A new variant of the Matsumoto-Imai cryptosystem through perturbation

Jintai Ding

Department of Mathematical Sciences,
University of Cincinnati,
Cincinnati, OH, 45220,
USA
ding@math.uc.edu

Abstract. Though the multivariable cryptosystems first suggested by Matsumoto and Imai was defeated by the linearization method of Patarin due to the special properties of the Matsumoto-Imai (MI) cryptosystem, many variants and extensions of the MI system were suggested mainly by Patarin and his collaborators. In this paper, we propose a new variant of the MI system, which was inspired by the idea of "perturbation". This method uses a set of r (a small number) linearly independent linear functions $z_i = \sum_{j=1}^{n} \alpha_{ij}x_j + \beta_i$, i=1,..,r, over the variables x_i, which are variables of the MI system. The perturbation is performed by adding random quadratic function of z_i to the MI systems. The difference between our idea and a very similar idea of the Hidden Field Equation and Oil-Vinegar system is that our perturbation is internal, where we do not introduce any new variables, while the Hidden Field Equation and Oil-Vinegar system is an "external" perturbation of the HFE system, where a few extra (external) new variables are introduced to perform the perturbation. A practical implementation example of 136 bits, its security analysis and efficiency analysis are presented. The attack complexity of this perturbed Matsumoto-Imai cryptosystem is estimated.
Keywords: open-key, multivariable, quadratic polynomials, perturbation

1 Introduction

Since the invention of the RSA scheme, there has been great interest to seek new public key cryptosystems, which may serve us better for different purposes. One direction to look for such systems is based on multivariable polynomials, in particular, quadratic polynomials. This method relies on the proven theorem that solving a set of multivariable polynomial equations over a finite field, in general, is an NP-hard problem, which, however, does not guarantee the security.

One of the basic ideas to design such a system was started by Matsumoto and Imai [MI], where they suggested to use a map F over a large field $\bar{K}$, a degree n extension of a finite field k. Through identifying $\bar{K}$ as k^n, first, one would identify this map F as a multivariable polynomial map from k^n to k^n, which we call $\tilde{F}$; then, one would "hide" this map $\tilde{F}$ by composing from both sides by two invertible affine linear maps L_1 and L_2 on k^n. This gives a quadratic map

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

from k^n to k^n (by $\circ$, we mean composition of two maps). The map F suggested by Matsumoto and Imai is 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 this scheme was proven insecure under an algebraic attack using the linearization equations by Patarin [P].

Since then, there has been intensive developments by Patarin and his collaborators to find all possible modifications and extensions of the Matsumoto-Imai systems, which are secure. Those ideas to directly extend the Matsumoto-Imai system can be divided into three groups in accordance with the method used.

1) Minus-Plus method [CGP1]: This is the simplest idea among all, namely one takes out (Minus method, which was first suggested in [S]) a few of the quadratic polynomial components of $\bar{F}$, and (or) add (Plus method) a few randomly chosen quadratic polynomials. The main reason to take the "Minus" action is due to security concerns. The Minus (only) method is very suitable for signature schemes. One of them is Sflash [ACDG,CGP], and it was recently accepted as one of the final selections in the New European Schemes for Signatures, Integrity, and Encryption: IST-1999-12324.

2) Hidden Field Equation Method (HFE) [P]: This method is suggested by Patarin to be the strongest. In this case, the difference from the original Matsumoto-Imai system is that F is replaced by the map (function)

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

where the coefficients are randomly chosen and the total degree of F must be small, otherwise the decryption process will become too slow. However a new algebraic attack using both the Minrank method and the relinearization method by Kipnis and Shamir [KS] shows that the number A can not be too small, but if A is big, the system is too slow due to the process of solving the polynomial equation in the decryption process. This is further confirmed by [C,FJ].

