New Signcryption Scheme based on Multivariate Public-key Cryptosystem

Han Yiliang
Department of Electronic Technology
Engineering University of CAPF
Xi'an, China, 710086
Email: yilianghan@hotmail.com

Abstract—Multivariate based cryptography possesses the characteristic of high efficiency as well as resistance of quantum attack, which makes it become one of the main candidates of being possible alternative to conditional public cryptography in post-quantum ear. A new signcryption scheme based on Multivariate was proposed. The proposal combined MMI with Cyclic Rainbow and performed the encryption and authentication in a logical operation. By modifying MMI scheme with the idea of constructing the central mapping in HFE, the new scheme has brought the new construction. Compared with the original MMI scheme, our scheme is more secure than before and layering attack is not available. Besides, the key size of signcryption is smaller than MMI after modification, and makes encryption and signature become realizable at the same time. It also has the 300 bits ciphertext size, which is more efficient than others. The scheme could be used to encryption the structure big data.

Keywords-multivariate; MMI; signcryption; public key cryptosystem; signature

I. INTRODUCTION

In recent years, Multivariate Public Key Cryptosystems (MPKC) has become a potential resolution alternative to public cryptosystems like RSA, which is famous and widely-used in our communication and data encryption. At the same time, MPKC is one of the main candidates among other schemes in post-quantum era, such as Code-based Cryptograph, Lattice-based Cryptograph, Hash-based Digital Signature Scheme and so on. In the system of MPKC, the public key is always chosen nonlinear polynomial equations over a finite field, and the security of MPKC depends on the difficulty of solving multivariate polynomial equations, which called MP problem. And MQ problem has been proved that it is a NP-hard problem [1]. Compared to traditional PKC, MPKC schemes are regarded to be much more computationally than number theoretic-based schemes in general. This has led to many new multivariate schemes from then on. The first multivariate encryption scheme had been proposed in 1988 by Matsumoto and Imai, which called MI or C*[2]. But Patarin attacked MI with linear equations in [3], so the security of MI had been broken. Although MI is not secure, the idea of constructing trapdoor has been admirable, and many improved schemes, new schemes has been put forwarded in the next few years, such as HFE, UOV and STS.

In [4] and [5] , Petzoldt showed a new idea to decrease the public key size of the Unbalanced Oil and Vinegar (UOV) and Rainbow signature schemes. The key method is to insert a highly structured matrix into the coefficient matrix of the public key. Meanwhile, in PQC 2013, Petzoldt and his workmates has also proved that the modification can realize not only the decrease of key size, but also the improved efficiency of verification in [6]. In the other hand, many improved schemes like MI minus scheme, MI plus scheme had been proposed while MI was known as unsafe. And in order to avoid the linearization attack and differential attack against the Matsumoto-Imai (MI) scheme, Jiao Luyao has given different solution to construct the central map, the new structure of central map named multi-layer central map which based on the original structure of MI. The new scheme is MMI [7], without losing the original efficient, MMI made the linearization attack and differential attack unavailable because of its multi-layer structure of central map.

As we all know, there are many multivariate encryption's or signature's schemes, but signcryption scheme based on multivariate is still few. Li Huixian has proposed Certificateless Multi-receiver signcryption Scheme Based on Multivariate Public Key Cryptography [8], however, it was only a model but not a practical implication. So in the passage, a new signcryption scheme has brought forth which combine MMI with Cyclic Rainbow. Furthermore, some changes in the central map of MMI had made to ensure high security, and analyze both security and efficient in detail.

II. PRELIMINARIES

A. *Rainbow signature*

Rainbow signature scheme was suggested by Ding in 2005 [9]. The key construction and its process of signature are as follow.

Public Key. For the scheme, the public key consists of the n-v_1 polynomial components of $\bar{F}$ and the field structure of K.

