Algebraic Attack on HFE Revisited

Jintai Ding[1], Dieter Schmidt[1], and Fabian Werner[2]

[1] University of Cincinnati
ding@math.uc.edu, dieter.schmidt@uc.edu
[2] Technical University of Darmstadt
fw@cccmz.de

Abstract. In this paper, we study how the algebraic attack on the HFE multivariate public key cryptosystem works if we build an HFE cryptosystem on a finite field whose characteristic is not two. Using some very basic algebraic geometry we argue that when the characteristic is not two the algebraic attack should not be polynomial in the range of the parameters which are used in practical applications. We further support our claims with extensive experiments using the Magma implementation of F_4, which is currently the best publicly available implementation of the Gröbner basis algorithm. We present a new variant of the HFE cryptosystems, where we project the public key of HFE to a space of one dimension lower. This protects the system from the Kipnis-Shamir attack and makes the decryption process avoid multiple candidates for the plaintext. We propose an example for a practical application on GF(11) and suggest a test challenge on GF(7).

Keywords: HFE, Gröbner basis, multivariate public key cryptosystem.

1 Introduction

The family of multivariate public key cryptosystems [16,4] is considered as one of the main candidates that have the potential to resist the future quantum computer attacks. MPKC's security relies on the fact that the direct attack, which we call the algebraic attack, needs to solve a set of multivariate quadratic equations, which is in general $\mathcal{NP}$-hard [8].

A major research topic in this area is the family of HFE cryptosystems. The HFE encryption systems were presented by Jacques Patarin at Eurocrypt'96 [15]. The fundamental idea is very similar to that of Matsumoto and Imai [13]. One selects a polynomial in 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 [11]. They lifted the public key back into the large field and attacked the system via a so-called MinRank [3] method. This attack was further improved by Courtois [2] using different ideas to solve the associated MinRank problem. The theoretical conclusion of these attacks is that, if one fixes the key parameter D of HFE (or more precisely $log(D)$) then the secret key can be found not in exponential but in polynomial time as the number

T.-C. Wu et al. (Eds.): ISC 2008, LNCS 5222, pp. 215–227, 2008.

n of variables increase. However these attacks were not fully substantiated by computer experiments.

Later on a direct attack on HFE with the new Gröbner basis methods like F_4 or F_5 did not show an exponential but a polynomial behavior [7,9]. Additionally, Faugère broke one of the challenges set by Patarin. This was later confirmed by Allen Steel with his Magma implementation of F_4 [12], whose performance is even better than the one used by Faugère. The overall conclusion seems to be that the HFE family of cryptosystems is not secure.

However, if we look more carefully at all current algebraic attacks, we see that all of them only deal with the case, where the finite field is exactly GF(2). A key point of these attacks is that the so called field equations

$$x_i^2 - x_i = 0, \qquad i = 1, \ldots, n$$

are used in the attack of the systems. If these field equations are not utilized, or more precisely could not be utilized efficiently, then the complexity of the algebraic attacks could be totally different. We first use some basic tools of algebraic geometry, including the idea of the so called solution at infinity [14], to argue that indeed the algebraic attacks should not work if the field equations are not fully utilized. We then support our claim by doing extensive experiments using the F_4 implementation in Magma, which is the best implementation that is publicly available.

The paper is arranged as follows. First we will briefly describe the HFE cryptosystem and the algebraic attacks. We then present a theoretical argument why the algebraic attack complexity will change if we do not utilize the field equations. In the next section we will show via computer experiments using the Magma implementation of the new Gröbner basis F_4 that the timing of the algebraic attack on simple cases of HFE should not be polynomial but should be exponential if we work on a field whose characteristic is not two. We will then present our challenge and give our conclusions.

