Cryptanalysis of MinRank

Jean-Charles Faugère[1], Françoise Levy-dit-Vehel[2], and Ludovic Perret[1]

[1] SALSA Project
INRIA, Centre Paris-Rocquencourt
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
104, avenue du Président Kennedy
75016 Paris, France
jean-charles.faugere@inria.fr, ludovic.perret@lip6.fr
[2] ENSTA, 32 Boulevard Victor, 75739 Paris cedex 15
levy@ensta.fr

Abstract. In this paper, we investigate the difficulty of one of the most relevant problems in multivariate cryptography – namely MinRank – about which no real progress has been reported since [19, 9]. Our starting point is the Kipnis-Shamir attack [19]. We first show new properties of the ideal generated by Kipnis-Shamir's equations. We then propose a new modeling of the problem. Concerning the practical resolution, we adopt a Gröbner basis approach that permitted us to actually solve challenges A and B proposed by Courtois in [8]. Using the multi-homogeneous structure of the algebraic system, we have been able to provide a theoretical complexity bound reflecting the practical behavior of our approach. Namely, when r' the dimension of the matrices minus the rank of the target matrix in the MinRank problem is constant, then we have a polynomial time attack $\mathcal{O}\left(\ln(q)\; n^{3\,r'^2}\right)$. For the challenge C [8], we obtain a theoretical bound of $2^{66.3}$ operations.

1 Introduction

The main purpose of this paper is the study of the MinRank (MR) problem. MR was originally introduced in [26] as one of the natural questions in linear algebra, and the authors there proved its NP-completeness. Later, it was restated in [8] in the cryptographic context. Since then, it has been shown to be related to several multivariate public key cryptosystems, for instance HFE [23, 19] and TTM [22, 9]. MR is also the basis of an efficient zero-knowlege authentication scheme [8]. According to the designer, this scheme is one of the most efficient post-quantum (i.e. based on a NP-complete problem) authentication scheme.

We can consider that MinRank – with the Polynomial System Solving (PoSSo) [17] and the Isomorphism of Polynomials (IP) [23] problems – is one of the main problems in multivariate cryptography. Contrarily to PoSSo for which progresses are reported continuously [12, 14], and IP which is now well mastered for most of its cryptographic applications [15, 16], no advance has been reported on MR since [19, 9]. To this respect, it has to be noted that the paper of X. Jiang, J. Ding and L. Hu [18] deals with the particular context of HFE. They show that due to the particular structure of the equations the complexity of the Kipnis-Shamir attack is exponential. The theoretical argument underlying his observation does not apply to the context of the generic MR problem.

There exists two non-trivial general techniques for solving MinRank. A first technique, called *kernel attack*, consists in guessing some vectors of an appropriate kernel, and then solve a resulting linear system [9, 8]. Another technique, due to Kipnis and Shamir [8, 19], consists in modeling MR as a PoSSo problem, i.e. one in which the purpose is to solve a quadratic system of equations. It is a transposition of an original attack on HFE [8, 19]. Initially, the complexity of this attack was evaluated using relinearization.

The starting point of our study is Kipnis-Shamir (KS) attack on MR. We begin by proving an exact correspondence between the solutions found by KS attack and the solutions of MR; moreover, we show how Kipnis-Shamir's approach somehow include the so-called *minors attack* and *Schnorr's attack* on MR. We then propose a new method for solving MR, which can be viewed as an extension of Schnorr's attack. After that, we present our practical way of solving MR, namely by means of fast Gröbner bases algorithms (e.g. [12]). Our main practical result is the breaking of the challenges A and B proposed for the MR-authentication scheme [8]. The MinRank problem being NP-hard, we cannot expect to solve efficiently all the instances. Thus, there is a set of parameters which remains out of the scope of our approach. But it has to be noted that the challenges we break correspond to sets of parameters which are the most interesting for practical use. Consequently, the place of MR-authentication scheme in the hierarchy of post-quantum schemes should be re-evaluated.

1.1 Organization of the paper. Main results.

In a first part of the paper, we recall known facts about the complexity of MR and its links with famous problems of coding theory. Then we detail two generic solving methods for MR, namely the kernel attack and Kipnis-Shamir attack. Section three is devoted to new properties satisfied by the equations generated by the Kipnis-Shamir attack (KS equations). In particular, we point out a bijection between the solutions of MR and the variety associated to the ideal generated by the KS equations. In the purpose of systematically studying and comparing all the modelings for MR, we show how the equations generated by other techniques – namely, the minors attack and Schnorr's attack – are included in the ideal of the KS equations. In section four, we describe our new modeling of the problem, that links the minors attack and Schnorr's attack. It appears that this new method is not the most efficient one, as quoted at the end of section 4. Thus, in order to evaluate the theoretical complexity of solving MR, we keep the best approach, that is, the one given by the KS equations. Section five provides such a theoretical complexity bound. It is obtained using multi-homogeneous properties of the equations. Our numerical results are presented in section six.

2 The MinRank problem

First, let us recall the MinRank problem over a field $\mathbb{K}$:

MinRank (MR)
Input : positive integers N, n, r, k, and matrices $M_0; M_1, \ldots, M_k$ in $\mathcal{M}_{N\times n}(\mathbb{K})$
Question : is there a k-tuple $(\lambda_1, \ldots, \lambda_k)$ of elements of $\mathbb{K}$ such that :

$$\text{Rank}\left(\sum_{i=1}^{k} \lambda_i \cdot M_i - M_0\right) \leq r.$$

We will in practice consider the search problem. If $N = n$, one gets a "square" instance of MR, that we call MR_s.

Property 1. MR_s and MR are poly-time many-one equivalent.

Proof. MR_s is a sub-problem of MR, in the sense that any instance of MR_s can be considered as an instance of MR.
Now, let g be a function from the set of instances of MR to the set of instances of MR_s, which maps a matrix M of size $N \times n$ to the square matrix of size $\max(N, n)$ obtained from M by adding $n - N$ rows (resp. $N - n$ columns) of zeroes (depending on whether $N < n$ or not). Then obviously $\text{Rank}(g(M))=\text{Rank}(M)$, so that any yes-instance of MR is mapped to a yes-instance of MR_s by g; and conversely, any instance of MR which, by g, becomes a yes-instance of MR_s, is indeed a yes-instance of MR. □

2.1 Complexity considerations.

Some complexity results have been proved for MR, linking it with other hard - or presumably hard - problems. The first one is a very simple reduction from Maximum Likelihood Decoding, proposed by Courtois in [9], which thus shows the NP-hardness of MR. Another less known fact is the link between MR and another problem in Coding Theory, namely Rank Decoding (RD). To this respect, the main result is that RD is poly-time many-one reducible to MR. The following lines are devoted to the RD problem and the proof of this result. Let us first recall what rank metric is.

