Algebraic Cryptanalysis of the Rank Decoding and the MinRank problems

Maxime Bros

Project-Team GRACE Seminar

November 22nd 2022, Inria Saclay

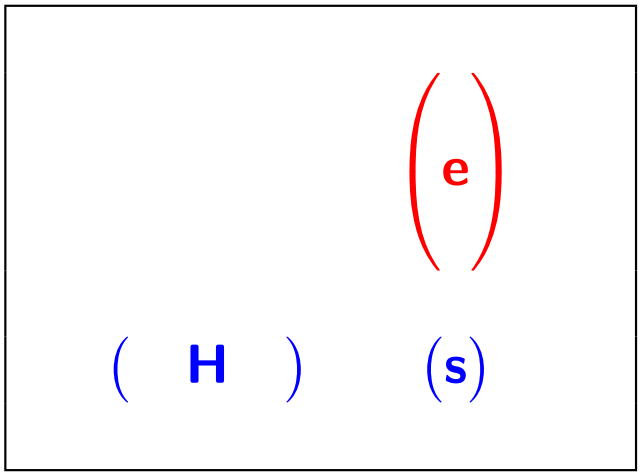
MinRank

$$\text{Rank}\left(\sum_i x_i M_i\right) \leq r$$

Multivariate-based Cryptography

HFE, Rainbow, ...

Rank Decoding



Rank-based Cryptography

ROLLO, RQC, Durandal, ...

Algebraic Cryptanalysis

Algebraic attack

- **Algebraic Attack:** one models a problem/cryptosystem with a **system of algebraic equations** and solves it.
- **Unique** solution.
- Solution: **private key** or the **plaintext**.
- Classic approaches:
  - multivariate resultant
  - regular chains
  - **Gröbner basis (GB) algorithms**
    (F4 [Faugère, 1999], F5 [Faugère, 2002], XL [Courtois et al., 2000].)

Linearization

- Number of equations $\approx$ number of **distinct monomials** in the system.
- Solve the system directly by **linearization**,
- $\Longrightarrow$ huge **linear system**.
- Strassen (1969) or Wiedemann (1986) algorithms.

$$\begin{cases} f_1 = xz + yz + z \\ f_2 = yz + z + 1 \\ f_3 = xyz + xz + 1 \\ f_4 = xyz + z + 1 \end{cases}, \quad \in \mathbb{F}_2[x, y, z].$$

- $(x_0, y_0, z_0) \in (\mathbb{F}_2)^3$ s.t.

$$f_i(x_0, y_0, z_0) = 0, \ \forall \ i \in \{1, 2, 3, 4\}.$$

- 20 dictinct monomials of degree less than or equal to 3 in $\mathbb{F}_2[x, y, z]$.
- **5 monomials / 4 equations.**

$$(c_1, c_2, c_3, c_4, 1)^\top \in \mathrm{Ker}_R\left(\mathcal{M}^{\mathrm{ac}}_{\leq 3}\right)$$

$$\begin{array}{c} \begin{matrix} xyz & xz & yz & z & 1 \end{matrix} \\ \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array} \Longrightarrow \begin{cases} xyz &= 0 \\ xz &= 1 \\ yz &= 0 \\ z &= 1 \end{cases} \Longrightarrow \begin{cases} x &= 1 \\ y &= 0 \\ z &= 1 \end{cases}$$

MinRank

Definition (MinRank Problem)

Input: K matrices $m \times n$ with coefficients in $\mathbb{F}_q$: $M_1, M_2, \ldots, M_K$, and an integer $r \in \mathbb{N}$.
Output: elements $x_1, x_2, \ldots, x_K \in \mathbb{F}_q$, such that $(x_1, x_2, \ldots, x_K) \neq (0, 0, \ldots, 0)$ and

