Rank Metric Trapdoor Functions with Homogeneous Errors

Étienne Burle[1] Philippe Gaborit[2] Younes Hatri[1] Ayoub Otmani[1]

[1] LITIS, University of Rouen Normandie, Normandie Univ, France

[2] XLIM, Université de Limoges, France

Najac, 15/10/2023

Introduction

Context:

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

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*

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

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*

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

- 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

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 *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 $(\mathbf{H}, \mathbf{e}\mathbf{H}^{\mathsf{T}})$, recover $\mathbf{e}$

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 $(\mathbf{H}, \mathbf{e}\mathbf{H}^{\mathsf{T}})$, recover $\mathbf{e}$

Remark : Distinguishing $(\mathbf{H}, \mathbf{e}\mathbf{H}^{\mathsf{T}})$ from $(\mathbf{H}, \mathbf{s})$ is the decision version of the problem

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 $(\mathbf{H}, \mathbf{e}\mathbf{H}^{\mathsf{T}})$, recover $\mathbf{e}$

Remark : Distinguishing $(\mathbf{H}, \mathbf{e}\mathbf{H}^{\mathsf{T}})$ from $(\mathbf{H}, \mathbf{s})$ 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]

---

[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*

Rank decoding's hardness

Proposition

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

Combinatorial attacks[2]	Algebraic attacks [3]
$O\left((n-k)^3 m^3 q^{w\frac{(k+1)m}{n}-m}\right)$	Exponential

[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

	Transformed code	Hidden structure	Ciphertext in two parts
Description	$\mathbf{G} \rightarrow \mathbf{SGT}$	$\mathbf{G} \rightarrow \mathbf{SG}$	(C_1, C_2) : $C_2 - C_1\mathbf{V} = \mathbf{mG} + \mathbf{e}$
Used code	Gabidulin	Ideal LRPC	Gabidulin
Schemes	1991 GPT[4] 2017 Loidreau	2019 ROLLO	2020 RQC
Security problems	RD IfRD	IRD IfRD	IRD

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

[4] Gabidulin, Paramonov, Tretjakov

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

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 $\mathcal{E}$

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 $\mathcal{E}$

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

	Nature	Complexity	Condition
2017[5]	Combinatorial	Poly	$N \geq nt$

[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

	Nature	Complexity	Condition
2017[5]	Combinatorial	Poly	$N \geq nt$
2018[6]	Algebraic	Sub-exp	$N > kt$

[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

	Nature	Complexity	Condition
2017[5]	Combinatorial	Poly	$N \geq nt$
2018[6]	Algebraic	Sub-exp	$N > kt$
2021[7]	Algebraic	Exp	Thwarted when $N < kt$

[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

	Nature	Complexity	Condition
2017[5]	Combinatorial	Poly	$N \geq nt$
2018[6]	Algebraic	Sub-exp	$N > kt$
2021[7]	Algebraic	Exp	Thwarted when $N < kt$
2022[8]	Combinatorial	Poly	$N > ktm/(m-t)$

[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

	Transformed code	Hidden structure	Ciphertext in two parts
Description	$\mathbf{G} \to \mathbf{SGT}$	$\mathbf{G} \to \mathbf{SG}$	(C_1, C_2) : $C_2 - C_1\mathbf{V} = \mathbf{mG} + \mathbf{E}$
Used code	Gabidulin	LRPC	Gabidulin
Schemes	2022 LowMS	2022[9]	2019 Li-Ping Wang
Security problems	RSL IfRD	RSL IfRD	RSL

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

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

$\mathbf{H} \in \mathbb{F}_{q^m}^{\ell \times n}$ 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

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

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

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).

$\mathbf{H} \in \mathbb{F}_{q^m}^{\ell \times n}$ is semi-homogeneous of weight w if the support of each of its rows is of low dimension w.
The *support* of $\mathbf{H}$ is $(W_1, \ldots, W_\ell)$, where W_i is the support of its i-th row.

- Use of a transformed code

Our scheme

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

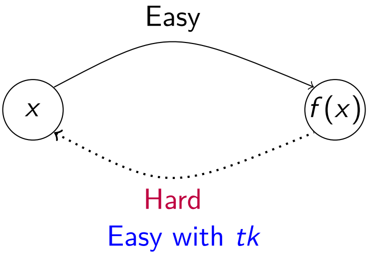
Definitions

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

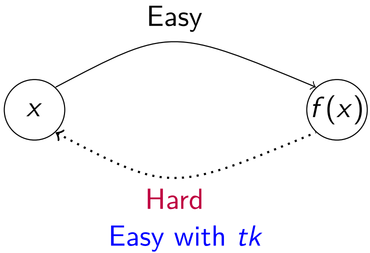
$\mathbf{H} \in \mathbb{F}_{q^m}^{\ell \times n}$ is semi-homogeneous of weight w if the support of each of its rows is of low dimension w.
The *support* of $\mathbf{H}$ is $(W_1, \ldots, W_\ell)$, where W_i is the support of its i-th row.

