Algebraic Relation of Three MinRank Algebraic Modelings

Hao Guo[1] and Jintai Ding[2,3]

[1] Tsinghua University, Beijing, China
guoh22@mails.tsinghua.edu.cn
[2] Ding Lab, Yanqi Lake Beijing Institute of Mathematical Sciences and Applications, Beijing, China
jintai.ding@gmail.com
[3] Yau Mathematical Sciences Center, Tsinghua University, Beijing, China

Abstract. We give algebraic relations among equations of three algebraic modelings for MinRank problem: support minors modeling, Kipnis–Shamir modeling and minors modeling.

Keywords: MinRank problem · quadratic equation · algebraic modeling

1 Introduction

In 2020, Bardet et al. introduced the support minors modeling [1] for solving MinRank problem, whose applications include the novel attacks on GeMSS [20] and Rainbow [2]. The powerful attacks make us wonder whether some new algebraic structures exist in support minors modeling and help it reduce the complexity of MinRank. In this paper we explore the algebraic relation between this modeling and other two modelings, namely minors modeling [11] and Kipnis–Shamir modeling [17].

The MinRank problem asks for a nonzero linear combination of given matrices with low rank. It has been used to attack some NIST-PQC candidates, for example ROLLO, RQC, GeMSS and Rainbow. In rank-metric-based code (for example ROLLO and RQC [1]) and rank syndrome problem [14] it is natural to consider MinRank problem since metric is defined by matrix rank. In multivariate cryptography, traditional ways to design a cryptography system and make trapdoors include two ways: using BigField structure [18,8,19] and using properties of BigField to build trapdoors; using UOV structure [16,7] and assigning vinegar variables to build trapdoors. Some of these trapdoors include special restrictions which can be detected by matrix rank, for example in HFE [18] the degree restriction of univariate polynomial and in Rainbow [7] the multi-layer oil and vinegar variable structure, therefore MinRank problem can be used to attack

these schemes. On the other hand, since Buss et al. proved that MinRank problem is generally NP-hard [4], there exists some zero-knowledge scheme based on MinRank, for example [6].

There are many ways to solve the MinRank problem, including minors modeling, Kipnis–Shamir modeling and linear algebra search [15]. Besides these basic ideas, Wang et al. [22] also considered the hybrid method that combines Kipnis–Shamir modeling and minors modeling. Moreover, previous works also concern the complexity of MinRank. Faugere et al. focused on the case of under-determined and well-determined cases [13,11,12] and proved that minors modeling is better than Kipnis–Shamir modeling by a little. For the over-determined case, Verbel et al. considered the case of the so-called 'superdetermined' case for Kipnis–Shamir modeling [21] which uses Jacobian of the matrix to induce equations.

Most of these modelings and analyses above fall into the step of calculating Gröbner basis [3] for the ideal corresponding to equations, which is the conceptual generalization of Gaussian Elimination and Euclid's greatest common factor. Efficient algorithm for solving Gröbner basis are F_4 [9] and its variant F_5 [10]. Meanwhile, support minors modeling does not require Gröbner basis computation and turns to XL-like methods [5,23] which has its full power when the number of equations is more than that of variables.

In this paper we focus on the quadratic equations given by Kipnis–Shamir modeling and support minors modeling. We found that by substituting c_T variables in equations of the support minors modeling with determinant-like polynomials in $y_{i,j}$ variables from equations of the Kipnis–Shamir modeling, all former equations become linear combination of latter equations with coefficients in the polynomial ring of $y_{i,j}$ variables. As a byproduct, we offer a constructive proof of the fact that the equations of the minors modeling come from linear combination of that of Kipnis–Shamir modeling with coefficients in the polynomial ring of $y_{i,j}$'s and linear variables x_k's.

2 Notation

We list some useful notations for the following statements and proofs:

- $\mathcal{I}$ (calligraphic font) stands for some index set with $r+1$ elements corresponding to either rows or columns. The row (column) number always starts from 1.
- $\{i_1 < \cdots < i_l \leq r < i_{l+1} < \cdots < i_{r+1}\}$ stands for $\{i_1, \ldots, i_{r+1}\}$, with orders in the set specified as $i_1 < \cdots < i_l \leq r < i_{l+1} < \cdots < i_{r+1}$.

