Cryptanalysis of HFEv and internal perturbation of HFE

Jintai Ding[1] and Dieter Schmidt[2]

Department of Mathematical Sciences[1],
Department of Electrical & Computer Engineering and Computer Science[2],
University of Cincinnati,
Cincinnati, OH, 45221,
USA
ding@math.uc.edu[1] , dieter.schmidt@uc.edu[2]

Abstract. Hidden field equation (HFE) multivariable cryptosystems were first suggested by Patarin. Kipnis and Shamir showed that to make the cryptosystem secure, a special parameter D of any HFE cryptosystem can not be too small. Consequently Kipnis, Patarin and Goubin proposed an enhanced variant of the HFE cryptosystem by combining the idea of Oil and Vinegar construction with the HFE construction. Essentially they "perturb" the HFE system with some external variables. In this paper, we will first present a new cryptanalysis method for the HFEv schemes. We then use the idea of internal perturbation to build a new cryptosystem, an internally perturbed HFE cryptosystem (IPHFE).

Keywords: Public-key, multivariable, quadratic polynomials, Hidden field equation, internal perturbation.

1 Introduction

Since the invention of the RSA scheme, there has been great interest in constructing other public key cryptosystems. One of the directions is to use multivariable polynomials, in particular, quadratic polynomials. This construction relies on the proven theorem that solving a set of multivariable polynomial equations over a finite field is, in general, an NP-hard problem [GJ79]. Nevertheless, it is not enough to guarantee the security of such a cryptosystem.

One of the basic designs in this directions was started by Matsumoto and Imai [MI88]. They suggested to use a map F over a large field $\bar{K}$, which is a degree n extension of a smaller finite field k. By identifying $\bar{K}$ with k^n the map F produces a multivariable polynomial map from k^n to k^n, which is denoted by $\tilde{F}$. Then one "hides" this map $\tilde{F}$ by composing from the left and the right by two invertible affine linear maps L_1 and L_2 on k^n. This generates a quadratic map $\bar{F}$:

$$\bar{F} = L_1 \circ \tilde{F} \circ L_2$$

from k^n to k^n ($\circ$ means composition of two maps). Matsumoto and Imai suggested the map $F : X \longmapsto X^{1+q^i}$, where q is the number of elements in k, X is an element in $\bar{K}$ and k is of characteristic 2. However Patarin [Pat95] showed that this scheme is insecure under an algebraic attack when linearization equations are used.

Since then, Patarin and his collaborators have made a great effort to find secure modifications of the Matsumoto-Imai system. These modified cryptosystems can be divided into two types:

1) Minus-Plus method [PGC98]: The Minus method was first suggested in [Sha98] and is the simplest idea among all. In the Minus method one removes a few of the components of $\bar{F}$, and in the Plus method one adds a few randomly chosen quadratic polynomials. It is possible to combine both methods. The main reason to take the "Minus" action is the necessity to make the corresponding equations more difficult to solve so that the linearization equations can no longer be used. Minus (only) method is well suited for signature schemes. One such scheme, Sflash^{v2} [ACDG03,PCG01], was last year accepted as one of the final selections in the New European Schemes for Signatures, Integrity, and Encryption: IST-1999-12324, although Patarin has now proposed that Sflash^{v2} should be replaced by the new version Sflash^{v3} [CGP03].

2) Hidden Field Equation Method (HFE) [Pat95]: Patarin believes that this construction is the strongest. The difference of this scheme to the original system of Matsumoto-Imai is that F is substituted by a new map (function)

$$F : X \longmapsto \sum_{0,0}^{D} a_{ij} X^{q^i+q^j} + \sum_{0}^{D} b_i X^{q^i} + c,$$

where the polynomial coefficients are randomly chosen. The total degree of F can not be too large, because the decryption process needs to solve the polynomial equation $F(X) = Y'$ for a constant Y'. However a new algebraic attack by Kipnis and Shamir [KS99] using both Minrank and relinearization shows that the number D can also not be too small. This is confirmed by [Cou01,FJ03].

Another direction Patarin and his collaborators have pursued is inspired by the linearization equations mentioned above. This type of construction includes Dragon [Pat96a], Little Dragon [Pat96a], Oil and Vinegar [Pat97], and Unbalanced Oil and Vinegar [KPG99]. From the point view of our paper, the interesting ones are the last two schemes, where the basic idea is that certain quadratic equations can be easily solved if we are allowed to guess a few variables. The key map is a map O from $k^n = k^{o+v}$ to k^o:

$$O(x_1, ..., x_o, x'_1, ..., x'_v) = (O_1(x_1, ..., x_o, x'_1, ..., x'_v), ..., O_o(x_1, ..., x_o, x'_1, ..., x'_v)),$$

such that each O_i is a Oil and Vinegar polynomial in the form:

$$O_i(x_1, \ldots, x_o, x'_1, \ldots, x'_v) = \sum a_{ij} x_i x'_j + \sum b_{ij} x'_i x'_j + \sum c_i x_i + \sum d_i x'_j + e$$

where the x_i's are called Oil variables and the x'_j's Vinegar variables. One can see the similarity of the above formula with the linearization equations. This family of cryptosystems are designed specially for signature schemes, where we need only to find one solution of a given equation not a unique solution.