2 The HFE Scheme

The HFE encryption scheme utilizes two finite fields. We denote the small field with q elements as $\mathbf{F}$, and $\mathbf{K}$ as the extension field of degree n over $\mathbf{F}$. Patarin recommended that the choice for HFE should be $q = 2$ and $n = 128$. Given a basis of $\mathbf{K}$ over $\mathbf{F}$, we can identify $\mathbf{K}$ 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

$$P(X) = \sum_{i=0}^{r-1} \sum_{j=i}^{r-1} p_{ij} X^{q^i + q^j} + \sum_{i=0}^{r_1} p_i X^{q^i} + p, \tag{1}$$

where the coefficients p_{ij}, p_i, p are randomly chosen from $\mathbf{K}$ and r, r_1 are small such that the degree of $P(X)$ is less than some fixed parameter D. The limitation

on the degree D of $P(X)$ is required so that it is possible to find the roots of $P(X)$ efficiently during the decryption, for example by using Berlekamp's algorithm.

Let

$$\bar{P}(x_1, \ldots, x_n) = T \circ \varphi \circ P \circ \varphi^{-1} \circ S(x_1, \ldots, x_n) \quad (2)$$

$$= (\bar{P}_1(x_1, \ldots, x_n), \ldots, \bar{P}_n(x_1, \ldots, x_n)), \quad (3)$$

where T and S are two randomly chosen invertible affine transformations on $\mathbf{F}^n$. The private key of the HFE scheme is formed by $P(X)$, S and T. The public key $\bar{P}(x_1, \ldots, x_n)$ consists of

$$\{\bar{P}_1(x_1, \ldots, x_n), \ldots, \bar{P}_n(x_1, \ldots, x_n)\},$$

which are n quadratic polynomials in the n variables in $\mathbf{F}$.

3 The Algebraic Attack

Let us assume that someone uses the HFE cryptosystem for encryption of a message or plaintext $(x'_1, \ldots, x'_n)$. What he or she does is to compute

$$(y'_1, \ldots, y'_n) = \bar{P}(x'_1, \ldots, x'_n),$$

the ciphertext, and sends it to the owner of the public key.

In order to attack HFE or any multivariate public key cryptosystem, an attacker has already the public key $\bar{P}$ and he or she also has access to the ciphertext $(y'_1, \ldots, y'_n)$. This means that if the attacker can solve the equation

$$\bar{P}(x_1, \ldots, x_n) = (y'_1, \ldots, y'_n),$$

the solution will give the attacker the plaintext $(x'_1, \ldots, x'_n)$ and he or she breaks the cryptosystem. Solving the set of equations above directly is called the algebraic attack.

The Gröbner basis method [1] is the classical method of solving multivariate polynomial equations. However, it is very slow in general. Recently major improvements have been made by Faugère [5,6] with his F_4 and F_5 algorithms. We will not give the details of the algorithms and refer the reader to the references instead.

Let us assume that we need to solve the set of equations

$$f_1(x_1, \ldots, x_n) = \cdots = f_n(x_1, \ldots, x_n) = 0,$$

over any field. When the solutions of this set of equations has dimension 0, or more precisely, when the system has only finitely many solutions (including the solutions over the extension field of the field we work on), the Gröbner basis algorithm finds a set of polynomials of the form

$$\{g_1(x_1, \ldots, x_n), g_2(x_2, \ldots, x_n), g_3(x_3, \ldots, x_n), \ldots, g_n(x_n)\}$$

such that the set of polynomials g_i and the set of polynomials f_i generate exactly the same ideal in the polynomial ring. Then one can find the solution by solving first the equation

$$g_n(x_n) = 0,$$

to find the value of x_n. One can now plug the value of x_n into

$$g_{n-1}(x_{n-1}, x_n) = 0$$

to find the value of x_{n-1}, and so on until all x_i are found.

In order for this process to work correctly, the Gröbner basis must be computed with respect to a special ordering, mostly called lex-order. Henceforth we mean "Gröbner basis in lex order" when we speak of Gröbner basis, because we want it to have the elimination property for actually solving the system.

Faugère and Joux showed that in the process of finding the Gröbner basis the degree of the polynomials that the Gröbner basis algorithm will generate should not be higher than $log(D)$. This makes the algorithm complexity to be polynomial once one fixes D, since $log(D)$ is very small due to the considerations for decryption.