- For matrix A, $A_{\mathcal{I},\mathcal{J}}$ stands for submatrix of A with rows $\mathcal{I}$ and columns $\mathcal{J}$.
- For a $m \times n$ matrix $A, \mathcal{I} \subset \{1, \ldots, m\}$ and $\mathcal{J} \subset \{1, \ldots, n\}$, if $|\mathcal{I}| = |\mathcal{J}|$, $|A|_{\mathcal{I},\mathcal{J}}$ stands for the minor of A with rows $\mathcal{I}$ and $\mathcal{J}$.
- For a $m \times n$ matrix A and $|\mathcal{J}| = m$, $A_{*,\mathcal{J}}$ is acronym for $A_{\{1,\ldots,m\},\mathcal{J}}$, and $|A|_{*,\mathcal{J}}$ is acronym for $|A|_{\{1,\ldots,m\},\mathcal{J}}$.
- T (letter 'T') stands for some index set subset of $\{1, \ldots, n\}$ with r elements.
- c_T represents $|C|_{*,T}$, where C is the coefficient matrix in support minors modeling.
- For matrix A, A^t stands for transpose of A.

3 Preliminaries

MinRank problem We give the statement of the MinRank problem:

Definition 1 (MinRank problem). *Fix a field $\mathbb{K}$. We denote $\mathbb{K}^{m\times n}$ as the vector space of matrices with m rows and n columns and entries in $\mathbb{K}$.*

Given matrices $M_1, \ldots, M_l \in \mathbb{K}^{m\times n}$ and a target rank r, the MinRank problem asks for elements $x_1, \ldots, x_l \in \mathbb{K}$ that are not all zero, such that the linear combination $M = \sum_{k=1}^{l} x_k M_k$ has rank no more than r.

Notice that sometimes the solution is restricted to some subfield $L \subset \mathbb{K}$ (for example in some BigField schemes). However, in this paper we only consider the case that solution takes value in $\mathbb{K}$.

Algebraic modelings for solving MinRank problem Below we describe three algebraic modelings for MinRank problem.

minors modeling The matrix M has rank $\leq r$ iff all its $r+1$ minors are zero. Minors modeling simply uses these minor conditions as equations. There are $\binom{m}{r+1}\binom{n}{r+1}$ minors in matrix M, and they are all $r+1$ degree polynomials in the variables $x_1, \ldots, x_l$, since each entry of M is a linear form of these variables.

If we denote $M = (a_{i,j})$, then each $a_{i,j}$ can be written as

$$a_{i,j} = \sum_{k=1}^{l} a_{i,j}^{(k)} x_k \tag{1}$$

where $a_{i,j}^{(k)}$ is the (i,j)-th element of M_k. Each $(r+1)$-minor of M is a homogeneous polynomial of degree $r+1$ in the $a_{i,j}$'s, so when substituting

$a_{i,j}$ with x_k's, we get a homogeneous polynomial of degree $r+1$ in the x_k's. If we make these polynomials equal to zero we get the corresponding equations of minors modeling.

Kipnis–Shamir modeling We recall the following rank–nullity theorem from linear algebra:

Lemma 1. *For a linear map $A\colon \mathbb{K}^n \to \mathbb{K}^m$, we have*

$$\dim A(\mathbb{K}^n) + \dim \ker(A) = n$$

Since the matrix M has rank $\leq r$, the dimension of the kernel of M is no less than $n-r$, hence it must contain a $(n-r)$-dim subspace. So there exists a full-rank matrix $Y \in \mathbb{K}^{n\times(n-r)}$ such that $MY = 0$. Notice further that for any invertible matrix $R \in \mathrm{GL}_{n-r}(\mathbb{K})$, we have $M(YR) = (MY)R = 0$, and YR also has full rank, so we can restrict some entries of Y and still expect a solution. Therefore, we solve the following matrix equation

$$M \begin{bmatrix} -Y' \\ I_{n-r} \end{bmatrix} = 0 \tag{2}$$

where I_{n-r} is the $(n-r)\times(n-r)$ identity matrix, and

$$Y' = \begin{bmatrix} y_{1,1} & \cdots & y_{1,n-r} \\ \vdots & & \vdots \\ y_{r,1} & \cdots & y_{r,n-r} \end{bmatrix} \tag{3}$$

is a $r \times (n-r)$ matrix. If (2) has a solution, then the rank of M must be less than r.

