Multivariate Cryptography and MinRank Attacks

ICERM Graduate Workshop on Linear Algebra over Finite Fields & Applications

Ryann Cartor

Clemson University

August 21, 2025

Recall: Multivariate Cryptography

Problem (MQ: Multivariate Quadratic)

Given a system of multivariate quadratic equations over a finite field, find a solution.

- General Public Key Structure:

$$P(x) = T(F(S(x)))$$

■ Linear, ■ Quadratic (Easy to invert),
■ Quadratic (hopefully, difficult to invert)

MinRank Problem

Problem (MinRank)

Given $\mathbf{M}_1, \ldots, \mathbf{M}_k \in \mathbb{F}_q^{m \times n}$ and a positive integer r, find $a_1, \ldots, a_k \in \mathbb{F}_q$ (not all zero) such that

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

Complexity depends on choice of algorithm:
Exhaustive search, Combinatorial method/linear, Kipnis-Shamir, **Support Minors**, ...

Solving MinRank Using Exhaustive Search

- Given $\mathbf{M}_1, \ldots, \mathbf{M}_k \in \mathbb{F}_q^{m \times n}$:
  1. Choose random $a_1, \ldots, a_k \in \mathbb{F}_q$

     Q: How many ways can we choose $a_1, \ldots, a_k \in \mathbb{F}_q$?

     A: There are q^k many ways
  2. Compute $\widehat{\mathbf{M}} := \sum_{i=1}^{k} a_i \mathbf{M}_i$
     - This is just scalar multiplication and matrix addition– not computationally expensive
  3. Check if rank $\left(\widehat{\mathbf{M}}\right) \leq r$

     Q: What is the complexity of checking the rank of $\hat{\mathbf{M}}$?

     A: This is the same as the complexity of multiplying two $n \times n$ matrices, which can be estimated as n^ω where $2 \leq \omega < 3$
- We estimate the complexity of solving an instance of MinRank using Exhaustive Search as:

$$q^k n^\omega, \quad \omega \approx 2.37$$

Support Minors Modeling

- Introduced by Bardet et. al. at Asiacrypt 2020
- Algebraic approach to solve MinRank
- Things to remember:
  - $\text{Rank}(\mathbf{M}) = \dim(\text{Col}(\mathbf{M})) = \dim(\text{Row}(\mathbf{M}))$
  - Minor of $\mathbf{M}$ is determinant of submatrix of $\mathbf{M}$

Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray A. Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, Javier A. Verbel, "Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank Problems," ASIACRYPT (2020).

Support Minors Modeling

Given $\mathbf{M}_1, \ldots, \mathbf{M}_k \in \mathbb{F}_q^{n \times m}$:

- Consider $\widehat{\mathbf{M}} := \sum_{i=i}^{k} x_i \mathbf{M}_i$, where rank$(\widehat{\mathbf{M}}) \leq r$.
- We know there exists $\mathbf{S} \in \mathbb{F}_q^{n \times r}$ and $\mathbf{C} \in \mathbb{F}_q^{r \times m}$ such that

$$\mathbf{SC} = \widehat{\mathbf{M}}$$

- Let $\mathbf{r}_j$ be the jth row of $\widehat{\mathbf{M}}$ and create n new matrices $\mathbf{C}_j$:

$$\mathbf{C}_j = \begin{pmatrix} \mathbf{r}_j \\ \mathbf{C} \end{pmatrix} \in \mathbb{F}_q^{(r+1) \times m} \leftarrow \text{Q: What is rank}(\mathbf{C}_j)?$$

- All maximal minors of $\mathbf{C}_j$ are zero! This gives us:
  - $k + \binom{m}{r}$ many variables $\leftarrow$(# x_i's)+(# $r \times r$ minors of $\mathbf{C}$)
  - $(n)\binom{m}{r+1}$ many bilinear equations $\leftarrow$(# $\mathbf{C}_j$'s)(# max minors)

Support Minors Modeling

Q1: How do we solve a bilinear system of $(n)\binom{m}{r+1}$ many equations in $k + \binom{m}{r}$ many variables?

A1: One way: XL algorithm (use Macaulay matrices, reduce)

(monomials up to degree b)
$\downarrow$

(polynomials in the system) $\rightarrow \begin{bmatrix} & & \\ & & \\ & & \end{bmatrix}$

Q2: What is the complexity of solving this system with XL?