$$\text{Rank}\left(\sum_{i=1}^{K} x_i M_i\right) \leq r.$$

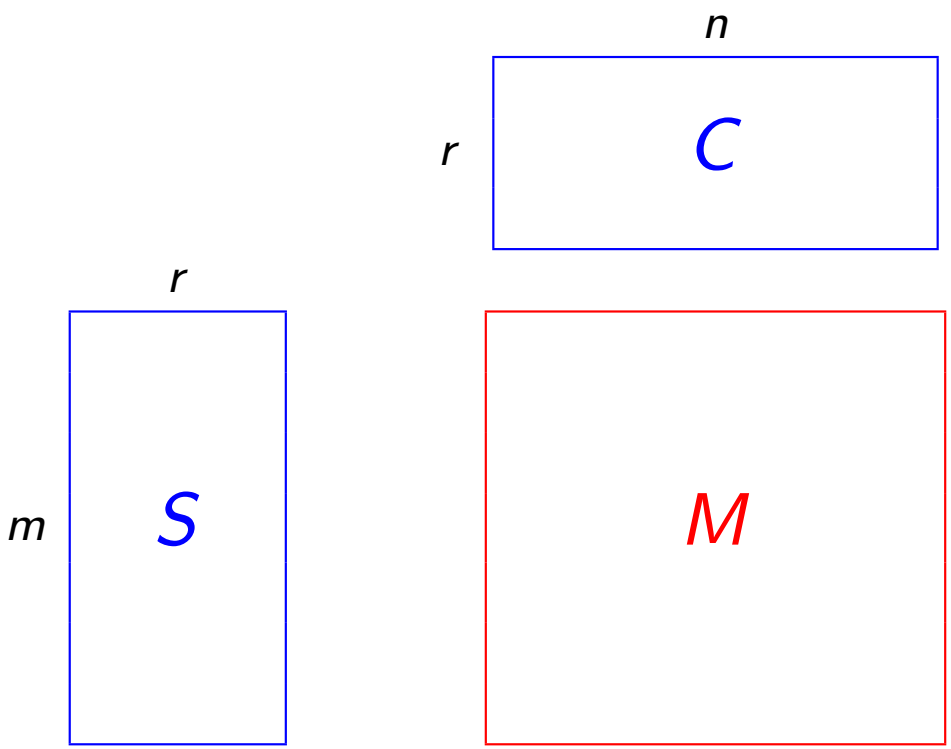
MinRank proven NP-complete in 1999 (Buss et al.).