From (2) we can get $m(n-r)$ equations, each of the form

$$f_{i,j} = a_{i,r+j} - \sum_{k=1}^{r} a_{i,k} y_{k,j} = 0 \tag{4}$$

for $i = 1, \ldots, m$, $j = 1, \ldots, n-r$. If we plug in (1), we get quadratic equations with no square terms and the equations are linear in x_k's. Total number of variables is $p + r(n-r)$.

support minors modeling We recall the following rank decomposition theorem from linear algebra:

Lemma 2. *A $m\times n$ matrix M has rank $\leq r$ iff there exists a $m\times r$ matrix S and a $r\times n$ matrix C, such that $M = SC$.*

Since the rank of M is no more than r, we can find some matrices S and C such that $\sum_{k=1}^{p} x_k M_k = M = SC$. While we cannot make both S and C full rank (otherwise we know M is of rank r), we can assure that C has full rank by expanding the row space of M into a r-dim vector space and solve for entries of S. Since C has full rank, we know that each row $\mathbf{r}_i$ is in the row space of C, so the augmented matrix

$$C_i = \begin{bmatrix} \mathbf{r}_i \\ C \end{bmatrix}$$

has rank r. Therefore the maximal minors of C_i should be zero. If we denote c_T for the maximal minors of C with columns T, then using Laplace expansion of determinant, each maximal minor of C_i is a bilinear form in a_{ij} and c_T. By evaluating these maximal minors to be zero, we get $m\binom{n}{r+1}$ quadratic equations

$$|C_i|_{*,\mathcal{J}} = 0 \tag{5}$$

for $i = 1, \ldots, m$ and all subset $\mathcal{J} \subset \{1, \ldots, n\}$ with $r+1$ elements. If we plug in (1), we get equations bilinear in x_k's and c_T's. Total number of variables is $p + \binom{n}{r}$.

4 Main results and proofs

4.1 Relation between Kipnis–Shamir modeling and support minors modeling

We will adopt the following matrix

$$C' = \begin{bmatrix} I_r \; Y' \end{bmatrix}$$

where Y' is the $r \times (n-r)$ matrix defined by (3). The core idea of this subsection is to make substitution $\phi\colon c_T \mapsto |C'|_{*,T}$ in support minors modeling. This is the same as replacing the coefficient matrix C from support minors modeling with C'.

The reason we consider matrix C' comes from cryptographical situations. In practical use of MinRank problem, the target rank r is often the smallest rank that $\sum_{k=1}^{p} x_k M_k$ can attain besides zero. In this case the rank decomposition $M = SC$ tells us that row space of C is the same as that of the M. Therefore from (2) we also get

$$C \begin{bmatrix} -Y' \\ I_{n-r} \end{bmatrix} = 0 \tag{2'}$$

We claim that

Lemma 3. *The reduced row echelon form of C is C'.*

Proof. Denote C'' to be the reduced row echelon form of C. Since C is full row rank, all rows in C'' have pivot elements. Since C'' is in reduced row echelon form, the r-th row of C'' must begin with $r-1$ zeros. Therefore it suffices to show that the (r,r)-th element of C'' is 1 instead of 0.

Assume instead that the r-th row of C'' begin with r zeros, then this row has the shape of

$$\begin{bmatrix} 0 \cdots 0 & z_1 \cdots & z_{n-r} \end{bmatrix}$$

for some $z_1, \ldots, z_{n-r} \in \mathbb{K}$. Using (2'), we get that

$$0 = \begin{bmatrix} 0 \cdots 0 \end{bmatrix} (-Y') + \begin{bmatrix} z_1 \cdots & z_{n-r} \end{bmatrix} I_{n-r} = \begin{bmatrix} z_1 \cdots & z_{n-r} \end{bmatrix}$$

So the r-th row of C'' is a zero row, which contradicts the fact that C has full rank. Therefore the (r,r)-th element of C'' is 1, and we get C'' has the shape of C'.