In order to enhance the security of the HFE system, Patarin and his collaborators proposed later a new scheme, which is a combination of the HFE system with the Unbalanced Oil and Vinegar system. They denote it by the Hidden Field Equation Vinegar (HFEv) schemes. The basic idea besides the HFE method is to add a few new (Vinegar) variables to make the system more complicated [Pat96b]. This method essentially replaces F with an even more complicated map from $\bar{K} \times k^r$ to $\bar{K}$ of the form:

$$F_v(X, x'_1, \ldots, x'_r) = \tag{1}$$
$$\sum_{0,0}^{D,D} a_{ij} X^{q^i+q^j} + \sum_{0}^{D} b_i X^{q^i} + \sum_{0}^{D} \Omega_i(x'_1, \ldots, x'_r) X^{q^i} + U_0(x'_1, \ldots, x'_r),$$

where Ω_i is a randomly chosen k linear affine injective map from k^r to $\bar{K}$ and U_0 is a randomly chosen quadratic map from k^r to $\bar{K}$.

One can see that these new variables are mixed in a special way with the original variables (like oil and vinegar). The decryption process requires a search on these added small number of variables. For the signature case, the Vinegar variables can be selected at random. It has a good probability to succeed, otherwise another selection is made until a correct answer is found.

As far as we know, there does not exist any algebraic attack using the structure of HFEv. However, in this paper, we will show that it is possible that the attack in [KS99] can also be applied here to separate the Vinegar variables and attack the system if both D and r are small. The basic idea is to use the algebraic method to find a way to purge out the Vinegar variables. The complexity of such an attack is, however, exponential in term of r.

After all the papers mentioned above, it seems that all possible extensions and generalizations of the Matsumoto-Imai system are exhausted, but recently a new idea was proposed by Ding [Din04] to enhance the Matsumoto-Imai system. It is called internal perturbation and represents a very general idea.

In a very broad context the HFE and Oil-Vinegar methods can also be seen as an extension of a commonly used idea in mathematics and physics, namely perturbation. A good way to deal with a continuous system often is to "perturb" the system at a minimum scale. In terms of this view, the HFEv and Oil-Vinegar methods can be viewed as perturbations of the HFE method by the newly added Vinegar variables. However, the perturbation is in some sense more an "external" perturbation, as a few extra (external) variables (Vinegar) are introduced. The idea of internal perturbation is to use internal variables instead, which map to a small subspace of the original variables.

We call the new system an internally perturbed HFE (IPHFE) system. For a IPHFE system, this method essentially replaces F with a new function:

$$F : (X) \longmapsto$$

$$\sum_{0,0}^{D,D} a_{ij} X^{q^i+q^j} + \sum_{0}^{D} b_i X^{q^i} + \sum_{0,0}^{D,n-1} c_{i,j} X^{q^i} \tilde{X}_r^{q^j} + \sum_{0,0}^{n-1,n-1} \alpha_{ij} \tilde{X}_r^{q^i+q^j} + \sum_{0}^{n-1} \beta_i \tilde{X}_r^{q^i} + \gamma.$$

The new internal perturbation variable $\tilde{X}_r$ is given by $\tilde{X}_r = \sum_0^{n-1} a_i X^{q^i}$. The function $Z(X) = \sum_0^{n-1} a_i X^{q^i}$, when viewed as a linear map from k^n to k^n, has an image space of low dimension r, which we call the perturbation dimension.

This perturbation is performed through a small set of variables "inside" the space k^n (therefore they are "internal" variables) and one does **not** introduce any new variables. Namely given a quadratic multivariable system $\bar{F}$ over k^n, we randomly find a linear map Z from k^n to k^n with the image space of a small dimension r, then we try to "perturb" the system through the small number variables related to Z.

Although we use the same basic idea of internal perturbation as in [Din04], the perturbation here is done differently. In the original method only terms like U_0 were used, whereas here a mixing of the linear terms from the original and perturbation variables $Z(X)$ occurs, so that the perturbation variables and the original variables are fully mixed. This makes the system more complicated.

The motivation for our work came from our attack method to purge out the external perturbation. This lead us to construct new systems that are resistant to the algebraic attack [Pat95,KS99] and its extensions like XL, but without sacrificing much of the efficiency of the system. An additional advantage of the new systems is that the internal perturbation makes the process of elimination of unnecessary candidates in the decryption process much faster.

In the first section of the paper, we will introduce, in detail, our idea of how to attack an HFEv system. Then we will present the IPHFE system and a practical implementation example of an 89 bits cryptosystem system, where we choose the perturbation dimension to be 2. We will show that it should have a very high security level against all known attacking methods. We will analyze the security and efficiency of the system.

