How to design a McEliece like encryption scheme in Rank metric ?

Pierre Loidreau

DGA MI and IRMAR, CNRS, Université de Rennes
OpeRa
Caserta Feb 15th, 2024

Outline of the talk

The agencies requirements

- Request for Post-Quantum encryption schemes or KEMs with IND-CPA or IND-CCA security
  - NIST standardization process or Chinese competition
- No use of structure such as quasi-cyclicity
  - European request: ANSSI and BSI [1]

[1] www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Migration_to_Post_Quantum_Cryptography.html

The agencies requirements

- Request for Post-Quantum encryption schemes or KEMs with IND-CPA or IND-CCA security
  - NIST standardization process or Chinese competition
- No use of structure such as quasi-cyclicity
  - European request: ANSSI and BSI [1]

[1] www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Migration_to_Post_Quantum_Cryptography.html

NIST's IND-CCA Solutions [2]

- Lattice-Based cryptography
  - Structured: `Kyber`
  - Unstructured: `FrodoKEM`
- Code-Based cryptography
  - Structured: `BIKE, HQC`
  - Unstructured: `ClassicMcEliece`

[2] https://csrc.nist.gov/projects/post-quantum-cryptography

NIST's IND-CCA Solutions [2]

- Lattice-Based cryptography
  - Structured: `Kyber`
  - Unstructured: `FrodoKEM`
- Code-Based cryptography
  - Structured: `BIKE`, `HQC`
  - Unstructured: `ClassicMcEliece`

[2] https://csrc.nist.gov/projects/post-quantum-cryptography

NIST's IND-CCA Solutions

- Lattice-Based cryptography
  - ~~Structured: `Kyber`~~
  - Unstructured: `FrodoKEM`
- Code-Based cryptography
  - ~~Structured: `BIKE`, `HQC`~~
  - Unstructured: `Classic McEliece`

$\Rightarrow$ Only `Classic McEliece` left in code based cryptography

- Goal of the recipe: design rank metric based unstructured McEliece scheme with reasonable parameters.

NIST's IND-CCA Solutions

- Lattice-Based cryptography
  - ~~Structured: `Kyber`~~
  - Unstructured: `FrodoKEM`
- Code-Based cryptography
  - ~~Structured: `BIKE`, `HQC`~~
  - Unstructured: `Classic McEliece`

$\Rightarrow$ Only `Classic McEliece` left in code based cryptography

- Goal of the recipe: design rank metric based unstructured McEliece scheme with reasonable parameters.

NIST's IND-CCA Solutions

- Lattice-Based cryptography
  - ~~Structured: `Kyber`~~
  - Unstructured: `FrodoKEM`
- Code-Based cryptography
  - ~~Structured: `BIKE`, `HQC`~~
  - Unstructured: `Classic McEliece`

$\Rightarrow$ Only `Classic McEliece` left in code based cryptography

- Goal of the recipe: design rank metric based unstructured McEliece scheme with reasonable parameters.

NIST's IND-CCA Solutions

- Lattice-Based cryptography
  - ~~Structured: `Kyber`~~
  - Unstructured: `FrodoKEM`
- Code-Based cryptography
  - ~~Structured: `BIKE`, `HQC`~~
  - Unstructured: `Classic McEliece`

$\Rightarrow$ Only `Classic McEliece` left in code based cryptography

- Goal of the recipe: design rank metric based unstructured McEliece scheme with reasonable parameters.

Outline of the talk

Ingredients

- $\mathcal{V}$: metric vector space of dimension n
- $\mathcal{F}$: A family of **easily** decodable linear $[n, k]$-codes over a set $\mathcal{D} \subset \mathcal{V}$ with a $\texttt{Decode}_{\mathcal{C}}$ procedure:
  - Probabilistic with good probability of success
  - Deterministic

The recipe I

1. $\texttt{KeyGen}()$
   - $\mathcal{C} \xleftarrow{\$} \mathcal{F}$
   - $L \xleftarrow{\$}$ Invertible linear transformation of $\mathcal{V}$
   - $\texttt{Return sk} = (\mathcal{C}, L)$, $\texttt{pk} = L(\mathcal{C})$
2. $\texttt{Encrypt}(\texttt{pt}, \texttt{pk} := \langle \mathrm{G} \rangle = L(\mathcal{C}) \; ; \; r)$
   - $\mathrm{e} \xleftarrow{\$_r} L(\mathcal{D})$
   - $\texttt{Return ct} := \texttt{pt}\mathrm{G} + \mathrm{e}$
3. $\texttt{Decrypt}(\texttt{ct}, \texttt{sk})$
   - $\texttt{pt}^* := \texttt{Decode}_{\mathcal{C}}(L^{-1}(\texttt{ct}) = \texttt{pt}L^{-1}(\mathrm{G}) + L^{-1}(\mathrm{e}))$
   - $\texttt{Return pt}^*$

The recipe II

- Consistency - $\mathtt{pt}^* = \mathtt{pt}$?
  - Probabilistic if $\mathtt{Decode}_{\mathcal{C}}$ is probabilistic
  - Deterministic else
- Security reduction
  - OW-CPA games reduction to **difficult** problems

The OW-CPA game I

GAME G_1 (OW-CPA)

1. $\mathcal{C}, L \leftarrow \texttt{KeyGen}()$
2. $\langle \mathrm{G} \rangle = L(\mathcal{C})$
3. $\mathrm{e} \overset{\$_r}{\leftarrow} \mathcal{D}$
4. $\mathtt{pt} \overset{\$}{\leftarrow} \mathcal{P}$
5. $\mathtt{ct} = \mathtt{pt}\mathrm{G} + \mathrm{e}$
6. $\mathtt{pt}^* \leftarrow \mathcal{A}(\mathtt{ct}, \mathrm{G})$
7. $\mathtt{Return}\ \mathtt{pt}^* == \mathtt{pt}$?

The OW-CPA game II

GAME G_2

1. $\cancel{\mathcal{C}, L \leftarrow \texttt{KeyGen}()}$
2. $\mathsf{G} \leftarrow \mathsf{Random}$
3. $\mathsf{e} \overset{\$_r}{\leftarrow} \mathcal{D}$
4. $\mathtt{pt} \overset{\$}{\leftarrow} \mathcal{P}$
5. $\mathtt{ct} = \mathtt{pt}\mathsf{G} + \mathsf{e}$
6. $\mathtt{pt}^* \leftarrow \mathcal{A}(\mathtt{ct}, \mathsf{G})$
7. $\texttt{Return } \mathtt{pt}^* == \mathtt{pt}$?