3) Hidden Field Equation and Oil-Vinegar Method [CGP2]: After the Hidden Field Equation Method, it is suggested to combine the Hidden Field Equation Method with another new method, Oil-Vinegar method. The basic idea is, on top of the HFE method, to add a few new variables to make the system more complicated. This method is essentially to replace F with an even more complicated function:

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

$$\sum_{i,j}^{A} a_{ij} X^{q^i+q^j} + \sum_{i,j}^{B,B'} b_{i,j} X^{q^i} \bar{X}^{q^j} + \sum_{i,j}^{A'} \alpha_{ij} \bar{X}^{q^i+q^j} + \sum_{i,j}^{B'} \beta'_i \bar{X}^{q^i} + \sum_{i,j}^{B} b_i X^{q^i} + c,$$

where the new Vinegar variables given by the variable $\bar{X}$ is of a small dimension. 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 an exhaustive search on these added small number of variables. For the signature case the search becomes a random selection, which has a good probability to succeed each time, and it continues until a correct answer is found. We recently observed that the attack in [KS] can also be applied here to actually eliminate the small number of added variables and attack the system. The basic idea is to use the algebraic method to find a way to purge out the Vinegar variables.

After all the efforts mentioned above, it seems that all the possible extensions and generalizations of the Matsumoto-Imai system are exhausted, but our construction provides another alternative.

The motivation for our work is to develop new constructions that could be strongly resistant to the algebraic attack [P,KS] and its extensions like XL, but without much sacrifice to the efficiency of the system.

From a very general point of view, the third method above (the HFE and Oil-Vinegar method) can also be interpreted as an extension of a commonly used idea in mathematics and physics, perturbation. Namely a good way to deal with a continuous system often is to "perturb" the system at a minimum scale. The HFE and Oil-Vinegar method can be viewed as a perturbation of the HFE method by the newly added Vinegar variables. However, because of the "Oil-Vinegar" idea, this perturbation, in some sense, is more of an "external" perturbation, where a few extra (external) new variables (Vinegar) are introduced to do so.

For our construction, the idea is very similar, nevertheless, what we suggest is rather an idea of "internal" perturbation. Our perturbation is performed through a small set of variables "inside" the space k^n (therefore they are "internal" variables) and we do **not** introduce any new variables. Namely given a quadratic multivariable system $\bar{F}$ over k^n, we randomly find a surjective affine linear map Z from k^n to k^r with a small dimension r, then we try to "perturb" the system through the small number variables related to Z.

This idea of internal perturbation is a very general idea that can be applied to all existing multivariable cryptosystems.

A suitable example is the case of Matsumoto-Imai system. The perturbation is performed by two steps:

1) first, we randomly choose r (small) linearly independent functions:

$$z_i = \sum_{i}^{n} \alpha_{ij} x_j + \beta_i,$$

where x_i are the variables of $\tilde{F}$, which can be treated as components of a surjective affine linear map Z from k^n to k^r;

2) then, we add randomly quadratic polynomial of z_i to the components of $\tilde{F}$ to define a new map $\bar{\bar{F}}$ to replace $\tilde{F}$:

$$\bar{\bar{F}}(x_1, ..., x_n) = (\tilde{F}_1(x_1, ..., x_n) + f_1(z_1, .., z_r), \tilde{F}_2(z_1, ..., z_n) + f_2(z_1, ..., z_r), \cdots,$$

$$\tilde{F}_n(x_1, ..., x_n) + f_n(z_1, ..., z_r)).$$

The rest is the same as that of the Matsumoto-Imai system.

In this case, the third method above is not applicable here due to the fact that there are no linear terms to mix Oil and Vinegar.

We will call our method hidden perturbation equation method due to the hidden equations that define the perturbation.

The advantages of such new systems include the facts that they may be able to resist well existing algebraic attacks [KS,C], which may make the system very secure, and 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 the application of our general method to the Matsumoto-Imai cryptosystem. Then we will present a practical implementation example with 136 bits for the perturbation of a Matsumoto-Imai system, where we choose r to be 6. We will show that it should have a very high security level against all the known attacking methods. We will analyze the security and efficiency of the system and compare them with other multivariable cryptosystems with similar parameters.

2 Perturbation of Matsumoto-Imai system

2.1 The original Matsumoto-Imai Cipher

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. In general, the condition of characteristic 2 is not necessary, then we should modify the system slightly due to the multiplicity concern of the final map.