Private Key. The private key consists of the maps L_1, L_2 and F. Let $L_1 : K^o \to K^o$ and $L_2 : K^{o+v_1} \to K^{o+v_1}$ (n=o+v_1) be two randomly chosen affine linear maps which can be defined by: $\bar{F}(x_1,\mathrm{K}\ ,x_n) = L_1 \circ F \circ L_2(x_1,\mathrm{K}\ ,x_n)$.

F is a map from K^{o+v_1} to K^o such that: $F(x_1,...,x_n,\bar{x}_1,...,\bar{x}_n)=(f_1,\mathrm{K},f_o)$.

Each f_i ($i=1,...,n$) is the linear space of quadratic polynomials spanned by polynomials of the form: $f=\sum_{i=1}^{o}\sum_{j=1}^{v}a_{i,j}x_i\bar{x}_j+\sum_{i=1}^{v}\sum_{j=1}^{v}b_{i,j}\bar{x}_i\bar{x}_j+\sum_{i=1}^{o}c_ix_i+\sum_{j=1}^{v}d_jx_j+e$,

Where $f\in(x_1,...,x_n,\bar{x}_1,...,\bar{x}_n)$, $a_{i,j}$, $b_{i,j}$,c_i,d_j, $e\in K$.

Singing. Let $Y'=(y',\mathrm{K},y'_{n-v_1})$ be a document or a digest in K^{n-v_1}, which want to be signed, then we need to find a solution of the equation: $\bar{F}(x_1,\mathrm{K},x_n,\bar{x}_1,\mathrm{K},\bar{x}_n)=L_1\circ F\circ L_2(x_1,\mathrm{K},x_n)=Y'$

(1) Compute $\bar{Y}'=L_1^{-1}(Y')=(\bar{y}'_1,\mathrm{K},\bar{y}'_{n-v_1})$ firstly.

(2) Apply the inverse of F and to solve the equation $F(x_1,\mathrm{K}\ x_n)=\bar{Y}'=(\bar{y}'_1,\mathrm{K},\bar{y}'_{n-v_1})$.

To choose the values of x_1,x_2,K,x_n and plug them into the first layer of o_1 equations given by $P_1^{(i)}(\bar{x}'_1,\mathrm{K},\bar{x}'_{v_1},x'_{v_1+1},\mathrm{K},x'_{v_2})=(\bar{y}'_1,\mathrm{K},\bar{y}'_{o_1})$, it returns $\bar{x}'_{v_1+1},\mathrm{K},\bar{x}'_{v_2}$.

(3) Plug $\bar{x}'_{v_1+1},\mathrm{K},\bar{x}'_{v_2}$ into the second layer of polynomials, it return us $\bar{x}'_{v_2+1},\mathrm{K},\bar{x}'_{v_3}$ .To repeat the procedure until we find a solution for $F(x_1,\mathrm{K},x_n)=\bar{Y}'$.

(4) If it does not have a solution, we will start from the beginning again by choosing another set of values for x_1,K,x_{v_1}.

(5) To apply the inverse of L_2 and compute $X'=L_2^{-1}(\bar{X}')=(x'_1,\mathrm{K},x'_n)$, which we w-ill gain a signature of $Y'=(y',\mathrm{K},y'_{n-v_1})$.To verify a signature, one only needs t -o check if indeed: $\bar{F}(\bar{X}')=Y'$.

In [4], a new improved Rainbow named Cyclic Rainbow was proposed to decrease the key size of public key without changing the security of the scheme. Moreover, Petzoldt in [6] has proved the efficient of verification has been improved at the same time, and it has a great advantage of practical implementation.

B. The MMI scheme

The central map of the original MI scheme can be regarded as $K^n\xrightarrow{\varnothing^{-1}}L_n\xrightarrow{\bar{f}}L_n\xrightarrow{\varnothing}K^n$. As for MI, its central map construction has been proved that it was not safe enough, because linearization attack and differential attack introduced in the preceding part of the text are the most effective attacks against MI. However, the MMI scheme which was proposed in [7] can make these attacks unavailable. To design a multi-layer central map, MMI can eliminate the drawback brought by the special character of the original central map.