2 Cryptanalysis of HFEv cryptosystem.

2.1 The HFEv cryptosystem.

Let $\bar{K}$ be a degree n extension of a finite field k of characteristic 2 with q elements, and $\bar{K} \cong k[x]/g(x)$, where $g(x)$ is a degree n irreducible polynomial over k. That k has characteristic 2 is not essential here.

Let ϕ be the standard k-linear map that identifies $\bar{K}$ with k^n:

$$\phi : \bar{K} \longmapsto k^n,$$

such that

$$\phi(a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}) = (a_0, a_1, a_2, \cdots, a_{n-1}).$$

The idea of lifting a map over spaces of a small finite field [KS99] to a larger field is the key idea, which leads us to a new formulation of the HFEv explained in the introduction.

Lemma 1 *[KS99] Let $Q(x_1,\ldots,x_n)=(Q_1(x_1,\ldots,x_n),\ldots,Q_n(x_1,\ldots,x_n))$ be a linear map from k^n into k^n. Then there exist $a_0,\ldots,a_{n-1}$ in $\bar{K}$, such that*

$$\phi^{-1}\circ Q(x_1,\ldots,x_r)=\sum_{i=0}^{n-1}a_iX^{q^i},$$

where $X=\phi^{-1}(x_1,\ldots,x_n)$.

From this lemma, we have

Lemma 2 *Let $Q(x'_1,\ldots,x'_r)=(Q_1(x'_1,\ldots,x'_r),\ldots,Q_n(x'_1,\ldots,x'_r))$ be a linear map from k^r into k^n. Then there exist $a_0,\ldots,a_{n-1}$ in $\bar{K}$, such that*

$$\phi^{-1}\circ Q(x'_1,\ldots,x'_r)=\sum_{i=0}^{n-1}a_i\bar{X}_r^{q^i},$$

where $\bar{X}_r=\phi^{-1}(x'_1,\ldots,x'_r,0,\ldots,0)$.

This lemma is a simple corollary from Lemma 1 above from [KS99]. It allows us to reformulate the key function (1) and give an equivalent description:

$$F:(X,X_r)\longmapsto$$

$$\sum_{0,0}^{D,D}a_{ij}X^{q^i+q^j}+\sum_{0}^{D}b_iX^{q^i}+\sum_{0,0}^{D,n-1}c_{i,j}X^{q^i}\bar{X}_r^{q^j}+\sum_{0,0}^{n-1,n-1}\alpha_{ij}\bar{X}_r^{q^i+q^j}+\sum_{0}^{n-1}\beta_i\bar{X}_r^{q^i}+\gamma,$$

where $X_r=(x'_1,\ldots,x'_r)$ represents the new Vinegar variables. The first two terms are the same as in (1), the third term here is derived from the third term in (1), and the last three terms come from U_0.

This new formulation is the key to our attack. Let $\tilde{F}$ be a map from k^{n+r} to k^n and

$$\tilde{F}(x_1,\ldots,x_n,x'_1,\ldots,x'_r)=\phi\circ F\circ(\phi^{-1}\times Id)(x_1,\ldots,x_n,x'_1,\ldots,x'_r)=$$

$$(\tilde{F}_1(x_1,...,x_n,x'_1,...,x'_r),\tilde{F}_2(x_1,...,x_n,x'_1,...,x'_r),\cdots,\tilde{F}_n(x_1,...,x_n,x'_1,...,x'_r)).$$

Here $\tilde{F}_i(x_1,\ldots,x_r,x'_1,\ldots,x'_r)$ are quadratic polynomials of $n+r$ variables.

Let L_1 and L_2 be two randomly chosen invertible affine linear maps one over k^n and the other over k^{n+r}.

$$\bar{F}(x_1,\ldots,x_n,x'_1,\ldots,x'_r)=L_1\circ\tilde{F}\circ L_2(x_1,\ldots,x_n,x'_1,\ldots,x'_r)=$$

$$(\bar{F}_1(x_1,...,x_n,x'_1,...,x'_r),\bar{F}_2(x_1,...,x_n,x'_1,...,x'_r),...,\bar{F}_n(x_1,...,x_n,x'_1,...,x'_r))$$

is the cipher for the HFEv system. No effective algebraic attack method exists for it yet, which uses the properties of the map F.

2.2 Cryptanalysis for the case $r = 1$

In this section, we will present a new attack method for the HFEv cryptosystem, which is an extension of an idea of Kipnis and Shamir. We will show how it works when $r = 1$, which we will assume throughout this section.

When $r = 1$, the map F from $\bar{K} \times k$ to $\bar{K}$, which is used to define the HFEv system, is:

$$F : (X, x'_1) \longmapsto$$

$$\sum_{0,0}^{D} a_{ij} X^{q^i+q^j} + \sum_{0}^{D} b_i X^{q^i} + \sum_{0}^{D} c_i X^{q^i} T_1(x'_1) + \alpha T_1(x'_1)^2 + \beta T_1(x'_1) + \gamma$$

where x'_1 represents the new Vinegar variables, $\bar{X} = \phi^{-1}(x'_1, 0, \ldots, 0)$ is the image of a k linear embedding map T_1 from k to $\bar{K}$: $T_1(x) = \phi^{-1}(x, 0, \ldots, 0)$.

