Rank Analysis of Cubic Multivariate Cryptosystems

John Baena[1], Daniel Cabarcas[1], Daniel Escudero[2*], Karan Khathuria[3], and Javier Verbel[1]

[1] Universidad Nacional de Colombia
{jbbaena,dcabarc,javerbelh}@unal.edu.co
[2] Aarhus University
escudero@cs.au.dk
[3] University of Zurich
karan.khathuria@math.uzh.ch

Abstract. In this work we analyze the security of cubic cryptographic constructions with respect to rank weakness. We detail how to extend the big field idea from quadratic to cubic, and show that the same rank defect occurs. We extend the min-rank problem and propose an algorithm to solve it in this setting. We show that for fixed small rank, the complexity is even lower than for the quadratic case. However, the rank of a cubic polynomial in n variables can be larger than n, and in this case the algorithm is very inefficient. We show that the rank of the differential is not necessarily smaller, rendering this line of attack useless if the rank is large enough. Similarly, the algebraic attack is exponential in the rank, thus useless for high rank.

Keywords: multivariate cryptography, cubic polynomials, tensor rank, min-rank

1 Introduction

The min-rank problem (MR) is, given k $m \times n$ matrices and a target rank r, to determine whether there exists a linear combination of the matrices of rank less or equal to r. Although NP-complete in its general setting, there are efficient algorithms to solve it for certain parameters. Indeed, Kipnis and Shamir modeled an attack on the HFE system as an MR problem and were able to break it. Since then, other multivariate public key schemes (MPK) have been subject to similar attacks. Rank defects also lead to other weakness such as a fixed degree of regularity in the algebraic attack on HFE [6].

The importance of the rank itself, and the prevalence of MR as an attack technique in MPK suggest a more central role as the underlying problem that supports security. For example, we can think of HFE as a way to construct low rank quadratic polynomials. Their low rank allows inversion, but it is insecure

[*] Work done whilst at Universidad Nacional de Colombia

because the same low rank is preserved as a linear combination of the public key which can be efficiently solved through the Kipnis-Shamir modeling (KS) of MR.

Although the MR problem is stated for two-dimensional matrices, it can be naturally extended to d-dimensional matrices. It is particularly interesting to analyze it for three-dimensional matrices, since rank problems become much harder there. For example, simply determining the rank of a matrix is difficult for three-dimensional matrices, and it is not even known the maximum possible rank a matrix may have (see e.g. [15]).

Three-dimensional matrices lead to cubic polynomials. They are less common than quadratic polynomials in MPKs for two reasons. First, they are larger thus less efficient than quadratics. But more important, if f is cubic, its differential $Df_{\mathbf{a}}(\mathbf{x}) := f(\mathbf{x}+\mathbf{a}) - f(\mathbf{x}) - f(\mathbf{a})$ is a quadratic map that preserves some of the properties of f. Thus, it is possible to extend rank analysis techniques from quadratics to cubics targeting the differential, c.f. [26]. Yet one important question remains open: Is this a general property of any cubic map that dooms any such construction? In this paper we address this question, by taking a general perspective not focused on a particular construction.

1.1 Our Contribution

In order to close the knowledge gap, we gather the appropriate literature to frame the discussion of the rank of cubic polynomials. We use the language of tensors that allows for very natural extensions of key concepts from two to d-dimensional matrices.

We extend the MR problem to three-dimensional matrices and we propose two ways to solve it, which naturally extend the KS modeling. Interestingly, if the rank is small, the complexity is even lower than for the quadratic case. However, the rank of a cubic polynomial in n variables can be larger than n, and in this case the attack is very inefficient.

We also discuss the relevance of two other typical lines of attack for MPK in the context of cubic low rank polynomials, namely the algebraic and differential attacks. We show that the rank of the differential is not necessarily much smaller than the rank of the cubic polynomial, rendering this line of attack inefficient if the rank is large enough. Similarly, the algebraic attack is exponential in the rank, thus useless for high rank.

Although our approach is general, we provide a detailed example. We show how to efficiently construct cubic polynomials over a finite field from a weight three polynomial over a field extension, extending the so called big field idea. And then, we show that the rank is preserved by this construction in the sense that, a low rank core polynomial leads to a set of cubic polynomials with a low rank linear combination.

1.2 Related Work

In [26] and [25], Moody, Perlner, and Smith-Tone do a rank analysis of the cubic ABC scheme [7]. They expose a subspace differential invariant extending the ideas used in the quadratic case [24]. They show that the MR attack used in [24] can be adapted to this cubic case.

Their work avoids discussing the rank of cubic polynomials by focusing on the differentials. This is rewarding in the ABC case because of the band structure of the scheme. There are linear combinations of the public polynomials with a band structure (they show it for the second differential) whose rank is bounded (possibly by a factor of s^2). The rank of some of their slices (or the second differential evaluated at some vectors as they show) drops by a square root factor to $2s$. This allows an attack on cubic ABC even more efficient than on its quadratic counterpart.

For a good reason, they approach the MR problem by guessing kernel vectors instead of using the Kipnis-Shamir or minors modeling (see Section 2.4 for a discussion of these techniques). The subspace differential invariant allows a tight analysis of the efficiency of this approach.

2 Preliminaries

2.1 Notation

Given a natural number n, the set $\{1, \ldots, n\}$ is denoted by $[n]$. Let $\mathbb{F}$ be a finite field of order q which, unless explicitly stated, has characteristic different from 2 or 3. Vectors are denoted by bold letters, e.g. $\mathbf{u}, \mathbf{v}$, and they are treated as column vectors by default unless stated otherwise. The vector $\mathbf{e}_i$ denotes the i-th canonical vector, i.e. the vector whose only non-zero entry is the i-th one, which is equal to 1. The i-th entry of a vector $\mathbf{u}$ is denoted by $\mathbf{u}[i]$, but sometimes we also use the non-bold version of the corresponding letter with subscript i: u_i. The space of all $n \times m$ matrices is denoted by $\mathbb{F}^{n \times m}$. The entry of a matrix A indexed by (i, j) is denoted by $A[i, j]$. We use the notation $A[i, \cdot]$ to refer to the i-th row of a matrix A (as a row vector), and $A[\cdot, j]$ to refer to the j-th column of A (as a column vector). A three dimensional matrix of dimensions $n \times m \times \ell$ is an array of elements in $\mathbb{F}$ indexed by tuples (i, j, k), where $1 \leq i \leq n$, $1 \leq j \leq m$ and $1 \leq k \leq \ell$. The vector space of these three-dimensional matrices is denoted by $\mathbb{F}^{n \times m \times \ell}$, and the entry indexed by (i, j, k) in a matrix $A \in \mathbb{F}^{n \times m \times \ell}$ will be denoted by $A[i, j, k]$. We denote by $A[i, \cdot, \cdot]$ the two-dimensional matrix whose entry (j, k) is given by $A[i, j, k]$, and similarly for $A[\cdot, j, \cdot]$ and $A[\cdot, \cdot, k]$. For $\mathbf{u} \in \mathbb{F}^n$ and $\mathbf{v} \in \mathbb{F}^m$, $\mathbf{u} \otimes \mathbf{v}$ denotes the Kronecker product which we usually see as the matrix $\mathbf{u}\mathbf{v}^\intercal$.

2.2 Rank and Trilinear Forms

Let n, m, l be positive integers and let U, V and W be the vector spaces $\mathbb{F}^n$, $\mathbb{F}^m$ and $\mathbb{F}^l$, respectively. The rank of a matrix $A \in \mathbb{F}^{n \times m}$ can be defined as the minimum number of summands r required to write A as

$$A = \sum_{i=1}^{r} \mathbf{u}_i \otimes \mathbf{v}_i,$$

where $\mathbf{u}_i \in U$ and $\mathbf{v}_i \in V$ for all $i = 1, \ldots, r$. This definition of rank is more flexible than other definitions as it is independent of the number of dimensions so it can be extended to three-dimensional matrices as follows.

Definition 1. *Let $A \in \mathbb{F}^{n \times m \times \ell}$ be a three-dimensional matrix, we define the rank of A as the minimum number of summands r required to write A as*

$$A = \sum_{i=1}^{r} \mathbf{u}_i \otimes \mathbf{v}_i \otimes \mathbf{w}_i,$$

where $\mathbf{u}_i \in U$, $\mathbf{v}_i \in V$ and $\mathbf{w}_i \in W$ for all $i = 1, \ldots, r$. We denote this number by $\mathsf{Rank}(A)$.

