MI-T-HFE, a New Multivariate Signature Scheme

Wenbin Zhang and Chik How Tan

Temasek Laboratories
National University of Singapore
tslzw@nus.edu.sg and tsltch@nus.edu.sg

Abstract. In this paper, we propose a new multivariate signature scheme named MI-T-HFE as a competitor of QUARTZ. The core map of MI-T-HFE is of an HFEv type but more importantly has a specially designed trapdoor. This special trapdoor makes MI-T-HFE have several attractive advantages over QUARTZ. First of all, the core map and the public map of MI-T-HFE are both surjective. This surjectivity property is important for signature schemes because any message should always have valid signatures; otherwise it may be troublesome to exclude those messages without valid signatures. However this property is missing for a few major signature schemes, including QUARTZ. A practical parameter set is proposed for MI-T-HFE with the same length of message and same level of security as QUARTZ, but it has smaller public key size, and is more efficient than (the underlying HFEv- of) QUARTZ with the only cost that its signature length is twice that of QUARTZ.

Keywords: post-quantum cryptography, multivariate signature scheme, QUARTZ, HFEv

1 Introduction

Multivariate public key cryptosytems (MPKCs) are constructed using polynomials and their public keys are represented by a polynomial map $F = (f_1, \ldots, f_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ where $\mathbb{F}_q$ is the field of q elements and each f_i is a polynomial. The security of MPKCs relies on the following MP problem:

MP Problem Solve the system $f_1(\mathbf{x}) = 0, \ldots, f_m(\mathbf{x}) = 0$, where each f_i is a polynomial in $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{F}_q^n$ and all coefficients are in $\mathbb{F}_q$.

This problem is usually called the MQ problem if the degree of the system is two; namely each f_i is a quadratic polynomial. The MP problem is NP-hard if the degree is at least two [GJ79]. Especially the MQ problem is also NP-hard in general. Based on this NP-hardness and along with its computational efficiency, MPKCs is considered as a potential candidate for post-quantum cryptography.

To use polynomial maps $F = (f_1, \ldots, f_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ for public key cryptography, one needs to design trapdoors in the polynomial maps. Currently the most common construction of such a trapdoor is of the following bipolar form [DY09]:

$$\bar{F} = L \circ F \circ R : \mathbb{F}_q^n \xrightarrow{R} \mathbb{F}_q^n \xrightarrow{F} \mathbb{F}_q^m \xrightarrow{L} \mathbb{F}_q^m$$

where L, R are invertible affine maps and $F = (f_1, \ldots, f_m)$ is a polynomial map. The public key is $\bar{F}$ while the secret key usually consists of L, R, F. It should be efficient to invert the central map F but infeasible to invert $\bar{F}$ unless one knows L, R, F.

In MPKCs multivariate polynomials can be used for both encryption schemes and signature schemes, and encryption schemes can often be converted to signature schemes, but here we shall focus on signature schemes only. The public key of a multivariate signature scheme is a specially designed polynomial map $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$, a message is a vector $\mathbf{y} \in \mathbb{F}_q^m$ and a signature is a vector $\mathbf{x} \in \mathbb{F}_q^n$. Given any message $\mathbf{y}$, the signer need to solve the equation $F(\mathbf{x}) = \mathbf{y}$ using the trapdoor to find a solution as a signature $\mathbf{x}$. The verifier verifies if a signature $\mathbf{x}$ is valid by checking if it satisfies the equation $F(\mathbf{x}) = \mathbf{y}$. Notice that any message should have valid signatures in general. Hence F should be a surjective map, or otherwise there should be a good control on those invalid messages, i.e., those messages having no valid signatures. However having a good control on invalid messages may be troublesome, so it is preferred to have F being surjective.

Since the famous Matsumoto-Imai (MI) cryptosystem [MI88] was proposed in 1980's, various multivariate encryption and signature schemes have been constructed. The MI cryptosystem was broken by Patarin in 1995 [Pat95], but it has influenced many important variants. A few of them are to modify the MI cryptosystem by simple methods, such as FLASH for signature [PCG99] and Ding's internal perturbation of MI for encryption [Din04]. However all these simple modification of MI turned out to insecure. In 1996, Patarin [Pat96] proposed the famous Hidden Field Equation (HFE) encryption scheme which has been developed into a big family. Though the original HFE has been thoroughly broken [KS99, GJS06, BFP13], some of its variants still survive until now, such as HFEv for encryption and HFEv- for signature, especially QUARTZ as an instance of HFEv- [PCG01]. Inspired by the linearization attack to the MI cryptosystem, Patarin proposed the Oil-Vinegar (OV) signature scheme [Pat97]. OV was broken soon, but its variant Unbalanced Oil-Vinegar signature scheme [KPG99] and Rainbow [DS05b] survive until now. There were also many other schemes intended for signatures, but major signature schemes that remain secure are HFEv, HFEv-, QUARTZ, UOV, Rainbow, etc. However, the public map of HFEv, HFEv- generally cannot be surjective because their central polynomials are chosen randomly with restriction only on the degree. For UOV and Rainbow, it is not guaranteed that any message do have a valid signature though the failure probability is very small. So to implement these schemes in practice, one still has to handle those invalid messages.