- Use of a transformed code
- Security relying on Rank decoding and RSL only

Construction of trapdoor function

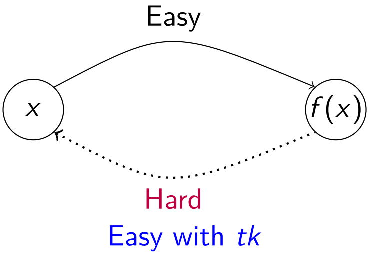


Construction of trapdoor function



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

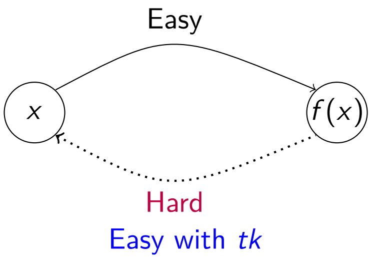
Construction of trapdoor function



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

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

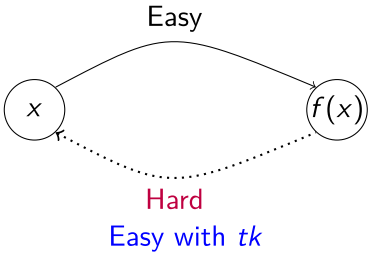
Construction of trapdoor function



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

1. pk,tk $\leftarrow Gen(\mathbb{1}^{\lambda})$
2. $Eval(\text{pk}, \mathbf{x})$ will evaluate with public key pk in $\mathbf{x}$

Construction of trapdoor function



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

1. pk,tk $\leftarrow$ *Gen*$(\mathbb{1}^{\lambda})$
2. *Eval*(pk,$\mathbf{x}$) will evaluate with public key pk in $\mathbf{x}$
3. Invert(tk,*Eval*(pk,$\mathbf{x}$)) returns $\mathbf{x}$ with overwhelming probability

Gen

1. $\mathbf{R} \xleftarrow{\$} \mathbb{F}_{q^m}^{k \times L}$

Gen

1. $\mathbf{R} \xleftarrow{\$} \mathbb{F}_{q^m}^{k \times L}$
2. $\mathbf{W} \xleftarrow{\$} \mathbb{F}_{q^m}^{n \times L}$: **semi-homogeneous** of weight w

Gen

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

Gen

1. $\mathbf{R} \xleftarrow{\$} \mathbb{F}_{q^m}^{k \times L}$
2. $\mathbf{W} \xleftarrow{\$} \mathbb{F}_{q^m}^{n \times L}$: **semi-homogeneous** of weight w
3. Return $(\mathbf{R} | -\mathbf{R}\mathbf{W}^{\top}), \mathbf{W}$

Public key : $\mathbf{G} = (\mathbf{R} | -\mathbf{R}\mathbf{W}^{\top}) \in \mathbb{F}_{q^m}^{k \times (n+L)}$

Gen

1. $\mathbf{R} \xleftarrow{\$} \mathbb{F}_{q^m}^{k \times L}$
2. $\mathbf{W} \xleftarrow{\$} \mathbb{F}_{q^m}^{n \times L}$: **semi-homogeneous** of weight w
3. Return $(\mathbf{R} | -\mathbf{R}\mathbf{W}^\intercal), \mathbf{W}$

Public key : $\mathbf{G} = (\mathbf{R} | -\mathbf{R}\mathbf{W}^\intercal) \in \mathbb{F}_{q^m}^{k \times (n+L)}$

Secret key : $\mathbf{W}$

Gen

1. $\mathbf{R} \xleftarrow{\$} \mathbb{F}_{q^m}^{k \times L}$
2. $\mathbf{W} \xleftarrow{\$} \mathbb{F}_{q^m}^{n \times L}$: **semi-homogeneous** of weight w
3. Return $(\mathbf{R} | -\mathbf{R}\mathbf{W}^\top), \mathbf{W}$

Public key : $\mathbf{G} = (\mathbf{R} | -\mathbf{R}\mathbf{W}^\top) \in \mathbb{F}_{q^m}^{k \times (n+L)}$

