TOT, a Fast Multivariate Public Key Cryptosystem with Basic Secure Trapdoor

Wuqiang Shen and Shaohua Tang*

School of Computer Science & Engineering, South China University of Technology, Guangzhou 510006, China
csshtang@scut.edu.cn, shtang@IEEE.org

Abstract. In this paper, we design a novel one-way trapdoor function, and then propose a new multivariate public key cryptosystem called TOT, which can be used for encryption, signature and authentication. Through analysis, we declare that TOT is secure, because it can resist current known algebraic attacks if its parameters are properly chosen. Some practical implementations for TOT are also given, and whose security level is at least 2^{90}. The comparison shows that TOT is more secure than HFE, HFEv and Quartz (when $n \geq 81$ and $D_{HFE} \geq 129$, HFE is still secure), and it can reach almost the same speed of computing the secret map by C* and Sflash^{v2} (even though C* was broken, its high speed has been affirmed).

Keywords: TOT; multivariate public key cryptosystem; one-way trapdoor function; algebraic attack

1 Introduction

Since Shor [1] [2] proposed the polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, researchers had been devoting to studying public key cryptosystems that can resist quantum computer attacks to replace the traditional public key cryptosystems, such as RSA, ECC, etc.. The system that is immune to quantum computer attacks goes by the name of Post Quantum Cryptography (PQC) [3]. Multivariate Public Key Cryptosystem (MPKC) [4] [5] [6] is a branch of PQC.

MPKC is based on the observation that solving a system of Multivariate Quadratic polynomial equations over a finite field is an NP-complete problem [7]. This problem is also known as MQ problem. In other words, the security of a MPKCs relies on the intractability of the MQ problem.

In the 1980s, the development of MPKCs was great, but many of them were broken. Matsumoto and Imai [8] presented C* scheme (or called MI) with a special type of trapdoor. However, it was broken by Patarin's algebraic attack via linearization equations [9]. Surprisingly, Patarin lately applied the idea of the linearization equation attack on C* to construct an Oil-Vinegar signature

* Corresponding author.

scheme (OV) [10]. The basic OV signature scheme was broken by Kipnis et al. in 1999, and they presented a modified scheme called Unbalanced Oil-Vinegar scheme (UOV) [11]. So far, UOV is secure from the structural point of view. In 2005, Ding and Schmidt introduced a multi-layer unbalanced Oil-Vinegar construction called Rainbow signature scheme [12]. Rainbow is still secure currently with parameters properly choosen. Moreover, C^* cryptosystem can be generalized by the Plus method, the Minus method, and the Perturbed method. There are thus many variants of C^*, such as Sflash [13] [14], Flash [15], C^{*+} [16], $C^{*\pm}$ [16], PMI [17], and PMI^+ [18]. It is worth mentioning that Paterin fully generalized C^* cryptosystem and eventually invented Hidden Field Equation cryptosystem (HFE) [19] in 1996. Researchers also utilized the Plus method, the Minus method, and the Perturbed method to generate many variants of HFE, for example HFE^- [19], $HFE^{\pm}$ [19], IPHFE [20] and HFEv [20] [11]. HFEv is a combination of the basic HFE with the idea of Oil-Vinegar. In succession, many variants of HFEv also came out, such as Quartz [21].

On the other hand, Triangular Scheme (TS) family is a different and special kind of construction in MPKC. In 1999, Moh [22] proposed Tame Transformation Method (TTM) cryptosystem which belongs to TS family. Unfortunately, it was attacked by Goubin and Courtois [23] in 2000. It is interesting that they also formulated a new family of cryptosystems called Triangular-Plus-Minus (TPM) to let their attack in a more general way. Both TTM and TPM can be attacked by the MinRank method [23]. Later, new TTM schemes were introduced in [24]. However, Ding and Schmidt [25] pointed out that they are insecure. Besides, Tame Transformation Signature (TTS) of the TS family also experienced the same rough process [26] [27] [28]. In a nutshell, MPKCs are always heuristic.

MPKCs now mainly consist of some basic schemes and their variants, and are divided into five categories [4] [5] [6]: C^* family, HFE family, UOV family, TS family and Others. Thus it is obvious that the trapdoors of MPKCs are limited, and they have also been greatly challenged. Therefore, it is impatient to strengthen the security of the original systems, or to seek new basic one-way trapdoor functions to construct multivariate cryptosystems. The latter is more important because it can enrich the field of multivariate public key cryptography.

In this paper, we design a novel trapdoor, and then propose a new multivariate public key cryptosystem called TOT based on this trapdoor, which can be used for encryption, signature and authentication. We analyze the security of TOT, and claim that it can resist current known algebraic attacks if parameters are properly chosen. Moreover, because our designed trapdoor has some special properties, we can quickly compute the secret map, namely the decryption process or the signing process, of TOT. From the aspects of both security and efficiency, we compare TOT with other multivariate schemes including encryption and signature schemes. Then we can learn that the security level of TOT is higher than that of HFE, HFEv and Quartz if properly choosing t, where t is the time in the trapdoor function referred in Section 3. The computation speed of the secret map of TOT is as fast as C^* or $Sflash^{v2}$. In addition, TOT can generate a practical signature with a length of 128 bits like Quartz. We believe

that our proposed TOT is a novel, secure, and fast cryptosystem, and is a better choice among MPKCs in terms of both security and efficiency.

