Kipnis-Shamir Attack on HFE Revisited

Xin Jiang[1], Jintai Ding[2], and Lei Hu[1]

[1] State Key Lab of Information Security, Chinese Academy of Sciences, Beijing, China
{xjiang,hu}@is.ac.cn
[2] University of Cincinnati, USA
and
Technical University of Darmstadt, Germany
ding@math.uc.edu

Abstract. In this paper, we show the claims in the original Kipnis-Shamir attack on the HFE cryptosystems and the improved attack by Courtois that the complexity of the attacks is polynomial in terms of the number of variables are invalid. We present computer experiments and a theoretical argument using basic algebraic geometry to explain why it is so. Furthermore we show that even with the help of the powerful new Gröbner basis algorithm like F_4, the Kipnis-Shamir attack still should be exponential but not polynomial. This again is supported by our theoretical argument.

Keywords: HFE, MinRank, XL algorithm, relinearization, Gröbner basis, multivariate public key cryptosystem.

1 Introduction

The family of multivariate public key cryptosystems [19,5] is considered as one of the main candidates that have the potential to resist the future quantum computer attacks. One of the major research topics in this area is the HFE family of cryptosystems. The HFE encryption systems were presented by Jacques Patarin at Eurocrypt'96 [15], where the fundamental idea is very similar to that of Matsumoto and Imai [14], namely one first builds some polynomial system on a large field and then transforms it into a polynomial system over a vector space of a much smaller field. The first attack on HFE was presented by Kipnis and Shamir [12], where they lifted the public key back to the large field and attacked the system via a so-called MinRank problem [3]. This attack was further improved by Courtois [2] using different methods to solve the associated MinRank problem. The conclusion of these attacks is that to find the secret key and break the HFE cryptosystem is not exponential but polynomial in terms of the number of variables n once one fixes the key parameter D of HFE (or more precisely, $log(D)$). Later it was shown that if one uses new Gröbner basis methods to attack the HFE directly, it should be again not exponential but polynomial [9,11], in particular, Faugère broke one of the challenges set by Patarin. The overall conclusion seems to be that the HFE family itself is over.

Dingyi Pei et al. (Eds.): Inscrypt 2007, LNCS 4990, pp. 399–411, 2008.

However, there are still HFE variants, which we consider viable for practical applications [16,6], and resistant to the Gröbner basis attacks. The possibility of extension of Kipnis-Shamir attack seems to be quite appealing as in the case of the attack on HFEv in [6]. Therefore it seems to be a good idea to do a complete study of the original Kipnis, Shamir, and Courtois work including complete computer experiments to verify the claims and to derive a good estimate on the complexity in terms of practical attacks. To our surprise, our experiments show that the claims made by Kipnis, Shamir, and Courtois are actually invalid in the sense that the timing is far beyond what is expected. This made us to think what happened and we presented a theoretical explanation why this happens using some basic theoretical tools in algebraic geometry. Furthermore, we apply the new Gröbner basis method of Faugère by using the Magma implementations to this problem. Though the performance is clearly much better than the previous methods, it still confirms that the original Kipnis-Shamir attack is not polynomial rather it should be exponential.

The paper is arranged as follows. First we will briefly describe the original Kipnis-Shamir attack and the improvement of Courtois. Then in the next section, we will show that through experiments, the complexity of the attacks of Kipnis-Shamir are not as claimed. We present a theoretical argument why the claims of Kipnis, Shamir, and Courtois are not valid. In the next section, we will show via computer experiments using the Magma implementation of the new Gröbner basis F_4 that if we use the new Gröbner basis algorithm to improve the attack, the timing should be exponential and not polynomial. Then we will present our conclusion.

2 Kipnis-Shamir Attack on the HFE Scheme

2.1 The HFE Scheme

The HFE encryption scheme uses two finite fields. We denote the small field with q elements as $\mathbf{F}$, and $\mathbf{K}$ as its extension field of degree n over $\mathbf{F}$. A recommended choice for HFE is $q = 2$ and $n = 128$. Given a basis of $\mathbf{K}$ over $\mathbf{F}$, we can identity $\mathbf{K}$ with an n-dimensional vector space over $\mathbf{F}$ by $\varphi : \mathbf{K} \to \mathbf{F}^n$ and its inverse φ^{-1}. The design of HFE is based on a univariate polynomial $P(x)$ over $\mathbf{K}$ of the form

$$P(x) = \sum_{i=0}^{r-1} \sum_{j=0}^{r-1} p_{ij} x^{q^i+q^j}, \tag{1}$$

where the coefficients p_{ij} are randomly chosen from $\mathbf{K}$ and r is much smaller than n so that the degree of $P(x)$ is less than some fixed parameter D. (Here for simplification reason we consider only the case of $P(x)$ being a homogeneous polynomial.) The limitation on the degree D of $P(x)$ is required to make it possible to invert $P(x)$ efficiently at decryption.

