Computers and Mathematics with Applications 62 (2011) 3973–3979

Contents lists available at SciVerse ScienceDirect

Computers and Mathematics with Applications

journal homepage: www.elsevier.com/locate/camwa

Ring signature scheme based on multivariate public key cryptosystems

Shangping Wang [a,*], Rui Ma [a], Yaling Zhang [b], Xiaofeng Wang [a]

[a] School of Science, Xi'an University of Technology, 710054 Xi'an Shaanxi, China

[b] School of Computer Science and Engineering, Xi'an University of Technology, 710048 Xi'an Shaanxi, China

ARTICLE INFO

Article history:
Received 24 January 2011
Received in revised form 21 September 2011
Accepted 22 September 2011

Keywords:
Ring signature
Multivariate public key cryptosystem
Algebraic attacks
Quantum computing
Security

ABSTRACT

The ring signature scheme is an important cryptographic primitive that enables a user to sign a message on behalf of a group in authentic and anonymous way, i.e. the recipient of the message is convinced that the message is valid and it comes from one of the group members, but does not know who the actual signer is. Currently, all the existing ring signatures are based on traditional cryptosystems. However, the rapid advances in the field of quantum computing indicate a growing threat to traditional cryptosystems. Multivariate public key cryptosystems (MPKCs) is one of the promising alternatives which may resist future quantum computing attacks. In this work, we propose a novel ring signature scheme based on multivariate polynomials with the security model for the first time. Our ring signature scheme has a great advantage in efficiency compared to many existing ring signature schemes, and currently it seems to be immune to quantum computing attacks.

1. Introduction

Rivest et al. [1] first formally introduced the concept of the ring signature scheme, and proposed the first ring signature scheme based on RSA. A ring signature scheme can be viewed as a group signature scheme with no anonymity revocation and simple group setup. A ring signature scheme allows a signer to realize unconditional anonymous signature to a message, that is, there is no way to trace the identity of the signer. Ring signature can be used in e-voting, electronic cash, leaking secrets anonymously and anonymous authentication in communication, etc. Up till now a variety of ring signature schemes have been proposed. In 2002, Abe et al. proposed the first ring signature scheme based on the discrete logarithm over finite fields [2]. Bilinear pairings were used to design ring signature schemes [3,4], however computing pairings lead to low efficiency. Emmanuel Bresson et al. put forward the concept of a threshold ring signature scheme. In view of the needs of privacy protection, Naor proposed a deniable ring authentication scheme [5].

In 2003, Susilo et al. presented a non-interactive deniable ring authentication scheme [6]. Lv and Wang proposed an anonymity-revocable ring signature scheme—the Verifiable Ring Signature Scheme [7]. Herranz and Saez put forward Forking Lemmas so as to simplify the security proof of ring signature scheme [8].

In 2004, Dodis et al. introduced an ad hoc anonymous identification scheme [9], which was a new multi-user cryptographic primitive that allowed participants from a user population to form ad-hoc groups, and then proved membership anonymously in such groups. The scheme was based on the notion of an accumulator with a one-way domain.

In 2005, a further study of the threshold ring signature was made in the literature [10,11]. Lee et al. proposed another anonymity-revocable ring signature scheme [12] and applied it in both e-voting and electronic cash systems. For the problem of key exposure, Liu and Wong proposed the first forward secure ring signature scheme and the first key-insulated ring signature scheme [13].

* Corresponding author.
E-mail addresses: spwang@mail.xaut.edu.cn, spwang99@hotmail.com, spang@mail.xaut.edu.cn (S. Wang), ylzhang@xaut.edu.cn (Y. Zhang).

0898-1221/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.camwa.2011.09.052

With the development of ring signature, in 2006, Benderet al. analyzed previous definitions of security for ring signature schemes and suggested that most of these prior definitions were too weak [14]. The paper showed the first constructions of ring signature schemes in the standard model.

In 2007, Fujisaki and Suzuki proposed a traceable ring signature scheme that can restrict "excessive" anonymity in [15]. The traceable ring signature has a tag that consists of a list of ring members and an issue that refers to, for instance, a social affair or an election. The traceable ring signature can be used in many applications, such as an anonymous voting on a BBS, a dishonest whistle-blower problem. The literature [15] formalized the security definitions for this primitive and showed an efficient and simple construction.

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 ring signatures. Building a new public key cryptosystem which can replace the cryptosystems based on the number theory and survive from future attacks utilizing quantum computers is imminent. Multivariate public key cryptosystems (MPKCs) potentially could resist future quantum computing attacks, and it is much more computationally efficient than number theoretic-based systems. Therefore, the research of multivariate public key cryptography becomes a very active topic.