In this paper, we propose a new multivariate signature scheme, named MI-T-HFE, to resolve the problem on surjectivity while maintaining efficiency and security. The core map of MI-T-HFE is a definitely surjective polynomial map, indeed an HFEv polynomial, and thus its public map is also surjective. The design of MI-T-HFE is motivated by the idea of [ZT14] where they propose a double perturbation of

the MI cryptosystem by two perturbation methods, triangular perturbation and dual perturbation. Here we also modify the MI cryptosystem by two maps, an extended version of triangular maps and a special type of HFEv polynomials. The final map of this modification is an HFEv polynomial which has a large number of vinegar variables. This construction can also be viewed as an HFEv polynomial with a trapdoor embedded in its vinegar variables. In the name MI-T-HFE, MI, T and HFE stand for the MI cryptosystem, triangular perturbation and HFE polynomials respectively. Compared to QUARTZ, the signature generation of MI-T-HFE can be performed much faster, and MI-T-HFE can have smaller public key size. We examine the security of this construction against current main attacks in multivariate public key cryptography, and show that it can have the same level of security as QUARTZ.

This paper is organized as follows. Section 2 is a brief review of some previous results to be used in this paper. Our new signature scheme MI-T-HFE is then constructed in Section 3. Section 4 is devoted to the cryptanalysis of MI-T-HFE, then followed by a practical example given in Section 5. Finally Section 6 concludes this paper.

2 Preliminaries

In this section, we shall briefly review a few previous results which will be used in the rest of this paper.

2.1 The Matsumoto-Imai Cryptosystem

We first recall the Matsumoto-Imai (MI) cryptosystem [MI88] as follows. Let q be a power of 2, $\mathbb{K}$ a degree n extension of $\mathbb{F}_q$ and $\phi : \mathbb{K} \to \mathbb{F}_q^n$ the standard $\mathbb{F}_q$-linear map

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

Let θ be an integer such that, $0 < \theta < n$ and $\gcd(q^\theta + 1, q^n - 1) = 1$. Define the following simple polynomial

$$\tilde{F} : \mathbb{K} \to \mathbb{K}, \quad \tilde{F}(X) = X^{1+q^\theta}.$$

This polynomial $\tilde{F}$ is invertible and its inverse is $\tilde{F}^{-1}(Y) = Y^\eta$ where $\eta(1 + q^\theta) \equiv 1 \mod q^n - 1$.

The MI cryptosystem uses $F = \phi \circ \tilde{F} \circ \phi^{-1} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ as the central map and its public map is constructed from F by composing two invertible affine transformation at the two ends $\bar{F} = L \circ F \circ R$. Since F is invertible, the MI cryptosystem is an encryption scheme. For convenience, we shall call such an F an MI map.

2.2 HFE

After breaking the MI cryptosystem [Pat95], Patarin then proposed Hidden Field Equations (HFE) for encryption in 1996 [Pat96] which significantly influences the development of multivariate public key cryptography.

Let q be a power of a prime (odd or even) and $\mathbb{K}$ a degree n extension of $\mathbb{F}_q$. HFE uses the following type of polynomials over $\mathbb{K}$ as the central map

$$H(X) = \sum a_{ij} X^{q^i+q^j} + \sum b_i X^{q^i} + c.$$

where the coefficients are randomly chosen in $\mathbb{K}$ and the degree of H is bounded by a relatively small number D. We shall call such an F an HFE map (polynomial).

The parameter D determines the efficiency and security level of HFE. $H(X) = Y$ can be solved by Berlekamp's algorithm and the complexity is known as

$$O(nD^2 \log_q D + D^3)$$

So it can be efficient if $\deg(H) \leq D$ is small enough. However, it is first found that D cannot be too small otherwise it can be broken by attacks [KS99, Cou01, FJ03], and later on HFE was thoroughly broken by [GJS06, BFP13].

2.3 HFEv

Though HFE has been broken, some simple modification can make it secure against those attacks to HFE: HFEv which adds vinegar variables and HFEv- which deletes a few components from the public map.

HFEv uses the following type of polynomials as the central map

$$H(X, V) = \sum a_{ij} X^{q^i+q^j} + \sum b_{ij} X^{q^i} V^{q^j} + \sum c_{ij} V^{q^i+q^j} + \sum d_i X^{q^i} + \sum e_i V^{q^i} + f$$

where the degree of X is bounded by a relatively small parameter D but the degree of V can be arbitrary high. In addition, V varies only in a certain subspace of $\mathbb{K}$ of dimension v corresponding to the subspace $\mathbb{F}_q^v$ of $\mathbb{F}_q^n$. To invert H, one first assign a random value to V and then H is reduced to an HFE polynomial and thus can be solved by Berlekamp's algorithm. If HFEv is used for encryption, the parameter v should be small so that decryption won't be too slow.

HFEv- is HFEv with a few components deleted from the public map. It is intended for signature schemes. The most famous example of HFEv- is QUARTZ [PCG01] which has parameters $(q, D, n, v, r) = (2, 129, 103, 4, 3)$ where r is the number of components deleted.

The central polynomials of HFE, HFEv and HFEv- are randomly chosen with only one restriction on the degree, so the probability that are surjective is very small. Additional effort is then necessary to take care of those messages without valid signatures when using them for signature schemes. This could be quite troublesome, so a signature scheme with the public map being surjective is still preferred.

