An Algebraic Attack on Rank Metric Code-Based Cryptosystems

Maxime Bros

Journées Codage & Cryptographie 2020

Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, Vincent Neiger, Olivier Ruatta, Jean-Pierre Tillich

November, 2020

A simple problem in linear algebra

Let $k < n$ be integers, $H \in \mathbb{F}_q^{(n-k)\times n}$, $e \in \mathbb{F}_q^{n\times 1}$, and $s \in \mathbb{F}_q^{(n-k)\times 1}$.

$$\begin{pmatrix} & \mathbf{H} & \end{pmatrix} \begin{pmatrix} \\ e \\ \\ \end{pmatrix} = \begin{pmatrix} s \end{pmatrix}$$

A simple problem in linear algebra

Let $k < n$ be integers, $H \in \mathbb{F}_q^{(n-k)\times n}$, $e \in \mathbb{F}_q^{n\times 1}$, and $s \in \mathbb{F}_q^{(n-k)\times 1}$.

$$\begin{pmatrix} \mathrm{H} & \boxed{A} \end{pmatrix} \begin{pmatrix} e \end{pmatrix} = \begin{pmatrix} s \end{pmatrix}$$

$\implies A^{-1}s$ gives a solution for e

- One easily finds one or several solutions for e

A simple problem in linear algebra

Let $k < n$ be integers, $H \in \mathbb{F}_q^{(n-k)\times n}$, $e \in \mathbb{F}_q^{n\times 1}$, and $s \in \mathbb{F}_q^{(n-k)\times 1}$.

$$\begin{pmatrix} \mathrm{H} & A \end{pmatrix} \begin{pmatrix} e \end{pmatrix} = \begin{pmatrix} s \end{pmatrix} \implies A^{-1}s \text{ gives a solution for } e$$

- One easily finds one or several solutions for e
- Therefore, one can not control the **weight** of e for a given metric !

Rank Syndrome Decoding Problem (RSD)

Definition (Syndrome Decoding (SD) Problem - computational version)

Input : a parity-check matrix $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ of a code $\mathcal{C}$ (i.e. a subspace of $\mathbb{F}_{q^m}^n$), an integer $r \in \mathbb{N}$ and a vector $s \in \mathbb{F}_{q^m}^{n-k}$.
Output : a vector $e \in \mathbb{F}_{q^m}^n$ such that $He^T = s^T$ and $w(e) \leq r$.

Definition (Decoding Problem - computational version)

Input : a code $\mathcal{C}$ (i.e. a subspace of $\mathbb{F}_{q^m}^n$), an integer $r \in \mathbb{N}$ and a vector $y \in \mathbb{F}_{q^m}^n$.
Output : $c \in \mathcal{C}$ such that $w(y-c) = w(e) \leq r$.

Rank Syndrome Decoding Problem (RSD)

Definition (Syndrome Decoding (SD) Problem - computational version)

Input : a parity-check matrix $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ of a code $\mathcal{C}$ (i.e. a subspace of $\mathbb{F}_{q^m}^n$), an integer $r \in \mathbb{N}$ and a vector $s \in \mathbb{F}_{q^m}^{n-k}$.
Output : a vector $e \in \mathbb{F}_{q^m}^n$ such that $He^T = s^T$ and $w(e) \leq r$.

Definition (Decoding Problem - computational version)

Input : a code $\mathcal{C}$ (i.e. a subspace of $\mathbb{F}_{q^m}^n$), an integer $r \in \mathbb{N}$ and a vector $y \in \mathbb{F}_{q^m}^n$.
Output : $c \in \mathcal{C}$ such that $w(y-c) = w(e) \leq r$.

These 2 problems are equivalent.

Rank Syndrome Decoding Problem (RSD)

Definition (Syndrome Decoding (SD) Problem - computational version)

Input : a parity-check matrix $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ of a code $\mathcal{C}$ (i.e. a subspace of $\mathbb{F}_{q^m}^n$), an integer $r \in \mathbb{N}$ and a vector $s \in \mathbb{F}_{q^m}^{n-k}$.
Output : a vector $e \in \mathbb{F}_{q^m}^n$ such that $He^T = s^T$ and $w(e) \leq r$.

