Copyright ⓒ2017 KSII

HS-Sign: A Security Enhanced UOV Signature Scheme Based on Hyper-Sphere

Jiahui Chen[1], Shaohua Tang[1]* and Xinglin Zhang[1]
[1] School of Computer Science & Engineering,South China University of Technology
Guangzhou, China
[e-mail: jhchen86@qq.com csshtang@scut.edu.cn zhxlinse@gmail.com]
*Corresponding author: Shaohua Tang

Received December 7, 2016; revised March 13, 2017; accepted March 29, 2017; published June 30, 2017

Abstract

For “generic” multivariate public key cryptography (MPKC) systems, experts believe that the Unbalanced Oil-Vinegar (UOV) scheme is a feasible signature scheme with good efficiency and acceptable security. In this paper, we address two problems that are to find inversion solution of quadratic multivariate equations and find another structure with some random Oil-Oil terms for UOV, then propose a novel signature scheme based on hyper-sphere (HS-Sign for short) which directly answers these two problems. HS-Sign is characterized by its adding Oil-Oil terms and more advantages compared to UOV. On the one side, HS-Sign is based on a new inversion algorithm from hyper-sphere over finite field, and is shown to be a more secure UOV-like scheme. More precisely, according to the security analysis, HS-Sign achieves higher security level, so that it has larger security parameters choice ranges. On the other side, HS-Sign is beneficial from both the key side and computing complexity under the same security level compared to many baseline schemes. To further support our view, we have implemented 5 different attack experiments for the security analysis and we make comparison of our new scheme and the baseline schemes with simulation programs so as to show the efficiencies. The results show that HS-Sign has exponential attack complexity and HS-Sign is competitive with other signature schemes in terms of the length of the message, length of the signature, size of the public key, size of the secret key, signing time and verification time.

Keywords: Multivariate Cryptography; UOV Signature Scheme; Hyper-sphere

This work was supported by the National Natural Science Foundation of China (Nos. 61632013, U1135004 and 61170080), 973 Program (No. 2014CB360501), Guangdong Provincial Natural Science Foundation (No. 2014A030308006), and Guangdong Provincial Project of Science and Technology (No. 2016B090920081).

https://doi.org/10.3837/tiis.2017.06.020 **ISSN : 1976-7277**

1. Introduction

In recent years, finding alternative public key cryptosystem which has resistance against a quantum computer has become a vital challenge, i.e., when a practical quantum computer is built so the public key cryptosystems used today (RSA, ECC, El Gamal, etc.) are broken. The multivariate public key cryptography (MPKC) is one of the promising candidates for post-quantum cryptography. In order to resist the attacks of quantum computing, the Post-Quantum Cryptography [1] has attracted cryptographers' intensive attentions. Some cryptosystems, such as hash-based cryptography, coding-based cryptography, lattice-based cryptography and multivariate public key cryptography (MPKC), belong to the area of Post-Quantum Cryptography. Security of MPKC is based on the hardness of solving a set of multivariate polynomial equations over a finite field, which is called an MQ problem [2] and is proven to be an NP-hard problem [3-4], and the quantum computers do not appear to have any advantages when dealing with this NP-hard problems. Except resistance to quantum computer attacks, MPKC enjoys other beneficial properties. In particular, they are quite fast compared to conventional schemes and require only very moderate resources, since the arithmetic operations are performed over a small finite field. This makes MPKC systems excellent candidates for use in resource constraint devices, like WSN nodes, RFIDs and smart cards, etc. However, there are two drawbacks that become obstacles to use MPKC systems. The first one is the largeness of its key sizes. The second drawback is that the security of MPKC relies both on the MQ problem and on the Isomorphism of Polynomials (IP) problem, so the schemes in MPKC may be faced with not only direct attacks but also structural attacks. Under this situation, quite a few attempts have been undertaken in order to tackle these two problems. For example, in the recent paper [5] the authors undertook an attempt to reduce the public key size, based on yet unbroken (under proper parameter choice) Unbalanced Oil and Vinegar (UOV) scheme [6]. Sakumoto et al. proposed provably secure identification/signature schemes based on the MQ problem [2]. There has been plenty of proposals for MPKC systems, as is explained in the overview in [7][1]. On the disadvantage for the designers, the cryptanalytic process has also been substantial. New proposals aim mainly at fixing problems exposed by the cryptanalysis, but then it often happens that “fixed” proposals get broken again. This is due to the fact that little attention has been given to provable security for the MPKC schemes. Although some expert studied provable security against key-only attack on Quartz which is a variant of HFE [8], the security against chosen-message attack is unclear.

Traditionally, basing on the four basic schemes MI [9], HFE [8], STS [10] and UOV [6], the MQ public key cryptosystems are divided in four groups. The first two are known as mixed field and they use a ground field and an extension field to construct the trapdoor. The last two are single field systems, and the trapdoor is constructed only in one field with some specific structure. In addition, one uses the Plus method, the Minus method and the Perturbed method to modify MI and HFE. Therefore, there are many variant schemes, such as Sflash [11], C*-+[12], PMI [13], PMI+ [14], HFE- [15], HFE+ [15], IPHFE[16], HFEv [6][16], Quartz [17] and so on. It is clear that secure MPKC schemes are extremely rare. Recently, researchers have proposed some new multivariate cryptosystems, such as HLY-2012 scheme [18], YTS-2013 scheme [19], ABC [20], matrix-based Rainbow [21], YTS-2014 scheme [22], cubic-ABC [23], ZHFE [24], RGB [25] and the extension field cancellation by Ding et al. [26]. However, we need more time to verify their securities. Also, current focus on MPKC is developing

``advanced" cryptosystems, such as threshold ring signature scheme [27], proxy signature [28] and online/offline signature [29].

In this paper, we focus on the single field system, and take a different path to explore a new trapdoor to construct a scheme.

1.1 Motivation and Contribution

For “generic” quadratic systems, experts believe that the Unbalanced Oil-Vinegar (UOV) scheme [6] is a feasible signature scheme with good efficiency and acceptable security. The UOV scheme is a well-known and deeply studied scheme in MPKC. This scheme uses a trapdoor one-way function whose security relies both on the MQ problem and on the isomorphism of polynomials (IP) problem (which will be described in the next section). To see deeply, since there are no Oil-Oil quadratic terms in the central map of UOV, the inversion of UOV scheme (to solve the Oil variate after fixing the Vinegar variate) is equal to solve a system of linear multivariate equations. And the UOV scheme is an extensive scheme of balanced Oil and Vinegar scheme [30], which is broken by [31]. The main weakness of [30] is that to construct linear multivariate equations, its central map lacks Oil-Oil terms, this fact makes it have less resistant to some structural attack (i.e. separation attack of Oil and Vinegar variate [31]). So our motivation comes directly, to get a more secure UOV-like scheme, two problems we address are therefore: Is there another inversion solution of quadratic multivariate equations so as to replace the inversion solution to linear multivariate equations? Can we find another structure with some random Oil-Oil terms and it can also construct an UOV-like trapdoor?.

Our contribution is twofold. On the theoretical side, we explore a new inversion algorithm based on hyper sphere which can be efficiently used to construct multivariate public key cryptosystem, we then use this trapdoor to construct a new UOV-like signature scheme, which directly answers the above two questions. Analysis and theories are provided to show the security and efficiencies of our proposed scheme. On the practical side, we have implemented 5 different attack experiments for our new scheme to show its security and also we have programmed for our scheme and some baseline schemes so as to show its efficiency.

In this paper, motivated by the above analysis, we proposed a novel signature scheme called HS-Sign which is based on a new inversion algorithm from hyper-sphere over finite field, and is shown to be a more secure UOV-like scheme.

1.2 Organization

The rest of the paper is organized as follows. In Section 2, we describe the preliminaries about hyper-spheres, signature models, multivariate cryptography and basic UOV signature scheme. We present HS-Sign scheme in Section 3. Then we give security analysis in Section 4 which contains a plenty of attack experiments. Experiments and comparisons are given in Section 5. Finally, in Section 6, we conclude the paper with a discussion.

2. Preliminaries

2.1 Hyper-sphere

In general, An N-dimensional hyper-sphere (also call an N-sphere) for any natural number $N \in \mathrm{N}$ (N presents all the natural numbers), is a generalization of the surface of an ordinary sphere to arbitrary dimension. Particularly, a 0-sphere is a pair of points on a line, an 1-sphere

is a circle in a plane, and a 2-sphere is an ordinary sphere in three-dimensional space, as is illustrated in **Fig. 1**. For spheres with dimension $N > 2$, we call them hyper-spheres.

