Quantum Attack-Resistent Certificateless Multi-Receiver Signcryption Scheme

Article *in* PLoS ONE · June 2013

DOI: 10.1371/journal.pone.0049141 · Source: PubMed

4 authors, including:

Huixian Li
Wayne State University
31 PUBLICATIONS **277** CITATIONS
SEE PROFILE

Liaojun Pang
Wayne State University
58 PUBLICATIONS **623** CITATIONS
SEE PROFILE

OPEN ACCESS Freely available online

PLOS ONE

Quantum Attack-Resistent Certificateless Multi-Receiver Signcryption Scheme

Huixian Li[1,2]*, Xubao Chen[1], Liaojun Pang[3], Weisong Shi[2]

1 School of Computer Science and Engineering, Northwestern Polytechnical University, Xi'an, China, **2** Department of Computer Science, Wayne State University, Detroit, Michigan, United States of America, **3** School of Life Sciences and Technology, Xidian University, Xi'an, China

Abstract

The existing certificateless signcryption schemes were designed mainly based on the traditional public key cryptography, in which the security relies on the hard problems, such as factor decomposition and discrete logarithm. However, these problems will be easily solved by the quantum computing. So the existing certificateless signcryption schemes are vulnerable to the quantum attack. Multivariate public key cryptography (MPKC), which can resist the quantum attack, is one of the alternative solutions to guarantee the security of communications in the post-quantum age. Motivated by these concerns, we proposed a new construction of the certificateless multi-receiver signcryption scheme (CLMSC) based on MPKC. The new scheme inherits the security of MPKC, which can withstand the quantum attack. Multivariate quadratic polynomial operations, which have lower computation complexity than bilinear pairing operations, are employed in signcrypting a message for a certain number of receivers in our scheme. Security analysis shows that our scheme is a secure MPKC-based scheme. We proved its security under the hardness of the Multivariate Quadratic (MQ) problem and its unforgeability under the Isomorphism of Polynomials (IP) assumption in the random oracle model. The analysis results show that our scheme also has the security properties of non-repudiation, perfect forward secrecy, perfect backward secrecy and public verifiability. Compared with the existing schemes in terms of computation complexity and ciphertext length, our scheme is more efficient, which makes it suitable for terminals with low computation capacity like smart cards.

Citation: Li H, Chen X, Pang L, Shi W (2013) Quantum Attack-Resistent Certificateless Multi-Receiver Signcryption Scheme. PLoS ONE 8(6): e49141. doi:10.1371/journal.pone.0049141

Editor: Gerardo Adesso, University of Nottingham, United Kingdom

Received September 12, 2012; **Accepted** March 22, 2013; **Published** June 5, 2013

Funding: This work was supported by Natural Science Foundation of China under Grant Nos. 61103178 and 60803151, and the Research Fund for the Doctoral Program of Higher Education of China under Grant No. 20096102120045. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Competing Interests: The authors have declared that no competing interests exist.

* E-mail: lihuixian@nwpu.edu.cn

Introduction

Signcryption is a cryptographic primitive that provides both signature and encryption simultaneously to sensitive information at a lower computation and communication overhead than the traditional signature-then-encryption approach [1]. In terms of the implementation method, there are two kinds of signcryption schemes. One is based on traditional public key infrastructure [2], which causes the costly certificate management problem; the other is based on identity-based public key cryptography [3], which avoids the certificate management, but induces the key escrow problem.

In 2003, Al-Riyami et al. [4] proposed the certificateless cryptosystem (CLC). In their certificateless cryptosystem, a user's secret key is derived from two parts: one is an identity-based secret key generated by Key Generation Center (KGC) and the other is a self-generated secret key. Thus CLC solves the key escrow problem as well as the certificate management problem, and it also reduces the implementation complexity of the cryptosystem. In 2008, Barbosa et al. [5] first proposed the certificateless signcryption scheme (CLSC) based on bilinear pairing operations. However, they did not give the security proof of their scheme. Since then, certificateless signcryption schemes [6–7] have been studied extensively. In 2010, Li et al. proposed another CLSC [8] and proved its security formally. However, these schemes [5–8] are inefficient in computation because they use the bilinear pairing operation, a quite complex computation. Selvi et al. [9] and Jing et al. [10] constructed an efficient CLSC based on the CDH (Computational Diffie-Hellman) problem without bilinear pairing operations, respectively. At the same time, they proved their schemes' security in the random oracle model. However, their schemes are only single-receiver ones. If there are multiple receivers at the same time, these schemes need to signcrypt the same message for each receiver separately, so they are very inefficient for the multi-receiver scenario. In order to improve the efficiency of signcryption in the multi-receiver setting, Selvi et al. [11] proposed the certificateless multi-receiver signcryption scheme (CLMSC), and this scheme only needs two bilinear pairing operations and $(t+2)$ exponentiation operations (t denotes the number of the receivers) in the signcryption and designcryption phases. However, they found that this scheme cannot resist the forgery attack and then presented an enhanced scheme [12] later. But Miao et al. [13] showed that the enhanced scheme is still insecure against the internal attack and provided a detailed security analysis.