Definition (Decoding Problem - computational version)

Input : a code $\mathcal{C}$ (i.e. a subspace of $\mathbb{F}_{q^m}^n$), an integer $r \in \mathbb{N}$ and a vector $y \in \mathbb{F}_{q^m}^n$.
Output : $c \in \mathcal{C}$ such that $w(y - c) = w(e) \leq r$.

These 2 problems are equivalent.

- Euclidian metric $\Longrightarrow$ lattice-based cryptography
- Hamming metric $\Longrightarrow$ code-based cryptography
- Rank metric $\Longrightarrow$ rank-based cryptography

- SD proven NP-complete for the Hamming metric in 1978 (Berlekamp and al.)

Rank Syndrome Decoding Problem (RSD)

Definition (Syndrome Decoding (SD) Problem - computational version)

Input : a parity-check matrix $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ of a code $\mathcal{C}$ (i.e. a subspace of $\mathbb{F}_{q^m}^n$), an integer $r \in \mathbb{N}$ and a vector $s \in \mathbb{F}_{q^m}^{n-k}$.
Output : a vector $e \in \mathbb{F}_{q^m}^n$ such that $He^T = s^T$ and $w(e) \leq r$.

Definition (Decoding Problem - computational version)

Input : a code $\mathcal{C}$ (i.e. a subspace of $\mathbb{F}_{q^m}^n$), an integer $r \in \mathbb{N}$ and a vector $y \in \mathbb{F}_{q^m}^n$.
Output : $c \in \mathcal{C}$ such that $w(y - c) = w(e) \leq r$.

These 2 problems are equivalent.

- Euclidian metric $\Longrightarrow$ lattice-based cryptography
- Hamming metric $\Longrightarrow$ code-based cryptography
- Rank metric $\Longrightarrow$ rank-based cryptography

- SD proven NP-complete for the Hamming metric in 1978 (Berlekamp and al.)
- **Rank-SD (RSD)** strongly believed to be NP-complete as well
- Randomized reduction from an NP-complete problem in 2017 (Gaborit, Zémor)

Rank metric with an example

Let $B = \{1, b_2, b_3, b_4\}$ be a basis of $\mathbb{F}_{2^4}$ seen as an $\mathbb{F}_2$-vector space.

$$v := \quad \begin{pmatrix} \alpha^9 & 1 & \alpha^9 & 0 & \alpha^7 \end{pmatrix} \in (\mathbb{F}_{2^4})^5$$

Rank metric with an example

Let $B = \{1, b_2, b_3, b_4\}$ be a basis of $\mathbb{F}_{2^4}$ seen as an $\mathbb{F}_2$-vector space.

$$v := \begin{pmatrix} \alpha^9 & 1 & \alpha^9 & 0 & \alpha^7 \end{pmatrix} \in (\mathbb{F}_{2^4})^5$$

$$M := \begin{array}{c} 1 \\ b_2 \\ b_3 \\ b_4 \end{array} \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix} \in (\mathbb{F}_2)^{4 \times 5}$$

Rank metric with an example

Let $B = \{1, b_2, b_3, b_4\}$ be a basis of $\mathbb{F}_{2^4}$ seen as an $\mathbb{F}_2$-vector space.

$$v := \begin{pmatrix} \alpha^9 & 1 & \alpha^9 & 0 & \alpha^7 \end{pmatrix} \in (\mathbb{F}_{2^4})^5$$

$$M := \begin{array}{c} 1 \\ b_2 \\ b_3 \\ b_4 \end{array} \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix} \in (\mathbb{F}_2)^{4\times 5}$$

$$\mathrm{Rank}(v) := \mathrm{Rank}(M) = 2.$$

Why is the RSD problem important ?

Why is the RSD problem important ?

- **RSD** is at the core of Rank-based cryptosystems.

Why is the RSD problem important ?

- **RSD** is at the core of Rank-based cryptosystems.
- 2 Rank-based cryptosystems (ROLLO and RQC) made it to the 2^{nd} Round of the celebrated NIST Post-Quantum Standardization Process.