Let $N, n \in \mathbb{N}^*$, and q be a power of a prime. We consider $\mathbb{F}_{q^N}$ as a vector space of dimension N over $\mathbb{F}_q$, and we fix a basis $\mathcal{B} = (b_1, \ldots, b_N)$ of it. For $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^N}^n$, we denote by $\text{Rank}(\mathbf{x} \,|\, \mathbb{F}_q)$, the rank of the $(N \times n)$ matrix with entries in $\mathbb{F}_q$ given by $X = (x_{ij})_{ij}$, where, for each j, $1 \leq j \leq n$, $x_j = \sum_{i=1}^{N} x_{ij} b_i$. In other words, X is obtained from $\mathbf{x}$ by expressing each coordinate of x in $\mathcal{B}$. For any two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^N}^n$, the quantity $d(\mathbf{x}, \mathbf{y}) = \text{Rank}(\mathbf{x} - \mathbf{y} \,|\, \mathbb{F}_q)$ defines a distance over $\mathbb{F}_{q^N}^n$, called *rank distance*. For codes over an extension field, rank distance is an analogue - although less discriminant - to the classical Hamming distance.

The Rank Decoding problem states as follows:

Rank Decoding (RD)
Input : positive integers N, n, r, k, a matrix G in $\mathcal{M}_{k\times n}(\mathbb{F}_{q^N})$ and a vector $c \in \mathbb{F}_{q^N}^n$.
Question : is there a vector $m \in \mathbb{F}_{q^N}^k$, such that $e = c - mG$ has rank $\mathrm{Rank}(e \,|\, \mathbb{F}_q) \leq r$?

If it is known a priori that $\mathrm{Rank}(e \,|\, \mathbb{F}_q) <= \lfloor (d-1)/2 \rfloor$, where d is the minimum (rank) distance of the considered code, then exactly one solution exists.

It is to be noted that MR can be seen as a *subfield subcode rank decoding* problem, where m has to be searched over the ground field $\mathbb{F}_q$. Indeed, let (N, n, r, k, G, c) be an instance of RD. Let $\mathcal{B} = (b_1, \ldots, b_N)$ be a basis of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$. Expressing each coordinate of c in this basis, we get an $N \times n$ matrix with entries in $\mathbb{F}_q$, that we call M_0. Analogously, for $1 \leq i \leq k$, expressing every entry of every row L_i of G in $\mathcal{B}$, we get an $N \times n$ matrix M_i over $\mathbb{F}_q$. Then $(N, n, r, k, M_0; M_1, \ldots, M_k)$ is an instance of MR that exactly corresponds to the instance (N, n, r, k, G, c) of RD in the sense that a solution $m = (\lambda_1, \ldots, \lambda_k)$ of this instance of MR will be a solution over $\mathbb{F}_q$ of the instance of RD, if ever such a solution exists.

As RD is in NP, we have that RD is poly-time many-one reducible to MR. A proof of this has been sketched in [7]. We give below a completely written proof of this property:
Proposition. [7] RD is poly-time many-one reducible to MR.

Proof. Fix a basis $\mathcal{B} = (b_1, \ldots, b_N)$ of $\mathbb{F}_{q^N}$, considered as an N-dimensional vector space over $\mathbb{F}_q$. Let f be the function that, to an instance $(N, n, r, k, G = (L_1, \ldots, L_k), c)$ of RD, associates the instance $(N, n, r, kN, M_0; M_1, \ldots, M_{kN})$ of MR, where M_0 is the $N \times n$ matrix with entries in $\mathbb{F}_q$ representing the vector $c \in \mathbb{F}_{q^N}^n$ in the basis $\mathcal{B}$, and $M_\ell = b_j L_i$ with $\ell = (i-1)N + j$, $1 \leq i \leq k$, $1 \leq j \leq N$, is the $N \times n$ matrix over $\mathbb{F}_q$ representing the product $b_j L_i$.
Let now $(N, n, r, k, G = (L_1, \ldots, L_k), c)$ be a yes-instance of RD, and let $m = (m_1, \ldots, m_k)$ be a vector of $\mathbb{F}_{q^N}^k$, solution to this instance, i.e. $\mathrm{Rk}((c - mG)|\mathbb{F}_q) = \mathrm{Rk}((c - \sum_{i=1}^k m_i L_i)|\mathbb{F}_q) \leq r$. For $1 \leq i \leq k$, let $m_i = \sum_{j=1}^N m_{ij} b_j$, $m_{ij} \in \mathbb{F}_q$, in the basis $\mathcal{B}$. Then, $m_i L_i = \sum_{j=1}^N m_{ij} b_j L_i$. We thus get

$$\mathrm{Rank}((c - mG)|\mathbb{F}_q) =$$

$$\mathrm{Rank}(M_0 - \sum_{i=1}^k \sum_{j=1}^N m_{ij} b_j L_i) = \mathrm{Rank}(M_0 - \sum_{i=1}^k \sum_{j=1}^N m_{ij} M_{(i-1)N+j}). \quad (1)$$

As this rank is $\leq r$, $\{m_{ij}\}_{1\leq i\leq k,\, 1\leq j\leq N}$ is a solution of the instance $(N, n, r, kN, M_0; M_1, \ldots, M_{kN}) = f(N, n, r, k, G, c)$ of MR.

Now let $(N, n, r, k, G = (L_1, \ldots, L_k), c)$ be an instance of RD, such that $f(N, n, r, k, G, c) = (N, n, r, kN, M_0; M_1, \ldots, M_{kN})$ is a yes-instance of MR. Let $m \in \mathbb{F}_q^{kN}$ be a solution of it. Then

$$\mathrm{Rk}(M_0 - \sum_{\ell=1}^{kN} m_\ell M_\ell) \leq r$$

Write $\ell = (i-1)N+j$, $1 \leq i \leq k$, $1 \leq j \leq N$. The equalities (1) then imply that the vector $(\sum_{j=1}^{N} m_j b_j, \sum_{j=1}^{N} m_{N+j} b_j, \ldots, \sum_{j=1}^{N} m_{(k-1)N+j} b_j)$, expressed in the basis $\mathcal{B}$ of $\mathbb{F}_{q^N}$, is a solution in $\mathbb{F}_{q^N}$ of the considered instance of RD.

2.2 Solving MinRank: known methods

We here consider a square instance $(n, r, M_0; M_1, \ldots, M_k)$ of MR. We are going to survey two methods to solve this problem. First, note that exhaustive search to find a tuple $(\lambda_1, \ldots, \lambda_k)$ of elements of $\mathbb{K}$ needs at most $(\#\mathbb{K}^k)n^3$ elementary operations on $n \times n$ matrices over $\mathbb{K}$.

The kernel attack. This first non-trivial attack on MR was proposed by Courtois and Goubin in citettmcrypt. It works as follows. First choose m vectors $\mathbf{x^{(i)}} \in \mathbb{F}_q^n,\ 1 \leq i \leq m$ at random. Secondly, solve the system of mn equations for $(\mu_1, \ldots, \mu_k) \in \mathbb{F}_q^k : (M_0 - \sum_{j=1}^{k} \mu_j M_j)\mathbf{x^{(i)}} = \mathbf{0}_n,\ \forall 1 \leq i \leq m$. Note that if $m = \lceil \frac{k}{n} \rceil$, this system essentially has only one solution $\lambda = (\lambda_1, \ldots, \lambda_k)$.