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

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

such that

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

Let

$$F(X) = X^{1+q^i},$$

over $\bar{K}$ such that g.c.d.$(1 + q^i, q^n - 1)$= 1.

F is an invertible map and its inverse is given by

$$F^{-1}(X) = X^t,$$

where $t(1+q^i) = 1$ modulo $(q^n - 1)$.

Let $\tilde{F}$ be a map over k^n and

$$\tilde{F}(x_1, ..., x_n) = \phi \circ F \circ \phi^{-1}(x_1, ..., x_n)$$

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

Here $\tilde{F}_i(x_1, ..., x_n)$ are quadratic polynomials of n variables.

Let L_1 and L_2 be two randomly chosen invertible affine linear maps over k^n.

$$\bar{F}(x_1, ..., x_n) = L_1 \circ \tilde{F} \circ L_2(x_1, ..., x_n)$$

$$= (\bar{F}_1(x_1, ..., x_n), \bar{F}_2(x_1, ..., x_n), \cdots, \bar{F}_n(x_1, ..., x_n))$$

is the cipher suggested by Matsumoto-Imai, which was defeated by the algebraic attack using linearization equations by Patarin.

2.2 The perturbed Matsumoto-Imai cipher

Let r be a small number and

$$z_1(x_1, ..., x_n) = \sum_1^n \alpha_{j1} x_j + \beta_1,$$

$$\cdots$$

$$z_r(x_1, .., x_n) = \sum_1^n \alpha_{jr} x_j + \beta_r,$$

be a set of randomly chosen linear functions of x_i over k^n such that the terms of degree one are linearly independent. Let

$$Z(x_1, ..., x_n) = (z_1, \cdots, z_r) = (\sum_i^n \alpha_{i1} x_j + \beta_1, \cdots, \sum_i^n \alpha_{ir} x_j + \beta_r),$$

which gives a map from k^n to k^r.

Let

$$\bar{\bar{F}}(x_1, ..., x_n) = (\bar{\bar{F}}_1(x_1, ..., x_n), \bar{\bar{F}}_2(x_1, ..., x_n), \cdots, \bar{\bar{F}}_n(x_1, ..., x_n))$$

$$= (\tilde{F}_1(x_1, ..., x_n) + f_1(z_1, .., z_r), \tilde{F}_2(z_1, ..., z_n) + f_2(z_1, ..., z_r), \cdots,$$
$$\tilde{F}_n(x_1, ..., x_n) + f_n(z_1, ..., z_r)),$$

where f_i are randomly chosen quadratic polynomials with r variables.

Let $f(z_1, .., z_r) = (f_1(z_1, .., z_r), f_2(z_1, ..., z_r), \cdots, f_r(z_1, ..., z_r))$ and f can be viewed as a map from k^r to k^n. Let P be the set consisting of the pairs (λ, μ), where λ is a point that belongs to the image of f, and μ is the set of pre-images of λ under f. We call P the perturbation set. Here, we know that P has q^r elements probabilistically, and it does not include any pair whose first component is the zero vector.

We call $\overline{\overline{F}}$ a perturbation of $\tilde{F}$ by Z.

$$\hat{F}(x_1, ..., x_n) = L_1 \circ \overline{\overline{F}} \circ L_2(x_1, ..., x_n) = (y_1(x_1, ..., x_n), ..., y_n(x_1, ..., x_n)),$$

where y_i are quadratic polynomial components of $\hat{F}$. We call $\hat{F}$ the perturbed Matsumoto-Imai cipher.

Let $\tilde{f}(x_1, .., x_n) = f(z_1(x_1, ..., x_n), .., z_r(x_1, ..., x_n))$, which is a map from k^n to k^n. We can see that

$$\hat{F}(x_1, ..., x_n) = L_1 \circ \tilde{F} \circ L_2 + L_1 \circ \tilde{f} \circ L_2(x_1, ..., x_n),$$

and the perturbation is performed by just adding $L_1 \circ \tilde{f} \circ L_2(x_1, ..., x_n)$ to the original Matsumoto-Imai cipher.

We can use it to establish a public key cryptosystem.

2.3 The public key

The public key include

1) the field k including its addition and multiplication structure;

2) the n quadratic polynomials $y_1(x_1, ..., x_n), ..., y_n(x_1, ..., x_n)$.