Adversaries and advantages

- $\mathtt{Adv}^{G_1}(\mathcal{A}) := \Pr_{G_1}(\mathcal{A}(\mathrm{ct}, \mathrm{G}) == \mathrm{pt})$
  - advantage of the encryption scheme $\mathtt{Adv}^{OW}(\mathcal{A})$
- $\mathtt{Adv}^{G_2}(\mathcal{A}) := \Pr_{G_2}(\mathcal{A}(\mathrm{ct}, \mathrm{G}) == \mathrm{pt})$
  - advantage of the generic game where $L(\mathcal{C})$ is replaced by random: $\mathtt{Adv}^{OW}_{\mathtt{GenDecode}}(\mathcal{A})$
- If $\mathtt{Adv}_{\mathtt{Dist}}(D)$: probability of distinguishing $L(\mathcal{C})$ from random.

$$\mathtt{Adv}^{OW}(\mathcal{A}) \leq \mathtt{Adv}^{OW}_{\mathtt{GenDec}}(\mathcal{A}) + \mathtt{Adv}_{\mathtt{Dist}}(D)$$

Maximize over all $\mathcal{A}$ working in polynomial-time.

Adversaries and advantages

- $\texttt{Adv}^{G_1}(\mathcal{A}) := \Pr_{G_1}(\mathcal{A}(\texttt{ct}, \mathsf{G}) == \texttt{pt})$
  - advantage of the encryption scheme $\texttt{Adv}^{OW}(\mathcal{A})$
- $\texttt{Adv}^{G_2}(\mathcal{A}) := \Pr_{G_2}(\mathcal{A}(\texttt{ct}, \mathsf{G}) == \texttt{pt})$
  - advantage of the generic game where $L(\mathcal{C})$ is replaced by random: $\texttt{Adv}^{OW}_{\texttt{GenDecode}}(\mathcal{A})$
- If $\texttt{Adv}_{\texttt{Dist}}(D)$: probability of distinguishing $L(\mathcal{C})$ from random.

$$\texttt{Adv}^{OW}(\mathcal{A}) \leq \texttt{Adv}^{OW}_{\texttt{GenDec}}(\mathcal{A}) + \texttt{Adv}_{\texttt{Dist}}(D)$$

Maximize over all $\mathcal{A}$ working in polynomial-time.

Adversaries and advantages

- $\mathtt{Adv}^{G_1}(\mathcal{A}) := \Pr_{G_1}(\mathcal{A}(\mathtt{ct}, \mathsf{G}) == \mathtt{pt})$
  - advantage of the encryption scheme $\mathtt{Adv}^{OW}(\mathcal{A})$
- $\mathtt{Adv}^{G_2}(\mathcal{A}) := \Pr_{G_2}(\mathcal{A}(\mathtt{ct}, \mathsf{G}) == \mathtt{pt})$
  - advantage of the generic game where $L(\mathcal{C})$ is replaced by random: $\mathtt{Adv}^{OW}_{\mathtt{GenDecode}}(\mathcal{A})$
- If $\mathtt{Adv}_{\mathtt{Dist}}(D)$: probability of distinguishing $L(\mathcal{C})$ from random.

$$\mathtt{Adv}^{OW}(\mathcal{A}) \leq \mathtt{Adv}^{OW}_{\mathtt{GenDec}}(\mathcal{A}) + \mathtt{Adv}_{\mathtt{Dist}}(D)$$

Maximize over all $\mathcal{A}$ working in polynomial-time.

Adversaries and advantages

- $\mathtt{Adv}^{G_1}(\mathcal{A}) := \Pr_{G_1}(\mathcal{A}(\mathtt{ct}, \mathrm{G}) == \mathtt{pt})$
  - advantage of the encryption scheme $\mathtt{Adv}^{OW}(\mathcal{A})$
- $\mathtt{Adv}^{G_2}(\mathcal{A}) := \Pr_{G_2}(\mathcal{A}(\mathtt{ct}, \mathrm{G}) == \mathtt{pt})$
  - advantage of the generic game where $L(\mathcal{C})$ is replaced by random: $\mathtt{Adv}^{OW}_{\mathtt{GenDecode}}(\mathcal{A})$
- If $\mathtt{Adv}_{\mathtt{Dist}}(D)$: probability of distinguishing $L(\mathcal{C})$ from random.

$$\mathtt{Adv}^{OW}(\mathcal{A}) \leq \mathtt{Adv}^{OW}_{\mathtt{GenDec}}(\mathcal{A}) + \mathtt{Adv}_{\mathtt{Dist}}(D)$$

Maximize over all $\mathcal{A}$ working in polynomial-time.

Adversaries and advantages

- $\mathtt{Adv}^{G_1}(\mathcal{A}) := \Pr_{G_1}(\mathcal{A}(\mathtt{ct}, \mathrm{G}) == \mathtt{pt})$
  - advantage of the encryption scheme $\mathtt{Adv}^{OW}(\mathcal{A})$
- $\mathtt{Adv}^{G_2}(\mathcal{A}) := \Pr_{G_2}(\mathcal{A}(\mathtt{ct}, \mathrm{G}) == \mathtt{pt})$
  - advantage of the generic game where $L(\mathcal{C})$ is replaced by random: $\mathtt{Adv}^{OW}_{\mathtt{GenDecode}}(\mathcal{A})$
- If $\mathtt{Adv}_{\mathtt{Dist}}(D)$: probability of distinguishing $L(\mathcal{C})$ from random.

$$\mathtt{Adv}^{OW}(\mathcal{A}) \leq \mathtt{Adv}^{OW}_{\mathtt{GenDec}}(\mathcal{A}) + \mathtt{Adv}_{\mathtt{Dist}}(D)$$

Maximize over all $\mathcal{A}$ working in polynomial-time.