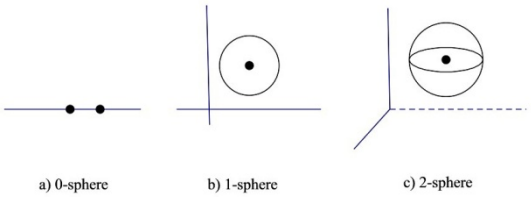

Fig. 1. Particular spheres

2.1.1 Hyper-sphere in Euclidean Space

An (N-1)-sphere of radius $r \in \mathrm{N}$ with a central point $C = (c_1, c_2, ..., c_N) \in \mathrm{R}^N$ is defined as the set ofpoints in N-dimensional Euclidean space which are at distance r from the central point C. Any point $X = (x_1, x_2, ..., x_N) \in \mathrm{N}^N$ on the hyper-sphere can be represented by the equation

$$(x_1 - c_1)^2 + (x_2 - c_2)^2 + ... + (x_N - c_N)^2 = r^2. \tag{1}$$

Any given N+1 points $G_i = (g_{i,1}, g_{i,2}, ..., g_{i,N}) \in \mathrm{N}^N, i = (1, 2, ..., N+1)$, can uniquely determine a hyper-sphere as long as certain conditions are satisfied, which is described in [32]. That is, by applying the coordinates of the points $G_1, G_2, ..., G_{N+1}$ to the above fomula, we can obtain a system of N + 1 equations

$$\begin{cases} (g_{1,1} - c_1)^2 + (g_{1,2} - c_2)^2 + ... + (g_{1,N} - c_N)^2 = r^2 \\ (g_{2,1} - c_1)^2 + (g_{2,2} - c_2)^2 + ... + (g_{2,N} - c_N)^2 = r^2 \\ \quad ... \\ (g_{N+1,1} - c_1)^2 + (g_{N+1,2} - c_2)^2 + ... + (g_{N+1,N} - c_N)^2 = r^2 \end{cases} \tag{2}$$

Then we can obtain a system of linear equations with N unknowns $(c_1, c_2, ..., c_N)$:

$$\begin{cases} 2(g_{1,1} - g_{2,1})c_1 + 2(g_{1,2} - g_{2,2})c_2 + ... + 2(g_{1,N} - g_{2,N})c_N = \sum_{j=1}^{N} (g_{1,j}^2 - g_{2,j}^2) \\ 2(g_{2,1} - g_{3,1})c_1 + 2(g_{2,2} - g_{3,2})c_2 + ... + 2(g_{2,N} - g_{3,N})c_N = \sum_{j=1}^{N} (g_{2,j}^2 - g_{3,j}^2) \\ \quad ... \\ 2(g_{N,1} - g_{N+1,1})c_1 + ... + 2(g_{N,N} - g_{N+1,N})c_N = \sum_{j=1}^{N} (g_{N,j}^2 - g_{N+1,j}^2) \end{cases} \tag{3}$$

For this system of linear equations, if and only if the determinant of the coefficients in (3) is non-zero, we can have a unique solution (c_1,c_2,...,c_N). By applying the values of (c_1,c_2,...,c_N) to one of the equations in (2), we can obtain r_2.

2.1.1 Hyper-sphere over Finite Field

Here we extend the concept of Hyper-sphere to finite fields. For simplicity, the Galois field $GF(p)$ is adopted as the ground field, where p is a large prime number. However, the results can be easily extended to other forms of finite fields. For any given positive integer N, and vector $C=(c_1,c_2,...,c_N)\in GF(p)^N$, we define function $\mathrm{R}:GF(p)^N\to GF(p)$ as

$$\mathrm{R}(X)=\| X-C\|^2 \pmod p,$$

where $X=(x_1,x_2,...,x_N)\in GF(p)^N$, and $\| X-C\|^2=(x_1-c_1)^2+...+(x_N-c_N)^2$.

Specifically, a sphere over finite field is defined by

$$\mathrm{R}(X)=\bar{R}(\mathrm{mod}\ p), \tag{4}$$

where $\bar{R}\in GF(p)$. And it is a trivial case of hyper-sphere over finite field if N = 2 in (4), and a circle over finite field is another special case of hyper-sphere over finite field if N = 1. Given N, C and $\bar{R}$, we can find at least p^{N-1}different points on the hyper-sphere determined by C and $\bar{R}$. This fact is proven by Theorem 1 in the supplementary file of [32].

2.2 Signature Scheme

Difinition 1. A signature scheme (Gen, Sign, Ver) is defined as follows:

Gen: is a probabilistic algorithm which given 1^{λ}, outputs a pair ofmatching public and secret keys (pk,sk).

Sign: is a probabilistic algorithm which takes the message M to be signed and a secret key sk, and returns a signature $\sigma = \mathrm{Sign}_{sk}(M)$.

Ver: takes a message M, a candidate signature σ and pk, and returns a bit $\mathrm{Ver}_{pk}(M,\sigma)$. The signature is accepted only if the bit is equal to one. Otherwise, it is rejected. If $\sigma \leftarrow \mathrm{Sign}_{sk}(M)$, then $\mathrm{Ver}_{pk}(M, \sigma) = 1$.

2.3 Multivariate Cryptography

The basic objects of multivariate cryptography are systems of multivariate quadratic equations over a finite field $K=GF(p)$. Such a system of m questions in n variables is defined as

$$\begin{cases} \sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij}^{(1)}\cdot x_i\cdot x_j+\sum_{j=i}^{n}\beta_i^{(1)}\cdot x_i+\gamma_i^{(1)}=0 \\ \qquad\qquad ... \\ \sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij}^{(m)}\cdot x_i\cdot x_j+\sum_{j=i}^{n}\beta_i^{(m)}\cdot x_i+\gamma_i^{(m)}=0. \end{cases} \tag{5}$$

The security of multivariate cryptosystems is based on the MQ-Problem which is defined as follows:

Definition 2. Given m quadratic polynomials $p_1,...,p_m$ in n variables over a finite field, find a vector $\mathbf{x}=(x_1,...,x_n)\in K^n$ such that $p_1(\mathbf{x})=...=p_m(\mathbf{x})=0$.

This problem is proven to be NP-hard even for quadratic systems over the field of two elements [4].

However, for most of the existing multivariate public key cryptosystems, the coefficients of the public system P (P is a collection of m quadratic polynomials $p_1,...,p_m$ in n variables) are not chosen randomly. Instead one starts with an easily invertible quadratic map F (called central map) and combines it with two invertible affine maps S and T to get a public key of the form $P = S \circ F \circ T$. Therefore, the security of the scheme is based not only on the MQ-Problem, but also on the IP-Problem (defined as follows).

Definition 3. The Problem of Isomorphism of Polynomials (abbreviated IP Problem) is the problem to find an isomorphism (S,T) from P to F, where P and F are two public sets of u quadratic equations, and S and T are isomorphic.

There is not much knowledge about the hardness of the IP-Problem, and this is the main obstacle for researchers to give security proofs for their multivariate public key cryptosystems.

2.4 UOV Signature Scheme

The idea of the Oil and Vinegar trapdoor was first proposed by J. Patarin and comes from his cryptanalysis of the Matsumoto-Imai scheme [9]. However, the original scheme was broken by Kipnis and Shamir in [31], and it was recommended in [6] to choose $v > o$ (Unbalanced Oil and Vinegar). The UOV scheme is a single field construction, so we work solely in the polynomial ring $K[X]$, where $X = x_1,...,x_n$. We divide the variable set X into two sets: Vinegar variables $(x_i)_{i \in V}$, $V = \{1,...,v\}$ and Oil variables $(x_i)_{i \in O}$, $O = \{v + 1,...,n\}$. Here $|V| = v$, $|O| = o$ and $v + o = n$. We define o quadratic polynomials $q_k(X) = q_k(x_1,...,x_n)$ by

$$q_k(X) = \sum_{i \in O,\, j \in V} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j \in V,\, i \le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V \cup O} \gamma_i^{(k)} x_i + \eta^{(k)}, k = 1,...,o \quad (6)$$

The map $Q = (q_1(X),...,q_o(X))$ can be easily inverted. First, we choose the values of the v Vinegar variables $x_1,...,x_v$ at random. Then we may get a system of o linear equations in the o variables $x_{v+1},...,x_n$ which can be solved by Gaussian elimination. If it does not have a solution, we simply choose other values of $x_1,...,x_v$ and try again. The public key P of the UOV scheme consists of o quadratic polynomials in n variables:

$$P = (p^{(1)},..., p^{(o)})$$

$$= \left(\sum_{i=1}^{n} \sum_{j=i}^{n} p_{ij}^{(1)} x_i x_j + \sum_{i=1}^{n} p_i^{(1)} x_i + p_0^{(1)},..., \sum_{i=1}^{n} \sum_{j=i}^{n} p_{ij}^{(o)} x_i x_j + \sum_{i=1}^{n} p_i^{(o)} x_i + p_0^{(o)} \right).$$

To hide the structure of Q in the public key, one concatenates it with an affine invertible map $T : F^n \to F^n$, then the public key of the UOV signature scheme is $P = Q \circ T$.