To date, the implementations of almost all certificateless signcryption schemes [5–13] are based on traditional public key cryptosystems, in which the security mainly relies on the hard problems, such as factor decomposition and discrete logarithm. However, in 1994, Shor [14] proposed a polynomial-time

quantum algorithm that can successfully factor large integers, which shows that quantum computing has brought a potential challenge to these hard mathematical problems. Once quantum computers is developed successfully, they will pose a fatal threat to the security of almost all certificateless signcryption schemes which are based on public key cryptosystems such as RSA, ElGamal and ECC. So it is more and more urgent to design a certificateless signcryption scheme that can resist quantum attack. Multivariate public key cryptography (MPKC), which can resist quantum attack, is one of the alternative solutions to guarantee the security of communications in the post-quantum age. The security of MPKC is based on the Multivariate Quadratic (MQ) problem and the Isomorphism of Polynomials (IP) problem. Compared with identity-based cryptography, MPKC has lower calculation complexity and is higher in efficiency, which makes MPKC well suitable to implement strongly secure communications for low-end devices. The MPKC-based schemes have been studied widely, and several excellent schemes have been proposed. For example, SFLASH, a signature scheme based on MPKC, has been recommended by the NESSIE European Consortium since 2003 as the best known solution for implementation on low-cost smart cards [15].

Our contribution. Motivated by these concerns, we employ MPKC to construct an efficient quantum attack-resistent certificateless multi-receiver signcryption scheme, which combines the certificateless cryptosystem and MPKC. The new scheme not only has the advantage of the certificateless cryptosystem, which avoids the problem of key management, but also resists quantum attack only with light-weight computation like the multivariate quadratic polynomial operations. In our scheme, multivariate quadratic polynomial operations, which have lower computation complexity than bilinear pairing operations, are employed in signcrypting a message for a certain number of receivers. Therefore, our scheme is more efficient than the existing CLMSC schemes, and it is suitable for mobile terminals with low computing power. Security analysis shows that our scheme is a secure MPKC-based multi-receiver signcryption scheme, and it also has the important security properties such as message confidentiality, unforgeability, non-repudiation, perfect forward secrecy, perfect backward secrecy and public verifiability.

Preliminaries

1 MQ Problem and IP Problem

In this section, we shall briefly recall some basic concepts of MPKC including multivariate polynomial equations, the MQ problem and the IP problem.

Let G be a finite field of prime order p. Let n be the number of variables, namely, $x_1, x_2, \ldots, x_n$ in the multivariate polynomial equation, g be the number of the multivariate polynomial equations, and d be the degree of the multivariate polynomial equations.

A tuple of multivariate quadratic polynomials consists of a finite ordered set of polynomials of the following form:

$$p_i(x_1,x_2,\ldots,x_n)=\sum_{1\le j\le k\le n} a_{ijk}x_jx_k+\sum_{j=1}^{n} b_{ij}x_j+c_i \qquad (1)$$

where $i=1, 2, \ldots, g$, and $x_j, x_k \in G$, and the coefficients $\{a_{ijk}, b_{ij}, c_i\}$ are over G [16]. Then, the MQ problem can be described as follows:

Definition 1. (MQ). Given a tuple $P=(p_1, p_2, \ldots, p_g)$ of g multivariate quadratic polynomials with n unknowns defined over G, and the image $y=(p_1(z), p_2(z), \ldots, p_g(z))$ of an element z randomly chosen from G^n (G^n denotes the nth extension of G), the problem to find an element x of G^n such that $y=(p_1(x), p_2(x), \ldots, p_g(x))$ is called the MQ problem [16].

Solving a set of randomly chosen quadratic equations with several variables over a finite field is considered as an NP hard problem [17].

Definition 2. (IP). Given P and Q be two public sets of n quadratic equations with n variables over G, if P and Q are isomorphism, then $P=T\circ Q\circ V$ ($\circ$ denotes composition of mappings), where T and V are two invertible affine transformations on $G^n \to G^n$. Finding (T, V) for P, Q such that $P=T\circ Q\circ V$ is called the IP problem [18].

2 Multivariate Public Key Cryptosystem

In a primitive multivariate public key cryptosystem [19], for a user U with identity ID_U, his/her public key is $P_U=T\circ Q\circ V$, and his/her secret key is the 3-tuple $P_U^{-1}=(T,Q,V)$. The encryption operation for a message m is denoted by $\sigma=P_U(m)$ and the corresponding decryption operation for the ciphertext σ is denoted by $m=P_U^{-1}(\sigma)$. For example, Alice wants to send a message m to Bob with identity ID_B. Alice computes the ciphertext $\sigma=P_B(m)=T\circ Q\circ V(m)=T(Q(V(m)))$with Bob's public key. Bob receives the ciphertext σ from Alice and then decrypts the ciphertext σ by computing $P_B^{-1}(\sigma)$. In a word, Bob computes $\sigma_T=T^{-1}(\sigma)$, $\sigma_Q=Q^{-1}(\sigma_T)$and $m=V^{-1}(\sigma_Q)$ sequentially. At last, Bob obtains the plaintext message $m=P_B^{-1}(\sigma)$.

3 Framework of CLMSC

A certificateless multi-receiver signcryption scheme consists of five probabilistic polynomial-time algorithms, namely Setup, Partial Key Extract, Key Extract, Signcrypt and De-signcrypt. According to the features of MPKC, we improve the existing CLMSC model, that is, KGC produces the common partial public key and partial secret key in the phase of Partial Key Extract.