Multivariate public key cryptography has already experienced 20 years of development. There have been an MIA family, OV family, HFE family, TTM family, MFE family and an l IC family and other systems. 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. Then the square cryptosystems appeared [16]. The square cryptosystems are based on design ideas taken from both the HFE cryptosystem and the UOV cryptosystem. However, the important properties of the square cryptosystems are that they are defined over fields of odd characteristics and their internal transformations are quadratic. The existing multivariate public key cryptosystem over a finite field of odd characteristics are mainly the MIO scheme [17], the projected HFE cryptosystem (PHFE) [18], Odd-Char Multivariate Hidden Field Equations [19], the Square encryption scheme [20] and Square-Vinegar Signature Scheme [21] and so on. The Square encryption scheme [20] and Square-Vinegar Signature Scheme [21] are the representatives of the square cryptosystem [16]. However, in Asiacrypt2009, Olivier and Gilles proposed a method [16] which can break the Square encryption scheme [20]. For this reason, Crystal Clough and others proposed a modified square: square+ in May 2009 [22,23]. The square+ system [22,23] is a modified square encryption scheme [20]. The square+ system [22,23] has a simple core map, allowing for high signature efficiency and enhanced security. So far, the square+ system can resist all known attacks [22,23] in Multivariate public key cryptosystems.

Our contributions. The existing ring signatures based on traditional cryptosystems such as RSA will face a serious security threat under quantum computing. To address this problem, in this work, we propose a novel multivariate ring signature scheme based on multivariate polynomials, and present a security model for a multivariate ring signature scheme. The security of the multivariate ring signature scheme is analyzed. The conclusion is that our multivariate ring signature satisfies the property of completeness, anonymity against full key exposure and it can resist known attacks on MPKCs, if we suppose that the underlying MPKCs, which is used in our ring signature scheme, is secure against known attacks on MPKCs such as Algebraic Attacks, Linearization Equation Attacks, Rank Attacks, and Differential Attacks. Our ring signature scheme has great advantages in efficiency over many existing ring signature schemes, and currently it seems to be immune to quantum computing attacks.

The paper is organized as follows. In Section 2, we introduce the concept of ring signature schemes and multivariate public key cryptosystems. In Section 3, we give a generic multivariate ring signature scheme with its security model. And then we present a ring signature scheme based on odd-characteristic multivariate polynomials. We conclude the paper in Section 4.

2. Preliminaries

2.1. Ring signature scheme

In a ring signature scheme, the signer chooses a group of users including himself, using his private key and public keys of other users to sign on a message; and the name of the ring signature comes from the fact that the signature usually forms a circle in the verifying procedure, the group sometimes is called a ring. The verifier can be convinced that the signature was indeed generated by one of the ring members; however, the verifier is unable to tell which member actually produced the signature, thus the ring signature scheme is signer anonymous.

A ring signature scheme [1] constitutes of four protocol procedures:

Parameter-generator: generate the system parameters.

Key-generator: generates each user's public key and private key pairs PK_i/SK_i, $i = 1, \ldots, t$.

Ring-sign: a probabilistic algorithm which takes as input a key pair $(pk; sk)$ and a set of public keys R that constitutes the ring, along with a message M in some message space to be signed. It is required that $pk \in R$ holds true. The algorithm returns a ring signature σ on M for the ring R.

Ring-verify: a deterministic algorithm takes as input a set of public keys R that constitutes the ring and a purported ring signature σ on a message M. It returns either valid or invalid.

2.2. Multivariate signature scheme

The generic multivariate signature scheme is as follows:

Key-generating. Let k is a finite field, F be a map $k^n \to k^m$, L_1 be an injective affine map over k^m and L_2 be an invertible affine map over k^n. The cipher $\overline{F}$ is constructed as a composition of three maps:

$$\overline{F} = L_1 \circ F \circ L_2 = \left(\overline{f}_1(x_1, \ldots, x_n), \overline{f}_2(x_1, \ldots, x_n), \ldots, \overline{f}_m(x_1, \ldots, x_n)\right), \tag{2.1}$$

where $\overline{f}_j\ (j = 1, 2, \ldots, m) \in k[x_1, x_2, \ldots, x_n]$.

The private key. The private key includes the two affine transformations L_1 and L_2. The map F 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 $\overline{f}_1(x_1, \ldots, x_n), \ldots, \overline{f}_m(x_1, \ldots, x_n) \in k[x_1, x_2, \ldots, x_n]$.

Signing-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 (2.2).

$$(x'_1, \ldots, x'_n) = \overline{F}^{-1}(y'_1, \ldots, y'_m) = L_2^{-1} \circ F^{-1} \circ L_1^{-1}(y'_1, \ldots, y'_m). \tag{2.2}$$

Then the signature on the message $(y'_1, \ldots, y'_m)$ is $(x'_1, \ldots, x'_n)$.

