}_k(\mathbb{F}_{q^m})$.
- Pick a random matrix $\boldsymbol{X} \in \mathbb{F}_{q^m}^{k \times \ell}$
- $\boldsymbol{P} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$ be a random non-singular matrix
- Compute

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

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

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 cipher-text is the vector

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

Decryption.

1. Compute $\vec{c}\boldsymbol{P}$ $\quad \vec{m}\boldsymbol{S}\,(\boldsymbol{X} \mid \boldsymbol{G}) + \vec{e}\boldsymbol{P}$
2. And $\vec{y} = Dec_{(\boldsymbol{X}|\boldsymbol{G})}(\vec{c}\boldsymbol{P})$ $\quad \vec{y} = \vec{m}\boldsymbol{S}$ since $\|\vec{e}\boldsymbol{P}\|_q = \|\vec{e}\|_q \leqslant t$
3. Return $\vec{m}' = \vec{y}\boldsymbol{S}^{-1}$ $\quad \vec{m}' = \vec{m}$

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 cipher-text is the vector

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

Decryption.

1. Compute $\vec{c}\boldsymbol{P}$ $\quad \vec{m}\boldsymbol{S}\,(\boldsymbol{X} \mid \boldsymbol{G}) + \vec{e}\boldsymbol{P}$
2. And $\vec{y} = Dec_{.(\boldsymbol{X}|\boldsymbol{G})}(\vec{c}\boldsymbol{P})$ $\quad \vec{y} = \vec{m}\boldsymbol{S}$ since $\|\vec{e}\boldsymbol{P}\|_q = \|\vec{e}\|_q \leqslant t$
3. Return $\vec{m}' = \vec{y}\boldsymbol{S}^{-1}$ $\quad \vec{m}' = \vec{m}$

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 cipher-text is the vector

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

Decryption.

1. Compute $\vec{c}\boldsymbol{P}$ — $\vec{m}\boldsymbol{S}\left(\boldsymbol{X} \mid \boldsymbol{G}\right) + \vec{e}\boldsymbol{P}$
2. And $\vec{y} = Dec_{\cdot(\boldsymbol{X}|\boldsymbol{G})}(\vec{c}\boldsymbol{P})$ — $\vec{y} = \vec{m}\boldsymbol{S}$ since $\|\vec{e}\boldsymbol{P}\|_q = \|\vec{e}\|_q \leqslant t$
3. Return $\vec{m}' = \vec{y}\boldsymbol{S}^{-1}$ — $\vec{m}' = \vec{m}$

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 cipher-text is the vector

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

Decryption.

1. Compute $\vec{c}\boldsymbol{P}$ — $\vec{m}\boldsymbol{S}\left(\boldsymbol{X} \mid \boldsymbol{G}\right) + \vec{e}\boldsymbol{P}$
2. And $\vec{y} = Dec_{\cdot(\boldsymbol{X}|\boldsymbol{G})}(\vec{c}\boldsymbol{P})$ — $\vec{y} = \vec{m}\boldsymbol{S}$ since $\|\vec{e}\boldsymbol{P}\|_q = \|\vec{e}\|_q \leqslant t$
3. Return $\vec{m}' = \vec{y}\boldsymbol{S}^{-1}$ — $\vec{m}' = \vec{m}$

Overbeck's Attack

Definition 2 (Distinguisher)

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

Define the application Λ_f by:

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

Remark 1

- *For* $\mathbf{P} \in \mathrm{GL}_n(\mathbb{F}_q)$

$$\Lambda_f(\mathscr{U}\mathbf{P}) = \Lambda_f(\mathscr{U})\mathbf{P}$$

Overbeck's Attack

Definition 2 (Distinguisher)

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

Define the application Λ_f by:

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

Remark 1

- For $\boldsymbol{P} \in \mathrm{GL}_n(\mathbb{F}_q)$

$$\Lambda_f(\mathscr{U}\boldsymbol{P}) = \Lambda_f(\mathscr{U})\boldsymbol{P}$$

Overbeck's Attack

Definition 2 (Distinguisher)

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

Define the application Λ_f by:

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

Remark 1

- *For* $\boldsymbol{P} \in \mathrm{GL}_n(\mathbb{F}_q)$

$$\Lambda_f(\mathscr{U}\boldsymbol{P}) = \Lambda_f(\mathscr{U})\boldsymbol{P}$$

Overbeck's Attack

Proposition 3

- $f \leqslant n-k-1$

$$\Lambda_f(\mathcal{G}_k(\vec{g})) = \mathcal{G}_{k+f}(\vec{g})$$

In particular,

$$\dim \Lambda_f(\mathcal{G}_k(\vec{g})) = k + f$$

Theorem 3

For a "random" $(n,k)-$code $\mathscr{R}$,

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

with a high probability.

Overbeck's Attack

Proposition 3

- $f \leqslant n - k - 1$

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

In particular,

$$\dim \Lambda_f(\mathscr{G}_k(\vec{g})) = k + f$$

Theorem 3

For a "random" $(n, k)-$code $\mathscr{R}$,

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

with a high probability.

Overbeck's Attack

Proposition 3

- $f \leqslant n - k - 1$

$$\Lambda_{f}(\mathscr{G}_k(\vec{g})) = \mathscr{G}_{k+f}(\vec{g})$$

In particular,

$$\dim \Lambda_{f}(\mathscr{G}_k(\vec{g})) = k + f$$

Theorem 3

For a "random" $(n, k)-$code $\mathscr{R}$,

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

with a high probability.

Overbeck's Attack

Proposition 4

- *Let* $\boldsymbol{G}_{pub} = \boldsymbol{S}\left(\boldsymbol{X} \mid \boldsymbol{G}\right)\boldsymbol{P}^{-1}$ *be a generator matrix of* $\mathscr{C}_{\text{pub}}$

$\Lambda_{n-k-1}\left(\mathscr{C}_{pub}\right) \subset \mathbb{F}_{q^m}^{n+\ell}$ *is generated by:*

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

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

Overbeck's Attack

Remark 2

$$\dim \Lambda_{n-k-1}(\mathscr{C}_{pub}) = n - 1 + Rank\,(\boldsymbol{X}_2)$$

Theorem 4

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

- $$\dim \Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp} = 1$$
- $$\Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp} = < \left(0 \mid \vec{h}\right) \boldsymbol{P}^{T} >$$

Remark 2

$$\dim \Lambda_{n-k-1}(\mathscr{C}_{pub}) = n - 1 + Rank\left(\boldsymbol{X}_2\right)$$

Theorem 4

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

- $$\dim \Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp} = 1$$
- $$\Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp} = < \begin{pmatrix} 0 \mid \vec{h} \end{pmatrix} \boldsymbol{P}^{T} >$$

Overbeck's Attack

Remark 2

$$\dim \Lambda_{n-k-1}(\mathscr{C}_{pub}) = n - 1 + Rank\,(\boldsymbol{X}_2)$$

Theorem 4

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

- $$\dim \Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp} = 1$$
- $$\Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp} =< \begin{pmatrix} 0 \mid \vec{h} \end{pmatrix} \boldsymbol{P}^T >$$

Overbeck's Attack

Remark 2

$$\dim \Lambda_{n-k-1}(\mathscr{C}_{pub}) = n - 1 + Rank\left(\boldsymbol{X}_2\right)$$

Theorem 4

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

- $$\dim \Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp} = 1$$
- $$\Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp} = < \left(0 \mid \vec{h}\right) \boldsymbol{P}^T >$$

Overbeck's Attack

Summary

- Compute

$$\Lambda_{n-k-1}(\mathscr{C}_{pub})$$

- If

$$\dim \Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp} = 1$$

- Choose $\vec{h} \in \Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp}, \quad \vec{h} \neq \mathbf{0}$
- Find $\boldsymbol{T} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$ such that $\vec{h} = (\mathbf{0} \mid \vec{h}')\boldsymbol{T}$, $\vec{h}' \in \mathbb{F}_{q^m}^n$ Easy : Linear algebra