4 The Algebraic Attack Revisited

Now we would like to do a careful analysis what role the field equations play in the algebraic attacks of HFE. In the case of $q = 2$, the field equations, which are also quadratic, are easily used in the computations of the Gröbner basis. But if we work in a bigger field, say GF(11), then the field equations

$$x_i^{11} - x_i = 0, \qquad i = 1, \ldots, n$$

are of degree 11. The field equations can only be utilized in the computation of the Gröbner basis if the degree of a polynomial is at least 11. This means that even dealing with a relatively small number of variables, like 32, the number of monomials of a degree 11 polynomial is already $\frac{(32+11)!}{11!32!}$, which is roughly 2^{32}. With our current memory capacity, if n is more than 64, the Gröbner basis algorithm can not really use the field equations, even if we try to add them to the set of equations we want to solve.

Before we go on further, we would like to make the following remark to clear the concepts that often cause confusions. Given a polynomial $f(x_1, \ldots, x_n)$ over $\mathbf{F}$, we have two different ways to look at it: One way is to look at it as an element in the polynomial ring $\mathbf{F}[x_1, \ldots, x_n]$, or we can look at it as an element in the function ring

$$\mathbf{F}[x_1, \ldots, x_n] / < x_1^q - x_1, \ldots, x_n^q - x_n > .$$

In the second case we identify x_i^q with x_i.

Let $f_1(x_1, \ldots, x_n) = 0, \ldots, f_n(x_1, \ldots, x_n) = 0$ be a set of n multivariate polynomial equations in n variables over $\mathbf{F}$. If we only want the solutions in $\mathbf{F}$, we actually need to solve the set of equations

$$f_1(x_1, \ldots, x_n) = 0, \ \ldots, \ f_n(x_1, \ldots, x_n) = 0, \ x_1^q - x_1 = 0, \ \ldots, \ x_n^q - x_n = 0.$$

In this case, we need to find the Gröbner basis for the ideal generated by the set of polynomials

$$f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n), x_1^q - x_1, \ldots, x_n^q - x_n$$

in the ring $\mathbf{F}[x_1, \ldots, x_n]$. So we generally work on the ring $\mathbf{F}[x_1, \ldots, x_n]$, and if we want to work in the function ring we include the field equations.

Let us consider the case in which we do not take the field equations into account. Our key observation is that for any system of multivariate polynomial equations, if there are d different values for each variable (including the values in the extension field, or its algebraic closure), we should not be able to solve this system directly via the Gröbner basis algorithm with a maximum degree of this variable lower than d.

Proposition 1. *Let $f_1(x_1, \ldots, x_n) = 0, \ \ldots, \ f_n(x_1, \ldots, x_n) = 0$ be a set of n multivariate polynomial equations in n variables over $\mathbf{F}$; for each x_i, $1 \leq i \leq n$, if x_i has d different solutions $\beta_1, \ldots, \beta_d$ (including the ones in the algebraic closure of $\mathbf{F}$), the maximum degree of the corresponding Gröbner basis – in particular $g_n(x_n)$ – must have a degree higher or equal to d.*

Proof. We can prove it easily by contradiction. Suppose we get exactly d values for x_n by the equations generated by the f_i. If the degree of $g_n(x_n)$ is d' with $d' < d$, then we will have only d' values for x_n. This is impossible.

Similarly we have

Proposition 2. *Let $f_1(x_1, \ldots, x_n) = 0, \ \ldots, \ f_n(x_1, \ldots, x_n) = 0, \ x_1^q - x_1 = 0, \ \ldots, \ x_n^q - x_n = 0$ be the set of $2n$ multivariate polynomial equations in n variables over $\mathbf{F}$; for each x_i, $1 \leq i \leq n$, if x_i has d different solutions $\beta_1, \ldots, \beta_d$ in $\mathbf{F}$, the maximum degree of the corresponding Gröbner basis – in particular $g_n(x_n)$ – must have a degree higher or equal to d.*

Proof. We can prove it as in the proposition above.

So if we include the field equations, then we are indeed looking for solutions in the original field. If we do not include the field equations, we are actually looking for the solutions in the algebraic closure of the original field.