Let $A \in \mathbb{F}^{n \times m \times \ell}$ be a three-dimensional matrix. Then clearly, $\mathsf{Rank}(A) = 0$ if and only if A is zero (empty sum). For an arbitrary $A \in \mathbb{F}^{n \times n \times n}$, the maximal value that $\mathsf{Rank}(A)$ can attain is unknown. To our knowledge, the best known upper bound for the maximal value of $\mathsf{Rank}(A)$ is $\lceil (3/4)n^2 \rceil$ (see [17, Theorem 7]).

A bilinear map $B : U \times U \to \mathbb{F}$ is a map that is linear in each argument, so it can be written as

$$B(\mathbf{x}, \mathbf{y}) = \mathbf{x}^{\mathsf{T}} A \mathbf{y} \tag{1}$$

where $A \in \mathbb{F}^{n \times n}$ is the matrix such that $A[i, j] = B(\mathbf{e}_i, \mathbf{e}_j)$.

A bilinear map B is symmetric if for all $\mathbf{a}, \mathbf{b} \in U$ it holds that $B(\mathbf{a}, \mathbf{b}) = B(\mathbf{b}, \mathbf{a})$, which is equivalent to A being symmetric.

Given a bilinear map B we can obtain a quadratic homogeneous polynomial $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ by defining $f(\mathbf{x}) := B(\mathbf{x}, \mathbf{x})$. Different bilinear maps can yield the same quadratic polynomial. Yet, symmetric bilinear maps are in bijection with the set of quadratic homogeneous polynomials. The symmetric bilinear map from a quadratic homogeneous polynomial f can be computed as $B(\mathbf{x}, \mathbf{y}) := \frac{1}{2}\left(f(\mathbf{x} + \mathbf{y}) - f(\mathbf{x}) - f(\mathbf{y})\right)$.

Similarly, a trilinear map $T : U \times U \times U \to \mathbb{F}$ is a map that is linear in each argument. It can be written as

$$T(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \sum_{i,j,k \in [n]} x_i y_j z_k \cdot \alpha_{i,j,k}$$

where $\alpha_{i,j,k} := T(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$. Let $A \in \mathbb{F}^{n \times n \times n}$ be such that $A[i, j, k] = \alpha_{i,j,k}$. We say that T is symmetric if for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in U$, it is invariant under any permutation of the indices, i.e.

$$T(\mathbf{a}, \mathbf{b}, \mathbf{c}) = T(\mathbf{a}, \mathbf{c}, \mathbf{b}) = T(\mathbf{b}, \mathbf{a}, \mathbf{c}) = T(\mathbf{c}, \mathbf{a}, \mathbf{b}) = T(\mathbf{b}, \mathbf{c}, \mathbf{a}) = T(\mathbf{c}, \mathbf{b}, \mathbf{a}),$$

or equivalently, the three-dimensional matrix A is symmetric. Given a trilinear form T (symmetric or not) we can obtain the homogeneous cubic polynomial $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ defined as $f(\mathbf{x}) := T(\mathbf{x}, \mathbf{x}, \mathbf{x})$, and given a homogeneous polynomial f of degree 3 we can obtain the corresponding symmetric trilinear form as

$$\begin{aligned} T(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \frac{1}{3!}(&f(\mathbf{x}+\mathbf{y}+\mathbf{z}) - f(\mathbf{y}+\mathbf{z}) - f(\mathbf{x}+\mathbf{z}) \\ &- f(\mathbf{x}+\mathbf{y}) + f(\mathbf{x}) + f(\mathbf{y}) + f(\mathbf{z})). \end{aligned} \quad (2)$$

For a cubic homogeneous polynomial $f \in \mathbb{F}[\mathbf{x}]$, we define its rank, denoted by $\mathsf{Rank}(f)$, as the rank of the corresponding three-dimensional symmetric matrix.

2.3 Big Field Idea

Let n be a positive integer. Let $g(y) = y^n + a_{n-1}y^{n-1} + \cdots + a_1 y + a_0$ be an irreducible polynomial of degree n over $\mathbb{F}$. Consider the degree n field extension $\mathbb{K} = \mathbb{F}[y]/\left(g(y)\right)$. Notice that $\mathbb{K}$ can be seen as a vector space over $\mathbb{F}$ of dimension n, so $\mathbb{K} \cong \mathbb{F}^n$ through the usual vector space isomorphism $\phi : \mathbb{K} \to \mathbb{F}^n$ given by

$$\phi(u_1 + u_2 y + \cdots + u_n y^{n-1}) = (u_1, u_2, \ldots, u_n).$$

Let Δ be the matrix whose i-th row is given by the Frobenius powers $((y^0)^{q^{i-1}}, (y^1)^{q^{i-1}}, \ldots, (y^{n-1})^{q^{i-1}})$.

The matrix Δ, whose transpose is known as a Moore matrix, is invertible because $\left\{y^0, y^1, \ldots, y^{n-1}\right\}$ is a basis of $\mathbb{K}$ over $\mathbb{F}$ ([21], Page 109).

For $\beta \in \mathbb{K}$ let $\mathsf{Fr}(\beta)$ denote the vector $(\beta, \beta^{q^1}, \ldots, \beta^{q^{n-1}}) \in \mathbb{K}^n$. If $\alpha \in \mathbb{K}$, then it is easy to see that $\mathsf{Fr}(\alpha) = \Delta \cdot \phi(\alpha)$.

We refer to a polynomial in $\mathbb{K}[X]$ of the form

$$\mathcal{F}(X) = \sum_{0 \le i_1 \le \cdots \le i_d \le n-1} \alpha_{i_1,\ldots,i_d} X^{q^{i_1} + \cdots + q^{i_d}}$$

where $\alpha_{i_1,\ldots,i_d} \in \mathbb{K}$ as a homogeneous weight d polynomial. Notice that a homogeneous weight 0 polynomial is simply a constant polynomial, i.e. an element of $\mathbb{K}$. A weight d polynomial $\mathcal{F} \in \mathbb{K}[X]$ is a polynomial that can be written as $\mathcal{F} = \mathcal{F}_0 + \cdots + \mathcal{F}_d$ where each $\mathcal{F}_j \in \mathbb{K}[X]$ is a homogeneous weight j polynomial.

The main property of this type of polynomials is that if $\mathcal{F} \in \mathbb{K}[X]$ is homogeneous of weight d then the map $F = \phi \circ \mathcal{F} \circ \phi^{-1} : \mathbb{F}^n \to \mathbb{F}^n$ can be represented as evaluation of n homogeneous multivariate polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ of degree d. We state this formally in the following theorem.

Theorem 1. *Let $\mathcal{F} \in \mathbb{K}[X]$ be a homogeneous weight d polynomial. There exist homogeneous degree d polynomials $f_1, \ldots, f_n \in \mathbb{F}[x_1, \ldots, x_n]$ such that for all $\mathbf{a} \in \mathbb{F}^n$ it holds that $F(\mathbf{a}) = (f_1(\mathbf{a}), \ldots, f_n(\mathbf{a}))^\intercal$ where F is the composition $\phi \circ \mathcal{F} \circ \phi^{-1}$.*

$$\begin{tikzcd}
& \mathbb{K} \arrow[r, "\mathcal{F}"] & \mathbb{K} \arrow[d, "\phi"] & \\
\mathbb{F}^n \arrow[r, "S"] \arrow[rrr, bend right, "P"'] & \mathbb{F}^n \arrow[u, "\phi^{-1}"] \arrow[r, "F"] & \mathbb{F}^n \arrow[r, "T"] & \mathbb{F}^n
\end{tikzcd}$$

Fig. 1: Big Field Idea

Proof (sketch). Since for any $j \in \{0, 1, \ldots, n-1\}$, $X \mapsto X^{q^j}$ is an $\mathbb{F}$-linear map over $\mathbb{K}$, and $X^{q^{i_1}+\cdots+q^{i_d}} = X^{q^{i_1}} \cdots X^{q^{i_d}}$, then it is easy to see that each component of F is a degree d multivariate polynomial over $\mathbb{F}$. A more detailed proof can be found in [8] as Theorem 6.2.1. $\square$

The previous property has been used extensively in order to generate sequences of multivariate quadratic polynomials $(f_1, \ldots, f_n)$ that can be inverted with the help of some secret information. Usually, some weight 2 polynomial $\mathcal{F} \in \mathbb{K}[X]$ is chosen, along with two invertible matrices $S, T \in \mathbb{F}^{n \times n}$. The previous theorem states that the composition $F = \phi \circ \mathcal{F} \circ \phi^{-1}$ is given by n multivariate quadratic polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ and therefore the composition $P = T \circ F \circ S = T \circ \phi \circ \mathcal{F} \circ \phi^{-1} \circ S$ is also given by n multivariate quadratic polynomials in $\mathbb{F}[x_1, \ldots, x_n]$. Usually, $\mathcal{F}$ is referred as the core or central polynomial. If we ensure that $\mathcal{F}$ is a univariate polynomial that is easy to invert, then we can invert P if we know S, T and $\mathcal{F}$. This construction can be observed in Figure 1.