2.4 Encryption

Given a message vector $M = (x'_1, ..., x'_n)$ as the plaintext, the ciphertext is the vector

$$(y'_1, ..., y'_n) = (y_1(x'_1, ..., x'_n), ..., y_n(x'_1, ..., x'_n)).$$

2.5 The private key and the decryption

The private key includes:

1) the map F,

2) the set of linear functions $z_1, ..., z_r$,

3) the set of points in P (or the set of the polynomials $f_i(z_1, ..., z_r)$),

4) the two affine linear maps L_1, L_2.

2.6 Decryption

Once we have the ciphertext $(y'_1, ..., y'_n)$, the decryption includes the following steps:

I) compute $(\bar{y}_1, ..., \bar{y}_n) = L_1^{-1}(y'_1, ..., y'_n)$;

II) take all the elements one by one (λ, μ) in P, compute

$$(y_{\lambda 1}, ..., y_{\lambda n}) = \phi^{-1} \circ F^{-1}((\bar{y}_1, ..., \bar{y}_n) + \lambda),$$

and check if $Z(y_{\lambda 1}, ..., y_{\lambda n})$ is the same as the corresponding μ, if no, discard it, if yes, go to next step;

III) compute $(x_{\lambda 1}, ..., x_{\lambda n}) = L_2^{-1} \circ \phi(y_{\lambda 1}, ..., y_{\lambda n})$. If there is only one solution, it is the plaintext. However, it is very possible that we have more than one solution, then we can use the same technique as suggested for the HFE method, namely we can use a few hash functions to differentiate which one is the right one. In our computer experiments, it seems that, in general the multiplicity seems to be surprisingly small, and the multiplicity of solutions behaves as expected like that of randomly chosen functions.

We call our system a perturbed Matsumoto-Imai cryptosystem (PMI). It is evident that our method is a very general method that it can be used to perturb any multivariable cryptosystem, such as that the HFE cryptosystem. After perturbation, the security should be much stronger, but the decryption process is slower (by a factor of q^r).

3 A practical implementation

For practical use, we suggest a 136 bits implementation of the PMI system.

We choose k to be F_2.

We choose $\bar{K}$ to be an 136 degree extension of F_2 and

$$g(x) = 1 + x + x^2 + x^{11} + x^{136}.$$

We choose r to be 6, which means the dimension of the perturbation space is 6.

We choose

$$F(X) = X^{2^{5\times 8}+1},$$

In general, to have a security level of 2^{80}, we suggest n to be at least 96 and r not less than 5. Our implementation example has a much stronger security level at around 2^{136}.

3.1 Implementation

Public key size The public key contains 136 quadratic polynomials. Each polynomial has $136 \times 137/2$ quadratic terms, 136 linear terms and one constant term. The key size is about 100K bytes, which is rather big, but should not be a problem for any PC.

Encryption computation complexity For encryption, we need to compute the value of a set of quadratic polynomials for a given set of $x_1, ..., x_n$, we can rewrite a quadratic polynomial in the following way:

$$\sum_1^n x_i (b_i + \sum_{j=i}^n a_{i,j} x_j) + c,$$

which allows us to compute the value at roughly one and an half times of the speed of a direct calculation. Therefore we need roughly 19,000 binary (including both addition and multiplication) operations to calculate the value of each polynomial. Therefore, on average, each message bit needs 19,000 binary operations.

Private key size The private key is much smaller in general, the main parts are: the 8 linear functions z_i, which is of the size 127×8 bits, the two linear transformations L_1 and L_2 and their inverses, which needs $127 \times 128 \times 4$ bits and the perturbation set P, which needs roughly $64 \times 3 \times 64$ bits. The total is around 80,000 bits.

Decryption computation complexity For decryption, we need first calculate the action of L_1^{-1} on the ciphertext vector, which needs roughly $136 \times 136 + 136$ calculations, which can be neglected compared to the computations required for the second step. The same is true for the third step. The main part of the decryption process is the step II, where we need to calculate 64 times the values of F^{-1} and the values of z_i and compare it with the second components of the corresponding element in P. The main part surely is to calculate F^{-1}. Due to the linearization method by Patarin, we can actually find F^{-1} by solving a set of homogeneous linear equations. In this case, we will implement a fast algorithm to accomplish this as follows.