From the analysis above, we can also see that the minimum degrees a Gröbner basis (in lex order) needs to deal with in these two cases are very different, one is determined by the number of solutions in the original field and another one is determined by the extension field or algebraic closure.

Now let us move back to our case, the HFE cryptosystems. First, we know that T has no impact on the number of solutions, and it is also clear that S also has no impact on the number of solutions, because it is just a change of basis. Therefore the number of solutions of the public equations is determined by the number of solutions of the equations in the form of

$$P(X) - P' = 0$$

over the big field **K**. Also because S is a random transformation, we have, in general, a high probability that for each variable all solutions will not have the same value.

In the case that we include the field equations, then we are looking for solutions of the following equations

$$P(X) - P' = 0,$$
$$X^{q^n} - X = 0.$$

From the argument of Faugère and Joux that the degree of the algebraic attack using the new Gröbner basis is less or equal to $log(D)$, we can actually make the following conjecture:

Conjecture. The number of solutions to the public equation in the case of $q = 2$ for HFE in the field **F** is less or equal to $log(D)$.

This easily follows from the argument above with the assumption of Faugère and Joux's claims. We also note here that in their argument about the complexity, they implicitly used the field equations, namely the equation:

$$X^{q^n} - X = 0.$$

We also have that

Theorem 1. *If we do not include the field equation, the overall Gröbner basis algorithm (including algorithms like FGLM for switching the term ordering) has to deal with polynomials whose degree is at least equal to the number of solutions of the equation*

$$P(X) - P' = 0$$

in the algebraic closure of **K**.

From the theory of the functions over a finite field, we know that given any polynomial, we have a high probability that it is irreducible and therefore has the number of solutions, which is the same as its degree. But our case clearly is different in the sense that we know already it has at least one solution in the field **K**. From the general theory we estimate that the number of solutions of the equation

$$P(X) - P' = 0$$

in the algebraic closure of **K** should not be less than half of D statistically speaking. We will confirm this from experiments in section 5.1.

This implies that the minimum degree that a Gröbner basis needs to handle is at least $D/2$, and if D is $11^2+11 = 132$, we simply can not calculate the Gröbner basis because we can not store a polynomials with 32 variables of degree 66.

This also implies that the field equations in the case of $q = 2$ play a critical role in determining the algebraic attack complexity on HFE. However, as the characteristic increases it becomes much more difficult to utilize the field equations. Therefore, from the theoretical arguments given above, we expect (or more precisely we speculate) that for an HFE cryptosystem over GF(11) and with degree

$D = 132$, the algebraic attack should not be polynomial but rather exponential in the parameters we consider practical, that is for the range $n \leq 128$. We do not have precise theoretical arguments to prove such a statement, but we will try to confirm this speculation with our computer experiments.

We also would like to note here that Faugère and Joux's argument, stating that the degree of the polynomials which the Gröbner basis algorithm will generate should not be higher than $log(D)$, relies very much on using the field equations of characteristic two. Their argument will definitely fail if it is not the case of characteristic two. This can be shown by a very complicated combinatorial argument. Giving a detailed analysis is beyond the scope of this paper and we will present it in a separate paper.

5 Computer Experiments

Our experiments are split up in two parts. The first one is on the number of solutions in the algebraic closure and the second one is on the amount of time and memory it takes F_4 to calculate a Gröbner basis for different HFE systems. All experiments have been done on a computer at the Technical University of Darmstadt, Germany. The computer is a SunFire-280R which has an UltraSparc 1.2 GHz processor with 5120 MB of memory installed. The operating system is SunOS 5.8 (also called Solaris 8).

5.1 Experiment on the Number of Solutions

In order to verify the claim that the number of solutions of $P(X) - P' = 0$ in terms of X is generically at least $D/2$ we ran an experiment: First, we set up an HFE system and its hidden field polynomial $P(X)$. We then encrypted a random plaintext X' by finding $P' = P(X')$. Afterwards the program calculated $P(X) - P'$ and factored this polynomial. We did 800 test cases, 400 using $n = 17$ and 400 using $n = 19$. Not a single factorization contained a factor with a multiplicity higher than one, which means that the number of solutions in all 800 tests was exactly D which is trivially bigger than $D/2$.