3. Description of Our Signature Scheme

3.1 New Inversion Algorithm from N-dimensional Hyper-sphere over Finite Field

As we have mentioned before, we are interested in finding some technique to solve multivariate equations with certain quadratic terms. Luckily we find that it can be solved using technique of N-dimensional hyper-sphere over finite field. The method is straight-forward. Assume we have to solve a system of multivariate equations as follows:

$$\begin{cases} (x_1 - c_{1,1})^2 + (x_2 - c_{1,2})^2 + \ldots + (x_n - c_{1,n})^2 = r_1 \\ (x_1 - c_{2,1})^2 + (x_2 - c_{2,2})^2 + \ldots + (x_n - c_{2,n})^2 = r_2 \\ \ldots \\ (x_1 - c_{m,1})^2 + (x_2 - c_{m,2})^2 + \ldots + (x_n - c_{m,n})^2 = r_m \end{cases} \tag{7}$$

If we treat the variate $(x_1,x_2,\ldots,x_n)$ as a point on the $(n-1)$-sphere determined by $C = (c_{1,1},c_{1,2},\ldots,c_{1,n})$ and r_1. Solving the first one of the above equations is equal to find a point of p^{N-1}different points on such hyper-sphere, Similarly, solving the first two of the above equations is to find a point of different points on the intersection of two $(n-1)$-spheres determined by $C = (c_{1,1},c_{1,2},\ldots,c_{1,n})$ and r_1 and $C = (c_{2,1},c_{2,2},\ldots,c_{2,n})$ and r_2, respectively. If there is no intersection of these hyper-spheres, the solution fails and there is no solution for these equations. To illustrate, we can take a look at the 1-sphere situation. That is, assume we want to solve a system of multivariate equations with two variate as follows:

$$\begin{cases} (x_1 - c_{11})^2 + (x_2 - c_{12})^2 = r_1 \\ (x_1 - c_{21})^2 + (x_2 - c_{22})^2 = r_2 \\ (x_1 - c_{31})^2 + (x_2 - c_{32})^2 = r_3 \end{cases}.$$

Without loss of generality, we assume these three equations form three circle (A_1,A_2,A_3) in a plane in **Fig. 2**. The inversion of such system is to find the intersection point of these three circle (named G in **Fig. 2**). On the other side, if we assume these three equations form three circle (A_1,A_2,A_4) in a plane in **Fig. 2**. It is obviously there is no intersection of these three hyper-spheres, the solution fails and there is no solution for this system. In addition, assume that there are only two equations from two circle in the system as follows

$$\begin{cases} (x_1 - c_{11})^2 + (x_2 - c_{12})^2 = r_1 \\ (x_1 - c_{21})^2 + (x_2 - c_{22})^2 = r_2 \end{cases}.$$

If these two equations are form two circle (A_1,A_2) in a plane in **Fig. 2**, we can see that there are two solutions (point G and point E in **Fig. 2**). However, if these two equations are form two circle (A_2,A_4), there is no solution for this system.

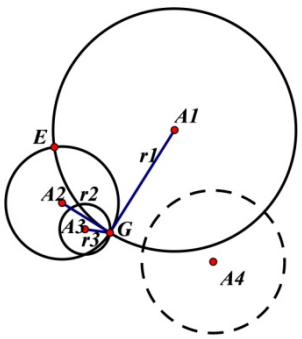

Fig. 2. Inversion example for 1-sphere

As the same situation on linear inversion of UOV scheme, we do not need to consider whether there is solution or not, since we can just reselect the value of vinegar variate to fix it. Thereby, the main problem of inversion becomes how to find a point on the intersection of the hyper-spheres in a system if we assume there is indeed some intersection of all the hyper-spheres. Our inversion algorithm of a systems like (7) can be described as follows in **Algorithm 1**:

Algorithm 1 Inversion(*sys*)

Input:

sys: *m* equations of (*n*-1)-spheres with the form (7);

Output:

X: $X = (x_1,...,x_n)$ is the coordinates of a point in *n*-dimension space ;

1: Obtain m equations with n multivariate from sys:

$$\begin{cases} (x_1 - c_{1,1})^2 + (x_2 - c_{1,2})^2 + ... + (x_n - c_{1,n})^2 = y_1 \\ (x_1 - c_{2,1})^2 + (x_2 - c_{2,2})^2 + ... + (x_n - c_{2,n})^2 = y_2 \\ ... \\ (x_1 - c_{m,1})^2 + (x_2 - c_{m,2})^2 + ... + (x_n - c_{m,n})^2 = y_m \end{cases};$$

2: Subtract the above *j*-th equation from the (*j* + 1)-th equation, *j* = 1,2,...,*m* and obtain :

$$\begin{cases} (2c_{2,1} - 2c_{1,1})x_1 + ... + (2c_{2,n} - 2c_{1,n})x_n + (c_{1,1}^2 - c_{2,1}^2) + ... + (c_{1,n}^2 - c_{2,n}^2) = y_1 - y_2 \\ ... \\ (2c_{m,1} - 2c_{m-1,1})x_1 + ... + (2c_{m,n} - 2c_{m-1,n})x_n + (c_{m-1,1}^2 - c_{m,1}^2) + ... + (c_{m-1,n}^2 - c_{m,n}^2) = y_{m-1} - y_m \end{cases};$$

3: **Repeat**

4: Randomly choose the values of the last *n*-*m* multivariate ($x_m,..,x_n$) in *K* and obtain:

$$\begin{cases} (2c_{2,1} - 2c_{1,1})x_1 + ... + (2c_{2,m-1} - 2c_{1,m-1})x_{m-1} = r_1 \\ ... \\ (2c_{m,1} - 2c_{m-1,1})x_1 + ... + (2c_{m,m-1} - 2c_{m-1,m-1})x_{m-1} = r_{m-1}, \end{cases}$$

where $r_i = y_i - y_{i+1} + \sum_{j=m}^{n} (2c_{i,j} - 2c_{i+1,j})x_j + \sum_{j=1}^{n} (c_{i+1,j}^2 - c_{i,j}^2), 1 \le i \le m-1;$

5: Solve the above equations using Gauss elimination and obtain $x_1,..,x_{m-1}$;

6: **Until** $(x_1 - c_{11})^2 + (x_2 - c_{12})^2 + ...(x_n - c_{1n})^2 = y_1$

7: **Return** $X = (x_1, ..., x_n)$.

From the above algorithm, we can see that the inversion needs also only the linear elimination, so the computing complexity is competitive. But you can see we will have many advantages below in our constructions.

3.2 HS-Sign: The Proposed UOV-like Signature Scheme

Similar to the UOV scheme, our proposed scheme is also a single field construction, so we work solely in the polynomial ring *K*[*X*], where $X = x_1,...,x_n$. We divide the variable set *X* into two sets: Vinegar variables $(x_i)_i \in V = \{1,...,v\}$ and Oil variables $(x_i)_i \in O = \{v + 1,...,n\}$.

Here $|V| = v$, $|O| = o$ and $v + o = n$. We use a new set V_O denotes the first o variables of the vinegar variables. Then we define m quadratic polynomials $q_k(X) = q_k(x_1,...,x_n)$ by

$$q_k(X) = \sum_{i\in O,\, j\in V_O} \alpha_i (x_i - c_{ij}^{(k)} x_j)^2 + \sum_{i,\, j\in V, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V} \gamma_i^{(k)} x_i + \eta^{(k)} \tag{8}$$

where α_i, $c_{ij}^{(k)}$, $\beta_{ij}^{(k)}$, $\gamma_i^{(k)}$, $\eta^{(k)}$ are randomly selected in the ground field K, and map $Q = (q_1(X), \ldots, q_m(X))$ is kept as secret key and can be easily inverted. The inversion is straightforward. Firstly, we divide all the equations with α_i. Secondly, we choose the values of the v vinegar variables at random. Then we can get a system of m equations with the form of hyper-spheres in the o variables $x_1,...,x_o$ which can be solved by using the above inversion algorithm described in Algorithm 1. Also, to hide the structure of the above Q in the public key, we concatenate it with an affine invertible map T, then the public key of our proposed signature scheme is $P = Q \circ T$.