Let

$$G(x) = \varphi^{-1} \circ T \circ \varphi \circ P \circ \varphi^{-1} \circ S \circ \varphi(x), \tag{2}$$

where T and S are two randomly chosen invertible linear transformations on $\mathbf{F}^n$, and they are part of the private key of the HFE scheme together with polynomial $P(x)$. The public key is $\varphi \circ G \circ \varphi^{-1}$, which are n homogeneous quadratic polynomials in n variables on $\mathbf{F}$.

2.2 Kipnis-Shamir Attack

The attack of Kipnis and Shamir on HFE scheme in [12] is done over the big field $\mathbf{K}$. They proved that the linear transformations S and T when lifted to the big field $\mathbf{K}$ have the form

$$S(x) = \sum_{i=0}^{n-1} s_i x^{q^i},\ T^{-1}(x) = \sum_{i=0}^{n-1} t_i x^{q^i}, \tag{3}$$

where $s_i, t_i \in \mathbf{K}$. It simplifies the expression of public key polynomial $G(x)$ to $G(x) = T(P(S(x)))$ using the univariate polynomial form over the big field, which also gives the expression $T^{-1}(G(x)) = P(S(x))$. They rewrote the public key polynomial as a matrix form:

$$G(x) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} g_{ij} x^{q^i+q^j} = \underline{x} G \underline{x}^t, \tag{4}$$

where $G = [g_{ij}]$ is a matrix over $\mathbf{K}$, and $\underline{x} = (x^{q^0}, x^{q^1}, \cdots, x^{q^{n-1}})$ is the vector over $\mathbf{K}$, and $\underline{x}^t$ is its transpose, and this implies that

$$T^{-1}(G(x)) = \sum_{k=0}^{n-1} t_k \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} (g_{i-k,j-k})^{q^k} x^{q^i+q^j}, \tag{5}$$

and

$$P(S(x)) = \underline{x} W P W^t \underline{x}^t, \tag{6}$$

where we use the same notation P to denote a matrix $[p_{ij}]$, W is a specified matrix with its (i,j)-entry $W_{ij} = s_{j-i}^{q^i}$. (Here and henceforth the subscripts are computed modulo n.)

Let G^{*k} be the matrix derived from G by raising all entries of G to the q^k-th power and cyclically rotating all rows and columns of G forwards by k steps. Then $T^{-1}(G(x)) = \underline{x} G' \underline{x}^t$, where

$$G' = \sum_{k=0}^{n-1} t_k G^{*k} = W P W^t. \tag{7}$$

It is not hard to show that both ranks of matrices P and WPW^t do not exceed r, where $r \ll n$ and are roughly $log(D)$. Kipnis and Shamir found that if one made a correct choice for the values of $t_0, t_1, \cdots, t_{n-1}$, then the rank of G' would not be more than r; otherwise for a random choice of values the expected rank

would be close to n. The difference between the correct and random choices is clear, and below is a specific method to recovering $(t_0, t_1, \cdots, t_{n-1})$. Surely here in terms of explicit form of the matrix, we need to use the symmetric form of the matrix and in the case of characteristic 2, the diagonal entries shall all be 0.

The matrix G can be easily obtained from the public key of the HFE scheme, then all G^{*k} can be computed. Take $t_0, t_1, \cdots, t_{n-1}$ as n variables. The matrix $G^{'}$ can be represented by G^{*k} and $(t_0, t_1, \cdots, t_{n-1})$. Since its rank does not exceed r, its left kernel, defined as $\{\underline{x} : \underline{x}G' = 0\}$, is an (at least) $n - r$ dimensional vector subspace, and there are $n - r$ independent n-dimensional vectors $\widetilde{x}_1, \cdots, \widetilde{x}_{n-r}$ such that in the kernel. Assigning random values for these vectors in their first $n-r$ entries and taking new variables for each of the remaining r entries, one adds $r(n - r)$ new variables. Each $\widetilde{x}_i G^{'} = 0$ brings n scalar equations over $\mathbf{K}$, a total of $(n - r)n$ equations can be obtained in $n + r(n - r)$ variables $(t_0, t_1, \cdots, t_{n-1}$ and $r(n - r)$ new variables).