5.2 Experiment of Solving Equations by F_4

Currently it is commonly accepted that the new Gröbner basis algorithm F_4 [5] and F_5 [6] are the most powerful tools to solve polynomial equations. Because F_4 is the only one which is publicly available, we used the Magma implementation of F_4 in order to see what the complexity of the algebraic attacks are indeed like.

We first generated the public key equations and then used Magma to try to find the Gröbner basis of this system. The experiments, as expected, produced the full triangular Gröbner basis in lex order. Our program then found all solutions and verified that indeed they included the correct solution. All experiments were done without using the field equations as this slows things down (see Fig. 6).

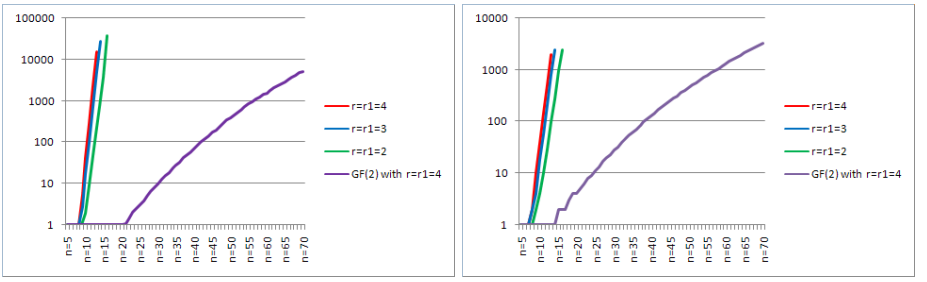

Fig. 1. Timings and memory usage for HFE systems over *GF(3)*

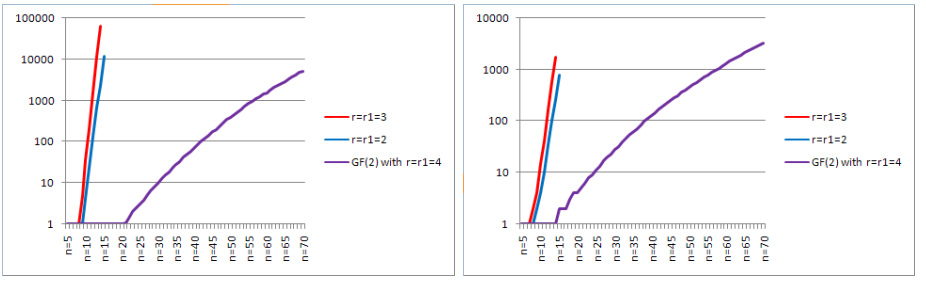

Fig. 2. Timings and memory usage for HFE systems over *GF(5)*

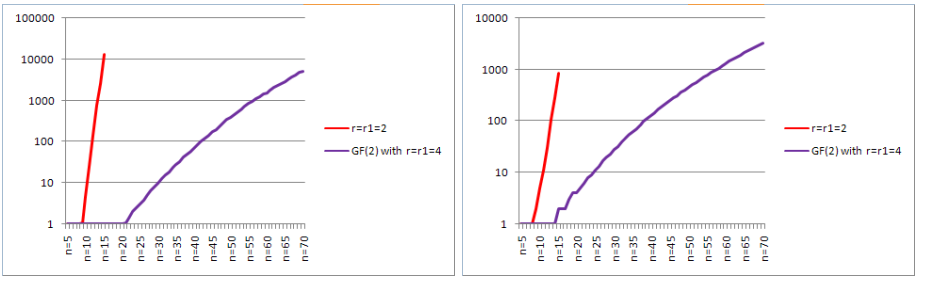

Fig. 3. Timings and memory usage for HFE systems over *GF(7)*

Tables below show the running time and the required memory of each n. In both figures we take n as the X-coordinate and show the running time (on the left, in seconds) and the required memory (on the right, in MB) as the logarithmic Y-coordinate. It clearly shows the exponential growing tendency with increasing n. The timing, we conclude, should be exponential and not polynomial. A more detailed overview over timings and memory usage can be found in the appendix. Much more theoretical and experimental work is still needed to fully understand the whole behavior.