Since C' is the reduced row echelon form of C in cryptographical situations, it suffices to replace C with C' and use this to relate the support minors modeling and Kipnis–Shamir modeling. Notice that in general the row space of M is only contained in that of C, therefore (2') cannot be derived from (2).

Denote

$$C'_i = \begin{bmatrix} \mathbf{r}_i \\ C' \end{bmatrix} \tag{6}$$

the augmented matrix C_i with block C replaced by C'.

Some properties of ϕ are listed below:

Lemma 4. $\phi(c_{\{1,\ldots,r\}}) = 1$.

Lemma 5. $\phi(c_{\{1,\ldots,r\}\setminus\{i\}\cup\{r+j\}}) = (-1)^{r-i} y_{i,j}$.

Proof. Direct calculation. We have

$$|C'|_{*,\{1,\ldots,r\}\setminus\{i\}\cup\{r+j\}} = \begin{vmatrix} I_{i-1} & 0_{(i-1)\times(r-i)} & *_{(i-1)\times 1} \\ 0_{1\times(i-1)} & 0_{1\times(r-i)} & y_{ij} \\ 0_{(r-i)\times(i-1)} & I_{r-i} & *_{(r-i)\times 1} \end{vmatrix} = (-1)^{r-i} y_{i,j}$$

maximal minors of C'_i To calculate maximal minors of C'_i and relate this with f_{ij} from Kipnis–Shamir modeling (see (4)), we consider the following matrix

$$L_i = \begin{bmatrix} 1 & -a_{i,1} \cdots & -a_{i,r} \\ 0_{r\times 1} & & I_r \end{bmatrix} \tag{7}$$

L_i is invertible matrix and has determinant 1. Also, when calculating maximal minors of $L_iC'_i$, we have

$$|L_iC'_i|_{*,\mathcal{J}} = (\det L_i)|C'_i|_{*,\mathcal{J}} = |C'_i|_{*,\mathcal{J}} \tag{8}$$

since the determinant function is multiplicative. Therefore it suffices to consider the matrix $L_iC'_i$. Denote

$$L_iC'_i = \begin{bmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{bmatrix}$$

where Q_1 is $1 \times r$ matrix, Q_4 is $r \times (n-r)$ matrix, and the shape of Q_2 and Q_3 follows from the block matrix rules. We have $Q_3 = I_rI_r = I_r$, $Q_4 = I_rY' = Y'$. Also,

$$Q_1 = \begin{bmatrix} a_{i,1} & \cdots & a_{i,r} \end{bmatrix} + \begin{bmatrix} -a_{i,1} & \cdots & -a_{i,r} \end{bmatrix} I_r = 0$$

$$Q_2 = \begin{bmatrix} a_{i,r+1} & \cdots & a_{i,n} \end{bmatrix} + \begin{bmatrix} -a_{i,1} & \cdots & -a_{i,r} \end{bmatrix} \begin{bmatrix} y_{1,1} & \cdots & y_{1,n-r} \\ \vdots & & \vdots \\ y_{r,1} & \cdots & y_{r,n-r} \end{bmatrix} = \begin{bmatrix} f_{i,1} & \cdots & f_{i,n-r} \end{bmatrix}$$

So

$$L_iC'_i = \begin{bmatrix} 0_{1\times r} & f_{i,1} & \cdots & f_{i,n-r} \\ I_r & & Y' & \end{bmatrix} \tag{9}$$

From (9) and (8) we know that $|C'_i|_{*,\{1,\ldots,r\}\cup\{r+j\}} = (-1)^r f_{i,j}$. Therefore after applying substitution ϕ, equations of Kipnis–Shamir modeling can be viewed as a subset of equations of support minors modeling (up to a constant of -1). In general, we have

Proposition 1. *Suppose* $\mathcal{J} = \{j_1 < \cdots < j_l \leq r < j_{l+1} < \cdots < j_{r+1}\}$, *then*

$$|C'_i|_{*,\mathcal{J}} = \sum_{k=l+1}^{r+1} (-1)^{k-1} f_{i,j_k-r} |C'|_{*,\mathcal{J}\setminus\{j_k\}} \tag{10}$$

Proof. Simply use Laplace expansion.