Verifying-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 (2.3) is hold.

$$y'_j = \overline{f}_j(x'_1, \ldots, x'_n), \quad j = 1, 2, \ldots, m. \tag{2.3}$$

If it is true, then accept the signature $(x'_1, \ldots, x'_n)$ as valid; otherwise reject.

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

As we can see from the above signature scheme, the core of multivariate signature scheme over a finite field should be the selection of the center invertible mapping F. Therefore, according to the different F, we get different multivariate signature schemes over a finite field. The security of these cryptosystems depends on the problem of multivariate quadratic polynomial equations, that is, solving a set of multivariate quadratic polynomial equations over a finite field, in general, is proven to be an NP-hard problem [24,25].

3. A generic multivariate ring signature scheme and its security analysis

3.1. Definitions of multivariate ring signature schemes

Currently, most of the ring signature schemes are based on traditional cryptosystems. However, the rapid advances in the field of quantum computing indicate a growing threat to traditional cryptosystems. Multivariate public key cryptosystems is one of the promising alternatives which may resist quantum computing attacks. So in this section we present a generic multivariate ring signature scheme based on multivariate polynomials, which is expected be secure under the quantum computing attacks, and we also present a security model for the multivariate ring signature scheme.

A generic definitions of a multivariate ring signature schemer based on MPKCs

Definition 1 (*Multivariate Ring Signature Based on MPKCs*)**.** A ring signature scheme based on MPKCs consists of a triple of PPT algorithms (*Key-Gen*; *Ring-Sign*; *Ring-Vrfy*) that, respectively, generate keys for a user, sign a message, and verify the signature:

Key-Gen, a probabilistic algorithm outputs the system parameters, the public key PK and secret key SK for each user in the system. The system parameters should include a finite field k, the number of multivariable equations m, and the number of the variables n. Besides, usually it should include a cryptographic secure hash function with $H : \{0, 1\}^* \to k^n$ and other needed parameters. The public key PK_i satisfies $PK_i \hat{=} \overline{F}_i = L_{1_i} \circ F_i \circ L_{2_i},\ i = 1, \ldots, t$ where $F_i : k^n \to k^m$ is an invertible map, $L_{1_i} : k^m \to k^m$ and $L_{2_i} : k^n \to k^n$ are two invertible affine linear maps, the private key corresponding to PK_i is $SK_i = \{L_{1_i}, F_i, L_{2_i}\}$.

Ring-Sign$_{SK_\pi}(M, R)$, a probabilistic algorithm which takes as inputs private key SK_π of the signer, and an ordered set of public keys $R = (PK_1, \ldots, PK_t)$ with $PK_\pi \in R$, and a message M to be signed, produces a ring signature σ on the message M with respect to the ring $R = (PK_1, \ldots, PK_t)$.

Ring-Vrfy$_R(M, \sigma)$, a deterministic algorithm that takes as inputs a message M and a claimed ring signature σ with respect to the ring R, it returns either valid or invalid.

A Security model of a multivariate ring signature scheme based on MPKCs

Completeness: The completeness requirement of a ring signature scheme is that for any integer t, any $\{(PK_i, SK_i)\}_{i=1}^{t}$ outputted by *Key-Gen*, any $\pi \in [t]$, and any message M, it holds that

$$\textit{Ring-Vrfy}_R\left(M, \textit{Ring-Sign}_{SK_\pi}(M, R)\right) = 1, \quad \text{where } R = (PK_1, \ldots, PK_t).$$

Anonymity: informally anonymity means that any adversary should not be able to determine which ring member in the ring $R = (PK_1, \ldots, PK_t)$ generated a ring signature σ. Rivest et al. [1] gave a formalization which has been used in much subsequent work. Recently, Bender et al. [14] described several possible stronger formulations of each notion. Anonymous against full key exposure is the strongest definition considered by Bender et al. [14]. We now adapt their definition of anonymity for our multivariate ring signature base on MPKCs, see [14] for additional details and motivation.

Definition 2 (*Anonymity Against Full Key Exposure*)**.** Let (*Key-Gen*; *Ring-Sign*; *Ring-Vrfy*) be a multivariate ring signature scheme, for any PPT adversary A, any positive integer number $t \geq 2$, and, consider the following game:

For $i = 1$ to t, generate $(PK_i; SK_i) \leftarrow \textit{Key-Gen}(\omega_i)$ for randomly-chosen ω_i. Give to A the set of public keys $S \stackrel{def}{=} \{(PK_i)\}_{i=1}^{t}$.

The adversary A is also given access to a Ring-signing oracle *O-Ring-sign* $(\cdot, \cdot, \cdot)$ such that *O-Ring-sign* $(\pi; M; R)$ returns $\textit{Ring-Sign}_{SK_\pi}(M, R)$, where we require $R \subseteq S$ and $PK_\pi \in R$.

