On the Failure of the Smart Approach of the GPT Cryptosystem

Hervé Talé Kalachi

AFRIMath Seminar

June 25, 2021







 Hervé Talé Kalachi
 June 25, 2021
 1/2

Gabidulin-Paramonov-Tretjakov cryptosystem '91

- Rank metric with Gabidulin codes
- 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

Gabidulin-Paramonov-Tretjakov cryptosystem '91

- 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

Gabidulin-Paramonov-Tretjakov cryptosystem '91

- 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

◆ロト ◆団 ト ◆ 恵 ト ◆ 恵 ・ 夕 Q C ・

Gabidulin-Paramonov-Tretjakov cryptosystem '91

- Rank metric with Gabidulin codes
- 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

◆ロト ◆団 ト ◆ 恵 ト ◆ 恵 ・ り へ ②

Gabidulin-Paramonov-Tretjakov cryptosystem '91

- Rank metric with Gabidulin codes
- 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

4 D > 4 P > 4 E > 4 E > E 990

Gabidulin-Paramonov-Tretjakov cryptosystem '91

- Rank metric with Gabidulin codes
- 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

(ロ) (型) (注) (注) 注 り(で)

Outline

GPT Cryptosystem and Variants

Polynomial Structural Attack

Conclusion and Related Work

4□ > 4□ > 4 ≥ > 4 ≥ > ≥ 900

Example of isometry for rank metric

•
$$\vec{x} \in \mathbb{F}_{q^m}^n$$

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

$$\|\vec{x}\,\mathbf{T}\|_q = \|\vec{x}\|_q$$

Definition 1 (Gabidulin code)

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

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

$$m{G} = egin{pmatrix} g_1^{q^0} & g_2^{q^0} & \dots & g_n^{q^0} \ g_1^{q^1} & g_2^{q^1} & \dots & g_n^{q^1} \ & & \ddots & & \ddots \ & & \ddots & & \ddots \ & & \ddots & & \ddots \ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \dots & g_n^{q^{k-1}} \end{pmatrix}$$

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

Hervé Talé Kalachi June 25, 2021 5/27

Proposition 1

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

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

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

◆ロト ◆団 ト ◆ 恵 ト ◆ 恵 ・ 夕 Q C ・

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

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

Proposition 2

- ullet $\mathscr{G}_{k}\left(ec{g}
 ight)$ a (n,k)-Gabidulin code on $\mathbb{F}_{q^{m}}$
- $T \in \mathsf{GL}_n(\mathbb{F}_q)$

$$\mathscr{G}_{k}\left(\vec{g}\right)\mathbf{T}=\mathscr{G}_{k}\left(\vec{g}\,\mathbf{T}\right)$$

Proof.

For the proof, remark that

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

for any integer i.

4□ > 4団 > 4豆 > 4豆 > 豆 り9○

Proposition 2

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

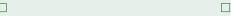
$$\mathscr{G}_{k}\left(\vec{g}\right)\mathbf{T}=\mathscr{G}_{k}\left(\vec{g}\,\mathbf{T}\right)$$

Proof.

For the proof, remark that

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

for any integer i.



4 D > 4 B > 4 E >

Plan

GPT Cryptosystem and Variants

Polynomial Structural Attack

3 Conclusion and Related Work

◆ロト ◆団ト ◆差ト ◆差ト 差 めらぐ

Key generation.

- $oldsymbol{G} \in \mathbb{F}_{q^m}^{k imes n}$ a generator matrix of $\mathscr{G}_k\left(ec{g}
 ight)$
- Pick at random $S \in GL_k(\mathbb{F}_{q^m})$.
- ullet Pick a random matrix $oldsymbol{X} \in \mathbb{F}_{q^m}^{k imes \ell}$
- ullet $oldsymbol{P} \in \mathsf{GL}_{n+\ell}(\mathbb{F}_q)$ be a random non-singular matrix
- Compute

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

The public key is (\boldsymbol{G}_{pub},t) where $t\stackrel{\mathrm{der}}{=}|rac{n-k}{2}|$

◆ロト ◆団 ト ◆ 恵 ト ◆ 恵 ・ 夕 Q C ・

Key generation.

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

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

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

Key generation.

