Rank Metric Trapdoor Functions with Homogeneous Errors

Étienne Burle, Philippe Gaborit, Younes Hatri, Ayoub Otmani

1 LITIS, University of Rouen Normandie, Normandie Univ, France
2 XLIM, Université de Limoges, France

Najac, 15/10/2023
Introduction

Context:

Code based post-quantum cryptography (NIST call)
Designing an injective one-way function based on rank metric linear codes

Main result:
Security relying on classical problems
For some parameters, public key statistically indistinguishable from a random matrix $2^{25}$
Introduction

Context:

• Code based post-quantum cryptography (NIST call)
Introduction

Context:

- Code based post-quantum cryptography (NIST call)
- Designing an injective one-way function based on rank metric linear codes
Introduction

Context:

- Code based post-quantum cryptography (NIST call)
- Designing an injective one-way function based on rank metric linear codes

Main result:
Introduction

Context:

• Code based post-quantum cryptography (NIST call)
• Designing an injective one-way function based on rank metric linear codes

Main result:

• Security relying on classical problems
Introduction

Context:

- Code based post-quantum cryptography (NIST call)
- Designing an injective one-way function based on rank metric linear codes

Main result:

- Security relying on classical problems
- For some parameters, public key statistically indistinguishable from a random matrix
1 Rank-based encryption schemes

2 One-way trapdoor function

3 Analysis and security of the scheme
1. Rank-based encryption schemes

2. One-way trapdoor function

3. Analysis and security of the scheme
Rank metric

\( \mathbb{F}_q \) : finite field of cardinality \( q \)
Rank metric

$\mathbb{F}_q$ : finite field of cardinality $q$

$\mathbb{F}_{q^m}$ : finite field of cardinality $q^m$ viewed as $\mathbb{F}_q$-vector space of dimension $m$
Rank metric

\( \mathbb{F}_q \): finite field of cardinality \( q \)

\( \mathbb{F}_{q^m} \): finite field of cardinality \( q^m \) viewed as \( \mathbb{F}_q \)-vector space of dimension \( m \)

\( x = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n \)
Rank metric

\( \mathbb{F}_q \): finite field of cardinality \( q \)

\( \mathbb{F}_{q^m} \): finite field of cardinality \( q^m \) viewed as \( \mathbb{F}_q \)-vector space of dimension \( m \)

\[ x = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n \]

- The support of \( x \) is \( \langle x_1, \ldots, x_n \rangle_{\mathbb{F}_q} \subset \mathbb{F}_{q^m} \), the sub-vector space of \( \mathbb{F}_{q^m} \) generated by its elements
Rank metric

\( \mathbb{F}_q \) : finite field of cardinality \( q \)

\( \mathbb{F}_{q^m} \) : finite field of cardinality \( q^m \) viewed as \( \mathbb{F}_q \)-vector space of dimension \( m \)

\[ \mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n \]

- The support of \( \mathbf{x} \) is \( \langle x_1, \ldots, x_n \rangle_{\mathbb{F}_q} \subset \mathbb{F}_{q^m} \), the sub-vector space of \( \mathbb{F}_{q^m} \) generated by its elements
- The rank of \( \mathbf{x} \) is the dimension of its support
Generic problem

Search Rank decoding

- $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$ a random matrix
- an integer $t > 0$
- $\mathbf{e} \in \mathbb{F}_{q^m}^n$ a random vector of rank $t$ called \textit{error vector}
Generic problem

**Search Rank decoding**

- \( \mathbf{H} \in \mathbb{F}_{q^m}^{(n-k) \times n} \) a random matrix
- an integer \( t > 0 \)
- \( \mathbf{e} \in \mathbb{F}_{q^m}^n \) a random vector of rank \( t \) called *error vector*

**Problem**: Given \((\mathbf{H}, \mathbf{eH}^T)\), recover \( \mathbf{e} \)
Search Rank decoding

- \( \mathbf{H} \in \mathbb{F}_{q^m}^{(n-k) \times n} \) a random matrix
- an integer \( t > 0 \)
- \( \mathbf{e} \in \mathbb{F}_{q^m}^n \) a random vector of rank \( t \) called *error vector*

**Problem**: Given \((\mathbf{H}, \mathbf{eH}^T)\), recover \( \mathbf{e} \)

**Remark**: Distinguishing \((\mathbf{H}, \mathbf{eH}^T)\) from \((\mathbf{H}, \mathbf{s})\) is the decision version of the problem
Generic problem

Search Rank decoding

- \( H \in \mathbb{F}_{q^m}^{(n-k) \times n} \) a random matrix
- an integer \( t > 0 \)
- \( e \in \mathbb{F}_{q^m}^n \) a random vector of rank \( t \) called error vector

**Problem**: Given \((H, eH^T)\), recover \( e \)

**Remark**: Distinguishing \((H, eH^T)\) from \((H, s)\) is the decision version of the problem

**Assumption**

*Decision version of rank decoding in as hard as search version*
Rank decoding’s hardness

Proposition

There is a probabilistic reduction from decoding in Hamming metric to rank decoding.¹


²Aragon, Gaborit, Hauteville, Tillich. *A new algorithm for solving the rank syndrome decoding problem*, ISIT 2018

³Bardet, Briaud, Bros, Gaborit, Tillich. *Revisiting algebraic attacks on MinRank and on the rank decoding problem*, 2022
Rank decoding’s hardness

**Proposition**

There is a probabilistic reduction from decoding in Hamming metric to rank decoding.\(^1\)

<table>
<thead>
<tr>
<th>Combinatorial attacks(^2)</th>
<th>Algebraic attacks (^3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(O\left((n-k)^3 m^3 q^{w \frac{(k+1)m}{n} - m}\right))</td>
<td>Exponential</td>
</tr>
</tbody>
</table>

---

\(^1\) Gaborit, Zemor. *On the hardness of the decoding and the minimum distance problems for rank codes*, ISIT 2016.