This type of "trapdoor" polynomials yield public key encryption schemes where the public key is the polynomials themselves, the secret key is the trapdoor information that allows the inversion of the polynomials, encryption is just evaluation and decryption is inversion. This concept is known as the Big Field Idea, and some examples of schemes that follow this paradigm are MI [23], HFE [27], and variants of HFE [28, 5, 29].

An important remark is that the polynomials representing the map F can be efficiently computable from the coefficients of the polynomial $\mathcal{F}$. The construction for $d = 2$ can be found in [8, Section 6.3]. We will show the construction for $d = 3$ in Section 4.

2.4 Two-Dimensional MinRank Attack

Buss et al. [4] introduced the min-rank problem (MR) in the context of linear algebra and proved its NP-completeness.

Definition 2 (MinRank Problem). *Given positive integers m, n, r, k, and matrices $M_0, \ldots, M_k \in \mathcal{M}_{m \times n}(\mathbb{F})$, determine whether there exist $\lambda_1, \ldots, \lambda_k \in \mathbb{F}$ such that the rank of $\sum_{i=1}^{k} \lambda_i M_i - M_0$ is less or equal to r.*

In the context of cryptography MR first appeared as part of an attack against the HFE cryptosystem by Kipnis and Shamir[18]. The HFE cryptosystem, proposed in 1996 by Jacques Patarin [27], is based on the big field idea presented in Section 2.3, with a low rank central polynomial $\mathcal{F} \in \mathbb{K}[X]$. Kipnis and Shamir showed that an attack on HFE can be reduced to an instance of MR with a small rank r. In particular, if $M_1, \ldots, M_n \in \mathbb{F}^{n \times n}$ are the symmetric matrices representing public polynomials, then there exists a linear combination $\sum_{i=1}^{n} \lambda_i M_i$ having rank at most the rank of $\mathcal{F}$. Moreover, these coefficients can be used to construct an equivalent secret key. For more details on the MinRank attack on HFE we refer the reader to [18]. We discuss below some of the most common approaches to solve the min-rank problem.

The Kipnis-Shamir Modeling Let $A = \sum_{i=1}^{k} t_i M_i - M_0$ be the matrix with entries in the polynomial ring $\mathbb{F}[t_1, \ldots, t_k]$. Then it is easy to see that the matrix A has rank at most r if and only if the dimension of its right kernel is at least $n-r$. Hence we construct $(n-r)$ linearly independent vectors in the right kernel of M by solving the following system of equations in $\mathbb{F}[t_1, \ldots, t_k, v_{1,1}, \ldots, v_{r,n-r}]$:

$$A \cdot \begin{pmatrix} I_{n-r} \\ V \end{pmatrix} = 0_{n \times (n-r)}, \tag{3}$$

where V is the matrix given by $V[i,j] = v_{i,j}$ for $i = 1, \ldots, r$ and $j = 1, \ldots, n-r$. This relation produces a system of $n(n-r)$ bi-homogeneous polynomials of bi-degree (1,1) in $k + r(n-r)$ variables. Clearly, if $(t_1, \ldots, t_k, v_{1,1}, \ldots, v_{r,n-r})$ is a solution of the system, then the evaluation of the matrix A at the point $(t_1, \ldots, t_k)$ has rank at most r.

Guessing Kernel Vectors As with any system of equations, it is possible to guess some variables in (3) and solve for the others. Because of the structure of this system, it is particularly appealing to guess kernel vectors (i.e. the $v_{i,j}$ variables) and solve the resulting linear system in the t_i variables, as proposed in [13] (in fact, since the linear system is very overdetermined, it is enough to guess k/n kernel vectors). The complexity of such attack is dominated by the guessing part and depends on the probability of a correct guess. A tight bound on this probability can be significantly improved by understanding the structure of the solution space, e.g. by exploiting the interlinked kernel structure [33] or by using the subspace differential invariant structure [24].

The Minors Modeling In [12], Faugère et al. introduced the minors method approach to solve the min-rank problem and in [3] they improved the MinRank attack on HFE using this modeling. Let $M = \sum_{i=1}^{k} t_i M_i$ be the matrix with entries in the polynomial ring $\mathbb{F}[t_1, \ldots, t_k]$. Let I be the ideal in $\mathbb{F}[t_1, \ldots, t_k]$ generated by all the $(r+1) \times (r+1)$ minors of M. Let $V(I) \subseteq \mathbb{F}^k$ be the zero locus of I. If $(\lambda_1, \ldots, \lambda_k) \in V(I) \cap \mathbb{F}^k$, then all the $(r+1) \times (r+1)$ minors of the matrix M evaluated at $(\lambda_1, \ldots, \lambda_k)$ are zero. As a result the rank of the matrix

M evaluated at $(\lambda_1,\ldots,\lambda_k)$ is at most r. Each $(r+1)$-minor is a homogeneous polynomial in $\mathbb{F}[t_1,\ldots,t_k]$ of degree $r+1$, and the number of $(r+1)$-minors in M is $\binom{n}{r+1}^2$.

3 Rank Analysis of Cubic Polynomials

Despite the disadvantages in terms of efficiency of considering cubic polynomials, one possible advantage would be avoiding the MinRank attack on the quadratic case. This might be expected since the MinRank attack relies on the fact that the degree is 2. For instance, this allows us to represent the polynomials as $\mathbf{x}^\intercal A\mathbf{x}$, which is crucial as the attack performs matrix operations and properties of such. Therefore, a natural question is whether or not the MinRank attack applies in a cubic setting. Let us start by defining the MinRank problem in this context.

Definition 3 (Cubic MinRank Problem). *Given positive integers l, m, n, r, k, and three-dimensional matrices $M_0,\ldots,M_k \in \mathbb{F}^{n\times m\times l}$, determine whether there exist $\lambda_1,\ldots,\lambda_k \in \mathbb{F}$ such that the rank of $\sum_{i=1}^k \lambda_i M_i - M_0$ is less or equal to r.*

In this section we show that if there is a low-rank linear combination of the cubic polynomials of the public key then the resulting instance of the MinRank problem can be solved with an extension of the Kipnis-Shamir modeling. This is by itself a weakness on the scheme as it allows an adversary to distinguish between a public key and a random polynomial system of equivalent size. Thereafter, we discuss other consequences of the low-rank for the differentials and for the direct algebraic attack.

3.1 Solving the Three-Dimensional Min-Rank Problem

The following characterization of rank for cubic matrices leads to a generalization of the Kipnis-Shamir modeling for the min-rank problem (for a proof, see e.g. [20]).