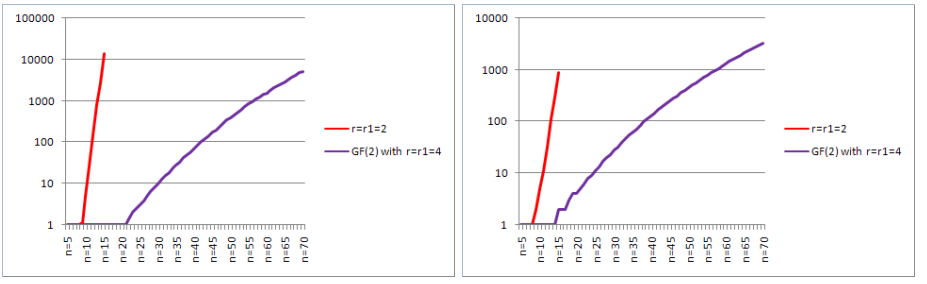

Fig. 4. Timings and memory usage for HFE systems over *GF(11)*

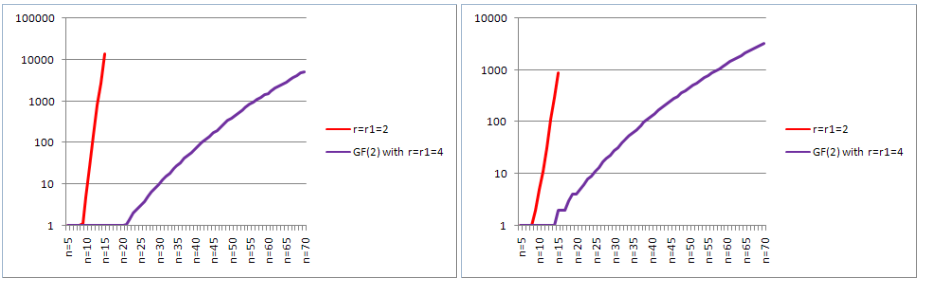

Fig. 5. Timings and memory usage for HFE systems over *GF(13)*

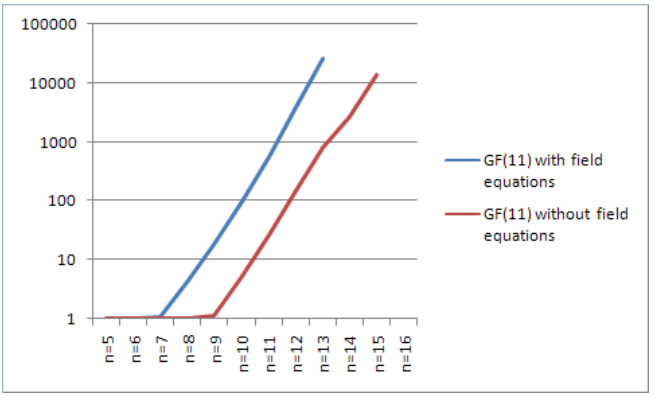

Fig. 6. Timings for HFE over *GF(11)* with and without field equations "$x_i^{11} - x_i$"

Currently it is not completely clear to us what the Magma F_4 implementation does when it comes to bigger characteristics. For GF(11), the implementation produced Gröbner bases, whose degree is higher than expected.

In order to see that the field equations do not help but even slow down the calculations, if they are not used properly, we re-ran the tests for GF(11) after putting in the field equations. The result also looks like expected, see Fig. 6.

6 New HFE Cryptosystems for Encryption

From the analysis above, we conclude that with a proper choice of parameters on the right field, we can build an HFE cryptosystem that could resist the algebraic attacks. But we also know that for any HFE cryptosystem, one must consider the Kipnis-Shamir attack. The recent work [10] actually shows that this attack does not work as efficiently as claimed. With this, we conclude one can build a reasonably secure HFE cryptosystem.