These equations are quadratic and form an over-defined system of about n^2 equations in about rn variables where $r \ll n$. In their attack Kipnis and Shamir propose to solve it by relinearization technique. Surely, if they had solved this over-defined system and derived the values of $t_0, t_1, \cdots, t_{n-1}$, it was easy to recover T^{-1} and T, and there is also a specific way to recover S by solving linear over-defined equations over $\mathbf{F}$. Therefore the crucial point of the attack is to recover the transformations T^{-1} and T. The later developed XL algorithm is an improved algorithm over the relinearization method.

Later Courtois pointed out that the point of the attack of Kipnis and Shamir can be viewed as a MinRank problem and he proposed some further improvement on how to find T using some of known methods for the MinRank problem.

3 Can Kipnis-Shamir Attack and Courtois' MinRank Attack Really Work?

Now we would like to do a careful analysis in theory under what condition that the Kipnis-Shamir attack will work.

3.1 Another Look at the Kipnis-Shamir Attack

If we look at the relinearization method, we know immediately that in order for it to work, the equations must satisfy the condition that the solution is actually unique because we expect to find the solution via solving a set of nondegenrate linear equations.

Originally, the part T of the private key of HFE scheme is fixed and its corresponding form, of which the coefficients are $(t_0, t_1, \cdots, t_{n-1})$, in the big field is unique too. Unfortunately, we have equivalent keys.

First, the solutions to our problem is not unique, because if $(a_0, a_1, \cdots, a_{n-1})$ is a solution for $(t_0, t_1, \cdots, t_{n-1})$, then $u(a_0, a_1, \cdots, a_{n-1})$ is still a solution for any constant u. This problem can be easily solved by fixing one variable, say t_0, to be 1. Furthermore, if r is even, we need to fix two variables, because

any symmetric matrix over characteristic 2 with 0 diagonal entries of odd size is degenerate. This implies if r is even, if $(a_0, a_1, \cdots, a_{n-1})$ is a solution, then $u(a_0, a_1, \cdots, a_{n-1}) + v(a_{n-1}^q, a_0^q, \cdots, a_{n-2}^q)$ is also a solution.

Then we realize that this is not enough. If $(a_0, a_1, \cdots, a_{n-1})$ is a solution of $(t_0, t_1, \cdots, t_{n-1})$, it is easy to see that $(a_{n-1}^q, a_0^q, \cdots, a_{n-2}^q)$ is also a solution, and furthermore $(a_{n-i}^{q^i}, a_{n-i+1}^{q^i}, \cdots, a_{n-i-1}^{q^i})$ is also a solution for any i from 2 to $n-1$. This is due to the fact that we only use the condition that the rank of $G^{'}$ can not exceed r in Kipnis-Shamir attack not how it looks like, and the fact that raising the q-th powering of the entries of a matrix and rotating its rows and columns accordingly do not change the rank.

This can also be stated as follows.

Proposition 1. *Let the notation $G, T, P, S, G^{'}, G^{*k}$, and W be as defined before; Let $(a_0, a_1, \cdots, a_{n-1})$ be a solution of $(t_0, t_1, \cdots, t_{n-1})$, and the rank of matrix $G^{'} = \sum_{k=0}^{n-1} a_k G^{*k}$ does not exceed r. Given $(\alpha_0^l, \alpha_1^l, \cdots, \alpha_{n-1}^l) = (a_{n-l}^{q^l}, a_{n-l+1}^{q^l}, \cdots, a_{n-l-1}^{q^l})$, the rank of matrix $G^{'l} = \sum_{k=0}^{n-1} \alpha_k^l G^{*k}$ does not exceed r as well, and $G^{'l}$ and $G^{'}$ are actually of the same rank.*

Proof. From Section 2.2, we raise the both sides of equations (5) and (6) to q^l-th powering, and for each $0 \leq l \leq n-1$, we have

$$(T^{-1}(G(x)))^{q^l} = \sum_{k=0}^{n-1} a_k^{q^l} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (g_{i-l-k, j-l-k})^{q^{k+l}} x^{q^i + q^j}, \tag{8}$$

and

$$(P(S(x)))^{q^l} = \underline{x} W^{'} P^{(l)} W^{'t} \underline{x}^t, \tag{9}$$

where $P^{(l)}$ is derived from P by $P_{ij}^{(l)} = P_{i-l,j-l}^{q^l}$, $W^{'}$ is generated from W with that $W_{ij}^{'} = W_{i-l,j-l}^{q^l}$. Therefore, the rank of matrix $W^{'} P^{(l)} W^{'t}$ cannot exceed r as $P^{(l)}$ contains at most r nonzero rows. Equations (5) and (6) are identical, hence (8) and (9) are identical too. Then we have

$$G^{'l} = \sum_{k=0}^{n-1} a_k^{q^l} G^{*(k+l)} = W^{'} P^{(l)} W^{'t}. \tag{10}$$