A2: $3(\#$ cols in Mac Mat when rank is high enough$)^2(r+1)k$

$$\min_{m' \leq m} 3\binom{m'}{r}^2 \binom{k+b-2}{b}^2 (k-1)(r+1)$$

where b is the smallest integer such that
$\binom{m'}{r}\binom{k+b-2}{b} - 1 \leq \sum_{i=1}^{b}(-1)^{i+1}\binom{m'}{r+1}\binom{n+i-1}{i}\binom{k+b-i}{b-i}$.

Complexity Comparisons

Consider the MinRank Instance with...

1. $\mathbf{M}_1, \ldots, \mathbf{M}_{15} \in \mathbb{F}_2^{25\times 25}$, $r = 12$.
   - Complexity of solving with exhaustive search:
   $$q^k n^\omega \approx 2^{26}$$
   - Complexity of solving with support minors:
   $$m' = 15, b = 7 \rightarrow \approx 2^{60}$$
2. $\mathbf{M}_1, \ldots, \mathbf{M}_{15} \in \mathbb{F}_{256}^{25\times 25}$, $r = 8$.
   - Complexity of solving with exhaustive search:
   $$q^k n^\omega \approx 2^{131}$$
   - Complexity of solving with support minors:
   $$m' = 12, b = 2 \rightarrow \approx 2^{40}$$

MinRank: ZK-protocols

Digitial Signatures Round 2: Mirath (Merger of MIRA and MiRitH)

MIRA: a Digital Signature Scheme based on the MinRank problem and the MPC-in-the-Head paradigm

Nicolas Aragon[1], Loïc Bidoux[2], Jesús-Javier Chi-Domínguez[2], Thibauld Feneuil[3,4], Philippe Gaborit[5], Romaric Neveu[5], and Matthieu Rivain[4]

[1] Naquidis Center, Talence, France
[2] Technology Innovation Institute, UAE
[3] Sorbonne Université, CNRS, INRIA, Institut de Mathématiques de Jussieu-Paris Rive Gauche, Ouragan, Paris, France
[4] CryptoExperts, Paris, France
[5] University of Limoges, France

l 2023

Name of the Proposal:

MiRitH
(MinRank in the Head)

June 2023

Inventors of the Scheme:

Gora Adj[1], Luis Rivera-Zamarripa[1], Javier Verbel[1]

Additional Designers:

Emanuele Bellini[1], Stefano Barbero[2], Andre Esser[1], Carlo Sanna[2†], Floyd Zweydinger[1]

MinRank Attacks Against Rank-Metric CB Cryptosystems

Problem (Rank Decoding Problem)

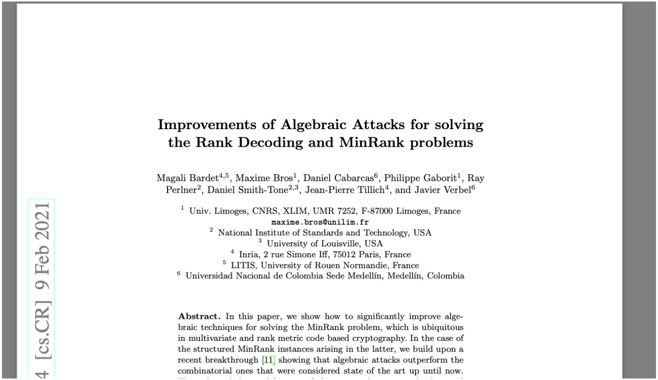
Given a matrix $\mathbf{G} \in \mathbb{F}_{q^m}^{k\times n}$, a vector $\mathbf{y} \in \mathbb{F}_{q^m}^{n}$, and a positive integer r, find vectors $\mathbf{e} \in \mathbb{F}_{q^m}^{n}, \mathbf{x} \in \mathbb{F}_{q^m}^{k}$ such that

$$\mathbf{y} = \mathbf{e} + \mathbf{x}\mathbf{G}, \text{ and } wt_{\mathsf{rank}}(\mathbf{e}) \leq r$$

$$\begin{aligned} wt_{\mathsf{rank}}(\mathbf{e}) &= wt_{\mathsf{rank}}(\mathbf{y} - \mathbf{x}\mathbf{G}) \leq r \\ &= \mathsf{rank}(\widehat{\mathbf{Y}} - x_i \widehat{\mathbf{G}_\mathbf{i}}) \leq r \end{aligned}$$