3.3 Construction of HS-Sign

The details of our scheme are as follows.

The key generation algorithm Gen (described in **Algorithm 2**) takes as inputs the underlying field, the number of Oil and Vinegar variables, the number of multivariate quadratic polynomials and returns the private central map Q ,the hiding affine invertible map T and the public map P, where $P = Q \circ T$.

Algorithm 2 Gen(K,o,v,m)

Input:
K: the ground field (e.g. $K = GF(31)$);
o,v: the number of Oil and Vinegar variables respectively;
m: the number of multivariate quadratic polynomials;

Output:
(Q,T): the private central map Q ,the hiding affine invertible map $T : F^n \rightarrow F^n$;
P: the public map P, where $P = Q \circ T$;

1: Choose coefficients of the central map at random and construct Q with m quadratic polynomials in the form of (8);
2: Choose an $n \times n$ invertible matrix T at random, where $n = o + v$; :
3: Compute coefficients of public polynomials by composing Q and T and construct$P$;
4: **Return** (Q, T, P).

The construction of signing algorithm Sign of our scheme is to use the above inversion **Algorithm 1** and is described in **Algorithm 3**.

Algorithm 3 Sign(M,(T,Q))

Input:
M: *t*he message to sign;
(T,Q): the private key to sign the message;

Output:
V : the signature on message M;

1: $y \leftarrow M$;
2: **Repeat**
3: $x_v \in_R k^v$;
4: Substitute x_v into Q and get a system of equations $Q = y$;
5: Divide each equations with α_i and get a system like (7);
6: Solve the system and get $x_n = X$ using **algorithm 1**;
7: **Until** $x_n \neq \varnothing$;
8: $X \leftarrow T^{-1}(x_n, x_v)$;
9: **Return** $V = X$.

At last, the verification algorithm Ver(V ,M) returns 1 if $P(V) = M$, otherwise it returns 0.

4. Security Analysis

We begin this section by an observation.

Observation 1. *HS-Sign is as least as secure as the UOV scheme. More precisely, it is equal to a UOV scheme with some random Oil-Oil terms.*

proof. Typically, the central map Q of our construction is

$$q_k(X) = \sum\nolimits_{i\in O, j\in V_O} \alpha_i (x_i - c_{ij}^{(k)} x_j)^2 + \sum_{i,j\in V, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V} \gamma_i^{(k)} x_i + \eta^{(k)},$$

by expansion, the multivariate polynomials become

$$q_k(X) = \sum_{i\in O} \alpha_i x_i^2 + \sum\nolimits_{i\in O, j\in V_O} 2\alpha_i c_{ij}^{(k)} x_i x_j + \sum\nolimits_{i\in O, j\in V_O} \alpha_i x_j^2 + \sum_{i,j\in V, i\le j} \beta_{ij}^{(k)} x_j^2 + \sum_{i\in V} \gamma_i^{(k)} x_i + \eta^{(k)},$$

if we let

$$\lambda_{ij}^{(k)} = 2\alpha_i c_{ij}^{(k)}, \mu_{ij}^{(k)} = \begin{cases} \alpha_i + \beta_{ij}^{(k)}, i = j \\ \beta_{ij}^{(k)}, others \end{cases}.$$

Then the multivariate polynomials become

$$q_k(X) = \sum_{i\in O} \alpha_i x_i^2 +$$

$$\sum\nolimits_{i\in O, j\in V_O} \lambda_{ij}^{(k)} x_i x_j + \sum_{i,j\in V, i\le j} \mu_{ij}^{(k)} x_j^2 + \sum_{i\in V} \gamma_i^{(k)} x_i + \eta^{(k)}.$$

Since α_i, $c_{ij}^{(k)}$, $\beta_{ij}^{(k)}$, $\gamma_i^{(k)}$, $\eta^{(k)}$ are randomly selected in K, $\lambda_{ij}^{(k)}, \mu_{ij}^{(k)}$ are also random, compare the above polynomials with a UOV center map, it is obvious that the polynomials is a UOV structure with some random Oil quadratic terms $(\sum_{i\in O} \alpha_i x_i^2)$. So our proposed signature scheme is equal to a basic UOV scheme with some random Oil-Oil terms.

Next we will study the security of the current attack technique on our proposed scheme in order to additionally show how much we get from this observation.

4.1 The Kipnis and Shamir Attack

The Kipnis and Shamir Attack [31] is first proposed by Kipnis and Shamir to attack the balanced Oil and Vinegar (OV) scheme. The goal of this attack is to find the pre-image of the Oil subspace $O = \{x \in K_n: x_1 = ... = x_v = 0\}$ under the affine invertible transformation T. To

achieve this, it forms a random linear combination $P = \sum_{j=1}^{o} \beta_j H_j$, multiplies it with the inverse of one of the H_i and figures out the invariant subspaces of this matrix.

The Kipnis and Shamir attack is extremely efficient to the OV scheme. Since there are no Oil-Oil terms in the OV scheme, it takes only $O(m^4)$ to break a (q,v,o)-OV scheme. However, in the balanced situation of HS- Sign, this attack is useless because of the existence of o random Oil-Oil terms. Taking into account a exhaustive search for these random variate, the complexity of this attack on HS-Sign is $O(q^o m^4)$.

Now we take a look at the unbalanced situation, as described in the recent technique [33], the Kipnis and Shamir attack takes time about $O(q^{v-o-1}o^4)$ to break a (q,v,o)-UOV scheme. However, while using such technique to attack HS-Sign, the invariant Oil subspaces is not unique, and is hidden by the inserting random Oil quadratic terms, also taking into account the enumeration of the random Oil quadratic terms, it will take time about $O(q^{v-1}o^4)$ to break HS-Sign scheme.

To illustrate, we give an analysis example below. If we represent a UOV scheme's central polynomial by its corresponding matrix, and the Vinegar variables are denoted by its first v = 52 variables. Then the matrices of the polynomials in central equation should be in the form of **Fig. 3**.

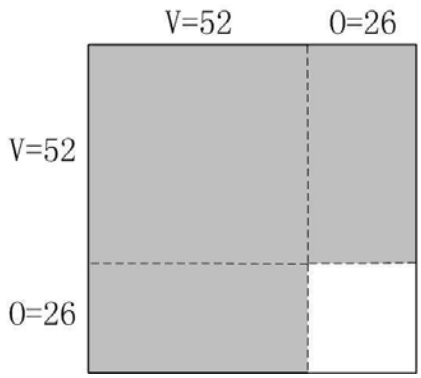

Fig. 3. Corresponding Matrix of Oil-Vinegar Scheme

In **Fig. 3**, the grey areas represent the random entries while blank areas denote zero entries. The rest part of this paper follows the same rules. If we represent an HS-Sign's central polynomial by its corresponding matrix, and the Vinegar variables are denoted by its first v = 52 variables. Then the matrices of the polynomials in central equation should be in the form of **Fig. 4**.

To further show the above situation of resistance to KS attack in both schemes, we run three small parameters tests programmed with MAGMA [34] v2.20-5, which contains an efficient implementation of F_4 algorithm [35] for computing Gröbner bases. All experiments are running on an Inspur NF5280M3 server, with two Intel Xeon E5-2660V2 CPUs (10 cores and 2.2GHz each core) and 192 GB of main memory and the operation system is RedHat Linux 6.4. Each scheme we test for 100 times and record its average attacking time. The result is shown in **Table 1**.