- **Setup**: This algorithm is run by KGC. It takes as input a security parameter s and returns the public parameters *params*.
- **Partial Key Extract**: This algorithm is run by KGC. KGC first chooses a random number w as the system master key. Then it takes as input w and *params* and returns the common partial public key PP_u and partial secret key PS_u.
- **Key Extract**: This algorithm is run by a user U. It takes as input *params*, PP_u, PS_u and an identity ID_u and returns the full public key PK_u and the full secret key SK_u of the user.
- **Signcrypt**: To securely send a message m to a group of receivers $\{\mathrm{ID}_1, \mathrm{ID}_2, \ldots, \mathrm{ID}_t\}$, the sender S should run this algorithm to signcrypt it first. It takes as input *params*, a message m, the sender's identity ID_S, the full keys PK_u and SK_u of the sender, and lists of the receiver identities and their public keys, and returns a ciphertext σ.
- **De-signcrypt**: This algorithm takes as input a ciphertext σ, the receiver's identity ID_i, the receiver's full keys PK_i and SK_i, the identity ID_s and the public key PK_s of the sender, and returns either a plaintext m or an error symbol $\perp$.

4 Security Model for CLMSC

Our security model is established based on Selvi et al.'s security model [11]. For a certificateless signcryption scheme, there are two types of attacks corresponding to two types of attackers, namely A_1 and A_2. In the attack of Type 1, A_1 does not have access to the

system master key, but he/she has the ability to replace the public key of any user with a value that he/she chooses arbitrarily. A_2 has access to the master key, but he/she cannot change public key of any user.

Definition 3. Confidentiality under the attack of Type 1. A certificateless multi-receiver signcryption scheme is Type-1-CCA2 secure if no probabilistic polynomial-time attacker A has a non-negligible advantage in winning the IND-CLMSC-CCA2-1 game [11].

For A, there are the following constraints. A can not have access to the master key w. No Extract Secret Key query is allowed on any of the challenge identities. No De-signcrypt query is allowed on the challenge ciphertext.

Definition 4. Confidentiality under the attack of Type 2. A certificateless multi-receiver signcryption scheme is Type-2-CCA2 secure if no probabilistic polynomial-time attacker A has a non-negligible advantage in winning the IND-CLMSC-CCA2-2 game [11].

For A, there are the following constraints. No Extract Secret Key query is allowed on any of the challenge identities. No Replace Public Key query is allowed on any of the challenge identities. No De-signcrypt query is allowed on the challenge ciphertext.

Definition 5. Unforgeability under the attack of Type 1. A certificateless multi-receiver signcryption scheme is Type-1-sEUF-CMA-1 secure if no probabilistic polynomial-time attacker A has a non-negligible advantage in winning the EUF-CLMSC-CMA-1 game [11].

For A, there are the following constraints. A can not have access to the master key w. No Extract Secret Key query is allowed on any of the challenge identities.

Definition 6. Confidentiality under the attack of Type 2. A certificateless multi-receiver signcryption scheme is Type-2-sEUF-CMA-2 secure if no probabilistic polynomial-time attacker A has a non-negligible advantage in winning the EUF-CLMSC-CMA-2 game [11].

For A, there are the following constraints. No Extract Secret Key query is allowed on any of the challenge identities. No Replace Public Key query is allowed on any of the challenge identities.

Methods

In order to construct our scheme, we employed the Perturbed Matsumoto-Imai-Plus (PMI+) cryptosystem [20], which can resist the linearization attack, rank attacks, and the differential attack and is much faster than RSA and ECC. The new scheme that we proposed consists of five probabilistic polynomial-time algorithms, namely Setup, Partial Key Extract, Key Extract, Signcrypt and De-signcrypt. We shall give a detailed description of the proposed scheme as follows.

Setup. Given a security parameter s as input, KGC returns a big positive integer q and a small positive integer p. Let G be a finite field of order q and characteristic two, and define two non-collision hash functions H_1: $\{0,1\}^* \times \{0,1\}^* \times G^{n+p} \rightarrow G^{n+p}$and H_2: $\{0,1\}^* \times G^n \times G^{n+p} \rightarrow \{0,1\}^{l_m}$, where G^n is the nth extension of G and G^{n+p} is the $(n+p)$th extension of G. The positive integer n is the number of variables in the equation (1) and l_m is the bit length of the message m. Then KGC selects a positive integer g to denote the number of equations. At last, KGC publishes the public parameters *params* denoted by(G,g,n,q,p,H_1,H_2).

Partial Key Extract

1) KGC selects a secure MPKC, which is PMI+ in our scheme. The system public key can be expressed as a typical multivariate quadratic system: $\bar{F} = T \circ F \circ V$ where T is a randomly chosen invertible affine transformation on $G^{n+p} \rightarrow G^{n+p}$, V is a randomly chosen invertible affine transformation on $G^n \rightarrow G^n$, and F is a public set of $(n+p)$ quadratic equations with n variables over G. The system secret key is (T, F, V). The related parameters refer to [20].
2) KGC randomly chooses T_0 and V_0, where T_0 is a randomly chosen invertible affine transformation on$G^{n+p} \rightarrow G^{n+p}$ and V_0 is a randomly chosen invertible affine transformation on $G^n \rightarrow G^n$. Then, compute $\bar{F}_0 = T_0 \circ \bar{F} \circ V_0$. $\bar{F}_0$ is the system partial public key, and $(T_0 \circ T, F, V \circ V_0)$ is the system partial secret key. It is worth noting that KGC needs to compute the new system partial secret key when some user drops out of the group.