\(^2\) Aragon, Gaborit, Hauteville, Tillich. *A new algorithm for solving the rank syndrome decoding problem*, ISIT 2018

\(^3\) Bardet, Briaud, Bros, Gaborit, Tillich. *Revisiting algebraic attacks on MinRank and on the rank decoding problem*, 2022
### Encryption schemes relying on rank decoding

<table>
<thead>
<tr>
<th>Description</th>
<th>Transformed code</th>
<th>Hidden structure</th>
<th>Ciphertext in two parts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(G \rightarrow \text{SGT})</td>
<td>(G \rightarrow \text{SG})</td>
<td>((C_1, C_2) : C_2 - C_1 V = mG + e)</td>
</tr>
<tr>
<td>Used code</td>
<td>Gabidulin</td>
<td>Ideal LRPC</td>
<td>Gabidulin</td>
</tr>
<tr>
<td>Schemes</td>
<td>1991 GPT(^4)</td>
<td>2019 ROLLO</td>
<td>2020 RQC</td>
</tr>
<tr>
<td></td>
<td>2017 Loidreau</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security problems</td>
<td>RD</td>
<td>IRD</td>
<td>IRD</td>
</tr>
<tr>
<td></td>
<td>IfRD</td>
<td>IfRD</td>
<td></td>
</tr>
</tbody>
</table>

RD : Rank decoding, IRD: Ideal rank decoding, IfRC: Indistinguishability from a random code

\(^4\)Gabidulin, Paramonov, Tretjakov
New generic problem

Rank support learning (RSL)

- \(H \in \mathbb{F}_{q^m}^{(n-k) \times n}\) a random matrix
- an integer \(t > 0\)
- \(E \in \mathbb{F}_{q^m}^{n \times N}\) a random matrix such that the \(\mathbb{F}_q\)-vector space \(\mathcal{E}\) generated by its entries is of dimension \(t\)
New generic problem

Rank support learning (RSL)

- \( H \in \mathbb{F}_{q^m}^{(n-k) \times n} \) a random matrix
- an integer \( t > 0 \)
- \( E \in \mathbb{F}_{q^m}^{n \times N} \) a random matrix such that the \( \mathbb{F}_q \)-vector space \( E \) generated by its entries is of dimension \( t \)

**Problem** : Given \((H, HE)\), recover \( E \)
New generic problem

**Rank support learning (RSL)**

- \( H \in \mathbb{F}_{q^m}^{(n-k) \times n} \) a random matrix
- an integer \( t > 0 \)
- \( E \in \mathbb{F}_{q^m}^{n \times N} \) a random matrix such that the \( \mathbb{F}_q \)-vector space \( E \) generated by its entries is of dimension \( t \)

**Problem**: Given \((H, HE)\), recover \( E \)

**Remark**: \( E \) is homogeneous of degree \( t \) with support \( E \)
New generic problem

**Rank support learning (RSL)**

- $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$ a random matrix
- an integer $t > 0$
- $\mathbf{E} \in \mathbb{F}_{q^m}^{n \times N}$ a random matrix such that the $\mathbb{F}_q$-vector space $\mathcal{E}$ generated by its entries is of dimension $t$

**Problem** : Given $(\mathbf{H}, \mathbf{HE})$, recover $\mathcal{E}$

**Remark** : $\mathbf{E}$ is homogeneous of degree $t$ with support $\mathcal{E}$

**Assumption**

*Rank support learning is as hard as rank decoding if $N < kt$.***
Attacks on rank support learning

<table>
<thead>
<tr>
<th>Year</th>
<th>Nature</th>
<th>Complexity</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>Combinatorial</td>
<td>Poly</td>
<td>$N \geq nt$</td>
</tr>
</tbody>
</table>

---

5. Gaborit, Hauteville, Phan, Tillich. *Identity-based encryption from rank metric*, CRYPTO2017

6. Debris-Alazard, Tillich. *Two attacks on rank metric code-based schemes: Ranksign and an identity-based encryption scheme* ASIACRYPT 2018

7. Bardet, Briaud. *An algebraic approach to the rank support learning problem*, PQCrypto2021

8. Bidoux, Briaud, Bros, Gaborit. *RQC revisited and more cryptanalysis for rank-based cryptography*, 2022
## Attacks on rank support learning

<table>
<thead>
<tr>
<th>Year</th>
<th>Nature</th>
<th>Complexity</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>Combinatorial</td>
<td>Poly</td>
<td>$N \geq nt$</td>
</tr>
<tr>
<td>2018</td>
<td>Algebraic</td>
<td>Sub-exp</td>
<td>$N &gt; kt$</td>
</tr>
</tbody>
</table>

---

5. Gaborit, Hauteville, Phan, Tillich. *Identity-based encryption from rank metric*, CRYPTO2017


7. Bardet, Briaud. *An algebraic approach to the rank support learning problem*, PQCrypto2021

8. Bidoux, Briaud, Bros, Gaborit. *RQC revisited and more cryptanalysis for rank-based cryptography*, 2022
Attacks on rank support learning

<table>
<thead>
<tr>
<th>Year</th>
<th>Nature</th>
<th>Complexity</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>Combinatorial</td>
<td>Poly</td>
<td>$N \geq nt$</td>
</tr>
<tr>
<td>2018</td>
<td>Algebraic</td>
<td>Sub-exp</td>
<td>$N &gt; kt$</td>
</tr>
<tr>
<td>2021</td>
<td>Algebraic</td>
<td>Exp</td>
<td>Thwarted when $N &lt; kt$</td>
</tr>
</tbody>
</table>