Let $\hat{K}$ be the $n + 1$ dimensional k subspace in $\bar{K} \times \bar{K}$ such that for any element $\hat{X} = (X_1, X_2)$,

$$\phi(X_2) = (x'_1, 0, \ldots, 0).$$

The map $F(X, x'_1)$ can be reinterpreted as a map from $\hat{K}$ to K, so that we have

$$F : (X, \bar{X}) \longmapsto$$

$$\sum_{i,j}^{D} a_{ij} X^{q^i+q^j} + \sum_{0}^{D} b_i X^{q^i} + \sum_{i}^{D} c_i X^{q^i} \bar{X} + \alpha \bar{X}^2 + \beta \bar{X} + \gamma,$$

with

$$\phi(\bar{X}) = (x'_1, 0, \ldots, 0).$$

We should recall that

$$\bar{X}^q = \bar{X},$$

and this is why the formula above has no high power terms of $\bar{X}$. Let P_1 be the projection such that

$$P_1(x_1, \ldots, x_n) = x_1.$$

Let $\phi_1 = \phi \times (P_1 \circ \phi)$ be the standard map from $\hat{K}$ to k^{n+1}, then

$$\tilde{F} = \phi \circ F \circ \phi_1^{-1}$$

and the cipher (public key) is given as

$$\bar{F} = L_1 \circ \tilde{F} \circ L_2,$$

where L_1 is an invertible affine linear map on k^n and L_2 is an affine linear map on k^{n+1}.

The public key consists of the polynomial components of $\bar{K}$. The private key is L_1, L_2 and F and its related field structure.

One way to attack the system is to find L_1 and L_2 such that if we compose from the two ends with their inverses we would recover F.

To attack, the first observation we have is that:

$$\begin{aligned}\hat{F} &= \phi^{-1}\circ\bar{F}\circ\phi_1 = \phi^{-1}\circ L_1\circ\tilde{F}\circ L_2\circ\phi_1\\ &= (\phi^{-1}\circ L_1\circ\phi)\circ F\circ(\phi_1^{-1}\circ L_2\circ\phi_1).\end{aligned}$$

We know what $(\phi\circ L_1\circ\phi^{-1})$ is like from Lemma 1 and for $\phi_1\circ L_2\circ\phi_1^{-1}$, we have the following lemma

Lemma 3 *Let $Q(x_1,\dots,x_n,x_1') = (Q_1(x_1,\dots,x_1'),\dots,Q_{n+1}(x_1,\dots,x_1'))$ be a linear map from k^{n+1} to k^{n+1}. Then there exist $a_0,\dots,a_{n-1},a_0',a,b$ in $\bar{K}$, such that*

$$\phi_1^{-1}\circ Q(x_1,\dots,x_n,x_1') = (\sum_0^{n-1} a_iX^{q^i} + a_0'\bar{X}, b\bar{X} + \sum_0^{n-1} a^{q^i}X^{q^i}),$$

as a k linear map over $\hat{K}$, where $\bar{X} = \phi^{-1}(x_1',0,\dots,0)$, $X = \phi^{-1}(x_1,\dots,x_n)$ and $\phi(b) = (b,0,\dots,0)$.

This can be proven with the same argument as the one for Lemma 1 in [KS99].

In order to simplify the presentation, from now on we will assume that L_1 and L_2 and F are homogeneous. Our attack works the same way for the non–homogeneous case, because we can simply drop all lower degree terms.

In this case,

$$F : (X,\bar{X}) \longmapsto \sum_{0,0}^{D} a_{ij}X^{q^i+q^j} + \sum_0^D c_iX^{q^i}\bar{X} + \alpha\bar{X}^2.$$

From the lemma above, we can set

$$\bar{L}_1(X) = \phi\circ L_1\circ\phi^{-1}(X) = \sum_0^{n-1} l_{1i}X^{q^i},$$

as in Lemma 1;

$$\bar{L}_2(X,\bar{X}) = \phi_1\circ L_2\circ\phi_1^{-1}(X,\bar{X}) = (\sum_0^{n-1} l_{2i}X^{q^i} + l_{2,0}'\bar{X}, l_{2,1}'\bar{X} + \sum_0^{n-1} l_2^{q^i}X^{q^i}),$$

as in Lemma 3. This means that

$$\hat{F}(X,\bar{X}) = \sum_{0,0}^{n-1,n-1} \hat{a}_{ij}X^{q^i+q^j} + \sum_0^D \hat{c}_iX^{q^i}\bar{X} + \hat{\alpha}\bar{X}^2.$$

Once we have the public key, it is clear that $\hat{F}$ can be easily found by solving a set of a linear equations, once we fix the field structure of $\bar{K}$. Because all finite fields with the same size are isomorphic, any choice would work in this case as was pointed out in [KS99].