Key Extract. Each user runs this algorithm to compute his/her full public and secret keys. The user U randomly chooses T_u and V_u, where T_u is an invertible affine transformation on $G^{n+p} \rightarrow G^{n+p}$and V_u is an invertible affine transformation on $G^n \rightarrow G^n$. Then, compute the public key F_u of user U, that is, $F_u = T_u \circ \bar{F}_0 \circ V_u$, which should be sent to KGC. The secret key of user U is $(T_u \circ T_0 \circ T, F, V \circ V_0 \circ V_u)$.

Signcrypt. Suppose that Alice, whose identity is ID_A, wants to signcrypt a message m to t different receivers denoted by $L = \{\mathrm{ID}_1, \mathrm{ID}_2, \ldots, \mathrm{ID}_t\}$. Alice performs the following steps:

1) Alice chooses $r \in G^n$ randomly, and computes $X = \bar{F}(r), Y = H_1(m, \mathrm{ID}_A, X)$ and $S = F_A^{-1}(Y)$.
2) For all IDi, i = 1, 2, ..., t, compute $W_i = F_i(S \| X)$and$Z = H_2(\mathrm{ID}_A, S, X) \oplus m$.
3) Return ciphertext $\sigma = (S, Y, Z, W_1, W_2, ..., W_t, L)$.

De-signcrypt. Each receiver ID_i, $i = 1, 2, \ldots, t$, uses his/her secret key to decrypt σ.

1) IDi extracts his/her corresponding ciphertext information (S, Y, Z, Wi) according to his/her position in L.
2) IDi computes $Y' = F_A(S)$ and checks whether the equation $Y' = Y$ holds. If it holds, IDi continues to decrypt σ as follows; otherwise, IDi outputs $\perp$.
3) IDi computes$S' \| X' = F_i^{-1}(W_i)$and $m' = Z \oplus H_2(\mathrm{ID}_A, S', X')$.
4) Check whether the equations $S = S'$ and $Y' = H_1(m', \mathrm{ID}_A, X')$ hold. If both of them hold, output $m = m'$; otherwise, output $\perp$.

Discussion

1 Correctness Analysis

Theorem 1. The De-signcrypt algorithm is correct.

Proof. Upon receiving a ciphertext σ, each receiver ID_i, $i = 1, 2, \ldots, t$, extracts his/her own corresponding ciphertext information (S, Y, Z, W_i) from σ. According to the Signcrypt algorithm, we have $S = F_A^{-1}(Y)$, so the receiver ID_i can compute $Y' = F_A(F_A^{-1}(Y')) = F_A(S) = Y$. It is worth noting that only the sender, Alice, can generate the correct Y such that $Y' = Y$ because only she knows her secret keyF_A^{-1}. The receiver, ID_i, can decrypt the ciphertext by computing $F_i^{-1}(W_i) = F_i^{-1}(F_i(S' \| X')) = S' \| X'$ and $m' = Z \oplus H_2(\mathrm{ID}_A, S', X')$. ID_i can judge whether m' is correct by checking whether $S = S'$ and $Y' = H_1(m', \mathrm{ID}_A, X')$ hold. Note

that only ID_i can obtain $m' = Z \oplus H_2(ID_A, S', X')$correctly because only he/she knows his/her secret key F_i^{-1}. Therefore, the Designcrypt algorithm of our scheme is correct.

2 Security Analysis

2.1 Security of MPKC. In the last twenty years, many MPKC schemes were proposed, and they are mainly based on four basic MPKC schemes including the Matsumoto Imai (MI) cryptosystem, the Hidden Field Equation (HFE) cryptosystem, the Oil Vinegar (OV) cryptosystem and the Stepwise Triangular System [20]. Although most of them have been broken, some variants of the basic MPKC schemes, such as Rainbow and PMI+ [20], have survived known attacks like the linearization equation attack, the rank attack and the differential attack. In 2011, Hashimoto et al. [21] proposed two types of fault attacks which further weaken the security of the MPKC schemes. They detailed the fault attack on the MPKC schemes such as UOV, Rainbow, TTS and HFE, and most of the MPKC schemes were proven insecure. However, the PMI+ cryptosystem is one of the few approved cryptosystems which survived the linearization equation attack, the rank attack, the differential attack and even the fault attacks. PMI+ uses the Plus (+) method of external perturbation to prevent attacks without significantly decreasing the efficiency of the system [20]. So in our work, we used PMI+ which is based on the IP problem to construct our scheme.