2.4 Triangular Maps and Perturbation

Triangular maps are of the following form

$$G(\mathbf{x}) = \begin{pmatrix} x_1 \\ x_2 + g_1(x_1) \\ \vdots \\ x_n + g_{n-1}(x_1, \ldots, x_{n-1}) \end{pmatrix}$$

where $g_1, \ldots, g_s$ are randomly chosen polynomials. The great advantage of this triangular structure is that G is bijective and it is very easy to solve $G(\mathbf{x}) = \mathbf{y}$ inductively.

In [ZT14], triangular maps are turned into a modification method, called triangular perturbation. Their method is to add to the central map the following triangular map

$$G(\mathbf{x}) = G(\mathbf{x}_1, \mathbf{x}_2) = \begin{pmatrix} x_{n+1} + g_1(\mathbf{x}_1) \\ x_{n+2} + g_2(\mathbf{x}_1, x_{n+1}) \\ \vdots \\ x_{n+s} + g_s(\mathbf{x}_1, x_{n+1}, \ldots, x_{n+s-1}) \end{pmatrix}$$

Namely, the modified central map is

$$F'(\mathbf{x}) = F(\mathbf{x}_1) + S \cdot G(\mathbf{x}_1, \mathbf{x}_2)$$

where S is a randomly chosen $m \times s$ matrix. Triangular perturbation can preserve the efficiency and surjectivity of the original scheme, because $G(\mathbf{x}_1, \mathbf{x}_2) = \mathbf{y}$ always has a solution $\mathbf{x}_2 = (x_{n+1}, \ldots, x_{n+s})$ for any $\mathbf{x}_1, \mathbf{y}$ and $x_{n+1}, \ldots, x_{n+s}$ can be computed straightforward by induction. However it cannot enhance the security if it is applied alone as its triangular structure is vulnerable to high rank attack.

In [ZT14], they also propose another modification method, called dual perturbation, and a new signature scheme by combining the two methods. They claim that the two methods can protect each other to resist current attacks. However we find that their scheme is indeed insecure. The reason is that their dual perturbation can be simplified as adding a random polynomial only on the second part of the variables after a linear transformation on the variables, and thus can be removed, contradicting their claim on the security.

3 The New Multivariate Signature Scheme MI-T-HFE

Though the construction of [ZT14] is insecure due to the failure of dual perturbation, we find that their idea of double perturbation, i.e., using two maps to protect each other remains interesting. In this section, we will apply their idea to embed a trapdoor into HFEv and thus construct a new signature scheme, named MI-T-HFE.

3.1 Preparation

Before giving the construction of MI-T-HFE, we shall first introduce two types of polynomial maps. The first type of polynomial map is an extended version of triangular maps,

$$G(\mathbf{x}) = G(\mathbf{x}_1, \mathbf{x}_2) = \begin{pmatrix} \phi_1(x_{n+1}) + g_1(\mathbf{x}_1) \\ \phi_2(x_{n+2}) + g_2(\mathbf{x}_1, x_{n+1}) \\ \vdots \\ \phi_s(x_{n+s}) + g_s(\mathbf{x}_1, x_{n+1}, \ldots, x_{n+s-1}) \end{pmatrix}$$

where $g_1, \ldots, g_s$ are randomly chosen polynomials and $\phi_i : \mathbb{F}_q \to \mathbb{F}_q$ are invertible polynomials, which can be easily inverted. If we want G to be quadratic, then choose g_i, ϕ_i to be quadratic. For example, if $k > 1$, $\mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$, $x \mapsto x^2$ has an inverse $y \mapsto y^{2^{k-1}}$. Then each $\phi_i : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ can be chosen as $\phi_i(x) = a_i x^2$ where $a_i \in \mathbb{F}_{2^k}$ and $a_i \neq 0$. This type of maps with each $\phi_i(x) = x^2$ appears in [PG97]. We make the convention that if $q = 2$, we choose each $\phi_i(x) = x$ and if $q > 2$, we choose each $\phi_i(x) = a_i x^2$ for a constant $a_i \neq 0$.

Like the triangular perturbation [ZT14], extended triangular maps can also be used as a modification method, called extended triangular perturbation. It also preserves the efficiency and surjectivity of the original scheme, but is insecure against high rank attack. To protect (extended) triangular perturbation, the triangular structure should be hidden by adding a large amount of quadratic terms and cross terms of $\mathbf{x}_1, \mathbf{x}_2$.

Next we propose a special type of HFEv polynomials. Let $\mathbb{K} = \mathbb{F}_q[x]/(g(x))$ be a degree t extension of $\mathbb{F}_q$ where $g(x) \in \mathbb{F}_q[x]$ is a degree s irreducible polynomial. Let $\phi : \mathbb{K} \to \mathbb{F}_q^t$ be the standard $\mathbb{F}_q$-linear map

$$\phi(a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}) = (a_0, a_1, \ldots, a_{t-1}).$$

Define the following type of polynomial over $\mathbb{K}$:

$$H(X_1, X_2) = \sum_{0 \leq i < t} \sum_{1 \leq q^j \leq D} a_{ij} X_1^{q^i} X_2^{q^j} + \sum_{1 \leq q^i + q^j \leq D} b_{ij} X_2^{q^i + q^j} + \sum_{1 \leq q^j \leq D} c_j X_2^{q^j}.$$

Here D is a relatively small number. Fixing a value of X_1, $H(X_1, X_2)$ is then an HFE polynomial of X_2, so X_2 can be solved efficiently from $H(X_1, X_2) = 0$ with a given X_1. Notice that this equation always has the zero solution $X_2 = 0$, but a nonzero solution is preferred. We can apply Berlekamp's algorithm to solve it and among those solutions, we pick a nonzero solution as X_2. We shall accept the zero solution $X_2 = 0$ if there is only the zero solution. It would be ideal that there is a nonzero solution for most values of X_1.