Secret key : $\mathbf{W}$

Remark : $\mathbf{G}(\mathbf{W}, \mathbf{I}_n)^\top = 0$

Eval

Public key : $\mathbf{G}$

Eval

Public key : $\mathbf{G}$

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

Eval

Public key : $\mathbf{G}$

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

Eval

Public key : $\mathbf{G}$

1. $\mathbf{X} \in \mathbb{F}_{q^m}^{N \times k}$: *input*
2. $\mathbf{E} \xleftarrow{\$} \mathbb{F}_{q^m}^{N \times (n+L)}$ *homogeneous of weight* t
3. Compute and return the output

$$\mathbf{C} = \mathbf{X}\mathbf{G} + \mathbf{E}$$

Invert

Secret key : $\mathbf{W}$

Invert

Secret key : $\mathbf{W}$

1. $\mathbf{C} = \mathbf{X}\mathbf{G} + \mathbf{E}$: *input*

Invert

Secret key : $\mathbf{W}$

1. $\mathbf{C} = \mathbf{X}\mathbf{G} + \mathbf{E}$: *input*

2. Compute $\mathbf{C}(\mathbf{W}, \mathbf{I}_n)^\mathsf{T} = (\mathbf{X}\mathbf{G} + \mathbf{E})(\mathbf{W}, \mathbf{I}_n)^\mathsf{T}$

$$= \mathbf{X}\mathbf{G}(\mathbf{W}, \mathbf{I}_n)^\mathsf{T} + \mathbf{E}(\mathbf{W}, \mathbf{I}_n)^\mathsf{T}$$

$$= \mathbf{E}(\mathbf{W}, \mathbf{I}_n)^\mathsf{T}$$

Invert

Secret key : $\mathbf{W}$

1. $\mathbf{C} = \mathbf{X}\mathbf{G} + \mathbf{E}$: *input*

2. Compute $\mathbf{C}(\mathbf{W}, \mathbf{I}_n)^\intercal = (\mathbf{X}\mathbf{G} + \mathbf{E})(\mathbf{W}, \mathbf{I}_n)^\intercal$

$$= \mathbf{X}\mathbf{G}(\mathbf{W}, \mathbf{I}_n)^\intercal + \mathbf{E}(\mathbf{W}, \mathbf{I}_n)^\intercal$$
$$= \mathbf{E}(\mathbf{W}, \mathbf{I}_n)^\intercal$$

3. Recover $\mathbf{E}$ with *Homogeneous error decoding*

Invert

Secret key : $\mathbf{W}$

1. $\mathbf{C} = \mathbf{X}\mathbf{G} + \mathbf{E}$: *input*

2. Compute
$$\begin{aligned} \mathbf{C}(\mathbf{W}, \mathbf{I}_n)^\intercal &= (\mathbf{X}\mathbf{G} + \mathbf{E})(\mathbf{W}, \mathbf{I}_n)^\intercal \\ &= \mathbf{X}\mathbf{G}(\mathbf{W}, \mathbf{I}_n)^\intercal + \mathbf{E}(\mathbf{W}, \mathbf{I}_n)^\intercal \\ &= \mathbf{E}(\mathbf{W}, \mathbf{I}_n)^\intercal \end{aligned}$$

3. Recover $\mathbf{E}$ with *Homogeneous error decoding*

4. Compute $\mathbf{C} - \mathbf{E} = \mathbf{X}\mathbf{G}$ and recover $\mathbf{X}$ with linear algebra

Invert

Secret key : $\mathbf{W}$

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

2. Compute
$$\mathbf{C}(\mathbf{W}, \mathbf{I}_n)^\intercal = (\mathbf{XG} + \mathbf{E})(\mathbf{W}, \mathbf{I}_n)^\intercal = \mathbf{XG}(\mathbf{W}, \mathbf{I}_n)^\intercal + \mathbf{E}(\mathbf{W}, \mathbf{I}_n)^\intercal = \mathbf{E}(\mathbf{W}, \mathbf{I}_n)^\intercal$$

3. Recover $\mathbf{E}$ with *Homogeneous error decoding*

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

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 $t > 0$
- $\mathbf{S} \in \mathbb{F}_{q^m}^{\ell \times N}$

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 $\mathbf{HE} = \mathbf{S}$

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, Hartri, 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

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

Homogeneous error decoding

- $\mathbf{H} \in \mathbb{F}_{q^m}^{\ell \times n}$ semi-homogeneous of weight w and support $(W_1, \dots, W_\ell)$
- 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, Hartri, 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

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

Asymptotically equivalent to ℓq^{tw-m}

Homogeneous error decoding

$$\mathbf{HE} = \mathbf{S}$$

Homogeneous error decoding

$$\mathbf{HE} = \mathbf{S}$$

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

Homogeneous error decoding

$$\mathbf{HE} = \mathbf{S}$$

1. Considering $\mathbf{h}_i$ and $\mathbf{s}_i$ the i-th row of $\mathbf{H}$ and $\mathbf{S}$, we have the equation $\mathbf{h}_i\mathbf{E} = \mathbf{s}_i$.
    - W_i : support of $\mathbf{h}_i$