Theorem 2. *Given a three-dimensional matrix $A \in \mathbb{F}^{n\times m\times \ell}$, the rank of A is the minimal number r of rank one matrices $S_1,\ldots,S_r \in \mathbb{F}^{m\times \ell}$, such that, for all slices $A[i,\cdot,\cdot]$ of A, $A[i,\cdot,\cdot] \in \operatorname{span}(S_1,\ldots,S_r)$.*

Let $M_0,\ldots,M_k \in \mathbb{F}^{n\times n\times n}$. Then, $A = \sum_{i=1}^k \lambda_i M_i - M_0$ is of rank r, if and only if, there exist rank one matrices $S_1,\ldots,S_r \in \mathbb{F}^{n\times n}$, such that, for $i = 1,\ldots,n$, $A[i,\cdot,\cdot] \in \operatorname{span}(S_1,\ldots,S_r)$. Since each S_i matrix is of rank one, we can write it as $S_i = \mathbf{u}_i\mathbf{v}_i^T$ for some vectors $\mathbf{u}_i, \mathbf{v}_i \in \mathbb{F}^n$. Considering the entries of the $\mathbf{u}_i$'s, $\mathbf{v}_i$'s, and the linear combination coefficients as variables yields a cubic system of n^3 equations in $r(2n) + rn + k = 3rn + k$ variables

$$\sum_{j=1}^{r} \alpha_{ij}\mathbf{u}_j\mathbf{v}_j^T = A[i,\cdot,\cdot], \text{ for } i = 1,\ldots,n. \tag{4}$$

n	r	vars	eqns	d-reg	cpx
10	10	310	1000	67	699
11	11	374	1331	74	798
12	12	444	1728	81	899
13	13	520	2197	89	1010
14	14	602	2744	97	1123
15	15	690	3375	105	1240

Table 1: Complexity of MR by KS modeling for cubic system. For different values of n, KS yields a cubic system of n^3 equations in $(3r+1)n$ variables (assuming $k = n$). The d-reg column gives the degree of regularity for such a semi-regular system without field equations. The complexity column, gives the log base 2 of $\binom{vars+d-1}{d}^{2.8}$.

If $r \ll n$ we can do much better. In that case, for most such rank r matrices A, the first r slices $A[1,\cdot,\cdot],\ldots,A[r,\cdot,\cdot]$ are linearly independent. In this case, $\operatorname{span}(S_1,\ldots,S_r) = \operatorname{span}(A[1,\cdot,\cdot],\ldots,A[r,\cdot,\cdot])$. Then, for $i = r+1,\ldots,n$, $A[i,\cdot,\cdot] \in \operatorname{span}(A[1,\cdot,\cdot],\ldots,A[r,\cdot,\cdot])$. Considering the coefficients of the linear combinations as variables yields a system of $n^2(n-r)$ quadratic equations in $(n-r)r+k$ variables

$$\sum_{j=1}^{r} \alpha_{ij} A[j,\cdot,\cdot] = A[i,\cdot,\cdot], \text{ for } i = r+1,\ldots,n. \tag{5}$$

Notice that the converse is not necessarily true. A solution to the system in (5) does not necessarily implies the existence of the rank one S_i matrices, neither that A has rank r. However, this is a very overdetermined system, hence a solution is very unlikely, unless indeed A has rank r.

Another approach in the $r < n$ case is to take differentials (or slices) and reduce the problem to a two-dimensional MR problem. If $A \in \mathbb{F}^{n\times n\times n}$ has rank r, the corresponding symmetric trilinear map is likely to have rank r as well. Then, the differentials of this map will have rank less or equal to r. Since the differential operator is lineal, we have an MR problem among the differentials of the symmetric trilinear maps corresponding to $M_0,\ldots,M_k$. In the next section we discuss the relation between the rank of a cubic and its differential in more detail.

To the best of our knowledge, the complexity of solving a system such as (4) has not been studied. It can be seen as a multi-homogeneous system of multi-degree $(1,1,1,1)$, i.e. a tetra-linear system, and assuming some notion of tetra-regularity, analyze it using the techniques in [9]. It should be noticed that the techniques in [9] do not address the semi-regularity inherent to such an overdetermined system. Alternatively, the techniques in [2] could be used to establish the asymptotic behavior of an upper bound of the degree of regularity based on the semi-regularity assumption. Although a complete asymptotic analysis is outside the scope of this paper, Table 1 shows the growth of such bound for selected parameters.

In the case $r \ll n$, the system in (5) has $\mathcal{O}(n^3)$ quadratic equations in $\mathcal{O}(n)$ variables. Since the number of degree two monomials is $\mathcal{O}(n^2)$ the system can be solved by relinearization at degree 2, which reduces to solving a $\mathcal{O}(n^2)$ square matrix. Notice that this is much faster than the KS approach in the two-dimensional case.

3.2 Differentials

Given an instance of the cubic MinRank problem, one can always obtain a quadratic instance by taking the differential (defined below) of the associated polynomials. For example, it is known ([14]) that computing the differential of the public polynomials of a cubic HFE instance yields an instance of the quadratic HFE scheme, and therefore we can perform a quadratic MinRank attack. In this section we explore the relation between the rank of a cubic polynomial and the rank of its differential. More precisely, given a random homogeneous cubic polynomial $f \in \mathbb{F}[\mathbf{x}]$ of rank r, we want to estimate the rank of the quadratic part of its differential $D_{\mathbf{a}}f(\mathbf{x}) = f(\mathbf{x}+\mathbf{a}) - f(\mathbf{x}) - f(\mathbf{a})$.

The first and principal problem that we face in our analysis is: given an integer r, how can we generate random homogeneous cubic polynomials of rank r? Or equivalently, how can we generate random symmetric three-dimensional matrices of rank r? To address these questions, we introduce the concept of symmetric rank. We then choose random polynomials and use Kruskal's theorem to guarantee that those polynomials have certain symmetric rank.

Definition 4. *Let $S \in \mathbb{F}^{n\times n\times n}$ be a three-dimensional symmetric matrix. We define the symmetric rank of S as the minimum number of summands s required to write S as*

$$S = \sum_{i=1}^{s} t_i \mathbf{u}_i \otimes \mathbf{u}_i \otimes \mathbf{u}_i,$$

where $\mathbf{u}_i \in \mathbb{F}^n$, $t_i \in \mathbb{F}$. If such decomposition does not exist, this number is defined to be ∞. We denote this number by $\mathsf{SRank}(S)$.

The following proposition gives us a sufficient condition over $\mathbb{F}$ to guarantee that for all matrices in $\mathbb{F}^{n\times n\times n}$ the symmetric rank is finite. A more general result is shown in [31, Proposition 7.2].

Proposition 1. *Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| \geq 3$. Then each three-dimensional symmetric matrix $S \in \mathbb{F}^{n\times n\times n}$ can be written as $S = \sum_{i=1}^{s} t_i \mathbf{u}_i \otimes \mathbf{u}_i \otimes \mathbf{u}_i$, where $\mathbf{u}_i \in \mathbb{F}^n$ and $t_i \in \mathbb{F}$.*

By the previous proposition, if $|\mathbb{F}| \geq 3$, any homogeneous cubic polynomial f can be written as $\sum_{i=1}^{k} t_i u_i(\mathbf{x}) u_i(\mathbf{x}) u_i(\mathbf{x})$, where each $u_i(\mathbf{x})$ is a homogeneous linear polynomial and k depends on f. Furthermore, the symmetric rank of a homogeneous cubic $f \in \mathbb{F}[\mathbf{x}]$, denoted by $\mathsf{SRank}(f)$ and defined as the symmetric rank of its symmetric matrix representation, does exist.

The symmetric rank is a good parameter to consider because it is a bound of the rank of the differential.

Proposition 2. *Let $f \in \mathbb{F}[\mathbf{x}]$ be a homogeneous cubic polynomial. If g is the quadratic homogeneous part of $Df_{\mathbf{a}}(\mathbf{x})$, then* $\mathsf{Rank}(g) \leq \mathsf{SRank}(f)$.

Proof. If f can be written as $f(\mathbf{x}) = \sum_{i=1}^{r} t_i u_i(\mathbf{x}) u_i(\mathbf{x}) u_i(\mathbf{x})$, then for any $\mathbf{a} \in \mathbb{F}^n$ the quadratic part of $Df_{\mathbf{a}}(\mathbf{x})$ is $\sum_{i=1}^{r} 3t_i u_i(\mathbf{a}) u_i(\mathbf{x}) u_i(\mathbf{x})$. □

Let $U = \mathbb{F}^n$. Clearly, each symmetric matrix $A \in \mathbb{F}^{n\times n\times n}$ with symmetric rank r can be written as a sum of exactly r terms of the form $t\mathbf{u} \otimes \mathbf{u} \otimes \mathbf{u}$, where $t \in \mathbb{F} - \{0\}$ and $\mathbf{u} \in U$.

Let $\mathcal{S}_r$ be the function which outputs $A = \sum_{i=1}^{r} t_i \mathbf{u}_i \otimes \mathbf{u}_i \otimes \mathbf{u}_i$, for $t_i \in \mathbb{F} - \{0\}$ and $\mathbf{u}_i \in U$. By Proposition 1, if $|\mathbb{F}| \geq 3$, then each symmetric matrix $A \in \mathbb{F}^{n\times n\times n}$ with symmetric rank equal to r is in the codomain of $\mathcal{S}_r$. But some symmetric matrices having symmetric rank less than r can also be there.