Cryptosystems based on the IP problem belong to a major category of MPKC. Faugère et al. [22] gave an upper bound on the theoretical complexity of the "IP-like" problem, and presented a new algorithm to solve the IP problem when S and T are linear mappings. Bouillaguet et al. [23] proposed an improved algorithm combining the linear algebra techniques, together with Gröbner bases and statistical tools. To date, the best algorithm for the IP problem is exponential. For the IP problem used in our scheme, the attacking complexity of the best algorithm will be $O(n^{3.5} \cdot q^{n/2})$ [24], where n is the number of variables and q is the cardinality of the finite field. So the IP problem will be computationally hard if we can choose the parameter properly.

With the knowledge of the most efficient attacks on the IP problem, in order to strengthen the security of our scheme, we suggest that the parameters of our scheme should satisfy the following conditions: the transformations T and V should be affine; the polynomials in P and Q should be homogeneous. In our method, for example, if we choose $n = 16$ and $q = 2^9$, the attacking complexity should be greater than $O(n^{3.5} \cdot q^{n/2}) = 16^{3.5} \bullet (2^9)^{16/2} = 2^{86}$. Usually, it is considered to be a computationally secure MPKC scheme if the attacking complexity is greater than 2^{80} [24]. Therefore, our scheme is a secure MPKC-based scheme.

Although we used PMI+ for the construction of the proposed multi-receiver signcryption scheme, there are still some other multivariate cryptosystems suitable for the construction of our scheme, such as the internally perturbed HFE cryptosystem (IPHFE) [25]. Different from PMI+, IPHFE is build by using the idea of internal perturbation. Vivien et al. [26,27] and Ding et al. [28,29] analyzed the security of IPHFE, and their work showed that IPHFE with appropriate parameters can withstand all known attacks. So IPHFE can be substituted for PMI+ in our construction. Due to space limitations, we do not introduce the detailed realization of the construction based on IPHFE.

2.2 Message Confidentiality. Theorem 2. Confidentiality under the attack of Type 1. In the random oracle model, if an IND-CLMSC-CCA2-1 adversary A has a non-negligible advantage ε against the security of our scheme when performing q_{H_i} queries to random oracles H_i ($i = 1, 2$), q_{ske} Extract Secret Key queries, q_{pke} Extract Public Key queries, q_{pkr} Replace Public Key queries, q_{sc} Signcrypt queries and q_{dsc} Designcrypt queries, then there exists an algorithm C that can solve the MQ problem with advantage defined as:

$$\varepsilon' > \frac{\varepsilon}{t \cdot q_{sc} + q_{H_1}} \left(1 - \frac{q_{sc} \cdot (t \cdot q_{sc} + q_{H_2})}{2^{G_2}}\right)\left(1 - \frac{q_{dsc}}{2^{G_2 - 1}}\right) \qquad (2)$$

where t is the number of receivers in the challenge set and G_2 denotes the bit length of the element over G^n.

Proof. We show how to build an algorithm C that solves the MQ problem with the help of an adversary A. Let C receive a random instance $\{f(x), Y_0 = f(X_0)\}$ of the MQ problem, and the goal of C is to compute X_0. To solve this problem, C acts as A's challenger in the IND-CLMSC-CCA2-1 game.

Setup. C sets $\bar{F} = T \circ F \circ V$ as the system public key, chooses an invertible affine transformation T_0 on $G^{n+p} \to G^{n+p}$, and chooses an invertible affine transformation V_0 on $G^n \to G^n$ randomly. So the system partial secret key is $(T_0 \circ T, F, V \circ V_0)$, and the partial public key is $\bar{F}_0 = T_0 \circ \bar{F} \circ V_0$. C sends the system parameters $(G, g, n, q, p, H_1, H_2)$, the system public key and the system partial secret key to A. Then A outputs a set of target identities, denoted by $L^* = \{ID_1^*, ID_2^*, \ldots, ID_t^*\}$. To handle A's queries, C maintains a list L_i for each H_i ($i = 1, 2$) query.

Phase1. C simulates A's queries as follows:

***H_1* queries.** A can perform an H_1 query on the input of (m, ID_i, X, L) and then C checks the list L_1. If an entry corresponding to (m, ID_i, X, L) is present in L_1, then C retrieves the hash value h_i from L_1 and returns h_i. Otherwise, it returns a random number $h_i \in G^{n+p}$ and stores the entry (h_i, m, ID_i, X, L, ∇, Δ) in L_1, where the symbols ∇ and Δ denote the signature information and the encryption information of the message m, respectively.

***H_2* queries.** A can perform an H_2 query on the input of (ID_s, S, X) for ID_i and then C checks the list L_2. If an entry corresponding to ID_i is present in L_2, then C retrieves Z_i from L_2 and returns Z_i. Otherwise, it returns a random number Z_i and stores the entry (Z_i, ID_s, S, X, ID_i, Λ, $\square$, $\diamond$, $b_i = 0$) in L_2, where the symbols Λ, $\square$ and $\diamond$ denote the public key F_i, the secret parameters T_i and V_i, respectively. The bit b_i is a flag bit used to denote whether the public keys have been replaced or not.