Organization. The rest of this paper is organized as follows. In Section 2, we introduce some notations and concepts on the multivariate public key cryptosystems. In Section 3, we design a novel one-way trapdoor function, and propose a multivariate cryptosystem named TOT. We analyze the security of TOT by methods of current known algebraic attacks in Section 4, and assess its security level. In Section 5, we evaluate the performance of TOT, and present the computation complexity and some practical parameters. In Section 6, we compare TOT with other multivariate schemes including HFE, HFEv, PMI$^+$, Sflash^{v2}, Quartz, UOV and Rainbow. Finally, we summarize the paper in Section 7.

2 Preliminary

2.1 Notation

Throughout this paper, we will use the following notations. Let F be a finite field of cardinality q and characteristic p, where p is a prime number and $q = p^k$ ($k \in \mathrm{N}$). We take $f(x) \in F[x]$ to be any irreducible polynomial of degree n ($\in \mathrm{N}$), then define the field $E = F[x]/(f(x))$ as an extension of degree n of F. Obviously E is isomorphic to F_{q^n}, and has q^n elements. We then let $\varphi : E \to F^n$ be the standard F-linear isomorphism between E and F^n given by

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

The subfield F of E is embedded in F^n in the standard way:

$$\varphi(a) = (a, 0, ..., 0), \quad \forall a \in F.$$

Moreover, in a (bipolar) multivariate public key cryptosystem we also let $n \in \mathrm{N}$ be the number of variables, $m \in \mathrm{N}$ be the number of equations. Note that n may be equal to m.

The public key is given by a map $P : F^n \to F^m$,

$$P(x_1, ..., x_n) = (p_1, ..., p_m),$$

where each p_i ($i \in \mathrm{N}, 1 \le i \le m$) is a polynomial in $F[x_1, ..., x_n]$.

We build a map $\overline{P} : F^n \to F^m$, which is defined by

$$\overline{P}(\overline{x}_1, ..., \overline{x}_n) = (\overline{p}_1, ..., \overline{p}_m),$$

where each $\overline{p}_i$ ($i \in \mathrm{N}, 1 \le i \le m$) is a polynomial in $F[\overline{x}_1, ..., \overline{x}_n]$. We will know that $\overline{P}$ is a map of the intermediary structure in multivariate cryptosystem.

Let $S(x_1, ..., x_n) = (\overline{x}_1, ..., \overline{x}_n)$ be a randomly chosen invertible affine transformation from F^n to F^n, and $T(\overline{y}_1, ..., \overline{y}_m) = (y_1, ..., y_m)$ be also a randomly chosen invertible affine transformation from F^m to F^m. These affine bijections can be represented in a basis by polynomials of total degree 1 and with coefficients of the polynomials in F.

2.2 Some Concepts on MPKC

Multivariate public key cryptosystem can also be based on the problem of solving any nonlinear system of multivariate polynomial equations over a finite field. However, from the perspectives of both security and efficiency we usually choose polynomial equations of total degree two to construct multivariate public key schemes. MPKC schemes thus also go by the name of Multivariate Quadratic (MQ) schemes [6].

From a structural point of view, this system of equations must be embedded into a special trapdoor which can make it possible to solve this system efficiently [6] [7]. Hence we can distinguish difference multivariate cryptosystems from their basic trapdoors. Generally, a multivariate public key cryptographic system consists of a trapdoor $(S, \overline{P}, T)$ and a public key map P, where the trapdoor $(S, \overline{P}, T)$ is embedded into the system of equations P, namely $P = T \circ \overline{P} \circ S(x_1, ..., x_n)$. S and T are secret keys, and the map $\overline{P}$ may or may not be part of the secret key depending on its precise nature. In addition, we call the map $\overline{P}$ as "the central map", P as "the public map", and P^{-1} as "the secret map". Obviously, we must need the knowledge of the basic trapdoor to compute the secret map P^{-1}, or equivalently "inverting" the public map P.

3 The Proposed Multivariate Cryptosystem

Notations are the same as ones described in Section 2.

3.1 A Novel One-Way Trapdoor Function

We design a new one-way trapdoor function in this sub-section, which is used to construct the new multivariate public key cryptosystem TOT.

We first define a function g over the extension field E (with cardinality q^n) by

$$g(X) = \sum_{i=1}^{d} (X - h_i), \tag{1}$$

where $h_i \in E$ and $d = \deg(g(X))$.

Next, we define another function G over the filed E by

$$G(X) = g(X)^t, \tag{2}$$

where $t \in \mathrm{Z}_{q^n}$ is the time of g, and $\gcd(t, q^n - 1) = 1$. If v is an inverse of t, then

$$t \cdot v \equiv 1 \bmod (q^n - 1).$$

Moreover, we denote the degree of G by $D = \deg(G(X))$. The function G is our expected one-way trapdoor function.

Obviously, for a given specific value $Y' \in E$, we can solve the equation $G(X) = Y'$ in unknown X through the following two steps.

(1) We compute the Modular Exponentiation $(Y')^v \bmod (q^n - 1)$, and denote the result by Y''. This step can be performed by the square-and-multiply method. Note that the square-and-multiply method can be enhanced, or we can use more efficient methods of [13] and [14] to compute the Modular Exponentiation.

(2) We solve the equation $g(X) = Y''$ in unknown X by the probabilistic Berlekamp algorithm [29] [30] [31] [32].