---

5 Gaborit, Hauteville, Phan, Tillich. *Identity-based encryption from rank metric*, CRYPTO2017
6 Debris-Alazard, Tillich. *Two attacks on rank metric code-based schemes: Ranksign and an identity-based encryption scheme* ASIACRYPT 2018
7 Bardet, Briaud. *An algebraic approach to the rank support learning problem*, PQCrypto2021
8 Bidoux, Briaud, Bros, Gaborit. *RQC revisited and more cryptanalysis for rank-based cryptography*, 2022
# Attacks on rank support learning

<table>
<thead>
<tr>
<th>Year</th>
<th>Nature</th>
<th>Complexity</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>Combinatorial</td>
<td>Poly</td>
<td>( N \geq nt )</td>
</tr>
<tr>
<td>2018</td>
<td>Algebraic</td>
<td>Sub-exp</td>
<td>( N &gt; kt )</td>
</tr>
<tr>
<td>2021</td>
<td>Algebraic</td>
<td>Exp</td>
<td>Thwarted when ( N &lt; kt )</td>
</tr>
<tr>
<td>2022</td>
<td>Combinatorial</td>
<td>Poly</td>
<td>( N &gt; ktm/(m-t) )</td>
</tr>
</tbody>
</table>

---

5 Gaborit, Hauteville, Phan, Tillich. *Identity-based encryption from rank metric*, CRYPTO2017

6 Debris-Alazard, Tillich. *Two attacks on rank metric code-based schemes: Ranksign and an identity-based encryption scheme* ASIACRYPT 2018

7 Bardet, Briaud. *An algebraic approach to the rank support learning problem*, PQCrypto2021

8 Bidoux, Briaud, Bros, Gaborit. *RQC revisited and more cryptanalysis for rank-based cryptography*, 2022
## RSL-based encryption schemes

<table>
<thead>
<tr>
<th>Description</th>
<th>Transformed code</th>
<th>Hidden structure</th>
<th>Ciphertext in two parts</th>
</tr>
</thead>
<tbody>
<tr>
<td>G → SGT</td>
<td>G → SG</td>
<td>(C₁, C₂) :</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C₂ − C₁V = mG + E</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Used code</th>
<th>Gabidulin</th>
<th>LRPC</th>
<th>Gabidulin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schemes</td>
<td>2022 LowMS</td>
<td>2022⁹</td>
<td>2019 Li-Ping Wang</td>
</tr>
<tr>
<td>Security problems</td>
<td>RSL</td>
<td>RSL</td>
<td>RSL</td>
</tr>
<tr>
<td></td>
<td>IfRD</td>
<td>IfRD</td>
<td></td>
</tr>
</tbody>
</table>

**RSL**: Rank syndrome learning,  
**IfRC**: Indistinguishability from a random code

---

⁹ Aguilar-Melchor, Aragon, Dyseryn, Gaborit, and Zémor. *LRPC codes with multiple syndromes: near ideal-size KEMs without ideals*
Our scheme

Uses a generalisation of LRPC codes (that can only decode multiple syndromes) with semi-homogeneous matrices.
Our scheme

Uses a generalisation of LRPC codes (that can only decode multiple syndromes) with semi-homogeneous matrices.

Definitions

$\mathbf{H} \in \mathbb{F}_{q^m}^{\ell \times n}$ is homogeneous of weight $w$ if the support of the hole matrix is of low dimension $w$ (used in LRPC).
Our scheme

Uses a generalisation of LRPC codes (that can only decode multiple syndromes) with semi-homogeneous matrices.

Definitions

\( H \in \mathbb{F}_{q^m}^{\ell \times n} \) is homogeneous of weight \( w \) if the support of the hole matrix is of low dimension \( w \) (used in LRPC).

\( H \in \mathbb{F}_{q^m}^{\ell \times n} \) is semi-homogeneous of weight \( w \) if the support of each of its rows is of low dimension \( w \).
Our scheme

Uses a generalisation of LRPC codes (that can only decode multiple syndromes) with semi-homogeneous matrices.

Definitions

\( H \in \mathbb{F}_{q^m}^{\ell \times n} \) is homogeneous of weight \( w \) if the support of the hole matrix is of low dimension \( w \) (used in LRPC).

\( H \in \mathbb{F}_{q^m}^{\ell \times n} \) is semi-homogeneous of weight \( w \) if the support of each of its rows is of low dimension \( w \).

The support of \( H \) is \( (W_1, \ldots, W_\ell) \), where \( W_i \) is the support of its \( i \)-th row.
Our scheme

Uses a generalisation of LRPC codes (that can only decode multiple syndromes) with semi-homogeneous matrices.

<table>
<thead>
<tr>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbf{H} \in \mathbb{F}^{\ell \times n}_{q^m} ) is homogeneous of weight ( w ) if the support of the hole matrix is of low dimension ( w ) (used in LRPC).</td>
</tr>
<tr>
<td>( \mathbf{H} \in \mathbb{F}^{\ell \times n}_{q^m} ) is semi-homogeneous of weight ( w ) if the support of each of its rows is of low dimension ( w ).</td>
</tr>
<tr>
<td>The support of ( \mathbf{H} ) is ( (W_1, \ldots, W_\ell) ), where ( W_i ) is the support of its ( i )-th row.</td>
</tr>
</tbody>
</table>

- Use of a transformed code
Our scheme

Uses a generalisation of LRPC codes (that can only decode multiple syndromes) with semi-homogeneous matrices.

Definitions

$H \in \mathbb{F}_{q^m}^{\ell \times n}$ is homogeneous of weight $w$ if the support of the hole matrix is of low dimension $w$ (used in LRPC).