Notice that $|C'|_{*,\mathcal{J}\setminus\{j_k\}}$ is maximal minor of C', which in turn is polynomial in $y_{i,j}$'s. So we know that $|C'_i|_{*,\mathcal{J}}$ is a linear combination of $f_{i,j}$'s with coefficients in $\mathbb{K}[y_{1,1}, \ldots, y_{r,n-r}]$.

4.2 Solution space of c_T's from support minors modeling

We know that c_T is denoted to be the maximal minor of C with columns T. However when c_T becomes variables of equations, it becomes not so clear if any solution of equations from support minors modeling still has the meaning that corresponding M is of rank $\leq r$. It is intuitive that if M has rank $\leq r$, then we can expand the row space of M into a r dimensional space, and get a matrix A of r rows and n columns, whose maximal minors is a nonzero solution of (5) since A has full rank. Also, if M has rank $< r$, then different ways of expanding the row space of M will possibly give linear independent solutions for (5). In particular, we are interested in the following questions:

1. For some specific choice of x_k's such that M has rank $> r$, is the solution space of c_T's the zero space?
2. For some specific choice of x_k's such that M has rank r, is the solution space of c_T's dimension 1?
3. For some specific choice of x_k's such that M has rank $< r$, what can we say about the solution space of c_T's?

Nonetheless, we give the following proposition:

Proposition 2. *Suppose for some specific choice of x_k's, the rank of M is r'. Then the solution space of c_T has dimension $\binom{n-r'}{n-r}$. In particular, when $r' > r$ the only solution for c_T's is zero solution.*

Proof. We know that the equations (5) come from augmenting matrix C with a row of M and calculating the $r+1$ minors. In general, we can also augment C with b rows of M to get a b-augmented matrix

$$\begin{bmatrix} \mathbf{r}_{i_1} \\ \vdots \\ \mathbf{r}_{i_b} \\ C \end{bmatrix}$$

where $1 \leq i_1, \ldots, i_b \leq m$, and calculate its $r+b$ minors. Since all rows of M are in the row space of C, all these $r+b$ minors are zero as long as $r+b \leq n$. Using Laplace expansion along the first row we get a linear combination of $r+b-1$ minors of $(b-1)$-augmented matrix. Therefore the equations (5) are not linearly independent.

Since we know that M has rank r', it suffices to use these r' independent rows to generate augmented matrices. There are $\binom{r'+b-1}{b}$ different

ways to b-augment the matrix C. Using some knowledge of syzygy, it is easy to deduce the number of independent equations as

$$\sum_{b=1}^{n-r}(-1)^{b-1}\binom{r'+b-1}{b}\binom{n}{r+b} \tag{11}$$

Lemma 6. *We have the following combinatorial identity:*

$$\sum_{b=0}^{n-r}(-1)^{b}\binom{r'+b-1}{b}\binom{n}{r+b} = \binom{n-r'}{n-r} \tag{12}$$

Proof. Denote

$$G(r',r,n) = \sum_{b=0}^{n-r}(-1)^{b}\binom{r'+b-1}{b}\binom{n}{r+b} \tag{13}$$

Since $\binom{n}{r+b} = \binom{n-1}{r+b} + \binom{n-1}{r-1+b}$, we have $G(r',r,n) = G(r',r,n-1) + G(r',r-1,n-1)$. Also $G(r',r,r) = (-1)^0\binom{r'-1}{0}\binom{r}{r} = 1$. So it suffices to prove that $G(r',r',n) = 1$.