1) We identify $\bar{K}$ as a degree 17 extension of a field $\tilde{K}$, which is a degree 8 extension over F_2. In this case we can identify $\bar{K}$ as $\tilde{K}^8$.

2) The map $F(X) = X^{2^{5\times 8}+1}$ can then be identified again as a quadratic map on $\tilde{K}^8$. Then with the relinearization by Patarin, finding the inverse of K becomes the process of solving a set of 17 homogeneous linear equations of rank 16, and then solving an equation in the form $x^2 = b$ over the field $\tilde{K}$.

3) This process can be performed by making a multiplication table for the field $\tilde{K}$. The table takes $2^{16} \times 24$ bits and each search is on a space of 2^{16} bits. Overall, each F^{-1} calculation becomes a process mainly to solve a set of 17 linear equations over the field $\tilde{K}$. Because the message is 136 bits, one can conclude that the decryption process will take roughly half of the time to solve a 17 linear equations over $\tilde{K}$ per bit.

We may also use the algorithm in [ACDG] to make this process even faster.

3.2 Security Analysis

In general, a set of 136 quadratic polynomials with 136 variables, are difficult to solve. However, special methods are invented to attack specially designed systems. The Matsumoto-Imai system itself is not secure, which mainly is due to the linearization attack. Namely, any given a plaintext $(x_1, ..., x_n)$ and its ciphertext $(y_1, ..., y_n)$ satisfy a set of linearization equations in the form

$$\sum_i x_i \sum_j a_{i,j} y_j = 0.$$

These equations essentially allow us to find enough linear equations satisfied by the plaintext from a ciphertext to defeat the system. Since then, new methods have been invented to attack multivariable cryptosystems, mainly the algebraic method [KS] and its extension the XL method, and for the case of Matsumoto-Imai Minus system, a method to search for "missing" terms.

Next, we will analyze one by one the impact of all the existing attacking methods on the perturbed Matsumoto-Imai system.

The attack by linearization method From the name, we can see the PMI system should have a lot in common with the original MI system.

Let

$$H_1 = \{Y|Y = \sum_i a_i \bar{F}_i(x_1, ..., x_n)\},$$

where $\bar{F}_i$ are components of the original Matsumoto-Imai cipher.

Let

$$H_2 = \{Y|Y = \sum_i a_i \bar{y}_i(x_1, ..., x_n)\},$$

where $\bar{y}_i$ are components of the perturbed Matsumoto-Imai cipher.

Let

$$H_3 = H_1 \cap H_2.$$

Because the perturbation dimension is 6, the dimension of all the linear and quadratic polynomials of a dimension 6 space of F_2 is 21, where 15 are from quadratic terms and 6 are from linear terms, the dimension of H_3 is, therefore 115=136-21. Intuitively, one can view our system as if we take out 21 terms out of the total 136 public polynomials. This clearly eliminates all the possible linearization equations, which we confirm by our computer experiment. Therefore, the linearization method cannot be applied here to attack the system.

The attack methods related to the MI Minus systems The MI Minus systems are suggested for signature purpose. The method simply takes out a few public quadratic polynomials (Minus method) to improve the security. The main attack method of this system is to search for quadratic polynomials we can add to the system such that it becomes the original MI system. The search process uses the property that the map F is a permutation polynomial on the field $\bar{K}$. This will allow the algebraic attack using linearization equations by Patarin to be applied successfully again.

For the PMI case, this method is not applicable due to mainly two reasons.

1) In the PMI systems, the perturbed map is not any more an injective (also not surjective) map, therefore the properties of permutation polynomials can no longer be applied here to search for the missing terms, because no terms is actually missing.