Substitute k by $k+l$, we get that

$$G^{'l} = \sum_{k=0}^{n-1} a_{k-l}^{q^l} G^{*k} = \sum_{k=0}^{n-1} \alpha_k^l G^{*k}. \tag{11}$$

Obviously, the rank of $G^{'l}$ is the same as that of $P^{(l)}$ and does not exceed r, and $(a_{n-l}^{q^l}, a_{n-l+1}^{q^l}, \cdots, a_{n-l-1}^{q^l})$ is a solution. □

The above proposition states that each solution $(a_0, a_1, \cdots, a_{n-1})$ for $(t_0, t_1, \cdots, t_{n-1})$ is accompanied by $n-1$ additional solutions $(a_{n-l}^{q^l}, a_{n-l+1}^{q^l}, \cdots, a_{n-l-1}^{q^l})$, $1 \leq l \leq n-1$. These solutions are usually different. More precisely, we have the following.

Proposition 2. *Let T be a randomly chosen linear transformation over $\mathbf{F}^n$, and $(a_0, a_1, \cdots, a_{n-1})$ be a solution corresponding to T. Set $(\alpha_0^l, \alpha_1^l, \cdots, \alpha_{n-1}^l) = (a_{n-l}^{q^l}, a_{n-l+1}^{q^l}, \cdots, a_{n-l-1}^{q^l})$, $0 \leq l \leq n-1$. Then*

$$Prob(\alpha_i^j = \alpha_i^k : j \neq k, 0 \leq i, j, k \leq n-1) \leq \mathcal{O}(n^2 q^{-n}).$$

Proof. Since T is a randomly chosen linear transformation over $\mathbf{F}^n$, $(a_0, a_1, \cdots, a_{n-1})$ is a random vector with entries chosen from $\mathbf{K} = GF(q^n)$. By the birthday paradox, we have

$$Prob(a_i = a_j^{q^l} : j \neq i, 0 \leq i, j, l \leq n-1) \leq 1 - (1 - nq^{-n})^n. \tag{12}$$

Since

$$1 - (1 - nq^{-n})^n \leq \mathcal{O}(n^2 q^{-n}), \tag{13}$$

we have

$$\begin{aligned} & Prob(\alpha_i^j = \alpha_i^k : j \neq k, 0 \leq i, j, k \leq n-1) \\ = \; & Prob(a_i = a_j^{q^l} : j \neq i, 0 \leq i, j, l \leq n-1) \\ \leq \; & \mathcal{O}(n^2 q^{-n}) \end{aligned} \tag{14}$$

□

This means even if we fix one variable like t_0 to be 1 or two variables if r is even, we still expect that there should be at least n different solutions. Therefore, we can conclude that mostly each variable of the over-defined $(n-r)n$ quadratic equations system in $n+r(n-r)$ variables from Kipnis-Shamir attack has at least about n different solutions. This reminds us the case of the famous challenges of cyclic equations [22].

It is now clear that for this kind of equation system we can not find the solutions by relinearization technique [12]. Then one may ask how about the XL algorithm [13], which is the improved relinearization algorithm. We will argue that for this kind of equation system we can not find the solutions by XL algorithm easily as well.

The key point is the observation that to any system of multivariate polynomial equations, if one variable has d different solutions, we should not be able to solve this system directly by the XL algorithm with the maximum degree of this variable arisen in terms lower than d.

Proposition 3. *Let $P_0(x_0, \cdots, x_{n-1}) = 0, \cdots, P_{m-1}(x_0, \cdots, x_{n-1}) = 0$ be any set of m multivariate polynomial equations in n variables over $\mathbf{K}$; for each x_i, $0 \leq i \leq n-1$, if x_i has d different solutions $\beta_0, \cdots, \beta_{d-1}$ in $\mathbf{K}$, we can not determine the values of x_i directly from the equations generated by the XL algorithm with the maximum degree of this variable arisen in terms lower than d.*

Proof. We can prove it by contradiction. Suppose we get the exact d values of x_i by the equations generated by the XL algorithm with the maximum degree of this variable arisen and noted as $d^{'}$, and $d^{'} < d$. To get the exact values of x_i, the last step of the XL algorithm is linearization to get a univariate polynomial equation just with one variable x_i. While, we all know that the degree of univariate polynomial equation must be at most $d^{'}$ and lower than d. The contradiction is that we can not get d different values $\beta_0, \cdots, \beta_{d-1}$ of x_i by solving a univariate polynomial equation with the degree lower than d. □

The first proposition in this section shows that each variable of the quadratic equations system generated by Kipnis-Shamir attack has at least n solutions; the second proposition in this section supposes that for each variable, we expect to have n different solutions in general; and this proposition shows that if we want to get the solutions of $(t_0, t_1, \cdots, t_{n-1})$ by XL algorithm, we must raise the degree of monomials at least to n in the solving process. This is quite different from what Kipnis and Shamir claimed which should be $log(D)$, which has nothing to do with n. This means the complexity of the attack should be more than what was claimed.