Next we will introduce details about the MMI scheme as follow. Let $\varnothing_1,\varnothing_2,\mathrm{K},\varnothing_r$ be r isomorphism between L_n and K_n, then we need to choose another r integers: $\theta_1,\theta_2,\mathrm{K},\theta_r$, which satisfies $(1+q^{\theta_i},q^n-1)=1$, so we can get t_i through Euclid algorithm, satisfying $t_i(1+q^{\theta_i})=1\bmod(q^n-1)$.

Firstly, the first layer of central map is $f_1(x_1,\mathrm{K},x_n)=\varnothing_1\circ\bar{f}_1\circ\varnothing_1^{-1}(x_1,\mathrm{K},x_n)=(x_{1,1},\mathrm{K},x_{1,n})$, where, $\varnothing_1^{-1}(x_1,\mathrm{K},x_n)=X_1$, $\bar{f}_1(X)=X_1^{1+q^{\theta_1}}=Y_1$, $f_i=(x_{i-1,1},\mathrm{K},x_{i-1,n})=\varnothing_i\circ\bar{f}_i\circ\varnothing_i^{-1}(x_{i-1,1},\mathrm{K},x_{i-1,n})=(x_{i,1},\mathrm{K},x_{i,n})$, then we can get $\bar{f}_1^{-1}(X_1)=X_1^{t_1}$.

Secondly, the i-th layer of central map can be expressed as follow.

$f_i=(x_{i-1,1},\mathrm{K},x_{i-1,n})=\varnothing_i\circ\bar{f}_i\circ\varnothing_i^{-1}(x_{i-1,1},\mathrm{K},x_{i-1,n})=(x_{i,1},\mathrm{K},x_{i,n})$

where, $\varnothing_i^{-1}(x_{i-1,1},\mathrm{K},x_{i-1,n})=X_i$, $\bar{f}_i(X)=X_i^{1+q^{\theta_i}}=Y_i$, $\varnothing_i^{-1}(Y_i)=(x_{i,1},\mathrm{K},x_{i,n})$, and we can get $\bar{f}_i^{-1}(X_i)=X_i^{t_i}$.

In a word, the central map of MMI can be defined as follow.

$$f=f_i(f_{i-1}(\mathrm{K}\ f_2(f_1(x_1,\mathrm{K},x_n))))$$

Public key. $F_2=T\circ f\circ S$

Private key. $(T,S)(T,S,\varnothing_1,\varnothing_2,\mathrm{K},\varnothing_i,\theta_1,\mathrm{K},\theta_i)$, T,S are two affine directions of K^n, and the process of encryption and decryption for MMI is not be discussed here, it is just a computation of multi-layer for MI.

III. SIGNCRYPTION SCHEME BASED ON MPKC

A. Syntax

The syntax of signcryption based on MPKC could be defined as follow.

Setup. Taking as input a main secure parameter *S*, then run this algorithm to generate a list of global public parameters *params* , finally return *params* .

Keys Generation. This algorithm is run by KGC, KGC will generate the system's master key *w*. Then take *params* and *w* as input，it will return a public private key pair after verifying the soundness of user *U*, and give them to *U*.

Signcryption. Taking as input *params*, the sender A runs this algorithm with input{*S*, sk_A, pk_B, *M*}. *M* is a message which user A want to send to user B, then this algorithm produces a ciphertext σ for the message.

Unsigncryption. User B takes $\{sk_B,pk_A,\sigma\}$ as input and run this algorithm , this algorithm returns a pair of a public key and a plaintext, or a failure symbol $\perp$. In a word, here exists an equation after correct unsigncryption,

M=Unsigncrypt(*S*, Signcrypt(*S*, sk_A, pk_B, *M*)sk_B,pk_A).