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

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

The public key is $(oldsymbol{G}_{pub},t)$ where $t\stackrel{\mathsf{def}}{=}\lfloor rac{n-k}{2}
floor$

Key generation.

- $oldsymbol{G} \in \mathbb{F}_{q^m}^{k imes n}$ a generator matrix of $\mathscr{G}_k\left(ec{g}
 ight)$
- Pick at random $\boldsymbol{S} \in \mathsf{GL}_k(\mathbb{F}_{q^m})$.
- ullet Pick a random matrix $oldsymbol{X} \in \mathbb{F}_{q^m}^{k imes \ell}$
- $P \in GL_{n+\ell}(\mathbb{F}_q)$ be a random non-singular matrix
- Compute

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

The public key is $(oldsymbol{G}_{pub},t)$ where $t\stackrel{\mathsf{def}}{=}\lfloor rac{n-k}{2}
floor$

Key generation.

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

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

Key generation.

- $oldsymbol{G} \in \mathbb{F}_{q^m}^{k imes n}$ a generator matrix of $\mathscr{G}_k\left(ec{g}
 ight)$
- Pick at random $\boldsymbol{S} \in GL_k(\mathbb{F}_{q^m})$.
- ullet Pick a random matrix $oldsymbol{X} \in \mathbb{F}_{q^m}^{k imes \ell}$
- $P \in GL_{n+\ell}(\mathbb{F}_q)$ 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 $t\stackrel{\text{def}}{=}\lfloor\frac{n-k}{2}\rfloor$

4 L P 4 B P 4 E P 4 E P 5 E 9)4 (**

Encryption.

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

- **①** Generate $\vec{e} \in \mathbb{F}_{a^m}^n$ such that $\|\vec{e}\|_a \leqslant t$.
- The cipher-text is the vector

$$ec{c} = ec{m} oldsymbol{G}_{pub} + ec{e}$$

$$\vec{m}S(X \mid G) + \vec{e}P$$

$$ec{y} = ec{m} oldsymbol{S}$$
 since $\|ec{e} oldsymbol{P}\|_q = \|ec{e}\|_q \leqslant t$

$$\vec{m}' = \vec{m}$$

Encryption.

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

- **①** Generate $\vec{e} \in \mathbb{F}_{a^m}^n$ such that $\|\vec{e}\|_a \leqslant t$.
- The cipher-text is the vector

$$ec{c} = ec{m} oldsymbol{G}_{pub} + ec{e}$$

Decryption.

Ompute *c* **P**

$$\vec{m}S(X \mid G) + \vec{e}P$$

② And
$$\vec{y} = Dec_{.(X|G)}(\vec{c}P)$$

$$\vec{y} = \vec{m} S$$
 since $\|\vec{e} P\|_q = \|\vec{e}\|_q \leqslant t$

Encryption.

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

- **①** Generate $\vec{e} \in \mathbb{F}_{a^m}^n$ such that $\|\vec{e}\|_a \leqslant t$.
- The cipher-text is the vector

$$ec{c} = ec{m} oldsymbol{G}_{pub} + ec{e}$$

Decryption.

Ompute *c* **P**

$$\vec{m}S(X \mid G) + \vec{e}P$$

2 And
$$\vec{y} = Dec_{.(X|G)}(\vec{c}P)$$

$$ec{y} = ec{m} oldsymbol{S}$$
 since $\|ec{e} oldsymbol{P}\|_q = \|ec{e}\|_q \leqslant t$

Encryption.

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

- **①** Generate $\vec{e} \in \mathbb{F}_{a^m}^n$ such that $\|\vec{e}\|_a \leqslant t$.
- The cipher-text is the vector

$$\vec{c} = \vec{m} G_{pub} + \vec{e}$$

Decryption.

Ompute *c* **P**

$$\vec{m}S(X \mid G) + \vec{e}P$$

2 And
$$\vec{y} = Dec_{.(X|G)}(\vec{c}P)$$

$$ec{y} = ec{m} oldsymbol{S}$$
 since $\|ec{e} oldsymbol{P}\|_a = \|ec{e}\|_a \leqslant t$

6 Return
$$\vec{m}' = \vec{y} S^{-1}$$

$$\vec{m}' = \vec{m}$$

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

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

$$ullet$$
 For $oldsymbol{P}\in\mathsf{GL}_n(\mathbb{F}_q)$

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

Definition 2 (Distinguisher)

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

Define the application Λ_f by:

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

• For
$$P \in \mathsf{GL}_n(\mathbb{F}_q)$$

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

Definition 2 (Distinguisher)

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

Define the application Λ_f by:

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

Remark 1

• For $P \in \mathsf{GL}_n(\mathbb{F}_q)$

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

Proposition 3

•
$$f \le n - k - 1$$

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

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

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

Proposition 3

•
$$f \le n - k - 1$$

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

In particular,

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

Theorem 3

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

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

with a high probability.