A outputs a message M, and two distinct indices i_0, i_1, and a ring R for which $PK_{i_0}, PK_{i_1} \in R$; furthermore, a random bit b is chosen and A is given the ring signature $\sigma \leftarrow \textit{Ring-Sign}_{SK_{i_b}}(M, R)$, where the real signer's private key is SK_{i_b}. Then the adversary A is given the entire secret key $\{(SK_i)\}_{i=1}^{t}$.

The adversary A outputs a bit $\tilde{b}$, and succeeds if $\tilde{b} = b$.

The Ring-signature scheme (*Key-Gen*; *Ring-Sign*; *Ring-Vrfy*) achieves anonymity against full key exposure if, for any PPT A and any positive integer number $t \geq 2$, the success probability of A in the above game is negligibly close to $1/2$.

Anonymity. The anonymity requirement is that for any message M and any integer $t \in \mathrm{N}$, setting $(pk_i, sk_i) \leftarrow \text{key-gen}(\omega_i)$ for all $i \in [t]$, $R = \{pk_i\}_{i\in[t]}$, and signatures $\sigma_1 \leftarrow \textit{Sign}_{SK_{i_1}}(M, R)$,$\sigma_2 \leftarrow \textit{Sign}_{SK_{i_2}}(M, R)$, it holds that the distributions $(\{sk_i\}, R, M, \sigma_1)$ and $(\{sk_i\}, R, M, \sigma_2)$ are computationally indistinguishable (where all of our constructions in fact achieve statistical indistinguishability).

Unforgeability w.r.t. known attacks against MPKCs. One of the biggest concerns of *MPKCs* is the lack of provable security results. Today the security of MPKCs is still very much ad hoc. Proposed schemes are evaluated against known attacks. Thus for the unforgeability of our multivariate ring signature scheme based on MPKCs, we will also use this model to define its security, that is, we will say that our multivariate ring signature scheme based on MPKCs is unforgeability if the selected system parameters satisfy some requisite security level under all the known attacks against MPKCs.

Definition 3 (*Unforgeability w.r.t. Known Attacks Against MPKCs*)**.** A multivariate ring signature scheme (*Key-Gen*; *Ring-Sign*; *Ring-Vrfy*) is unforgeable w.r.t. known attacks for some given security level, saying 2^l multiplications on the finite field k, if for any PPT adversary A and for any positive integer number $t \geq 2$, the computational complexity that A succeeds in the following game is at least 2^l multiplications :

Suppose that Key pairs $\{(PK_i, SK_i)\}_{i=1}^{t}$ are generated by *Key-Gen*, and the set of public keys $S \stackrel{def}{=} \{(PK_i)\}_{i=1}^{t}$ is given to A.

The adversary A is also given access to a signing oracle *O-Ring-sign* $(\cdot, \cdot, \cdot)$ such that *O-Ring-sign* $(\pi; M; R)$ returns $\textit{Ring-Sign}_{SK_\pi}(M, R)$, where we require that the condition $R \subseteq S$ and $PK_\pi \in R$ are satisfied.

A is also given the ability of using the known attacks against MPKCs such as Direct Algebraic attacks, Linearization and Higher-Order Linearization Equation (HOLE) attack, Rank and High Rank attack, Differential attack, and so on.

Finally A outputs a ring signature $\tilde{\sigma}$ on the message $\tilde{M}$ with respect to a ring $\tilde{R}$, and succeeds if $\textit{Ring-Vrfy}_{\tilde{R}}(M, \tilde{\sigma}) = 1$,and A never queries $\left(*, \tilde{M}, \tilde{\sigma}\right)$, where $\tilde{R} \subseteq S$.

3.2. A generic multivariate ring signature scheme based on MPKCs

In this section we propose a generic multivariate ring signature scheme based on MPKCs, whose aim is to replace the traditional ring signature and to resist future quantum computing attacks. Our ring signature scheme (*Key-Gen*; *Ring-Sign*; *Ring-Vrfy*) is as follows:

Key-Gen: a probabilistic algorithm outputs the system parameters (k, q, ξ, 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. Message digest space is the vector space k^n. Let $H : \{0, 1\}^* \to k^n$ be a cryptographic secure hash function.

The system parameter generation algorithm 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 $i = 0, 1, 2, \ldots, t-1$. The public key is $PK_i = \overline{F}_i = L_{1i} \circ F_i \circ L_{2i}$, and the corresponding private key is $SK_i = \{L_{1i}, F_i, L_{2i}\}$, where $F_i : k^n \to k^m$ is an

invertible map, $L_{1i} : k^m \to k^m$ and $L_{2i} : k^n \to k^n$ are two invertible affine linear maps, $i = 0, 1, 2, \ldots, t-1$. The ring $R = (PK_0, \ldots, PK_{t-1}) = \left(\overline{F}_0, \overline{F}_1, \ldots, \overline{F}_{t-1}\right)$ is the ordered set of public keys.

