# A New Multivariate-based Ring Signature Scheme

Ling ling Wang
College of Information Science &Technology,
Qingdao University of Science &Technology,
Qingdao 266061, China
E-mail: teacherwll@163.com

***Abstract*—Most of the existing ring signature schemes are based on traditional cryptography, such as RSA and discrete logarithm. Unfortunately these schemes would be broken if quantum computers emerge. The MQ-problem based Public-Key Cryptosystem (MPKC) is an important alternative to traditional PKCs for its potential to resist future attacks of quantum computers. In this paper, we proposed a new ring signature scheme based on MPKC, which has the properties of consistent, unforgery, signer-anonymity.**

***Keywords: ring signature; multivariate public-key cryptosystem; anonymity***

## I. INTRODUCTION

Ring signatures were first introduced and implemented by Rivest and Tauman[1]. In a ring signature scheme, the formation of all possible signers, i.e. ring members, serves as a part of the ring signature for the signed messages. A valid ring signature will convince a verifier that the signature is generated by one of the ring members, without revealing any information about which participant is the actual signer. Ring signatures were originally proposed as a secret leaking technique. It guarantees the anonymity of the revealer. Now most of the existing ring signature schemes are based on traditional Public key cryptosystem, such as RSA, DLP, IDB, etc. Ring signature schemes based on bilinear pairings and identify-based cryptography [2] was first proposed by Zhang. Later, Wang[3,4] proposed a XTR-based and certificateless ring signature schemes.

With the existence of quantum computers, the problems such as integer factoring or discrete logarithms can be solved in polynomial time, which will be a serious threat to the security of existing deniable ring signatures. It is imminent to build a new public key cryptosystem which can replace the cryptosystems based on the number theory and survive from future attacks utilizing quantum computers. Multivariate public key cryptosystems (MPKCs) potentially could resist future quantum computing attacks, and it is much more computationally efficient than number theoretic-based systems. Multivariate public key cryptography has already experienced 20 years of development. There are many MPKCs, such as MIA family[5], OV family[6], HFE family[7], TTM family, MFE family and an *l*IC family. Multivariate public key cryptosystems over a finite field of odd characteristics is a new idea to get fast signature schemes. Odd-characteristic systems can be much simpler than their even-characteristic counterparts while still evading algebraic attacks. As multivariate public key cryptosystem over a finite field of odd characteristic is a safer and more efficient cryptosystem, it has recently been widespread [8,9,10].

Recently, Sakumoto et al.[13] presented a new identification based on MPKC and proved it secure. In this paper, we extended the identification scheme by applying the Fiat-Shamir paradigm [14] to transform it into a signature scheme. We proposed a new ring signature scheme based on Multivariate Public-Key Cryptosystem. We also give a specific scheme which was proved secure. By virtue of the Multivariate Public-Key Cryptosystem, our scheme can survive from future attacks utilizing quantum computers. And it is much more computationally efficient than number theoretic-based systems.

The rest of this paper is structured as follow. In section 2, we review briefly multivariate public key cryptography and deniable ring authentication. In section 3, we present a generic construction for MPKC-based ring signature scheme and the security analysis. In section 4, we draw our conclusions.

## II. PRELIMINARIES

### A. Ring Signatures

We call a set of possible signers *a ring*, the ring member who produces the actual signature *the signer* and each of the other ring members *a non-signer*. Assume there are $n$ members in a ring. A ring signature scheme is defined by the following procedures:

**–Key-Gen**($k$) is a probabilistic polynomial algorithm that accepts security parameter $k$, and returns system parameters and key pairs(public key $P_i$ and the corresponding secret key $S_i$).

**–ring-sign**($m$, $P_1$, $P_2$,…, $P_r$, $s$, $S_s$) is a probabilistic polynomial algorithm that produces a ring signature $\sigma$ for the message $m$, given the public keys $P_1$, $P_2$,…, $P_r$ of $r$ ring members, together with the secret key $S_s$ of the $s$-th member (who is the actual signer).

**–ring-verify**($m$, $S_s$) is a deterministic algorithm that takes a message $m$ and a signature $\sigma$ (which includes the public keys of all the possible signers), outputs either *true* if the ring signature is valid, or *false* otherwise.