B. Signcryption scheme based on MPKC

This section presents our signcryption schemes combined MMI and cyclic Rainbow, its security analysis and efficiency analysis will be introduced in followed section. Parameters and mapping can be defined as follow.

Let *K* be a finite field. Let *o* and *v* be two integers, which satisfies *n=o+v*, here *n* is also a integer. According to [4], [6] and [7], we choose *i=2* in MMI and *u=2* in

Rainbow. Besides, let T, L_1 and L_2 are affine mapping which satisfy the above schemes.

In our scheme, we choose $i=2$ as the numbers of layer in MMI, meanwhile, we make some improvement in the last layer in MMI to improve scheme's security while designing our scheme. Taking the idea of constructing the central map in HFE[10] as reference, we change the construction of central map in the last layer. It can be expressed as $\bar{f}_2 = \sum_{i=0}^{w_2-1}\sum_{j=0}^{i} c_{i,j} X_i^{q^i+q^j} + \sum_{i=0}^{w_1-1} d_i X_i^{q^{\theta_1}}$.

Here, let $c_{i,j}$, $d_i \in L$. Let w_1, w_2 be two integers chosen depended on $d=deg(\bar{F})$. To compute the inverse of $\bar{F}$, the variant of Berlekamp algorithm can be used to solve this problem quickly. And according to [10], the complexity of computing the inverse of $\bar{F}$ is totally about $O(nd^2logd+d^3)$, so d is chosen to be small. It can make w_1, w_2 become small, which will not decrease the efficiency of finding a solution for the equation. In order to make a better description, here our scheme is represented in detail as follow.

Let m be a message needed to signcrypt in K^n, the sender A performs the following step.

Setup. Taking as input a main secure parameter S, KGC generates two integers p and l. p denotes as characteristic, q as cardinality of a finite field K, which $q=p^l$. Besides, let H be a secure Hash function satisfies: $K^n \times K^n \to K^n$, let $n=o+v$. Finally, return *params(K,l,g, n,q,p,H)*.

Key Extract. Let T, L_1, L_2 be three invertible affine mapping which satisfies $K^n \to K^n$, then we get the syste m's public key $F_2 = T \circ f \circ L_2$, private key ($T$, L_1, L_2), her e we replace L_2 as S to decrease the key size of private key.

Signcrypt:

$\sigma_1 \leftarrow F_2(m)$

$h \leftarrow H(\sigma_1)$

$\bar{Y}' \leftarrow L_1^{-1}(h)$

$\bar{X}' \leftarrow F^{-1}(\bar{Y}')$

$\sigma_2 \leftarrow L_2^{-1}(\bar{X}')$

$\sigma \leftarrow (\sigma_1, \sigma_2)$

Designcrypt:

$h \leftarrow \bar{F}(\sigma_2)$

$\bar{h} \leftarrow Hash(\sigma_1)$

If $h == \bar{h}$, then $m = F_2^{-1}(\sigma_1)$;

Else return $\perp$

IV. SECURITY ANALYSIS OF MMI

A. *Some common attacks*

In this session, security analysis of our scheme aims at the construction of central map. Although we made some improvement of the last layer of MMI, its security level is not reduced. In the other hand, the security of L_1, L_2 has introduced in detail in [9], so we should not repeat once more in this session.

- Linearization attack. In [7], to illustrate how can MMI can resist linearization attack, we take r=2 as an example. According to the design and definition of the central map, two special algebraic equations can be found as follow.