For $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{F}_q^t$, define the following map to be used next

$$\bar{H} : \mathbb{F}_q^t \times \mathbb{F}_q^t \to \mathbb{F}_q^t, \quad \bar{H}(\mathbf{x}_1, \mathbf{x}_2) = \phi(H(\phi^{-1}(\mathbf{x}_1), \phi^{-1}(\mathbf{x}_2))).$$

3.2 Construction of MI-T-HFE

Let q be a power of 2, $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ an MI map, $1 \leq s \leq n$ and $1 \leq t \leq n$. Combining the extended triangular map G and the HFEv map H defined above, we define the following trapdoor function for $\mathbf{x}_1 \in \mathbb{F}_q^n$, $\mathbf{x}_2 \in \mathbb{F}_q^s$, $\mathbf{x}_3 \in \mathbb{F}_q^t$,

$$F' : \mathbb{F}_q^{n+s+t} \to \mathbb{F}_q^n,$$

$$F'(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3) = F(\mathbf{x}_1) + S \cdot G(\mathbf{x}_1, \mathbf{x}_2) + T_2 \cdot \bar{H}(T_1 \cdot (\mathbf{x}_1, \mathbf{x}_2), \mathbf{x}_3) \tag{3.1}$$

where S is an $n \times s$ matrix, T_1 an $t \times (n+s)$ matrix and T_2 an $n \times t$ matrix. This trapdoor function will serve as the central map of MI-T-HFE.

It should be noted that F' is indeed an HFEv map with $(\mathbf{x}_1, \mathbf{x}_2)$ as the $n+s$ vinegar variables. In addition, it is also a scheme obtained from the MI cryptosystem by perturbing it using an extended triangular map and an HFEv map just like the situation in [ZT14].

Randomly choose two invertible affine transformations $L_1 : \mathbb{F}_q^{n+s+t} \to \mathbb{F}_q^{n+s+t}$ and $L_2 : \mathbb{F}_q^n \to \mathbb{F}_q^n$. Then the public map of MI-T-HFE is

$$P(x_1, \ldots, x_{n+s+t}) = L_2 \circ F' \circ L_1 : \mathbb{F}_q^{n+s+t} \to \mathbb{F}_q^n.$$

The signature scheme MI-T-HFE is described as follows.

Public Key: The public key of MI-T-HFE consists of

1. The finite field $\mathbb{F}_q$.
2. The n polynomials in $P(x_1, \ldots, x_{n+s})$.

Private Key: The private key of MI-T-HFE consists of

1. The θ of the MI map F.
2. The extended triangular map G.
3. The matrix S.
4. The polynomial H.
5. The two matrices T_1, T_2.
6. The two invertible affine transformations L_1, L_2.

Signature Verification: For a given a message $\mathbf{y} \in \mathbb{F}_q^n$, a signature $\mathbf{x} \in \mathbb{F}_q^{n+s+t}$ will be accepted if it satisfies $\bar{F}'(\mathbf{x}) = \mathbf{y}$.

Signature Generation: For a given message $\mathbf{y} \in \mathbb{F}_q^n$, a valid signature is generated in the following procedure:

1. Compute $\mathbf{y}' = L_2^{-1}(\mathbf{y})$.
2. Randomly choose $\mathbf{u} = (u_1, \ldots, u_s) \in \mathbb{F}_q^s$, then solve $F(\mathbf{x}_1) = \mathbf{y}' - S \cdot \mathbf{u}$ to get a solution $\mathbf{x}_1$.
3. Substitute $\mathbf{x}_1$ into $G(\mathbf{x}_1, \mathbf{x}_2) = \mathbf{u}$ to get a solution $\mathbf{x}_2$ given by

$$x_{n+1} = \phi_1^{-1}(u_1 - g_1), \ldots, x_{n+s} = \phi_s^{-1}(u_s - g_s). \tag{3.2}$$

4. Substitute $\mathbf{x}_1, \mathbf{x}_2$ into the equation $\bar{H}(S_1 \cdot (\mathbf{x}_1, \mathbf{x}_2), \mathbf{x}_3) = 0$ and solve it by Berlekamp's algorithm.

5. Among those solutions, pick a nonzero solution and assign it to $\mathbf{x}_3$. If there is only the zero solution, then let $\mathbf{x}_3 = 0$.
6. Then $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3)$ is a solution to $F'(\mathbf{x}) = \mathbf{y}$.
7. Finally compute $\mathbf{x} = L_1^{-1}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3)$ which is then a signature.

From the above signature generation, it is easy to see that for any message, there is always a valid signature. Namely the trapdoor function is a surjective map. This is very important for a signature scheme. In addition, we remark that the MI map F in MI-T-HFE can be replaced by any other trapdoor function.