The statements above can be reexplained in terminology of algebraic geometry. Let V be the algebraic variety of the quadratic equations derived from the Kipnis-Shamir attack, and σ be the action of first q-th powering every component of an n-dimensional vector and then cyclically rotating all components right by one. Then V is invariant under the action of the order n cyclic group generated by σ. This variety must contain at least n distinct points (Proposition 2), and the univariate polynomial over $\mathbf{K}$ representing the variety is then of degree n.

We will confirm this with our computer experiment. Furthermore, in our experiment, we have given a toy example that even if we raise the degree of monomials by the XL algorithm to n or even larger than n, we still can not find the solutions.

3.2 What about Courtois' MinRank Attack?

Courtois tried to improve the Kipnis-Shamir attack for basic HFE [2]. From the matrix $G^{'}$ above, instead of by relinearization, he proposed to solve it by MinRank attack directly [3]. Taken $(t_0, t_1, \cdots, t_{n-1})$ as variables, he suggested that we could derive a set of equations from the fact that every $(r+1) \times (r+1)$ submatrix of $G^{'}$ has determinant 0. Therefore, there are $\binom{n}{r+1}^2$ equations with about $\binom{n}{r+1}$ monomials, and it is expected that there are more than $\binom{n}{r+1}$ equations linearly independent so that this equation system can be solved by Gaussian reduction.

However, $(t_0, t_1, \cdots, t_{n-1})$ has at least about n solutions because this MinRank attack does also use the fact that the rank of $G^{'}$ can not exceed r as in Kipnis-Shamir attack, and in the equations of MinRank attack, the degree of monomials is not larger than $r+1$. For $r+1 \ll n$, we can not solve this system by Gaussian reduction from Proposition 3, and we need to go up to degree n to find the solutions.

4 Computer Experiments

We have programmed some experiments of Kipnis-Shamir attack and MinRank attack by Magma V2.11 on a Pentium IV 2.9GHz PC with 512M memory. Our experiments works on the simplest case, where r is 2. From the theoretical argument above, we can fix the variable $t_0 = 1 \in \mathbf{K}$ to decrease the number of solutions, and also we can fix one new variable to 1 when we simulate Kipnis-Shamir attack because $r = 2$ is even. Surely, we also have the experiments without fixing any variable, and they behave essentially in the same way.

4.1 Experiment on Kipnis-Shamir Attack

We choose $q = 2$, $n \in \{5, 6, \cdots, 12\}$, $r = 2$, so $\mathbf{F} = GF(2)$ and $\mathbf{K} = GF(2^n)$; choose $P(x) = ax^3$ and two random invertible linear transformations T and S, where $a \neq 0$ is randomly chosen from $\mathbf{K}$. Following the description in Section 2.2, we derive the quadratic equation system and then try to solve it. In [12] Kipnis and Shamir intended to solve this system by the relinearization technique, while we just use the XL algorithm to simulate it. For each n, select the degree of the parameter [20] needed for the XL algorithm to be $D = 4$ and record the result of experiments in Table 1.

Table 1. Experiment of Kipnis-Shamir Attack with $r = 2$, $D = 4$, and $n \in \{5, 6, \cdots, 12\}$

	$n=5$	$n=6$	$n=7$	$n=8$	$n=9$	$n=10$	$n=11$	$n=12$
equations $n(n-r)$	15	24	35	48	63	80	99	120
variables $r(n-r)+n-2$	9	12	15	18	21	24	27	30
monomials of degree $\leq D$	715	1820	3876	7315	12650	20475	31465	46376
monomials not emergence	105	280	621	1211	2150	3555	5560	8316
number of XL monomials	610	1540	3255	6104	13995	16920	25905	38060
number of XL equations	825	2184	4760	9120	10500	26000	40194	59520
rank of the matrix	556	1408	2983	5605	9658	15586	23893	35143

As the same for each $n \in \{5, 6, 7, 8\}$, select the parameter $D = 5$ and record the experimental result in Table 2.