Some existing instantiations

- Hamming metric, $\mathcal{V} = \mathbb{F}_2^n$
  - $\mathcal{F}$: Family of Goppa codes
  - $\mathcal{D}$: Set of binary vectors of Hamming weight w
  - L: Linear permutation of the vectors of the support
- Rank metric, $\mathcal{V} = \mathbb{F}_{q^m}^n$
  - Deterministic decoding based
    - $\mathcal{F}$: Family of Gabidulin codes
    - $\mathcal{D}$: Set of binary vectors of rank weight w
    - L: Rank metric preserving linear transformation of the vectors of the support

Some existing instantiations

- Hamming metric, $\mathcal{V} = \mathbb{F}_2^n$
  - $\mathcal{F}$: Family of Goppa codes
  - $\mathcal{D}$: Set of binary vectors of Hamming weight w
  - L: Linear permutation of the vectors of the support
- Rank metric, $\mathcal{V} = \mathbb{F}_{q^m}^n$
  - Deterministic decoding based
    - $\mathcal{F}$: Family of Gabidulin codes
    - $\mathcal{D}$: Set of binary vectors of rank weight w
    - L: Rank metric preserving linear transformation of the vectors of the support

Outline of the talk

Rank metric [Gab85, Del78]

Definition

- $\gamma_1, \ldots, \gamma_m$, *basis of* $\mathbb{F}_{2^m}/\mathbb{F}_2$,
- $\mathrm{e} = (e_1, \ldots, e_n) \in (\mathbb{F}_{2^m})^n$, $e_i \mapsto (e_{i1}, \ldots, e_{in})$,

$$\forall \mathrm{e} \in (\mathbb{F}_{2^m})^n, \quad \mathrm{Rk}(\mathrm{e}) \stackrel{def}{=} \mathrm{Rk}\begin{pmatrix} e_{11} & \cdots & e_{1n} \\ \vdots & \ddots & \vdots \\ e_{m1} & \cdots & e_{mn} \end{pmatrix}$$

- $[n, k, d]_r$ code: $\mathcal{C} \subset \mathbb{F}_{2^m}^n$, k-dimensional, $d = \min_{c \neq 0 \in \mathcal{C}} \mathrm{Rk}(\mathrm{c})$
- Singleton property $d - 1 \leq n - k$ (if $n \leq m$)
- $\mathrm{Rk}(\mathrm{e}) = t \Leftrightarrow \exists \mathcal{V} \subset \mathbb{F}_{2^m}$, s.t. $\dim_2(\mathcal{V}) = t$ and $e_i \in \mathcal{V}$, $\forall i$

Rank metric [Gab85, Del78]

Definition

- $\gamma_1, \ldots, \gamma_m$, *basis of* $\mathbb{F}_{2^m}/\mathbb{F}_2$,
- $\mathrm{e} = (e_1, \ldots, e_n) \in (\mathbb{F}_{2^m})^n$, $e_i \mapsto (e_{i1}, \ldots, e_{in})$,

$$\forall \mathrm{e} \in (\mathbb{F}_{2^m})^n, \quad \mathrm{Rk}(\mathrm{e}) \overset{def}{=} \mathrm{Rk}\begin{pmatrix} e_{11} & \cdots & e_{1n} \\ \vdots & \ddots & \vdots \\ e_{m1} & \cdots & e_{mn} \end{pmatrix}$$

- $[n, k, d]_r$ code: $\mathcal{C} \subset \mathbb{F}_{2^m}^n$, k-dimensional, $d = \min_{\mathrm{c} \neq 0 \in \mathcal{C}} \mathrm{Rk}(\mathrm{c})$
- Singleton property $d - 1 \leq n - k$ (if $n \leq m$)
- $\mathrm{Rk}(\mathrm{e}) = t \Leftrightarrow \exists \mathcal{V} \subset \mathbb{F}_{2^m}$, s.t. $\dim_2(\mathcal{V}) = t$ and $e_i \in \mathcal{V}$, $\forall i$

Rank metric [Gab85, Del78]

Definition

- $\gamma_1, \ldots, \gamma_m$, *basis of* $\mathbb{F}_{2^m}/\mathbb{F}_2$,
- $\mathrm{e} = (e_1, \ldots, e_n) \in (\mathbb{F}_{2^m})^n$, $e_i \mapsto (e_{i1}, \ldots, e_{in})$,

$$\forall \mathrm{e} \in (\mathbb{F}_{2^m})^n, \quad \mathrm{Rk}(\mathrm{e}) \overset{def}{=} \mathrm{Rk} \begin{pmatrix} e_{11} & \cdots & e_{1n} \\ \vdots & \ddots & \vdots \\ e_{m1} & \cdots & e_{mn} \end{pmatrix}$$

- $[n, k, d]_r$ code: $\mathcal{C} \subset \mathbb{F}_{2^m}^n$, k-dimensional, $d = \min_{c \neq 0 \in \mathcal{C}} \mathrm{Rk}(c)$
- Singleton property $d - 1 \leq n - k$ (if $n \leq m$)
- $\mathrm{Rk}(\mathrm{e}) = t \Leftrightarrow \exists \mathcal{V} \subset \mathbb{F}_{2^m}$, s.t. $\dim_2(\mathcal{V}) = t$ and $e_i \in \mathcal{V}$, $\forall i$

Rank metric [Gab85, Del78]

Definition

- $\gamma_1, \ldots, \gamma_m$, *basis of* $\mathbb{F}_{2^m}/\mathbb{F}_2$,
- $\mathrm{e} = (e_1, \ldots, e_n) \in (\mathbb{F}_{2^m})^n$, $e_i \mapsto (e_{i1}, \ldots, e_{in})$,

$$\forall \mathrm{e} \in (\mathbb{F}_{2^m})^n, \quad \mathrm{Rk}(\mathrm{e}) \overset{def}{=} \mathrm{Rk}\begin{pmatrix} e_{11} & \cdots & e_{1n} \\ \vdots & \ddots & \vdots \\ e_{m1} & \cdots & e_{mn} \end{pmatrix}$$

- $[n, k, d]_r$ code: $\mathcal{C} \subset \mathbb{F}_{2^m}^n$, k-dimensional, $d = \min_{\mathrm{c} \neq 0 \in \mathcal{C}} \mathrm{Rk}(\mathrm{c})$
- Singleton property $d - 1 \leq n - k$ (if $n \leq m$)
- $\mathrm{Rk}(\mathrm{e}) = t \Leftrightarrow \exists \mathcal{V} \subset \mathbb{F}_{2^m}$, s.t. $\dim_2(\mathcal{V}) = t$ and $e_i \in \mathcal{V}$, $\forall i$

Example

$$e = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

In $\mathbb{F}_{2^5}$ we have $e = (\alpha, \beta, \alpha + \beta, \beta, \beta, \alpha + \beta)$