Proposition 3

•
$$f \leqslant n - k - 1$$

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

In particular,

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

Theorem 3

For a "random" (n, k)—code \mathcal{R} ,

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

with a high probability.

◆ロト ◆回 ト ◆ 差 ト ◆ 差 ・ 釣 Q (*)

Proposition 4

ullet Let $extbf{\textit{G}}_{ extit{pub}} = extbf{\textit{S}}\left(extbf{\textit{X}} \mid extbf{\textit{G}}
ight) extbf{\textit{P}}^{-1}$ be a generator matrix of $\mathscr{C}_{ ext{pub}}$

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

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

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

Remark 2

$$\dim \Lambda_{n-k-1}(\mathscr{C}_{pub}) = n-1 + Rank(X_2)$$

Theorem 4

If
$$Rank(X_2) = \ell$$
,

a

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

0

$$\Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp} = <\left(0\mid ec{h}
ight)oldsymbol{P}^{T}$$
 :

Remark 2

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

Theorem 4

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

0

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

0

$$igwedge_{n-k-1}(\mathscr{C}_{pub})^{\perp} = <\left(0\mid ec{h}
ight)oldsymbol{P}^{T}$$
 :

Remark 2

$$\dim \Lambda_{n-k-1}(\mathscr{C}_{pub}) = n-1 + Rank(X_2)$$

Theorem 4

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

•

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

0

$$egin{aligned} lacksquare _{n-k-1}(\mathscr{C}_{pub})^{ot} = <\left(0\mid ec{h}
ight)oldsymbol{P}^{oldsymbol{ au}} \end{aligned}$$

Remark 2

$$\dim \Lambda_{n-k-1}(\mathscr{C}_{pub}) = n-1 + Rank(X_2)$$

Theorem 4

If Rank
$$(X_2) = \ell$$
,

•

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

•

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

Summary

Compute

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

• If

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

- ullet Choose $ec{h} \in \Lambda_{n-k-1}(\mathscr{C}_{ extit{pub}})^{\perp}, \quad ec{h}
 eq \mathbf{0}$
- ullet Find $m{T}\in\mathsf{GL}_{n+\ell}(\mathbb{F}_q)$ such that $ec{h}=(m{0}\midec{h}')\,m{T},\ ec{h}'\in\mathbb{F}_{q^m}^n$

Easy: Linear algebra

Summary

Compute

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

If

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

- ullet Choose $ec{h} \in \Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp}, \quad ec{h}
 eq \mathbf{0}$
- $m{\phi}$ Find $m{T}\in\mathsf{GL}_{n+\ell}(\mathbb{F}_q)$ such that $ec{h}=(m{0}\midec{h}')m{T},\ ec{h}'\in\mathbb{F}_{q^m}^n$

Easy: Linear algebra

Summary

Compute

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

If

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

- ullet Choose $ec{h} \in \Lambda_{n-k-1}(\mathscr{C}_{pub})^{\perp}$, $ec{h}
 eq \mathbf{0}$
- ullet Find $m{T}\in\mathsf{GL}_{n+\ell}(\mathbb{F}_q)$ such that $ec{h}=(m{0}\midec{h}')\,m{T},\ ec{h}'\in\mathbb{F}_{q^m}^n$

Easy: Linear algebra

Summary

Compute

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

If

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

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

Easy: Linear algebra

Hervé Talé Kalachi

Remark 3

The success of this attack is based on two facts:

- $lackbox{0} lackbox{\textbf{\textit{P}}} \in \mathsf{GL}_{n+\ell}(lackbox{\mathbb{F}}_{oldsymbol{q}})$
- 2 X_2 must be a of full rank, $Rank(X_2) = \ell$