In a ring signature, different members can use different independent public key signature schemes, with different key and signature sizes. We can see that a ring signature scheme satisfies the properties of anonymity (or signer-ambiguity) and spontaneity (namely, no setup procedure). Rivest, et al. [1] formalized “Ring Signature” because their construction of the signature forms a ring structure. Some other works in

Published by Atlantis Press, Paris, France.

the literature also call this kind of signature (with the above properties) "Ring Signature" although some of them may not have a ring structure for their construction.

### B. Multivariate Signature Scheme

Multivariate Public Key Cryptography is one of the main approaches for secure communication in the post-quantum world. The principle idea is to choose a multivariate system $F$ of quadratic polynomials which can be easily inverted. After that one chooses two affine linear invertible maps $S$ and $T$ to hide the structure of the central map. The public key of the cryptosystem is the composed map $P = S \circ F \circ T$ which is difficult to invert. The private key consists of $S$, $F$ and $T$ and therefore allows inverting $P$.

The generic multivariate signature scheme is as follows:

***Key-Generating*:** Let $k$ is a finite field, $P$ be a map $k^n \rightarrow k^m$, $S$ be an injective affine map over $k^m$ and $T$ be an invertible affine map over $k^n$ . The cipher $P$ is constructed as a composition of three maps:

$P = S \circ F \circ T = (f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$, where $f_j$ $(j = 1, 2, \ldots, m) \in k[x_1, x_2, \ldots, x_n]$.

The private key: The private key includes the two affine transformations $S$ and $T$. The map $P$ may or may not be part of the secret key depending on its precise nature.

The public key: The public key includes the following:

(1) The field $k$ including its additive and multiplicative structure;

(2) The $m$ polynomials $f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n) \in k[x_1, x_2, \ldots, x_n]$.

***Sign-algorithm*:** Let $(y_1', \ldots, y_m') \in k^m$ be a message (or message digests) to be signed. The signer computes the ring signature by the equation: $(x_1', \ldots, x_n') = P^{-1}(y_1', \ldots, y_m') = T^{-1} \circ F^{-1} \circ S^{-1}(y_1', \ldots, y_m')$. Then the signature on the message $(y_1', \ldots, y_m')$ is $(x_1', \ldots, x_n')$.

***Verify-algorithm*:** To verify that $(x_1', \ldots, x_n')$ is indeed a valid signature for the message $(y_1', \ldots, y_m')$, the recipient determines whether or not the following equation holds.

$y_j' = f_j(x_1', \ldots, x_n')$, $j$=1,2,…,$m$.

The above process can be completed by anyone, because the public key is available for anyone.

**MQ-Problem**: Given m quadratic polynomials $p_1, \ldots, p_m$ in $n$ variables over a finite field $F$, find a vector $\mathbf{x} = (x_1, \ldots, x_n) \in F^n$ such that $p_1(x) = \ldots = p_m(x) = 0$.

The MQ-Problem is proven to be NP-hard[11] even for quadratic systems over the field of two elements [12].

### C. The MQ-based identification scheme

At CRYPTO 2011 Sakumoto et al. presented a new identification scheme whose security is based solely on the MQ-Problem [13]. In the scheme, every user chooses a vector $s \in F^n$ as his secret key and compute his public key as $v = P(s) \in F^m$. In order to create a zero-knowledge proof of the vector $s$, a *polar form* of the multivariate system $P$ is needed, which is defined as

$G(x; y) = P(x+ y) - P(x) - P(y)$

Since $G(x; y)$ is bilinear in x and y, the knowledge of $s$ is equivalent to knowing a tuple $(r_0, r_1, t_0, t_1, e_0, e_1)$ satisfying $G(t_0, r_1) + e_0 = v - P(r_1) - G(t_1, r_1) - e_1$ and $(t_0, e_0) = (r_0 - t_1, P(r_0) - e_1)$. The 3-pass identification scheme between a prover and a verifier is as follows:

(1) the prover chooses $r_0, t_0 \in_R F^n$, $e_0 \in_R F^m$, computes $r_1 = s - r_0$, $t_1 = r_0 - t_0$, $e_1 = P(r_0) - e_0$; and computes commitments $c_0 = Com(r_1, G(t_0, r_1) + e_0)$, $c_1 = Com(t_0, e_0)$, $c_2 = Com(t_1, e_1)$, then sends $(c_0, c_1, c_2)$ to the verifier.