The following theorem is a particular case of the known Kruskal's theorem [19,30]. We use it to argue that if $t_i \in \mathbb{F} - \{0\}$ and $\mathbf{u}_i \in U$ are chosen uniformly at random, then with high probability the corresponding output A of $\mathcal{S}_r$ has symmetric rank equal to r. Moreover, by Kruskal's theorem with high probability $\mathsf{Rank}(A) = \mathsf{SRank}(A)$. The Kruskal rank of a matrix with columns $\mathbf{u}_1, \ldots, \mathbf{u}_m$, denoted by $\mathsf{KRank}(\mathbf{u}_1, \ldots, \mathbf{u}_m)$, is defined as the maximum integer k such that any subset of $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ of size k is linearly independent.

Theorem 3. *Let $\mathbb{F}$ be a finite field, $\mathbf{u}_1, \ldots, \mathbf{u}_r \in U$ and $t_1, \ldots, t_r \in \mathbb{F}$. Suppose that $A = \sum_{i=1}^{r} t_i \mathbf{u}_i \otimes \mathbf{u}_i \otimes \mathbf{u}_i$ and that $2r + 2 \leq \mathsf{KRank}(t_1\mathbf{u}_1, \ldots, t_r\mathbf{u}_r) + 2 \cdot \mathsf{KRank}(\mathbf{u}_1, \ldots, \mathbf{u}_r)$. Then $\mathsf{Rank}(A) = r$.*

Suppose $2 \leq r \leq n$. If $\mathbf{u}_1, \ldots, \mathbf{u}_r \in U$ are taken uniformly at random, then with high probability a matrix with columns $\mathbf{u}_1, \ldots, \mathbf{u}_r$ has full rank. If a matrix with columns $\mathbf{u}_1, \ldots, \mathbf{u}_r \in U$ is full rank, then $\mathsf{KRank}(\mathbf{u}_1, \ldots, \mathbf{u}_r) = r$ and $\mathsf{KRank}(t_1\mathbf{u}_1, \ldots, t_r\mathbf{u}_r) = r$, for any $t_1, \ldots, t_r \in \mathbb{F} - \{0\}$. In this case, by Theorem 3 the corresponding output A of $\mathcal{S}_r$ is such that $\mathsf{Rank}(A) = \mathsf{SRank}(A) = r$.

We experimentally analyze the behavior of the rank of the differential of a polynomial that is the output of $\mathcal{S}_{r^2}$. The experimental results are shown in Figure 2, where each curve represents the percentage of times that a rank is obtained, over 100,000 iterations.

3.3 Direct Algebraic Attack

The direct algebraic attack, or simply the direct attack, refers to the case when an attacker aims to find the plaintext associated with a ciphertext $(c_1, \ldots, c_n)$ directly from the public multivariate equations $p_1 = c_1, \ldots, p_n = c_n$, without the knowledge of any other information of the system. In almost all the cases, the most efficient way to perform this attack is to compute a Gröbner basis of the ideal I generated by the multivariate polynomials $p_1 - c_1, \ldots, p_n - c_n$.

Gröbner bases have played an important role not only in multivariate cryptography, but also in coding theory and lattices [34,1]. There is a general consensus that when computing a Gröbner basis over a finite field, one of the most efficient ways to do it is to use the F_4 or F_5 algorithms [10,11]. In a recent work

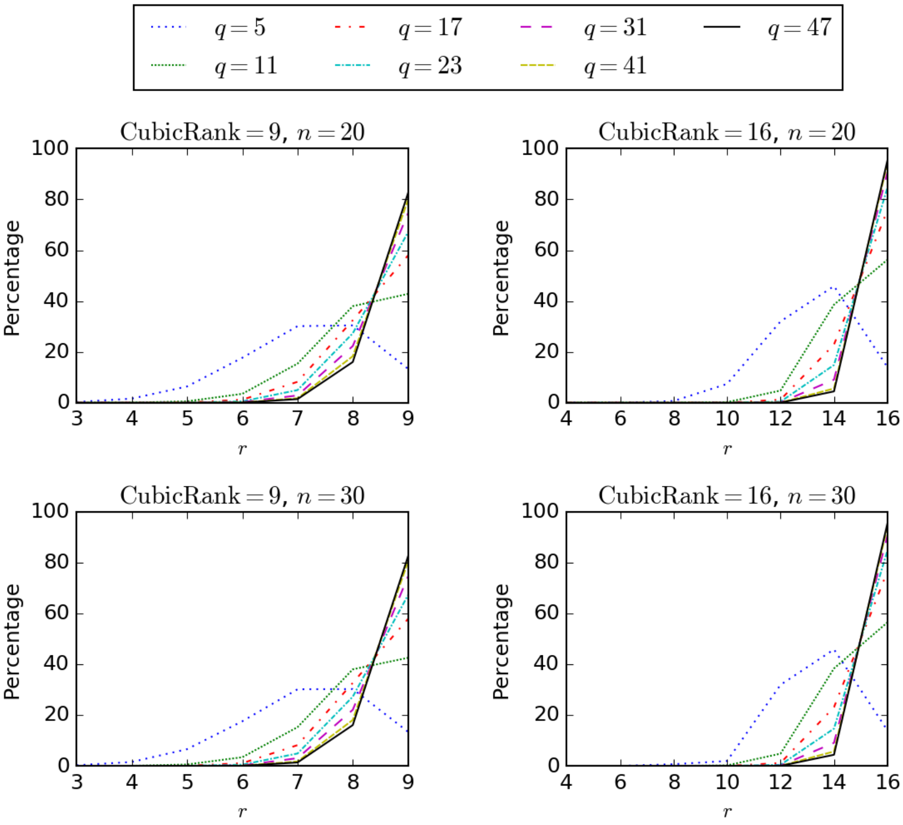

Fig. 2: For different values of q, CubicRank, and n a polynomial f is chosen according $\mathcal{S}_{\text{CubicRank}}$, the $\mathsf{Rank}(Df_{\mathbf{a}})$ is computed for a random $\mathbf{a} \in U$. Each graph represents the percentage of times that a particular value $\mathsf{Rank}(Df_{\mathbf{a}})$ is obtained over 100,000 iterations.

[22], the authors used their M4GB algorithm to solve some of Fukuoka's MQ challenges within 11 days. The complexity of all these algorithms depends on the *degree of regularity* of the system. Since the degree of regularity is hard to determine, it is usually approximated by its *first fall degree*, defined as the first degree at which non-trivial relations between the polynomials $p_1, \dots, p_n$ occur.

Let p be a linear combination of the polynomials $p_1, \dots, p_n$. We now want to derive an upper bound for the first fall degree $D_{\mathrm{ff}}(p_1, \dots, p_n)$ of the system that depends on $\mathsf{Rank}(p)$. Before we do that, we need the following definition.

Definition 5. *The* LRank *of a homogeneous* $\lambda \in \mathbb{F}[x_1, \dots, x_n]$ *is the smallest integer* s *such that there exist linear homogeneous* $\mu_1, \dots, \mu_s \in \mathbb{F}[x_1, \dots, x_n]$ *with* λ *contained in the algebra* $\mathbb{F}[\mu_1, \dots, \mu_s]$.

Hodges et al. [16] proved that $D_{\text{ff}}(p_1, \ldots, p_n)$ is bounded by

$$D_{\text{ff}}(p_1, \ldots, p_n) \leq D_{\text{ff}}(p) \leq \frac{\mathsf{LRank}(p)(q-1)+5}{2}.$$

Also, since $\mathsf{LRank}(p) \leq 3 \cdot \mathsf{Rank}(p)$ then

$$D_{\text{ff}}(p_1, \ldots, p_n) \leq \frac{3 \cdot \mathsf{Rank}(p)(q-1)+5}{2}. \tag{6}$$

On the other hand, the complexity of finding a Groebner basis $\mathcal{G}$ for the ideal I is bounded by

$$O\left(\binom{n + D_{\text{ff}}}{D_{\text{ff}}}^{\omega}\right),$$

where $2 \leq \omega \leq 3$ is the linear algebra constant. When n grows to infinity, the complexity [4] becomes $O\left(n^{\omega D_{\text{ff}}}\right)$. Therefore, according to the bound in (6), the complexity of finding $\mathcal{G}$ is bounded by

$$O\left(n^{\omega \frac{3 \cdot \mathsf{Rank}(p)(q-1)+5}{2}}\right).$$

Thus, if q and $\mathsf{Rank}(p)$ are constant, then the complexity of finding $\mathcal{G}$ is polynomial in the number of variables n. We also observe that the complexity is exponential in $\mathsf{Rank}(p)$.