4 Security Analysis

In this section, we shall analyze the security of MI-T-HFE against current major attacks and discuss the choice of parameters accordingly.

The trapdoor function (3.1)

$$F'(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3) = F(\mathbf{x}_1) + S \cdot G(\mathbf{x}_1, \mathbf{x}_2) + T_2 \cdot \bar{H}(T_1 \cdot (\mathbf{x}_1, \mathbf{x}_2), \mathbf{x}_3)$$

of MI-T-HFE is a sum of the following three parts:

1. The inner map is an MI map $F(\mathbf{x}_1)$,
2. The middle map is an extended triangular map $S \cdot G(\mathbf{x}_1, \mathbf{x}_2)$, and
3. The outer map is an HFEv map $T_2 \cdot \bar{H}(T_1 \cdot (\mathbf{x}_1, \mathbf{x}_2), \mathbf{x}_3)$.

From the point of view of perturbation [ZT14], the extended triangular map and the HFEv map in MI-T-HFE are designed to help each other similar to [ZT14]. One reason for this design is that the middle triangular map has an amount of random quadratic terms of the variables $\mathbf{x}_1$ to hide $F(\mathbf{x}_1)$, but its triangular structure makes the additional variables $\mathbf{x}_2$ detectible by high rank attack. The outer map does not have quadratic terms of $\mathbf{x}_1, \mathbf{x}_2$ but has all other quadratic terms of the variables. So the middle map can add random quadratic terms of $\mathbf{x}_1$ to perturb $F(\mathbf{x}_1)$ while the outer map can cover the triangular structure of the middle triangular map if t is big. Further reasons for the design of the trapdoor will become clear in the cryptanalysis below.

We first explain why the design of MI-T-HFE can prevent the simple attack of collecting a large amount of pairs of messages and signatures. In the signature generation, a random value $\mathbf{u} \in \mathbb{F}_q^s$ is assigned to G and $\mathbf{x}_1$ is solved from $F(\mathbf{x}_1) = \mathbf{y} - S \cdot \mathbf{u}$ with $\mathbf{y}$ perturbed by the random value $S \cdot \mathbf{u}$. In addition, notice that $\mathbf{x}_3$ can be zero in the signature generation, but in the signature generation, a nonzero solution to H is preferred and it is of high probability that there is a nonzero solution for a given message by the properties of HFE polynomials. The first feature can randomize $\mathbf{x}_1$ to break relationship between $\mathbf{x}_1$ and $\mathbf{y}$, and the second feature can assure that most $\mathbf{x}_3$ are nonzero so that information of the subspace of vectors $(\mathbf{x}_1, \mathbf{x}_2, 0)$ won't be recovered from the collected pairs of messages and signatures.

In the rest of this section, we will consider rank attacks, differential attack, linearization attack, and attacks to HFE (including MinRank attack and direct attacks).

4.1 Rank Attacks

There are two types of rank attacks, MinRank attack (or called low rank attack) and high rank attack. The MinRank attack tries to find those central polynomials or their linear combinations with the least number r of variables. Its complexity is dominated by $O(q^r)$ and successfully break Triangle-Plus-Minus schemes [GC00]. However, this attack is not applicable to MI-T-HFE in practice, because the least number of vairables that the central map has is no less than n which is large enough, noticing that the public map is F' from $\mathbb{F}_q^{n+s+t}$ to $\mathbb{F}_q^n$. The high rank attack, on the contrast, tries to find those central polynomials or their linear combinations with the most number of variables, or equivalently to find those variables which appears the fewest times r in the central map. It has complexity $O(q^r)$ and is a powerful way to break triangular schemes [CSV97, GC00, YC05]. In the case of MI-T-HFE, if the outer map is small, i.e., if t is small, then high rank attack can be applied to find the last variables $\mathbf{x}_3$ first and then find the triangular structure of the second map; namely the three parts of the trapdoor function (3.1) of MI-TT-HFE can be separated. Hence t should be big enough to protect the trapdoor against high rank attack. For example, to have the security level of at least 2^{80}, we should have t such that $q^t \geq 2^{80}$.

4.2 Differential Attack

Although the public map F' of MI-T-HFE is an HFEv map and it has been shown that HFE, HFE- and HFEv are generally secure against differential attack [DST14], the differential attack [FGS05] to Ding's internal perturbation of the MI cryptosystem (IPMI) [Din04] should still be taken into account.

The differential attack to IPMI relies on the two facts: 1) there is a large linear subspace U restricted to which the internal perturbation disappears; 2) a vector $\mathbf{u}$ can be detected if it is in U by checking if the dimension of the kernel of the differential at $\mathbf{u}$ is a specific number.

For MI-T-HFE, we find that the first fact does hold here. Notice that if $\mathbf{x}_3 = 0$, the HFEv polynomial H then automatically disappears. So the linear subspace of vectors $(\mathbf{x}_1, \mathbf{x}_2, 0)$ is an important subspace. If there is no triangular map in the middle, i.e., $s = 0$, then the situation is similar to IPMI and thus the differential attack to IPMI applies. Notice that (extended) triangular maps can resist differential attack and perturbing the MI map by an (extended) triangular perturbation can break the differential invariant. Namely if $s > 0$ then the second fact does not hold anymore, and when s increases, the dimension varies in a bigger range so that the differential attack [FGS05] is no longer applicable here. To resist the differential

attack, we guess that s can be just a small number but further careful analysis is needed to estimate it.