$H \in \mathbb{F}_{q^m}^{\ell \times n}$ is semi-homogeneous of weight $w$ if the support of each of its rows is of low dimension $w$.

The support of $H$ is $(W_1, \ldots, W_\ell)$, where $W_i$ is the support of its $i$-th row.

- Use of a transformed code
- Security relying on Rank decoding and RSL only
1 Rank-based encryption schemes

2 One-way trapdoor function

3 Analysis and security of the scheme
Construction of trapdoor function

\[
x \quad \xrightarrow{E} \quad f(x) \quad \xleftarrow{H} \quad x
\]

Easy with \( tk \)
Construction of trapdoor function

Three polynomial-time algorithms: \((Gen, Eval, Invert)\)
Construction of trapdoor function

Three polynomial-time algorithms: \((Gen, Eval, Invert)\)

1. \(pk, tk \leftarrow Gen(1^\lambda)\)
Construction of trapdoor function

Three polynomial-time algorithms: \((Gen, Eval, Invert)\)

1. \(pk, tk \leftarrow Gen(1^\lambda)\)

2. \(Eval(pk, x)\) will evaluate with public key \(pk\) in \(x\)
Construction of trapdoor function

Three polynomial-time algorithms: \((\text{Gen}, \text{Eval}, \text{Invert})\)

1. \(pk, tk \leftarrow \text{Gen}(1^\lambda)\)

2. \(\text{Eval}(pk, x)\) will evaluate with public key \(pk\) in \(x\)

3. \(\text{Invert}(tk, \text{Eval}(pk, x))\) returns \(x\) with overwhelming probability
Gen

$R \leftarrow \mathbb{F}_k \times_L \mathbb{L}$

Remark: $G(W, I_n) = 0$
Rank Metric
Trapdoor
Functions with
Homogeneous
Errors

Étienne Burle,
Philippe
Gaborit,
Younes Hatri,
Ayoub Otmani

Rank-based
encryption
schemes

One-way
trapdoor
function

Analysis and
security of the
scheme

Gen

1. \( R \leftarrow F_{q^m}^{k \times L} \)
2. \( W \leftarrow F_{q^m}^{n \times L} : \text{semi-homogeneous of weight } w \)
Rank Metric Trapdoor Functions with Homogeneous Errors

Étienne Burle, Philippe Gaborit, Younes Hatri, Ayoub Otmani

Rank-based encryption schemes
One-way trapdoor function
Analysis and security of the scheme

Gen

1. $R \leftarrow \mathbb{F}_{q^m}^{k \times L}$
2. $W \leftarrow \mathbb{F}_{q^m}^{n \times L}$: semi-homogeneous of weight $w$
3. Return $(R | - RW^T), W$
Rank Metric Trapdoor Functions with Homogeneous Errors

Étienne Burle, Philippe Gaborit, Younes Hatri, Ayoub Otmani

Rank-based encryption schemes
One-way trapdoor function
Analysis and security of the scheme

Gen

1. $R \leftarrow \mathbb{F}_{q^m}^{k \times L}$
2. $W \leftarrow \mathbb{F}_{q^m}^{n \times L}$ : semi-homogeneous of weight $w$
3. Return $(R \mid - RW^T), W$

Public key : $G = (R \mid - RW^T) \in \mathbb{F}_{q^m}^{k \times (n+L)}$
Étienne Burle, Philippe Gaborit, Younes Hatri, Ayoub Otmani

Rank-based encryption schemes
One-way trapdoor function
Analysis and security of the scheme

Rank Metric Trapdoor Functions with Homogeneous Errors

\[ \text{Gen} \]

1. \( R \leftarrow \mathbb{F}_{q^m}^{k \times L} \)
2. \( W \leftarrow \mathbb{F}_{q^m}^{n \times L} : \text{semi-homogeneous of weight } w \)
3. Return \((R | - RW^T), W\)

**Public key** : \( G = (R | - RW^T) \in \mathbb{F}_{q^m}^{k \times (n+L)} \)

**Secret key** : \( W \)
Rank Metric Trapdoor Functions with Homogeneous Errors

Étienne Burle, Philippe Gaborit, Younes Hatri, Ayoub Otmani

Rank-based encryption schemes
One-way trapdoor function
Analysis and security of the scheme

\[ \text{Gen} \]

1. \( R \leftarrow F_{q^m}^{k \times L} \)
2. \( W \leftarrow F_{q^m}^{n \times L} : \text{semi-homogeneous of weight } w \)
3. Return \((R| - RW^\top), W\)

Public key: \( G = (R| - RW^\top) \in F_{q^m}^{k \times (n+L)} \)

Secret key: \( W \)

Remark: \( G(W, I_n)^\top = 0 \)
Rank Metric
Trapdoor Functions with Homogeneous Errors

Étienne Burle, Philippe Gaborit, Younes Hatri, Ayoub Otmani

Rank-based encryption schemes
One-way trapdoor function
Analysis and security of the scheme

Public key: $G$

Eval
Eval

Public key : \( G \)

1. \( X \in \mathbb{F}_{q^m}^{N \times k} : \) input

Public key : \( G \)

\[ \text{Eval} \]

Public key : \( G \)

1. \( X \in \mathbb{F}_{q^m}^{N \times k} : \) input
Public key: \( G \)

1. \( X \in \mathbb{F}_{q^m}^{N \times k} \) : input
2. \( E \leftarrow \mathbb{F}_{q^m}^{N \times (n+L)} \) homogeneous of weight \( t \)
Eval