Now set $E_\lambda = M_0 - \sum_{j=1}^{k} \lambda_j M_j$; we want E_λ to be of rank $\leq r$. If this were the case, then $\dim(\mathrm{Ker} E_\lambda) \geq n - r$ and so, for $\mathbf{x} \in \mathbb{F}_q^n$ chosen at random,

$$\Pr\{\mathbf{x} \in \mathrm{Ker}E_\lambda\} \geq q^{-r} \text{ and } \Pr\{\{\mathbf{x^{(i)}},\ 1 \leq i \leq m\} \subseteq\ \mathrm{Ker}E_\lambda\} \geq q^{-mr}.$$

Thus, in order to find a λ such that E_λ has the desired rank, we have to run the above experiment (i.e. steps (1) and (2)) q^{mr} times on average. Taking the value of m as above, the complexity of this attack is thus $\mathcal{O}(q^{\lceil \frac{k}{n} \rceil r} k^3)$.

Kipnis-Shamir's attack In this attack, the MR problem is modeled as an MQ problem, i.e. one in which the purpose is to solve a quadratic system of equations. It is a transposition of an original attack on HFE due to Shamir and Kipnis [19]. In its principle, this attack is somehow dual to the previous one. The idea is to try to find a set of $n - r$ independent vectors of a special form in the kernel of : $E_\lambda = \sum_{i=1}^{k} \lambda_i \cdot M_i - M_0$. Putting the constraints into equations yields a quadratic system with unknowns a subset of coordinates of these vectors, together with the vector $\lambda = (\lambda_1, \ldots, \lambda_k)$.

In details, it works as follows: when λ is a solution of the considered MR instance, $\mathrm{rank}(E_\lambda) \leq r$. We want to express this rank condition as a large number of equations in a small number of variables. As $\dim\left(\mathrm{Ker}(E_\lambda)\right) \geq n - r$, there exists $n - r$ linearly independent vectors in $\mathrm{Ker}(E_\lambda)$. Name those vectors $x^{(1)}, \ldots, x^{(n-r)}$. Even if we fix the first $n - r$ coordinates of each vector to arbitrarily chosen values, we can still expect to get $n - r$ independent vectors. Each $x^{(i)}$ is thus of the form $x^{(i)} = (z_1, \ldots, z_{n-r}, x_1^{(i)}, \ldots, x_r^{(i)})$, where the z_is are chosen arbitrarily and $x_j^{(i)}$s are defined as new variables. The equalities :

$$\left(\sum_{i=1}^{k} \lambda_i \cdot M_i - M_0\right) x^{(i)} = \ \mathbf{0}_n, \text{ for all } i, 1 \leq i \leq n - r,$$

then yield a quadratic system of $(n-r)\cdot n$ equations in $r\cdot(n-r)+k$ unknowns. For $1 \leq i \leq n-r$ and $1 \leq j \leq n$, let $f_{i\,n+j}$ be the quadratic equation corresponding to j-th componant of $\left(\sum_{i=1}^{k} \lambda_i \cdot M_i - M_0\right) x^{(i)} = \mathbf{0}_n$.Here and in what follows, we shall denote by $\mathcal{I}_{\mathrm{KS}} = \left\langle f_1, \ldots, f_{n\,(n-r)} \right\rangle$ the ideal generated by these quadratic equations. Here, and in what follows, we shall denote by $\mathcal{I}_{\mathrm{KS}}$ the ideal generated by these quadratic equations.

3 A Fresh look at Kipnis-Shamir's attack

We here go deeper in the investigation of the properties of $\mathcal{I}_{\mathrm{KS}}$. First, we precise the link between the variety associated to $\mathcal{I}_{\mathrm{KS}}$ and the solutions of MR.

3.1 Properties of KS equations

The next theorem shows that the modeling proposed by Kipnis and Shamir is somehow optimal, in the sense that the zeroes of the KS equations exactly correspond to the solutions of MR.

Theorem 1. *Let $(n, k, M_0; M_1, \ldots, M_k, r) \in L_{\mathrm{MR}}$[3]. We shall denote by $\mathcal{S}ol(n, k, M_0; M_1, \ldots, M_k, r)$ the set of solutions of MinRank on $(n, k, M_0; M_1, \ldots, M_k, r)$. There is a one-to-one correspondence between $\mathcal{S}ol(n, k, M_0; M_1, \ldots, M_k, r)$ and the variety :*

$$V_{\mathbb{K}}(\mathcal{I}_{\mathrm{KS}}) = \{\mathbf{z} \in \mathbb{K}^{r\cdot(n-r)+k} : f(\mathbf{z}) = 0, \textit{for all } f \in \mathcal{I}_{\mathrm{KS}}\},$$

$\mathcal{I}_{\mathrm{KS}}$ being the ideal defined from the considered instance of MR as in Section 2.

Proof. Let $\mathbf{s} \in V_{\mathbb{K}}(\mathcal{I}_{\mathrm{KS}}) \subset \mathbb{K}^{r\cdot(n-r)+k}$. We can suppose w.l.o.g. that the last $r\cdot(n-r)$ components of $\mathbf{s}$ correspond to the variables $x_j^{(i)}$s, i.e. the unknowns corresponding to the $n-r$ linearly independent vectors of a suitable kernel.
We can then write $\mathbf{s} = (\lambda, \mathbf{s}_1, \ldots, \mathbf{s}_{n-r}) \in \mathbb{K}^{r\cdot(n-r)+k}$, where each $\mathbf{s}_i \in \mathbb{K}^r$ and $\lambda = (\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^k$. We then construct :

$$\mathbf{x}^{(i)} = (\underbrace{0, \ldots, 0}_{n-r \text{ zeroes}}, \mathbf{s}_i) \in \mathbb{K}^n.$$

By definition of $\mathcal{I}_{\mathrm{KS}}$, it holds that $\left(\sum_{t=1}^{k} \lambda_t \cdot M_t - M_0\right) \mathbf{x}^{(i)} = \mathbf{0}_n$, for all $i, 1 \leq i \leq n-r$. The vectors $\mathbf{x}^{(i)}, 1 \leq i \leq n-r$ being independent vectors, we get :

$$\mathrm{Rank}\left(\sum_{t=1}^{k} \lambda_t \cdot M_t - M_0\right) \leq r.$$

i.e. $\lambda = (\lambda_1, \ldots, \lambda_k)$ is a solution of MR on $(n, k, M_0; M_1, \ldots, M_k, r)$.
Conversely, the fact that any element of $\mathcal{S}ol(n, k, M_0; M_1, \ldots, M_k, r)$ corresponds to a point of $V_{\mathbb{K}}(\mathcal{I}_{\mathrm{KS}})$ has been explained in 2.2. $\square$

[3] The language associated to MinRank.