Our formulation changes the problem of finding L_1 and L_2 into a problem of finding $\bar{L}_1$ and $\bar{L}_2$.

Now we will use the same method as in [KS99], namely we treat the map $\hat{F}$ and F as a quadratic form, to which we associate a $(n+1)\times(n+1)$ matrix for a corresponding bilinear form.

In this case, we associate a symmetric matrix $\hat{A}$ with $\hat{F}$ such that

$$\hat{A} = \begin{pmatrix} 0 & \hat{a}_{0,1}+\hat{a}_{1,0} & . & . & . & . & \hat{a}_{0,n-1}+\hat{a}_{n-1,0} & \hat{c}_0 \\ \hat{a}_{0,1}+\hat{a}_{1,0} & 0 & . & . & . & . & \hat{a}_{1,n-1}+\hat{a}_{n-1,1} & \hat{c}_1 \\ \hat{a}_{0,2}+\hat{a}_{2,0} & \hat{a}_{1,2}+\hat{a}_{2,1} & . & . & . & . & \hat{a}_{2,n-1}+\hat{a}_{n-1,2} & \hat{c}_2 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ \hat{a}_{0,n-1}+\hat{a}_{n-1,0} & \hat{a}_{0,n-1}+\hat{a}_{n-1,0} & . & . & . & . & 0 & \hat{c}_{n-1} \\ \hat{c}_0 & \hat{c}_1 & . & . & . & . & \hat{c}_{n-1} & 0 \end{pmatrix}.$$

We associate a matrix A to F as

$$A = \begin{pmatrix} 0 & a_{0,1}+a_{1,0} & ... & a_{0,D}+a_{D,0} & 0 & .. & 0 & c_0 \\ a_{0,1}+a_{1,0} & 0 & ... & a_{1,D}+a_{D,1} & 0 & .. & 0 & c_1 \\ a_{0,2}+a_{2,0} & a_{1,2}+a_{2,1} & ... & a_{2,D}+a_{D,2} & 0 & .. & 0 & c_2 \\ . & . & ... & . & . & .. & . & . \\ a_{0,D}+a_{D,0} & . & ... & 0 & 0 & .. & 0 & c_D \\ 0 & . & ... & . & . & .. & 0 & c_{D+1} \\ . & . & ... & . & . & .. & . & . \\ 0 & . & ... & . & . & .. & 0 & c_{n-1} \\ c_0 & c_1 & ... & c_D & . & .. & c_{n-1} & 0 \end{pmatrix}.$$

Then we can show that the matrix $\bar{A}$ associated to $F \circ \bar{L}_2$ is:

$$\bar{A} = B_2^t \; A \; B_2,$$

and

$$B_2 = \begin{pmatrix} l_{2,0} & l_{2,1} & ... & . & . & l_{2,n-2} & l_{2,n-1} & {l'}_{2,0} \\ l_{2,n-1}^q & l_{2,0}^q & ... & . & . & l_{2,n-3}^q & l_{2,n-2}^q & {l'_{2,0}}^q \\ l_{2,n-2}^{q^2} & l_{2,n-1}^{q^2} & ... & . & . & l_{2,n-4}^{q^2} & l_{2,n-3}^{q^2} & {l'}_{2,0}^{q^2} \\ . & . & ... & . & . & . & . & . \\ l_{2,1}^{q^{n-1}} & l_{2,2}^{q^{n-1}} & ... & . & . & l_{2,n-4}^{q^{n-1}} & l_{2,n-3}^{q^{n-1}} & {l'}_{2,0}^{q^{n-1}} \\ l_2 & l_2^q & ... & . & . & l_2^{q^{n-2}} & l_2^{q^{n-1}} & l'_{21} \end{pmatrix}.$$

The matrix $\tilde{A}$ associated to $\bar{L}_1 \circ F$ is:

$$\tilde{A} = l_{1,0}A + l_{1,1}A_1 + ... + l_{1,n-1}A_{n-1},$$

where A_l corresponding to the polynomial F^{q^l} and we can see that

$$(A_l)_{i,j} = A^{q^l}_{i-l(mod(n)),j-l(mod(n))}, \text{ for } 0 < i,j < n+1;$$

$$(A_l)_{n+1,j} = A^{q^l}_{n+1,j-l(mod(n))}, \text{ for } j < n+1;$$

$$(A_l)_{j,n+1} = A^{q^l}_{j-l(mod(n)),n+1}, \text{ for } j < n+1;$$

$$(A_l)_{n+1,n+1} = 0.$$

Therefore we have

$$\bar{A} = B_2^t(l_{1,0}A + l_{1,1}A_1 + \cdots + l_{1,n-1}A_{n-1})B_2.$$

What we know is $\bar{A}$, because the invertibility of L_1 and L_2, the problem to attack the system becomes a problem to find $\bar{L}_1^{-1}$ and $\bar{L}_2^{-1}$ or equivalently to find B_2^{-1} and $\bar{L}_1^{-1}(X) = \sum_0^{n-1} l'_{1i}X^{q^i}$. This will allow us to recover A because

$$A = (B_2^t)^{-1}(l'_{1,0}\bar{A} + l'_{1,1}\bar{A}_1 + \cdots + l'_{1,n-1}\bar{A}_{n-1})B_2^{-1}$$

where $\bar{A}_l$ is the matrix corresponding to $(\bar{F})^{q^l}$ similar to the case of A_l.