Ring-Sign$_{SK_\pi}$ (M, R): To get a ring signature on a message M with respect to the ring $R = \left(\overline{F}_0, \overline{F}_1, \ldots, \overline{F}_{t-1}\right)$, the signer U_π $(0 \le \pi \le t-1)$ acts as follows:

Chooses at random an element $u \in k^n$, and computes

$$c_{\pi+1(\mathrm{mod}\ t)} = H\left(R, M, \overline{F}_\pi(u)\right);$$

(2) For $i = \pi+1, \pi+2, \ldots, t-1, 0, 1, \ldots, \pi-1$, uniformly picks $s_i \in k^n$, and computes

$$c_{i+1(\mathrm{mod}\ t)} = H\left(R, M, \overline{F}_i(c_i) + \overline{F}_i(s_i)\right); s_\pi = L_{2\pi}^{-1} \circ F_\pi^{-1} \circ L_{1\pi}^{-1}\left(\overline{F}_\pi(u) - \overline{F}_\pi(c_\pi)\right).$$

Thus the ring signature on message M with respect to the ring $R = \left(\overline{F}_0, \overline{F}_1, \ldots, \overline{F}_{t-1}\right)$ is $\sigma = (c_0, s_0, s_1, \ldots, s_{t-1})$.

Ring-Vrfy$_R$ (M, σ): To verify a claimed ring signature $\sigma = (c_0, s_0, s_1, \ldots, s_{t-1})$ on message M with respect to the ring $R = \left(\overline{F}_0, \overline{F}_1, \cdots, \overline{F}_{t-1}\right)$, the recipient computes $c_{i+1} = H\left(R, M, \overline{F}_i(c_i) + \overline{F}_i(s_i)\right)$ for $i = 0, 1, 2, \ldots, t-1$, and finally checks whether $c_t = c_0$. If yes, returns 1 or valid. Otherwise 0 or invalid.

3.3. The security analysis of our multivariate ring signature scheme

In this section we will analyze the security properties of our ring signature scheme, the security properties include completeness, anonymity against full key exposure and Unforgeability w.r.t. known attacks against MPKCs.

3.3.1. Completeness

Conclusion 1. The proposed ring signature scheme satisfies the property of Completeness.

In fact, suppose that any receiver gets a ring signature $\sigma = (c_0, s_0, s_1, \ldots, s_{t-1})$ on message M with respective to the ring $R = \left(\overline{F}_0, \overline{F}_1, \ldots, \overline{F}_{t-1}\right)$, and if the ring signature is generated according to the signing process *Ring-Sign*$_{SK_\pi}$ (M, R) above, and it is not changed in the process of transmission, then from the ring signature algorithm we have $\overline{F}_\pi(u) = \overline{F}_\pi(c_\pi) + \overline{F}_\pi(s_\pi)$, thus

$$c_{\pi+1(\mathrm{mod}\ t)} = H\left(R, M, \overline{F}_\pi(u)\right) = H\left(R, M, \overline{F}_\pi(c_\pi) + \overline{F}_\pi(s_\pi)\right)$$

so that $c_{i+1(\mathrm{mod}\ t)} = H\left(R, M, \overline{F}_i(c_i) + \overline{F}_i(s_i)\right)$ holds for $i = 0, 1, 2, \ldots, t-1$, especially for $i = t-1$, we have $c_0 = H\left(R, M, \overline{F}_{t-1}(c_{t-1}) + \overline{F}_{t-1}(s_{t-1})\right)$, and we note that $c_t = H\left(R, M, \overline{F}_{t-1}(c_{t-1}) + \overline{F}_{t-1}(s_{t-1})\right)$, so it holds that $c_t = c_0$, this completes our proof.

3.3.2. Anonymity against full key exposure

Conclusion 2 (*Anonymity Against Full Key Exposure*)**.** The proposed ring signature scheme satisfies the property of anonymity against full key exposure in Definition 1.

Here we use the Definition 1 of *anonymity against full key exposure* in Section 3.1, and we consider the game described in Definition 1. Suppose an attacker is given access (throughout the entire game) to a Ring-signing oracle *O-Ring-sign* $(\cdot, \cdot, \cdot)$ such that *O-Ring-sign* $(\pi; M; R)$ returns *Sign*$_{SK_\pi}$ (M, R), where we require $R \subseteq S$ and $PK_\pi \in R$. The attacker outputs a message M, distinct indices i_0, i_1. Then a random bit b $(b = 0$ or $b = 1)$ is chosen, and the attacker is given the ring signature $\sigma \leftarrow$ *Ring-Sign*$_{SK_{i_b}}$ (M, R), where the real signer's private key is SK_{i_b}. Then the adversary A is given the entire secret key $\{(SK_i)\}_{i=0}^{t-1}$.