NIST
National Institute of
Standards and Technology

Why is the RSD problem important ?

- **RSD** is at the core of Rank-based cryptosystems.
- 2 Rank-based cryptosystems (ROLLO and RQC) made it to the 2^{nd} Round of the celebrated NIST Post-Quantum Standardization Process.

NIST
National Institute of
Standards and Technology

- They did not reach the Third Round... **because of our attacks !**

Why is the RSD problem important ?

- **RSD** is at the core of Rank-based cryptosystems.
- 2 Rank-based cryptosystems (ROLLO and RQC) made it to the 2^{nd} Round of the celebrated NIST Post-Quantum Standardization Process.

NIST
National Institute of
Standards and Technology

- They did not reach the Third Round... **because of our attacks !**
- Nevertheless, in their report "NISTIR 8309" on the Second Round, NIST emphasized on the importance to keep studying Rank-based cryptography :

"Despite the development of algebraic attacks, NIST believes rank-based cryptography should continue to be researched. The rank metric cryptosystems offer a nice alternative to traditional hamming metric codes with comparable bandwidth."

Algebraic attack

- **Algebraic Attack :** one models a problem with a **system of equations** and solve it.
- Classic approach : Gröbner basis (GB) computation

Algebraic attack

- **Algebraic Attack :** one models a problem with a **system of equations** and solve it.
- Classic approach : Gröbner basis (GB) computation
- The more equations, the easier.

Complexity of GB algorithms

System of equations

$\{f_1, \ldots, f_m\} \in \mathbb{F}_q[x_1, \ldots, x_n]$

$$\begin{cases} f_1(x_1, x_2, \ldots, x_n) = 0 \\ f_2(x_1, x_2, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, x_2, \ldots, x_n) = 0 \end{cases}$$

Complexity of GB algorithms

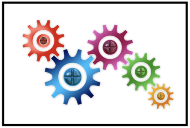
System of equations

$\{f_1, \dots, f_m\} \in \mathbb{F}_q[x_1, \dots, x_n]$

$$\begin{cases} f_1(x_1, x_2, \dots, x_n) = 0 \\ f_2(x_1, x_2, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, x_2, \dots, x_n) = 0 \end{cases}$$

$\longrightarrow$

Gröbner basis algorithm



$\longrightarrow$

Solution

$$\begin{cases} x_1 = c_1 \in \mathbb{F}_q \\ x_2 = c_2 \in \mathbb{F}_q \\ \vdots \\ x_n = c_n \in \mathbb{F}_q \end{cases}$$

Complexity of GB algorithms

System of equations

$\{f_1, \ldots, f_m\} \in \mathbb{F}_q[x_1, \ldots, x_n]$

$$\begin{cases} f_1(x_1, x_2, \ldots, x_n) = 0 \\ f_2(x_1, x_2, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, x_2, \ldots, x_n) = 0 \end{cases}$$

Gröbner basis algorithm

$$\mathcal{O}\left(\binom{n+d}{d}^{2.807}\right)$$

Solution

$$\begin{cases} x_1 = c_1 \in \mathbb{F}_q \\ x_2 = c_2 \in \mathbb{F}_q \\ \vdots \\ x_n = c_n \in \mathbb{F}_q \end{cases}$$

The core of our attack

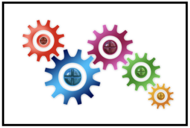
System of equations

$\{f_1, \dots, f_m\} \in \mathbb{F}_q[x_1, \dots, x_n]$

$$\begin{cases} f_1(x_1, x_2, \dots, x_n) = 0 \\ f_2(x_1, x_2, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, x_2, \dots, x_n) = 0 \end{cases}$$

Additional equations

Gröbner basis algorithm



$$\mathcal{O}\left(\binom{n+d}{d}^{2.807}\right)$$

Solution

$$\begin{cases} x_1 = c_1 \in \mathbb{F}_q \\ x_2 = c_2 \in \mathbb{F}_q \\ \vdots \\ x_n = c_n \in \mathbb{F}_q \end{cases}$$