GPT Reparations

Reparation ideas linked to \boldsymbol{X}_2

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

4□▶
4□▶
4□▶
4□▶
4□▶
4□▶
4□
9
0

GPT Reparations

Reparation ideas linked to \boldsymbol{X}_2

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

Hervé Talé Kalachi June 25, 2021 17 /

RGH Reparation: Smart Approach '10

The Reparation is related to X

• In the Key generation, chose X_1 and such that

$$m{X}_1 = egin{pmatrix} b_1^{[0]} & \cdots & b_a^{[0]} \ dots & & dots \ b_1^{[k-1]} & \cdots & b_a^{[k-1]} \end{pmatrix}$$

- $X_2 \in \mathbb{F}_{q^m}^{k \times (\ell-a)}$
- $\bullet X = (X_1 \mid X_2)$

$$G_{pub} \stackrel{\text{def}}{=} S(X \mid G)P^{-1} = S(X_1 \mid X_2 \mid G)P^{-1}$$

Plan

GPT Cryptosystem and Variants

Polynomial Structural Attack

Conclusion and Related Work

$$m{G}_{ ext{pub}} = m{S} \left(egin{array}{ccccc} m{b}_{1}^{[0]} & \cdots & m{b}_{a}^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} & m{g}_{1}^{[0]} & \cdots & m{g}_{n}^{[0]} \\ dots & dots & dots & dots & dots & dots \\ m{b}_{1}^{[k-1]} & \cdots & m{b}_{a}^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} & m{g}_{1}^{[k-1]} & \cdots & m{g}_{n}^{[k-1]} \end{array}
ight) m{P}^{-1}$$

$$ullet$$
 Let $ec{g}' = \left(ec{b} \mid ec{g}
ight) \in \mathbb{F}_{q^m}^{a+n}$

$$\bullet \|\vec{g}'\|_q \geqslant \|\vec{g}\|_q = n$$

•
$$\|\vec{g}'\|_q = n + s \leqslant m$$
 with $s \leqslant a$.

•
$$\|(X_1 \mid G)\|_q = \|\vec{g}'\|_q = n + s$$

ullet There exists a matrix $oldsymbol{Q}\in\mathsf{GL}_{n+a}(\mathbb{F}_q)$ such that

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

ullet There exists a matrix $oldsymbol{T}\in\mathsf{GL}_{n+\ell}(\mathbb{F}_{\sigma})$

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

....b = $S(0 \mid X_2 \mid G^*) \ T^{-1}P^{-1}$

Hervé Talé Kalachi June 25, 2021 20/27

$$m{G}_{ ext{pub}} = m{S} \left(egin{array}{ccccc} m{b}_{1}^{[0]} & \cdots & m{b}_{a}^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} & m{g}_{1}^{[0]} & \cdots & m{g}_{n}^{[0]} \\ dots & dots & dots & dots & dots & dots \\ m{b}_{1}^{[k-1]} & \cdots & m{b}_{a}^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} & m{g}_{1}^{[k-1]} & \cdots & m{g}_{n}^{[k-1]} \end{array}
ight) m{P}^{-1}$$

- ullet Let $ec{g}' = \left(ec{b} \mid ec{g}
 ight) \in \mathbb{F}_{q^m}^{a+n}$
- $\bullet \|\vec{g}'\|_a \geqslant \|\vec{g}\|_a = n$
- $\|\vec{g}'\|_a = n + s \leqslant m$ with $s \leqslant a$.

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

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

 $_{\text{nub}} = S(0 \mid X_2 \mid G^*) T^{-1}P^{-1}$

Hervé Talé Kalachi

$$\boldsymbol{G}_{\mathrm{pub}} = \boldsymbol{S} \left(\begin{array}{cccc} b_{1}^{[0]} & \cdots & b_{a}^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} & g_{1}^{[0]} & \cdots & g_{n}^{[0]} \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ b_{1}^{[k-1]} & \cdots & b_{a}^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} & g_{1}^{[k-1]} & \cdots & g_{n}^{[k-1]} \end{array} \right) \boldsymbol{P}^{-1}$$

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

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

ullet There exists a matrix $oldsymbol{\mathcal{T}}\in\mathsf{GL}_{n+\ell}(\mathbb{F}_q)$