(2)the verifier chooses the challenge $Ch \in_R \{0,1,2\}$, and sends $Ch$ to the prover.

(3) If $Ch$=0, the prover sends $Rsp = (r_0, t_1, e_1)$ back;

If $Ch$=1, the prover sends $Rsp = (r_1, t_1, e_1)$ back;

If $Ch$=2, the prover sends $Rsp = (r_1, t_0, e_0)$ back;

(4) If the verifier chooses 0 as the challenge $Ch$, he checks whether $c_1 = Com(r_0 - t_1, P(r_0) - e_1)$ and $c_2 = Com(t_1, e_1)$ holds. If $Ch$=1, check whether $c_0 = Com(r_1, v - P(r_1) - G(t_1, r_1) - e_1)$ and $c_2 = Com(t_1, e_1)$ holds; If $Ch$=2, check whether $c_0 = Com(r_1, G(t_0, r_1) + e_0)$ and $c_1 = Com(t_0, e_0)$ holds.

## III. A MPKC-BASED RING SIGNATURE SCHEME AND ITS SECURITY ANALYSIS

### A. A MPKC-Based ring signature scheme

In this section, we present our MPKC-Based ring signature scheme (MRSS) by extending the identification scheme in [13]. We describe MRSS by providing the description of the following algorithms: Setup, MRSS-Sign and MRSS-Verify.

**Setup:** a probabilistic algorithm outputs the system parameters $(k, q, \xi, n, m, H)$, where $k = GF(q)$ is a finite field with $q = p^{\xi}$, and $p$ is a prime, $m$ is the number of multivariate equations, $n$ is the number of variables. Let $H$: $\{0, 1\}^* \rightarrow Z_p^*$ be a cryptographic secure hash functions. It also outputs the public key $PK$ and secret key $SK$ for each user in the system. Suppose that $PK_i/SK_i$ are the public key and private key pairs of user $U_i$, where $i = 0, 1, 2, \ldots, t-1$. Every user $U_i$ chooses randomly a vector $s_i$. The public key is $PK_i = P_i$: $F^n \rightarrow F^m$ , where $P_i(s_i)=0$.

**MRSS-Sign**: To get a ring signature on a message $m$ with respect to the ring $U = (U_0, U_1, \ldots, U_{N-1})$, a signer $U_s$ $(0 \leqslant s \leqslant N-1)$ who owns the private key $SK_s$ generates a signature of message $m$ as follows.

*a) Choose* $r_0^s, t_0^s \in F^n, e_0^s \in F^m$, compute

$$r_1^s = Ss - r_0^s,\ t_1^s = r_0^s - t_0^s,\ e_1^s = P_i(r_0^s) - e_0^s;$$
$$c_0^s = Com(r_1^s, Gs(t_0^s, r_1^s) + e_0^s),$$
$$c_1^s = Com(t_0^s, e_0^s),$$
$$c_2^s = Com(t_1^s, e_1^s),$$

*b) For* j$\in\{0, 1, \ldots, s-1, s+1, \ldots, N-1\}$, *using 0 as "secret" key* $s_i$, *and compute* $c_0^j$, $c_1^j$, $c_2^j$ *for the N-1 non-signers,*

Let $C_0 = Com(c_0^1, \ldots, c_0^N)$

$C_1 = Com(c_1^1, \ldots, c_1^N)$

$C_2 = Com(c_2^1, \ldots, c_2^N)$

And compute $ch = H(m||C_0||C_1||C_2)$

*c) For* $i \in \{0, 1, \ldots, N-1\}$,

*If* $ch=0$, let $Rsp_i = (r_0^i, t_1^i, e_1^i)$

*If ch*=1, let $Rsp_i=(r_1^i,\ t_1^i,\ e_1^i)$

*If ch*=2, let $Rsp_i=(r_1^i,\ t_1^i,\ e_1^i)$

*Let RSP*=( $Rsp_0$|| $Rsp_1$||…|| $Rsp_{N-1}$)

*The resulting signature is* $\sigma = (C_0||\ C_1||\ C_2\ ||\ RSP)$.