Now we analyze the distribution of the ring signature $\sigma = (c_0, s_0, s_2, \ldots, s_{t-1})$. Because $s_i \in k^n$ $(i \ne i_b)$ is randomly selected, and u is randomly selected, as $s_{i_b} = L_{2i_b}^{-1} \circ F_{i_b}^{-1} \circ L_{1i_b}^{-1}\left(\overline{F}_{i_b}(u) - \overline{F}_{i_b}\left(c_{i_b}\right)\right)$, so we can conclude that s_{i_b} should be regarded as randomly distributed, that is, $(s_0, s_1, \ldots, s_{t-1})$ is uniformly distributed. In addition, from the equation $c_0 = H\left(R, M, \overline{F}_{t-1}(c_{t-1}) + \overline{F}_{t-1}(s_{t-1})\right)$ we know that c_0 is randomly distributed in k^m, this is because that s_{t-1} is randomly selected. Thus the ring signature $\sigma = (c_0, s_0, s_2, \ldots, s_{t-1})$ 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 from SK_{i_0} and SK_{i_1} should not be greater than 1/2. As a result, the ring signature scheme should satisfy the property of *anonymity against full key exposure*.

3.3.3. Unforgeability

Conclusion 3 (*Unforgeability w.r.t. Known Attack Against MPKCs*)**.** The proposed multivariate ring signature scheme based on MPKCs is unforgeable w.r.t. known attacks for some given security level, saying 2^l multiplications on the finite field, if

for any PPT adversary A the computational complexity to attack the underlying multivariate signature scheme used in the multivariate ring signature scheme is at least 2^l for known attacks against MPKC, such attacks including Direct Algebraic attacks, Linearization and Higher-Order Linearization Equation (HOLE) attacks, Rank and High Rank attacks, Differential attacks, and so on.

Now we consider the game in the Definition 2.

Suppose that Key pairs $\{(PK_i, SK_i)\}_{i=1}^t$ are generated by *Key-Gen*, and the set of public keys $S \stackrel{def}{=} \{(PK_i)\}_{i=1}^t$ is given to A.

The adversary A is also given access to a signing oracle *O-Ring-sign* $(\cdot, \cdot, \cdot)$ such that *O-Ring-sign* (π, M, R) returns *Ring-Sign*$_{SK_\pi}$ (M, R), where we require that the conditions $R \subseteq S$ and $PK_\pi \in R$ are satisfied.

A is also given the ability of using the known attacks against MPKCs such as Direct Algebraic attacks, Linearization and Higher-Order Linearization Equation (HOLE) attacks, Rank and High Rank attacks, Differential attacks, and so on.

Finally A outputs a ring signature $\tilde{\sigma}$ on the message $\tilde{M}$ with respect to a ring $\tilde{R}$, and succeeds if *Ring-Vrfy*$_{\tilde{R}}$ $(M, \tilde{\sigma}) = 1$ and A never queries $\left(*, \tilde{M}, \tilde{\sigma}\right)$, where $\tilde{R} \subseteq S$.

We now analyze the computational complexity for A to output the forged ring signature $\left(\tilde{R}, \tilde{M}, \tilde{\sigma}\right)$, assuming that attacker A as the signer u_π forges the ring signature $\left(\tilde{R}, \tilde{M}, \tilde{\sigma}\right)$ in the name of the ring$\tilde{R}$. Without loss of generality we assume that $\tilde{R} = \left\{\overline{F}_0, \overline{F}_1, \ldots, \overline{F}_{t-1}\right\}$, according to the ring signature *Ring-Sign*$_{SK_\pi}$ $\left(\tilde{M}, \tilde{R}\right)$, the attacker A calculates in accordance with the signature generation process in steps (1) and (2) of Section 3.2. But in order to forge a signature $\tilde{\sigma} = (c_0, s_1, s_2, \ldots, s_{t-1})$ of message M, the attacker needs to compute s_π such that

$$\overline{F}_\pi(s_\pi) = \left(\overline{F}_\pi(u) - \overline{F}_\pi(c_\pi)\right),$$

where u is randomly selected by the attacker. This is a fundamental problem in the MPKC. To solve this kind of problem there are several known attacks:

Direct Algebraic attacks: it means that to find $s_\pi \in k^n$ from the equation $\overline{F}_\pi(s_\pi) = \left(\overline{F}_\pi(u) - \overline{F}_\pi(c_\pi)\right)$ for the attacker A on condition that he does not know the private key $SK_\pi = \{L_{1\pi}, F_\pi, L_{2\pi}\}$. The Gröbner base and XL method are the most powerful attacks for this problem. If we suppose that computational complexity is at least 2^l to attack the underlying multivariate signature scheme used in the ring signature scheme by using the Gröbner base or XL method attacks, then the computational complexity to find $s_\pi \in k^n$ is at least 2^l.