Overbeck's Attack

Summary

- Compute

$$\Lambda_{n-k-1}(\mathscr{C}_{pub})$$

- If

$$\dim \Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp} = 1$$

- Choose $\vec{h} \in \Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp}, \quad \vec{h} \neq \mathbf{0}$
- Find $\boldsymbol{T} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$ such that $\vec{h} = (\mathbf{0} \mid \vec{h}')\boldsymbol{T}$, $\vec{h}' \in \mathbb{F}_{q^m}^n$ Easy : Linear algebra

Overbeck's Attack

Summary

- Compute

$$\Lambda_{n-k-1}(\mathscr{C}_{pub})$$

- If

$$\dim \Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp} = 1$$

- Choose $\vec{h} \in \Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp}, \quad \vec{h} \neq \mathbf{0}$

- Find $\boldsymbol{T} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$ such that $\vec{h} = (\mathbf{0} \mid \vec{h}')\boldsymbol{T}$, $\vec{h}' \in \mathbb{F}_{q^m}^n$ Easy : Linear algebra

Overbeck's Attack

Summary

- Compute

$$\Lambda_{n-k-1}(\mathscr{C}_{pub})$$

- If

$$\dim \Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp} = 1$$

- Choose $\vec{h} \in \Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp}, \quad \vec{h} \neq \mathbf{0}$
- Find $\boldsymbol{T} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$ such that $\vec{h} = (\mathbf{0} \mid \vec{h}')\boldsymbol{T}$, $\vec{h}' \in \mathbb{F}_{q^m}^n$ Easy : Linear algebra

Overbeck's Attack

Remark 3

The success of this attack is based on two facts:

1. $\boldsymbol{P} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$
2. $\boldsymbol{X}_2$ *must be a of full rank,* $Rank\,(\boldsymbol{X}_2) = \ell$

GPT Reparations

Reparation ideas linked to $\boldsymbol{X}_2$

- **Loidreau '10** : Proposition of parameters such that $Rank\left(\Lambda_f(\mathscr{C}_{pub})^{\perp}\right) > 1$.
- **Rashwan-Gabidulin-Honary '10** : Similar approach called "Smart approach".

GPT Reparations

Reparation ideas linked to $\boldsymbol{X}_2$

- **Loidreau '10** : Proposition of parameters such that $Rank\left(\Lambda_f(\mathscr{C}_{pub})^{\perp}\right) > 1$.

- **Rashwan-Gabidulin-Honary '10** : Similar approach called "Smart approach".

The Reparation is related to $\boldsymbol{X}$

- In the Key generation, chose $\boldsymbol{X}_1$ and such that

$$\boldsymbol{X}_1 = \begin{pmatrix} b_1^{[0]} & \cdots & b_a^{[0]} \\ \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} \end{pmatrix}$$

- $\boldsymbol{X}_2 \in \mathbb{F}_{q^m}^{k \times (\ell - a)}$
- $\boldsymbol{X} = (\boldsymbol{X}_1 \mid \boldsymbol{X}_2)$

$$\boldsymbol{G}_{pub} \stackrel{\text{def}}{=} \boldsymbol{S}(\boldsymbol{X} \mid \boldsymbol{G})\boldsymbol{P}^{-1} = \boldsymbol{S}(\boldsymbol{X}_1 \mid \boldsymbol{X}_2 \mid \boldsymbol{G})\boldsymbol{P}^{-1}$$

Plan

Cryptanalysis

$$\boldsymbol{G}_{\text{pub}} = \boldsymbol{S} \left(\begin{array}{ccc|ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} & g_1^{[0]} & \cdots & g_n^{[0]} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} & g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{array} \right) \boldsymbol{P}^{-1}$$

- Let $\vec{g}' = \left(\vec{b} \mid \vec{g}\right) \in \mathbb{F}_{q^m}^{a+n}$
- $\|\vec{g}'\|_q \geqslant \|\vec{g}\|_q = n$
- $\|\vec{g}'\|_q = n + s \leqslant m$ with $s \leqslant a$.
- $\|(\boldsymbol{X}_1 \mid \boldsymbol{G})\|_q = \|\vec{g}'\|_q = n + s$
- There exists a matrix $\boldsymbol{Q} \in \mathrm{GL}_{n+a}(\mathbb{F}_q)$ such that

$$(\boldsymbol{X}_1 \mid \boldsymbol{G})\,\boldsymbol{Q} = (\boldsymbol{0} \mid \boldsymbol{G}^*)$$