Table 2. Experiment of Kipnis-Shamir Attack with $r = 2$, $D = 5$, and $n \in \{5, 6, 7, 8\}$

	$n=5$	$n=6$	$n=7$	$n=8$
equations $n(n-r)$	15	24	35	48
variables $r(n-r)+n-2$	9	12	15	18
monomials of degree $\leq D$	2002	6188	15504	33649
monomials not emergence	182	588	1539	3465
number of XL monomials	1820	5600	13965	30184
number of XL equations	3300	10920	28560	63840
rank of the matrix	1738	5363	13403	29020

In both tables, line 4 is the number of the monomials of degree $\leq D$ in $r(n-r)+n-2$ variables. For not all these monomials would appear in the equations in the XL computation, line 5 is the number of these not emerging in the equations; line 6 is the difference of line 4 and line 5, and it is the number of the monomials of those equations; line 7 is the number of equations. For the data of line 7 is larger than that of line 6, we try to solve this system by Gaussian reduction as linearization technique. However, it does not work even though the XL equations are much more than the XL monomials. Then we get the rank of matrix recorded in line 8, which is formed by that each equation as a row and each monomial as a column. In both tables, each number of line 8 is smaller than what is needed to solve the equations, and we are unable to recover the variables $t_0, t_1, \cdots, t_{n-1}$.

4.2 Toy Example of How the XL Algorithm Terminates

In Section 4.1, we have showed that when $D = 4$ or 5 and $n \in \{5, 6, \cdots, 12\}$, XL can not terminate because we can not solve the equations system directly by Gaussian reduction. Therefore, here we fix $n = 5$ and keep all other parameters as before, except that $D \in \{4, 5, 6, 7\}$. Well, $n(n-r)=15$ equations and $r(n-r)+n-2=9$ variables of the generated quadratic equation system are invariable as n and r fixed. The result of experiment is recorded in Table 3.

Table 3. Experiment of Increasing D for Solving Equations by XL

	$D=4$	$D=5$	$D=6$	$D=7$
monomials of degree $\leq D$	715	2002	5005	11440
monomials not emergence	105	182	294	450
number of monomials	610	1820	4711	10990
number of equations	825	3300	10725	30030
rank of the matrix	556	1738	4595	10834
difference of lines 4 and 6	54	82	116	156

From this table, we find that the difference between the number of monomials and rank of the matrix is increasing by the growth of D. We can not solve the original equation system when increasing the parameter D of XL algorithm only by a few degrees.

4.3 Experiment of MinRank Attack

Similarly as the previous subsection, we choose $q = 2$, $n \in \{5, 6, \cdots, 10\}$; choose two kinds of public key polynomials: $r = 2$ and $P(x) = ax^3$, and $r = 3$ and $P(x) = ax^3 + bx^5 + cx^6$, where a, b, and c are random elements chosen from $\mathbf{K}$, respectively; choose two random invertible linear transformations T and S.

When $P(x) = ax^3$. Here we can fix two variables. There are $\binom{n}{r+1}^2$ equations with $\binom{n-1}{3} + (n-2)(n-1) + (n-1)$ monomials in $n-2$ variables. We try

Table 4. Simulation of MinRank Attack of $r = 2$ and $P(x) = ax^3$

	$n = 5$	$n = 6$	$n = 7$	$n = 8$	$n = 9$	$n = 10$
monomials of degree $\leq r + 1$	20	35	56	84	120	165
rank of the matrix	15	29	49	76	111	155
difference of above two lines	5	6	7	8	9	10

Table 5. Experiment of MinRank Attack of $r = 3$ and $P(x) = ax^3 + bx^5 + cx^6$

	$n = 6$	$n = 7$	$n = 8$	$n = 9$
monomials of degree $\leq r + 1$	126	210	330	495
rank of the matrix	90	161	266	414
difference of above two lines	36	49	64	81

to solve the equation system by Gaussian reduction, and we also find that it is impossible to be solved. Then we record the rank of the matrix, which is formed as above, in Table 4.

When $P(x) = ax^3 + bx^5 + cx^6$. Here $r = 3$, so we can fix one variable, and we choose $n \in \{6, 7, 8, 9\}$. As the same as before, we can not solve this equation system of $\binom{n}{r+1}^2$ equations with $\binom{n}{4} + n\binom{n-1}{2} + n(n-1) + \binom{n}{2} + n$ monomials in $n - 1$ variables. Then we record the rank of the matrix generated from the equation system in Table 5.

We can observe from Tables 4 and 5 that the difference between the number of monomials of degree $r + 1$ and the rank of the matrix is equal to or larger than n and very regular. Therefore, we can conclude that MinRank attack is unsuccessful to recover the secret $t_0, t_1, \cdots, t_{n-1}$.