Linearization attacks: A Linearization Equation is a relation between the $v_\pi \hat{=} \overline{F}_\pi(s_\pi) = \left(\overline{F}_\pi(u) - \overline{F}_\pi(c_\pi)\right) \in k^m$ and $s_\pi \in k^n$ that always holds for a given public keys $\overline{F}_\pi$, it has the following form:

$$\sum_{i,j} a_{ij} s_{\pi,i} v_{\pi,j} + \sum_i b_i s_{\pi,i} + \sum_j c_j v_{\pi,j} + d = 0.$$

A Higher-Order Linearization Equation (HOLE) is an equation that uses high order terms of the cipher text variables $\left(v_\pi = \overline{F}_\pi(s_\pi) = \left(\overline{F}_\pi(u) - \overline{F}_\pi(c_\pi)\right) \in k^m\right)$ while using only linear terms of plain text variables (s_π). In particular, a SOLE (second order linearization equation) would look like

$$\sum_{i<j} a_{ijk} v_{\pi,i} v_{\pi,j} s_{\pi,k} + \sum_{i \le j} b_{ij} v_{\pi,i} v_{\pi,j} + \sum_{ij} c_{ij} v_{\pi,i} s_{\pi,j} + \sum_i d_i v_{\pi,i} + \sum_j e_j s_{\pi,j} + f = 0.$$

In which we get an affine (linear) relation between s_π and v_π when substituted with the actual values of $v_\pi \in k^n$. If we suppose that the computational complexity is at least 2^l to attack the underlying multivariate signature scheme used in the ring signature scheme by using of such Linearization attacks or HOLE attacks, then the computational complexity to find $s_\pi \in k^n$ is at least 2^l.

Rank attacks: Goubin and Courtois show the MinRank attack for Triangular-Plus-Minus systems. Yang and Chen generalize the idea of Rank attack for multivariate systems in [26]. The complexity of the Rank attack is about $q^r \frac{\left(m^2\left(\frac{n}{2} - \frac{m}{6}\right) + mn^2\right)}{k}$ multiplications, where k is the number of linear combinations of the components of F_π which reach the minimal rank r.

A Dual Rank (or High Rank) attack means to find a variable appearing the fewest number of times in a central equation cross-term. If this least number is s, the complexity of the High Rank attack [26] is about $q^s\left(\frac{n^3}{6}\right)$ multiplications. If we suppose that the parameters were well selected so that the computational complexity to attack the underlying multivariate signature scheme used in the ring signature scheme is at least 2^l for both Rank attacks and High Rank attacks, then the computational complexity to find $s_\pi \in k^n$ is at least 2^l.

Differential attacks. Given the public key of MPKCs, which we denote as $\overline{F}_\pi$, a set of quadratic polynomials, its differential $D\overline{F}_\pi(x, c)$, a set of linear functions in x, is defined as $D\overline{F}_\pi(x, c) = \overline{F}_\pi(x + c) - \overline{F}_\pi(x) - \overline{F}_\pi(c) + \overline{F}_\pi(0)$. The key of this attack against the cryptosystem is by use of the hidden structures in the differential. If we suppose that the parameters were well selected such that the computational complexity to attack the underlying multivariate signature scheme used in the ring signature scheme is at least 2^l with differential attacks, then the computational complexity to find $s_\pi \in k^n$ is at least 2^l.

From the above analysis we can see that if for any PPT adversary A the computational complexity to attack the underlying multivariate signature scheme used in the ring signature scheme is at least 2^l against known attacks against MPKC, such attacks including Algebraic Attacks, Linearization Attacks, Rank Attacks, Differential attacks, and so on, then the proposed multivariate ring signature scheme based on MPKCs is unforgeable w.r.t. known attacks for some given security level, say 2^l multiplications on the finite field.

4. Conclusions

In this paper we present a generic multivariate ring signature scheme based on MPKCs, and its security model. Through the security analysis, the scheme satisfies the completeness, anonymity against full key exposure and unforgeability w.r.t. known attack against MPKCs if we suppose that the underlying multivariate signature scheme is unforgeability w.r.t. known attack against MPKCs. Our multivariate ring signature scheme could survive future attacks utilizing quantum computers. Our research results in this work give a new way to build ring signature schemes.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under grants 60873268, 61173192, Research Foundation of Education Department of Shaanxi Province of China under grants 09JK678 and 09JK660. Thanks also go to the anonymous reviewers for their useful comments.