- There exists a matrix $\boldsymbol{T} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$

$$(\boldsymbol{X}_1 \mid \boldsymbol{X}_2 \mid \boldsymbol{G})\,\boldsymbol{T} = (\boldsymbol{0} \mid \boldsymbol{X}_2 \mid \boldsymbol{G}^*)$$

$$\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}\,(\boldsymbol{0} \mid \boldsymbol{X}_2 \mid \boldsymbol{G}^*)\,\boldsymbol{T}^{-1}\boldsymbol{P}^{-1}$$

$$\boldsymbol{G}_{\mathrm{pub}} = \boldsymbol{S} \left(\begin{array}{ccc|ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} & g_1^{[0]} & \cdots & g_n^{[0]} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} & g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{array} \right) \boldsymbol{P}^{-1}$$

- Let $\vec{g}' = \left(\vec{b} \mid \vec{g} \right) \in \mathbb{F}_{q^m}^{a+n}$
- $\|\vec{g}'\|_q \geqslant \|\vec{g}\|_q = n$
- $\|\vec{g}'\|_q = n + s \leqslant m$ with $s \leqslant a$.
- $\|(\boldsymbol{X}_1 \mid \boldsymbol{G})\|_q = \|\vec{g}'\|_q = n + s$
- There exists a matrix $\boldsymbol{Q} \in \mathrm{GL}_{n+a}(\mathbb{F}_q)$ such that

$$(\boldsymbol{X}_1 \mid \boldsymbol{G})\,\boldsymbol{Q} = (\boldsymbol{0} \mid \boldsymbol{G}^*)$$

- There exists a matrix $\boldsymbol{T} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$

$$(\boldsymbol{X}_1 \mid \boldsymbol{X}_2 \mid \boldsymbol{G})\,\boldsymbol{T} = (\boldsymbol{0} \mid \boldsymbol{X}_2 \mid \boldsymbol{G}^*)$$

$$\boldsymbol{G}_{\mathrm{pub}} = \boldsymbol{S}\,(\boldsymbol{0} \mid \boldsymbol{X}_2 \mid \boldsymbol{G}^*)\,\boldsymbol{T}^{-1}\boldsymbol{P}^{-1}$$

Cryptanalysis

$$\boldsymbol{G}_{\mathrm{pub}} = \boldsymbol{S}\left(\begin{array}{ccc|ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} & g_1^{[0]} & \cdots & g_n^{[0]} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} & g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{array}\right)\boldsymbol{P}^{-1}$$

- Let $\vec{g}' = \left(\vec{b} \mid \vec{g}\right) \in \mathbb{F}_{q^m}^{a+n}$
- $\|\vec{g}'\|_q \geqslant \|\vec{g}\|_q = n$
- $\|\vec{g}'\|_q = n + s \leqslant m$ with $s \leqslant a$.
- $\|(\boldsymbol{X}_1 \mid \boldsymbol{G})\|_q = \|\vec{g}'\|_q = n + s$
- There exists a matrix $\boldsymbol{Q} \in \mathrm{GL}_{n+a}(\mathbb{F}_q)$ such that

$$(\boldsymbol{X}_1 \mid \boldsymbol{G})\,\boldsymbol{Q} = (\boldsymbol{0} \mid \boldsymbol{G}^*)$$

- There exists a matrix $\boldsymbol{T} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$

$$(\boldsymbol{X}_1 \mid \boldsymbol{X}_2 \mid \boldsymbol{G})\,\boldsymbol{T} = (\boldsymbol{0} \mid \boldsymbol{X}_2 \mid \boldsymbol{G}^*)$$

$$\boldsymbol{G}_{\mathrm{pub}} = \boldsymbol{S}\,(\boldsymbol{0} \mid \boldsymbol{X}_2 \mid \boldsymbol{G}^*)\,\boldsymbol{T}^{-1}\boldsymbol{P}^{-1}$$