4.3 Linearization Attack

The linearization attack is proposed by Patarin [Pat95] to break the MI cryptosystem. The MI cryptosystem and some other schemes may have a large amount of linear equations between $\mathbf{x}$ and $\mathbf{y}$ (or linear on $\mathbf{x}$ but nonlinear on $\mathbf{y}$). From these equations, part of $\mathbf{x}$ may be computed and the rest of $\mathbf{x}$ may be tried one by one. However it is known that linearization attack is not applicable to triangular maps and HFE maps. The trapdoor function (3.1) of MI-TT-HFE is a mixture of an MI map, an extended triangular map and an HFE map which breaks the linear relationship. So if t is big, there would be very few linear equations among $\mathbf{x}_1$ and $\mathbf{y}$ so that linearization attack is resisted. Moreover even if $\mathbf{x}_1$ could be recovered, the rest of the variables $\mathbf{x}_2, \mathbf{x}_3$ are still unknown and the number of them is big enough so that guessing all of them is infeasible.

4.4 Attacks to HFEv

If we lift the trapdoor function (3.1)

$$F'(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3) = F(\mathbf{x}_1) + S \cdot G(\mathbf{x}_1, \mathbf{x}_2) + T_2 \cdot \bar{H}(T_1 \cdot (\mathbf{x}_1, \mathbf{x}_2), \mathbf{x}_3)$$

of MI-T-HFE to the extension field $\mathbb{K}$, it has the following form of an HFEv polynomial

$$\begin{aligned} H'(V, X) = &\sum a'_{ij} V^{q^i+q^j} + \sum b'_i V^{q^i} \\ &+ \sum_{0 \le i < t} \sum_{1 \le q^j \le D} a_{ij} V^{q^i} X^{q^j} + \sum_{1 \le q^i + q^j \le D} b_{ij} V^{q^i} X^{q^j} + \sum_{1 \le q^j \le D} c_j X^{q^j}. \end{aligned}$$

Here the vinegar variable V corresponds $(\mathbf{x}_1, \mathbf{x}_2)$ and variable X corresponds to $\mathbf{x}_3$; $F + SG$ corresponds to the sum of the monomials $V^{q^i+q^j}, V^{q^i}$ and $T_2\bar{H}$ corresponds to the sum of the rest monomials.

Attacks applicable to the HFE family are Kipnis-Shamir's attack [KS99] based on the MinRank problem and direct attack [FJ03]. In [DS05a] Ding and Schmidt improve Kipnis-Shamir's attack to cryptanalyze HFEv. They show that Kipnis-Shamir's attack can break HFEv for very small v such as $v = 1$, but as v increases, the complexity increases fast and when v is close to the extension degree of the field $\mathbb{K}$ over $\mathbb{F}_q$, HFEv would be just like a random system of quadratic polynomials.

For direct attack, Ding and Yang provide in [DY13] a solid theoretical estimation on the complexity of direct attack on HFEv and HFEv- by calculating the degree of regularity. Their conclusion is the same as the case of Kipnis-Shamir's attack; namely, direct attack remains feasible for very small v but infeasible for big v. Especially for QUARTZ whose parameters are $(2, 129, 103, 4, 3)$, its degree of regularity

is bounded by 9 and its security level is estimated as 2^{92} in [DY13]. Notice that QUARTZ has 4 vinegar variables only.

In the case of MI-T-HFE, the number of vinegar variables is $n + s$ bigger than the extension degree t. So if q^t is big enough, such as $q^t \geq 2^{80}$ and D is around 100, then MI-T-HFE is just like a random system of quadratic polynomials against Kipnis-Shamir's attack, and has high degree of regularity by the formulas in [DY13] so that it is secure against direct attack.

5 A Practical Example and Comparison with QUARTZ

Based on the cryptanalysis in the preceding section, we shall propose a practical parameter set to compare with QUARTZ. It should be mentioned that here we are comparing the essential part of QUARTZ, i.e, the HFEv- scheme with the QUARTZ parameters $(2, 129, 103, 4, 3)$. The full design of QUARTZ [PCG01] applies this essential part a few times iteratively to increase the security but it was later found that this iterative structure does not contribute to the security. We shall propose a parameter set with (almost) identical length of message and same level of security, and compare the key sizes and efficiency.

We suggest the following set of parameters for MI-T-HFE

$$(q, n, s, t, D) = (8, 33, 5, 32, 72).$$

According to the cryptanalysis, the best attack to MI-T-HFE with this set of parameters is the high rank attack, and its complexity is 2^{96}. In other words, MI-T-HFE with parameters $(8, 33, 5, 32, 72)$ has 96-bit security. As a comparison with QUARTZ, its degree of regularity is bounded by 143.5 according to the formulas in [DY13], which is much higher than the bound, 9, for QUARTZ. Based on the degree of regularity, the security level of MI-T-HFE $(8, 33, 5, 32, 72)$ against direct attack should be higher than QUARTZ, which is estimated as 2^{92} in [DY13]. So the overall security of the two schemes are 2^{96} and 2^{92} respectively, which may be regarded as at the same level.