- Hamming weight: 5
- Rank: 2

Gabidulin codes [Gab85, Del78]

Definition (Gabidulin codes)

Let $\mathrm{g} = (g_1, \ldots, g_n) \in (\mathbb{F}_{2^m})^n$, $\mathbb{F}_2$*-l.i.*, $[i] \stackrel{def}{=} 2^i$

$$Gab_k(\mathrm{g}) = \langle \mathrm{G} \rangle, \ \ where\ \mathrm{G} = \begin{pmatrix} g_1 & \cdots & g_n \\ \vdots & \ddots & \vdots \\ g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix}$$

- Remarks on $\mathrm{Gab}_k(\mathrm{g})$
  - P-time quadratic decoding up to $t = \lfloor (n-k)/2 \rfloor$, [Gab85]
  - Evaluation codes of linearized polynomials, see Alessandro's talk

Outline of the talk

Generic instantiations I

- $\mathcal{V} = \mathbb{F}_{2^m}^n$
- $\mathcal{D} \subset \mathcal{V} =$ vectors of rank w
- $\mathcal{F} = \{(\mathrm{X} \mid \mathrm{Gab}_{n-2w}(\mathrm{g})) \subset \mathbb{F}_{2^m}^{\ell+n},\ \mathrm{g}\}$
    - $\mathtt{Decode}_{\mathcal{C}}$
        1. Puncture on the ℓ positions of X : $\mathcal{C} \mapsto \widehat{\mathcal{C}} = \mathrm{Gab}_{n-2w}(\mathrm{g})$
        2. Decode $\widehat{\mathcal{C}}$

Generic instantiations II

1. KeyGen()
   - $\mathcal{C} \xleftarrow{\$} \mathcal{F}$
   - $\mathrm{P} \xleftarrow{\$} \mathcal{M}_{n+\ell}(\mathbb{F}_2)$
   - Return sk $=(\mathcal{C}, \mathrm{P})$, pk $= \mathcal{C}\mathrm{P}$
2. Encrypt(pt, pk $:= \langle \mathrm{G} \rangle = \mathcal{C}\mathrm{P}$; r)
   - $\mathrm{e} \xleftarrow{\$_r} \mathcal{D}\mathrm{P} = \mathcal{D}$
   - Return ct $:=$ ptG $+$ e
3. Decrypt(ct, sk)
   - pt* $:=$ Decode$_{\mathcal{C}}$(ctP^{-1} $=$ ptGP^{-1} $+$ eP^{-1})
   - Return pt*

Generic instantiations III

- Security : $\mathtt{Adv}^{OW}(\mathcal{A}) \leq \mathtt{Adv}^{OW}_{\mathtt{GenDec}}(\mathcal{A}) + \mathtt{Adv}_{\mathtt{Dist}}(D)$
  - $\mathtt{Adv}^{OW}_{\mathtt{GenDec}}(\mathcal{A})$: difficulty of solving *RD* problem - see Magali's talk
  - $\mathtt{Adv}_{\mathtt{Dist}}(D)$: see next

Overbeck's distinguisher - [GPT91, Ksh07, RGH10, OKN16]

- Note that $\mathtt{pk} = \langle (\mathrm{X} \mid \underbrace{\mathrm{G}}_{Gab_{n-2w}(\mathrm{g})=\langle \mathrm{G} \rangle})\mathrm{P} \rangle$, $\mathrm{P} \in M_n(\mathbb{F}_2)$
- Principle
  1. Compute $\mathtt{pk}^{[i]} = \langle (\mathrm{X}^{[i]} \mid \mathrm{G}^{[i]})\ \mathrm{P} \rangle$
  2. Compute $\widetilde{\mathcal{C}} = \mathtt{pk} + \cdots + \mathtt{pk}^{[2w-1]}$
  3. If $\widetilde{\mathcal{C}}^{\perp}$ of dimension 1, linear algebra
     - $\Rightarrow$ P^*
     - $\Rightarrow$ X' and $Gab_{n-2w}(\mathrm{g}') = \mathrm{G}'$ such that $\mathtt{pk} = \langle (\mathrm{X}' \mid \mathrm{G}')\mathrm{P}^* \rangle$
- $\mathtt{Adv}_{\mathtt{Dist}}(D)$: p-time, large probability of success
- Not only a distinguisher: Recovers a decryption machine in polynomial-time

Overbeck's distinguisher - [GPT91, Ksh07, RGH10, OKN16]

- Note that $\mathrm{pk} = \langle (\mathrm{X} \mid \underbrace{\mathrm{G}}_{Gab_{n-2w}(\mathrm{g})=\langle \mathrm{G} \rangle})\mathrm{P} \rangle$, $\mathrm{P} \in M_n(\mathbb{F}_2)$
- Principle
  1. Compute $\mathrm{pk}^{[i]} = \left\langle \left(\mathrm{X}^{[i]} \mid \mathrm{G}^{[i]} \right) \mathrm{P} \right\rangle$
  2. Compute $\widetilde{\mathcal{C}} = \mathrm{pk} + \cdots + \mathrm{pk}^{[2w-1]}$
  3. If $\widetilde{\mathcal{C}}^{\perp}$ of dimension 1, linear algebra

     $\Rightarrow$ P^*

     $\Rightarrow$ X' and $Gab_{n-2w}(\mathrm{g}') = \mathrm{G}'$ such that $\mathrm{pk} = \langle (\mathrm{X}' \mid \mathrm{G}')\mathrm{P}^* \rangle$
- $\mathtt{Adv}_{\mathtt{Dist}}(D)$: p-time, large probability of success
- Not only a distinguisher: Recovers a decryption machine in polynomial-time

Overbeck's distinguisher - [GPT91, Ksh07, RGH10, OKN16]