One more point we notice is that if we do a change of variable X by aX, it does not affect the rank of F at all, therefore this freedom allows us to assume that $l_2 = 1$, which we will assume now.

Now we can see that we have reduced our problem to exactly the same problem that was dealt with in [KS99], and we can apply the whole machinery developed in [KS99]. But here we suggest an improved method of applying the Minrank attack method for HFE in [Cou01], such that we first find $\bar{L}_1^{-1}$ and then find B_2^{-1}. We know that the rank of A is at most and in general $D+1$. Using results in [Cou01], we know that recovering the secret key (or equivalent key) has a complexity of $(n+1)^{3(D+1)+O(1)}$. This means our attack is subexponential, and in general, if $D = 3$ and $n \leq 2^6$, the security is less than 2^{80}. We did some computer simulations with $n < 20$ and $D = 1, 2$ and the results are as predicted.

For the more general $r > 1$ case our method can be extended directly and our initial analysis shows that the attack complexity is $(n+r)^{3(D+r)+O(1)}$. But the details of the attack are much more complicated, and we will present them in the full version of this paper. This attack complexity depends on n, r and D and the exponent depends on D and r. It would be much better if we could find some attack such that r would not be in the exponent. But from a point view of symmetry, this is impossible. If we consider the case when r is large (bigger than n), then the property of the HFEv polynomial should be dominated by the r Vinegar variables and these polynomials are more or less than what can be treated with randomly chosen polynomials. From this point of view, we think that this attack complexity must include r in some way in the exponent and we speculate our attack method could be very close to what might be achieved in general.

In addition, we think our attack could lead to some new ways of attacking HFEv using the XL family of methods, see [Cou01].

3 Internal Perturbation of HFE

From the above, we can see that HFEv is indeed a cryptosystem derived through perturbation of HFE through some external variable. It is possible to purge the external variables using the method we proposed above. Now we will suggest a new cryptosystem through internal perturbation, which we will call an internally perturbed HFE cryptosystem – IPHFE.

In this section, we will present the new cryptosystem. The idea is very simple, namely we will not add new variables, but instead we will perturb the system by using some internal variables, such that the above attack can no longer be used.

3.1 The IPHFE cryptosystem

Here we will use the same notations as in the section above, namely $\bar{K}$, a degree n extension of the finite field k of characteristic 2 with q elements. That k is of characteristic 2 is not essential. Let $\bar{K} \cong k[x]/g(x)$ and $\phi : \bar{K} \longmapsto k^n$ again be the standard k-linear map that identifies $\bar{K}$ with k^n. Let $D > 1$, $r \geq 1$ be two small integers.

Let $Z(X) = \sum_0^{n-1} z_i X^{q^i}$ be a randomly chosen k linear map from $\bar{K}$ to $\bar{K}$ such that the dimension of the image space of Z in k^n is r. We can also say that the linear map $\phi \circ Z \circ \phi^{-1}$ from k^n to k^n has a kernel of dimension $n - r$.

Let F be a map from $\bar{K}$ to $\bar{K}$, and

$$F : (X) \longmapsto$$

$$\sum_{0,0}^{D} a_{ij} X^{q^i+q^j} + \sum_{0}^{D} b_i X^{q^i} + \sum_{0,0}^{D,n-1} c_{i,j} X^{q^i} \tilde{X}_r^{q^j} + \sum_{0,0}^{n-1,n-1} \alpha_{ij} \tilde{X}_r^{q^i+q^j} + \sum_{0}^{n-1} \beta_i \tilde{X}_r^{q^i} + \gamma,$$

where the new internal perturbation variable $\tilde{X}_r$ is given as $\tilde{X}_r = \sum_0^{n-1} z_i X^{q^i}$.

Let L_1 and L_2 be two randomly chosen invertible affine linear maps on k^n and let $\bar{F} = L_1 \circ \phi \circ \tilde{F} \circ \phi^{-1} \circ L_2$.

For this public-key cryptosystem, $\bar{F}$, that is the set of n quadratic polynomials of $\bar{F}$ and the structure of the field k form the public key. L_1, L_2, the field structure of $\bar{K}$, F, and Z are the secret key.

To encrypt a message $(x'_1, \ldots, x'_n)$, one just finds the value of $\bar{F}(x'_1, \ldots, x'_n)$.