2) For our case, finding the "missing terms" is essentially to purge out the perturbation. For the pure Matsumoto-Imai Minus system, the attacker uses the fact that there is a good set of polynomials, namely the given polynomials actually come from the original MI system. For our case this is no longer the case, as all terms are mixed together. Therefore, there does not exist a good way to find the subspace of dimension 115 of the polynomials from the original MI system, namely the subspace H_3. One possible way is certainly just to guess which one is from H_3 and the probability to guess a right one is 1/64, which is

not bad at all. The problem is that we have no way to judge if anyone is the right guess or not. We conclude it is essentially impossible to find the missing terms through this way.

The PMI and the Matsumoto-Imai Plus-Minus systems can be viewed in a very similar way. The similarity is that in the PMI system, we take out 21 quadratic polynomials, and add 21 new polynomials, except that in our case, we did not add randomly 21 polynomials, but 21 perturbed polynomials. The attack on the Matsumoto-Imai Plus-Minus system is essentially the XL method, which we will discuss below.

The attack methods on the HFE The special advantage of the perturbed MI system, is its resistance to the algebraic attack methods that first was suggested for attacking the HFE systems. The basic attacking point of the algebraic attack method [KS] is that the quadratic part of the HFE: $\sum_{i,j}^{A} a_{ij} X^{q^i+q^j}$ can be viewed as a quadratic form with its variables being X^{q^i}, and the attack is to find a transformation to reduce a quadratic form into the above form with low rank using Minrank method. For the PMI systems, this method is not applicable due to the fact that there is no way that when using the above method, the perturbed polynomials can be rewritten into low rank quadratic form. The reason for this is that, in the attack process using the algebraic method in [KS], the map Z from k^{136} to k^6 is lifted as an embedding map $\bar{Z}$ from k^n to k^n:

$$\bar{Z}(x_1, ..., x_n) = (Z(x_1, ..., x_n), 0, .., 0);$$

then it is further lifted as a k affine linear map from $\bar{K}$ to $\bar{K}$ in the form of

$$\tilde{Z}(X) = \sum_{i}^{\bar{A}} a_j X^{q^i},$$

where the highest term $\bar{A}$ should be at least 130, because the dimension of the pre-image of any point of this map is 130. Therefore, from the analysis of the efficiency of this method [KS,C], we know it should take much more than 2^{136} computations to defeat the system by this method. This suggests that it should resist other related attacks as well [CDF,FJ].

XL attack The XL method is a very general method for solving multivariable equations. This method can be viewed as a generalization of the algebraic attack using linearization equations, where one basically has to search for functions of only one variable in the ideal generated by $Y_i = y_i(x_1, ..., x_n) - y'_i$ by looking at linear combinations of terms like

$$\sum_{l \le D-2} a_{i_1 i_2 i_3 \dots i_l} x_{i_1} x_{i_2} x_{i_3} \dots x_{i_l} Y_i,$$

where y_i is the i-th public polynomial and y'_i is the corresponding component of the ciphertext. The success of this method depends on the degree D. In

[CKPS], there is an argument about asymptotic growth of the complexity to attack a system with more equations than variables, but no final conclusion about the complexity is given. What is given are estimates based on some computer experiments, in particular, the case when there are 2 or more equations than variables, which for our case can be easily achieved by guessing values of any 2 variables. According to their estimate, for our case, D should be 12, which is given by the square root of 136, and the XL attack needs to do a Gaussian elimination on about 136!/124!12! roughly 2^{55} variables, which requires more than 2^{136} operations.

For the case of F_2, there exist improved versions of XL [CP], for example, by adding the equations $x_i^2 = x_i$ into the system and one may argue that the PMI system is not a general system, but a system based on the perturbation of the MI system. Therefore the attack complexity might be different. It is reasonable to believe that D should be determined by r in our case. For this, we did some computer experiments, which suggests that the security level is about the level mentioned above. But our experiment is on a much smaller scale ($n = 27, r = 3$). There is some evidence suggesting that D should be roughly $r(r-1)/2$, when n is much bigger than r. According to such an estimate, the complexity of the attack is bigger than 2^{100}. However this formula is not a proven formula, but a conjecture, and it is an open question to find a precise formula of D for the PMI system in terms of both n and r, which then will tell us how we should choose r given n to ensure the desired security.

From, the argument, we believe (not proven) that, with all the known attack methods, the security of our system has the attack complexity of 2^{100}.