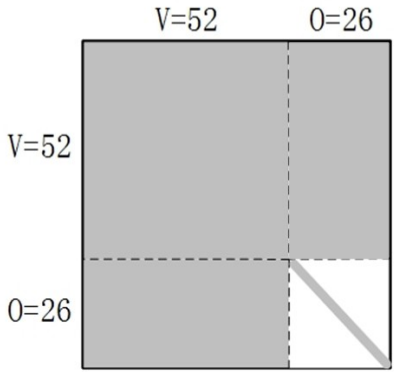

Fig. 4. Corresponding Matrix of HS-Sign

Table 1. Result of experiments with KS attack

Schemes	UOV	HS-Sign
Parameters 1	(GF (5),4,4)	(GF (5),4,4)
Time(s)	0	1.566
Memory(MB)	128	128
Parameters 2	(GF (5),4,8)	(GF (5),4,8,4)
Time(s)	13.211	15.435
Memory(MB)	128	128
Parameters 3	(GF (7),3,6)	(GF (7),3,6,4)
Time(s)	16.861	18.92
Memory(MB)	128	128

From **Table 1** we can see that the attacks of UOV is extremely fast when $o = v$, while it requires a few seconds to attack HS-Sign with the same parameters. Also the attack requirements of HS-Sign is larger than that of UOV in the same unbalanced parameters.
Note that this is an inspiring result on HS-Sign, which means that we can choose a wider range of parameters, i.e., even choose the same number of Oil and Vinegar variate.

4.2 Exhaustive Search Attack

The best exhaustive search algorithm is described in [36], which breaks MQ(n, m, F_2) in $2n+2\cdot \log 2n$ bit operations. Additionally, a traditional exhaustive search algorithm needs $q \cdot (n + 1) \cdot q^n$ bit operations to break our scheme.

Note that the best exhaustive search attack algorithm is valid only under the field of characteristic 2. To the best of our knowledge, there is still no other fast algorithms solving arbitrary fields. In the case of HS-Sign, it only uses the field of odd characteristic, which makes it efficiently be resistant to exhaustive search attack.

4.3 Rank Attack

Let H_i be the symmetric matrix representing the homogenous quadratic part of the i-th public polynomial. In the MinRank attack one tries to find linear combinations $H = \sum_{i=1}^{m} \alpha_i H_i$ of the matrices representing the homogeneous quadratic parts of the public polynomials such that rank(H) = r_{len}. While in the HighRank attack one tries to identify the variables appearing the lowest number of times in the central equations. To do this, one forms random linear combinations H of the matrices H_i, if H has nontrivial kernel, one checks if the solution set of

equation $(\sum_{i=1}^{m} \lambda_i H_i) \cdot \ker H = 0$ has dimension *n-o*. In the case of HS-Sign, one can find that all the matrices Qi representing the homogeneous quadratic parts of the central equations have full rank *n*. And this prevents the MinRank attack. Furthermore, all variables $x_1,...,x_n$ appear in each of the *o* central equations, which prevents HighRank attacks. More precisely, the full rank rate in the associated central symmetric matrix of HS-Sign is close to $\frac{q^{n(n-1)/2}\prod_{i=1}^{n}(q^i-1)}{q^{n^2}}$ (equal to the full rank rate of random matrix).

To further show this fact, similar to the work in [5], we run 10000 rank tests on each HS-Sign and record rank situation of them. The result is shown in **Table 2**.

Table 2. Rank situation of 10000 rank tests in HS-Sign (*GF*(31))

HS-Sign	(o,v,m)	(8,16,8)	(10,20,10)	(12,24,12)	(16,32,16)	(20,40,20)
Rank(*H*)	*n*	9965	9960	9959	9964	9958
	n-1	35	40	41	36	42
	n-2	0	0	0	0	0

4.4 Direct Attack

There are many direct attack algorithms working on MPKCs, such as Gröbner basis techniques and its variants F_4 [35]. The idea of direct attack on our scheme is to add *n-m* linear equations. In this way, the number of variables can be reduced to *m* so as to create a determined system. On the other hand, a system with *v+o* variables and *m* equations is expected to have $q^{(n-m)}$solutions on average. Therefore, adding a total of *n-m* linear equations will lead to one solution on average. Repeating this experiment a few times, we will find at least one solution. Still the concrete complexity of these algorithms are not fixed, but experts believe [37] that these methods will go up to a certain degree D_0 and then require the solution of a system of linear equations with *T* variables, where *T* is greater than $\binom{n}{D_0-1}$, and this will take at least $poly(n)\cdot T^2$ bit operations, where $poly(n) = 3(n)(n\text{-}1)/2$ under some hard assumptions.

In the case of HS-Sign, because of the linear affine transformation *T*, despite the difference of our construction of central map from a regular UOV, HS-Sign's public key also look totally random. Thus we expect HS-Sign have the same security level against direct attack as a regular UOV. To further show that our scheme can resist direct attack, we also carried out a number of experiments with MAGMA [34] v2.20-5, **Table 3** shows the results of our experiments to attack an instance of our scheme in *GF*(31).

As **Table 3** shows, the time and memory complexity increase as *n* grows. Also the memory increases as *n* grows which indicated that complexity is exponential. And we also chose random quadratic equations of the same dimensions as described in **Table 4**. It can find that the time and memory needed to solve such equations using Gröbner bases is essentially the same that is needed to solve the quadratic equations from HS-Sign.

Table 3. Result of experiments with direct attack on HS-Sign

Parameters	Time(ms)	Memory(MB)
$o = 3, v = 6, m = 4$	0.020	0.4
$o = 4, v = 8, m = 5$	0.250	30
$o = 5, v = 10, m = 6$	3.660	840
$o = 6, v = 12, m = 7$	326.600	7061
$o = 7, v = 14, m = 8$	11780	170021

Table 4. Result of experiments with direct attack on random quadratic equations

Parameters	Time(ms)	Memory(MB)
n=9, $m = 4$	0.020	0.9
$n = 12, m = 5$	0.240	32.1
$n = 15, m = 6$	3.609	828.2
$n = 18, m = 7$	326.439	7093
$n = 21, m = 8$	11515	170152

4.5 UOV Reconciliation Attack

UOV reconciliation attack [38] could be viewed as an improved version of direct attack. It tries to find a sequence of basis that could transform the public key of UOV into the central Oil-Vinegar form. However, the main part of this attack is still direct attack. Its complexity could be transformed into directly solving a quadratic system of $m = o$ equations in v variables. For a regular UOV, since $v > o$, directly solving public key of UOV or using reconciliation attack could all be transferred to directly solving an underdefined system(number of variables is greater than the number of equations). Before applying direct attack to an under-defined system, one should assign random values to variables to make the whole system a generic one or overdefined one [39]. Consequently, reconciliation attack against UOV is as difficult as a direct attack against it since both of them end up with solving a generic or over-defined system of quadratic equations with the same number of equations. Because of the linear affine transformation T, the public key of HS-Sign looks totally random so that we expect HS-Sign have the same security level against UOV reconciliation attack as a regular UOV. To verify our conclusions, we also develop magma programs about HS-Sign and regular UOV against such attack, we choose three small scale groups of parameters for each scheme. For each scheme, we test for 100 times and record their average attacking time. The results are listed in **Table 5**.

Table 5. Result of experiments with UOV reconciliation attack

Schemes	UOV	HS-Sign
Parameters 1	(GF (4),4,4)	(GF (3),4,8,4)
Time(s)	0.529	0.496
Memory(MB)	128	128
Parameters 2	(GF (5),4,8)	(GF (5),4,8,4)
Time(s)	3.201	3.435
Memory(MB)	128	128
Parameters 3	(GF (7),3,6)	(GF (7),3,6,4)
Time(s)	0.718	0.752
Memory(MB)	128	128

4.6 Other Attacks

There exists other attacks besides the above algebraic attacks in MPKC, such as the Thomae-Wolf attack, linearization equation attack and differential attack. However, according to the characteristics of these attacks, we find that they are inapplicable to attack HS-Sign. Below we show the analysis.

The Thomae-Wolf attack [40] is an efficient algebraic key recovery attack to break Enhanced STS, Enhanced TTS and their variants. This attack mainly makes use of "good keys" and "missing cross-terms" to attack systems. The good keys are a generalization of equivalent keys in a MPKC scheme, and the Thomae-Wolf attack is a generalization of the Rainbow Band Separation attack. Consequently, Thomae and Wolf demonstrated that the attack is inapplicable for a non-multilayer construction, such as UOV. In the case of HS-Sign, it is also a non-multilayer construction, so we can affirm that the Thomae-Wolf attack is inapplicable for HS-Sign.

The linearization equation attack is first discussed in [41] to break C*. Later, the high order linearization equation attack [42] was proposed to attack the MFE cryptosystem. The core essence of linearization equation attack is to construct a potential bijection between the ciphertext and the plaintext. However, the central map of HS-Sign is not a bijection, so the attack cannot work on HS-Sign.

The differential attack is successfully applied to break C*, PMI and Sflash. In this attack, one uses the fact that the differential of the public key of any MPKC is an affine map, and the dimension of the kernel of the differential is invariant. According to these facts, one can gain some information about the secret key to attack the corresponding cryptosystem. However, in the case of HS-Sign, the dimension of the expected kernel has no invariant in the central map. Thus, the attacker cannot find some linearly independent vectors to build the kernel. So the differential attack is unpractical to attack HS-Sign.