$$X_1^{q^{2\theta_1}} Y_1 = X_1 Y_1^{q^{\theta_1}} \qquad (1)$$

$$X_2^{q^{2\theta_2}} Y_2 = X_2 Y_2^{q^{\theta_2}} \qquad (2)$$

Besides, a relationship between X_2 and Y_1 can be expressed as $X_2 = \varnothing_2^{-1} \circ \varnothing_1(Y_1)$. And if we represent Eq.(1) and (2) in K^n, then we can get the following equations

$$\sum_{i=1,j=1}^{n} a_{i,j} x_i x_{1,j} + \sum_{i=1}^{n} b_i x_i + \sum_{i=1}^{n} c_i x_{1,i} + d = 0$$

$$\sum_{i=1,j=1}^{n} \bar{a}_{i,j} x_{1,i} y_i + \sum_{i=1}^{n} \bar{b}_i x_{1,i} + \sum_{i=1}^{n} \bar{c}_i y_i + \bar{d} = 0$$

Here $a_{ij}, b_i, c_i, d, \bar{a}_{ij}, \bar{b}_i, \bar{c}_i, \bar{d}$ are coefficients which are unknown. If $\varnothing_1$ and $\varnothing_2$ are well chosen, like $\varnothing_2^{-1} \circ \varnothing_1 \neq 1$, then there will not be a direct bilinear equation between X_2 and $Y_1$1. So it does not exit such a $B(X_1, Y_2)$ satisfied as follow $B(X_1, Y_2) = X_1^{q^a} Y_2^{q^b} - X_1^{q^c} Y_2^{q^d} = 0$. So PAtarin's linearization attack will be unavailable.

- Differential attack. In [7], Fouque and Granboulan's definition of differential attack is about the central map $\bar{f}$ and public key F which satisfy following relationship: $L_{\bar{f},X}(K) = X^{q^\theta} K + X K^{q^\theta} = X^{q^{\theta+1}} \left(K / X + (K / X)^{q^\theta} \right)$, $L_{F,(x_1,K\,x_n)} = T \circ \bar{\varphi}_X \circ \bar{\varphi} \circ \bar{v}_X \circ S$. But to the MMI, its construction of central map is $\bar{f}_1(X) = \left(\varnothing_2^{-1} \circ \varnothing_1 \left(X_1^{1+q^{\theta_1}} \right) \right)^{1+q^{\theta_2}}$. So the differential forms of it can be written in the form of $L_{\bar{f},X}(K) = \left(\varnothing_2^{-1} \circ \varnothing_1 \left(X_1^{1+q^{\theta_1}} \right) \right)^{q^{\theta_2}} K + \left(\varnothing_2^{-1} \circ \varnothing_1 \left(X_1^{1+q^{\theta_1}} \right) \right) K^{q^{\theta_2}}$. Similarly, if $\varnothing_1$ and $\varnothing_2$ are chosen probably, the differential equation of f is not given to us, so the design of multi-layer central map does not make differential attack available anymore.
- **XL** attack**.** XL is an equation-solving algorithm based on Grobner base, and XL-Like has already threatened some familiar schemes such as HFE、SFALS-H. Although MMI is a generic multivariate system, we still need to make an analysis of the security for MMI if put it under the cryptanalysis of XL-like system-solving method.

As for a generic system, the time complexity of XL depends on the minimum degree of scheme. Here, with l equations in m variants which degree is d, its time complexity is about $C_{XL} = E\left(\binom{l+d}{d}, m\binom{l+d-2}{d-2} \right)$.

Where $E(M,N)$ denotes the time complexity of solving M linear equations in N. We make a test for MMI with XL system-solving method, and we

get the time complexity as follows. $C_{XL} = q^s\left(C_0 + E\binom{l-s+d}{d}, m\binom{l-s+d-2}{d-2}\right)$.

However, XL could not bring its superiority into full play if it does not satisfy $m - l \geq 2$, and this is the reason why FXL has been proposed, it is a variant for XL to solve a system when $m=l$. As MMI is a system with m MQ equations in l variants ($m=l$), so we guess the attacker may attack MMI through FXL.

