A Novel Deniable Ring Authentication based on Multivariate Public-Key Cryptosystem

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

***Abstract*—Deniable ring authentication allows a member of an ad-hoc sunset of participants to authenticate a message without revealing which member has issued the signature, and the verifier cannot transfer the signature to any third party. It is an important cryptographic primitive for privacy and anonymous communication. As far as we know, most of deniable ring authentication signatures 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 Multivariate 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 firstly proposed a construction of deniable ring authentication based on MPKC, which has the properties of consistent, unforgery, signer-anonymity and non-transferable.**

Keywords-deniable ring authentication; privacy; multivariate public-key cryptosystem

I. Introduction

Deniable ring authentication, which merges ring signatures and deniable authentication, was first introduced in [1]. In a deniable ring authentication, it is possible to convince a verifier that a member of an ad-hoc subset of participants is authenticating a message *m* without revealing which member has issued the signature, and the verifier cannot convince any third party that the message *m* was indeed authenticated. It has been found in a number of various applications. To give an example [2], consider a situation when Alice, who is a member of the parliament, wishes to inform the prime minister about very sensitive information related to the country. In this situation, Alice does not want her identity to be revealed by the prime minister, and on the other hand, she also wants the prime minister to keep this information for him and not to be forwarded to any other person. To make the information reliable, it must be authenticated and this must be verifiable by the prime minister that it comes from one of the parliament's member, so that the prime minister can make his decision on this matter. Alice cannot use a standard ring signature, though Alice's identity can be hidden and the message can be identified to come from one of the parliament members without revealing who the actual signer is, the prime minister can quote this message and publish it as an authenticated message that comes from one of the parliament members - something that Alice does not want to happen. Another situation [1] is that where Bob is paying for some authentication (e.g. for checking a piece of software) should he be free to turn and give it away to Charlie?

The primitive introduced in [1] is particular useful in the above situations. However, their scheme requires an interactive zero knowledge protocol, in which an anonymous channel routing is assumed to be used. Further, the message size is longer even compared to a normal ring signature. By removing the interactivity of the protocol, Susio and Mu[2] presented a non-interactive deniable ring authentication scheme, which uses a combination of a ring signature and an chameleon hash function. However, there is a restriction that the verifier has to setup a chameleon hash function before a message can be sent to him/her, which is certainly not practical. Later, they drew on an ID-Based chameleon hash function to construct their scheme [3] in which the only requirement for the verifier is to have his ID published. Notice that the signature size of all the proposed deniable ring authentication schemes is dependent on the ring size, which is inefficient especially when the ring size is large. L.L Wang etc.[4] gave a generic construction for ID-based deniable ring authentication, and also proposed an ID-based deniable ring authentication scheme from bilinear parings, which is proved secure in the random oracle model. We can find that the existing deniable ring authentication schemes are based on traditional Public key cryptosystem, such as RSA, DLP, IDB, etc.

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

Published by Atlantis Press, Paris, France.

[8,9,10] .

Our contributions

In this paper, we firstly proposed a new deniable ring authentication 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 deniable ring authentication and the security analysis. In section 4, we draw our conclusions.

II. Preliminaries

A. 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:

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

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 fo $S\circ F\circ T$ llowing:

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

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

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

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

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

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

B. Deniable Ring Signature Scheme

The notion of *deniable ring authentication* is formalized in [11]. The setup and requirements of a deniable ring authentication scheme is summarized as follows.

Setup: a probabilistic polynomial time algorithm that generates the system parameters.

DeniableSign(m, sk, L,V): is a probabilistic polynomial time algorithm that takes a message $m \in \{0, 1\}^*$ and a list *L* that contains a set of public keys, including the one that corresponds to the secret key, *sk*, and outputs a signature σ, that can only be verified by V. *L* can include several types of public-keys at the same time, such as for RSA and Schnorr in a particular construction. The verifier V cannot convince any other third party about the authenticity of the message because he can always forge the signature by creating the required proof in the verification by himself.