- Note that $\mathtt{pk} = \langle (\mathrm{X} \mid \underbrace{\mathrm{G}}_{Gab_{n-2w}(\mathrm{g}) = \langle \mathrm{G} \rangle})\mathrm{P}\rangle$, $\mathrm{P} \in M_n(\mathbb{F}_2)$
- Principle
  1. Compute $\mathtt{pk}^{[i]} = \langle (\mathrm{X}^{[i]} \mid \mathrm{G}^{[i]})\,\mathrm{P}\rangle$
  2. Compute $\widetilde{\mathcal{C}} = \mathtt{pk} + \cdots + \mathtt{pk}^{[2w-1]}$
  3. If $\widetilde{\mathcal{C}}^{\perp}$ of dimension 1, linear algebra
     - $\Rightarrow$ P^*
     - $\Rightarrow$ X' and $Gab_{n-2w}(\mathrm{g}') = \mathrm{G}'$ such that $\mathtt{pk} = \langle (\mathrm{X}' \mid \mathrm{G}')\mathrm{P}^*\rangle$
- $\mathtt{Adv}_{\mathtt{Dist}}(D)$: p-time, large probability of success
- Not only a distinguisher: Recovers a decryption machine in polynomial-time

Overbeck's distinguisher - [GPT91, Ksh07, RGH10, OKN16]

- Note that $\mathtt{pk} = \langle (\mathbf{X} \mid \underbrace{\mathbf{G}}_{Gab_{n-2w}(\mathbf{g}) = \langle \mathbf{G} \rangle})\mathbf{P} \rangle$, $\mathbf{P} \in M_n(\mathbb{F}_2)$
- Principle
  1. Compute $\mathtt{pk}^{[i]} = \left\langle \left(\mathbf{X}^{[i]} \mid \mathbf{G}^{[i]}\right) \mathbf{P} \right\rangle$
  2. Compute $\widetilde{\mathcal{C}} = \mathtt{pk} + \cdots + \mathtt{pk}^{[2w-1]}$
  3. If $\widetilde{\mathcal{C}}^{\perp}$ of dimension 1, linear algebra
     - $\Rightarrow$ $\mathbf{P}^*$
     - $\Rightarrow$ $\mathbf{X}'$ and $Gab_{n-2w}(\mathbf{g}') = \mathbf{G}'$ such that $\mathtt{pk} = \langle (\mathbf{X}' \mid \mathbf{G}')\mathbf{P}^* \rangle$
- $\mathtt{Adv}_{\mathtt{Dist}}(D)$: p-time, large probability of success
- Not only a distinguisher: Recovers a decryption machine in polynomial-time

Some ideas to repair ?

- Find less structured codes for rank metric
  - Use of subfield subcodes ? Not sufficient !,[GL08]
- Find a new way to mask the structure
  - Simple
  - Efficient
  - Convincing

Some ideas to repair ?

- Find less structured codes for rank metric
  - Use of subfield subcodes ? Not sufficient !,[GL08]
- Find a new way to mask the structure
  - Simple
  - Efficient
  - Convincing

Intermezzo I

- How I met Gabidulin

Intermezzo II

- And did not meet Delsarte

Outline of the talk

Scrambling principle: rank multiplication

Proposition

Let $\mathcal{S} \subset \mathbb{F}_{2^m}$ *with* $\dim_2(\mathcal{S}) = \lambda$, *and let* $\mathrm{P} \in M_n(\mathcal{S})$, *then*

$$\forall \mathrm{x} \in \mathbb{F}_{2^m}^n, \;\; \mathrm{Rk}(\mathrm{xP}) \leq \lambda \, \mathrm{Rk}(\mathrm{x})$$

- Similar to taking subfield subcode in Hamming metric

Scrambling principle: rank multiplication

Proposition

Let $\mathcal{S} \subset \mathbb{F}_{2^m}$ *with* $\dim_2(\mathcal{S}) = \lambda$, *and let* $\mathrm{P} \in M_n(\mathcal{S})$, *then*

$$\forall \mathrm{x} \in \mathbb{F}_{2^m}^n, \ \ \mathrm{Rk}(\mathrm{xP}) \leq \lambda \, \mathrm{Rk}(\mathrm{x})$$

- Similar to taking subfield subcode in Hamming metric

The new encryption scheme- [Loi17] I

- $\mathcal{V} = \mathbb{F}_{2^m}^n$
- λ, integer
- $\mathcal{D} \subset \mathcal{V}$: vectors of rank w
- $\mathcal{F} = \{\mathrm{Gab}_{n-2\lambda w}(\mathrm{g}) \subset \mathbb{F}_{2^m}^n, \ \mathrm{g}\}$
  - $\mathtt{Decode}_{\mathcal{C}}$ algorithm
    - Deterministic
    - Up to errors of rank w

The new encryption scheme- [Loi17] II

1. $\texttt{KeyGen}()$
   - $\mathcal{C} \xleftarrow{\$} \mathcal{F}$
   - $\mathcal{S} \xleftarrow{\$} Gr_{\lambda,m}(\mathbb{F}_2)$,
   - $\mathsf{P} \xleftarrow{\$} \mathcal{M}_n(\mathcal{S})$
   - $\texttt{Return sk} = (\mathcal{C}, \mathsf{P})$, $\texttt{pk} = \mathcal{C}\mathsf{P}^{-1}$
2. $\texttt{Encrypt}(\texttt{pt}, \texttt{pk} := \langle \mathsf{G} \rangle = \mathcal{C}\mathsf{P}^{-1} \ ; \ r)$
   - $\mathsf{e} \xleftarrow{\$_r} \mathcal{D}$
   - $\texttt{Return ct} := \texttt{pt}\mathsf{G} + \mathsf{e}$
3. $\texttt{Decrypt}(\texttt{ct}, \texttt{sk})$
   - $\texttt{pt}^* := \texttt{Decode}_{\mathcal{C}}(\texttt{ct}\mathsf{P} = \texttt{pt}\mathsf{G}\mathsf{P} + \mathsf{e}\mathsf{P})$
   - $\texttt{Return pt}^*$

On the difficulty of computing $\mathtt{Adv}_{\mathtt{Dist}}(D)$

Two cases

1. $2w\lambda^2 < n \Leftrightarrow$ Rate $> (\lambda - 1)/\lambda$, [CC20, Gha22]
   1. Note that $\mathrm{pk}^\perp \subset \mathrm{Gab}_{2\lambda w}(\mathrm{g}_1) + \cdots + \mathrm{Gab}_{2\lambda w}(\mathrm{g}_\lambda)$
   2. Compute $\mathcal{C} = \mathrm{pk}^\perp + \cdots + (\mathrm{pk}^\perp)^{[\lambda]}$

      $\Rightarrow$ $\dim(\mathcal{C}) := d \leq \lambda(2w\lambda + 1)$
      - if $\mathrm{pk}^\perp$ random, then $\dim(\mathcal{C}) \approx \min(\underbrace{2w\lambda(\lambda+1)}_{>d}, n)$