3.3 Comparison with other cryptosystem

In this section, we would like to compare our system with other cryptosystems.

Comparison with RSA In the case of RSA, we know that a minimum of 512 bits is required at this moment to ensure a security level of 2^{100}. First the key size of RSA surely is very small for both private key and public keys, much smaller than the PMI system.

The case of public and private computation complexity is however a different story. In the encryption and decryption process, each needs roughly 512 multiplications of two numbers of 512 bits modulo a number of 512 bits to process a message 512 bits long. Therefore, each bit of information requires two operations of multiplying two numbers with 512 bits modulo a 512 bits long number.

The conclusion is that the public key size for the PMI system is much bigger than for the RSA system, (1M versus 1.5K) which however should not be a problem for any PC. In terms of per bit efficiency, the comparison is between, on one hand, the RSA, which requires two multiplications of two 512 bit number modulo another 512 bit number, on the other hand, the PMI system, which is an operation to solve 17 linear equation over a finite field of size 2^8 with a given multiplication table. Our preliminary test indicates that the PMI is much faster.

However this is based on our own implementation and the assumption of the security of the system. The situation will be different if we have to increase r for security purpose. If we assume that our system is secure, and since the key transmission is only a one time transaction, when substantial use is required, the PMI system could be better than the RSA system.

Comparison with other multivariable cryptosystems The implementation of multivariable cryptosystem is for either authentication purpose or encryption purpose.

The main examples of signature schemes are Quartz schemes, which are based on the HFE and Oil-Vinegar method, and the Sflash schemes, which are based on the Matsumoto-Imai Minus Method. Both of them were accepted for submission to the New European Schemes for Signatures, Integrity, and Encryption: IST-1999-12324, and Sflash was accepted in the final selection.

Current multivariable schemes that are still deemed secure and practical for encryption purpose are basically the HFE scheme, and the HFE and Oil-Vinegar schemes.

In terms of a broader point of view, the Matsumoto-Imai Minus-Plus method can also be viewed as a form of perturbation, except that the perturbation is done through taking out components and adding randomly more components. In this case, each component taken out means a one dimensional exhaustive search in the decryption process and if r components are taken out then a search on an r dimensional space is needed. However for our case, if we perturb by an r dimensional space, we basically perform an $r(r+1)/2$ dimensional Minus and then Plus operation, except here the Plus operation is not just to add randomly a set of components, rather a set of "perturbed" components. In this context, we believe our perturbation method is a better choice compared with the Matsumoto-Imai Minus-Plus system.

It is surely possible to modify the PMI system by the Minus method for a signature scheme as well. What we believe is that it will be a more secure but slower scheme. This is because the perturbed map is not bijective as is case for MI, and therefore one might have to go through a random search process during the signature process.

As we explained above, the idea of HFE is to replace the map F by a small degree map

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

but the degree cannot be too small due to the algebraic attack [KS] and the XL attack. For the case of a 128 bits implementation over F_2, the degree needs to be 2^{11} to ensure security level as in our implementation example. However to solve a degree 2^{11} polynomial equation on the 128 bits field, it needs about $2^{22} \times 128$ computations over the field to solve the equation for the decryption process, which is much slower than our scheme. Therefore, we believe that the PMI is a better scheme if our claim on the security is right, otherwise some version of HFE mixed with PMI will be even better.

Due to the fact that the HFE and Oil-Vinegar scheme is an "external" perturbation, namely a new set of variables is introduced to perturb the system. However, our recent observation shows that due to the nature of the "external" perturbation, we can extend the algebraic method [KS] from one variable to two variables case. It seems that we can actually use this generalized algebraic method of that in [KS] to purge out the perturbation if the polynomial F for the HFE equation before the perturbation is small. Once this is done, the original algebraic method [KS] and the XL can be used to attack the system again. Therefore, we think the security of the HFE and Oil-Vinegar scheme is based on the security of HFE part not the oil vinegar part [CDF,FJ]. The detail of this work will be given in a separate paper.