To decrypt a message, one just "inverts" each component of the composition. It is easy to invert everything except the function F. Here, by "inverting" F, we mean to solve the equation

$$F(x_1, \ldots, x_n) = (y'_1, \ldots, y'_n).$$

What we do is plug in all possible values of $\tilde{X}_r \in Z(\bar{K})$ into the equation, which consists of q^r elements, and then solve the corresponding degree q^{2D} polynomial equations. This is why both q and r must be small. It is possible for many of the cases, that there is no solution at all, but we should have at least one solution among all the possibilities. For each case of $\tilde{X}$, if we have any solution $X = (x_1, \ldots, x_n)$, we then have to make sure that the solution is consistent with the corresponding elements in $\bar{X} \in Z(\bar{K})$, namely the solution X must also satisfy the equation $\bar{X} = Z(X)$, otherwise the solution is discarded. This process helps us to eliminate efficiently most of the unwanted solutions.

In general, we should have a good chance to have only one solution, but due to the definition of F, we know that the map F is not necessarily injective, which requires us to add something extra just like in the case of HFE [Pat96b]. One can add hash functions or just add (Plus method) more randomly chosen quadratic polynomials.

Similarly we can apply the Minus method [Sha98] to build authentication schemes.

3.2 A practical realization of an IPHFE cryptosystem

For a practical realization, we have chosen $\bar{K}$ to be a degree $n = 89$ extension of the finite field $k = Z_2$ with $q = 2$ elements. We use $D = 3$, and $r = 2$. In this case, we will choose the terms $X^{2^3+2^3}$ to be zero. In terms of key size, the public key is the largest, which is the size of about 400,000 bits (50 KBytes). This implementation is comparable with any of the existing multivariable cryptosystems.

In this case, the decryption process requires us to solve four times an equation of degree 16 over a finite field of size 2^{89}, which can be done easily.

3.3 Cryptanalysis

We will now show that existing algebraic attacking methods for multivariable cryptosystems can no longer be used efficiently against IPHFE. This includes the method, which was suggested above for attacking HFEv. The reason is that the internal perturbation is fully mixed with the original system and can no longer be distinguished.

We will take a careful look at two algebraic methods. We start first with the attack method of [KS99,Cou01] for HFE. From the formula for Z we can see that F, when described as a polynomial of X, looks far more complicated than F in the HFE system. Essentially it has all possible terms of $X^{q^i+q^j}$, and the corresponding symmetric matrix for its related bilinear form is expected to have a very high rank in general. In all of our computer simulations it turns out that the rank of this matrix is exactly $D + r + 1$. Therefore, we conjecture that the rank of this matrix is exactly $D+r+1$, and we believe it is possible to actually prove this statement.

Let's now try to use the method of Kipnis-Shamir to attack our system. In the fist step, the Minrank method is used to recover part of the key L_1 and we know that for this step, the computational complexity for our implementation is $89^{3\times6}$, which is bigger than 2^{120}. Let's now further assume that this can be done, and that we already have part of the key, namely L_1. In the case of the attack by Kipnis-Shamir, the second step is essentially trivial due to fact that we know that the symmetric matrix corresponding to the original $n \times n$ matrix has the shape:

$$\begin{pmatrix} \Omega & 0 \\ 0 & 0 \end{pmatrix}$$

where Ω is a submatrix of size $(D+1) \times (D+1)$, whose null space therefore is known to us and can be used to find the second part of the key L_2. However, in our case, even if we successful recover L_1, we have no idea what the matrix corresponding to the original polynomial is. As we mentioned above, it is far more complicated and we have no way of knowing what its null space is like and therefore we still can not recover L_2, which is what happened in our computer simulations. Therefore the Kipnis-Shamir method and the key part, the Minrank method, can not be used anymore to attack IPHFE efficiently.

Second, we look at the method we use in this paper to attack HFEv. In the case of "internal" perturbations we can no longer use our method to differentiate what are the perturbation variables, or put into a more intuitive term, internal perturbation allows the perturbation to be fully "mixed" with the original variables. This is unlike the Oil-Vinegar "mixing" of the HFEv. Therefore we can no longer use the attack method in this paper to attack the IPHFE.

The only possible attack method we can see is the XL method or the method of improved Gröbner basis. But we can not see any reason why they would perform well against our construction, especially after experimenting with some examples. In order to really check how our system can resist such attacks, we need to find out how the attack complexity changes as r changes with a fixed D. Computer simulations should give us some reasonable way of estimating it, but it is in general a rather daunting time consuming task. A referee of our paper pointed out, that the results in [AFI+04], to be presented in Asiacrypt'04, show that the new Gröbner basis algorithm is actually more powerful than the XL method. This implies that we will only need to find out how our new schemes behave under the attack by the new Gröbner basis algorithm. We are now using an implementation of the new Gröbner basis algorithm in Magma to study this problem and preliminary results seem to be very supportive of our speculation on the security of our new schemes.