Cryptanalysis

$$\boldsymbol{G}_{\mathrm{pub}} = \boldsymbol{S} \left(\begin{array}{ccc|ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} & g_1^{[0]} & \cdots & g_n^{[0]} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} & g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{array} \right) \boldsymbol{P}^{-1}$$

- Let $\vec{g}' = \left(\vec{b} \mid \vec{g}\right) \in \mathbb{F}_{q^m}^{a+n}$
- $\|\vec{g}'\|_q \geqslant \|\vec{g}\|_q = n$
- $\|\vec{g}'\|_q = n + s \leqslant m$ with $s \leqslant a$.
- $\|(\boldsymbol{X}_1 \mid \boldsymbol{G})\|_q = \|\vec{g}'\|_q = n + s$
- There exists a matrix $\boldsymbol{Q} \in \mathrm{GL}_{n+a}(\mathbb{F}_q)$ such that

$$(\boldsymbol{X}_1 \mid \boldsymbol{G})\, \boldsymbol{Q} = (\boldsymbol{0} \mid \boldsymbol{G}^*)$$

- There exists a matrix $\boldsymbol{T} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$

$$(\boldsymbol{X}_1 \mid \boldsymbol{X}_2 \mid \boldsymbol{G})\, \boldsymbol{T} = (\boldsymbol{0} \mid \boldsymbol{X}_2 \mid \boldsymbol{G}^*)$$

$$\boldsymbol{G}_{\mathrm{pub}} = \boldsymbol{S}\,(\boldsymbol{0} \mid \boldsymbol{X}_2 \mid \boldsymbol{G}^*)\, \boldsymbol{T}^{-1} \boldsymbol{P}^{-1}$$

$$G_{\text{pub}} = S \left(\begin{array}{ccc|ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} & g_1^{[0]} & \cdots & g_n^{[0]} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} & g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{array} \right) P^{-1}$$

- Let $\vec{g}' = \left(\vec{b} \mid \vec{g}\right) \in \mathbb{F}_{q^m}^{a+n}$
- $\|\vec{g}'\|_q \geqslant \|\vec{g}\|_q = n$
- $\|\vec{g}'\|_q = n + s \leqslant m$ with $s \leqslant a$.
- $\|(X_1 \mid G)\|_q = \|\vec{g}'\|_q = n + s$
- There exists a matrix $Q \in \mathrm{GL}_{n+a}(\mathbb{F}_q)$ such that

$$(X_1 \mid G)\, Q = (0 \mid G^*)$$

- There exists a matrix $T \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$

$$(X_1 \mid X_2 \mid G)\, T = (0 \mid X_2 \mid G^*)$$

$$G_{\text{pub}} = S\,(0 \mid X_2 \mid G^*)\, T^{-1} P^{-1}$$

Cryptanalysis

$$\boldsymbol{G}_{\text{pub}} = \boldsymbol{S} \left(\begin{array}{ccc|ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} & g_1^{[0]} & \cdots & g_n^{[0]} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} & g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{array} \right) \boldsymbol{P}^{-1}$$

- Let $\vec{g}' = \left(\vec{b} \mid \vec{g}\right) \in \mathbb{F}_{q^m}^{a+n}$
- $\|\vec{g}'\|_q \geqslant \|\vec{g}\|_q = n$
- $\|\vec{g}'\|_q = n + s \leqslant m$ with $s \leqslant a$.
- $\|(\boldsymbol{X}_1 \mid \boldsymbol{G})\|_q = \|\vec{g}'\|_q = n + s$
- There exists a matrix $\boldsymbol{Q} \in \mathrm{GL}_{n+a}(\mathbb{F}_q)$ such that

$$(\boldsymbol{X}_1 \mid \boldsymbol{G})\,\boldsymbol{Q} = (\boldsymbol{0} \mid \boldsymbol{G}^*)$$