4 Rank Analysis for Cubic Big Field Constructions

As we pointed out in Section 2.3, the Big Field Idea has been a basis to propose quadratic multivariate encryption schemes for decades. Nevertheless, Theorem 1 is not restricted to any particular degree, which means that this approach works to generate polynomials of any degree, in particular degree 3. In this section we show that if the central map is a low rank cubic polynomial, then, as in the quadratic case, there must exists a low-rank linear combination of the polynomials of the public key. In particular, we obtain an instance of the cubic MinRank problem which can be solved using the techniques presented in section 3. Thereafter, we discuss the direct algebraic attack on cubic big field schemes having low rank central map.

4.1 Big Field Idea for Cubic Polynomials

Let $\mathcal{F} \in \mathbb{K}[X]$ be a homogeneous weight 3 polynomial given by

$$\mathcal{F}(X) = \sum_{1 \leq i,j,k \leq n} \alpha_{i,j,k} X^{q^{i-1}+q^{j-1}+q^{k-1}}$$

[4] Notice that we are using an upper bound to estimate the complexity. This is a customary usage for this kind of attacks. In practice, it has been observed [32] that, on average, this bound is not too far from the actual complexity.

and $S, T \in \mathbb{F}^{n\times n}$ invertible matrices. Our first goal is to give an explicit expression for the multivariate cubic polynomials of the composition $T \circ \phi \circ \mathcal{F} \circ \phi^{-1} \circ S$. We begin by representing the map $\mathcal{F}$ as $\mathcal{F}(X) = \mathcal{T}(\mathbf{X}, \mathbf{X}, \mathbf{X})$ where $\mathbf{X} = (X^{q^0}, \ldots, X^{q^{n-1}})^\intercal$ and $\mathcal{T} : \mathbb{K}^n \times \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ is the trilinear form given by

$$\mathcal{T}(\boldsymbol{\beta}, \boldsymbol{\delta}, \boldsymbol{\gamma}) = \sum_{1\le i,j,k\le n} \alpha_{i,j,k} \cdot (\beta_i \delta_j \gamma_k).$$

Let A be the three-dimensional matrix whose entry (i, j, k) is given by $\alpha_{i,j,k}$, and assume without loss of generality that the matrix A is symmetric (otherwise we can take the matrix whose (i, j, k) entry is given by $\frac{1}{3!} \cdot (A[i, j, k] + A[i, k, j] + A[j, i, k] + A[j, k, i] + A[k, i, j] + A[k, j, i])$, which represents the same trilinear form $\mathcal{T}$).

Let $\mathcal{T}' : \mathbb{K}^n \times \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ be the trilinear form given by $\mathcal{T}'(\boldsymbol{\beta}, \boldsymbol{\delta}, \boldsymbol{\gamma}) = \mathcal{T}(\Delta S\boldsymbol{\beta}, \Delta S\boldsymbol{\delta}, \Delta S\boldsymbol{\gamma})$, we can write this trilinear form as

$$\mathcal{T}'(\boldsymbol{\beta}, \boldsymbol{\delta}, \boldsymbol{\gamma}) = \sum_{1\le i,j,k\le n} \alpha'_{i,j,k} \cdot (\beta_i \delta_j \gamma_k)$$

where $\alpha'_{i,j,k} = \mathcal{T}'(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k) = \mathcal{T}(\Delta S\mathbf{e}_i, \Delta S\mathbf{e}_j, \Delta S\mathbf{e}_k)$.

Let A' be the three-dimensional matrix whose entry (i, j, k) is given by $\alpha'_{i,j,k}$. Notice that this is the cubic version of the matrix $(\Delta S)^\intercal A(\Delta S)$ from Section 2.3. It is easy to see that the matrix A' is symmetric since the matrix A is.

Let $\mathbf{a} \in \mathbb{F}^n$ and let $\alpha = \phi^{-1}(S\mathbf{a})$, we know that $\mathsf{Fr}(\alpha) = \Delta \cdot \phi(\alpha) = \Delta S \cdot \mathbf{a}$ and therefore

$$\begin{aligned}\mathcal{F} \circ \phi^{-1}(S\mathbf{a}) = \mathcal{F}(\alpha) &= \mathcal{T}(\mathsf{Fr}(\alpha), \mathsf{Fr}(\alpha), \mathsf{Fr}(\alpha)) = \mathcal{T}(\Delta S \cdot \mathbf{a}, \Delta S \cdot \mathbf{a}, \Delta S \cdot \mathbf{a}) \\ &= \mathcal{T}'(\mathbf{a}, \mathbf{a}, \mathbf{a}) = \sum_{1\le i,j,k\le n} \alpha'_{i,j,k} \cdot (a_i a_j a_k).\end{aligned}$$

Let $R_1, \ldots, R_n \in \mathbb{F}^{n\times n\times n}$ be three-dimensional symmetric matrices such that $A' = y^0 \cdot R_1 + y^1 \cdot R_2 + \cdots + y^{n-1} \cdot R_n$, where $y^0, y^1 \ldots y^{n-1}$ is the basis of $\mathbb{K}$ over $\mathbb{F}$, as explained in Section 2.3. Then

$$\begin{aligned}\mathcal{F} \circ \phi^{-1} \circ S(\mathbf{a}) &= \sum_{1\le i,j,k\le n} \alpha'_{i,j,k} \cdot (a_i a_j a_k) \\ &= \sum_{1\le i,j,k\le n} \left(\sum_{\ell=1}^{n} y^{\ell-1} R_\ell[i, j, k] \right) \cdot (a_i a_j a_k) \\ &= \sum_{\ell=1}^{n} y^{\ell-1} \underbrace{\left(\sum_{1\le i,j,k\le n} R_\ell[i, j, k] \cdot (a_i a_j a_k) \right)}_{t_\ell}.\end{aligned}$$

Since $t_\ell \in \mathbb{F}$, we obtain that $\phi \circ \mathcal{F} \circ \phi^{-1} \circ S(\mathbf{a}) = (t_1, \ldots, t_\ell)^\intercal$. Therefore, each cubic polynomial in the composition $\phi \circ \mathcal{F} \circ \phi^{-1} \circ S$ is given by $f_\ell(\mathbf{x}) =$

$\sum_{1\leq i,j,k\leq n} R_\ell[i,j,k]\cdot(x_ix_jx_k)$. Finally, when we apply the transformation T we obtain that each cubic polynomial in the composition $P = T\circ\phi\circ\mathcal{F}\circ\phi^{-1}\circ S$ is given by

$$p_\ell(\mathbf{x}) = \sum_{1\leq i,j,k\leq n}\left(\sum_{t=1}^{n} T[\ell,t]\cdot R_t[i,j,k]\right)\cdot(x_ix_jx_k).$$

As a conclusion, if we let A_ℓ be the matrix whose entry (i,j,k) is given by $\sum_{t=1}^{n} T[\ell,t]\cdot R_t[i,j,k]$ then we obtain that this is the symmetric matrix corresponding to the ℓ-th polynomial in P. In particular, this shows we can compute efficiently the composition $T\circ\phi\circ\mathcal{F}\circ\phi^{-1}\circ S$ from S,T and $\mathcal{F}$.

4.2 Existence of Low Rank Linear Combination

Let us continue with the same setting as before, and let r be the rank of A, which in particular means that A can be written as $\sum_{\ell=1}^{r}\mathbf{u}_\ell\otimes\mathbf{v}_\ell\otimes\mathbf{w}_\ell$. Suppose that r is small. In this section we prove that there exists a low-rank linear combination of the three-dimensional matrices representing the composition P, and in Section 3.1 we showed how to find such combination.