Important fact in our modelings

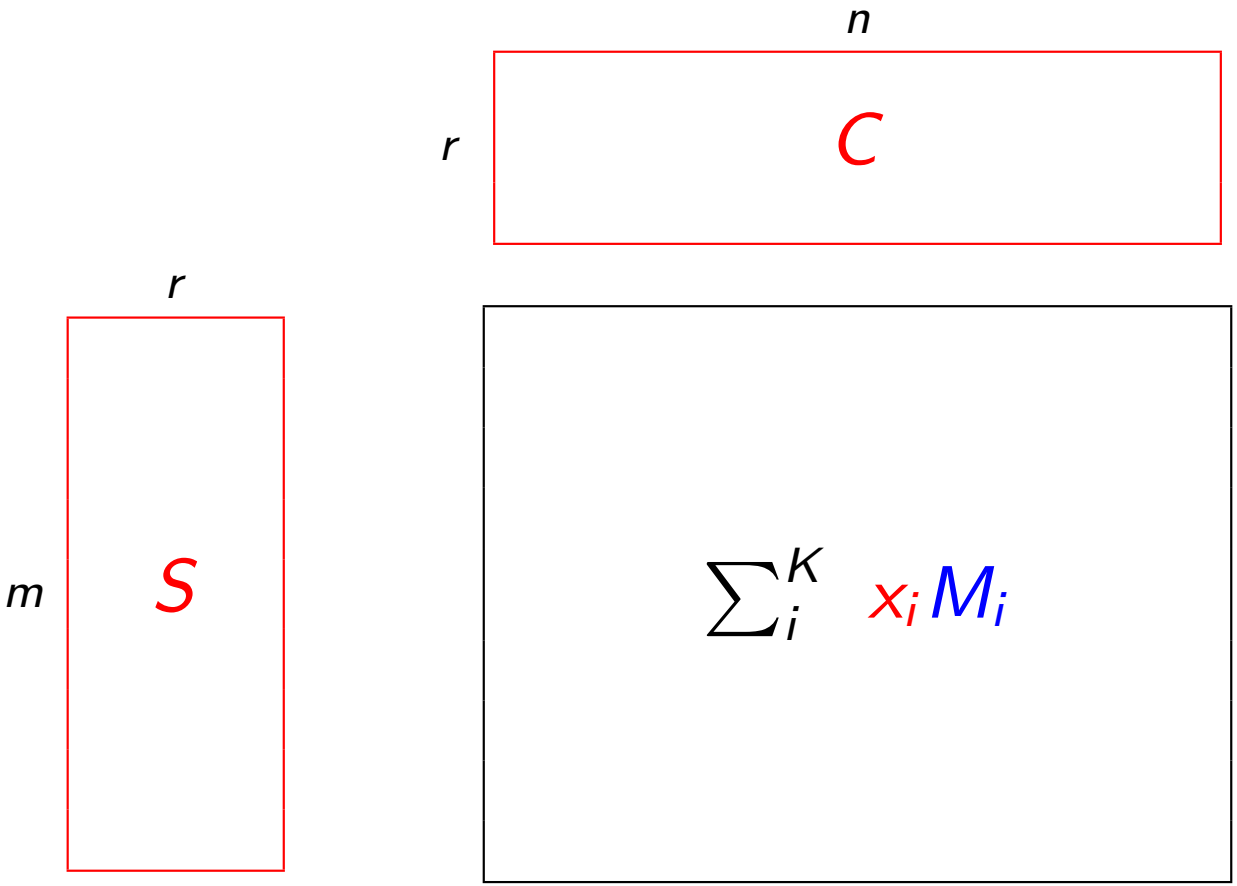
M of size $m \times n$ and rank r

$$\Longleftrightarrow$$

$$SC = M$$

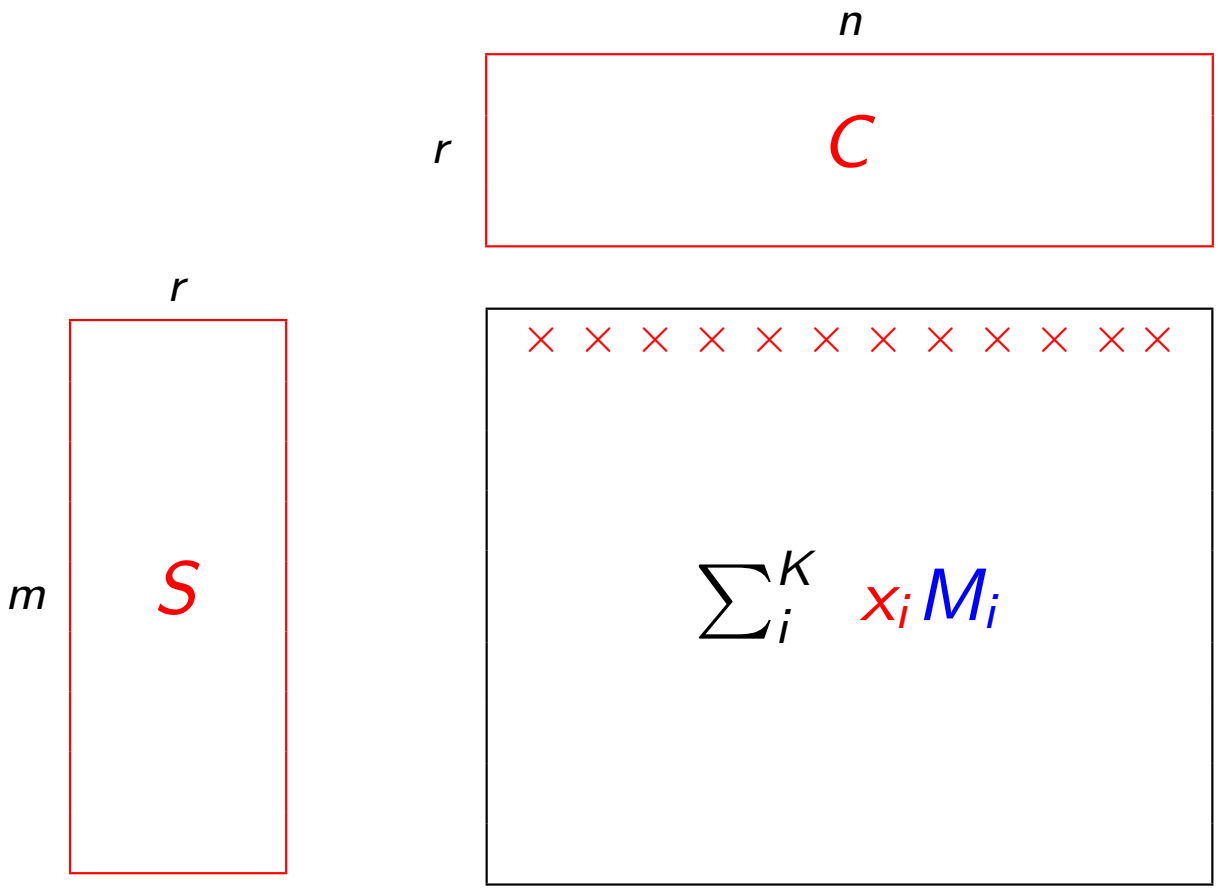


Our Modeling for MinRank

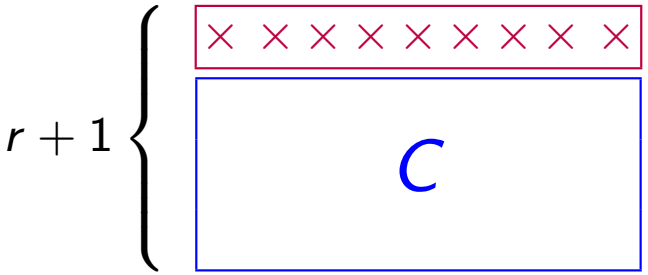


$$SC = \sum_i^K x_i M_i$$

Our Modeling for MinRank



Our Modeling for MinRank



$\Longrightarrow$ all maximal minors vanish!

- First row: linear form in the x_i's variables
- $\Longrightarrow$ equations of degree $r+1$ (1,r)

Core idea

Each maximal minors $(r \times r)$ of C $\Longrightarrow$ a variable c_T

- **Bilinear system (1,1) in the variables x_i's and c_T's.**
- **SupportMinors** modeling.

$$E := \underbrace{m\binom{n}{r+1}}_{\text{equations}} \qquad U := \underbrace{K\binom{n}{r}}_{\text{unknowns}}$$

Complexity of our algorithm against MinRank (heuristic):

When $E \geq U - 1$,

$$\mathcal{O}\left(E \times U^{\omega-1}\right).$$

If the condition $E \geq U - 1$ is not fulfilled:

- hybrid approaches
- new equations from multiplication by monomials in the x_i's