The core of our attack

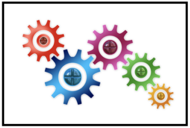
System of equations

$\{f_1, \ldots, f_m\} \in \mathbb{F}_q[x_1, \ldots, x_n]$

$$\begin{cases} f_1(x_1, x_2, \ldots, x_n) = 0 \\ f_2(x_1, x_2, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, x_2, \ldots, x_n) = 0 \end{cases}$$

Additional equations

Gröbner basis algorithm



$$\mathcal{O}\left(\binom{n+d}{d}^{2.807}\right)$$

$$d \searrow$$

Solution

$$\begin{cases} x_1 = c_1 \in \mathbb{F}_q \\ x_2 = c_2 \in \mathbb{F}_q \\ \vdots \\ x_n = c_n \in \mathbb{F}_q \end{cases}$$

The additional equations

- Let $G \in \mathbb{F}_{q^m}^{(k+1)\times n}$ be the generator matrix of a code $\mathcal{C}$ augmented by a received word $y = c + e$ where $c \in \mathcal{C}$ and $\mathrm{Rank}\,(e) \leq r$.
- The original modeling by Ourivski-Johansson is

$$(1, \alpha, \alpha^2, \ldots, \alpha^{m-1})S(C_2 - C_1 R) = 0, \quad \text{over } \mathbb{F}_{q^m} \text{ with solutions in } \mathbb{F}_q. \tag{1}$$

  (it comes from writting e as a product of two matrices S and $C := (C_1|C_2)$ **with entries in the ground field** $\mathbb{F}_q$)
- Our **additional equations** are all the maximal minors of the following matrix :

$$(C_2 - C_1 R).$$

- The new equations belong to the ideal generated by equations in (1).
- We found them using the **fundamental results** by Faugere and al. (2011) and Verbel and al. (2019). It is based on the use of **kernel of jacobian matrices** associated to the system.
- **With those new equations, d_{solv} goes down to r or $r+1$ for most of the cryptographic parameters.**

Our attack

Cryptosystem	Parameters (m, n, k, r)	Our attack	Previous
Loidreau	$(128, 120, 80, 4)$	**96.3**	256
ROLLO-I-128	$(79, 94, 47, 5)$	**114.9**	128
ROLLO-I-192	$(89, 106, 53, 6)$	**142.2**	192
ROLLO-I-256	$(113, 134, 67, 7)$	**195.3**	256
ROLLO-II-128	$(83, 298, 149, 5)$	**132.3**	128
ROLLO-II-192	$(107, 302, 151, 6)$	**161.5**	192
ROLLO-II-256	$(127, 314, 157, 7)$	**215.4**	256
ROLLO-III-128	$(101, 94, 47, 5)$	**117.1**	128
ROLLO-III-192	$(107, 118, 59, 6)$	**145.7**	192
ROLLO-III-256	$(131, 134, 67, 7)$	**197.5**	256
RQC-I	$(97, 134, 67, 5)$	**121.1**	128
RQC-II	$(107, 202, 101, 6)$	**154.2**	192
RQC-III	$(137, 262, 131, 7)$	**211.9**	256

To be continued...

We improved our algebraic attack against RSD in a new paper :

"Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems".

To be continued...

We improved our algebraic attack against RSD in a new paper :

"Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems".

- New modeling based on the previous one together with equations coming from a new modeling to solve the **MinRank Problem**.
- **Improvements of algebraic attacks against MinRank as well.**
- **No more Gröbner basis !**
- Joint work with : Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel.

To be continued...

We improved our algebraic attack against RSD in a new paper :

"Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems".

- New modeling based on the previous one together with equations coming from a new modeling to solve the **MinRank Problem**.
- **Improvements of algebraic attacks against MinRank as well.**
- **No more Gröbner basis !**
- Joint work with : Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel.

I will present this work with more details during a 1 hour talk at the seminar of the **Computer Algebra Team of XLIM, University of Limoges** at

10h30 a.m, December 3rd, 2020.

You are very welcome to attend it online, contact me at:

maxime.bros@unilim.fr