Extract Secret Key queries. A can perform an Extract Secret Key query on the input of ID_i. C first checks whether $ID_i = ID_j^*, j \in \{1,2,\ldots,t\}$ holds. If $ID_i = ID_j^*, j \in \{1,2,\ldots,t\}$holds, then C aborts the query. Otherwise, C retrieves the entry (Z_i, ID_s, S, X, ID_i, F_i, T_i, V_i, $b_i = 0$) from L_2. If $b_i = 0$, then C returns the secret key $(T_i \circ T_0 \circ T, F, V \circ V_0 \circ V_i)$; otherwise, the public key of the identity ID_i has been replaced and in this case, C asks A for the new secret parameters (T_i, V_i), computes the new secret key $(T_i \circ T_0 \circ T, F, V \circ V_0 \circ V_i)$ and returns it to A.

Extract Public Key queries. A can perform an Extract Public Key query on the input of ID_i and then C checks L_2. If an entry corresponding to ID_i is present in L_2, then C retrieves F_i from L_2 and returns F_i. Otherwise, C chooses $T_i \in_R G^{n+p}, V_i \in_R G^n$, returns the public key $F_i = T_i \circ \bar{F}_0 \circ V_i$ and updates the entry corresponding to ID_i in L_2 with T_i, V_i and F_i.

Replace Public Key queries. When A performs a Replace Public Key query on the input of (ID_i, F_i'), C searches the corresponding entry $(\cdot, ID_i, \cdot)$ in L_2. If the entry is found, then C replaces the public key in the entry corresponding to ID_i in L_2 with F'_i and sets the flag bit b_i to 1. Otherwise, C generates the public key using the Extract Public Key query and then replaces the public key of ID_i with F'_i.

Signcrypt queries. A can perform a Signcrypt query on the input of (m, ID_s, $L = \{ID_{R1}, ID_{R2}, \ldots, ID_{Rt}\}$). If $ID_s = ID_{Ri}$,

$i \in \{1,2,...,t\}$, or if $ID_s \in L^*$ and at least one $ID_{Ri} \in L^*, i \in \{1,2,...,t\}$, then C aborts the query. Otherwise, C knows the secret key of the sender and performs the computations as the signcryption algorithm to return the ciphertext $\sigma = (S, Y, Z, W_1, W_2, ..., W_t, L)$. If $ID_s = ID_j^*, j \in \{1,2,...,t\}$, C does not know the secret key of the sender and in this case, it generates the ciphertext as follows:

First, C retrieves the entry $(\cdot, ID_s, F_s, T_s, V_s, b_s)$ from L_2 and chooses $r \in_R G^n$ and $Z_s \in_R \{0,1\}^{l_m}$. C computes $X = \bar{F}(r)$, extracts $Y = h_s$ by calling the oracle H_1 with the input (m, ID_S, X, L) and computes the signature S. Then, C retrieves the corresponding entry $(\cdot, ID_{Ri}, \cdot, b_{Ri})$ in L_2 and then computes $W_i = F_i(S \| X)$ and $\mathcal{Z} = Z_s \oplus m$. C updates the corresponding entry in L_1. Note that if $b_i = 1$, then the public key of the receiver has been replaced and in this case, the challenger asks A for (T_i, V_i) and uses it in place of the old value stored in the entry. Finally, add $(Z_s, ID_s, S, X, ID_{Ri}, F_i, T_i, V_i, b_i)$ in L_2 (C fails if H_2 is already defined on any of such entries, but this happens only with probability $\frac{t \cdot q_{sc} + q_{H_2}}{2^{G_2}}$). At last, C sends $\sigma = (S, Y, Z, W_1, W_2, ..., W_t, L)$ to A.

Designcrypt queries. When A submits a ciphertext $\sigma = (S, Y, Z, W_1, W_2, ..., W_t, L)$, a receiver's identity ID_R and a sender's identity ID_s, C extracts $(S, Y, \mathcal{Z}, W_i, L)$ from σ. If $ID_R \notin L^*$, then C knows the secret key of ID_R and hence designcrypts σ using the De-signcrypt Algorithm. Otherwise, C searches all entries $(Y, \cdot, ID_s, \cdot, L, \cdot, \mathcal{Z})$ in L_1, and if no such entries exist, the symbol $\perp$ is returned to indicate that the ciphertext is invalid. Meanwhile, C searches the entry $(\mathcal{Z}, ID_s, S, X, ID_s, F_s, T_s, V_s, b_s)$ in L_2, and if it is not found, C rejects the ciphertext σ. If the ciphertext σ passes the above verification, C computes $Y' = F_s(S), S' \| X' = F_i^{-1}(W_i)$, and $m' = Z \oplus H_2(ID_s, S', X')$. If $Y' = Y$ and $S' = S$ hold, and (m', X') passes the verification, then C returns m; otherwise, C rejects σ. Note that a valid ciphertext is rejected with probability at most $\frac{q_{dsc}}{2^{G_2 - 1}}$.

Challenge. A outputs two messages m_0 and m_1 together with an arbitrary sender's identity $ID_s \notin L^*$ on which A wishes to be challenged. C selects a bit $b \in_R \{0,1\}$ and sends m_b to the t target identities denoted by $L^* = \{ID_1^*, ID_2^*, ..., ID_t^*\}$. C chooses $X^* \in_R G^{n+p}, S^* \in_R G^n$ and $Z_s \in_R \{0,1\}^{l_m}$, sets $X_0 = X^* \| S^*$ and then computes $Y^* = F_s(S^*), W_i^* = F_i(X_0)$ and $Z^* = Z_s \oplus m_b$. Then, C responds with the ciphertext $\sigma^* = < Y^*, S^*, Z^*, W_1^*, W_2^*, ..., W_t^*, L^* >$.