$x_I c_T$ **(1,1)**

$\Downarrow$ $\Downarrow$

$\underbrace{x_i \dots x_j}_{\text{deg. } b-1}\ x_I c_T$ **(b,1)**

Case $b = 2$

$$\underbrace{Km\binom{n}{r+1}}_{\text{equations}} \qquad \underbrace{\overbrace{\binom{K+1}{2}}^{\text{deg. 2 mono. in the } x_i}\binom{n}{r}}_{\text{unknowns}}$$

Let J be a subset of $\{1, \ldots, n\}$ of size $r+2$, and $1 \leq i_1 < i_2 \leq m$,

$$\left| \begin{pmatrix} \frac{r_{i_1}}{r_{i_2}} \\ \hline C \end{pmatrix} \right|_J + \left| \begin{pmatrix} \frac{r_{i_2}}{r_{i_1}} \\ \hline C \end{pmatrix} \right|_J = 0$$

$$\sum \lambda_i x_i \underbrace{\left| \begin{pmatrix} \frac{r_{i_2}}{} \\ \hline C \end{pmatrix} \right|_J}_{\substack{\text{an original equation } (\text{“}x_i c_T\text{”}) \\ \hline \text{a new equation } (\text{“}x_i x_j c_T\text{”})}} + \sum \mu_i x_i \underbrace{\left| \begin{pmatrix} \frac{r_{i_1}}{} \\ \hline C \end{pmatrix} \right|_J}_{\substack{\text{an original equation } (\text{“}x_i c_T\text{”}) \\ \hline \text{a new equation } (\text{“}x_i x_j c_T\text{”})}} = 0$$