- There exists a matrix $\boldsymbol{T} \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$

$$(\boldsymbol{X}_1 \mid \boldsymbol{X}_2 \mid \boldsymbol{G})\,\boldsymbol{T} = (\boldsymbol{0} \mid \boldsymbol{X}_2 \mid \boldsymbol{G}^*)$$

$$\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}\,(\boldsymbol{0} \mid \boldsymbol{X}_2 \mid \boldsymbol{G}^*)\,\boldsymbol{T}^{-1}\boldsymbol{P}^{-1}$$

Cryptanalysis

$$G_{\mathrm{pub}} = S \left(\begin{array}{ccc|ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} & g_1^{[0]} & \cdots & g_n^{[0]} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} & g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{array} \right) P^{-1}$$

- Let $\vec{g}' = \left(\vec{b} \mid \vec{g}\right) \in \mathbb{F}_{q^m}^{a+n}$
- $\|\vec{g}'\|_q \geqslant \|\vec{g}\|_q = n$
- $\|\vec{g}'\|_q = n + s \leqslant m$ with $s \leqslant a$.
- $\|(X_1 \mid G)\|_q = \|\vec{g}'\|_q = n + s$
- There exists a matrix $Q \in \mathrm{GL}_{n+a}(\mathbb{F}_q)$ such that

$$(X_1 \mid G)\, Q = (0 \mid G^*)$$

- There exists a matrix $T \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$

$$(X_1 \mid X_2 \mid G)\, T = (0 \mid X_2 \mid G^*)$$

$$G_{\mathrm{pub}} = S\,(0 \mid X_2 \mid G^*)\, T^{-1} P^{-1}$$

Polynomial Structural Attack

$$G_{\text{pub}} = S \left(\begin{array}{ccc|ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} & g_1^{[0]} & \cdots & g_n^{[0]} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} & g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{array} \right) P^{-1}$$

Lemma 5

There exists

1. $P^* \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$
2. $G^* \in \mathbb{F}_{q^m}^{k\times(n+s)}$ *generating a Gabidulin code*
3. $s \in \mathbb{N}$ *s.t* $0 \leqslant s \leqslant a$ *and* $n+s \leqslant m$.

such that

$$G_{\text{pub}} = S \left(\begin{array}{ccc|ccc|ccc} 0 & \cdots & 0 & x_{21,1} & \cdots & x_{21,\ell-a} & g_1^{*[0]} & \cdots & g_{n+s}^{*[0]} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & x_{2k,1} & \cdots & x_{2k,\ell-a} & g_1^{*[k-1]} & \cdots & g_{n+s}^{*[k-1]} \end{array} \right) P^*$$

Polynomial Structural Attack

$$G_{\text{pub}} = S \left(\begin{array}{ccc|ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} & g_1^{[0]} & \cdots & g_n^{[0]} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} & g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{array} \right) P^{-1}$$

Lemma 5

There exists

1. $P^* \in \mathrm{GL}_{n+\ell}(\mathbb{F}_q)$
2. $G^* \in \mathbb{F}_{q^m}^{k \times (n+s)}$ *generating a Gabidulin code*
3. $s \in \mathbb{N}$ *s.t* $0 \leqslant s \leqslant a$ *and* $n + s \leqslant m$.

such that

$$G_{\text{pub}} = S \left(\begin{array}{ccc|ccc|ccc} 0 & \cdots & 0 & x_{21,1} & \cdots & x_{21,\ell-a} & {g_1^*}^{[0]} & \cdots & {g_{n+s}^*}^{[0]} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & x_{2k,1} & \cdots & x_{2k,\ell-a} & {g_1^*}^{[k-1]} & \cdots & {g_{n+s}^*}^{[k-1]} \end{array} \right) P^*$$

Polynomial Structural Attack

Proposition 5

$\mathscr{C}_{\text{pub}}$ is the public code of a general GPT cryptosystem with $w = a - s$ redundancies.

Proposition 6

- $f = n + s - k$
- $\boldsymbol{I} = \{i_1, ..., i_w\} \subset \{1, 2, ..., n + \ell\}$

$\boldsymbol{I}$ is a "redundancy set" of $\mathscr{C}_{\text{pub}}$ if and only if for any subset $\boldsymbol{J} \subset \boldsymbol{I}$,

$$\dim \Lambda_f(\mathscr{C}_{\text{pub}}^{\boldsymbol{J}}) = n + s + \ell - a$$

Remark that for $\boldsymbol{I}$ that is not a "redundancy set",

$$\dim \Lambda_f(\mathscr{C}_{\text{pub}}^{\boldsymbol{J}}) < n + s + \ell - a$$

Polynomial Structural Attack

Proposition 5

$\mathscr{C}_{\text{pub}}$ is the public code of a general GPT cryptosystem with $w = a - s$ redundancies.