Homogeneous error decoding

$$\mathbf{HE} = \mathbf{S}$$

1. Considering $\mathbf{h}_i$ and $\mathbf{s}_i$ the i-th row of $\mathbf{H}$ and $\mathbf{S}$, we have the equation $\mathbf{h}_i\mathbf{E} = \mathbf{s}_i$.
   - W_i : support of $\mathbf{h}_i$
   - $\mathcal{E}$: support of $\mathbf{E}$

Homogeneous error decoding

$$\mathbf{HE} = \mathbf{S}$$

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

Homogeneous error decoding

$$\mathbf{HE} = \mathbf{S}$$

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

Homogeneous error decoding

$$\mathbf{HE} = \mathbf{S}$$

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

Recover $\mathcal{E}$ with $\mathbf{s}_i$ and W_i of basis $(f_1 \ldots f_w)$:

Homogeneous error decoding

$$\mathbf{HE} = \mathbf{S}$$

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

Recover $\mathcal{E}$ with $\mathbf{s}_i$ and W_i of basis $(f_1 \dots f_w)$:

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

Homogeneous error decoding

$$\mathbf{HE} = \mathbf{S}$$

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

   Recover $\mathcal{E}$ with $\mathbf{s}_i$ 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 ℓtw equations and nt unknowns

Homogeneous error decoding

$$\mathbf{HE} = \mathbf{S}$$

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

   Recover $\mathcal{E}$ with $\mathbf{s}_i$ and W_i of basis $(f_1 \dots f_w)$:

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

2. $\mathbf{E}$ can then be recovered solving N linear systems with ℓtw equations and nt unknowns $\rightarrow \ell w \geq n$

Security of the scheme

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

Various aspects of security rely on classical problems :

Security of the scheme

$$\mathbf{G} = (\mathbf{R} | -\mathbf{R}\mathbf{W}^\top)$$

Various aspects of security rely on classical problems :

- Inversion of the function : *Rank Support Learning*

  (Recover $\mathbf{X}$ and $\mathbf{E}$ from $\mathbf{XG}+\mathbf{E}$)

Security of the scheme

$$\mathbf{G} = (\mathbf{R} | -\mathbf{R}\mathbf{W}^\top)$$

Various aspects of security rely on classical problems :

- Inversion of the function : *Rank Support Learning*
  (Recover $\mathbf{X}$ and $\mathbf{E}$ from $\mathbf{XG}+\mathbf{E}$)
- Recovery of the trapdoor : *Search Rank Decoding*
  (Recover $\mathbf{W}$ from $\mathbf{G}$)

Security of the scheme

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

Various aspects of security rely on classical problems :

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

Security of the scheme

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

Various aspects of security rely on classical problems :

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

$\Rightarrow$ $\mathbf{G}$ *computationally indistinguishable* from a uniform matrix

Parameters

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

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

Parameters

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

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

Security	pkSize (KB)	ctSize (KB)
128	1.90	2.04
192	2.29	2.41
256	2.50	2.63

Table: ROLLO encryption parameters

Other property on $\mathbf{G}$

$$\mathbf{G} = (\mathbf{R} | -\mathbf{R}\mathbf{W}^{\intercal})$$

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

Other property on $\mathbf{G}$

$$\mathbf{G} = (\mathbf{R} | -\mathbf{R}\mathbf{W}^{\intercal})$$

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

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

Other property on $\mathbf{G}$

$$\mathbf{G} = (\mathbf{R} | -\mathbf{R}\mathbf{W}^{\top})$$

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

→ proved with generalized Leftover Hash Lemma

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

Other property on $\mathbf{G}$

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

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

$\rightarrow$ proved with generalized Leftover Hash Lemma

New condition :

Choose parameters in order to have this distance $< 2^{-\lambda}$:
$\mathbf{G}$ statistically indistinguishable from uniform

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

Statistically indistinguishable parameters

λ	m	L	k	n	w	t	pk	ct
80	499	59	17	163	16	13	212	2,813
128	907	130	21	261	19	20	860	16,450
192	1657	234	29	391	26	28	3,496	92,033
256	2707	129	36	521	35	35	7,304	263,116

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 $\mathcal{E}$, one of those two events occur :
   - $\langle \mathbf{s}_i \rangle_{\mathbb{F}_q} \neq \mathcal{E} \cdot W_i$
   - $\langle \mathbf{s}_i \rangle_{\mathbb{F}_q} = \mathcal{E} \cdot W_i$ but recovering $\mathcal{E}$ fails

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

   ℓ rows for $\mathbf{H} \to \ell$ 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 $\mathbf{E}$, not possible if $\dim(W_i \cdot \mathcal{E}) < \dim W_i \dim \mathcal{E}$

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

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

Probability of error upper bounded by :

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

Rank metric

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

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_{q^m}^m$ 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

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

Then $\mathbf{x} = \boldsymbol{\alpha}\mathbf{M}$ and $|\mathbf{x}| = \mathrm{Rank}(\mathbf{M})$.