4.7 Attack Complexity

From the above security analysis, we see that the best known attack to HS-Sign is the direct attack. In [39], Bettale et al. asserted that, for a semi-regular system, the computational complexity of F_5 is bounded by $O\left(\left(m\binom{n+d_{reg}-1}{d_{reg}}\right)^{\omega}\right)$, where n is the number of variables, m is the number of equations, ω is a linear algebra constant and $2 \leqslant \omega \leqslant 3$, in general we set $\omega = 2$ for cryptanalyst, d_{reg} is the degree of regularity of the system, which is the index of the first non-positive coefficient in the Hilbert series $S_{m,n}$ with

$$S_{m,n} = \frac{\prod_{i=1}^{m}(1-z^{d_i})}{(1-z)^n},$$

where d_i is the degree of the i-th equation.

In the case of HS-Sign, if we let $n = \alpha m$, since the degree of regularity is associated with n and m, then the complexity of HS-Sign is determined by m. when $m \geqslant 24$, $n \geqslant 54$, we can gain the degree of regularity of HS-Sign $d_{reg} \geqslant 13$, and then the attack complexity of HS-Sign over these parameters is greater than 2^{80}.

5. Experiments and Comparisons

5.1 Performance of HS-Sign and Comparisons

Suppose that the length of the prime p in binary expression is L bits. **Table 6** shows the performance requirements of HS-Sign and UOV.

Table 6. Performance Requirements by our Proposed Signature Scheme and the Baseline Scheme

	HS-Sign(q,o,v,m)	**UOV(q,o,v)**
Private key size(bit)	$\left(\begin{matrix} o+m\cdot(o\cdot o+v\cdot(v+1)/2) \\ +m\cdot(n+1)+n\cdot(n+1) \end{matrix}\right)\cdot L$	$\left(\begin{matrix} m\cdot(o\cdot v+v\cdot(v+1)/2) \\ +m\cdot(n+1)+n\cdot(n+1) \end{matrix}\right)\cdot L$
Public key size(bit)	$m\cdot(\frac{(n+1)(n+2)}{2})\cdot L$	$o\cdot(\frac{(n+1)(n+2)}{2})\cdot L$
Key generation	$O(o\cdot n^2)$	$O(o\cdot n^2)$
Signature generation	$O(m\cdot v)+m+m\cdot(o-m)+S$	$O(o\cdot v)+S$
signature verification	$O(n)$	$O(n)$

Notation for **Table 6**:
o,v: the number of Oil and Vinegar variables respectively;
n: $n = v + o$;
m: the number of multivariate polynomials;
S: average time required by a Gaussian Elimination function.

5.1.1 Private Key Size

In UOV, each signature needs to store the coefficients of all the central mapping polynomials and the affine invertible map, each polynomial contains $(o \cdot v + v \cdot (v + 1)/2 + n + 1) + n \cdot (n + 1))$ elements, the affine invertible map contains $n\cdot(n + 1)$ elements and the number of polynomials is o, so the private key size is $(o \cdot (o \cdot v + v \cdot (v + 1)/2 + n + 1)+n\cdot(n+1))\cdot L$ bits. And in our proposed signature scheme, we can see that each polynomial contains $o + (o \cdot o + v \cdot (v + 1)/2+ n+ 1)$ elements, the affine invertible map contains $n \cdot (n + 1)$ elements, the number of polynomials is m, but the first o elements is equal in each polynomial, so the private key size is $(o+m\cdot(o\cdot o+v\cdot(v+1)/2+n+1)+n\cdot(n+1))\cdot L$ bits.

5.1.2 Public Key Size

In UOV, each signature needs to store the total coefficients of all the public polynomials, we can find that these polynomials are randomly multivariate quadratic polynomials with n variate, so the public key size is $o\cdot(\frac{(n+1)(n+2)}{2})\cdot L$ bits. And HS-Sign gets the same conclusion except the number of polynomials is m.

5.1.3 Computation on Key Generation

The main computation of key generation in UOV is to randomly construct the map Q and P. It will need $O(n^2)$ to construct a random polynomial, so the computation complexity of key generation is $O(o \cdot n^2)$. And so is HS-Sign.

5.1.4 Computation on Signature Generation

The main computation of signature generation in UOV is to evaluate the polynomials with the

random v vinegar variables and solve o linear equations in the o variables. So the computation complexity of key generation is $O(o \cdot v)+S$. In HS-Sign, we need firstly to evaluate the polynomials with the random v vinegar variables with m polynomials, and then subtracting the m polynomials, and evaluate the polynomials with the random o-m variables and finally solve m linear equations in the m variables, so the complexity of key generation is $O(o \cdot n^2)$.

5.1.5 Computation on Signature Verification

The main computation of signature generation in UOV is to evaluate the public polynomials with the signature. So the computation complexity of key generation is $O(n)$. This conclusion also comes to HS-Sign.

5.2 Practical parameters for HS-Sign and Comparison

According to the above security analysis, we suggest that three practical parameter sets: {q = 31, o = 26, v = 52, m = 24}, {q = 253, o = 32, v = 64, m = 28} and {q = 253, o = 48, v = 96, m = 40}. Then, Table 7 compares HS-Sign with the baseline scheme UOV.

Table 7. Comparison of our Proposed Signature Scheme and UOV

Security	Schemes	HS-Sign(q,o,v,m)	UOV(q,o,v)
2^{80}	Parameters	(31,26,52,24)	(32,26,52)
	Oil-Oil terms	Yes	No
	Public key	9.25 KB	10.03 KB
	Private key	7 KB	9.67 KB
2^{96}	Parameters	(253,32,64,28)	(256,32,64)
	Oil-Oil terms	Yes	No
	Public key	128.4 KB	148.53 KB
	Private key	94.9 KB	139.13 KB
2^{128}	Parameters	(253,48,96,40)	(256,48,96)
	Oil-Oil terms	Yes	No
	Public key	408.6 KB	490.36 KB
	Private key	250.78 KB	451.24 KB

As **Table 7** shows, HS-Sign can produce shorter public key and private key than the baseline schemes. The reason for this is that we can adjust the parameters more concisely to get the same security level in HS-Sign. Also there are Oil-Oil terms in HS-Sign so that we can expect more resistance of structural attack of HS-Sign than that of the baseline schemes.

5.3 Running Time of HS-Sign and Comparison

To further show the efficiency of HS-Sgin, we compare it with other signature schemes (including multivariate signature schemes and non-multivariate signature schemes) from the length of the message, length of the signature, size of the public key, size of the secret key, signing time and verification time.

5.3.1 Comparison with other multivariate signature schemes

We compare HS-Sign with Gui [43], QUARTZ [17], UOV and Rainbow [44], which are current secure and promising multivariate signature schemes. All the schemes are running in MAGMA V2.19, with the hardware and software below: The CPU is Intel Xeon E5-2660V2 (10 cores and 2.2GHz each core), the memory is 192GB, the operating system is Redhat 9.0. Here we let all the scheme with security level 280and the comparison results are summarized

in **Table 8** in terms of efficiency and storage.

Table 8. Comparison between HS-Sign and other multivariate signature schemes

Schemes	Parameters	Message(bit)	Signature(bit)	PK(KB)	SK(KB)	Sign(ms)	Ver(ms)
Gui	(96,5,6,6)	160	128	61.6	3.1	89	12
QUARTZ	(103,129,3,4)	160	128	71.9	3.1	387	36
UOV	(32,26,52)	130	390	10.03	9.67	192	37
Rainbow	(256,18,12,12)	192	336	22.17	17.33	54	19
HS-Sign	(31,26,52,24)	120	390	9.25	7	187	31

From **Table 8** we can see that the signing time of HS-Sign is faster than that of UOV and QUARTZ, but a little slower than that of Gui and Rainbow scheme in the same security level, the reason is that both Gui and Rainbow are known for their quick computing but their security is questionable although they are secure now. More precisely, for Rainbow, there exists quite a lot of structural attacks such as Rainbow Band Separation and the Thomae-Wolf attack, while in the case of Gui, it is a simple combination of HFE with the vinegar method and the minus method, and its core scheme HFE are broken with the first challenge in [45]. Also, the public and private key size of HS-Sign is smaller than most of the other schemes, except the private key size of Gui and QUARTZ, the reason is that these two schemes are mixed field constructions. Finally for the message and signature size, all the schemes are approximated. The result shows that HS-Sign is competitive with all the current promising MPKC schemes, so we think it is a promising MPKC scheme.