From this theorem, we can propose a classification of MinRank instances. As explained in the previous section, $\mathcal{I}_{\mathrm{KS}}$ is generated by $(n-r)\cdot n$ equations in $r\cdot(n-r)+k$ variables. The system is underdefined as soon as the number of variables is greater than the number of equations. This implies that :

$$\Delta = r\cdot(n-r)+k-(n-r)n = (r-n)\cdot(n-r)+k = -(n-r)^2+k$$

variables can take arbitrary values of $\mathbb{K}$. According to the previous theorem, there is a one-to-one correspondence between the zeroes of $\mathcal{I}_{\mathrm{KS}}$ and the solutions of MR. It follows that an instance $(n,k,M_0;M_1,\ldots,M_k,r)\in L_{\mathrm{MR}}$ has at least $\#\mathbb{K}^{\Delta}$ solutions if $\Delta>0$. Our concern is to find only one solution. To this end, we can randomly fix Δ variables in the system corresponding to $\mathcal{I}_{\mathrm{KS}}$. We will then get a system with the same number of variables as equations. It is then very likely that the corresponding variety will be reduced to a unique point (which will correspond to a solution of MR). This can be interpreted as follows :

Lemma 1. *Let $(n,k,M_0;M_1,\ldots,M_k,r)\in L_{\mathrm{MR}}$, and set $\Delta=-(n-r)^2+k$. If $\Delta>0$ and $(\lambda_{\Delta+1},\ldots,\lambda_k)\in \mathcal{S}ol(n,k-\Delta,M_0;M_{\Delta+1},\ldots,M_k,r)$ then for all $\mathbf{r}=(r_1,\ldots,r_\Delta)\in\mathbb{K}^{\Delta}$:*

$$(r_1,\ldots,r_\Delta,\lambda_{\Delta+1},\ldots,\lambda_k)\in \mathcal{S}ol(n,k,M_0;M_1,\ldots,M_k,r).$$

That is, all the solutions of $(n,k,M_0;M_1,\ldots,M_k,r)\in L_{\mathrm{MR}}$ can be easily deduced from $\mathcal{S}ol(n,k-\Delta,M_0;M_{\Delta+1},\ldots,M_k,r)$. This leads us to introduce the following terminology.

Definition 1. *Let $(n,k,M_0;M_1,\ldots,M_k,r)\in L_{\mathrm{MR}}$, and set $\Delta=-(n-r)^2+k$.*

- *If $\Delta=0$, then we shall say that the instance $(n,k,M_0;M_1,\ldots,M_k,r)$ is **well defined**.*
- *If $\Delta>0$, then we shall call **normalization** the process of deleting the first Δ matrices of $(n,k,M_0;M_1,\ldots,M_k,r)$. The result of this process is a **normalized** instance $(n,k-\Delta,M_0;M_{\Delta+1},\ldots,M_k,r)$.*

In the sequel, we will always focus our attention to well defined instances. We would like to emphasize that this is not a restriction. Instances which are not well defined can be normalized, leading then to well defined instances. According to Lemma 1, it is sufficient to study such normalized instances, as a normalized instance will indeed permit to describe all the solutions of the initial instance.

We also would like to point out that Lemma 1 permits to classify instances of MR with respect to their difficulty. From the lemma, it is clear that if we are able to solve efficiently the well defined instance $(n,k,M_0;M_1,\ldots,M_k,r)$, then we will be able to solve efficiently any instance $(n,k',M_0;M_1,\ldots,M_{k'},r)$ of MR with $k'\geq k$.

3.2 Relating KS to other algebraic methods

We will here show another "optimality" feature of the KS equations, namely that the equations obtain via other algebraic methods are indeed included in the ideal generated by the KS equations.
In this section, we let $(n, k, M_0; M_1, \ldots, M_k, r) \in L_{\mathrm{MR}}$ be an instance of MinRank and $\mathcal{I}_{\mathrm{KS}}$ be the associated ideal. We will suppose that $\mathcal{I}_{\mathrm{KS}}$ is radical, i.e.

$$\sqrt{\mathcal{I}_{\mathrm{KS}}} = \{f \in \mathbb{K}[x_1, \ldots, x_m] : \exists r > 0 \text{ s. t. } f^r \in \mathcal{I}_{\mathrm{KS}}\} = \mathcal{I}_{\mathrm{KS}}.$$

In the cryptographic context, the ideals are usually radical. This is due to the fact that, for an ideal to be radical, it is sufficient that the field equations be included in it. In practice, we have not included the field equations in $\mathcal{I}_{\mathrm{KS}}$. However, for proving the radicality of $\mathcal{I}_{\mathrm{KS}}$, we can suppose w.l.o.g. that such equations are included in $\mathcal{I}_{\mathrm{KS}}$.

The minors method. This method comes back to the very definition of MR, and expresses that $(\lambda_1, \ldots, \lambda_k)$ is a solution of MR if and only if all the minors of degree $r' > r$ of the matrix $\sum_{i=1}^{k} \lambda_i M_i - M_0$ are zero. In this context, we have the following

Proposition 1. *Set* $E(x_1, \ldots, x_k) = \sum_{i=1}^{k} x_i M_i - M_0$. *Then all the minors of* $E(x_1, \ldots, x_k)$ *of degree* $r' > r$ *lie in* $\mathcal{I}_{\mathrm{KS}}$.

Proof. A solution of MR corresponds to a specialization of the variables $x_1, \ldots, x_k$ in $E(x_1, \ldots, x_k)$, leading to a matrix of rank $\leq r$. For such a specialization, all the minors $M_{r'}$ of rank $r' > r$ of the matrix $E(x_1, \ldots, x_k)$ must equal zero. A minor $M_{r'}$ is a polynomial of degree r' whose variables are $x_1, \ldots, x_k$.
It is clear that all the minors vanish on $V_{\mathbb{K}}(\mathcal{I}_{\mathrm{KS}})$. Therefore, by Hilbert's Strong Nullstellensatz [1] (th. 2.2.5), we get that all the minors of rank $r' > r$ lie in the radical of $\mathcal{I}_{\mathrm{KS}}$. This ideal being radical, it turns out that all those minors lie in $\mathcal{I}_{\mathrm{KS}}$. □

Schnorr's method. This unpublished method due to Schnorr was quoted in [7]. The idea is to consider the multivariate polynomial

$$P(x_1, \ldots, x_k) = \mathrm{Det}\left(\sum_{i=1}^{k} x_i M_i - M_0\right). \tag{2}$$

If $\lambda = (\lambda_1, \ldots, \lambda_k)$ is a solution of MR, then λ is a root of P of multiplicity greater than or equal to $n - r$. This means that such a λ is solution of $P(x_1, \ldots, x_k) = 0$ as well as $\left\{\frac{\partial^j P}{\partial x_i}(x_1, \ldots, x_k) = 0\right\}_{1 \leq i \leq k}$, for all j, $1 \leq j \leq n - r - 1$. This means that all these equations vanish on $V_{\mathbb{K}}(\mathcal{I}_{\mathrm{KS}})$ and therefore belong to $\mathcal{I}_{\mathrm{KS}}$.

To summarize, we have proved that the KS equations include the equations that one could obtain using minors or a basic property of the determinant. From a system solving point of view, this means that solving MR using KS equations is at least as efficient as solving MinRank using either of those alternative methods. We will see that KS equations lead to a more efficient solving. Before that, we present a new method for setting up a system of equations for MinRank.