Public key: $G$

1. $X \in \mathbb{F}_{q^m}^{N \times k}$: input

2. $E \leftarrow \mathbb{F}_{q^m}^{N \times (n+L)}$ homogeneous of weight $t$

3. Compute and return the output

$$C = XG + E$$
Invert

Secret key: $W$

---

Rank Metric Trapdoor Functions with Homogeneous Errors

Étienne Burle, Philippe Gaborit, Younes Hatri, Ayoub Otmani

Rank-based encryption schemes

One-way trapdoor function

Analysis and security of the scheme
Invert

Secret key : $\mathbf{W}$

1. $\mathbf{C} = \mathbf{XG} + \mathbf{E} : \text{input}$
$C = XG + E$ : input

2. Compute $C(W, I_n)^T = (XG + E)(W, I_n)^T$
   
   $= XG(W, I_n)^T + E(W, I_n)^T$
   
   $= E(W, I_n)^T$
Invert

Secret key: \( W \)

1. \( C = XG + E : \text{input} \)

2. Compute \( C(W, I_n)^T = (XG + E)(W, I_n)^T \)
   \[ = XG(W, I_n)^T + E(W, I_n)^T \]
   \[ = E(W, I_n)^T \]

3. Recover \( E \) with \textit{Homogeneous error decoding}
Invert

Secret key : \mathbf{W}

1. \textbf{C} = \mathbf{XG} + \mathbf{E} : \textit{input}

2. Compute \( \mathbf{C(W, I_n)^T} = (\mathbf{XG} + \mathbf{E})(\mathbf{W, I_n)^T} \)
   
   \[ = \mathbf{XG(W, I_n)^T} + \mathbf{E(W, I_n)^T} \]
   
   \[ = \mathbf{E(W, I_n)^T} \]

3. Recover \(\mathbf{E}\) with \textit{Homogeneous error decoding}

4. Compute \( \mathbf{C - E = XG} \) and recover \(\mathbf{X}\) with linear algebra
Invert

Secret key: \( W \)

1. \( C = XG + E : \text{input} \)

2. Compute \( C(W, I_n)^T = (XG + E)(W, I_n)^T \)
   \[ = XG(W, I_n)^T + E(W, I_n)^T \]
   \[ = E(W, I_n)^T \]

3. Recover \( E \) with \textit{Homogeneous error decoding}.

4. Compute \( C - E = XG \) and recover \( X \) with linear algebra.

5. Return \( (X, E) \).
Homogeneous error decoding

- \( H \in \mathbb{F}_{q^m}^{\ell \times n} \) semi-homogeneous of weight \( w \) and support \( (W_1, \ldots, W_\ell) \)
- An integer \( t > 0 \)
- \( S \in \mathbb{F}_{q^m}^{\ell \times N} \)
Homogeneous error decoding

- \( H \in \mathbb{F}_{q^m}^{\ell \times n} \) semi-homogeneous of weight \( w \) and support \((W_1, \ldots, W_\ell)\)
- An integer \( t > 0 \)
- \( S \in \mathbb{F}_{q^m}^{\ell \times N} \)

Recover \( E \) homogeneous of weight \( t \) from \( HE = S \)
Homogeneous error decoding

- $H \in \mathbb{F}_{q^m}^{\ell \times n}$ semi-homogeneous of weight $w$ and support $(W_1, \ldots, W_{\ell})$
- An integer $t > 0$
- $S \in \mathbb{F}_{q^m}^{\ell \times N}$

Recover $E$ homogeneous of weight $t$ from $HE = S$

**Theorem (Burle, Gaborit, Hartri, Otmani)**

If $N \geq wt$ and $\ell w \geq n$, there is a polynomial time algorithm that recovers $E$ with a failure probability upper bounded by

$$
\left(1 - \prod_{i=0}^{tw-1} (1 - q^{i-N}) + \frac{q^{2(w-1)t}}{q^m-q^{t-1}}\right)^{\ell} + 1 - \left(1 - \frac{q^{tw}}{q^m-q^{t-1}}\right)^{\ell}
$$
Homogeneous error decoding

- \( \mathbf{H} \in \mathbb{F}_{q^m}^{\ell \times n} \) semi-homogeneous of weight \( w \) and support \((W_1, \ldots, W_\ell)\)
- An integer \( t > 0 \)
- \( \mathbf{S} \in \mathbb{F}_{q^m}^{\ell \times N} \)

Recover \( \mathbf{E} \) homogeneous of weight \( t \) from \( \mathbf{HE} = \mathbf{S} \)

**Theorem (Burle, Gaborit, Hatri, Otmani)**

If \( N \geq wt \) and \( \ell w \geq n \), there is a polynomial time algorithm that recovers \( \mathbf{E} \) with a failure probability upper bounded by

\[
(1 - \prod_{i=0}^{tw-1} (1 - q^i - N) + \frac{q^{2(w-1)t}}{q^m - q^{t-1}})^\ell + 1 - \left(1 - \frac{q^{tw}}{q^m - q^{t-1}}\right)^\ell
\]

Asymptotically equivalent to \( \ell q^{tw-m} \)
Homogeneous error decoding

\[ HE = S \]
Homogeneous error decoding

\[ HE = S \]

1. Considering \( h_i \) and \( s_i \) the \( i \)-th row of \( H \) and \( S \), we have the equation \( h_i E = s_i \).
Homogeneous error decoding

\( HE = S \)

Considering \( h_i \) and \( s_i \) the \( i \)-th row of \( H \) and \( S \), we have the equation \( h_i E = s_i \).