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

Hervé Talé Kalachi June 25. 2021 20 / 27

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

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

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

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

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

Hervé Talé Kalachi 20 / 27

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

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

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

• There exists a matrix $T \in GL_{n+\ell}(\mathbb{F}_a)$

$$(oldsymbol{X}_1 \mid oldsymbol{X}_2 \mid oldsymbol{G}) oldsymbol{T} = (oldsymbol{0} \mid oldsymbol{X}_2 \mid oldsymbol{G}^*)$$
 $oldsymbol{S}_{\mathrm{pub}} = oldsymbol{S} (oldsymbol{0} \mid oldsymbol{X}_2 \mid oldsymbol{G}^*) oldsymbol{T}^{-1} oldsymbol{P}^{-1}$

Hervé Talé Kalachi

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

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

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

ullet There exists a matrix $oldsymbol{\mathcal{T}}\in\mathsf{GL}_{n+\ell}(\mathbb{F}_q)$

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

 $\boldsymbol{G}_{\mathrm{pub}} = \boldsymbol{S} \left(\boldsymbol{0} \mid \boldsymbol{X}_{2} \mid \boldsymbol{G}^{*} \right) \boldsymbol{T}^{-1} \boldsymbol{P}^{-1}$

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

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

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

ullet There exists a matrix $oldsymbol{\mathcal{T}}\in\mathsf{GL}_{n+\ell}(\mathbb{F}_q)$

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

 $oldsymbol{G}_{ ext{pub}} = oldsymbol{\mathcal{S}}\left(oldsymbol{0} \mid oldsymbol{\mathcal{X}}_2 \mid oldsymbol{G}^*
ight) oldsymbol{\mathcal{T}}^{-1}oldsymbol{P}^{-1}$

4 D > 4 D > 4 E > 4 E > E 9 Q C

Hervé Talé Kalachi

$$m{G}_{ ext{pub}} = m{S} \left(egin{array}{ccccc} m{b}_{1}^{[0]} & \cdots & m{b}_{a}^{[0]} & & x_{21,1} & \cdots & x_{21,\ell-a} & m{g}_{1}^{[0]} & \cdots & m{g}_{n}^{[0]} \\ dots & & dots & & dots & & dots \\ m{b}_{1}^{[k-1]} & \cdots & m{b}_{a}^{[k-1]} & & x_{2k,1} & \cdots & x_{2k,\ell-a} & m{g}_{1}^{[k-1]} & \cdots & m{g}_{n}^{[k-1]} \end{array}
ight) m{P}^{-1}$$

Lemma 5

There exists

- $\mathbf{G}^* \in \mathbb{F}_{q^m}^{k \times (n+s)}$ generating a Gabidulin code
- $3 s \in \mathbb{N}$ s.t $0 \leqslant s \leqslant a$ and $n + s \leqslant m$.

such that

$$m{G}_{ ext{pub}} = m{S} \left(egin{array}{ccccc} m{b}_{1}^{[0]} & \cdots & m{b}_{a}^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} & m{g}_{1}^{[0]} & \cdots & m{g}_{n}^{[0]} \\ dots & dots & dots & dots & dots & dots \\ m{b}_{1}^{[k-1]} & \cdots & m{b}_{a}^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} & m{g}_{1}^{[k-1]} & \cdots & m{g}_{n}^{[k-1]} \end{array}
ight) m{P}^{-1}$$

Lemma 5

There exists

$$m{O}$$
 $m{P}^*\in\mathsf{GL}_{n+\ell}(\mathbb{F}_q)$

- **2** $G^* \in \mathbb{F}_{q^m}^{k \times (n+s)}$ generating a Gabidulin code

such that

Proposition 5

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

•
$$f = n + s - k$$

•
$$I = \{i_1, ..., i_w\} \subset \{1, 2, ..., n + \ell\}$$

$$\dim \Lambda_f(\mathscr{C}^J_{\text{pub}}) = n + s + \ell - s$$

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

Hervé Talé Kalachi

Proposition 5

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

Proposition 6

•
$$f = n + s - k$$

•
$$I = \{i_1, ..., i_w\} \subset \{1, 2, ..., n + \ell\}$$

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

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

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

Proposition 5

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

Proposition 6

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

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

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

Remark that for *I* that is not a "redundancy set",

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

Steps of the attack

• Eliminate a "redundancy set" by testing :