Proposition 6

- $f = n + s - k$
- $\boldsymbol{I} = \{i_1, \dots, i_w\} \subset \{1, 2, \dots, n + \ell\}$

$\boldsymbol{I}$ is a "redundancy set" of $\mathscr{C}_{\text{pub}}$ if and only if for any subset $\boldsymbol{J} \subset \boldsymbol{I}$,

$$\dim \Lambda_f(\mathscr{C}_{\text{pub}}^{\boldsymbol{J}}) = n + s + \ell - a$$

Remark that for $\boldsymbol{I}$ that is not a "redundancy set",

$$\dim \Lambda_f(\mathscr{C}_{\text{pub}}^{\boldsymbol{J}}) < n + s + \ell - a$$

Polynomial Structural Attack

Proposition 5

$\mathscr{C}_{\text{pub}}$ is the public code of a general GPT cryptosystem with $w = a - s$ redundancies.

Proposition 6

- $f = n + s - k$
- $\boldsymbol{I} = \{i_1, ..., i_w\} \subset \{1, 2, ..., n + \ell\}$

$\boldsymbol{I}$ is a "redundancy set" of $\mathscr{C}_{\text{pub}}$ if and only if for any subset $\boldsymbol{J} \subset \boldsymbol{I}$,

$$\dim \Lambda_f(\mathscr{C}_{\text{pub}}^{\boldsymbol{J}}) = n + s + \ell - a$$

Remark that for $\boldsymbol{I}$ that is not a "redundancy set",

$$\dim \Lambda_f(\mathscr{C}_{\text{pub}}^{\boldsymbol{J}}) < n + s + \ell - a$$

Cryptanalysis

Steps of the attack

- Eliminate a "redundancy set" by testing :

$$\dim \Lambda_f(\mathscr{C}^i_{\mathrm{pub}})$$

for $i = 1...Length(\mathscr{C}_{\mathrm{pub}})$, $\mathscr{C}_{\mathrm{pub}} = \mathscr{C}^i_{\mathrm{pub}}$ if $\dim \Lambda_{n+s-k}(\mathscr{C}^i_{\mathrm{pub}}) = n + s + \ell - a$

- Apply Overbeck's attack on $\mathscr{C}_{\mathrm{pub}}$ with $f = n + s - k - 1$

Cryptanalysis - Smart Approach

1. **Overbeck's Attack**: Principal threat of Gabidulin-based Schemes
2. Taking a special distortion matrix $\boldsymbol{X}$ might protect against it
3. "Smart Approach" variant,

$$\boldsymbol{X} = \left(\begin{array}{ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} \\ \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} \end{array} \right)$$

$\rightsquigarrow$ **Global idea of our attack**

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

Cryptanalysis - Smart Approach

1. **Overbeck's Attack**: Principal threat of Gabidulin-based Schemes
2. Taking a special distortion matrix $\boldsymbol{X}$ might protect against it
3. "Smart Approach" variant,

$$\boldsymbol{X} = \left(\begin{array}{ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} \\ \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} \end{array}\right)$$

$\rightsquigarrow$ **Global idea of our attack**

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

Cryptanalysis - Smart Approach

1. **Overbeck's Attack**: Principal threat of Gabidulin-based Schemes
2. Taking a special distortion matrix $\boldsymbol{X}$ might protect against it
3. "Smart Approach" variant,

$$\boldsymbol{X} = \left(\begin{array}{ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} \\ \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} \end{array}\right)$$

$\rightsquigarrow$ **Global idea of our attack**

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

Cryptanalysis - Smart Approach

1. **Overbeck's Attack**: Principal threat of Gabidulin-based Schemes
2. Taking a special distortion matrix $\boldsymbol{X}$ might protect against it
3. "Smart Approach" variant,

$$\boldsymbol{X} = \left(\begin{array}{ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} \\ \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} \end{array} \right)$$