**MRSS-Verify:** To verity a signature ($m$, $\sigma$ ), the receiver performs the following.

*a) Compute ch=H(m||*$C_0$*||*$C_1$*||*$C_2$*);*

*b) If ch=0*, parses *RSP* into $r_0^1,\ t_1^1,\ e_1^1, r_0^2,\ t_1^2,\ e_1^2, \dots, r_0^N,\ t_1^N,\ e_1^N$, for *i*=0,1,…, *N*-1, *Compute*

$$c_1^i = Com\left(r_0^s - t_1^i, P_i(r_0^i) - e_1^i\right),$$

$$c_2^i = Com\left(t_1^i,\ e_1^i\right)$$

And check, if $C_1$= *Com*$(c_1^1, \dots, c_1^N)$ and $C_2$= *Com*$(c_2^1, \dots, c_2^N)$ If yes, returns 1 and accept it. Otherwise 0 and reject it.

*If ch=1*, parses *RSP* into $r_1^1,\ t_1^1,\ e_1^1, r_1^2,\ t_1^2,\ e_1^2, \dots, r_1^N,\ t_1^N,\ e_1^N$, for *i*=0,1,…, *N*-1, *Compute*

$$c_0^i = Com\left(r_1^i, -P_i(r_1^i) - G_i(t_1^i, r_1^i) - e_1^i\right),$$

$$c_2^i = Com\left(t_1^i,\ e_1^i\right)$$

And check, if $C_0$= *Com*$(c_0^1, \dots, c_0^N)$ and $C_2$= *Com*$(c_2^1, \dots, c_2^N)$ If yes, returns 1 and accept it. Otherwise 0 and reject it.

*If ch=2*, parses *RSP* into $r_1^1,\ t_0^1,\ e_0^1, r_1^2,\ t_0^2,\ e_0^2, \dots, r_1^N,\ t_0^N,\ e_0^N$, for *i*=0,1,…, *N*-1, *Compute*

$$c_0^i = Com\left(r_1^i, G_i(t_0^i, r_1^i) - e_0^i\right),$$

$$c_1^i = Com\left(t_0^i,\ e_0^i\right)$$

And check if $C_0$= *Com*$(c_0^1, \dots, c_0^N)$ and $C_1$= *Com*$(c_1^1, \dots, c_1^N)$. If yes, returns 1 and accept it. Otherwise 0 and reject it.

### B. Security analyses

**Theorem 1** MRSS is consistent.

***Proof.*** If the signature $\sigma = (C_0||\ C_1||\ C_2\ ||\ RSP)$ is not altered, since the following equations hold.

$G(t_0, r_1) + e_0 = v - P(r_1) - G(t_1, r_1) - e_1$;

$(t_0, e_0) = (r_0 - t_1, P(r_0) - e_1)$.

From the procedure of MRSS-Verify, the following equations will hold.

$$c_0^i = Com\left(r_1^i,\ G_i(t_0^i, r_1^i) - e_0^i\right) = Com\left(r_1^i,\ -P_i(r_1^i) - Gi(t_1^i, r_1^i) - e_1^i\right);$$

$$c_1^i = Com\left(r_0^s - t_1^i,\ P_i(r_0^i) - e_1^i\right) = Com\left(t_0^i,\ e_0^i\right);$$

$$c_2^i = Com\left(t_1^i,\ e_1^i\right).$$

Then, MRSS is consistent.

**Theorem 2** MRSS is resistant to forgery.

***Proof.*** Since the MQ-Problem is NP-hard even for quadratic systems over the field of two elements. Therefore, given the public keys of the ring, it is impossible to compute the secret key of the signer. Given a message-signature pair($m$, $\sigma$ ) and all public keys of the ring, it is infeasible to generate a valid ring signature. Hence, in the MRSS-Sign step, those who have no correct secret keys cannot forge the signature.