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

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

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

23 / 27

- Overbeck's Attack: Principal threat of Gabidulin-based Schemes
- Taking a special distortion matrix X might protect against it
- "Smart Approach" variant,

$$\mathbf{X} = \begin{pmatrix} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} \\ \vdots & & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} \end{pmatrix}$$

→ Global idea of our attack

 4 □ ▶

- **Overbeck's Attack**: Principal threat of Gabidulin-based Schemes
- Taking a special distortion matrix X might protect against it
- "Smart Approach" variant

$$X = \begin{pmatrix} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} \\ \vdots & & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} \end{pmatrix}$$

→ Global idea of our attack

 4 □ ▶

- **Overbeck's Attack**: Principal threat of Gabidulin-based Schemes
- Taking a special distortion matrix **X** might protect against it
- "Smart Approach" variant,

$$\mathbf{X} = \begin{pmatrix} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} \\ \vdots & & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} \end{pmatrix}$$

→ Global idea of our attack

Hervé Talé Kalachi

- Overbeck's Attack: Principal threat of Gabidulin-based Schemes
- Taking a special distortion matrix X might protect against it
- "Smart Approach" variant,

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

→ Global idea of our attack

	Matrix	Code generated	Length	Correction capability
Secret	G	$\mathscr{G}_{k}\left(\vec{g} ight)$	n	t
Public	$oldsymbol{G}_{ ext{pub}}$	$(n+\ell,k)$ —code	$n + \ell$	t

Hervé Talé Kalachi June 25, 2021 24/27

- Overbeck's Attack: Principal threat of Gabidulin-based Schemes
- Taking a special distortion matrix X might protect against it
- "Smart Approach" variant,

$$\mathbf{X} = \begin{pmatrix} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} \\ \vdots & & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} \end{pmatrix}$$

→ Global idea of our attack

	Matrix	Code generated	Length	Correction capability
Secret	G	$\mathscr{G}_{k}\left(ec{g} ight)$	п	t
		- K (8)		
Public	$oldsymbol{G}_{ ext{pub}}$	$(n+\ell,k)$ —code	$n + \ell$	t
A 1				

- Overbeck's Attack: Principal threat of Gabidulin-based Schemes
- Taking a special distortion matrix X might protect against it
- "Smart Approach" variant,

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

→ Global idea of our attack

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

- Overbeck's Attack: Principal threat of Gabidulin-based Schemes
- Taking a special distortion matrix X might protect against it
- "Smart Approach" variant,

$$X = \begin{pmatrix} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} \\ \vdots & & \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} \end{pmatrix}$$

→ Global idea of our attack

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

- Overbeck's Attack: Principal threat of Gabidulin-based Schemes
- Taking a special distortion matrix X might protect against it
- "Smart Approach" variant,

$$m{X} = \left(egin{array}{cccc} b_1^{[0]} & \cdots & b_a^{[0]} & x_{21,1} & \cdots & x_{21,\ell-a} \\ dots & & dots & dots & dots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} & x_{2k,1} & \cdots & x_{2k,\ell-a} \end{array}
ight)$$

→ Global idea of our attack

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

Hervé Talé Kalachi June 25. 2021 24/27

Plan

GPT Cryptosystem and Variants

Polynomial Structural Attack

Conclusion and Related Work

Code based encryption schemes

- Main drawback: Enormous size of the Keys
- Potential solution: Rank metric codes

Hervé Talé Kalachi June 25, 2021 26 / 27

Code based encryption schemes

- Main drawback: Enormous size of the Keys
- Potential solution: Rank metric codes
 - Gabidulin codes

--- Our works show that several attempts to mask them have failed

Hervé Talé Kalachi June 25, 2021 26 / 27

Code based encryption schemes

- Main drawback: Enormous size of the Keys
- Potential solution: Rank metric codes
 - Gabidulin codes

→ Our works show that several attempts to mask them have failed

Hervé Talé Kalachi June 25, 2021 26 / 27

Code based encryption schemes

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

→ Our works show that several attempts to mask them have failed

Hervé Talé Kalachi June 25, 2021 26 / 27

Code based encryption schemes

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

→ Our works show that several attempts to mask them have failed

Hervé Talé Kalachi June 25, 2021 26 / 27

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*