References

[1] R.L. Rivest, A. Shamir, Y. Tauman, How to Leak a Secret, in: Cryptology–Asiacrypt 2001, in: LNCS, vol. 2248, Springer-Verlag, Berlin, 2001, pp. 552–565.
[2] A. Masayuki, O. Miyako, S. Koutarou, L-out-of-n signatures from a variety of keys, in: Cryptology–Asiacrypt 2002, in: LNCS, vol. 2501, Springer-Verlag, Berlin, 2002, pp. 415–432.
[3] J. Xu, Z.F. Zhang, D. Feng, A ring signature scheme using bilinear pairings, in: WISA2004, in: LNCS, vol. 3325, Springer-Verlag, Berlin, 2004, pp. 160–170.
[4] F.G. Zhang, R.S. Naini, W. Susilo, An efficient signature scheme from bilinear pairings and its applications, in: Public Key Cryptography 2004, in: LNCS, vol. 2947, Springer-Verlag, Berlin, 2004, pp. 277–290.
[5] M. Naor, Deniable ring authentication, in: Cryptology-Crypto'02, in: LNCS, vol. 2442, Springer-Verlag, Berlin, 2002, pp. 481–498.
[6] W. Susilo, Y. Mu, Non-interactive deniable ring authentication, in: ICISC 2003, in: LNCS, vol. 2971, Springer-Verlag, Berlin, 2004, pp. 386–401.
[7] J.Q. Lv, X.M. Wang, Verifiable ring signature, in: CANS03, U.S.A, Sep 2003, DMS Proceedings, 2003, pp. 663–665.
[8] J. Herranz, G. Saez, Forking lemmas for ring signature schemes, in: Indocrypt 2003, in: LNCS, vol. 2904, Springer-Verlag, Berlin, 2003, pp. 266–279.
[9] Y. Dodis, A. Kiayias, A. Nicolost, et al., Anonymous identification in ad hoc groups, in: EUROCRYPT'04, in: LNCS, vol. 3027, Springer-Verlag, Berlin, 2004, pp. 609–626.
[10] T. Isshiki, K. Tanaka, An (n-t)-out-of-n threshold ring signature scheme, in: ACISP 2005, in: LNCS, vol. 3574, Springer-Verlag, Berlin, 2005, pp. 406–416.
[11] M.H. Au, J.K. Liu, P.P. Tsang, et al., A suite of ID-based threshold ring signature schemes with different levels of anonymity. http://eprint.iacr.Org/2005/326/.
[12] K.C. Lee, H. Wei, T. Hwang, Convertible ring signature, IEEE Proc. Commun. 152 (2005) 411–414.
[13] J.K. Liu, D.S. Wong, Solutions to key exposure problem in ring signature. http://eprint.iacr.org/2005/427/, 2005-10-25.
[14] A. Bender, J. Katz, R. Morselli, Ring signatures: stronger definitions, and constructions without random oracles, in: TCC 2006, in: LNCS, vol. 3876, Springer-Verlag, Berlin, 2006, pp. 60–79.
[15] E. Fujisaki, K. Suzuki, Traceable ring signature, in: Public Key Cryptography – PKC 2007, in: LNCS, vol. 4450, Springer-Verlag, Berlin, 2007, pp. 181–200.
[16] B. Olivier, M.R. Gilles, Cryptanalysis of the square cryptosystems, in: Advances in Cryptology-ASIACRYPT 2009, vol. 5912, Springer, Berlin, Heidelberg, 2009, pp. 451–468.
[17] 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/, 64 pages, Report 2005/077, 12th of May 2005.
[18] J.T. Ding, D. Schmidt, F. Werner, Algebraic attack on HFE revisited, in: The 11th Information Security Conference, in: LNCS, vol. 5222, Springer-Verlag, Berlin, 2008, pp. 215–227.
[19] M.S. Chen, J. Ding, C.H.O. Chen, F. Werner, B.Y. Yang, Odd-char multivariate hidden field equations. http://eprint.iacr.org/2008/543/, 2008-12-28.
[20] 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, vol. 5473, Springer-Verlag, Berlin, 2009, pp. 252–264.
[21] J. Baena, C. Clough, J.T. Ding, Square–vinegar signature scheme, in: PQCrypto 2008, in: LNCS, vol. 5299, Springer-Verlag, Berlin, 2008, pp. 17–30.
[22] Crystal L. Clough, Square: a new family of multivariate encryption schemes, University of Cincinnati, Cincinnati, 2009, pp. 67–73.
[23] C.L. Clough, J.T. Ding, Secure variants of the square encryption scheme, in: Post-Quantum Cryptography, vol. 6061, Springer-Verlag, Berlin, 2010, pp. 153–164.
[24] M. Garay, D. Johnson, Computers and intractability — a guide to the theory of NP-completeness, W H Freeman and Company, San Francisco, 1979, pp. 250–251.
[25] J. Patarin, L. Goubin, Trapdoor one-way permutations and multivariate polynomials, in: International Conference on Information Security and Cryptology 1997, in: LNCS, vol. 1334, Springer, Berlin, 1999, pp. 356–368.
[26] B.Y. Yang, J.M. Chen, TTS: rank attacks in tame-like multivariate PKCs. http://eprint.iacr.org/2004/061.