Rank-Metric Decoding with Hints

Anmoal Porwal[*], Harrison Banda[†], Jan Brinkman[†], Anna Baumeister[*], Juliane Krämer[†], Antonia Wachter-Zeh[*]

[*] Technical University of Munich

[†] University of Regensburg

27 February 2026
OpeRa Workshop
University of Bordeaux, Talence

Introduction

- There exist many cryptographic schemes such that:

  Scheme is secure $\Leftrightarrow$ Certain math problem is hard

- For example,

  Rabin's encryption scheme is 128-bit secure
  $\Leftrightarrow$ best solver for integer factorization takes 2^{128} operations

- Side-channel attacks might reveal parts of the secret (i.e., "hints")
- **Question:** If so, how does the complexity of the best solver decrease?
- We might ask,

  what is the security level of Rabin after we learn 3% of the secret?
  $\equiv$ what is the complexity of the best solver for integer factorization after we learn 3% of the secret?

Introduction

- **Rank-Metric problems used for cryptography**
  - MinRank Problem
  - Rank Syndrome Decoding (RSD)
- **Our question:** Given some hints about the secret, how do the complexity of the best solvers decrease?
- **Best solvers?**
  - Kernel Search (MinRank) (Goubin and Courtois, 2000)
  - Support Minors (MinRank) (Bardet et al., 2020)
  - GRS (RSD) (Gaborit, Ruatta, and Schrek, 2016)
  - MaxMinors (RSD) (Bardet et al., 2020)
- In this talk, we show to do this for **Kernel Search (MinRank)**, but our results extend to GRS (RSD) as well

The MinRank Problem

- Given matrices $\mathbf{M}_1, \ldots, \mathbf{M}_K \in \mathbb{F}_q^{m \times n}$ and a small integer $r > 0$, find nonzero $x_1, x_2, \ldots, x_K \in \mathbb{F}_q$ such that

$$\operatorname{rank}\left(\sum_{i=1}^{K} x_i \mathbf{M}_i\right) \leq r$$

- Example: find nonzero $x_1, \ldots, x_4 \in \mathbb{F}_3$ such that

$$x_1 \begin{bmatrix} 2 & 0 & 1 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{bmatrix} + x_2 \begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix} + x_3 \begin{bmatrix} 0 & 1 & 0 \\ 0 & 2 & 2 \\ 2 & 0 & 1 \end{bmatrix} + x_4 \begin{bmatrix} 1 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$$

  has rank $r = 1$
- For large parameters, MinRank is believed hard to solve

The Kernel Search Solver

- The MinRank Problem:

  Let $\mathbf{E}(\boldsymbol{x}) := \sum_{i=1}^{K} x_i \mathbf{M}_i \in \mathbb{F}_q^{m \times n}$

  Find $\boldsymbol{x} \in \mathbb{F}_q^K$ such that $\operatorname{rank}(\mathbf{E}(\boldsymbol{x})) \leq r$

- For example,

$$\mathbf{E}(\boldsymbol{x}) := \begin{bmatrix} 2x_1 + x_4 & 2x_2 + x_3 + x_4 & x_1 + x_2 + 2x_4 \\ x_1 + 2x_2 + 2x_4 & 2x_1 + x_2 + 2x_3 & 2x_3 + x_4 \\ x_2 + 2x_3 + x_4 & x_1 + 2x_4 & 2x_1 + 2x_2 + x_3 \end{bmatrix}$$

- $\mathbf{E}(\boldsymbol{x})$ has low rank $\Rightarrow$ $\mathbf{E}(\boldsymbol{x})$ has a large kernel
- Idea: guess vectors hoping they are in the kernel

  for each correct guess $\boldsymbol{v} \in \mathbb{F}_q^n$ we have $\mathbf{E}(\boldsymbol{x})\boldsymbol{v}^\mathsf{T} = \mathbf{0}^\mathsf{T} \in \mathbb{F}_q^m$

  this yields m equations in the variables $x_1, \ldots, x_K$

Kernel Search with Hints

The original Kernel Search algorithm:

1. Guess b vectors $\boldsymbol{v}_1, \ldots \boldsymbol{v}_b \in \mathbb{F}_q^n$
2. Solve $\mathbf{E}(\boldsymbol{x})\boldsymbol{v}_i^\mathsf{T} = \mathbf{0}$, $i = 1, \ldots, b$ for $x_1, \ldots, x_K$
3. If $\mathbf{E}(\boldsymbol{x})$ does not have low rank, repeat

What hint to consider?

$$\mathbf{E}(\boldsymbol{x}) = \overbrace{\begin{bmatrix} * & * & * \\ * & * & * \\ * & * & * \\ * & * & * \\ * & * & * \end{bmatrix}}^{\text{full-rank and size } m \times r} \overbrace{\left[\begin{array}{ccc|ccc} 1 & & & 1 & * & 2 & * \\ & 1 & & 0 & * & * & * \\ & & 1 & * & 1 & * & * \end{array}\right]}^{\text{size } r \times n} \in \mathbb{F}_q^{m \times n}$$

- Is it possible to improve Kernel Search using this information?
- This tells us, e.g., $(0\ 0\ 0\ 2\ 0\ 1\ 0)$ is *not* in the kernel (if $q \neq 2$)

The Guessing Problem

1. An oracle knows a secret subspace $\mathcal{S}$ ($\mathcal{S}^\perp$) $\subseteq \mathbb{F}_q^n$ of dimension $n - r$ (r)
2. Guess $\mathcal{K}$ ($\mathcal{K}^\perp$) $\subseteq \mathbb{F}_q^n$ of dimension $n - r - \ell$ ($r + \ell$) (for a given $\ell > 0$)
3. Oracle tells us whether $\mathcal{K} \subseteq \mathcal{S}$ ($\mathcal{K}^\perp \supseteq \mathcal{S}^\perp$) (success condition)

What is the optimal way to guess $\mathcal{K}$ ($\mathcal{K}^\perp$)?