$\rightsquigarrow$ **Global idea of our attack**

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

1. **Overbeck's Attack**: Principal threat of Gabidulin-based Schemes
2. Taking a special distortion matrix $\boldsymbol{X}$ might protect against it
3. "Smart Approach" variant,

$$\boldsymbol{X} = \left(\begin{array}{ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} \\ \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} \end{array}\right)$$

$\rightsquigarrow$ **Global idea of our attack**

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

1. **Overbeck's Attack**: Principal threat of Gabidulin-based Schemes
2. Taking a special distortion matrix $\boldsymbol{X}$ might protect against it
3. "Smart Approach" variant,

$$\boldsymbol{X} = \left(\begin{array}{ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} \\ \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} \end{array}\right)$$

$\rightsquigarrow$ **Global idea of our attack**

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

Cryptanalysis - Smart Approach

1. **Overbeck's Attack**: Principal threat of Gabidulin-based Schemes
2. Taking a special distortion matrix $\boldsymbol{X}$ might protect against it
3. "Smart Approach" variant,

$$\boldsymbol{X} = \left(\begin{array}{ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} \\ \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} \end{array} \right)$$

$\rightsquigarrow$ **Global idea of our attack**

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

Cryptanalysis - Smart Approach

1. **Overbeck's Attack**: Principal threat of Gabidulin-based Schemes
2. Taking a special distortion matrix $\boldsymbol{X}$ might protect against it
3. "Smart Approach" variant,

$$\boldsymbol{X} = \left(\begin{array}{ccc|ccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} \\ \vdots & & \vdots & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} \end{array}\right)$$

$\rightsquigarrow$ **Global idea of our attack**

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

Plan

Conclusion

Code based encryption schemes

- **Main drawback**: Enormous size of the Keys
- **Potential solution**: Rank metric codes
  - **Gabidulin codes**
  - Too structured $\rightsquigarrow$ Public code distinguishable

$\rightsquigarrow$ **Our works show that several attempts to mask them have failed**

Conclusion

Code based encryption schemes

- **Main drawback**: Enormous size of the Keys
- **Potential solution**: Rank metric codes
  - **Gabidulin codes**
  - Too structured $\rightsquigarrow$ Public code distinguishable

$\rightsquigarrow$ **Our works show that several attempts to mask them have failed**

Conclusion

Code based encryption schemes

- **Main drawback**: Enormous size of the Keys
- **Potential solution**: Rank metric codes
  - **Gabidulin codes**
  - Too structured $\rightsquigarrow$ Public code distinguishable

$\rightsquigarrow$ **Our works show that several attempts to mask them have failed**

Conclusion

Code based encryption schemes

- **Main drawback**: Enormous size of the Keys
- **Potential solution**: Rank metric codes
  - **Gabidulin codes**
  - Too structured $\rightsquigarrow$ Public code distinguishable

$\rightsquigarrow$ **Our works show that several attempts to mask them have failed**

Conclusion

Code based encryption schemes

- **Main drawback**: Enormous size of the Keys
- **Potential solution**: Rank metric codes
  - **Gabidulin codes**
  - Too structured $\rightsquigarrow$ Public code distinguishable

$\rightsquigarrow$ **Our works show that several attempts to mask them have failed**

Perspectives - Designing

- Gabidulin Codes Over Rings [1]
- Possible Application to Cryptography ?
- In a GPT settings ?

[1] [TM19] **H. Tchatchiem Kamche, C. Mouaha. Rank-Metric Codes Over Finite Principal Ideal Rings and Applications.** ***IEEE Trans. Inf. Theory***

Perspectives - Designing

- Gabidulin Codes Over Rings [1]
- Possible Application to Cryptography ?
- In a GPT settings ?

[1] [TM19] **H. Tchatchiem Kamche, C. Mouaha. Rank-Metric Codes Over Finite Principal Ideal Rings and Applications.** ***IEEE Trans. Inf. Theory***