The solving process of this equation $G(X) = Y'$ is based on the following observation:

$$\begin{aligned} & G(X) = Y' \\ \Rightarrow \quad & g(X)^t = Y' \\ \Rightarrow \quad & g(X)^{t \cdot v} = Y'^v \\ \Rightarrow \quad & g(X) = Y'^v \\ \Rightarrow \quad & X = g^{-1}(Y'^v). \end{aligned}$$

This observation is a well-done job. We can utilize it to establish a cryptosystem with basic secure trapdoor. In the following sub-sections, we are going to describe our proposed multivariate public key cryptosystem in detail.

3.2 TOT for Encryption

We let $n = m$, then P and $\overline{P}$ are maps from F^n to F^n. Let S and T be two affine transformations in F^n. Moreover, let

$$\overline{P}(x_1, ..., x_n) = \varphi \circ G \circ \varphi^{-1}(x_1, ..., x_n),$$

and

$$P(x_1, ..., x_n) = T \circ \overline{P} \circ S(x_1, ..., x_n).$$

The TOT public key cryptosystem is based on the field F of characteristic p.

Public Key:

The public key includes the following information.

1) The field F, which contains its additive and multiplicative structure.
2) The map P, which contains $p_1, ..., p_n$ satisfying

$$p_1(x_1, ..., x_n), ..., p_n(x_1, ..., x_n) \in F[x_1, ..., x_n].$$

Private Key:

The private key includes the following information.

1) The parameters h_i, d, t and their resultant functions g and G.
2) Two invertible affine transformations S and T.

Encryption:

Given a plaintext $(x'_1, ..., x'_n)$, we evaluate the map P with $(x'_1, ..., x'_n)$, and denote its result by $(y'_1, ..., y'_n)$. That is

$$y'_i = p_i(x'_1, ..., x'_n), \text{ for } i = 1, ..., n.$$

Then the corresponding ciphertext is $(y'_1, ..., y'_n)$.

Decryption:

Given the ciphertext $(y'_1, ..., y'_n)$, the process of decryption includes the following steps.

(1) Compute $(\overline{y}_1, ..., \overline{y}_n)$ by

$$(\overline{y}_1, ..., \overline{y}_n) = T^{-1}(y'_1, ..., y'_n).$$

(2) Obtain $\overline{Y}$ by computing

$$\overline{Y} = \varphi^{-1}(\overline{y}_1, ..., \overline{y}_n).$$

(3) Calculate the inverse of t, namely find v such that

$$t \cdot v \equiv \mod(q^n - 1).$$

Apply the resulted v to $\overline{Y}$, and we get $\widehat{Y}$ by

$$\widehat{Y} = \overline{Y}^v.$$

(4) Compute the set $\widehat{X}$, whose element $\widehat{X}_i$ $(1 \leq i \leq d)$ is the root of the function g for the given value $\widehat{Y}$. That is

$$g(\widehat{X}_i) = \widehat{Y}.$$

Note that Steps (3) and (4) are equivalent to computing the function $G^{-1}(\overline{Y})$.

(5) For each element $\widehat{X}_i \in \widehat{X}$, we compute

$$(x'_{i1}, ..., x'_{in}) = S^{-1} \circ \varphi(\widehat{X}_i).$$

If $i = 1$, then the solution $(x'_{11}, ..., x'_{1n})$ is our expected plaintext. Otherwise, we need apply some techniques, such as Hash Functions and Plus Method, to detect the expected plaintext.

3.3 TOT for Signature or Authentication

TOT can be used for signature, where the public key and the private key are the same as Section 3.2. For a given message $M = (y'_1, ..., y'_n)$ to be signed, the signer first calculates $\overline{Y} = \varphi^{-1} \circ T^{-1}(y'_1, ..., y'_n)$, then computes the set $\widehat{X}$ like Steps (3) and (4) of the decryption in Section 3.2. After that, the signer arbitrarily chooses an element $\overline{X}$ in the set $\widehat{X}$, and generates a signature $\sigma = (x'_1, ..., x'_n)$ on the message M by computing $(x'_1, ..., x'_n) = S^{-1} \circ \varphi(\overline{X})$. Finally, the verifier can verify the signature σ by evaluating $P(x'_1, ..., x'_n)$. If $P(x'_1, ..., x'_n) = (y'_1, ..., y'_n)$, then the signature σ is valid; otherwise, invalid.

Besides, TOT can also be used for authentication. The verifier encrypts a challenge first, then asks the user being verified for the corresponding plaintext. Therefore, the process of authentication is similar to ones in encryption and decryption of TOT.

4 Security Analysis

Currently, MPKC is still hard to rigorously reduce to some intractable problems from a provable security point of view. In general, we can analyze the security of a multivariate cryptosystem by algebraic attacks. At present, current known algebraic attacks for MPKC are divided into two classes [33]. The first one is **the structural attack** which can break some multivariate schemes according to the particular properties on the inner structure of the cryptosystem. Another is **the direct attack** that can solve a system of polynomial equations over a finite field, which usually contains Gröbner bases method [34] [35] [36] [37], XL method [38] [39] [40] and Zhuang-Zi method [41]. In the following sub-sections, we are going to adopt these approaches to elaborately analyze the TOT system. We assert that TOT is a secure multivariate cryptosystem, which can resist current known algebraic attacks if properly used.

4.1 Exhaustive Search Attack

Usually, in order to avoid exhaustive search attack [19], the length of a message M should be at least 64 bits. This can be easily realized by TOT.