      $\Rightarrow$ p-time probable distinguisher if $2w\lambda^2 < n$
2. $2w\lambda^2 \geq n \Leftrightarrow$ Rate $\leq (\lambda - 1)/\lambda$ - [Loi17, BL23]
   - See next

On the difficulty of computing $\mathtt{Adv}_{\mathtt{Dist}}(D)$

Two cases

1. $2w\lambda^2 < n \Leftrightarrow$ Rate $> (\lambda - 1)/\lambda$, [CC20, Gha22]
   1. Note that $\mathtt{pk}^{\perp} \subset \mathsf{Gab}_{2\lambda w}(\mathbf{g}_1) + \cdots + \mathsf{Gab}_{2\lambda w}(\mathbf{g}_\lambda)$
   2. Compute $\mathcal{C} = \mathtt{pk}^{\perp} + \cdots + (\mathtt{pk}^{\perp})^{[\lambda]}$

      $\Rightarrow$ $\dim(\mathcal{C}) := d \leq \lambda(2w\lambda + 1)$
      - if $\mathtt{pk}^{\perp}$ random, then $\dim(\mathcal{C}) \approx \min(\underbrace{2w\lambda(\lambda+1)}_{>d}, n)$

      $\Rightarrow$ p-time probable distinguisher if $2w\lambda^2 < n$
2. $2w\lambda^2 \geq n \Leftrightarrow$ Rate $\leq (\lambda - 1)/\lambda$ - [Loi17, BL23]
   - See next

On the difficulty of computing $\mathtt{Adv}_{\mathtt{Dist}}(D)$

Two cases

1. $2w\lambda^2 < n \Leftrightarrow$ Rate $> (\lambda - 1)/\lambda$, [CC20, Gha22]
   1. Note that $\mathtt{pk}^{\perp} \subset \mathsf{Gab}_{2\lambda w}(\mathsf{g}_1) + \cdots + \mathsf{Gab}_{2\lambda w}(\mathsf{g}_\lambda)$
   2. Compute $\mathcal{C} = \mathtt{pk}^{\perp} + \cdots + (\mathtt{pk}^{\perp})^{[\lambda]}$

      $\Rightarrow$ $\dim(\mathcal{C}) := d \leq \lambda(2w\lambda + 1)$
      - if $\mathtt{pk}^{\perp}$ random, then $\dim(\mathcal{C}) \approx \min(\underbrace{2w\lambda(\lambda+1)}_{>d}, n)$

      $\Rightarrow$ p-time probable distinguisher if $2w\lambda^2 < n$
2. $2w\lambda^2 \geq n \Leftrightarrow$ Rate $\leq (\lambda - 1)/\lambda$ - [Loi17, BL23]
   - See next

Outline of the talk

A linear approach

- $\mathrm{H} = (h_j^{[i]})_{i=0,j=0}^{2\lambda w-1,n-1}$, parity-check matrix for $\mathcal{C}$
  - Let $\alpha \in \mathbb{F}_2^m$ normal.

$$\exists \mathrm{M} \in \mathbb{F}_2^{m\times n}, \texttt{s.t.}\ \mathrm{H} = \underbrace{(\alpha^{[i+j]})_{i=0,j=0}^{2\lambda w-1,n-1}}_{\mathrm{H}_{norm}} \mathrm{M}$$

- Given H_{pub}, parity-check matrix for pk

$$\exists \mathrm{S} \in \mathcal{M}_{2\lambda w}(\mathbb{F}_{2^m}), \texttt{s.t.}\ \mathrm{H}_{pub} = \mathrm{S}^{-1}\mathrm{H}\,{}^t\mathrm{P} \qquad (1)$$

- Rewriting equation (1) we obtain

$$\mathrm{S}\mathrm{H}_{pub} = \mathrm{H}_{norm} \underbrace{\mathrm{M}\,{}^t\mathrm{P}}_{\mathrm{T}\in\mathcal{S}^{m\times n}}, \qquad (2)$$

A linear approach

- $\mathsf{H} = (h_j^{[i]})_{i=0,j=0}^{2\lambda w-1,n-1}$, parity-check matrix for $\mathcal{C}$
  - Let $\alpha \in \mathbb{F}_2^m$ normal.

$$\exists \mathsf{M} \in \mathbb{F}_2^{m\times n}, \texttt{s.t.}\ \mathsf{H} = \underbrace{(\alpha^{[i+i]})_{i=0,j=0}^{2\lambda w-1,n-1}}_{\mathsf{H}_{norm}} \mathsf{M}$$

- Given H_{pub}, parity-check matrix for pk

$$\exists \mathsf{S} \in \mathcal{M}_{2\lambda w}(\mathbb{F}_{2^m}), \texttt{s.t.}\ \mathsf{H}_{pub} = \mathsf{S}^{-1}\mathsf{H}\ {}^t\mathsf{P} \qquad (1)$$

- Rewriting equation (1) we obtain

$$\mathsf{S}\mathsf{H}_{pub} = \mathsf{H}_{norm} \underbrace{\mathsf{M}\ {}^t\mathsf{P}}_{\mathsf{T}\in\mathcal{S}^{m\times n}}, \qquad (2)$$

A linear approach

- $\mathsf{H} = (h_j^{[i]})_{i=0,j=0}^{2\lambda w-1,n-1}$, parity-check matrix for $\mathcal{C}$
  - Let $\alpha \in \mathbb{F}_2^m$ normal.

$$\exists \mathsf{M} \in \mathbb{F}_2^{m\times n}, \texttt{s.t. } \mathsf{H} = \underbrace{(\alpha^{[i+i]})_{i=0,j=0}^{2\lambda w-1,n-1}}_{\mathsf{H}_{norm}} \mathsf{M}$$

- Given H_{pub}, parity-check matrix for $\mathtt{pk}$

$$\exists \mathsf{S} \in \mathcal{M}_{2\lambda w}(\mathbb{F}_{2^m}), \texttt{s.t. } \mathsf{H}_{pub} = \mathsf{S}^{-1}\mathsf{H}\,{}^t\mathsf{P} \qquad (1)$$

- Rewriting equation (1) we obtain

$$\mathsf{S}\mathsf{H}_{pub} = \mathsf{H}_{norm} \underbrace{\mathsf{M}\,{}^t\mathsf{P}}_{\mathsf{T}\in\mathcal{S}^{m\times n}}, \qquad (2)$$