Phase2. A performs new queries as in Phase 1. However, A is not allowed to ask Designcrypt queries on σ^* for $ID_i^*, i = 1,2,...,t$.

Guess. At the end of the game, A returns his/her guess result. C ignores the answer to A's guess. According to the above discussion, we know that as long as the simulation of the attacker's environment is perfect, the probability that A asks the value of $W_i = F_i(X^* \| S^*)$, $i = 1, 2, \ldots, t$, by the H_1 oracle is the same as the probability in a real attack. C fetches a random entry $(h_i, m, ID_i, X, L, S, W_i)$ from L_1. With probability $\frac{1}{t \cdot q_{sc} + q_{H_1}}$ (as L_1 contains no more than $t \cdot q_{sc} + q_{H_1}$ elements by our construction), the chosen entry contains the right element $W_i = F_i(X^* \| S^*)$. C returns X_0 as a solution to the MQ problem.

Now, we analyze the probability of C's success. Let E be the event that A outputs the correct bit $b^* = b$.

Simulation fails if any of the following events occurs:

E_1: Extract Secret Key query is executed for some chosen challenge identity.

E_2: Both the sender and at least one of receivers belong to the challenge set in some Signcrypt query.

E_3: The H_2 oracle collides in Signcrypt queries.

E_4: C rejects a valid ciphertext in some Designcrypt query.

According to the above discussion, we know that $Pr[E] = \varepsilon$, where E implies that E_1 *and* E_2 never occur, that is, $\neg E_1 \wedge \neg E_2$. Also, we have $Pr[E_3] \leq \frac{q_{sc} \cdot (t \cdot q_{sc} + q_{H_2})}{2^{G_2}}$ since A conducts a total of q_{sc} Signcrypt queries and there are at most $t \cdot q_{sc} + q_{H_2}$ entries in L_2. $Pr[E_4] \leq \frac{q_{dsc}}{2^{G_2 - 1}}$ represents the probability of rejection of valid ciphertexts.

The event E_5 implies that C chooses the correct entry from L_1 in the Guess Phase. And we know that $Pr[E_5] \leq \frac{1}{t \cdot q_{sc} + q_{H_1}}$. So, the advantage ε' of C is defined as:

$$\varepsilon' = Pr[E \wedge \neg E_1 \wedge \neg E_2 \wedge \neg E_3 \wedge \neg E_4 \wedge E_5] \tag{3}$$

Therefore, we obtain

$$\varepsilon' > \frac{\varepsilon}{t \cdot q_{sc} + q_{H_1}} \left(1 - \frac{q_{sc} \cdot (t \cdot q_{sc} + q_{H_2})}{2^{G_2}}\right)\left(1 - \frac{q_{dsc}}{2^{G_2 - 1}}\right) \tag{4}$$

Theorem 3. Confidentiality under the attack of Type 2. In the random oracle model, if an IND-CLMSC-CCA2-2 adversary A has a non-negligible advantage ε against the security of our scheme when performing q_{H_i} queries to random oracles H_i ($i = 1, 2$), q_{ske} Extract Secret Key queries, q_{pke} Extract Public Key queries, q_{sc} Signcrypt queries and q_{dsc} Designcrypt queries, then there exists an algorithm C that can solve the MQ problem with an advantage ε' defined as:

$$\varepsilon' > \frac{\varepsilon}{t \cdot q_{sc} + q_{H_1}} \left(1 - \frac{q_{sc} \cdot (t \cdot q_{sc} + q_{H_2})}{2^{G_2}}\right)\left(1 - \frac{q_{dsc}}{2^{G_2 - 1}}\right) \tag{5}$$

where t is the number of receivers in the challenge set and G_2 denotes the bit length of the element over G^n.

The attacker has access to the master key, but cannot perform public key replacement under the attack of Type 2. The proof is similar to that of Theorem 2.

2.3 Unforgeability. Theorem 4. Unforgeability under the attack of Type 1. In the random oracle model, if an SUF-CLMSC-CMA-1 adversary A has a non-negligible advantage ε against the security of our scheme when performing q_{H_i} queries to random oracles H_i ($i = 1, 2$), q_{ske} Extract Secret Key queries, q_{pke} Extract Public Key queries, q_{pkr} Replace Public Key queries, q_{sc} Signcrypt queries and q_{ver} Verify queries, then there exists an algorithm C that can solve the IP problem with an advantage ε' defined as:

$$\varepsilon' > \frac{\varepsilon}{t(t \cdot q_{sc} + q_{H_2})} \left(1 - \frac{q_{sc} \cdot (t \cdot q_{sc} + q_{H_2})}{2^{G_2}}\right)\left(1 - \frac{q_{dsc}}{2^{G_2 - 1}}\right). \tag{6}$$

where t is the number of receivers in the challenge set and G_2 denotes the bit length of the element over G^n.