4.2 Affine Multiple Attack

The affine multiple attack, which can attack the basic HFE algorithm, was introduced by Patarin [19]. The idea is that for some polynomial G, there are always some affine multiples $A(X, Y')$ of the polynomial $G(X) - Y'$. In other words, each solution X' to $G(X) = Y'$ is also a solution to $A(X, Y') = 0$. Unfortunately, this case might occur in our system. However, this is not a flaw of TOT, but it will generate a weak key of TOT. Patarin [19] claimed that the asymptotic complexity of the affine multiple attack is $O(n^{O(D)})$ for a polynomial G of degree D. We thus can easily avoid this attack. If $n \geq 64$, $D \geq 17$, and G is well chosen to contain at least two monomials in X, then the complexity of the attack is greater than 2^{102}. Therefore, this attack is expected to fail completely in our system, since the degree of G in TOT is designed to be greater than 24.

4.3 Linearization Equation Attack

The linearization equation attack was introduced to destroy C^* scheme by Patarin [9]. However, the map G of the TOT system is not a bijection, thus this attack is no longer applicable to ours.

4.4 Kipnis-Shamir Attack and Distillation Attack

The Kipnis-Shamir attack is a general cryptanalytic approach, which is based on the fact that a system of n multivariate polynomials in n variables over a field F can be represented by a single univariate polynomial over the n-extension filed

E of F. This cryptanalytic method was used to attack both the HFE scheme [7] and the Dragon scheme [42] [7] . Unfortunately, owing to employing the "big field" structure which is used in the HFE scheme, the TOT system might also be attacked by the Kipnis-Shamir method. However, from the analyses of [7] and [43], we find that the original Kipnis-Shamir attack is in at most $n^{O(\log_q^2 D)}$ for TOT. This means that when choosing $n \geq 64$, $q = 2$ and $D \geq 16$, the TOT scheme is broken in at least 2^{96}. Obviously, the Kipnis-Shamir attack has a negligible effect on our scheme. Moreover, Courtois [43] presented a new advanced attack method called the distillation attack that is more efficient than the Kipnis-Shamir attack. However, the distillation attack need $n^{\frac{3}{2}\log_q D}$ computations to break our TOT system. Therefore, if we choose proper parameters, such as $n \geq 85$, $q = 2$ and $D \geq 400$, then TOT can be broken in at least 2^{82}. In addition, with the increase of n and D, the attack complexity will increase accordingly. For example, for $n \geq 170$, $q = 2$ and $D \geq 800$, the attack needs at least 2^{108} computations to wreck TOT. According to Section 3, we know that the decryption (or the signing process) of the TOT is almost not affected by the parameter D which is the degree of $G(X)$. Thus, TOT can resist both attacks if properly used.

4.5 Differential Cryptanalysis

Differential cryptanalysis is a general and powerful method to attack some cryptographic schemes. In multivariate quadratic systems, the differential of the public key is a affine map, and the dimension of its kernel is invariant [44]. One can then utilize these facts to obtain some information on the secret key. The differential attack was successfully applied to break some multivariate schemes, such as C*, PMI and Sflash [44] [45]. However, it cannot break the TOT system. Reasons are elaborated as follows.

Let us consider the linear part of the differential of the public key P. We can define the differential of P of TOT as $DP_k(x) = P(x+k) - P(x) - P(k) - P(0)$, where $x, k \in (F)^n$. It is not difficult to infer that the dimension of the expected kernel K (in the *cleartext space*) of the map DP_k is in $O(D)$. Thus an attacker has a success probability $\frac{\varepsilon}{q^{n \cdot O(D)}}$ to find $O(D)$ linearly independent vectors to construct the kernel K by some probabilistic algorithm, where ε is a probabilistic coefficient. Obviously, the success probability is negligible. Therefore, it is unpractical to attack ours by the differential method.

4.6 Attacks using Gröbner Bases and XL

The public key of a multivariate scheme is a set of multivariate quadratic polynomials over a finite field, so any method to solve this set of equations can attack the multivariate scheme. For example, Gröbner bases algorithm and XL algorithm are two well-established and general methods. However, the XL algorithm is essentially a Gröbner basis algorithm, and can even be regarded as a redundant variant of the Gröbner basis algorithm F_4 [46]. Some results also show that the

new Gröbner basis algorithm is actually more powerful than the XL algorithm [40]. Thus, we can focus on how some multivariate scheme behaves under an attack by Gröbner bases algorithm, instead of XL algorithm [4].

For Gröbner bases algorithm, we know that computing Gröbner bases of a random system of multivariate quadratic polynomials is simply exponential in 2^n [33] [47]. Thus, from a practical point of view, when choosing $n \geq 80$, it is impossible to solve a system of n equations of degree 2 in n variables. In other words, Gröbner bases method need to run in time at least 2^{80} to break the TOT system for using the parameter $n \geq 80$. Obviously, this method is unpractical to attack our algorithm so long as we properly choose parameters of TOT.

5 Performance

5.1 Computation Complexity of TOT

As we know, for two elements of F, an addition requires $O(k)$ basic computations and a multiplication needs $O(k^2)$ basic computations [9]. Thus, we can easily compute the complexity of the components of TOT according to this fact. The resultant complexities are shown in Table 1. Moreover, we need to notice that if k is not too big, we can turn multiplication of two elements of F into a table and store it [9]. So computing TOT algorithm will be about k^2 times faster.

Table 1. The Computation Complexity of TOT

Component	Complexity
Public key generation	$O(k^2n^5)$
Private key generation	$O(k^2n^2)$
Public map	$O(k^2n^3)$
Secret map	$O(k^3n^3)$

5.2 Practical Parameters for TOT

According to the security analysis in Section 4, we can give some practical implementations of TOT.