DeniableVerify(m,σ,L): is a deterministic non-interactive polynomialtime algorithm that takes a message *m*, a signature σ and a list of public keys *L*, and outputs either True or *false* meaning accept or reject, respectively.

III. A MPKC-Based deniable ring authentication scheme AND ITS SECURITY ANALYSIS

A. A MPKC-Based deniable ring authentication scheme

In this section, we present our MPKC-Based deniable ring authentication scheme (MDRA). We describe MDRA by providing the description of the following algorithms: Setup, DRA-Sign and DRA-Verify.

Setup: a probabilistic algorithm outputs the system parameters $(k, q, \xi, n, m, H, CHash())$, 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 $H: \{0, 1\}^* \rightarrow k^n$ 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, . . . , t−1. The public key is $PK_i =P_i =S_i\circ F_i\circ T_i$, and the corresponding private key is $SK_i =\{ S_i, F_i, T_i \}$, where P_i: $k^n \rightarrow k^m$ is an invertible map, S_i: $k^m \rightarrow k^n$ and T_i: $k^n \rightarrow k^n$ are two invertible affine linear maps, i = 0, 1, 2, . . . , t−1.

CHash-Gen: Suppose the receiver is B, the public key pairs are PK_B/SK_B. Given a message *m*, choose $r \in k^n$ randomly, and then compute the Chameleon hash functions $h=CHash(m, r, PK_B)=P_B(\mathrm{r})- P_B(H(m))$.

Forge: The Forge algorithm is defined as follows. Forge(*m*, *r*, PK_B, *h*, *m'*) = $r' = T_{\mathrm{B}}^{-1}$ ⍰$\circ F_{\mathrm{B}}^{-1}$ ⍰⍰⍰⍰⍰⍰$\circ S_{\mathrm{B}}^{-1}(P_B(\mathrm{r})- P_B(H(m))+ P_B(H(m')))$.

DRA-Sign: To get a deniable ring signature on a message *m* with respect to the ring R = $(P_0, P_1, . . . , \mathrm{P}_{t-1})$, a signer U_s ($0 \leqslant s\leqslant t-1$) who owns the private key SK_s generates a signature of message *m* as follows.

a) Select a random element r from k^n and compute h= $CHash(m, r, PK_B)= P_B(r)- P_B(H(m))$;

b) Choose an element $u \in k^n$ at random, and compute $c_{s+1(mod\ t)} =H(R, m, h, P_s(u))$;

c) For i =s+1, s+2, . . . , t−1, 0, 1, . . . ,s−1, uniformly pick $k_i \in k^n$, and compute $c_{i+1(mod\ t)} =H(R, m, h, P_i(c_i)+ P_i(k_i))$;

k_s= T_s^{-1} ⍰ $\circ F_s^{-1}$ ⍰⍰⍰⍰⍰⍰ $\circ S_s^{-1}(P_s(u)$- P_s $(c_s))$.

d) The resulting signature is σ = (R, c_0, k_0, k_1, . . . , k_{t-1}, r).

DRA-Verify: To verity a signature (*m*, σ), the receiver performs the following.

a) Compute h=CHash(m, r, PK_B)=P_B (r)- P_B (H(m))

b) Compute $c_{i+1(mod\ t)}$ =H(R, m, h, $P_i(c_i)$+ $P_i(k_i)$) for i = 0, 1, 2, . . . , t−1, and finally checks whether c_t = c_0. If yes, returns 1 and accept it. Otherwise 0 and reject it.

B. Security analyses and efficiency

Theorem 1 MDRA is consistent.

Proof. If the signature σ = (R, c_0, k_0, k_1, . . . , k_{t-1}, *r*) is not altered and P_B is the public key of the receiver, the following equations will hold.

h=CHash(*m*, *r*, PK_B)=P_B (r)- P_B (*H*(*m*))

Hence, in the procedure of DRA-Sign, we have $P_s(u)$=P_s (c_s)+ P_s (k_s), thus $c_{s+1(\mathrm{mod}\ t)}$ =*H*(R, *m*, *h*, $P_s(u)$)= *H*(R, *m*, *h*, P_s (c_s)+ P_s (k_s)), so that $c_{i+1(\mathrm{mod}\ t)}$ =*H*(R, *m*, *h*, $P_i(c_i)$+ $P_i(k_i)$) holds for *i* = 0, 1, . . . ,*t*−1.