"Cryptanalysis of MinRank," Jean-Charles Faugére, Francoise Levy-dit-Vehel, and Ludovic Perret (CRYPTO 2008)

MinRank Attacks Against Rank-Metric CB Cryptosystems



4 [cs.CR] 9 Feb 2021

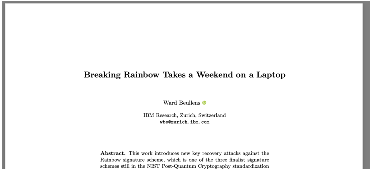
Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems

Magali Bardet[4,5], Maxime Bros[1], Daniel Cabarcas[6], Philippe Gaborit[1], Ray Perlner[2], Daniel Smith-Tone[2,3], Jean-Pierre Tillich[4], and Javier Verbel[6]

[1] Univ. Limoges, CNRS, XLIM, UMR 7252, F-87000 Limoges, France
maxime.bros@unilim.fr
[2] National Institute of Standards and Technology, USA
[3] University of Louisville, USA
[4] Inria, 2 rue Simone Iff, 75012 Paris, France
[5] LITIS, University of Rouen Normandie, France
[6] Universidad Nacional de Colombia Sede Medellín, Medellín, Colombia

Abstract. In this paper, we show how to significantly improve algebraic techniques for solving the MinRank problem, which is ubiquitous in multivariate and rank metric code based cryptography. In the case of the structured MinRank instances arising in the latter, we build upon a recent breakthrough [11] showing that algebraic attacks outperform the combinatorial ones that were considered state of the art up until now.

MinRank Attacks against Multivariate Cryptosystems



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

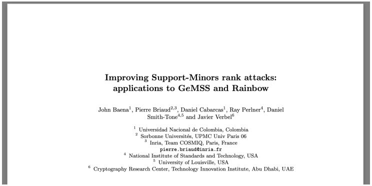
Improved Key Recovery of the HFEv- Signature Scheme

Chengdong Tao[2], Albrecht Petzoldt[3], Jintai Ding[1,2,4]

[1] Yau Mathematical Center, Tsinghua University, Beijing, China
[2] Ding Lab, Beijing Institute of Mathematical Sci. and Applications, Beijing, China
[3] FAU Erlangen-Nuremberg, Nuremberg, Germany
[4] University of Cincinnati, Cincinnati, Ohio, USA

taochengdong@bimsa.cn, albrecht.petzoldt@googlemail.com, jintai.ding@gmail.com

Abstract. The HFEv- signature scheme is a twenty year old multivariate public key signature scheme. It uses the Minus and the Vinegar modifier on the original HFE scheme. An instance of the HFEv- signature scheme called GeMSS is one of the alternative candidates for signature schemes in the third round of the NIST Post Quantum Crypto (PQC) Standardization Project. In this paper, we propose a new key recovery attack on the HFEv- signature scheme. We show that the Minus modification does



Improving Support-Minors rank attacks: applications to GeMSS and Rainbow

John Baena[1], Pierre Briaud[2,3], Daniel Cabarcas[1], Ray Perlner[4], Daniel Smith-Tone[4,5] and Javier Verbel[6]

[1] Universidad Nacional de Colombia, Colombia
[2] Sorbonne Universités, UPMC Univ Paris 06
[3] Inria, Team COSMIQ, Paris, France
pierre.briaud@inria.fr
[4] National Institute of Standards and Technology, USA
[5] University of Louisville, USA
[6] Cryptography Research Center, Technology Innovation Institute, Abu Dhabi, UAE

Signature Scheme Toy Example

Quadratic Central Map Equations

Question: How could we write quadratic maps as a matrix?