4 Discussion

This paper is a suggestion of a new multivariable cryptosystem, the Perturbed Matsumoto-Imai system, the PMI system. This new system is based on a new theoretical idea of "internal" perturbation. The practical scheme we suggest is an implementation of the idea that creates a 136 bits open-key cryptosystem and the key size is big (1M). However the main purpose of this paper is to introduce the theoretical idea of "internal" perturbation, which, we believe, is a very general and applicable idea. Actually our perturbation idea is not just restricted to the MI systems. We realizes actually it may be a much better idea to combine the HFE method with our "internal" perturbation method, rather than the "external" Oil-Vinegar scheme, namely we will perturb the HFE with a small subspace inside and we do not introduce any new variables. The security is improved because of the perturbation and the impossible task to purge out the perturbation. The reason for this is exactly due to the fact that it is internal, which therefore is fully mixed into the system unlike the case of Oil-Vinegar mixing.

The argument about security and efficiency in this paper is based on intuitive and rough ideas and not on strict mathematical arguments. We do not understand why we can do so as well and we believe it is a very interesting problem. Therefore, we plan to perform more computer simulations, which may give some ideas how things really are.

Acknowledgments

We thank the referee for suggestions. We thank Professor Dingfeng Ye and Professor Dieter Schmidt for useful discussions. Our research is partially supported by the Taft Fund at the University of Cincinnati

References

[ACDG] Mehdi-Laurent Akkar, Nicolas T. Courtois, Romain Duteuil, Louis Goubin, *A Fast and Secure Implementation of Sflash* Volume 2567, pp 267-278 Lecture Notes in Computer Science

[C] Nicolas T. Courtois *The Security of Hidden Field Equations (HFE)*, Volume 2020, pp 0266 Lecture Notes in Computer Science

[CDF] Nicolas Courtois, Magnus Daum and Patrick Felke, *On the Security of HFE, HFEv- and Quartz*, PKC 2003, LNCS 2567, Springer, pp. 337-350.

[CP] Nicolas Courtois, Jacques Patarin, *About the XL Algorithm over* $GF(2)$, Volume 2612, pp 141-157 Lecture Notes in Computer Science

[CGP] Nicolas Courtois, Louis Goubin, Jacques Patarin, FLASH, a Fast Multivariate Signature Algorithm, Volume 2020, pp 0298 Lecture Notes in Computer Science

[CGP1] Jacques Patarin, Louis Goubin, Nicolas Courtois, *C-+* and HM: Variations around Two Schemes of T. Matsumoto and H. Imai* Volume 1514, pp 0035 Lecture Notes in Computer Science

[CGP2] Jacques Patarin, Nicolas Courtois, Louis Goubin QUARTZ, 128-Bit Long Digital Signatures, Volume 2020, pp 0282 Lecture Notes in Computer Science

[CKPS] Nicolas Courtois, Alexander Klimov, Jacques Patarin, Adi Shamir *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations*, Volume 1807, pp 0392 Lecture Notes in Computer Science

[Dm] Dickerson, Matthew, *The inverse of an automorphism in polynomial time.* J. Symbolic Comput. 13 (1992), no. 2, 209–220.

[KS] Aviad Kipnis, Adi Shamir, *Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization* Volume 1666, pp 0019, Lecture Notes in Computer Science

[FJ] Jean-Charles Faugère, Antoine Joux, *Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases* Advances in cryptology – CRYPTO 2003, Dan Boneh (ed.), Volume 2729, Lecture notes in computer Sciences, Springer, New York 2003

[MI] Matsumoto, T., Imai, H., *Public quadratic polynomial-tuples for efficient signature verification and message encryption*, Advances in cryptology – EUROCRYPT '88 (Davos, 1988), 419–453, Lecture Notes in Comput. Sci., 330, Springer, Berlin, 1988.

[P] Patarin, J., *Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88.*, Des. Codes Cryptogr. 20 (2000), no. 2, 175–209.

[P1] Patarin, J., *Hidden field equations and isomorphism of polynomials*, Eurocrypto'96, 1996.

[S] Shamir, Adi, *Efficient signature schemes based on birational permutations*, Advances in cryptology – CRYPTO '98 (Santa Barbara, CA, 1998), 257–266, Lecture Notes in Comput. Sci., 1462, Springer, Berlin, 1998.