A linear approach

- $\mathsf{H} = (h_j^{[i]})_{i=0,j=0}^{2\lambda w-1,n-1}$, parity-check matrix for $\mathcal{C}$
  - Let $\alpha \in \mathbb{F}_2^m$ normal.

$$\exists \mathsf{M} \in \mathbb{F}_2^{m\times n}, \texttt{s.t. } \mathsf{H} = \underbrace{(\alpha^{[i+j]})_{i=0,j=0}^{2\lambda w-1,n-1}}_{\mathsf{H}_{norm}} \mathsf{M}$$

- Given H_{pub}, parity-check matrix for $\mathtt{pk}$

$$\exists \mathsf{S} \in \mathcal{M}_{2\lambda w}(\mathbb{F}_{2^m}), \texttt{s.t. } \mathsf{H}_{pub} = \mathsf{S}^{-1}\mathsf{H}\ {}^t\mathsf{P} \tag{1}$$

- Rewriting equation (1) we obtain

$$\mathsf{S}\mathsf{H}_{pub} = \mathsf{H}_{norm} \underbrace{\mathsf{M}\ {}^t\mathsf{P}}_{\mathsf{T}\in\mathcal{S}^{m\times n}}, \tag{2}$$

The key system I

System (γ)

$$\mathrm{V}\mathrm{H}_{pub} = \mathrm{H}_{norm}\mathrm{W}. \tag{3}$$

where $\mathrm{V} \in \mathbb{F}_{2^m}^{2\lambda w \times 2\lambda w}$ *and* $\mathrm{W} \in \mathcal{Z}^{\mathrm{m}\times\mathrm{n}}$, *where* $\mathcal{Z} \subset \mathbb{F}_{2^m}$ *with dimension* γ.

Remark

If (V, W) *satisfies* $\mathrm{System}(\gamma)$ *then* $(\alpha\mathrm{V}, \alpha\mathrm{W})$ *also*

The key system II

Properties of the system

- Number of equations: $2\lambda wn \times m$ over $\mathbb{F}_2$
- Number of variables: $(2\lambda w)^2 \times m + nm \times \gamma$ over $\mathbb{F}_2$

Estimated number of solutions: $\max(1, 2^{m[(2\lambda w)^2+n(\gamma-2\lambda w)]})$

$$\gamma < 2\lambda w\left(1-\frac{2\lambda w}{n}\right) = nR(1-R) \Longrightarrow \text{System overdefined}$$

Distinguisher and key system I

- Algorithm D(γ)
  1. $\mathcal{Z} \xleftarrow{\$} \mathcal{V}$ of dimension γ
  2. $\mathcal{N} \leftarrow \{(\mathsf{V}, \mathsf{W})\}$, $\mathsf{W} \subset \mathcal{Z}^{\mathsf{m} \times \mathsf{n}}$ solutions to system (3)
  3. if $\mathcal{N} \neq (0, 0)$ then return 1 else return 0
- D runs in polynomial-time
  - Step 2 solved by Gauss or Wiedemann
- $\mathtt{Adv}_{\mathtt{Dist}}(D) = \Pr(D \;\; \mathtt{returns} \;\; 1)$

Distinguisher and key system II

- (S, T) is a non-zero solution to System(λ)
- Assumption:

  If $\lambda \leq \gamma < nR(1-R)$, D returns 1 iff $\exists \alpha \neq 0$ such that $\mathcal{Z} = \alpha \mathcal{S}$

- Probability of success

$$\mathcal{P} = \Pr(\exists \alpha \in \mathbb{F}_{2^m}^*, \text{ s.t. } \alpha \mathcal{S} \subset \mathcal{Z}) = (q^m - 1) \frac{\begin{bmatrix} m \\ \gamma - \lambda \end{bmatrix}_2}{\begin{bmatrix} m \\ \gamma \end{bmatrix}_2}$$

$\Rightarrow$ $\gamma = nR(1-R)$ is the optimal choice

$$\mathtt{Adv}_{\mathtt{Dist}}(D) = \mathcal{P} \approx 2^{-(\lambda-1)m + \lambda\gamma}$$

More than that: recovering a decryption machine

Proposition

Let $\mathbf{V}$, $\mathbf{W}$ *solutions to* (3), *where*

- $\mathbf{W} \in \mathcal{W}^{m \times n}$, *with* $\dim_2(\mathcal{W}) \leq \lambda$

Then any ciphertext can be decrypted in polynomial time.

Some parameters

By taking into consideration

1. The approach in [BBC$^+$20]
2. The advantage of distinguisher D

$m = n$	λ	w	PK	CT	$\mathtt{Adv}^{OW}_{\mathtt{GenDec}}$	$\mathtt{Adv}_{\mathtt{Dist}}$
128	3	18	34 kB	1.8 kB	2^{-180}	2^{-261}
128	3	7	58 kB	1.3 kB	2^{-275}	2^{-311}

Some parameters

By taking into consideration

1. The approach in [BBC+20]
2. The advantage of distinguisher D

$m = n$	λ	w	PK	CT	$\mathtt{Adv}^{OW}_{\mathtt{GenDec}}$	$\mathtt{Adv}_{\mathtt{Dist}}$
128	3	18	34 kB	1.8 kB	2^{-180}	2^{-261}
128	3	7	58 kB	1.3 kB	2^{-275}	2^{-311}

Multidimensional approach - LowMS [ADG+22] I

- $\mathcal{V} = \mathbb{F}_{2^m}^{n\times\ell}$
- λ, integer
- ℓ, integer - interleaving order
- $\mathcal{D} =$ vectors of rank w subset of $\mathbb{F}_{2^m}^{n\times\ell}$
- $\mathcal{F} = \{\mathrm{Gab}_{n-k}(g) \otimes \cdots \otimes \mathrm{Gab}_{n-k}(g) \subset \mathbb{F}_{2^m}^{n\times\ell},\ g\}$
  - $\mathtt{IDecode}_{\mathcal{C},\ell}$
  - probabilistic with probability of success *DFR*