Example: $F : \mathbb{F}_{11}^4 \to \mathbb{F}_{11}^3$

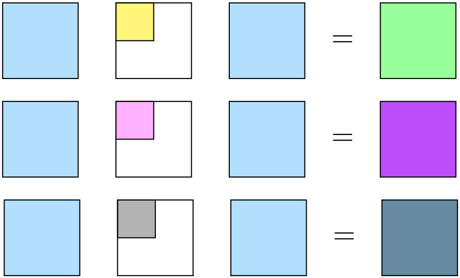
$$F\left(\begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{bmatrix}\right) = \begin{bmatrix} 2w_1^2 + 6w_1w_2 + 3w_1^2 \\ w_1^2 + 2w_1w_2 + 6w_2^2 \\ 8w_1^2 + 7w_1w_2 \end{bmatrix} := \begin{bmatrix} f_1(\mathbf{w}) \\ f_2(\mathbf{w}) \\ f_3(\mathbf{w}) \end{bmatrix}$$

$$f_1(\mathbf{w}) = \begin{bmatrix} w_1 & w_2 & w_3 & w_4 \end{bmatrix} \begin{bmatrix} 2 & 3 & 0 & 0 \\ 3 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{bmatrix}$$

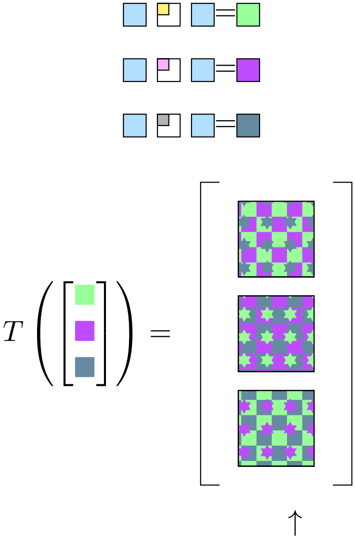
$$\mathbf{F}_1 = \begin{bmatrix} 2 & 3 & 0 & 0 \\ 3 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \mathbf{F}_2 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \mathbf{F}_3 = \begin{bmatrix} 8 & 9 & 0 & 0 \\ 9 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$f_i(U(\mathbf{x})) = f_i(\mathbf{U}\mathbf{x}) = (\mathbf{U}\mathbf{x})^\top \mathbf{F}_i(\mathbf{U}\mathbf{x})$$

$$\mathbf{U}^\top \times \mathbf{F}_i \times \mathbf{U} = z_i$$

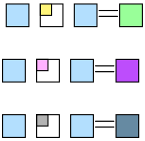


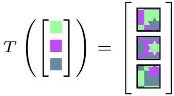
Full Rank | Rank$(\mathbf{F}_i) = r$ | Full Rank | RANK r



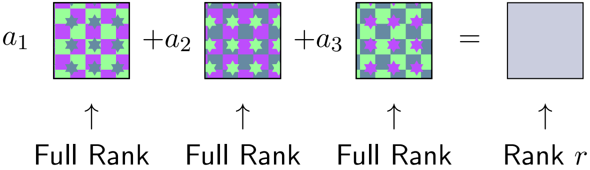
$\mathsf{Rank}(\mathbf{P}_i) = n$

$\mathbf{U}^\top \times \mathbf{F}_i \times \mathbf{U} = z_i$

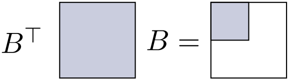




Question: Can we find $a_1, a_2, a_3 \in \mathbb{F}_q$ such that



If so, there exists some full rank matrix B such that



Recall: Unbalanced Oil and Vinegar

$$\mathbf{x} \in \mathbb{F}_q^n \longrightarrow \mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_v \\ x_{v+1} \\ \vdots \\ x_n \end{pmatrix}$$

← vinegar variables

← oil variables

$$P : \mathbb{F}_q^n \to \mathbb{F}_q^{n-v}, \quad P = U \circ F \circ T, \quad F = (f^{(1)}, \dots, f^{(n-v)})$$

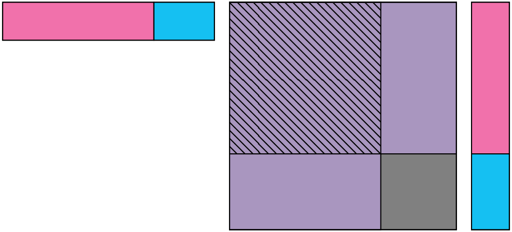
$$f^{(k)}(\mathbf{x}) = \sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{ijk} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{ijk} x_i x_j$$