- \( W_i \): support of \( h_i \)
Homogeneous error decoding

\[ HE = S \]

1. Considering \( h_i \) and \( s_i \) the \( i \)-th row of \( H \) and \( S \), we have the equation \( h_iE = s_i \).
   - \( W_i \) : support of \( h_i \)
   - \( E \) : support of \( E \)
Homogeneous error decoding

\[ HE = S \]

1. Considering \( h_i \) and \( s_i \) the \( i \)-th row of \( H \) and \( S \), we have the equation \( h_iE = s_i \).
   - \( W_i \) : support of \( h_i \)
   - \( E \) : support of \( E \)
   - \( s_i \in \mathbb{F}_q^N \) seen as a sample of \( N \) elements that generates \( W_i \cdot E \) (with \( E \cdot F := \langle ef \mid e \in E, f \in F \rangle_{\mathbb{F}_q} \))
Homogeneous error decoding

\[ HE = S \]

1. Considering \( \mathbf{h}_i \) and \( s_i \) the \( i \)-th row of \( \mathbf{H} \) and \( \mathbf{S} \), we have the equation \( \mathbf{h}_i \mathbf{E} = s_i \).

   - \( W_i \) : support of \( \mathbf{h}_i \)
   - \( \mathbf{E} \) : support of \( \mathbf{E} \)
   - \( s_i \in \mathbb{F}_{q^m}^N \) seen as a sample of \( N \) elements that generates \( W_i \cdot \mathbf{E} \) (with \( E \cdot F : = \langle ef | e \in E, f \in F \rangle_{\mathbb{F}_q} \) \( \rightarrow N \geq tw \))
Homogeneous error decoding

\[ \text{HE} = S \]

Considering \( h_i \) and \( s_i \) the \( i \)-th row of \( H \) and \( S \), we have the equation \( h_i \cdot E = s_i \).

- \( W_i \): support of \( h_i \)
- \( \mathcal{E} \): support of \( E \)
- \( s_i \in \mathbb{F}_{q^m}^N \) seen as a sample of \( N \) elements that generates \( W_i \cdot \mathcal{E} \) (with \( E \cdot F := \langle ef | e \in E, f \in F \rangle_{\mathbb{F}_q} \) \( \rightarrow N \geq tw \))

Recover \( \mathcal{E} \) with \( s_i \) and \( W_i \) of basis \( (f_1 \ldots f_w) \):
Homogeneous error decoding

\[
\text{HE} = S
\]

Considering \( h_i \) and \( s_i \) the \( i \)-th row of \( H \) and \( S \), we have the equation \( h_i E = s_i \).

- \( W_i \) : support of \( h_i \)
- \( E \) : support of \( E \)
- \( s_i \in \mathbb{F}_{q^m}^N \) seen as a sample of \( N \) elements that generates \( W_i \cdot E \) (with \( E \cdot F := \langle ef | e \in E, f \in F \rangle_{\mathbb{F}_q} \) \( \rightarrow N \geq tw \))

Recover \( E \) with \( s_i \) and \( W_i \) of basis \( (f_1 \ldots f_w) \):

\[
\bigcap f_j^{-1}(W_i \cdot E)
\]
Homogeneous error decoding

\[ HE = S \]

1. Considering \( h_i \) and \( s_i \) the \( i \)-th row of \( H \) and \( S \), we have the equation \( h_i E = s_i \).
   - \( W_i \) : support of \( h_i \)
   - \( E \) : support of \( E \)
   - \( s_i \in \mathbb{F}_q^N \) seen as a sample of \( N \) elements that generates \( W_i \cdot E \) (with \( E \cdot F := \langle ef | e \in E, f \in F >_{\mathbb{F}_q} \) \( \rightarrow N \geq tw \))

   Recover \( E \) with \( s_i \) and \( W_i \) of basis \((f_1 \ldots f_w)\):
   \[ \bigcap f_j^{-1}(W_i \cdot E) \]

2. \( E \) can then be recovered solving \( N \) linear systems with \( \ell tw \) equations and \( nt \) unknowns
Homogeneous error decoding

\[ \text{HE} = \text{S} \]

1. Considering \( \mathbf{h}_i \) and \( s_i \) the \( i \)-th row of \( \mathbf{H} \) and \( \mathbf{S} \), we have the equation \( \mathbf{h}_i \mathbf{E} = s_i \).
   - \( W_i \) : support of \( \mathbf{h}_i \)
   - \( \mathcal{E} \) : support of \( \mathbf{E} \)
   - \( s_i \in \mathbb{F}_{q^m}^N \) seen as a sample of \( N \) elements that generates \( W_i \cdot \mathcal{E} \) (with \( E \cdot F := \langle ef | e \in E, f \in F \rangle_{\mathbb{F}_q} \) \( \rightarrow N \geq tw \))

Recover \( \mathcal{E} \) with \( s_i \) and \( W_i \) of basis \((f_1 \ldots f_w)\):

\[ \bigcap f_j^{-1}(W_i \cdot \mathcal{E}) \]

2. \( \mathbf{E} \) can then be recovered solving \( N \) linear systems with \( \ell tw \) equations and \( nt \) unknowns \( \rightarrow \ell w \geq n \)
1 Rank-based encryption schemes

2 One-way trapdoor function

3 Analysis and security of the scheme
Security of the scheme

\[ G = (R | - RW^T) \]

Various aspects of security rely on classical problems:

- Inversion of the function: Rank Support Learning (Recover \( X \) and \( E \) from \( XG + E \))
- Recovery of the trapdoor: Search Rank Decoding (Recover \( W \) from \( G \))
- Indistinguishability of \( G \) from a random matrix: Decision Rank Decoding \( \Rightarrow \) \( G \) computationally indistinguishable from a uniform matrix
Security of the scheme

\[ G = (R| - RW^T) \]

Various aspects of security rely on classical problems:

- Inversion of the function: *Rank Support Learning* (Recover X and E from XG + E)
Security of the scheme

\[ G = (R| - RW^T) \]

Various aspects of security rely on classical problems:

- Inversion of the function: \textit{Rank Support Learning} (Recover \(X\) and \(E\) from \(XG + E\))