4 A new modeling

This new method will permit to link Schnorr and the minors methods. The starting point is similar to Schnorr's method, namely we will consider the polynomial given in (2). Remark that if $k = 1$, then $P(x_1) = \mathrm{Det}(x_1 \cdot I - M_0 M_1^{-1})$ is exactly the characteristic polynomial of $M_0 M_1^{-1}$. In this special context, MinRank corresponds to the problem of finding the eigenvalues of $M_0 M_1^{-1}$. It is well known that this can be done by computing the roots of the characteristic polynomial $P(x_1)$. Schnorr's method is a generalization of this technique.

We also would like to mention that MinRank is related to the so-called matrix pencils problem.The eigenvalue of a linear matrix pencil $(A, B) \in \mathcal{M}_{n\times n} \times \mathcal{M}_{n\times n}$ is a $\lambda \in \mathbb{K}$ such that $\mathrm{Det}(A - \lambda B) = 0$.

The generalized high order eigenvalue problem consists of finding the eigenvalues of for a matrix pencil $(M_1, \ldots, M_k) \in (\mathcal{M}_{n\times n})^k$; i.e. finding $\lambda \in \mathbb{K}$ such that $\mathrm{Det}\left(\sum_{i=1}^k \lambda^i M_i\right) = 0$. One can see that MinRank is a multivariate version of this problem.

We will now describe a new approach for modeling $\mathrm{MR}(n, k, r)$ as a set of algebraic polynomials. To do so, we remark that if $\lambda = (\lambda_1, \ldots, \lambda_k)$ is a solution of MinRank then λ is root of $P(x_1, \ldots, x_k)$ with "multiplicity" $n - r$. More precisely, the polynomial $P(x_1 + \lambda_1, \ldots, x_k + \lambda_k)$ has no terms of degree smaller or equal to $n - r$. Thus, similarly to the univariate case, the coefficients of the monomials of degree d are sums of the minors of degree $n - d$ of the matrix : $E(x_1, \ldots, x_k) = \sum_{i=1}^k x_i M_i - M_0$. In order to construct the system, we will introduce new variables $y_1, \ldots, y_k$ and consider the polynomial :

$$Q(y_1, \ldots, y_k) = P(x_1 + y_1, \ldots, x_k + y_k) \in \mathbb{K}\left[y_1, \ldots, y_k\right].$$

We can view this polynomial as a polynomial whose variables are $y_1, \ldots, y_k$ and coefficients are monomials in the variables $x_1, \ldots, x_k$. As explained, a solution of MinRank must vanish on all the monomials of degree smaller than $n - r$ in $Q(y_1, \ldots, y_k)$. The new system is then obtained by equating to zero the coefficients, in $Q(y_1, \ldots, y_k)$, of the monomials of degree d such that $0 < d < n - r$. Such coefficients are polynomials in the variables $x_1, \ldots, x_k$, of degree d, with $r < d < n$. Moreover, we can restrict our attention to the coefficients in $Q(y_1, \ldots, y_k)$ of degree $n-r-1$. Thus we obtain a subset of linearly independent minors of $\sum_{i=1}^k x_i M_i - M_0$ which are polynomials in $x_1, \ldots, x_k$ of degree $r + 1$.

This then permits to establish a link between Schnorr and the minors methods. Let $\mathrm{M}_d(m)$ be the set monomials of degree d in m variables. We have $\#\mathrm{M}_d(m) = \binom{m+d-1}{d}$. We can also count precisely the number of minors of degree $r + 1$, i.e. $\#\mathrm{M}_{n-r-1}(k)$. We have obtained a system of $\#\mathrm{M}_{n-r-1}(k)$ algebraic equations of degree $r + 1$. Similarly to the previous section, one can prove that these new equations will also lie in $\mathcal{I}_{\mathrm{KS}}$, and more precisely in $\mathcal{I}_{\mathrm{KS}} \cap \mathbb{K}[x_1, \ldots, x_k]$. From a practical point of view, it turns out that the new approach is a little less efficient than the one of computing a Gröbner basis of $\mathcal{I}_{\mathrm{KS}}$. This is quite surprising since our new method will generate an overdefined system of equations.

5 Theoretical bound on the complexity

We will now try to explain such a behavior, and evaluate the complexity of computing a Gröbner basis of $\mathcal{I}_{\mathrm{KS}}$. To do so, we recall that the complexity of all known Gröbner bases algorithms depends on the so-called *degree of regularity* of the system [10, 2–4]. This corresponds to the maximal degree reached during a Gröbner basis computation. If d_{reg} is the degree of regularity of $\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_m]$, then the complexity of computing a Gröbner basis of $\mathcal{I}$ with F_5 [12] is :

$$\mathcal{O}\big(\left(\#\mathrm{M}_{d_{\mathrm{reg}}}(m)\right)^{\omega} \big) ,$$

with $\omega, 2 \leq \omega \leq 3$ the linear algebra constant.

In general, it is a difficult problem to know *a priori* the degree of regularity. For *regular and semi-regular systems* [2–4] (i.e. "ramdom" systems of algebraic equations), the behavior of the regularity is well mastered. For instance, if we suppose that KS equations are semi-regular, then we obtain a degree of regularity equal to $m + 1$, $m = r(n - r) + k$. Besides, we also know that the number of solutions is bounded from above by the Bézout bound, which is equal to 2^m for KS equations.

In our context, this is unsatisfactory. Indeed, this does not match with the experimental results that we will present in the next section. Typically, we have observed a degree of regularity which seems to be $\approx r + 2$ (see Section 6). Similarly, computing the degree of regularity of the systems obtained with one of the three other methods presented so far will not lead to a satisfactory bound.

To fill this gap between theory and practice, we have remarked that the ideal $\mathcal{I}_{\mathrm{KS}}$ is *multi-homogeneous* (see for instance [21, 25]). Namely, the equations are homogeneous with respect to blocks of variables.

Definition 2. *Let $S = \{f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0\}$ be an algebraic system of equations, and $T = \{X^{(1)}, \ldots, X^{(k)}\}$ be a partition of $X = \{x_1, \ldots, x_n\}$ s.t. :*

$$X^{(j)} = \{x_{j_1}, \ldots, x_{j_{k_j}}\}.$$

We shall say that S is multi-homogeneous if the polynomials f_i are homogenous w.r.t. the $X^{(j)}$'s.

For such systems, one can obtain new bounds for the degree of regularity and number of solutions [20, 24, 21].

Definition 3. *Let $S = \{f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0\}$ be an algebraic system of equations, and $T = \{X^{(1)}, \ldots, X^{(k)}\}$ be a partition of $X = \{x_1, \ldots, x_n\}$ s.t. $X^{(j)} = \{x_{j_1}, \ldots, x_{j_{k_j}}\}$. We shall call partition vector of T the vector $K = [k_1, \ldots, k_m]$. Now, let $d_{i,j}$ be the degree of f_i restricted to the variables of $X^{(j)}$. We shall define the degree matrix under the partition T as :*

$$\begin{bmatrix} d_{1,1} & d_{1,2} & \cdots & d_{1,m} \\ d_{2,1} & d_{2,2} & \cdots & d_{2,m} \\ \vdots & \vdots & & \vdots \\ d_{n,1} & d_{n,2} & \cdots & d_{n,m} \end{bmatrix}.$$

The multi-homogeneous Bézout number associated to the partition T is defined as the coefficient of $z_1^{k_1} z_2^{k_2} \cdots z_m^{k_m}$ in the following polynomial :

$$(d_{1,1} z_1^{k_1} + d_{2,1} z_2^{k_2} + \cdots + d_{1,m} z_m^{k_m})(d_{2,1} z_1^{k_1} + \cdots d_{2,m} z_m^{k_m}) \cdots (d_{n,1} z_1^{k_1} + \cdots + d_{n,m} z_m^{k_m}).$$

This leads to the following result.