(1) When utilizing TOT to encrypt a plaintext, we suggest that the worthy parameters are $q = 2$, $n = 160$, $d \geq 6$ and $t \geq 128$. In this case, both P and $\overline{P}$ are maps from F^{160} to F^{160}.

- The public key. It consists of 160 quadratic polynomials with 160 variables. The total number of coefficients for the public key is at least $160 \times 161 \times 162/2 = 2086560$ bits ≈ 254.71 KB.
- The private key. It consists of at least 7 elements in the field E of cardinality 2^{160}, and two affine transformations over F^{160}. The total number of coefficients for the private key is at least $2\times(160\times160+160)+7\times160 = 52640$ bits, or about 6.43 KB of storage.

– The length of ciphertext: 160 bits.
– Complexity of best known attack: greater than 2^{105}.

(2) When using TOT to sign a message, we recommend that practical parameters are $q = 2$, $n = 128$, $d \geq 6$ and $t \geq 64$. In this case, both P and $\overline{P}$ are maps from F^{128} to F^{128}.

– The public key. It consists of 128 quadratic polynomials with 128 variables. The total number of coefficients for the public key is at least $128 \times 129 \times 130/2 = 1073280$ bits ≈ 131.02 KB.
– The private key. It consists of at least 7 elements in the field E of cardinality 2^{128}, and two affine transformations over F^{128}. The total number of coefficients for the private key is at least $2\times(128\times128+128)+7\times128 = 33920$ bits, or about 4.14 KB of storage.
– The length of signature: 128 bits.
– Complexity of best known attack: greater than 2^{90}.

Overall, the security of TOT should be at least 2^{90} under our values in accordance with the existing attack complexity. We thus claim that the best known attack method against the TOT system will be the brute force checking of all possible plaintexts one-by-one.

6 Comparison with Other Multivariate Schemes

Security and efficiency that are two important factors in evaluating a cryptographic system. We are going to compare TOT with other multivariate schemes, including encryption schemes and signature schemes.

In the aspect of security level, the comparison is presented in Table 2.

In the aspect of efficiency, we compare the computation complexity of TOT with ones of HFE, HFEv, Quartz, PMI$^+$ and Sflash^{v2} from the structural point of view, as shown in Table 3. We also compare TOT with UOV and Rainbow according to the size of public/private key, since it can determine the time to verify the signature or to sign a document. The comparison on the size of message, signature, and public/private key is summarized in Table 4, where Mes., Sig., PK, and SK stands for Message, Signature, Public Key, and Private Key, respectively.

We notice that the efficiency comparison of MPKC is often reflected in computing the secret map. That is, the computation speed of the secret map can estimate whether a MPKC scheme is efficient or not.

6.1 Comparison with HFE and HFEv

From the structural point of view, the secret map of HFE contains inverting two affine transformations T_{HFE} and S_{HFE} , and inverting the central map $\overline{P}_{HFE} = \varphi \circ G_{HFE} \circ \varphi^{-1}$. Namely, computing T^{-1}_{HFE}, G^{-1}_{HFE} and S^{-1}_{HFE}. We know that the computation complexity of G^{-1}_{HFE} is $O(nD^2_{HFE} \log D_{HFE} + D^3_{HFE})$ by

Table 2. Comparison on Security Level

	Encryption	Signature
TOT	2^{105}	2^{90}
HFE [43]	2^{67}	–
PMI$^+$ [5] [18]	2^{83}	–
Sflash^{v2} [13]	–	2^{80}
HFEv [11] [20]	–	2^{80}
Quartz [21]	–	2^{80}
UOV [48]	–	$2^{83.7}$
Rainbow [49]	–	2^{87}

Table 3. Comparison on Computation

Scheme	Time
TOT	$2A^{-1} + O(log(q^n - 1)^3) + O(n)$
HFE	$2A^{-1} + O(n(q^n - 1)^2 log(q^n - 1) + (q^n - 1)^3)$
HFEv	$Time(\text{HFE}) + F_v^{-1} + O(n)$
Quartz	$Time(\text{HFE}) + F_v^{-1} + O(n)$
PMI$^+$	$2A^{-1} + O(log(q^n - 1)^3) + O(q^r)$
Sflash^{v2}	$2A^{-1} + O(log(q^n - 1)^3) + O(n)$

A^{-1} denotes the time to invert an affine transformation A.
F_v^{-1} denotes the time to invert the "vinegar" function F_v.
$Time(\cdot)$ denotes the time to call a function "$\cdot$".

Table 4. Comparison on Size of Mes/Sig/PK/SK

	Mes.	Sig.	PK	SK	Total
Unit	bits	bits	KB	KB	KB
TOT	128	128	131.02	4.14	135.16
UOV [48]	224	672	99.94	87.31	187.25
Rainbow [49]	192	336	22.17	16.86	39.03

"Total" denotes the total size of public key and secret key.

using the probabilistic Berlekamp algorithm [29] [30] [31] [32], a greater upper bound is $O(nD_{HFE}^3)$ [4], where $D_{HFE} = \deg(G_{HFE}(X))$. For TOT, the secret map also contains T^{-1}, G^{-1} and S^{-1}. However, computing $G^{-1}(\overline{Y})$ in the TOT system is transformed into computing $\widehat{Y}' = \overline{Y}^v \bmod (q^n - 1)$ and $g^{-1}(\widehat{Y}')$, namely Steps 3 and 4 in Section 3.2. The complexity of Step 3 is $O(\log(q^n - 1)^3)$ by using the square-and-multiply method. It can be done ten times faster than naive square-and-multiply method [13] [14]. The complexity of Step 4 is $O(n)$, because the degree of g is designed as a small value. Thus the total complexity of $G^{-1}(\overline{Y})$ of TOT is $O(\log(q^n - 1)^3 + n)$. For both complexities, since the range of each parameter is different, it seems difficult to compare the complexity $O(\log(q^n - 1)^3 + n)$ with $O(nD_{HFE}^2 \log D_{HFE} + D_{HFE}^3)$. However, we know that the upper bound of D_{HFE} is $O(q^n - 1)$, thus we can think in theory that $O(nD_{HFE}^2 \log D_{HFE} + D_{HFE}^3)$ is greater than $O(\log(q^n - 1)^3 + n)$. In other words, the computation speed of the secret map of TOT is faster than that of HFE, at least not slower than it.