Recall that the matrix A' was defined as $A'[i,j,k] = \mathcal{T}(\mathit{\Delta} S\mathbf{e}_i, \mathit{\Delta} S\mathbf{e}_j, \mathit{\Delta} S\mathbf{e}_k)$, we claim that the rank of this matrix is at most the rank of A. We show this by exhibiting vectors $\mathbf{u}'_\ell,\mathbf{v}'_\ell,\mathbf{w}'_\ell\in\mathbb{K}^n$ such that $A' = \sum_{\ell=1}^{r}\mathbf{u}'_\ell\otimes\mathbf{v}'_\ell\otimes\mathbf{w}'_\ell$. Let M be the matrix $\mathit{\Delta} S$, we define $\mathbf{u}'_\ell = \sum_{i=1}^{n}\mathbf{u}_\ell[i]\cdot M[i,\cdot]$, $\mathbf{v}'_\ell = \sum_{i=1}^{n}\mathbf{v}_\ell[i]\cdot M[i,\cdot]$ and $\mathbf{w}'_\ell = \sum_{i=1}^{n}\mathbf{w}_\ell[i]\cdot M[i,\cdot]$, then

$$\begin{aligned}
&A'[i',j',k'] \\
&\quad= \mathcal{T}'(M\mathbf{e}_{i'}, M\mathbf{e}_{j'}, M\mathbf{e}_{k'}) \\
&\quad= \sum_{1\leq i,j,k\leq n} A[i,j,k]\cdot\big((M\mathbf{e}_{i'})[i]\cdot(M\mathbf{e}_{j'})[j]\cdot(M\mathbf{e}_{k'})[k]\big) \\
&\quad= \sum_{1\leq i,j,k\leq n}\left(\sum_{\ell=1}^{r}\mathbf{u}_\ell[i]\cdot\mathbf{v}_\ell[j]\cdot\mathbf{w}_\ell[k]\right)\big((M[i,\cdot]\mathbf{e}_{i'})\cdot(M[j,\cdot]\mathbf{e}_{j'})\cdot(M[k,\cdot]\mathbf{e}_{k'})\big) \\
&\quad= \sum_{\ell=1}^{r}\sum_{1\leq i,j,k\leq n}\big(\mathbf{u}_\ell[i]M[i,\cdot]\mathbf{e}_{i'}\big)\big(\mathbf{v}_\ell[j]M[j,\cdot]\mathbf{e}_{j'}\big)\big(\mathbf{w}_\ell[k]M[k,\cdot]\mathbf{e}_{k'}\big) \\
&\quad= \sum_{\ell=1}^{r}\left(\sum_{i=1}^{n}\mathbf{u}_\ell[i]M[i,\cdot]\mathbf{e}_{i'}\right)\left(\sum_{j=1}^{n}\mathbf{v}_\ell[j]M[j,\cdot]\mathbf{e}_{j'}\right)\left(\sum_{k=1}^{n}\mathbf{w}_\ell[k]M[k,\cdot]\mathbf{e}_{k'}\right) \\
&\quad= \sum_{\ell=1}^{r}\left[(\mathbf{u}'_\ell)\,\mathbf{e}_{i'}\right]\left[(\mathbf{v}'_\ell)\,\mathbf{e}_{j'}\right]\left[(\mathbf{w}'_\ell)\,\mathbf{e}_{k'}\right] \\
&\quad= \sum_{\ell=1}^{r}\mathbf{u}'_\ell[i']\cdot\mathbf{v}'_\ell[j']\cdot\mathbf{w}'_\ell[k'].
\end{aligned}$$

From this we conclude that $A' = \sum_{\ell=1}^{r}\mathbf{u}'_\ell\otimes\mathbf{v}'_\ell\otimes\mathbf{w}'_\ell$ and hence $\mathsf{Rank}(A')\leq r$.

Now let $(\lambda_1,\dots,\lambda_n) = (y^0,\dots,y^{n-1})\cdot T^{-1}$, then

$$\sum_{i=1}^{n}\lambda_i A_i = \sum_{i=1}^{n}\lambda_i\left(\sum_{j=1}^{n} T[i,j]\cdot R_j\right) = \sum_{j=1}^{n} R_j \sum_{i=1}^{n} T[i,j]\cdot\lambda_i = \sum_{j=1}^{n} R_j\cdot y^{j-1} = A'.$$

This shows that there is a linear combination of the matrices representing the public key whose result is a low rank three-dimensional matrix. This yields directly an instance of the cubic MinRank problem which can be solved with the extension of the Kipnis-Shamir modeling presented in Section 3. As we mentioned before, this is by itself a weakness of the scheme, as it allows distinguishing public keys from random polynomial systems and also have implications on the degree of regularity of the system, as stated in Section 3.3. Moreover, the coefficients we have obtained here carry the same information about the secret key as those in the original (quadratic) MinRank attack, and this can be used in a similar way to construct equivalent keys.

4.3 Algebraic Attack for Cubic Big Field Constructions

As a complement of Section 3.3, we now consider the case when the polynomials $p_1,\dots,p_n$ are constructed using the big field idea for cubic polynomials. Hodges et al. [16] proved that for a scheme with core polynomial of weight 3, its first fall degree $D_{\mathrm{ff}}(p_1,\dots,p_n)$ is bounded by

$$D_{\mathrm{ff}}(p_1,\dots,p_n) \le \frac{\mathsf{LRank}(P_0)(q-1)+5}{2}.$$

Here P_0 is the homogeneous part of highest degree of the core polynomial $\mathcal{F}$ seen as an element of the graded algebra $\mathbb{K}[X_0,\dots,X_{n-1}]/\left(X_0^q,\dots,X_{n-1}^q\right)$, where X_i corresponds to X^{q^i}, for $i=0,\dots,n-1$. In our case

$$P_0 = \sum_{1\le i,j,k\le n} \alpha_{i,j,k} X_{i-1}X_{j-1}X_{k-1}.$$

If we take α_{ijk} uniformly at random, then with high probability $\mathsf{LRank}(P_0) \le \mathsf{Rank}(P_0)$, so

$$D_{\mathrm{ff}}(p_1,\dots,p_n) \le \frac{\mathsf{Rank}(\mathcal{F})(q-1)+5}{2}, \tag{7}$$

since $\mathsf{Rank}(P_0) = \mathsf{Rank}(\mathcal{F})$.

In [16] the authors show that if $\deg\mathcal{F} = D$, then $\mathsf{LRank}(\mathcal{F}) \le \lfloor\log_q(D-2)\rfloor + 1$, and hence

$$D_{\mathrm{ff}}(p_1,\dots,p_n) \le \frac{(q-1)\lfloor\log_q(D-2)\rfloor + 4 + q}{2}. \tag{8}$$

We now want to experimentally study the tightness of the bound (8), as they did in [16] for different parameters[5]. In Table 2 we present some of the results

[5] Table 1 in [16] do not include the values for the parameters we are interested in, so we constructed our own version of it.

obtained for different values of the parameters q, n and t, where t is the smallest integer such that $D \leq q^t - 1$. The value B corresponds to the bound given by equation (8), and D_{ff} is the first fall degree of the system for each choice of the parameters, which is read from Magma's verbose output. All the polynomials used in the attack were built as it will be explained in Section 4.1, and for all cases we have included the field equations, i.e., $x_i^q - x_i$ for $i = 1, \ldots, n$.

q	t	n	B	D_{ff}
5	3	8	8	8
5	3	9	8	8
5	3	10	8	8
5	4	8	10	9
5	4	9	10	9
5	4	10	10	10
5	5	8	12	9
5	5	9	12	9
5	5	10	12	10

q	t	n	B	D_{ff}
7	3	8	11	10
7	3	9	11	10
7	3	10	11	10
7	4	8	14	10
7	4	9	14	11
7	4	10	14	12
7	5	8	17	10
7	5	9	17	11
7	5	10	17	12

q	t	n	B	D_{ff}
11	3	8	17	13
11	3	9	17	14
11	3	10	17	15
11	4	8	22	13
11	4	9	22	14
11	4	10	22	15
11	5	8	27	13
11	5	9	27	14
11	5	10	27	15

q	t	n	B	D_{ff}
17	3	8	26	17
17	3	9	26	18
17	3	10	26	18
17	4	8	34	17
17	4	9	34	18
17	4	10	34	18
17	5	8	42	17
17	5	9	42	18
17	5	10	42	18

Table 2: Experimental results to study the tightness of the bound for D_{ff} given by (8), for different choices of the parameters q, t and n. The value of D_{ff} is read from Magma's verbose output.

We notice that the bound given by (8) is very tight for small values of q and t, and that it starts to widen considerably as q increases, and with a smaller pace as t increases. We also observe that for fixed q and t, the bound gets tighter as n increases. It is very clear that the bound needs to be improved for larger values of q.