Theorem 2. *Let $r' = n - r$ be a constant, and we will consider instances of MinRank with parameters $\left(n, k = r'^2, r = n - r'\right)$. If we denote by $\mathcal{S}ol$ the set of solutions of MinRank on such instances, it holds that :*

$$\#\mathcal{S}ol \leq \binom{n}{r'}^{r'}$$

For those particular instances, we can compute the variety of $\mathcal{I}_{\mathrm{KS}}$ using Gröbner bases in :

$$\mathcal{O}\left(\ln(q)\; n^{3\, r'^2}\right),$$

where q is the size of the finite field $\mathbb{K}$.
In other words, the complexity of our attack is polynomial for instances of MinRank with $\left(n, k = r'^2, r = n - r'\right)$.

Proof. First, we will assume an upper bound, say D, on the number of solutions of $\mathcal{I}_{\mathrm{KS}}$. From such a D we can derive an upper bound on the complexity of computing a Lex-Gröbner basis from another (e.g. DRL) Gröbner basis using FGLM : D^3 (see [27, 13] for details).

Now to find such a D we exhibit a multi-homogeneous structure for the equations generating $\mathcal{I}_{\mathrm{KS}}$. We can consider the following partition :

$$T = T_0 \cup \cdots \cup T_{n-r} = T_0 \cup \bigcup_{i=1}^{n-r} X^{(i)},$$

where $T_0 = [\lambda_1, \ldots, \lambda_k]$ and $T_i = X^{(i)} = [x_1^{(i)}, \ldots, x_r^{(i)}]$ (the $x_j^{(i)}$ are defined as in 2.2).
T is a partition of the set of variables. The degree of the polynomials $\{f_j\}_{1 \leq j \leq n\cdot(n-r)}$ with respect to T_0 (resp. $X^{(i)}$) will be denoted by $d_\ell^{(0)}$ (resp. $d_\ell^{(i)}$). The degree matrix corresponding to the partition T is :

$$\begin{bmatrix} d_1^{(0)} & \cdots \cdots & d_1^{(n-r)} \\ d_2^{(0)} & \cdots \cdots & d_2^{(n-r)} \\ \vdots & & \vdots \\ d_{n\cdot(n-r)}^{(0)} & \cdots \cdots & d_{n\cdot(n-r)}^{(n-r)} \end{bmatrix}.$$

Here, the partition vector is $K = [k, r, \ldots, r]$. As explained, the multi-homogeneous Bezout number is thus the coefficient of $z_1^k z_2^r \cdots z_{n-r+1}^r$ into the polynomial :

$$(z_1 + z_2)^n (z_1 + z_3)^n \cdots (z_1 + z_{n-r+1})^n.$$

Consequently, we can bound the number of solutions ($\#\mathcal{S}ol$) by $D = \binom{n}{r}^{n-r} \approx \left(\frac{n^{r'}}{r'!}\right)^{r'} = \frac{n^{r'^2}}{(r'!)^{r'}}$ assuming that $r' = n - r$ is constant when $n \longrightarrow \infty$. $\square$

Theorem 2 applies to challenges A, B, C. We obtain the following complexity bounds:

(n, k, r)	$(6, 9, 3)$	$(7, 9, 4)$	$(11, 9, 8)$
$\#\mathcal{S}ol$ (MH Bezout bound)	8000	42875	$2^{22.1}$
Complexity bound $(\#\mathcal{S}ol)^3$	$2^{38.9}$	$2^{46.2}$	$2^{66.3}$

We would like to emphasize that such theoretical bounds are coherent with the results of the experiments that we are going to present.

6 Experimental results

Initially, the complexity of the Kipnis-Shamir attack was evaluated using relinearization [19]. Here, we propose to use a more efficient tool for solving algebraic systems, namely fast Gröbner bases [5, 6] algorithms : F_5 [12] together with FGLM [13]. This choice permits to go one step further in the cryptanalysis of MinRank, especially for instances used in the ZK authentication scheme proposed in [8]. We have quoted below the set of parameters of the ZK authentication scheme recommended by the author of [8]. We have also given the number of equations and variables obtained using KS :
A : $\mathbb{F}_{65521}, k = 10, n = 6, r = 3$ (18 eq., and 19 variables)
B : $\mathbb{F}_{65521}, k = 10, n = 7, r = 4$ (21 eq., and 22 variables)
C : $\mathbb{F}_{65521}, k = 10, n = 11, r = 8$ (33 eq., and 35 variables)
One can remark that these instances of MR are not well defined. Thus, as explained in Lemma 1, we can fix $\Delta = 1$ variables for the challenges A, B (resp. $\Delta = 2$ variables for challenge C). This is then equivalent to solve MinRank on the following parameters :
A : $\mathbb{F}_{65521}, k = 9, n = 6, r = 3$ (18 eq., and 18 variables)
B : $\mathbb{F}_{65521}, k = 9, n = 7, r = 4$ (21 eq., and 21 variables)
C : $\mathbb{F}_{65521}, k = 9, n = 11, r = 8$ (33 eq., and 33 variables)

The boldface letters **A**, **B**, **C** being the normalized of the challenges A, B, C respectively. Before presenting our practical results, we would like to explain the conditions of the experiments.

Generation of the instances
We have randomly generated k matrices $(M_1, \ldots, M_k) \in \mathcal{M}_{n,n}(\mathbb{K})^k$ and k coefficients $(\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^k$ such that $\lambda = \sum_{i=1}^{k} \lambda_i \neq 0$. Finally, we have randomly selected a matrix $M \in \mathcal{M}_{n,n}(\mathbb{K})$ of rank r and set $M_0 = \sum_{i=1}^{k} \lambda_i (M_i - M)$. Thus we have $\mathrm{Rank}\left(\sum_{i=1}^{k} \lambda_i M_i - M_0\right) = \mathrm{Rank}(\lambda M) = r$.