- Recovery of the trapdoor: \textit{Search Rank Decoding} (Recover \(W\) from \(G\))
Security of the scheme

\[ G = (R| - RW^T) \]

Various aspects of security rely on classical problems:

- Inversion of the function: \textit{Rank Support Learning} (Recover \( X \) and \( E \) from \( XG + E \))
- Recovery of the trapdoor: \textit{Search Rank Decoding} (Recover \( W \) from \( G \))
- Indistinguishability of \( G \) from a random matrix: \textit{Decision Rank Decoding}
Security of the scheme

\[ G = (R| - RW^T) \]

Various aspects of security rely on classical problems:

- Inversion of the function: *Rank Support Learning* 
  (Recover \( X \) and \( E \) from \( XG + E \))

- Recovery of the trapdoor: *Search Rank Decoding* 
  (Recover \( W \) from \( G \))

- Indistinguishability of \( G \) from a random matrix: *Decision Rank Decoding*
  \[ \Rightarrow G \text{ computationally indistinguishable from a uniform matrix} \]
Parameters

<table>
<thead>
<tr>
<th>$\lambda$</th>
<th>$m$</th>
<th>$L$</th>
<th>$k$</th>
<th>$n$</th>
<th>$w$</th>
<th>$t$</th>
<th>$N$</th>
<th>$\text{pk}$</th>
<th>$\text{ct}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>179</td>
<td>37</td>
<td>16</td>
<td>163</td>
<td>6</td>
<td>14</td>
<td>84</td>
<td>64</td>
<td>367</td>
</tr>
<tr>
<td>128</td>
<td>293</td>
<td>43</td>
<td>20</td>
<td>261</td>
<td>8</td>
<td>19</td>
<td>153</td>
<td>203</td>
<td>1,664</td>
</tr>
<tr>
<td>192</td>
<td>443</td>
<td>59</td>
<td>27</td>
<td>391</td>
<td>9</td>
<td>26</td>
<td>237</td>
<td>618</td>
<td>5,694</td>
</tr>
<tr>
<td>256</td>
<td>409</td>
<td>200</td>
<td>33</td>
<td>521</td>
<td>4</td>
<td>32</td>
<td>128</td>
<td>1,134</td>
<td>4,608</td>
</tr>
</tbody>
</table>

Table: $q = 2$, sizes of public key and ciphertext are in KB, probability of error $< 2^{-\lambda}$
Rank Metric
Trapdoor Functions with Homogeneous Errors

Étienne Burle, Philippe Gaborit, Younes Hatri, Ayoub Otmani

Rank-based encryption schemes
One-way trapdoor function
Analysis and security of the scheme

Parameters

<table>
<thead>
<tr>
<th></th>
<th>m</th>
<th>L</th>
<th>k</th>
<th>n</th>
<th>w</th>
<th>t</th>
<th>N</th>
<th>pk</th>
<th>ct</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>179</td>
<td>37</td>
<td>16</td>
<td>163</td>
<td>6</td>
<td>14</td>
<td>84</td>
<td>64</td>
<td>367</td>
</tr>
<tr>
<td>128</td>
<td>293</td>
<td>43</td>
<td>20</td>
<td>261</td>
<td>8</td>
<td>19</td>
<td>153</td>
<td>203</td>
<td>1,664</td>
</tr>
<tr>
<td>192</td>
<td>443</td>
<td>59</td>
<td>27</td>
<td>391</td>
<td>9</td>
<td>26</td>
<td>237</td>
<td>618</td>
<td>5,694</td>
</tr>
<tr>
<td>256</td>
<td>409</td>
<td>200</td>
<td>33</td>
<td>521</td>
<td>4</td>
<td>32</td>
<td>128</td>
<td>1,134</td>
<td>4,608</td>
</tr>
</tbody>
</table>

Table: $q = 2$, sizes of public key and ciphertext are in KB, probability of error $< 2^{-\lambda}$

<table>
<thead>
<tr>
<th>Security</th>
<th>pkSize (KB)</th>
<th>ctSize (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>1.90</td>
<td>2.04</td>
</tr>
<tr>
<td>192</td>
<td>2.29</td>
<td>2.41</td>
</tr>
<tr>
<td>256</td>
<td>2.50</td>
<td>2.63</td>
</tr>
</tbody>
</table>

Table: ROLLO encryption parameters
Other property on $G$

$$G = (R | - RW^T)$$

$S_w \left( \mathbb{F}_{q^m}^L \right)$: set of vectors of length $L$ and rank $w$
Other property on $G$

$$G = (R | - RW^T)$$

Theorem (Burle, Gaborit, Hartri, Otmani)

The statistical distance between $G$ and a uniformly random matrix in $\mathbb{F}_{q^m}^{k \times (n+L)}$ is

$$\leq \frac{n}{2} \sqrt{\frac{q^{mk}}{S_w(\mathbb{F}_{q^m}^L)}}$$

---

$S_w(\mathbb{F}_{q^m}^L)$ : set of vectors of length $L$ and rank $w$
Other property on $\mathbf{G}$

$\mathbf{G} = (\mathbf{R} | - \mathbf{RW}^T)$

Theorem (Burle, Gaborit, Hartri, Otmani)

The statistical distance between $\mathbf{G}$ and a uniformly random matrix in $\mathbb{F}_{q^m}^{k \times (n+L)}$ is 

$$\leq \frac{n}{2} \sqrt[ q^{mk} ]{ S_w(\mathbb{F}_q^L) }$$

→ proved with generalized Leftover Hash Lemma

$S_w(\mathbb{F}_q^L)$: set of vectors of length $L$ and rank $w$
Rank Metric Trapdoor Functions with Homogeneous Errors