Denote $F(r',n) = G(r',r',n)$. Notice that

$$\binom{n}{r'+b} = \binom{n-1}{r'+b} + \binom{n-1}{r'-1+b}$$
$$\binom{r'+b-1}{b} = \binom{r'-1+b-1}{b} + \binom{r'-1+b-1}{b-1}$$

Therefore $F(r',n) = F_1 + F_2 + F_3$, where

$$F_1 = \sum_{b=0}^{n-1-r'}(-1)^{b}\binom{r'+b-1}{b}\binom{n-1}{r'+b} = F(r',n-1)$$
$$F_2 = \sum_{b=0}^{n-r'}(-1)^{b}\binom{r'-1+b-1}{b}\binom{n-1}{r'-1+b} = F(r'-1,n-1)$$
$$F_3 = \sum_{b=1}^{n-r'}(-1)^{b}\binom{r'+b-1-1}{b-1}\binom{n-1}{r'+b-1} = -F(r',n-1)$$

So $F(r',n) = F(r'-1,n-1)$, hence

$$F(r',n) = F(1,n-r'+1) = \sum_{b=0}^{n-r'}(-1)^{b}\binom{n-r'+1}{b+1} = 1$$

i.e. $G(r',r',n) = 1$. Therefore $G(r',r,n) = \binom{n-r'}{r-r'} = \binom{n-r'}{n-r}$.

Therefore

$$\sum_{b=1}^{n-r}(-1)^{b-1}\binom{r'+b-1}{b}\binom{n}{r+b}=\binom{n}{r}-\binom{n-r'}{n-r}$$

Since we have $\binom{n}{r}$ variables c_T, the solution space dimension is $\binom{n-r'}{n-r}$. Therefore when $r' > r$ the binomial coefficient takes the value 0. This ends the proof of Proposition 2.

Notice that when $r' < r$, we know that the solution space of c_T's has dimension more than 1. Therefore if we do not make the target rank r' optimal, then original equations from support minors modeling have more than 1 dimension of solutions, which means XL-like algorithms cannot make out a solution as [1] said.

4.3 Relation between Kipnis–Shamir modeling and minors modeling

We will adopt the following matrix:

$$M'=\begin{bmatrix} a_{1,1} & \cdots & a_{1,r} & f_{1,1} & \cdots & f_{1,n-r} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{m,1} & \cdots & a_{m,r} & f_{r,1} & \cdots & f_{r,n-r} \end{bmatrix} \tag{14}$$

Since only r columns of M' are of the form $a_{i,j}$, if we calculate $r+1$ minors of M', at least one column is of the form $f_{i,j}$, so all $r+1$ minors lie in the ideal of $\mathbb{K}[\{x_k\},\{y_{i,j}\}]$ generated by $f_{i,j}$'s. Notice that from (4), M' and M are related by the matrix equation

$$M=M'R \tag{15}$$

where

$$R=\begin{bmatrix} I_r & Y' \\ 0 & I_{n-r} \end{bmatrix}. \tag{16}$$

Using Cauchy–Binet formula, we can calculate $r+1$ minors of M:

$$|M|_{\mathcal{I},\mathcal{J}}=\sum_{\mathcal{K}}|M'|_{\mathcal{I},\mathcal{K}}|R|_{\mathcal{K},\mathcal{J}} \tag{17}$$

where $\mathcal{K}$ takes value of each $r+1$ subset of $\{1,\ldots,n\}$. Since all $|M'|_{\mathcal{I},\mathcal{K}}$'s lie in the ideal generated by $f_{i,j}$'s, so does $|M|_{\mathcal{I},\mathcal{J}}$.

5 Conclusion and Discussion

We discussed the quadratic equations from Kipnis–Shamir modeling and support minors modeling, and give the proof that they can be derived from each other. We also give proof that from equations of Kipnis–Shamir modeling we can get the minors equations. Heuristically, the equations derived from support minors modeling can be viewed as an application of bilinear XL on those from Kipnis–Shamir modeling with bi-degree (b, r). This helps us make sure that support minors modeling contains no new algebraic structures from Kipnis–Shamir modeling. However, these calculations above are from the viewpoint of commutative algebra (symbolic calculation) and cannot explain why supports minors modeling has major improvement from other modelings. We believe that the efficiency of support minors modeling comes from the way it solves equations since it contains no additional Gröbner basis calculation.