Programming language – Workstation
The experimental results have been obtained with several Xeon bi-processors 3.2 Ghz, with 64 Gb of Ram. The instances of MinRank have been generated using

the Maple software. The F_5 [12] and FGLM [13] algorithms have been implemented in C in the FGb software. We used this implementation for computing Gröbner bases. From time to time, we use the last version of Magma (2.14) for obtaining these bases. This version of Magma includes efficient implementations of the F_4 [11] and FGLM algorithms. Hence, the reader can reproduce the experimental results. We were able to break the two challenges **A** and **B** using FGb or Magma. There is a huge gap between these challenges and challenge **C**, which seems intractable with the current implementation. However, we can estimate the complexity of our attack for the last challenge by :

- studying intermediate instances of the MinRank problem, i.e. $\mathrm{MR}(n,k,r)$ with $\mathbb{K} = \mathbb{F}_{65521}, n = r+3$, $k = (n-r)^2 = 9$ and $r = 3,4,5,6,7,8$.
- Since all the λ_i are in $\mathbb{K}$, we can perform an exhaustive search on some λ_i. Namely, we will suppose that we have $s > 0$ coefficients of a solution $(\lambda_1,\ldots,\lambda_k)$ of MinRank. This is equivalent to solve a $\mathrm{MR}(n-s,k,r)$ problem. From a system solving point of view, this means that we will solve $\#\mathbb{K}^s$ overdetermined systems. When $s > 0$ the number of solutions of the corresponding algebraic system is always 1 and any Gröbner basis for any monomial ordering gives the solution; consequently there is no need to apply the FGLM algorithm.

Table Notation
The following notation is used in the next table :

- T_{DRL} is the CPU time (in seconds) for computing a Gröbner basis for a total degree ordering.
- D is the number of solutions in the algebraic closure of $\mathbb{F}_{65521}$ ($D = 1$ when $s > 0$).
- T_{FGLM} is the CPU time (in seconds) for changing the basis to a lexicographic Gröbner basis using the FGLM algorithm. The complexity [13] is D^3.
- T is the time of our approach for finding a solution of MinRank; thus $T = T_{\mathrm{DRL}} + T_{\mathrm{FGLM}}$ when $s = 0$ and $T = T_{\mathrm{DRL}}$ when $s > 0$.
- d_{reg}, the maximum degree reached during the computation of a Gröbner basis with F_5.
- M, the maximum memory usage (in Mbytes) during a computation with F_5.
- $Log_2\,(N)$ is the log in base 2 of the number of arithmetic operations N for solving the MinRank problem. When $s = 0$, N is the total number of operations for the first Gröbner basis computation and FGLM.

Interpretation of the Results
Challenges **A** $(6,9,3)$ and **B** $(7,9,4)$ are completely broken. We emphasize that such sets of parameters were the most suited for a practical use of the ZK authentication scheme proposed in [8].

As explained in 3.1, we would be able to solve any instance $(n,k',M_0;M_1,\ldots,M_{k'}$ $,r)$ of MR, with n,r as in the challenges and for all $k' > 9$. For example, all instances $(6,k',M_0;M_1,\ldots,M_{k'},3)$, with $k' > 9$ can be solved in one minute.

		$\mathbb{K} = \mathbb{F}_{65521}$ MR(n,k,r)					
		Chall **A**	Chall **B**				Chall **C**
		$(6,9,3)$	$(7,9,4)$	$(8,9,5)$	$(9,9,6)$	$(10,9,7)$	$(11,9,8)$
$s=0$	$T_{\mathrm{DRL}} + T_{\mathrm{FGLM}}$ (FGb)	30.0+34.8	3794+2580	328233			
	T_{DRL}+ T_{FGLM} (Magma)	300+200	48745+∞	∞			
	memory : M	406.5	3113	58587			
	$Log_2\,(N)$	30.5	37.1	43,4			
	d_{reg}	5	6	7			
	Solutions: D	980	4116	14112			
$s=1$	T_{DRL} FGb	1.85	166.6	5649.7	590756		
	M	343.9	522.1	4548.7	43267		
	$Log_2\,(N)$	25,95	32.3	36.8	43.9		
	d_{reg}	4	5	6	6		
$s=2$	T_{DRL} FGb	0.5	5.5	632	14867		
	M	39.8	68.0	806,4	2510.3		
	$Log_2\,(N)$	24.1	27.5	34.1	38.7		
	d_{reg}	4	4	5	6		
$s=3$	T_{DRL} FGb	0.05	1.0	15.6	234.3	4248.4	56987
	M	35.5	44.9	75.4	888.6	2792.3	10539
	$Log_2\,(N)$	20.1	25.0	29.2	32.8	36.9	40.6
	d_{reg}	4	4	4	5	6	7

Fig. 1. Experimental results with FGb

We have observed in our experiments that the maximum degree d_{reg} seems to be equal to $\max(r+2,4)$. We recall that the complexity of computing a Gröbner basis with F_5 [12] is bounded by $\mathcal{O}\left(\#\mathrm{M}_{d_{\mathrm{reg}}}(N)^3\right)$, where N is the number of variables. Here, $N = r(n-r)+k$. For MR$(r+3,9,r)$, we have $N = 3\,(r+3)$, yielding the bound:

$$\binom{N+d_{\mathrm{reg}}-1}{d_{\mathrm{reg}}}^3 = \binom{3(r+3)+r+}{r+3}^3 \approx e^{3\,r+3\,(\frac{3}{2}+r)\ln(r)}.$$

For challenge **C**, we have $r=8$ and we will obtain a complexity bound of 2^{120}. Of course this is a very pessimistic bound. We will now improve this bound.

Estimated Complexity of the attack.

To obtain a better result, we use the following bound :

$$\#\mathrm{MR}(n,k,r) \leq (\#\mathbb{K})^s \times \#\mathrm{MR}(n-s,k,r),$$

where $\#\mathrm{MR}(n,k,r)$ is the number of operation to solve the corresponding min-rank problem MR(n,k,r). This bound is tight only when s is small. We can use our experimental results to derive new bounds for $\#\mathrm{MR}(r+3,9,r)$ and $\mathbb{K} = \mathbb{F}_{65521}$. For such parameters :

$$\log_2\left(\#\mathrm{MR}(r+3,9,r)\right) \leq 16s + \log_2\left(\#\mathrm{MR}(r+3-s,9,r)\right).$$

The following notation is used in the table below:
– $Nb(r, s) = 16s + \log_2 \big(\#\mathrm{MR}(r + 3 - s, 9, r)\big)$ is a logarithmic upper complexity bound for solving $\mathrm{MR}(r + 3, 9, r)$.
– $Nb(r) = \log_2 \big(\#\mathrm{MR}(r + 3, 9, r)\big)$ is the exact number of oper. of our attack.
– "Security Bound" is the Log_2 of the complexity of the best approach known so far for solving MinRank. This is based on [8].
– "Estimated Bound" is an extrapolation of the complexity. This bound is not rigorous.
– $(\mathrm{MHBezout})^3$ is the theoretical complexity bound obtained in the previous section.

	$\mathbb{K} = \mathbb{F}_{65521}$ $MR(n, k, r)$					
	Chall **A**	Chall **B**				Chall **C**
	(6,9,3)	(7,9,4)	(8,9,5)	(9,9,6)	(10,9,7)	(11,9,8)
$Nb(r)$	30,5	37,1	43,4			
$Nb(r, 1)$	42,0	48,3	52,8	59,9		
$Nb(r, 2)$	54,1	59,5	66,1	70,7		
$Nb(r, 3)$	68,2	72,9	77,2	80,8	84,9	88,6
Estimated Bound	30,5	37,1	43,4	50,4	57,4	64,4
Bezout^3	38,9	46,2	52,3	57,5	62,2	66,3
Security Bound	106	122				138

For challenge $(11, 9, 8)$ we obtain a complexity of 2^{88} for our attack. Clearly, this is not feasible in practice. However, this is much better than the previous security estimates (2^{138}) [8]. Still, this remains a pessimistic bound.