Étienne Burle, Philippe Gaborit, Younes Hatri, Ayoub Otmani

Rank-based encryption schemes
One-way trapdoor function
Analysis and security of the scheme

Other property on $G$

$$G = (R | -RW^T)$$

Theorem (Burle, Gaborit, Hartri, Otmani)

The statistical distance between $G$ and a uniformly random matrix in $\mathbb{F}_{q^m}^{k \times (n+L)}$ is

$$\leq \frac{n}{2} \sqrt{\frac{q^{mk}}{S_w(\mathbb{F}_q^L)}}$$

→ proved with generalized Leftover Hash Lemma

New condition:

Choose parameters in order to have this distance $< 2^{-\lambda}$:

$G$ statistically indistinguishable from uniform

$S_w(\mathbb{F}_q^L)$: set of vectors of length $L$ and rank $w$
Statistically indistinguishable parameters

<table>
<thead>
<tr>
<th>$\lambda$</th>
<th>$m$</th>
<th>$L$</th>
<th>$k$</th>
<th>$n$</th>
<th>$w$</th>
<th>$t$</th>
<th>pk</th>
<th>ct</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>499</td>
<td>59</td>
<td>17</td>
<td>163</td>
<td>16</td>
<td>13</td>
<td>212</td>
<td>2,813</td>
</tr>
<tr>
<td>128</td>
<td>907</td>
<td>130</td>
<td>21</td>
<td>261</td>
<td>19</td>
<td>20</td>
<td>860</td>
<td>16,450</td>
</tr>
<tr>
<td>192</td>
<td>1657</td>
<td>234</td>
<td>29</td>
<td>391</td>
<td>26</td>
<td>28</td>
<td>3,496</td>
<td>92,033</td>
</tr>
<tr>
<td>256</td>
<td>2707</td>
<td>129</td>
<td>36</td>
<td>521</td>
<td>35</td>
<td>35</td>
<td>7,304</td>
<td>263,116</td>
</tr>
</tbody>
</table>

Table: $q = 2$, sizes of public key and ciphertext are in KB, probability of error $< 2^{-\lambda}$
Conclusion

First rank metric trapdoor function with a public key statistically indistinguishable from uniform
Conclusion

First rank metric trapdoor function with a public key statistically indistinguishable from uniform

Remarks and perspectives
Conclusion

First rank metric trapdoor function with a public key statistically indistinguishable from uniform

Remarks and perspectives

→ Big key and cipher sizes essentially due to the constraints on the probability of error
Conclusion

First rank metric trapdoor function with a public key statistically indistinguishable from uniform

Remarks and perspectives

→ Big key and cipher sizes essentially due to the constraints on the probability of error
→ Reduce size of the keys using ideal codes or relaxing decoding constraint ($2^{-128}$ instead of $2^{-\lambda}$)
Conclusion

First rank metric trapdoor function with a public key statistically indistinguishable from uniform

Remarks and perspectives

→ Big key and cipher sizes essentially due to the constraints on the probability of error
→ Reduce size of the keys using ideal codes or relaxing decoding constraint ($2^{-128}$ instead of $2^{-\lambda}$)
→ Construct Key Encapsulation Mechanism (KEM) and encryption scheme, reducing sizes at the same time
Conclusion

First rank metric trapdoor function with a public key statistically indistinguishable from uniform

Remarks and perspectives

→ Big key and cipher sizes essentially due to the constraints on the probability of error

→ Reduce size of the keys using ideal codes or relaxing decoding constraint \(2^{-128}\) instead of \(2^{-\lambda}\)

→ Construct Key Encapsulation Mechanism (KEM) and encryption scheme, reducing sizes at the same time

Thank you for your attention!
Probability of error

1. For recovering $E$, one of those two events occur:
   - $\langle s_i \rangle_{\mathbb{F}_q} \neq E \cdot W_i$
   - $\langle s_i \rangle_{\mathbb{F}_q} = E \cdot W_i$ but recovering $E$ fails

   Probability $\leq 1 - \prod_{i=0}^{tw-1}(1 - q^{i-N}) + \frac{q^{2(w-1)t}}{q^m-q^{t-1}}$

   $\ell$ rows for $H \rightarrow \ell$ attempts:
   \[
   \leq \left( 1 - \prod_{i=0}^{tw-1}(1 - q^{i-N}) + \frac{q^{2(w-1)t}}{q^m-q^{t-1}} \right)^\ell
   \]

2. For recovering $E$, not possible if $\dim(W_i \cdot E) < \dim W_i \dim E$

   Probability $\leq \frac{q^{tw}}{q^m-q^{t-1}}$

   At least one of the $\ell$ spaces $\rightarrow \leq 1 - \left( 1 - \frac{q^{tw}}{q^m-q^{t-1}} \right)^\ell$

   Probability of error upper bounded by:

   \[
   \left( 1 - \prod_{i=0}^{tw-1}(1 - q^{i-N}) + \frac{q^{2(w-1)t}}{q^m-q^{t-1}} \right)^\ell + 1 - \left( 1 - \frac{q^{tw}}{q^m-q^{t-1}} \right)^\ell
   \]
Let \( \alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_{q^m}^m \) be a basis of \( \mathbb{F}_{q^m} \). For all \( i \in \{1 \ldots n\} \) we have

\[
x_i = \sum_{j=1}^{m} x_{i,j} \alpha_j
\]

So if we consider the matrix

\[
M \triangleq \begin{pmatrix}
x_{1,1} & \cdots & x_{n,1} \\
\vdots & \ddots & \vdots \\
x_{1,m} & \cdots & x_{n,m}
\end{pmatrix} \in \mathbb{F}_q^{m \times n}
\]

Then \( x = \alpha M \) and \( |x| = \text{Rank}(M) \).