4.4 Experiment of Solving Equations by F_4

From [18], it is true that XL acts as a redundant version of the F_4 algorithm. Currently it is commonly recognized that the new Gröbner basis algorithm F_4 [7] and F_5 [8] are the most powerful tools to solve polynomial equations [17,21]. Because F_4 is the only one which is publicly available, which is implemented in Magma, to further understand the quadratic equation system generated by the Kipnis-Shamir attack, we should use the Magma implementation of the new Gröbner basis F_4 to test if finding the solutions are indeed still polynomial.

Because of our degree argument, we do not expect Magma to run up to degree n and therefore we expect the complexity to grow up very fast. This time, we run the experiments by Magma V2.13 on a 2.6GHz AMD 64 computer in TU Darmstadt.

In the same way as above, we choose $q = 2$ and $r = 2$. We fix two variables to reduce the number of solutions and then we use Magma to try to find the Gröbner basis of this system. The experiments as expected produce the full triangular Gröbner basis is in lex order, and we get precisely n solutions from

Table 6. Experiment of Solving Equations by F_4

	$n=10$	$n=11$	$n=12$	$n=13$	$n=14$	$n=15$	$n=16$	$n=17$	$n=18$
time (seconds)	0.1	0.16	0.3	0.51	0.9	1.5	2.5	4	6.7
memory (megabit)	8.2	9.1	10	11.4	12.6	15	17	22	32.3
	$n=19$	$n=20$	$n=21$	$n=22$	$n=23$	$n=24$	$n=25$	$n=26$	$n=27$
time (seconds)	10.8	16.3	32.7	50.5	63	91.7	121.5	171.4	218
memory (megabit)	36	48	58	85	75.9	122	145	136.4	203

the Gröbner basis. Meanwhile, our program also verifies that they are indeed the solutions. Therefore, it supports our theoretical argument.

Table 6 below gives the running time and required memory of each n specifically. In Figure 1, we use logarithmic coordinate and take n as X-coordinate and running time and required memory as Y-coordinate respectively. It clearly shows the growing tendency when increasing n. Though the timing and memory data is smaller than what we expected, but for computing Gröbner basis when increasing the degree n, the timing, we still conclude, should be exponential and not polynomial. The reason that the timing and the memory is far less than what we expect is that the degree of the final Gröbner basis is indeed n. Also we want to emphasize that our result is just the simplest and the easiest case of the HFE family.

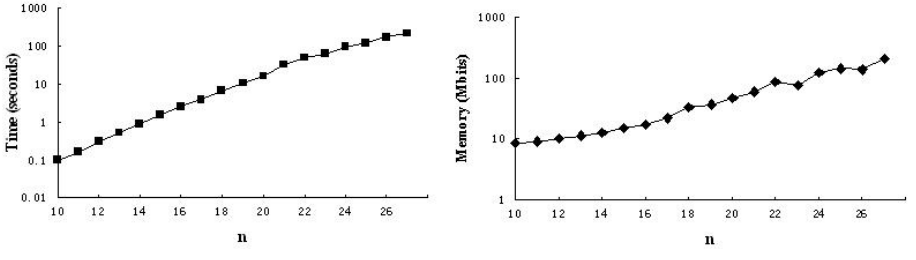

Fig. 1. Running Time and Required Memory

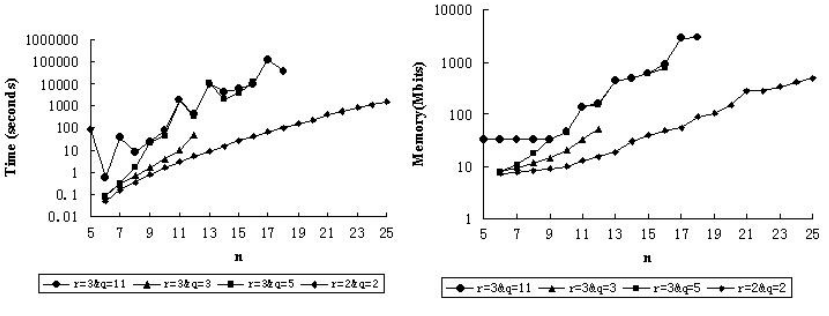

Fig. 2. Running Time and Required Memory Between Different q and r

We did some more experiments by increasing r to 3 or choosing different small field $\mathbf{F}$ as $q = 3, 5, 11$, and the result is compared by Figure 2. It shows that in this situation the equations are much more difficult to solve. This means that this set of systems of highly over-defined equations have much more structures that we still do not understand and much more theoretical and experimental work are still needed to understand fully the complexity behavior.