V. EFFICIENCY OF THE PROPOSAL

In this section, we will make an efficiency analysis for our scheme, which aims at the key size as it is the main drawback for MPKC. In [4], [5] and [6], without reducing the security of the scheme, it is a good idea to insert a highly structured matrix into the coefficient matrix of the public key to decrease the key size of Rainbow. Furthermore, through this method, it also improved the efficiency of signature's verification. In the other hand, we also make a small change in the construction of the central map of the last layer, and it does not obviously increase the key size.

As for our scheme, we choose the parameters as follo w: $K=GF(2^8),(v_1,o_1,o_2)=(17,13,13),n=32,u=2$. With chose n these parameters, the private size of MMI after modifica tion is about 10 Kb, and then we can get the table I about t he key size.

TABLE I. THE KEY SIZE

Scheme	Public key size (KB)	Private key size (KB)	Ciphertext length (Bits)
MMI scheme	17.5	10	256
Rainbow	25.1	19.1	344
Cyclic	9.5	19.1	344
Signcryption	27	25	300

According to table 2, we can find that the ciphertext length decreased by 50% after making improvement of the scheme. Although the public key size of the signcryption scheme has not been improved, the private key size decreased by 2% while realizing encryption as well as signature at the same time.

VI. CONCLUSIONS

This article proposes a signcryption scheme based on MMI and cyclic rainbow after making some changes to the central map, which makes use of the special character of multi-layer construction. Besides, with chosen parameters, we make an analysis for scheme's security and efficiency. However, our scheme was designed to sign a message after encryption, how to choose the optimizing parameter to improve the computation should be studied further.

ACKNOWLEDGEMENT.

This work is partially supported by Natural Science Foundation of China (61103231, 61272492), the Project funded by China Postdoctoral Science Foundation (2014M562445), and the Natural Science Basic Research Plan in Shaanxi Province of China (2014JQ8358, 2014JQ8307). We also thank Lan Jinjia for his comments.

REFERENCES

[1] Ding J T, Multivariate public key cryptosystems, Berlin Springer-Verlag, pp.1-10, 2006.

[2] Matsumoto, Tsutomu, and Hideki Imai, Public quadratic polynomial-tuples for efficient sig-nature-verification and message-encryption, Advances in Cryptology—EUROCRYPT'88. Davos, Swit- zerland, May 1988, LNCS Volume 330, pp.419–453, 1988.

[3] Patarin, Cryptoanalysis of the Matsumoto and Imai public key scheme of Euro- crypt'88, In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 248–261, 1995.

[4] Petzoldt, Bulygin and Buchmann, CyclicRainbow – A Multivariate Signature Scheme with a Partially Cyclic Public Key. INDOCRYPT 2010. LNCS, vol. 6498, pp. 33–48, 2010.

[5] Petzoldt, Bulygin and Buchmann, Linear Recurring Sequences for the UOV Key Generation, PKC 2011. LNCS, vol. 6571, pp. 335–350, 2011.

[6] Petzoldt, Albrecht, Stanislav Bulygin, and Johannes Buchmann, Fast Verification for Improved Versions of the UOV and Rainbow Signature Schemes, Berlin Springer Heidelberg, pp.188-202, 2013

[7] Jiao Luyao, Li Yifa and Qiao Shuaiting, A new scheme based on the MI scheme and its analysis, JOURNAL OF ELECTRONICS(CHINA),Vol.30 No.2, pp.198-203, 2013.

[8] Li Huixian, et al, Certificateless Multi—receiver signcryption Scheme Based on Multivariate Public Key Cryptography, Chinese Journal of Computers 35(9), pp.1881-1889, 2012.

[9] Jintai Ding and Dieter Schmidt, Rainbow- a New Multivariable Polynomial Signature Scheme, ACNS 2005, LNCS 3531, pp.164–175, 2005.

[10] Patarin and Jacques, Hidden fields equations (HFE) and isomorphisms of polynomials (I-P): Two new families of asymmetric algorithms, Advances in Cryptology—Eurocrypt'96, Berlin Springer-verlag, pp.188-202, 1996