However, here we would like to propose a new type of HFE variant, which we call the projected HFE cryptosystem or PHFE.

Let $\bar{P}(x_1, \ldots, x_n)$ be the public key of HFE, then we randomly choose a linear equation

$$a_1 x_1 + \cdots + a_n x_n + a = 0. \tag{4}$$

We will pick a nonzero element among the a_i's, which we assume here to be a_n. Then we substitute x_n (or x_i) in $\bar{P}$ by the function

$$-\frac{a_1}{a_n} x_1 - \cdots - \frac{a_{n-1}}{a_n} x_{n-1} - \frac{a}{a_n},$$

which results in a new function:

$$\hat{P}(x_1, \ldots, x_{n-1}) = \bar{P}(x_1, \ldots, x_{n-1}, -\frac{a_1}{a_n} x_1 - \cdots - \frac{a_{n-1}}{a_n} x_{n-1} - \frac{a}{a_n}).$$

This will be the public key of PHFE. In this case, we have n polynomials and $n-1$ variables. The linear equation above also becomes part of the private key. The encryption process will be just as before. Decryption only varies in one point: once we have derived a few possible candidates for the plaintext, we will choose only the specific one, which satisfies the equation (4).

The new public key $\hat{P}$ can be seen as a projection of the old public key function $\bar{P}$. This projection map will serve two purposes:

1. It will destroy the hidden field structure of the old public key $\bar{P}$, such that the Kipnis-Shamir attack becomes useless, which is self-evident.
2. It will make the map more likely to be bijective so that the problem of multiple decryption choices becomes very unlikely.

This idea of projection was mentioned previously in several places, but it was never considered to be of any use because it does not help in terms of resisting the algebraic attacks.

Now we will take a look at the choices of a proper field $\mathbf{F}$. From our argumentation it seems, as if the system's security grows with the size of the ground field $\mathbf{F}$, but this does not work in all cases. By choosing $\mathbf{F}$ to have characteristic 2 and therefore cardinality 2^m, one can easily transform the public key into polynomials over GF(2). The only difference is an increment in the number of equations and the number of variables m. Then the algebraic attack still works as before when the degree of the polynomial $P(X)$ is not big enough. Therefore, we propose not to use a field of characteristic two.

For practical applications, we suggest that we should use GF(11) to build a PHFE system. We suggest D to be $11^2+11 = 132$ and $n = 89$, which should have the security level of at least 2^{80} triple DES from our estimation by computational experiments. In comparison with the HFE challenge broken by Faugère, in terms of memory, the public key of this new cryptosystem is about 5 times the size. In terms of the most costly part of the computation, namely the decryption process, the new system takes about twice the time to decrypt. All in all, the new system is comparable to the HFE challenge broken by Faugère.

To make the subject more interesting, we propose a test challenge, which, we speculate, might be within the reach of a practical attack with the most powerful computers of today. For the challenge we choose the field to be GF(7) with $D = 7^2 + 7 = 56$ and $n = 67$. The point is that if the claims about the algebraic attack on HFE with characteristic 2 is also valid here then one should be able to break our challenge.

7 Conclusion

We revisited the algebraic attack on the HFE cryptosystems. We showed that the algebraic attack on the HFE cryptosystems using the new Gröbner basis algorithm behaves differently, if it can not utilize the field equation to the full extent and the algebraic attack then can not work as efficiently as in the case of GF(2). Furthermore, we have shown via the new Gröbner basis algorithm F_4, that the complexity of the attack should be exponential and not polynomial when the characteristic of the field is not two. 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 Gröbner basis algorithm is bounded from below by the number of solutions.

We also proposed a new variant of the HFE cryptosystems. The public key of HFE is projected to a space of one dimension lower. It serves the purpose to protect it form the Kipnis-Shamir attack and to avoid multiple candidates for the correct plaintext in the decryption process. We suggested an example for a practical application on GF(11), which we expect to be at the security level of 2^{80} triple DES, and a test challenge on GF(7) for practical attacks.