From the security point of view, we know that D_{HFE} plays a vital role in HFE. In theory, the larger D_{HFE} is, the more secure HFE is. The situation is similar in TOT, i.e., the larger D is, the more secure TOT is. However, D_{HFE} cannot unlimitedly grow, otherwise, the decryption process of HFE is inefficient. The difference between D and D_{HFE} is that, D can expand indefinitely, while the computation speed of the secret map of TOT may be more faster. This is a beautiful point of TOT. All in all, comparing with HFE, TOT can easily gain a higher security level.

For HFEv, we know that it is a combination of HFE with the idea of Oil-Vinegar. Its efficiency and security strictly rely on the basic HFE [20] [11]. Obviously, the running speed of the secret map of TOT is also faster than that of HFEv, then TOT can also get a higher security level.

Therefore, TOT is a better choice than HFE and HFEv.

6.2 Comparison with PMI$^+$

PMI$^+$ is a combination of PMI with the plus method, namely, a few additional polynomials are added to PMI which is an extension of C* with an internal perturbation. The secret map of PMI$^+$ is the same as that of PMI. Therefore, the total computation workload of the secret map of PMI$^+$ is equivalent to computing the secret map of C* and inverting "the perturbed map". Obviously, the workload of Steps 1-3, 5 of TOT (in Section 3.2) is equivalent to computing the secret map of C*. While the workload of Step 4 of TOT is less than that of inverting the perturbed map of PMI$^+$, because inverting the perturbed map needs $O(q^r)$ basic computations to obtain tentatively a correct solution. In general, the computations of the secret map of TOT is less than that of PMI$^+$.

In the aspect of security, Ding [5] [18] claimed that the security level of PMI$^+$ is 2^{83} with given practical parameters, while the security level of TOT is greater than 2^{105} in our first example.

We conclude that our scheme should be a better choice in terms of both security and efficiency.

6.3 Comparison with Sflash^{v2}

Currently, Sflash^{v2} is still considered to be secure [14]. Sflash^{v2} is a combination of C* with the minus method. From the above analyses in Sections 6.1 and 6.2, we know that the running speed of the secret map of TOT is very close to that of C* from a structural point of view. Therefore, we believe that the signature generation process of TOT will take as much time as Sflash^{v2}.

With the parameters in [13], Sflash^{v2} generates a signature of 259 bits, and its security level is up to 2^{80}. However, our second example has a short signature of 128 bits and a security level of 2^{90}. Thus, from aspects of both security and efficiency, we believe that TOT is a better choice compared to Sflash^{v2}.

6.4 Comparison with Quartz

Quartz is a practical HFEv$^-$ signature scheme with length of 128 bits. It was accepted as a short digital signature by NESSIE (New European Schemes for Signature, Integrity, and Encryption). The parameters for a Quartz scheme [21] are $q = 2$, $D_{Quartz} = 129$, $n = 103$, $v = 4$ and $r = 3$. In this case, the public key of Quartz is a map from F^{107} to F^{100}, and has the length of 71 KB which is about 1.8 times less than our second practical example. This implies that our public computation of verifying the signature will take about 1.8 times longer. However, from the structural point of view, the computation speed of the secret map of Quartz is obviously slower than that of HFE. In Section 6.1, we knew that the computation speed of the secret map of TOT is faster than that of HFE. Therefore, the computation speed of the secret map of TOT must be faster than that of Quartz. Moreover, both TOT and Quartz can generate signatures with the same length of 128 bits.

From the secure point of view, the security level of Quartz is 2^{80}, yet ours is greater than 2^{90}. Thus, we conclude that our scheme should be a better choice in terms of both security and efficiency.

6.5 Comparison with UOV

Up to now, UOV has not been broken from the structural side. A suit of practical parameters $(2^8, 84, 28, 56)$ for UOV was given in [48]. In this case, the public key of UOV is a map from F^{84} to F^{28}, and has a length of $8 \times 28 \times (85 \times 86)/2 = 818720$ bits ≈ 99.94 KB. Its private key consists of 28 Oil-Vinegar polynomials in 56 Vinegar variables and 28 Oil variables, and an invertible affine transformation $S : F^{84} \to F^{84}$. The size of the private key is thus $8 \times 28 \times (56 \times 28 + 56 \times 55/2 + 56 + 28 + 1) = 715232$ bits ≈ 87.31 KB, which is 21 times of ours. This implies that the secret calculation to sign the message will take about 21 times longer than ours. Moreover, the total size of public and private key is also larger than ours. UOV can generate a signature of 672 bits from a message of 224 bits. The size of signature of UOV is obviously 3 times the size of its message, and this can be considered to be a weak point of UOV. While TOT can produce a short signature with 128 bits, and its signature and message own the same length.