For MI-T-HFE with parameters $(8, 33, 5, 32, 72)$, a message is a vector in $\mathbb{F}_8^{33}$ whose length is 99 bits, and a signature is vector in $\mathbb{F}_8^{70}$ whose length is 210 bits. Its key sizes are calculated as follows. The public map $P : \mathbb{F}_q^{n+s+t} \to \mathbb{F}_q^n$ has n components and each component is a quadratic polynomial with $(n+s+t)(n+s+t+1)/2$ quadratic terms, $n+s+t$ linear terms and 1 constant term. Thus the public key size is

$$\frac{1}{2}n(n+s+t+1)(n+s+t+2)\log_2 q \text{ bits.}$$

With parameters $(8, 33, 5, 32, 72)$, the public key size is 31.6 Kbytes.

The private key consists of several parts. S has ns entries in $\mathbb{F}_q$, T_1, T_2 together have $2nt + st$ entries in $\mathbb{F}_q$, and L_1, L_2 together have $(n+s+t)^2 + n^2$ entries in $\mathbb{F}_q$.

G has 3165 coefficients in $\mathbb{F}_q$, and H has 101 coefficients in $\mathbb{K} \cong \mathbb{F}_{q^t}$, equivalently 3232 coefficients in $\mathbb{F}_q$. So the private key size is 5.6 Kbytes.

As comparison, a message of QUARTZ is 100 bits and a signature is 107-bit. Its public key consists of 100 quadratic polynomials each with 107 variables. Thus its public size is 72.3 Kbytes, more than twice that of MI-T-HFE $(8, 33, 5, 32, 72)$. Similarly its private key size is 3.9 Kbytes, a bit smaller than that of MI-T-HFE $(8, 33, 5, 32, 72)$.

We next consider the efficiency of signature generation. In the signature generation of HFEv and the core part of QUARTZ, one first assigns random values to the vinegar variables and then one solve the resulted HFE polynomials; if no solution then try other values of the vinegar variables. This design lowers down the efficiency as one may need to solve HFE polynomials a few times. MI-T-HFE has different design on signature generation: one first solve an MI map to get $\mathbf{x}_1$, then solve a triangular map to get $\mathbf{x}_2$, and finally solve the resulted HFE polynomial only *once*. This is because the resulted HFE equation in MI-T-HFE is of the following form $\sum a_{ij} X^{q^i+q^i} + \sum b_i X^{q^i} = 0$ which always has solutions — a nonzero solution is preferred if there is one. The first two steps are very fast with little computation time, confirmed by computer experiments, as inverting an MI map and a triangular map are both extremely fast. So the main cost for inverting the central map is on inverting the HFE polynomial of MI-T-HFE. Recall that the complexity of inverting an HFE polynomial by Berlekamp's algorithm is $O(nD^2 \log_q D + D^3)$. The value of $nD^2 \log_q D + D^3$ for MI-T-HFE $(8, 33, 5, 32, 72)$ is 1.2×10^6, much smaller than the value 14.2×10^6 for QUARTZ. So it is expected that the complexity of inverting the HFE map of MI-T-HFE is much less than that of HFEv and QUARTZ. We did computer experiments on MAGMA to compare the computation time of inverting their core HFE maps and found that it is on average about 0.42 seconds for QUARTZ and 0.13 seconds for MI-T-HFE $(8, 33, 5, 32, 72)$; namely the latter is more than three times faster. Hence we may conclude that MI-T-HFE $(8, 33, 5, 32, 72)$ is about three times faster than the underlying HFEv- of QUARTZ when generating a signature. Full implementation will be conducted to justify this claim in the future.

To summarize, QUARTZ, or its underlying HFEv- scheme with the QUARTZ parameters $(2, 129, 103, 4, 3)$, uses an HFE polynomial with very small number of vinegar variables but relatively higher degree to have a short signature and high enough security level, but the cost is bigger public key size and low efficiency. On the contrary, MI-T-HFE $(8, 33, 5, 32, 72)$ uses a special HFE polynomial with large number of vinegar variables but relatively smaller degree to have smaller public key size, better efficiency and high enough security level, and the only cost is longer signatures. Moreover MI-T-HFE is a definitely surjective scheme but QUARTZ is not.

6 Conclusion

In this paper we have constructed a new multivariate signature scheme, named MI-T-HFE, whose core map is of an HFEv type but has a trapdoor embedded in it. MI-T-HFE has a special HFE polynomial with relatively low degree and a large number of vinegar variables. Unlike the usual HFEv schemes, these vinegar variables are not randomly assigned values but have special structure; namely it is a certain combination of a Matsumoto-Imai map and a kind of extended triangular maps. This trapdoor can also be viewed as a double perturbation of the Matsumoto-Imai cryptosystem by extended triangular maps and HFEv maps. With this trapdoor, MI-T-HFE is a surjective signature scheme, namely there are always valid signatures for any message. The special HFE polynomial of MI-T-HFE and its low degree guarantee its efficiency, while the large amount of vinegar variables backs its security but does not distract efficiency. To be comparable with QUARTZ, we propose a parameter set for MI-T-HFE with the same length of message and same security level as QUARTZ. With the proposed parameters, the public key size of MI-T-HFE is about half of QUARTZ, and signature generation is about three times efficient than the underlying HFEv- scheme with the QUARTZ parameters — thus much more efficient than QUARTZ. Its disadvantage is that its signature length, 210 bits, is about twice that of QUARTZ. Hence we suggest to use MI-T-HFE instead of QUARTZ if longer signatures are accepted.