5.3.2 Comparison with other non-quantum signature schemes

At present, there are many non-multivariate public key signature schemes, such as RSA [46], ECDSA [47] and so on. To show the performance of HS-Sign, we also compare it with RSA, ECDSA on the same security level of 280, 296and 2128. The comparison results are shown in Table 9. Since traditional asymmetric cryptosystems such as RSA and ECC implemented in OpenSSL have already taken the advantages of Streaming SIMD Extensions (SSE), which is an SIMD instruction set extension to the x86 architecture. SSE can pack eight 16-bit integer operands in its 128-bit xmm registers and do eight integer operations per cycle. We thereafter implement HS-Sign using SSE instructions on a Dell workstation with Intel E5-2609 2.4GHz CPU and **Table 9** shows the result.

Table 9. Comparison between HS-Sign and other multivariate signature schemes

Security	Schemes	Parameters	PK(Byte)	SK(Byte)	Signature(bit)	Sign(ms)	Ver(ms)
2^{80}	RSA	1024	128	128	1024	0.30	0.02
	ECDSA	nistk163	40.75	20.375	326	0.34	0.93
	HS-Sign	(31,26,52,24)	9472	7168	390	0.23	0.12
2^{96}	RSA	2048	256	256	2048	2.14	0.06
	ECDSA	nistk233	58.25	29.125	466	1.15	2.38
	HS-Sign	(253,32,64,28)	131482	97178	768	0.39	0.20
2^{128}	RSA	3072	384	384	3072	6.69	0.14
	ECDSA	nistk283	69.5	35.375	556	2.57	3.67
	HS-Sign	(253,48,96,40)	418406	256799	1152	0.41	0.78

From **Table 9** we can see that the signing time of HS-Sign is about servel times faster than that of ECDSA scheme, but a little slower than that of RSA scheme in the same security levels, this result shows that HS-Sign is competitive with the traditional asymmetric cryptosystems.

The public key size and the private key size is much larger than that of both the RSA and ECDSA scheme, but considering that these keys do not need to update frequently, and this result is acceptable in the field of MPKC. Also we can see that the signature size of HS-Sign is smaller than that of RSA, and a little larger than that of ECDSA.

6. Conclusion

In this paper, motivated by two problems that are "to find inversion solution of quadratic multivariate equations" and "to find another structure with some random Oil-Oil terms for UOV", we proposed a new UOV-like multivariate public key digital signature scheme called HS-Sign based on hyper-spheres over finite field. A highlight of this paper is that it is a good exploration of MPKC systems, since HS-Sign is focusing on the intuitive drawbacks of UOV and is basing on hyper-spheres. We observe that HS-Sign is equal to UOV scheme with some random Oil-Oil terms and security analysis show that HS-Sign has better security resistance under current attack techniques on MPKC system than UOV. We have also implemented our new scheme and the baseline schemes to show the efficiencies and comparisons. The results show that HS-Sign has exponential attack complexity and HS-Sign is competitive with other signature schemes in terms of the length of the message, length of the signature, size of the public key, size of the secret key, signing time and verification time**.**

In the future work, we plan to find solutions to the drawbacks of other MPKC schemes, such as HFE, Rainbow, etc.

References

[1] Jintai Ding and Bo-Yin Yang, "Multivariate public key cryptography," in *Proc. of Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, editors, Post-Quantum Cryptography*, pp. 193-241, Springer Berlin Heidelberg, 2009. Article (CrossRef Link)

[2] Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari, "Public-key identification schemes based on multivariate quadratic polynomials," in *Proc. of Phillip Rogaway, editor, Advances in Cryptology -CRYPTO 2011, volume 6841 of Lecture Notes in Computer Science*, pp. 706-723, Springer Berlin Heidelberg, 2011. Article (CrossRef Link)

[3] Michael R Garey and David S Johnson, "Computer and intractability, A Guide to the theory of NP-Completeness," *Ney York, NY: WH Freeman and Company*, 1979.

[4] Jacques Patarin and Louis Goubin, "Trapdoor one-way permutations and multivariate polynomials," *Information and Communications Security*, pp. 356–368, 1997. Article (CrossRef Link)

[5] Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann, "CyclicRainbow - A multivariate signature scheme with a partially cyclic public key," in *Proc. of SCC*, pp. 229-235, 2010. Article (CrossRef Link)

[6] Aviad Kipnis, Jacques Patarin, and Louis Goubin, "Unbalanced Oil and Vinegar signature schemes, " in *Proc. of Jacques Stern, editor, Advances in Cryptology -EUROCRYPT'99, volume 1592 of Lecture Notes in Computer Science*, pp. 206-222, Springer Berlin Heidelberg, 1999. Article (CrossRef Link)

[7] Jintai Ding, Jason E Gower, and Dieter S Schmidt, "Multivariate public key cryptosystems," volume 25. Springer, 2006. Article (CrossRef Link)

[8] Jacques Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms, " in *Proc. of Advances in Cryptology -EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain*, pp. 33-48, May 12-16, 1996. Article (CrossRef Link)

[9] Tsutomu Matsumoto and Hideki Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption, " in *Proc. of D. Barstow, W. Brauer, P. Brinch Hansen, D. Gries, D. Luckham, C. Moler, A. Pnueli, G. Seegmüller, J. Stoer, N. Wirth, and ChristophG. Günther, editors, Advances in Cryptology -EUROCRYPT '98, volume 330 of Lecture Notes in Computer Science*, pp. 419-453, Springer Berlin Heidelberg, 1988. Article (CrossRef Link)

[10] Christopher Wolf, An Braeken, and Bart Preneel, "On the security of stepwise triangular systems," *Designs, Codes and Cryptography*, 40(3):285-302, 2006. Article (CrossRef Link)

[11] Mehdi-Laurent Akkar, Nicolas Courtois, Romain Duteuil, and Louis Goubin, "A fast and secure implementation of sflash, " in *Proc. of Public Key Cryptography - PKC 2003, 6th International Workshop on Theory and Practice in Public Key Cryptography, Miami, FL, USA*, pp. 267-278, January 6-8, 2003. Article (CrossRef Link)

[12] Jacques Patarin, Louis Goubin, and Nicolas Courtois, "C*-+and HM: variations around two schemes of t. matsumoto and h. imai, " in *Proc. of Advances in Cryptology - ASIACRYPT '98, International Conference on the Theory and Applications of Cryptology and Information Security, Beijing, Chin*a, pp. 35-49, October 18-22, 1998. Article (CrossRef Link)

[13] Jintai Ding, "A new variant of the matsumoto-imai cryptosystem through perturbation," in *Proc. of Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore*, pp. 305-318, March 1-4, 2004. Article (CrossRef Link)

[14] Jintai Ding and Jason E. Gower, "Inoculating multivariate schemes against differential attacks, " in *Proc. of Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA*, pp. 290-301, April 24-26, 2006. Article (CrossRef Link)

[15] Jacques Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms," in *Proc. of Ueli Maurer, editor, Advances in Cryptology EUROCRYPT 96, volume 1070 of Lecture Notes in Computer Science*, pp. 33-48, Springer Berlin Heidelberg, 1996. Article (CrossRef Link)

[16] Jintai Ding and Dieter Schmidt, "Cryptanalysis of hfev and internal perturbation of HFE, " in *Proc. of Public Key Cryptography - PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland*, pp. 288-301, January 23-26, 2005. Article (CrossRef Link)

[17] Jacques Patarin, Nicolas Courtois, and Louis Goubin, "Quartz, 128-bit long digital signatures, " in *Proc. of Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA*, pp. 282-297, April 8-12, 2001. Article (CrossRef Link)

[18] Yun-Ju Huang, Feng-Hao Liu, and Bo-Yin Yang, "Public-key cryptography from new multivariate quadratic assumptions, " in *Proc. of Public Key Cryptography - PKC 2012 -15th International Conference on Practice and Theory in Public Key Cryptography,Darmstadt, Germany*, pp. 190-205, May 21-23, 2012. Article (CrossRef Link)

[19] Takanori Yasuda, Tsuyoshi Takagi, and Kouichi Sakurai, "Multivariate signature scheme using quadratic forms, " in *Proc. of Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France*, pp. 243-258, June 4-7, 2013. Article (CrossRef Link)

[20] Chengdong Tao, Adama Diene, Shaohua Tang, and Jintai Ding, "Simple matrix scheme for encryption," in *Proc. of Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France*, pp. 231-242, June 4-7, 2013. Article (CrossRef Link)

[21] Takanori Yasuda, Jintai Ding, Tsuyoshi Takagi, and Kouichi Sakurai, "A variant of rainbow with shorter secret key and faster signature generation, " in *Proc. of the first ACM workshop on Asia public-key cryptography, AsiaPKC'13, Hangzhou, China*, pp. 57-62, May 8, 2013. Article (CrossRef Link)

[22] Takanori Yasuda, Tsuyoshi Takagi, and Kouichi Sakurai, "Efficient variant of rainbow using sparse secret keys," *JoWUA*, vol. 5, no. 3, pp. 3-13, 2014.