By using the estimated bound, which is less rigorous but more close to what we observed in practice (for the instances that we have been able to solve), we can evaluate the complexity of our attack to 2^{65} . We would like to emphasize that this is very close to the theoretical complexity bound $2^{66.3}$ obtained in the previous section using the particular structure of the algebraic system.

Conclusion
We have provided a unified view of the attacks known so far against the MinRank problem. We have also presented a new modeling of the problem that actually links the minors attack and Schnorr's method. From a practical point of view, our approach of solving the systems by means of fast Gröbner bases algorithms led to the breaking of the most practical challenges proposed for the MR-authentication scheme. On a more theoretical level, we showed that MinRank is polynomial when $n - r$ is constant. One line of research would now be to study the impact of our method on the solving of the Rank Decoding problem.

Acknowledgement. We wish to thank Mohab Safey El Din who brought multi-homogeneous papers to our attention.We also would like to thank the LIP6 for its cluster of computers that permitted us to conduct the experiments.

References

1. W.W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases.* Graduate Studies in Mathematics, Vol. 3, AMS, 1994.
2. M. Bardet. *Étude des Systèmes Algébriques Surdéterminés. Applications aux Codes Correcteurs et à la Cryptographie.* Thèse de doctorat, Université de Paris VI, 2004.
3. M. Bardet, J-C. Faugère, B. Salvy and B-Y. Yang. *Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems.* In Proc. of MEGA 2005, Eighth International Symposium on Effective Methods in Algebraic Geometry, 2005.
4. M. Bardet, J-C. Faugère, and B. Salvy *On the Complexity of Gröbner Basis Computation of Semi-Regular Overdetermined Algebraic Equations.* In Proc. International Conference on Polynomial System Solving (ICPSS), pp. 71–75, 2004. Available at *http://www-calfor.lip6.fr/ICPSS/papers/43BF/43BF.htm.*
5. B. Buchberger, G.-E. Collins, and R. Loos. *Computer Algebra Symbolic and Algebraic Computation.* Springer-Verlag, second edition, 1982.
6. B. Buchberger. *Gröbner Bases : an Algorithmic Method in Polynomial Ideal Theory.* Recent trends in multidimensional systems theory. Reider ed. Bose, 1985.
7. N. Courtois. *Decoding Linear and Rank-Distance Codes, MinRank problem and Multivariate Cryptanalysis.* CLC'06, Darmstadt, September 2006.
8. N. Courtois. *Efficient Zero-knowledge Authentication Based on a Linear Algebra Problem MinRank.* Advances in Cryptology – ASIACRYPT 2001, Lecture Notes in Computer Science, vol. 2248, Springer–Verlag, pp. 402–421, 2001.
9. N. Courtois and L. Goubin. *Cryptanalysis of the TTM Cryptosystem.* Advances in Cryptology, Proceedings of Asiacrypt 2000, Lecture Notes in Computer Science, vol. 1976, Springer-Verlag, pp. 44-57, 2000.
10. D. A. Cox, J.B. Little and D. O'Shea. *Ideals, Varieties, and algorithms: an Introduction to Computational Algebraic Geometry and Commutative algebra.* Undergraduate Texts in Mathematics. Springer-Verlag. New York, 1992.
11. J.-C. Faugère. *A New Efficient Algorithm for Computing Gröbner Basis: F_4.* Journal of Pure and Applied Algebra, vol. 139, pp. 61–68, 1999.
12. J.-C. Faugère. *A New Efficient Algorithm for Computing Gröbner Basis without Reduction to Zero: F_5.* Proceedings of ISSAC, pp. 75–83. ACM press, July 2002.
13. J.-C. Faugère and P. Gianni and D. Lazard and T. Mora. Efficient Computation of Zero-Dimensional Gröbner Basis by Change of Ordering. *Journal of Symbolic Computation*, 16(4):329–344, October 1993.
14. J.-C. Faugère, and A. Joux. *Algebraic Cryptanalysis of Hidden Field Equations (HFE) Cryptosystems using Gröbner Bases.* Advances in Cryptology - CRYPTO 2003, Lecture Notes in Computer Science, vol. 2729, Springer-Verlag, pp. 44–60, 2003.
15. J.-C. Faugère, and L. Perret. *Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects.* Advances in Cryptology – EUROCRYPT 2006, Lecture Notes in Computer Science, vol. 4004, pp. 30–47, 2006.
16. P.-A. Fouque, G. Macario-Rat, and J. Stern. *Key Recovery on Hidden Monomial Multivariate Schemes.* Advances in Cryptology – EUROCRYPT 2008, Lecture Notes in Computer Science, vol. 4965, pp. 19-30, 2008.
17. M. R. Garey, and D. B. Johnson. *Computers and Intractability. A Guide to the Theory of NP-Completeness.* W. H. Freeman, 1979.
18. X. Jiang, J. Ding and L. Hu. *Kipnis-Shamir's Attack on HFE Revisited.* Proc. of Inscrypt 2007, *available at http://eprint.iacr.org/2007/203.*

19. A. Kipnis and A. Shamir. *Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization.* Advances in Cryptology – CRYPTO 99, Lecture Notes in Computer Science, vol. 1666, Springer-Verlag, pp. 19-30, 1999.
20. T. Li, Z. Lin and F. Bai *Heuristic Methods for Computing the Minimal Multi-homogeneous Bézout Number* Applied Mathematics and Computation 146, pp. 237-256, 2003.
21. G. Malajovich and K. Meer. *Computing Minimal Multi-homogeneous Bézout Numbers Is Hard.* Proceedings of STACS 2005, LNCS 3404, pp. 244-255, 2005.
22. T. Moh. *A Public Key System with Signature and Master Key Functions.* Communications in Algebra, vol. 27, No.5, pp. 2207-2222, 1999.
23. J. Patarin. *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms.* Advances in Cryptology – EUROCRYPT 1996, Lecture Notes in Computer Science, vol. 1070, Springer–Verlag, pp. 33–48, 1996.
24. M. Safey El Din, and P. Trébuchet. *Strong bi-homogeneous Bezout theorem and its use in effective real algebraic geometry.* INRIA Research Report RR, 46 pages, 2006. Preliminary version is available at *http://hal.inria.fr/inria-00105204*
25. I.R. Shafarevich. *B*asic Algebraic Geometry. Springer Study Edition, Springer-Verlag, Berlin (1977).
26. J.O. Shallit, G.S. Frandsen, and J.F. Buss. *The Computational Complexity of some Problems of Linear Algebra*. BRICS series report, Aarhus, Denmark, RS-96-33. (also at http://www.brics.dk/RS/96/33).
27. H. T. Ha and A. Van Tuyl. *The regularity of points in multi-projective spaces.* Journal of Pure and Applied Algebra, Volume 187, Issues 1-3, 1 March 2004, Pages 153-167.