$$\approx 3.5\ 2^{m\left[(\ell+1)\left(\frac{\ell}{\ell+1}k-w\right)+1\right]}$$

Multidimensional approach - LowMS [ADG+22] II

1. KeyGen()
   - $\mathcal{C} \xleftarrow{\$} \mathcal{F}$
   - $\mathcal{S} \xleftarrow{\$} Gr_{\lambda,m}(\mathbb{F}_2)$,
   - $\mathrm{P} \xleftarrow{\$} \mathcal{M}_n(\mathcal{S})$
   - Return sk $=(\mathcal{C}, \mathrm{P})$, pk $= \mathcal{C}\mathrm{P}^{-1}$
2. $\mathtt{Encrypt}(\mathtt{pt}_1, \ldots, \mathtt{pt}_\ell, \mathtt{pk} := \langle \mathrm{G} \rangle = \mathcal{C}\mathrm{P}^{-1} \; ; \; r)$
   - $\mathrm{e}_1, \ldots, \mathrm{e}_\ell \xleftarrow{\$_r} \mathcal{D}$
   - Return $\mathtt{ct}_1 := \mathtt{pt}_1\mathrm{G} + \mathrm{e}_1, \ldots, \mathtt{ct}_\ell := \mathtt{pt}_\ell\mathrm{G} + \mathrm{e}_\ell$
3. $\mathtt{Decrypt}(\mathtt{ct}_1, \ldots, \mathtt{ct}_\ell, \mathtt{sk})$
   - $\mathtt{pt}_1^*, \ldots, \mathtt{pt}_\ell^* := \mathtt{IDecode}_{\mathcal{C},\ell}(\mathtt{ct}_1\mathrm{P}, \ldots, \mathtt{ct}_\ell\mathrm{P})$
   - Return $\mathtt{pt}_1^*, \ldots, \mathtt{pt}_\ell^*$

Multidimensional approach - LowMS [ADG+22] III

- Advantages

m	n	k	λ	w	ℓ	PK	CT	$\mathtt{Adv}^{OW}_{\mathtt{GenDec}}$	$\mathtt{Adv}_{\mathtt{Dist}}$	DFR
61	50	25	3	7	6	4.8 kB	1.2 kB	2^{-139}	2^{-131}	2^{-242}
101	88	44	4	9	5	24.4 kB	2.8 kB	2^{-278}	2^{-267}	2^{-503}

- Drawbacks
  - Probabilistic decoding $\Rightarrow$ More complex security analysis
  - $\mathtt{Adv}_{\mathtt{GenDec}}$: relies on *RSL* problem and not *RSD*

Designing Encryption Schemes for Dummies

- Use the proposed framework
- Beware of the advantages
- Take care of efficiency and security of implementations
  - Parameters sizes
  - Side-channel attacks (out of the scope of the talk)

Designing Encryption Schemes for Dummies

- Use the proposed framework
- Beware of the advantages
- Take care of efficiency and security of implementations
  - Parameters sizes
  - Side-channel attacks (out of the scope of the talk)

Designing Encryption Schemes for Dummies

- Use the proposed framework
- Beware of the advantages
- Take care of efficiency and security of implementations
  - Parameters sizes
  - Side-channel attacks (out of the scope of the talk)

Research directions

- Algebraic analysis of System (3)
- Use of other metrics to desing encryption schemes
- Fill the gap for the distinguisher
- Does Delsarte really exist ?

Research directions

- Algebraic analysis of System (3)
- Use of other metrics to desing encryption schemes
- Fill the gap for the distinguisher
- Does Delsarte really exist ?

Research directions

- Algebraic analysis of System (3)
- Use of other metrics to desing encryption schemes
- Fill the gap for the distinguisher
- Does Delsarte really exist ?

Research directions

- Algebraic analysis of System (3)
- Use of other metrics to desing encryption schemes
- Fill the gap for the distinguisher
- Does Delsarte really exist ?

Research directions

- Algebraic analysis of System (3)
- Use of other metrics to desing encryption schemes
- Fill the gap for the distinguisher
- Does Delsarte really exist ?

References I

N. Aragon, V. Dyseryn, P. Gaborit, P. Loidreau, J. Renner, and A. Wachter-Zeh.
LowMS: a new rank metric code-based KEM without ideal structure.
IACR Cryptol. ePrint Arch., page 1596, 2022.

M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. A. Perlner, D. Smith-Tone, J.-P. Tillich, and J. A. Verbel.
Improvements of algebraic attacks for solving the rank decoding and minrank problems.
In *ASIACRYPT 2020*, volume 12491 of *LNCS*, pages 507–536. Springer, 2020.

References II

P. Briaud and P. Loidreau.
Cryptanalysis of Rank-Metric Schemes Based on Distorted Gabidulin Codes.
In T. Johansson and D. Smith-Tone, editors, *14th International Workshop, PQCrypto 2023*, volume 14154 of *LNCS*, pages 38–56, 2023.

D. Coggia and A. Couvreur.
On the security of a Loidreau rank metric code based encryption scheme.
Des. Codes Cryptogr., 88(9):1941–1957, 2020.

P. Delsarte.
Bilinear forms over a finite field, with applications to coding theory.
J. Comb. Theory, Ser. A, 25(3):226–241, 1978.

References III

E. M. Gabidulin.
Theory of codes with maximum rank distance.
Probl. Inf. Transm., 21(1):3–16, 1985.

A. Ghatak.
Extending coggia-couvreur attack on loidreau's rank metric cryptosystem.
Des. Codes Cryptogr., 90:215–238, 2022.

E. M. Gabidulin and P. Loidreau.
Properties of subspace subcodes of Gabidulin codes.
Adv. in Math. of Comm., 2(2):147–157, 2008.

References IV

E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov.
Ideals over a non-commutative ring and their applications to cryptography.
In *Advances in Cryptology - EUROCRYPT'91*, number 547 in Lecture Notes in Comput. Sci., pages 482–489, Brighton, April 1991.

A. Kshevetskiy.
Security of GPT-like public-key cryptosystems based on linear rank codes.
In *3rd International Workshop on Signal Design and Its Applications in Communications, IWSDA 2007*, 2007.

References V

P. Loidreau.
A new rank metric codes based encryption scheme.
In *PQCrypto 2017*, volume 10346 of *LNCS*, pages 3–17. Springer, 2017.

A. Otmani, H. T. Kalashi, and S. Ndjeya.
Improved cryptanalysis of rank metric schemes based on Gabidulin codes.
http://arxiv.org/abs/1602.08549v1, 2016.

H. Rashwan, E. M. Gabidulin, and B. Honary.
A smart approach for GPT cryptosystem based on rank codes.
In *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, pages 2463–2467, 2010.