5 Conclusions and Future Work

The minimum rank of a linear combination of the public polynomials is an important property of multivariate schemes. We have shown that this is still true for cubic schemes. The rank for cubic maps can be directly studied and exploited.

Many attacks have shown that it is hard to escape a low-rank when constructing quadratic encryption schemes. A high rank defect is necessary to allow decryption, leaving a low rank map exposed. Our rank analysis of cubic cryptosystems shows that low, fixed rank constructions have no chance of being secure. On the other hand, we are convinced that cubic polynomials allow more versatile constructions than quadratic, where a rank defect can help decryption but leave a rank large enough so that it does not necessarily represent a weakness.

This work is preliminary in the sense that it opens new questions. Can we construct cubic maps with a rank defect that allows decryption but leave a rank large enough for security? Other algorithms to solve the cubic-min-rank problem are likely, for example based on the minors modeling or on guessing kernel vectors. The complexity of each of these approaches needs to be studied more carefully (even in the quadratic case). These attacks could also be extendable to the cases where the field has characteristic 2 or 3. Finally, the hardness of rank problems for three-dimensional matrices can be further harvest as a security assumption.

Acknowledgements: This work was partially supported by "Fondo Nacional de Financiamiento para la Ciencia, la Tecnología y la Innovación Francisco José de Caldas", Colciencias (Colombia), Project No. 111865842333 and Contract No. 049-2015.

We would like to thank Jintai Ding for very useful discussions. We would also like to thank the reviewers of PQCrypto 2018 for their constructive reviews and suggestions. And last but not least, we thank the Facultad de Ciencias of the Universidad Nacional de Colombia sede Medellín for granting us access to the Enlace server, where we ran most of the experiments of this paper.

References

1. M. Aliasgari, M. R. Sadeghi, and D. Panario. Gröbner Bases for Lattices and an Algebraic Decoding Algorithm. In *2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1414–1415, Sept 2011.
2. M. Bardet, J.-C. Faugère, B. Salvy, and B.-Y. Yang. Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems. In *MEGA 2005. Eighth International Symposium on Effective Methods in Algebraic Geometry*, pages 1–14, 2005.
3. Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of HFE, multi-HFE and Variants for Odd and Even Characteristic. *Designs, Codes and Cryptography*, 69(1):1–52, Oct 2013.
4. J. F. Buss, G. S. Frandsen, and J. O. Shallit. The Computational Complexity of Some Problems of Linear Algebra. *Journal of Computer and System Sciences*, 58(3):572 – 596, 1999.
5. Chia-Hsin Owen Chen, Ming-Shing Chen, Jintai Ding, Fabian Werner, and Bo-Yin Yang. Odd-Char Multivariate Hidden Field Equations. *IACR Cryptology ePrint Archive*, 2008:543, 2008.
6. Jintai Ding and Timothy J. Hodges. Inverting HFE Systems is Quasi-Polynomial for All Fields. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 724–742. Springer Berlin Heidelberg, 2011.
7. Jintai Ding, Albrecht Petzoldt, and Lih-chung Wang. The cubic simple matrix encryption scheme. In Michele Mosca, editor, *Post-Quantum Cryptography*, pages 76–87, Cham, 2014. Springer International Publishing.
8. Daniel Escudero. Groebner Bases and Applications to the Security of Multivariate Public Key Cryptosystems. Available online at `http://cs.au.dk/~escudero/files/TDG.pdf`, 2016. Accessed: 2017-11-25.

9. J.-C. Faugère, M. S. El Din, and P.-J. Spaenlehauer. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and complexity. *Journal of Symbolic Computation*, 46(4):406 – 437, 2011.
10. Jean-Charles Faugère. A New Efficient Algorithm for Computing Gröbner Bases (F_4). *J. Pure Appl. Algebra*, 139(1-3):61–88, 1999. Effective methods in algebraic geometry (Saint-Malo, 1998).
11. Jean Charles Faugère. A New Efficient Algorithm for Computing Gröbner Bases Without Reduction to Zero (f5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC '02, pages 75–83, New York, NY, USA, 2002. ACM.
12. Jean-Charles Faugère, Françoise Levy-dit Vehel, and Ludovic Perret. Cryptanalysis of Minrank. In *Advances in Cryptology – CRYPTO 2008*, pages 280–296, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.
13. Louis Goubin and Nicolas T. Courtois. *Cryptanalysis of the TTM Cryptosystem*, pages 44–57. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000.
14. Yasufumi Hashimoto. *Multivariate Public Key Cryptosystems*, pages 17–42. Springer Singapore, Singapore, 2018.
15. Christopher J. Hillar and Lek-Heng Lim. Most Tensor Problems are NP-Hard. *J. ACM*, 60(6):45:1–45:39, November 2013.
16. Timothy J. Hodges, Christophe Petit, and Jacob Schlather. First Fall Degree and Weil Descent. *Finite Fields Appl.*, 30:155–177, November 2014.
17. Thomas D. Howell. Global properties of tensor rank. *Linear Algebra and its Applications*, 22(Supplement C):9 – 23, 1978.
18. Aviad Kipnis and Adi Shamir. *Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization*, pages 19–30. Springer Berlin Heidelberg, Berlin, Heidelberg, 1999.
19. Joseph B. Kruskal. Three-way arrays: rank and uniqueness of trilinear decompositions, with application to arithmetic complexity and statistics. *Linear Algebra and its Applications*, 18(2):95 – 138, 1977.
20. Joseph M Landsberg. *Tensors: geometry and applications*, volume 128 of *Graduate Studies in Mathematics*. American Mathematical Society, 2012.
21. Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.
22. Rusydi H. Makarim and Marc Stevens. M4GB: An Efficient Gröbner-Basis Algorithm. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17, pages 293–300, New York, NY, USA, 2017. ACM.
23. Tsutomu Matsumoto and Hideki Imai. Public Quadratic Polynominal-Tuples for Efficient Signature-Verification and Message-Encryption. In *Eurocrypt*, volume 88, pages 419–453. Springer, 1988.
24. Dustin Moody, Ray Perlner, and Daniel Smith-Tone. *An Asymptotically Optimal Structural Attack on the ABC Multivariate Encryption Scheme*, pages 180–196. Springer International Publishing, Cham, 2014.
25. Dustin Moody, Ray Perlner, and Daniel Smith-Tone. Improved attacks for characteristic-2 parameters of the cubic abc simple matrix encryption scheme. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography*, pages 255–271, Cham, 2017. Springer International Publishing.
26. Dustin Moody, Ray Perlner, and Daniel Smith-Tone. Key recovery attack on the cubic abc simple matrix multivariate encryption scheme. In Roberto Avanzi and

Howard Heys, editors, *Selected Areas in Cryptography – SAC 2016*, pages 543–558, Cham, 2017. Springer International Publishing.

27. Jacques Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In *Advances in Cryptology — EUROCRYPT '96*, pages 33–48, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.
28. Jacques Patarin, Nicolas Courtois, and Louis Goubin. Quartz, 128-bit long digital signatures. In *Cryptographers' Track at the RSA Conference*, pages 282–297. Springer, 2001.
29. Jaiberth Porras, John Baena, and Jintai Ding. ZHFE, A New Multivariate Public Key Encryption Scheme. In *International Workshop on Post-Quantum Cryptography*, pages 229–245. Springer, 2014.
30. Friedland Shmuel. Remarks on the Symmetric Rank of Symmetric Tensors. *arxiv.org/pdf/1505.00860*, January 2016.
31. Friedland. Shmuel and Małgorzata Stawiska. Best Approximation on Semi-Algebraic Sets and k-border Rank Approximation of Symmetric Tensors. *arxiv.org/pdf/1311.1561*, November 2013.
32. P-J. Spaenlehauer. *Solving multi-homogeneous and determinantal systems. Algorithms - Complexity - Applications.* PhD thesis, PhD thesis, Université Paris 6, 2012.
33. Bo-Yin Yang and Jiun-Ming Chen. Building secure tame-like multivariate public-key cryptosystems: The new tts. In Colin Boyd and Juan Manuel González Nieto, editors, *Information Security and Privacy*, pages 518–531, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.
34. Ismara Álvarez Barrientos, Mijail Borges-Quintana, Miguel Angel Borges-Trenard, and Daniel Panario. Computing Gröbner Bases Associated with Lattices. *Adv. in Math. of Comm.*, 10(4):851–860, 2016.