Patarin, "The Oil and Vinegar Signature Scheme." (1997)
Kipnis, Shamir, "Cryptanalysis of the Oil & Vinegar Signature Scheme." (1998)

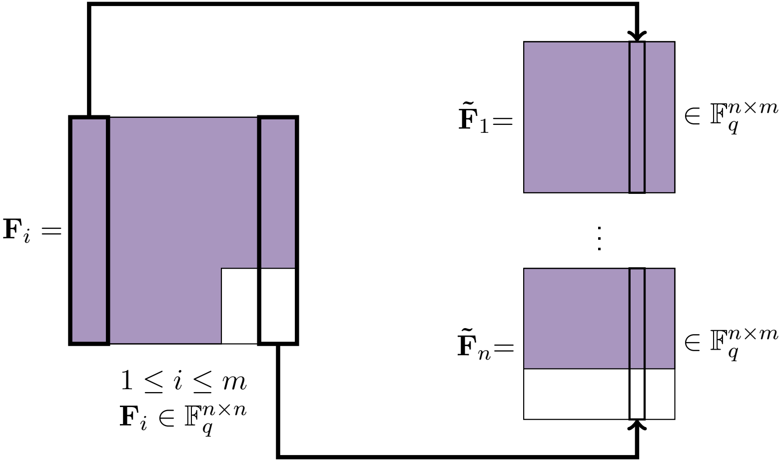
UOV Central Maps

Let $\mathbf{x} \in \mathbb{F}_q^n$, $f_k = \sum_{i=1}^{v}\sum_{j=i}^{v} \alpha_{ijk} x_i x_j + \sum_{i=1}^{v}\sum_{j=v+1}^{n} \beta_{ijk} x_i x_j$.

Consider matrices $\mathbf{F}_k$ such that $f_k(x) = \mathbf{x}^\top \mathbf{F}_k \mathbf{x}$.



Rectangular MinRank Against UOV *(and Rainbow)*



Beullens, "Improved Cryptanalysis of UOV and Rainbow," EUROCRYPT (2021)

Rectangular MinRank Against UOV *(and Rainbow)*

Table 2. The Rainbow parameter sets that were submitted to the second round and the finals of the NIST PQC standardization project.

Parameter set		Parameters q	n	m	o_2	$\lvert\mathsf{pk}\rvert$ (kB)	$\lvert\mathsf{sk}\rvert$ (kB)	$\lvert\mathsf{sig}\rvert$ (Bytes)
Second Round	Ia	16	96	64	32	149	93	64
	IIIc	256	140	72	36	710	511	156
	Vc	256	188	96	48	1705	1227	204
Finals	Ia	16	100	64	32	157	101	66
	IIIc	256	148	80	48	861	611	164
	Vc	256	196	100	64	1885	1376	212

Beullens, "Improved Cryptanalysis of UOV and Rainbow," EUROCRYPT (2021)

Rectangular MinRank Against UOV *(and Rainbow)*

Table 5. Comparison of the new MinRank instance with the known instance of the MinRank problem.

	Known instance of MinRank problem	New instance of MinRank problem
Size of matrices	n-by-n	n-by-m
Number of matrices	$o_2 + 1$	$n - o_2 + 1$
Rank of linear combination	m	o_2
Solution	vector in $W^{\perp}$	vector in O_2

Beullens, "Improved Cryptanalysis of UOV and Rainbow," EUROCRYPT (2021)

Rectangular MinRank Against UOV *(and Rainbow)*

Table 6. The optimal attack parameters of the new MinRank attack, and the corresponding gate complexity for the Rainbow parameter sets submitted to the second round and the finals of the NIST PQC standardization project.

Parameter set		Plain MinRank m'	b	$\log_2$ gates	MinRank and $\mathcal{P}(\mathbf{y}) = 0$ m'	b	$\log_2$ gates
Second round	Ia	51	2	131	40	6	124
	IIIc	59	2	153	52	4	151
	Vc	80	2	197	74	3	191
Finals	Ia	51	2	131	44	4	127
	IIIc	72	3	184	68	4	177
	Vc	95	4	235	87	6	226

Beullens, “Improved Cryptanalysis of UOV and Rainbow,” EUROCRYPT (2021)

Thank you for your attention!
Questions?