Acknowledgment

The authors would like to thank the anonymous reviewers for their helpful comments on improving this paper. The first author would like to thank the financial support from the National Natural Science Foundation of China (Grant No. 61572189).

References

[BFP13] L. Bettale, J. C. Faugère, and L. Perret. Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic. *Des. Codes Cryptography*, 69(1):1–52, 2013.

[Cou01] N. T. Courtois. The Security of Hidden Field Equations (HFE). In D. Naccache, editor, *CT-RSA 2001*, volume 2020 of *LNCS*, pages 266–281. Springer, 2001.

[CSV97] Don Coppersmith, Jacques Stern, and Serge Vaudenay. The security of the birational permutation signature schemes. *Journal of Cryptology*, 10:207–221, 1997.

[Din04] Jintai Ding. A new variant of the Mausomoto-Imai cryptosystem through perturbation. In F. Bao et al, editor, *PKC 2004*, volume 2947 of *LNCS*, pages 305–318. Springer, 2004.

[DS05a] Jintai Ding and Dieter Schmidt. Cryptanalysis of HFEv and the internal perturbation of HFE. In S. Vaudenay, editor, *PKC 2005*, volume 3386 of *LNCS*, pages 288–301. Springer, 2005.

[DS05b] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariate polynomial signature scheme. In J. Ioannidis, A. Keromytis, and M. Yung, editors, *ACNS 2005*, volume 3531 of *LNCS*, pages 164–175. Springer-verlag Berlin Heidelberg, 2005.

[DST14] Taylor Daniels and Daniel Smith-Tone. Differential Properties of the HFE Cryptosystem. In M. Mosca, editor, *PQCrypto 2014*, volume 8772 of *LNCS*, pages 59–75. Springer, 2014.

[DY09] Jintai Ding and Bo-Yin Yang. Multivariate public key cryptography. In DanielJ. Bernstein, Johannes Buchmann, and Erik Dahmen, editors, *Post-Quantum Cryptography*, pages 193–241. Springer Berlin Heidelberg, 2009.

[DY13] Jintai Ding and Bo-Yin Yang. Degree of Regularity for HFEv and HFEv-. In P. Gaborit, editor, *PQCrypto 2013*, volume 7932 of *LNCS*, pages 52–66. Springer, 2013.

[FGS05] Pierre-Alain Fouque, Louis Granboulan, and Jacques Stern. Differential cryptanalysis for multivariate schemes. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 341–353. Springer, 2005.

[FJ03] J.-C. Faugère and A. Joux. Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases. In D. Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 44–60. Springer, 2003.

[GC00] Louis Goubin and Nicolas T. Courtois. Cryptanalysis of the TTM cryptosystem. In Tatsuaki Okamoto, editor, *ASIACRYPT 2000*, volume 1976, pages 44–57. Springer, 2000.

[GJ79] Michael R. Garey and David S. Johnson. *Computers and intractability: A guide to the theory of NP-completeness*. W. H. Freeman, 1979.

[GJS06] L. Granboulan, A. Joux, and J. Stern. Inverting HFE is Quasipolynomial. In C. Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 345–356. Springer, 2006.

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

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

[MI88] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature verification and message encryption. In C. G. Guenther, editor, *EUROCRYPT'88*, volume 330 of *LNCS*, pages 419–453. Springer, 1988.

[Pat95] Jacques Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In D. Coppersmith, editor, *Advances in Cryptology — CRYPTO 1995*, volume 963, pages 248–261. Springer-Verlag Berlin Heidelberg, 1995.

[Pat96] Jacques Patarin. Hidden field equations (HFE) and isomorphism of polynomials (IP): Two new families of asymmetric algorithms. In U. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 33–48. Springer, 1996.

[Pat97] Jacques Patarin. The oil and vinegar signature scheme. Presented at the Dagstuhl Workshop on Cryptography, September 1997.

[PCG99] Jacques Patarin, Nicolas Courtois, and Louis Goubin. Flash, a fast multivariate signature algorithm. In D. Naccache, editor, *CT-RSA 2001*, volume 2020 of *LNCS*, pages 298–307. Springer, 1999.

[PCG01] Jacques Patarin, Nicolas Courtois, and Louis Goubin. QUARTZ, 128-bit long digital signatures. In D. Naccache, editor, *CT-RSA 2001*, volume 2020 of *LNCS*, pages 282–288. Springer, 2001.

[PG97] Jacques Patarin and Louis Goubin. Trapdoor one-way permutations and multivariate polynomials. In *Proc. of ICICS'97*, volume 1334 of *LNCS*, pages 356–368. Springer, 1997.

[YC05] B. Y. Yang and J. M. Chen. Building secure tame-like multivariate public-key cryptosystems: The new TTS. In *ACISP 2005*, volume 3574 of *LNCS*, pages 518–531. Springer, 2005.

[ZT14] Wenbin Zhang and Chi How Tan. A New Perturbed Matsumoto-Imai Signature Scheme. In *ASIAPKC '14 Proceedings of the 2Nd ACM Workshop on ASIA Public-key Cryptography*, pages 43–48, New York, NY, USA, 2014. ACM.