$\Longrightarrow$ Thus, we found **linear dependencies** between the new equations.

$x_I c_T$ **(1,1)**

$\Downarrow$ $\Downarrow$

$\underbrace{x_i \dots x_j}_{\text{deg. } b-1}\ x_I c_T$ **(b,1)**

Case $b = 2$

$$\underbrace{Km\binom{n}{r+1} - \binom{n}{r+2}\binom{m+1}{2}}_{\text{equations}} \qquad \underbrace{\overbrace{\binom{K+1}{2}}^{\text{deg. 2 mono. in the } x_i}\ \binom{n}{r}}_{\text{unknowns}}$$

Rainbow parameters				Complexity		
$(GF(q), v_1, o_1, o_2)$	n	K	r	**SM**	Prev. MinRank	Best/Type
Ia$(GF(16), 32, 32, 32)$	96	33	64	**155**	161	145/RBS
IIIc$(GF(256), 68, 36, 36)$	140	37	104	**208**	585	215/DA
Vc$(GF(256), 92, 48, 48)$	188	49	140	**272**	778	275/DA

[Beullens, Crypto 2022]

Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

IBM Research, Zurich, Switzerland
wbe@zurich.ibm.com

Abstract. This work introduces new key recovery attacks against the Rainbow signature scheme, which is one of the three finalist signature schemes still in the NIST Post-Quantum Cryptography standardization project. The new attacks outperform previously known attacks for all the

What is the idea behind the c_T's?

- Matrix $\mathbf{C}$: row space basis
- $\forall\ \mathbf{A}\ \in \mathrm{GL}_r(\mathbb{F}_q)$, **AC still works**
- Variables $C_{i,j}$ in $\mathbf{C}$:
  - **Degree r with minors**
  - **Too many solutions**
- **Plücker coordinates**: projective + "1 v.s / 1 solution"

$$p\colon \{W \subset \mathbb{F}_q^n \ :\ \dim(W) = r\} \longrightarrow \mathbb{P}^N(\mathbb{F}_q)$$
$$W \longmapsto (|\mathbf{C}|_{*,T_i})_{i\in\{1..N+1\}}.$$

where $N = \binom{n}{r} - 1$, and $T_i \subset \{1, 2, \ldots, n\}$.

Rank Decoding

Given $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ and $s \in \mathbb{F}_{q^m}^{n-k}$.

$\Longrightarrow$ Find e **small rank weight** such that:

$$He^\intercal = s^\intercal$$

Rank metric on a toy example

Let $B = \{1, \alpha, \alpha^2, \alpha^3\}$ be a basis of $\mathbb{F}_{2^4}$ seen as an $\mathbb{F}_2$-vector space; $\alpha^4 = \alpha + 1$.

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

$$\mathrm{Mat}(e) := \begin{matrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \end{matrix} \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in (\mathbb{F}_2)^{4\times 5}$$

$$\mathrm{Rank}(e) := \mathrm{Rank}(\mathrm{Mat}(e)) = 2.$$

$$
\begin{aligned}
& eH^\top = (0), \\
\iff & \left(1 \ \alpha \ \dots \ \alpha^{m-1}\right) \mathrm{Mat}(e) H^\top = (0), \\
\iff & \left(1 \ \alpha \ \dots \ \alpha^{m-1}\right) SCH^\top = (0), \\
\iff & \underbrace{\left(\left(1 \ \alpha \ \dots \ \alpha^{m-1}\right) S\right)}_{e'} \left(CH^\top\right) = (0),
\end{aligned}
$$

$$
e' \neq 0 \in \mathrm{Ker}\left(CH^\top\right) \implies \mathrm{Rank}\left(CH^\top\right) < r.
$$