[23] Jintai Ding, Albrecht Petzoldt, and Lih-chung Wang, "The cubic simple matrix encryption scheme," in *Proc. of Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada*, pp. 76-87, October 1-3, 2014. Article (CrossRef Link)

[24] Jaiberth Porras, John Baena, and Jintai Ding, "ZHFE, a new multivariate public key encryption scheme," in *Proc. of Post-Quantum Cryptography - 6th International Workshop,PQCrypto 2014, Waterloo, ON, Canada*, pp. 229-245, October 1-3, 2014. Article (CrossRef Link)
[25] Wuqiang Shen and Shaohua Tang, "RGB, a mixed multivariate signature scheme," *Comput. J.*, vol. 59, no. 4, pp. 439–451, 2016. Article (CrossRef Link)
[26] Alan Szepieniec, Jintai Ding, and Bart Preneel, "Extension field cancellation: A new central trapdoor for multivariate quadratic systems," in *Proc. of Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan*, pp. 182-196, February 24-26, 2016. Article (CrossRef Link)
[27] Albrecht Petzoldt, Stanislav Bulygin, and Johannes A. Buchmann, "A multivariate based threshold ring signature scheme," *Appl. Algebra Eng. Commun. Comput*, 24(3-4):255-275, 2013. Article (CrossRef Link)
[28] Shaohua Tang and Lingling Xu, "Towards provably secure proxy signature scheme based on isomorphisms of polynomials," *Future Generation Computer Systems*, 30(0):91 - 97, 2014. Article (CrossRef Link)
[29] Jiahui Chen, Shaohua Tang, Daojing He, and Yang Tan, "Online/offline signature based on uov in wireless sensor networks," *Wireless Networks*, pp. 1-12, 2016. Article (CrossRef Link)
[30] Jacques Patarin, "The oil and vinegar signature scheme," in *Proc. of Dagstuhl Workshop on Cryptography*, volume 80, 1997.
[31] Aviad Kipnis and Adi Shamir, "Cryptanalysis of the Oil and Vinegar signature scheme, " in *Proc. of Hugo Krawczyk, editor, Advances in Cryptology -CRYPTO '98, volume 1462 of Lecture Notes in Computer Science*, pp. 257-266, Springer Berlin Heidelberg, 1998. Article (CrossRef Link)
[32] Shaohua Tang, Lingling Xu, Niu Liu, Xinyi Huang, Jintai Ding, and Zhiming Yang, "Provably secure group key management approach based upon hyper-sphere," *Parallel and Distributed Systems, IEEE Transactions on*, PP(99):1-11, 2014. Article (CrossRef Link)
[33] W. Cao, L. Hu, J. Ding, and Z. Yin, "Kipnis-shamir attack on unbalanced oil-vinegar scheme," *Information Security Practice and Experience*, pages 168-180, 2011. Article (CrossRef Link)
[34] Wieb Bosma, John Cannon, and Catherine Playoust, "The Magma algebra system I: The user language," *Journal of Symbolic Computation*, 24(3-4):235 - 265, 1997. Article (CrossRef Link)
[35] Jean-Charles Faugère, "A new efficient algorithm for computing Gröbner bases (F4)," *Journal of Pure and Applied Algebra*, 139:61-88, 1999. Article (CrossRef Link)
[36] Charles Bouillaguet, Hsieh-Chung Chen, Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, Adi Shamir, and Bo-Yin Yang, "Fast exhaustive search for polynomial systems in F_2," in *Proc. of Stefan Mangard and Franois-Xavier Standaert, editors, Cryptographic Hardware and Embedded Systems, CHES 2010, volume 6225 of Lecture Notes in Computer Science*, pages 203-218, Springer Berlin Heidelberg, 2010. Article (CrossRef Link)
[37] Magali Bardet, Jean-Charles Faugere, and Bruno Salvy, "On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations," in *Proc. of Intl Conference on Polynomial System Solving*, pages 71-74, 2004. Article (CrossRef Link)
[38] Jintai Ding, Bo-Yin Yang, Chia-Hsin Owen Chen, Ming-Shing Chen, and Chen-Mou Cheng, "New differential-algebraic attacks and reparametrization of rainbow," in *Proc. of Applied Cryptography and Network Security, 6th International Conference, ACNS 2008, New York, NY, USA*, June 3-6, Proceedings, pages 242-257, 2008. Article (CrossRef Link)
[39] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret, "Hybrid approach for solving multivariate systems over finite fields," *J. Mathematical Cryptology*, 3(3):177-197, 2009. Article (CrossRef Link)
[40] Enrico Thomae and Christopher Wolf, "Cryptanalysis of enhanced tts, STS and all its variants, or: Why cross-terms are important," in *Proc. of Progress in Cryptology - AFRICACRYPT 2012 - 5th International Conference on Cryptology in Africa, Ifrance, Morocco*, July 10-12, Proceedings, pages 188-202, 2012. Article (CrossRef Link)

[41] Jacques Patarin, "Cryptanalysis of the matsumoto and imai public key scheme of eurocrypt'88, " in *Proc. of Advances in Cryptology - CRYPTO '95, 15th Annual International Cryptology Conference, Santa Barbara, California, USA*, August 27-31, 1995, Proceedings, pages 248-261, 1995. Article (CrossRef Link)
[42] Jintai Ding, Lei Hu, Xuyun Nie, Jianyu Li, and John Wagner, "High order linearization equation (HOLE) attack on multivariate public key cryptosystems," in *Proc. of Public Key Cryptography - PKC 2007, 10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China*, April 16-20, 2007, Proceedings, pages 233-248, 2007. Article (CrossRef Link)
[43] Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, Chengdong Tao, and Jintai Ding, "Design principles for hfev- based multivariate signature schemes," in *Proc. of Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand*, November 29 - December 3, Proceedings, Part I, pages 311-334, 2015. Article (CrossRef Link)
[44] Jintai Ding and Dieter Schmidt, "Rainbow, a new multivariable polynomial signature scheme, " in *Proc. of Applied Cryptography and Network Security, Third International Conference, ACNS 2005, New York, NY, USA*, June 7-10, Proceedings, pages 164-175, 2005. Article (CrossRef Link)
[45] Jean-Charles Faugère and Antoine Joux, "Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using gröbner bases," in *Proc. of Advances in Cryptology -CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA*, August 17-21, Proceedings, pages 44-60, 2003. Article (CrossRef Link)
[46] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, 21(2):120-126, 1978. Article (CrossRef Link)
[47] Don Johnson, Alfred Menezes, and Scott A. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Sec.*, 1(1):36-63, 2001. Article (CrossRef Link)

Jiahui Chen received the Bachelor degree (major in Computer Science) from South China Normal University and Master degree (Major in Network Security) from South China University of Technology. He is currently a Ph.D student in South China University of Technology, His research interests mainly focus on Multivariate Public Key Cryptography. Quantum Cryptography, Lattice Cryptography, General Cryptography, Applied Cryptography and network security are also included.

Shaohua Tang received the B.Sc. and M.Sc. degrees in applied mathematics, and the Ph.D. degree in communication and information system all from the South China University of Technology, in 1991, 1994, and 1998, respectively. He was a visiting scholar with North Carolina State University, and a visiting professor with the University of Cincinnati, Ohio. He has been a full professor with the School of Computer Science and Engineering, South China University of Technology since 2004. His current research interests include information security, networking, and cloud computing. He is a member of the IEEE and the IEEE Computer Society.

Xinglin Zhang received the B.E. degree from the School of Software, Sun Yat-sen University in 2010, and the Ph.D. degree from the Department of Computer Science and Engineering, Hong Kong University of Science and Technology in 2014. He is currently with the South China University of Technology. His research interests include wireless ad-hoc/sensor networks, mobile computing and crowdsourcing. He is a student member of the ACM.