With given practical parameters, the security level of our second example is greater than 2^{90}, while that of UOV is $2^{83.7}$.

Therefore, we still think that UOV is a better choice from both security and efficiency.

6.6 Comparison with Rainbow

Rainbow is a multi-layer UOV scheme. A set of practical parameters $GF(2^8)$ and $(18, 12, 12)$ for Rainbow was given in [49], which is a two-layer construction. Therefore, its public key consists of 24 quadratic polynomials in 42 variables. That is, the size of the public key is $8 \times 24 \times (43 \times 44)/2 = 181632$ bits $\approx$ 22.17 KB. Its private key consists of 12 polynomials in 18 Vinegar variables and 12 Oil variables in the first layer, and 12 polynomials in 30 Vinegar variables and 12 Oil variables in the second layer, and two invertible affine transformations $S : F^{42} \to F^{42}$ and $T : F^{24} \to F^{24}$. The total size of the private key is thus about 16.86 KB. Obviously, the size of the public key of Rainbow is about 6 times less than our second example, but the size of the private key of Rainbow is roughly 4 times larger than ours. Moreover, Rainbow generates a signature of 336 bits from a message of 192 bits. The size of signature is larger than that of message. This case is similar to UOV. Thus ours is better than Rainbow in this aspect. Besides, both TOT and Rainbow have almost the same security level.

7 Conclusion

We design a novel one-way trapdoor function with special properties, which can compute the secret map quickly. With the growth of t in $g(X)$, the security level of TOT can be enhanced, while the process of decryption or signing will not be affected. On the contrary, if t is properly chosen, the speed of decryption or signing can be faster. This is a good job compared to HFE, HFEv and Quartz. In addition, because the degree d of $g(X)$ is designed to choose a small value, the computation speed of the secret map of TOT is as fast as C^* and Sflash^{v2}. Meanwhile, TOT can withstand current known algebraic attacks as long as befittingly used. We give some practical implementations of TOT with the security level of greater than 2^{90}. Of course, one can choose more suitable parameters and let TOT reach a higher security level according to concrete situations. It is worth mentioning that TOT can generate a signature with the same length of 128 bits as Quartz. In terms of both security and efficiency, we believe that TOT will be a good choice for encryption, signature and authentication.

Acknowledgement

This work is supported by the National Natural Science Foundation of China (Grant Nos. U1135004 and 61170080), Guangdong Province Universities and Colleges Pearl River Scholar Funded Scheme (2011), and High-level Talents Project of Guangdong Institutions of Higher Education (2012).

The authors thank Jiahui Chen, Fengxia Li, Zhiniang Peng, and Xiaoyu Li for plenary discussions and suggestions on this paper.

References

1. Shor, P.W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing **26**(5) (1997) 1484–1509
2. Shor, P.W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Review **41**(2) (1999) 303–332
3. Bernstein, D.J., Buchmann, J.: Post-Quantum Cryptography. Springer (2009)
4. Ding, J., Schmidt, D.: Multivariate Public Key Cryptosystems. In: Advances in Information Security, Citeseer (2006)
5. Ding, J., Yang, B.Y.: Multivariate Public Key Cryptography. In: Post-Quantum Cryptography. Springer (2009) 193–241
6. Wolf, C., Preneel, B.: Taxonomy of Public Key Schemes based on the Problem of Multivariate Quadratic Equations. Cryptology ePrint Archive, Report 2005/077 (2005) http://eprint.iacr.org.
7. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In: Advances in Cryptology–CRYPTO'99, Springer (1999) 19–30
8. Matsumoto, T., Imai, H.: Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption. In: Advances in Cryptology–EUROCRYPT'88, Springer (1988) 419–453
9. Patarin, J.: Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88. In: Advances in Cryptology–CRYPTO'95. Springer (1995) 248–261
10. Patarin, J.: The Oil and Vinegar Signature Scheme. In: Dagstuhl Workshop on Cryptography. Volume 80. (1997)
11. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced Oil and Vinegar Signature Schemes. In: Advances in Cryptology–EUROCRYPT'99, Springer (1999) 206–222
12. Ding, J., Schmidt, D.: Rainbow, a New Multivariable Polynomial Signature Scheme. In: Applied Cryptography and Network Security, Springer (2005) 164–175
13. Akkar, M.L., Courtois, N.T., Duteuil, R., Goubin, L.: A Fast and Secure Implementation of Sflash. In: Public Key Cryptography–PKC 2003. Springer (2003) 267–278
14. Nicolas T. Courtois, L.G., Patarin, J.: $SFLASH^{v3}$, a Fast Asymmetric Signature Scheme. Cryptology ePrint Archive, Report 2003/211 (2003) http://eprint.iacr.org.
15. Patarin, J., Courtois, N., Goubin, L.: Flash, a Fast Multivariate Signature Algorithm. In: Topics in Cryptology–CT-RSA 2001. Springer (2001) 298–307
16. Patarin, J., Goubin, L., Courtois, N.: C^*_{-+} and HM: Variations Around Two Schemes of T. Matsumoto and H. Imai. In: Advances in Cryptology–ASIACRYPT'98, Springer (1998) 35–50
17. Ding, J.: A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation. In: Public Key Cryptography–PKC 2004. Springer (2004) 305–318
18. Ding, J., Gower, J.E.: Inoculating Multivariate Schemes against Differential Attacks. In: Public Key Cryptography–PKC 2006. Springer (2006) 290–301
19. Patarin, J.: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In Maurer, U., ed.: Advances in Cryptology–EUROCRYPT'96. Volume 1070 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (1996) 33–48