Moreover for *i*=*t*-1, we have c_0=*H*(R, *m*, *h*, $P_{t-1}(c_{t-1})$+ $P_{t-1}(k_{t-1})$), and we know that c_t =*H*(R, *m*, *h*, $P_{t-1}(c_{t-1})$+ $P_{t-1}(k_{t-1})$), so it holds that c_t= c_0.

Theorem 2 MDRA is resistant to forgery.

Proof. Since the core of multivariate signature scheme over a finite field should be the selection of the center invertible mapping *F*. Therefore, according to 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 [12,13]. In the DRA-Sign step, those who have no correct secret keys cannot forge the signature.

Theorem 3 MDRA provides signer- anonymity.

Proof. From the distribution of the deniable ring signature *σ =(R, c_0, k_0, k_1, . . . , k_{t-1}, r),* we can find that $k_i \in k^n$ $(i \neq s)$ is randomly selected, and u is randomly selected, as k_s= T_s^{-1} ⍰ $\circ F_s^{-1}$ ⍰⍰⍰⍰⍰⍰ $\circ S_s^{-1}(P_s(u)$- P_s $(c_s))$, so we can conclude that k_s should *b*e regarded as randomly distributed, that is (k_0, k_1, . . . , k_{t-1}) is uniformly distributed. In addition, from the equation c_0=*H(R, m, h, $P_{t-1}(c_{t-1})$+ $P_{t-1}(k_{t-1})$)*,we know that c_0 is randomly distributed in k^m, this is because that k_{t-1} is randomly selected. Meanwhile, *r* is randomly selected, so the ring signature *σ = (R, c_0, k_0, k_1, . . . , k_{t-1}, r)* 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.

Theorem 4 MDRA is non-transferable.

Proof. We notice that our MDRA does not allow the verifier *B* to convince any third party about the fact that *m* is authenticated. This is due to the use of chameleon hash function *CHash*(*m*, *r*, PK_B). The verifier *B* can always use his secret key SK_B and execute the algorithm Forge(*m*, *r*, PK_B, *h*, *m'*) to create a valid pair of (*m'*, *r'*) for $m \neq m'$, that will pass the algorithm DRA-Verify (*m'*, σ) for the same signature σ .

IV. Conclusions

In this paper, we present a generic deniable ring authentication based on MPKC and its security analysis. Our scheme has the properties of consistent, unforgery, signer-anonymity and non-transferable. 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] M. Naor, “Deniable Ring Authentication”, In: proceedings of Advances in Cryptology – Crypto’02. Springer-Verlag, 2002, LNCS 2442, 481–498.

[2] W. Susilo, Y.Mu, “Non-interactive Deniable Ring Authentication”, In: proceedings of ICISC2003. Springer-Verlag, 2004, LNCS 2971, 386–401.

[3] W.Susilo, Y. Mu, “Deniable Ring Authentication Revisited”, In: proceedings of ACNS 2004, Springer-Verlag, 2004, LNCS 3089, 149–163.

[4] L.L. Wang, G.Y. Zhang, C.G. Ma, “ID-based deniable ring authentication with constant-size signature”, Frontiers of Computer Science in China, 2008, 2(1): 106-112.

[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/, Report 2005/077, 12th of May 2005.

[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] Crystal 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] M. Naor, “Deniable Ring Authentication”, Advances in Cryptology - Crypto 2002, LNCS 2442, ,2002, 481–498.

[12] M. Garay, D. Johnson, “Computers and intractability — a guide to the theory of NP-completeness”, W H Freeman and Company, San Francisco, 1979, 250–251.

[13] 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.