Overall, in accordance with our own estimates the attack complexity of all existing methods should be at least 2^{80}. We believe that it could be much higher so that the best method to attack the IPHFE system might be brute force, that is, checking all possible answers one by one.

4 Conclusion

In this paper, we presented a new algebraic method to attack the HEFv cryptosystem. This is the first attack using the algebraic structure of the HFEv. The basic idea is to view the new Vinegar variables as an external perturbation and to try to separate them. This method allows us, for the cases when $D+r$ is small, to attack the system efficiently. However, the complexity of such an attack is indeed exponential in terms of r.

Then we used the method of internal perturbation developed by Ding [Din04] to improve the system such that this attack can no longer be applied. It gives us the internally perturbed HFE cryptosystem. This system, at this moment, seems to be very secure and can be implemented efficiently. However more work, in particular, large scale simulation should be done to study the explicit relation between the level of the security and the level of perturbation and confirm the claims in this paper. In general, it seems that internal perturbation is a method that can be used to improve substantially the security of multivariable cryptosystem without sacrificing much of the efficiency of such a system.

Acknowledgment

We would like to thank the anonymous referees for their suggestions. Jintai Ding would also like to thank Dingfeng Ye and Lei Hu for their useful discussions.

References

[ACDG03] Mehdi-Laurent Akkar, Nicolas T. Courtois, Romain Duteuil, and Louis Goubin. A fast and secure implementation of Sflash. In *PKC-2003, LNCS*, volume 2567, pages 267–278. Springer, 2003.

[AFI$^+$04] Gwénolé Ars, Jean-Charles Faugère, Hideki Imai, Mitsuru Kawazoe, and Makoto Sugita. Comparison between XL and Gröbner basis algorithms, 2004. To be presented in *Asiacrypt–2004*.

[CGP03] Nicolas Courtois, Louis Goubin, and Jacques Patarin. Sflash^{v3}, a fast asymmetric signature scheme, 2003. http://eprint.iacr.org.

[Cou01] Nicolas T. Courtois. The security of hidden field equations (HFE). In C. Naccache, editor, *Progress in cryptology, CT-RSA, LNCS*, volume 2020, pages 266–281. Springer, 2001.

[Din04] Jintai Ding. A new variant of the Matsumoto-Imai cryptosystem through perturbation. In F. Bao, R. Deng, and J. Zhou, editors, *Public Key Cryptosystems, PKC-2004, LNCS*, volume 2947, pages 305–318. Springer, 2004.

[FJ03] Jean-Charles Faugère and Antoine Joux. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In Dan Boneh, editor, *Advances in cryptology – CRYPTO 2003, LNCS*, volume 2729, pages 44–60. Springer, 2003.

[GJ79] M. R. Garey and D. S. Johnson. *Computers and intractability, A Guide to the theory of NP-completeness.* W.H. Freeman, 1979.

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In *Eurocrypt'99, LNCS*, volume 1592, pages 206–222. Springer, 1999.

[KS99] Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In M. Wiener, editor, *Advances in cryptology – Crypto '99, LNCS*, volume 1666, pages 19–30. Springer, 1999.

[MI88] T. Matsumoto and H. Imai. Public quadratic polynomial-tuples for efficient signature verification and message encryption. In C. G. Guenther, editor, *Advances in cryptology – EUROCRYPT '88, LNCS*, volume 330, pages 419–453. Springer, 1988.

[Pat95] J. Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In D. Coppersmith, editor, *Advances in Cryptology – Crypto '95, LNCS*, volume 963, pages 248–261, 1995.

[Pat96a] J. Patarin. Asymmetric cryptography with a hidden monomial. In N. Koblitz, editor, *Advances in cryptology, CRYPTO '96, LNCS*, volume 1109, pages 45–60. Springer, 1996.

[Pat96b] J. Patarin. Hidden field equations (HFE) and isomorphism of polynomials (IP): Two new families of asymmetric algorithms. In U. Maurer, editor, *Eurocrypt'96, LNCS*, volume 1070, pages 33–48. Springer, 1996.

[Pat97] J. Patarin. The oil and vinegar signature scheme. *Dagstuhl Workshop on Cryptography, September 1997*, 1997.

[PCG01] Jacques Patarin, Nicolas Courtois, and Louis Goubin. Flash, a fast multivariate signature algorithm. In *LNCS*, volume 2020, pages 298–307. Springer, 2001.

[PGC98] Jacques Patarin, Louis Goubin, and Nicolas Courtois. C^*_{-+} and HM: variations around two schemes of T. Matsumoto and H. Imai. In K. Ohta and D. Pei, editors, *ASIACRYPT'98, LNCS*, volume 1514, pages 35–50. Springer, 1998.

[Sha98] Adi Shamir. Efficient signature schemes based on birational permutations. In *LNCS, Advances in cryptology – CRYPTO '98 (Santa Barbara, CA, 1998)*, volume 1462, pages 257–266. Springer, 1998.