Thus, all **maximal minors of $CH^\top$ vanish.**

Proposition (Maximal Minors of $CH^\top$)

The Maximal Minors of $CH^\top$ are polynomials over $\mathbb{F}_{q^m}$ of the form

$$\sum_{T \subset \{1..n\}, \#T=r} (-1)^{f(T)} \det(H)_T \underbrace{\det(C)_T}_{:=c_T}$$

- $\Longrightarrow$ **linear system in the c_T's.**
- This is the **MaxMinors** modeling.

Proposition (Maximal Minors of $CH^\top$)

The Maximal Minors of $CH^\top$ are polynomials over $\mathbb{F}_{q^m}$ of the form

$$\sum_{T\subset\{1..n\},\#T=r} (-1)^{f(T)} \det(H)_T \underbrace{\det(C)_T}_{:=c_T}$$

- $\Longrightarrow$ **linear system in the c_T's.**
- This is the **MaxMinors** modeling.

Complexity of our algorithm against RD (conjecture):

When $m\binom{n-k-1}{r} \geq \binom{n}{r} - 1$,

$$\mathcal{O}\left(m\binom{n-k-1}{r}\binom{n}{r}^{\omega-1}\right).$$

$$\begin{cases} \binom{n}{r} - 1 & \text{variables } c_T\text{'s (in } \mathbb{F}_q), \\ m\binom{n-k-1}{r} & \text{equations over } \mathbb{F}_q. \end{cases}$$

Super-overdetermined case

One chooses **the biggest integer** p so that

$$m\binom{n-k-1-p}{r} \geq \binom{n-p}{r} - 1$$

$$\Longrightarrow \quad \mathcal{O}\left(m\binom{n-k-1-p}{r}\binom{n-p}{r}^{\omega-1}\right)$$

$$\begin{cases} \binom{n}{r} - 1 & \text{variables } c_T\text{'s (in } \mathbb{F}_q), \\ m\binom{n-k-1}{r} & \text{equations over } \mathbb{F}_q. \end{cases}$$

Hybrid case

One chooses **the smallest integer** a so that

$$m\binom{n-k-1}{r} \geq \binom{n-a}{r} - 1$$

$$\Longrightarrow \quad \mathcal{O}\left(q^{ar} m \binom{n-k-1}{r} \binom{n-a}{r}^{\omega-1}\right)$$

Comparison with previous Attacks

Cryptosystem	RD(m, n, k, r)	Sec.	Prev.	**MaxMinors**	(a, p)
Loidreau*	$(128, 120, 80, 4)$	**256**	98	**65**	$(0, 3)$
ROLLO-I	$(79, 94, 47, 5)$	**128**	117	**71**	$(0, 9)$
ROLLO-I	$(89, 106, 53, 6)$	**192**	144	**87**	$(0, 0)$
ROLLO-I	$(113, 134, 67, 7)$	**256**	197	**158**	$(8, 0)$
RQC-I	$(97, 134, 67, 5)$	**128**	123	**77**	$(0, 18)$
RQC-II	$(107, 202, 101, 6)$	**192**	156	**101**	$(0, 10)$
RQC-III	$(137, 262, 131, 7)$	**256**	214	**144**	$(3, 0)$

*[Loidreau, PQCrypto, 2017]

Bardet, Briaud, Bros, Gaborit, Neiger, Ruatta, and Tillich.
An Algebraic Attack on Rank Metric Code-Based Cryptosystems.
In *Eurocrypt*, 2020.

Bardet, Bros, Cabarcas, Gaborit, Perlner, Smith-Tone, Tillich, and Verbel.
Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems.
In *Asiacrypt*, 2020.

- Bardet, Briaud, Bros, Gaborit, Tillich.
  "Revisiting Algebraic Attacks on MinRank and on the Rank Decoding Problem",
  Preprint ArXiv, 2022.

Thank you for your attention!