5 Conclusion

We revisited the original Kipnis-Shamir attack on the HFE cryptosystems. We show in theory and experiments that the original Kipnis-Shamir attack on the HFE cryptosystems and the improved attack by Courtois can not work as efficiently as claimed. Furthermore, we showed that even by the new Gröbner basis algorithm F_4, the complexity of the attack should be exponential and not polynomial, though the performance of F_4 is clearly far better than the XL algorithm and more work is still needed to understand what is really going on. The key point of our theoretical argument is based on the simple idea that when solving a polynomial equation system, the degree parameter of the XL or similar algorithm is lower bounded by the number of solutions.

Acknowledgment. The authors would like to thank the anonymous referees for their helpful suggestions. The work of the second author was partially supported by the Charles Phelps Taft Research Center and the Alexander von Humboldt Foundation. The third author was supported by the by NSFC (60573053) and National 863 Project of China (2006AA01Z416).

References

1. Bardet, M., Faugère, J.-C., Salvy, B.: On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In: Proceedings of the International Conference on Polynomial System Solving, pp. 71–74 (2004) Previously appeared as INRIA report RR-5049.
2. Courtois, N.T.: The Security of Hidden Field Equations (HFE). In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, Springer, Heidelberg (2001)
3. Courtois, N.T.: The Minrank Problem. MinRank, a new Zero-knowledge scheme based on the NP-complete problem. Presented at the rump session of Crypto (2000), available at: `http://www.minrank.org`
4. Courtois, N., Klimov, A., Patarin, J., Shamir, A.: Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 392–407. Springer, Heidelberg (2000)
5. Ding, J., Gower, J., Schmidt, D.: Multivariate Public-Key Cryptosystems. In: Advances in Information Security, Springer, Heidelberg (2006)
6. Ding, J., Schmidt, D.S.: Cryptanalysis of HFEV and Internal Perturbation of HFE. In: Vaudenay, S. (ed.) PKC 2005. LNCS, vol. 3386, pp. 288–301. Springer, Heidelberg (2005)
7. Faugère, J.-C.: A New Efficient Algorithm for Computing Gröbner Bases (F_4). Journal of Plure and Applied Algebra 139, 61–88 (1999)

8. Faugère, J.-C.: A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero(F_5). In: Mora, T. (ed.) Proceeding of ISSAC, pp. 75–83. ACM Press, New York (2002)
9. Faugère, J.-C.: Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 44–60. Springer, Heidelberg (2003)
10. Garey, M.R., Johnson, D.S.: Computers and Intractability – A Guide to the Theory of NP-Completeness. W.H. Freeman and Company, New York (1979)
11. Granboulan, L., Joux, A., Stern, J.: Inverting HFE Is Quasipolynomial. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 345–356. Springer, Heidelberg (2006)
12. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, Springer, Heidelberg (1999)
13. Shamir, A., Patarin, J., Courtois, N., Klimov, A.: Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, Springer, Heidelberg (2000)
14. Matsumoto, T., Imai, H.: Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption. In: Günther, C.G. (ed.) EUROCRYPT 1988. LNCS, vol. 330, pp. 419–453. Springer, Heidelberg (1988)
15. Patarin, J.: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 33–48. Springer, Heidelberg (1996)
16. Patarin, J., Courtois, N., Goubin, L.: QUARTZ, 128-Bit Long Digital Signatures. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, Springer, Heidelberg (2001)
17. Diem, C.: The XL-Algorithm and a Conjecture from Commutative Algebra. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 323–337. Springer, Heidelberg (2004)
18. Imai, H., Sugita, M., Faugère, J.-C., Ars, G., Kawazoe, M.: Comparison Between XL and Gröbner Basis Algorithms. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 338–353. Springer, Heidelberg (2004)
19. Wolf, C., Preneel, B.:, Taxonomy of public key schemes based on the problem of multivariate quadratic equations. Cryptology ePrint Archive, Report 2005/077, 64 (12th of May, 2005), `http://eprint.iacr.org/2005/077/`
20. Yang, B.-Y., Chen, J.-M.: All in the XL Family: Theory and Practice. In: Park, C.-s., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 67–86. Springer, Heidelberg (2005)
21. Segers, A.J.M.: Algebraic Attacks from a Groebner Basis Perspective Master's Thesis, 10, 110 (2004)
`http://www.win.tue.nl/~bdeweger/ReportSegersGB2-11-04.pdf`
22. Björk, G.: Functions of modulus one on $\mathbf{Z}_p$ whose Fourier transforms have constant modulus. In: Proceedings of Alfred Haar Memorial Conference. Colloquia Mathematica Societatis Jnos Bolyai, Budapest, vol. 49 (1985)