References

1. Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Mathematical Institute, University of Innsbruck, Austria. Dissertation (1965)
2. Courtois, N.T.: The security of hidden field equations (HFE). In: Naccache, C. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 266–281. 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, `http://www.minrank.org`
4. Ding, J., Gower, J., Schmidt, D.: Multivariate Public Key Cryptosystems. In: Advances in Information Security, Springer, Heidelberg (2006) (ISBN 0-387-32229-9)

5. Faugère, J.-C.: A New Efficient Algorithm for Computing Gröbner Bases (F_4). Journal of Pure and Applied Algebra 139, 61–88 (1999)
6. 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)
7. Faugère, J.-C., Joux, A.: 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)
8. Garey, M.R., Johnson, D.S.: Computers and Intractability – A Guide to the Theory of NP-Completeness. W.H. Freeman and Company (1979) (ISBN 0-7167-1044-7 or 0-7167-1045-5)
9. 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)
10. Jiang, X., Ding, J., Hu, L.: Kipnis-Shamir's attack on HFE revisited Cryptology ePrint Archive (2007)
11. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 19–30. Springer, Heidelberg (1999)
12. MAGMA Computational Algebra System, `http://magma.maths.usyd.edu.au/magma/`
13. Matsumoto, T., Imai, H.: Tsutomu Matsumoto and Hideki Imai. In: Günther, C.G. (ed.) EUROCRYPT 1988. LNCS, vol. 330, pp. 419–453. Springer, Heidelberg (1988)
14. Moh, T.-T.: On the method of "XL" and its inefficiency to TTM Cryptology ePrint Archive, Report 2001/047, `http://eprint.iacr.org/`
15. Patarin, J.: Hidden field equations (HFE) and isomorphism of polynomials (IP): Two new families of asymmetric algorithms. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070. Springer, Heidelberg (1996)
16. Wolf, C., Preneel, B.: Taxonomy of public key schemes based on the problem of multivariate quadratic equations. Cryptology ePrint Archive, Report,2005/077, 12th of May 2005. 64 pages (2005), `http://eprint.iacr.org/2005/077/`

A Tables for GF(11) and GF(2)

TIMINGS	**GF(11)**	**GF(2)**
$n = 5$	0,01	0,01
$n = 6$	0,02	0,01
$n = 7$	0,07	0,01
$n = 8$	0,25	0,01
$n = 9$	1,13	0,01
$n = 10$	4,74	0,01
$n = 11$	25,87	0,02
$n = 12$	147,03	0,03
$n = 13$	799,96	0,04
$n = 14$	2722,40	0,13
$n = 15$	13744,27	0,17
$n = 16$	>84600	0,25
$n = 17$		0,32
$n = 18$		0,44
$n = 19$		0,61
$n = 20$		0,81
$n = 21$		1,05
$n = 22$		1,35
$n = 23$		1,94
$n = 24$		2,41
$n = 25$		3,03
$n = 30$		9,41
$n = 40$		70,98
$n = 50$		376,39
$n = 60$		1519,22
$n = 60$		1519,22
$n = 70$		4962,35

MEMORY USAGE	**GF(11)**	**GF(2)**
$n = 5$	0,76	0,67
$n = 6$	0,76	0,67
$n = 7$	0,95	0,67
$n = 8$	1,03	0,65
$n = 9$	1,06	0,72
$n = 10$	1,47	0,71
$n = 11$	2,88	0,74
$n = 12$	5,89	0,86
$n = 13$	14,23	0,93
$n = 14$	34,15	1,18
$n = 15$	105,76	1,35
$n = 16$		1,24
$n = 17$		2,55
$n = 18$		2,98
$n = 19$		1,72
$n = 20$		1,98
$n = 21$		2,21
$n = 22$		2,38
$n = 23$		2,52
$n = 24$		3,07
$n = 25$		3,45
$n = 30$		5,98
$n = 40$		16,20
$n = 50$		30,74
$n = 60$		59,57
$n = 70$		140,20