20. Ding, J., Schmidt, D.: Cryptanalysis of HFEv and Internal Perturbation of HFE. In Vaudenay, S., ed.: Public Key Cryptography–PKC 2005. Volume 3386 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2005) 288–301
21. Patarin, J., Courtois, N., Goubin, L.: Quartz, 128-bit Long Digital Signatures. In: Topics in Cryptology–CT-RSA 2001. Springer (2001) 282–297
22. Moh, T.: A Public Key System with Signature and Master Key Functions. Communications in Algebra **27**(5) (1999) 2207–2222
23. Goubin, L., Courtois, N.T.: Cryptanalysis of the TTM Cryptosystem. In: Advances in Cryptology–ASIACRYPT 2000. Springer (2000) 44–57
24. Moh, T., Chen, J.M.: On the Goubin-Courtois Attack on TTM. preprint (2001)
25. Ding, J., Schmidt, D.: The New Implementation Schemes of the TTM Cryptosystem Are Not Secure. In: Coding, Cryptography and Combinatorics. Springer (2004) 113–127
26. Chen, J.M., Yang, B.Y.: A More Secure and Efficacious TTS Signature Scheme. In: Information Security and Cryptology–ICISC 2003. Springer (2004) 320–338
27. Yang, B.Y., Chen, J.M., Natl Taiwan, U.: TTS: Rank Attacks in Tame-Like Multivariate PKCs. IACR Cryptology ePrint Archive **2004** (2004) 61
28. Ding, J., Yin, Z.: Cryptanalysis of TTS and Tame-like Multivariate Signature Schemes. In: Pre-Proceedings of the The Third International Workshop for Applied PKI, Fukuoka, Japan. (2004)
29. Berlekamp, E.R.: Factoring Polynomials over Finite Fields. Bell System Technical Journal **46**(1853-1859) (1967) 3
30. Berlekamp, E.R., Rumsey, H., Solomon, G.: On the Solution of Algebraic Equations over Finite Fields. Information and Control **10**(6) (1967) 553–564
31. Berlekamp, E.R.: Algebraic Coding Theory. Volume 111. McGraw-Hill New York (1968)
32. Berlekamp, E.R.: Factoring Polynomials over Large Finite Fields. Mathematics of Computation **24**(111) (1970) 713–735
33. Faugere, J.C., Joux, A.: Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems using Gröbner Bases. In: Advances in Cryptology–CRYPTO 2003. Springer (2003) 44–60
34. Buchberger, B.: A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner-Bases. In: Symbolic and Algebraic Computation. Springer (1979) 3–21
35. Buchberger, B.: Gröbner Bases: an Algorithmic Method in Polynomial Ideal Theory. Multidimensional Systems Theory (1985) 184–232
36. Faugere, J.C.: A New Efficient Algorithm for Computing Gröbner Bases (F_4). Journal of Pure and Applied Algebra **139**(1) (1999) 61–88
37. Faugère, J.C.: A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F_5). In: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ACM (2002) 75–83
38. Courtois, N., Klimov, A., Patarin, J., Shamir, A.: Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In: Advances in Cryptology–EUROCRYPT 2000, Springer (2000) 392–407
39. Moh, T.: On the Method of "XL" and Its Inefficiency to TTM. Cryptology ePrint Archive, Report 2001/047 (2001)
40. Diem, C.: The XL-Algorithm and a Conjecture from Commutative Algebra. In: Advances in Cryptology–ASIACRYPT 2004. Springer (2004) 323–337
41. Ding, J., Gower, J.E., Schmidt, D.S.: Zhuang-Zi: A New Algorithm for Solving Multivariate Polynomial Equations over a Finite Field. In: Workshop Record of

the International Workshop on Post-Quantum Cryptography (PQCrypto 2006). (2006) 227–240
42. Patarin, J.: Asymmetric Cryptography with a Hidden Monomial. In: Advances in Cryptology–CRYPTO'96, Springer (1996) 45–60
43. Courtois, N.T.: The Security of Hidden Field Equations (HFE). In: Topics in Cryptology–CT-RSA 2001. Springer (2001) 266–281
44. Fouque, P.A., Granboulan, L., Stern, J.: Differential Cryptanalysis for Multivariate Schemes. In: Advances in Cryptology–EUROCRYPT 2005. Springer (2005) 341–353
45. Gilbert, H., Minier, M.: Cryptanalysis of SFLASH. In: Advances in Cryptology–EUROCRYPT 2002, Springer (2002) 288–298
46. Ars, G., Faugere, J.C., Imai, H., Kawazoe, M., Sugita, M.: Comparison between XL and Gröbner Basis Algorithms. In: Advances in Cryptology–ASIACRYPT 2004. Springer (2004) 338–353
47. Bardet, M., Faugere, J.C., Salvy, B.: On the Complexity of Gröbner Basis Computation of Semi-Regular Overdetermined Algebraic Equations. In: Proceedings of the International Conference on Polynomial System Solving. (2004) 71–74
48. Thomae, E., Wolf, C.: Solving Underdetermined Systems of Multivariate Quadratic Equations Revisited. In: Public Key Cryptography–PKC 2012. Springer (2012) 156–171
49. Ding, J., Yang, B.Y., Chen, C.H.O., Chen, M.S., Cheng, C.M.: New Differential-Algebraic Attacks and Reparametrization of Rainbow. In: Applied Cryptography and Network Security, Springer (2008) 242–257