Acknowledgements This work has been supported by the National Key R&D Program of China (No. 2021YFB3100100).

References

1. Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R., Smith-Tone, D., Tillich, J.P., Verbel, J.: Improvements of algebraic attacks for solving the rank decoding and minrank problems. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 507–536. Springer (2020)
2. Beullens, W.: Improved cryptanalysis of uov and rainbow. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 348–373. Springer (2021)
3. Buchberger, B.: A theoretical basis for the reduction of polynomials to canonical forms. ACM SIGSAM Bulletin **10**(3), 19–29 (1976)
4. Buss, J.F., Frandsen, G.S., Shallit, J.O.: The computational complexity of some problems of linear algebra. Journal of Computer and System Sciences **58**(3), 572–596 (1999)
5. Courtois, N., Klimov, A., Patarin, J., Shamir, A.: Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 392–407. Springer (2000)
6. Courtois, N.T.: Efficient zero-knowledge authentication based on a linear algebra problem minrank. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 402–421. Springer (2001)
7. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: International conference on applied cryptography and network security. pp. 164–175. Springer (2005)
8. Ding, J., Yang, B.Y.: Multivariates polynomials for hashing. In: International Conference on Information Security and Cryptology. pp. 358–371. Springer (2007)

9. Faugere, J.C.: A new efficient algorithm for computing gröbner bases (f4). Journal of pure and applied algebra **139**(1-3), 61–88 (1999)
10. Faugere, J.C.: A new efficient algorithm for computing gröbner bases without reduction to zero (f 5). In: Proceedings of the 2002 international symposium on Symbolic and algebraic computation. pp. 75–83 (2002)
11. Faugere, J.C., El Din, M.S., Spaenlehauer, P.J.: Computing loci of rank defects of linear matrices using gröbner bases and applications to cryptology. In: Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation. pp. 257–264 (2010)
12. Faugere, J.C., El Din, M.S., Spaenlehauer, P.J.: On the complexity of the generalized minrank problem. Journal of Symbolic Computation **55**, 30–58 (2013)
13. Faugere, J.C., Levy-dit Vehel, F., Perret, L.: Cryptanalysis of minrank. In: Annual International Cryptology Conference. pp. 280–296. Springer (2008)
14. Gaborit, P., Ruatta, O., Schrek, J.: On the complexity of the rank syndrome decoding problem. IEEE Transactions on Information Theory **62**(2), 1006–1019 (2015)
15. Goubin, L., Courtois, N.T.: Cryptanalysis of the ttm cryptosystem. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 44–57. Springer (2000)
16. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 206–222. Springer (1999)
17. Kipnis, A., Shamir, A.: Cryptanalysis of the hfe public key cryptosystem by relinearization. In: Annual International Cryptology Conference. pp. 19–30. Springer (1999)
18. Patarin, J.: Hidden fields equations (hfe) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 33–48. Springer (1996)
19. Szepieniec, A., Ding, J., Preneel, B.: Extension field cancellation: a new central trapdoor for multivariate quadratic systems. In: Post-Quantum Cryptography. pp. 182–196. Springer (2016)
20. Tao, C., Petzoldt, A., Ding, J.: Efficient key recovery for all hfe signature variants. In: Annual International Cryptology Conference. pp. 70–93. Springer (2021)
21. Verbel, J., Baena, J., Cabarcas, D., Perlner, R., Smith-Tone, D.: On the complexity of "superdetermined" minrank instances. In: International Conference on Post-Quantum Cryptography. pp. 167–186. Springer (2019)
22. Wang, Y., Ikematsu, Y., Nakamura, S., Takagi, T.: Revisiting the minrank problem on multivariate cryptography. In: International Conference on Information Security Applications. pp. 291–307. Springer (2020)
23. Yang, B.Y., Chen, J.M., Courtois, N.T.: On asymptotic security estimates in xl and gröbner bases-related algebraic cryptanalysis. In: International Conference on Information and Communications Security. pp. 401–413. Springer (2004)