**Theorem 3** MRRS provides signer- anonymity.

***Proof.*** For the challenges 0, 1 and 2, the responses of both a signer and a non-signer are completely indistinguishable. Since $r_0$, $t_0$ and $e_0$ are chosen uniformly at random and therefore the responses are random, too. Hence, the ring signature $\sigma = (C_0||\ C_1||\ C_2\ ||\ RSP)$ is fully randomly distributed, even if the attacker has access to all private keys of the ring members, his probability to guess the identity of the real signer should not be greater than 1/2. As a result, the ring signature scheme should satisfy the property of anonymity.

## IV. CONCLUSIONS

In this paper, we present a new ring signature scheme based on MPKC by transforming the identificaiotn scheme in [13] and gave its security analysis. Our scheme has the properties of consistent, unforgery, signer- anonymity. Since solving a set of multivariate quadratic polynomial equations over a finite field, is an NP-hard problem, our scheme can survive future attacks utilizing quantum computers.

## ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China under grants No. 60902034, Shandong excellent young scientist research award fund under grants No. BS2011DX009. Thanks also go to the anonymous reviewers for their useful comments.

## REFERENCES

[1] R. Rivest, A. Shamir, and Y. Tauman, “How to Leak a Secret”, Proc. Asiacrypt ’01, Berlin: Springer-Verlag, LNCS 2248, 552-565.

[2] F.Zhang, K.Kim, “ID-based blind signature and ring signature from pairings”, In: Zheng Y L, ed. Proc of ASIACRYPT’02. LNCS 2501, Berlin: Springer-Verlag, 2002, 533–547

[3] L.Wang G.Zhang, C.Ma, "A Secure Ring Signcryption Scheme for Private and Anonymous Communication," 2007 IFIP International Conference on Network and Parallel Computing Workshops (NPC 2007) 107-111.

[4] L.Wang G.Zhang, C.Ma, “A new multi-bank e-cash protocol with anonymity control”, 2009 Fifth International Conference on Information Assurance and Security, vol. 1,.536-539.

[5] C. Wolf, B. Preneel, “Taxonomy of public key schemes based on the problem of multivariate quadratic equations”, Cryptology ePrint Archive. http://eprint.iacr.org/2005/077/.

[6] B. Olivier, M.R. Gilles, “Cryptanalysis of the square cryptosystems”, in: Advances in Cryptology-ASIACRYPT 2009, LNCS 5912, Springer, Berlin, 2009, 451−468.

[7] J.T. Ding, D. Schmidt, F. Werner, “Algebraic attack on HFE revisited”, in: The 11th Information Security Conference, in: LNCS 5222, Springer-Verlag, Berlin, 2008, 215−227.

[8] C. Clough, J. Baena, J. Ding, B.-Y. Yang, M.-S. Chen, Square, “a new multivariate encryption scheme”, in: Topics in Cryptology − CT-RSA 2009, in: LNCS 5473, Springer-Verlag, Berlin, 2009, 252−264.

[9] C.L. Clough, “Square: a new family of multivariate encryption schemes”, University of Cincinnati, Cincinnati, 2009, 67−73.

[10] C.L. Clough, J.T. Ding, “Secure variants of the square encryption scheme”, in: Post-Quantum Cryptography, LNCS 6061, Springer-Verlag, Berlin, 2010, 153−164.

[11] J. Patarin, L. Goubin, “Trapdoor one-way permutations and multivariate polynomials”, in: International Conference on

Information Security and Cryptology 1997, in: LNCS 1334, Springer, Berlin, 1999, 356−368.

[12] M. R. Garey and D. S. Johnson, “Computers and Intractability: A Guide to the Theory of NPCompleteness”, W.H. Freeman and Company, 1979.

[13] K. Sakumoto, T. Shirai and H. Hiwatari, “Public-Key Identi_cation Schemes based on Multivariate Quadratic Polynomials”, CRYPTO 2011, LNCS vol. 6841, 706 - 723.

[14] A. Fiat and A. Shamir, “How to Prove Yourself”, CRYPTO 1986, Springer 1986, LNCS vol. 263, 186 - 194.

Published by Atlantis Press, Paris, France.