Suppose we also know $\mathcal{S}$ ($\mathcal{S}^\perp$) is the kernel (row space) of the following matrix

$$\left[\begin{array}{c|cccc} & 1 & * & 2 & * \\ \mathbf{I} & 0 & * & * & * \\ & * & 1 & * & * \end{array}\right] \in \mathbb{F}_q^{r \times n}$$

New Problem Formulation

1. An oracle knows a secret subspace $\mathcal{T} \subseteq \mathbb{F}_q^n$ of dimension r
2. Guess $\mathcal{R} \subseteq \mathbb{F}_q^n$ of dimension $r + \ell$ (for a given $\ell > 0$)
3. Oracle tells us whether $\mathcal{R} \supseteq \mathcal{T}$ (success condition)

What is the optimal way to guess $\mathcal{R}$?

Suppose we also know $\mathcal{T}$ is the row space of the following matrix,

$$\left[\begin{array}{c|cccc} & 1 & * & 2 & * \\ \mathbf{I} & 0 & * & * & * \\ & * & 1 & * & * \end{array}\right] \in \mathbb{F}_q^{r \times n}$$

How to Solve it

We are given

$$(\mathbf{I} \mid \mathbf{C}') = \left[\begin{array}{c|cccc} & 1 & * & 2 & * \\ \mathbf{I} & 0 & * & * & * \\ & * & 1 & * & * \end{array}\right] \in \mathbb{F}_q^{r \times n}$$

Goal: guess $\mathbf{R} \in \mathbb{F}_q^{(r+\ell) \times n}$ such that $\mathrm{rowspan}(\mathbf{R}) \supseteq \mathrm{rowspan}(\mathbf{I} \mid \mathbf{C}')$

$$\mathbf{R} = \left[\begin{array}{c|cccc} & 1 & * & 2 & * \\ \mathbf{I} & 0 & * & * & * \\ & * & 1 & * & * \\ \hline \mathbf{0} & \multicolumn{4}{c}{\mathbf{A}} \end{array}\right] \begin{array}{l} \longleftarrow \mathbf{B} \text{ (let)} \\ \in \mathbb{F}_q^{(r+\ell) \times n} \end{array}$$

We succeed if and only if

> the ith row of $\mathbf{C}'$ is in the coset (the ith row of $\mathbf{B}$) + $\mathrm{rowspan}(\mathbf{A})$

For any given set of hints, possible to construct an optimal $\mathbf{A}$

Complexity with Hints

- Original Kernel search costs $q^{r\lceil \frac{K}{m} \rceil}$
- Kernel search with hints costs $q^{r\lceil \frac{K}{m} \rceil - h + t}$

  where h is the total number of hints
  and t is the minimum number of hints in any $(r \times (n - r - \lceil \frac{K}{m} \rceil))$ submatrix of $\mathbf{C}'$

% of known entries in $\mathbf{C}'$	Complexity[a] (bits)
0	144
10	83
20	50
30	27
40	10
50	4
60	1
70	0
80	0
90	0
100	0

For `Mirath-1a` parameter set $(q = 16, m = 16, n = 16, K = 143, r = 4)$

[a] without polynomial factors

Conclusion

ePrint (2026/132):
"Subspace Guessing and Rank-Metric Solvers with Hints"

- Can be shown our guessing strategy is optimal

  interesting consequence: the left matrix is easier to attack than right

$$\left[\begin{array}{c|ccc} \mathbf{I} & * & * & * \\ & * & * & * \\ & * & * & * \end{array}\right] \text{ vs } \left[\begin{array}{c|ccc} \mathbf{I} & * & * & * \\ & * & * & * \\ & * & * & * \end{array}\right]$$

- Can also be extended to *bit-level* hints
- Can be extended to the GRS solver for RSD
- **Future work:**

  What if the matrix $\mathbf{C}$ is not systematic?
  How to do this for other MinRank and RSD solvers?

Additional: Support Minors with Hints

- Write

$$\mathbf{E}(\boldsymbol{x}) = \overbrace{\begin{bmatrix} * & * & * \\ * & * & * \\ * & * & * \\ * & * & * \end{bmatrix}}^{\mathbf{S}} \overbrace{\left[\begin{array}{c|ccc} \mathbf{I} & 1 & * & * & * \\ & * & 0 & * & * \\ & * & 2 & * & * \end{array}\right]}^{(\mathbf{I} \mid \mathbf{C}')} \in \mathbb{F}_q^{m \times n}$$

- Let $(d_1, d_2, d_3, \ldots)$ be the determinants of all the $r \times r$ submatrices of $(\mathbf{I} \mid \mathbf{C}') \in \mathbb{F}_q^{r \times n}$
- Support Minors derives a system of the form

$$\begin{aligned} x_2 d_1 + x_4 d_2 + x_3 d_5 + \cdots &= 0, \\ x_1 d_3 + x_5 d_2 + x_2 d_4 + \cdots &= 0, \\ x_3 d_1 + x_1 d_6 + x_4 d_2 + \cdots &= 0 \end{aligned}$$

  and then tries to solve it
- **Open question:** How can hints help? Can we find additional equations involving d_i's using hints?