Proof. We show how to build an algorithm C that solves the IP problem with the help of an adversary A. Let C receive a random instance $(F_s = T_s \circ \bar{F}_0 \circ V_s, \bar{F}_0)$ of the IP problem, and the goal of C is to compute (T_s, V_s). To solve this problem, C acts as A's challenger in the SUF-CLMSC-CMA-1 game.

Setup. C sets $\bar{F} = T \circ F \circ V$ as the system public key, and chooses an invertible affine transformation T_0 on $G^{n+p} \to G^{n+p}$ and an invertible affine transformation V_0 on $G^n \to G^n$ randomly.

So the system partial secret key is $(T_0 \circ T, F, V \circ V_0)$, and the partial public key is $\bar{F}_0 = T_0 \circ \bar{F} \circ V_0$. C sends the system parameters $(G, g, n, q, p, H_1, H_2)$, the system public key and the system partial secret key to A. Then A outputs a set of target identities, denoted by $L^* = \{ID_1^*, ID_2^*, ..., ID_t^*\}$. To handle A's queries, C maintains a list L_i for each H_i ($i = 1, 2$) query.

Attack. C simulates A's queries as follows:

***H_1* queries.** A can perform an H_1 query on the input of (m, ID_i, X, L) and then C checks the list L_1. If an entry corresponding to (m, ID_i, X, L) is present in L_1, then C retrieves h_i from L_1 and returns h_i. Otherwise, it returns a random number $h_i \in G^{n+p}$ and stores the entry (h_i, m, ID_i, X, L, ∇, Δ) in L_1, where the symbols ∇ and Δ denote the signature information and the encryption information for message m, respectively.

***H_2* queries.** A can perform an H_2 query on the input of (ID_s, S, X) for ID_i and then C checks the L_2. If an entry corresponding to ID_i is present in L_2, then C retrieves Z_i from L_2 and returns Z_i. Otherwise, it returns a random number Z_i and stores the entry (Z_i, ID_s, S, X, ID_i, Λ, $\square$, $\diamond$, $b_i = 0$) in L_2, where the symbols Λ, $\square$ and $\diamond$ denote the public key F_i, the secret parameters T_i and V_i, respectively. The bit b_i is a flag bit used to denote whether the public keys have been replaced or not.

Extract Secret Key queries. A can perform an Extract Secret Key query on the input of ID_i, and C first checks whether $ID_i = ID_j^*, j \in \{1,2,...,t\}$ holds. If $ID_i = ID_j^*, j \in \{1,2,...,t\}$ holds, then C aborts the query. Otherwise, C retrieves the entry (Z_i, ID_s, S, X, ID_i, F_i, T_i, V_i, $b_i = 0$) from L_2. If $b_i = 0$, then C returns the secret key $(T_i \circ T_0 \circ T, F, V \circ V_0 \circ V_i)$. Otherwise, the public key of the identity ID_i has been replaced and in this case, C asks A for the new secret parameters (T_i, V_i), computes the new secret key $(T_i \circ T_0 \circ T, F, V \circ V_0 \circ V_i)$ and returns it to A.

Extract Public Key queries. A can perform an Extract Public Key query on the input of ID_i and then C checks L_2. If an entry corresponding to ID_i is present in L_2, then C retrieves F_i from L_2 and returns F_i. Otherwise C chooses $T_i \in_R G^{n+p}$ and $V_i \in_R G^n$, returns the public key $F_i = T_i \circ \bar{F}_0 \circ V_i$ and updates the entry corresponding to ID_i in L_2 with T_i, V_i and F_i.

Replace Public Key queries. When A performs a Replace Public Key query on the input of (ID_i, F'_i), C searches the corresponding entry $(\cdot, ID_i, \cdot)$ in L_2. If the entry is found, then C replaces the public keys in the entry corresponding to ID_i in L_2 with F'_i and sets the flag bit b_i to 1. Otherwise, C generates the public key using Extract Public Key query and then replaces the public key of ID_i with F'_i.

Signcrypt queries. A can performs a Signcrypt query on the input of (m, ID_s, $L = \{ID_{R1}, ID_{R2}, \ldots, ID_{Rt}\}$). If $ID_s = ID_{Ri}, i \in \{1,2,...,t\}$, or if $ID_s \in L^*$ and at least one $ID_{Ri} \in L^*, i \in \{1,2,....,n\}$, then C aborts the query. If $ID_s \neq ID_j^*, j \in \{1,2,...,t\}$, then C knows the secret key of the sender and performs the computations as the Signcrypt algorithm to return the ciphertext $\sigma = (S, Y, Z, W_1, W_2, ..., W_t, L)$. If $ID_s = ID_j^*, j \in \{1,2,...,t\}$, C does not know the secret key of the sender and hence it generates the ciphertext as follows:

First, C retrieves the entry ($\cdot$, ID_s, F_s, T_s, V_s, b_s) from L_2 and chooses $r \in_R G^n$ and $Z_s \in_R \{0,1\}^{l_m}$. C computes $X = \bar{F}(r)$, extracts $Y = h_s$ by calling the oracle H_1 with the input (m, ID_s, X, L) and computes the signature S. Then, C retrieves the corresponding entry $(\cdot, ID_{Ri}, \cdot, b_{Ri})$ in L_2 and then computes $W_i = F_i(S \| X)$ and $Z = Z_s \oplus m$. C updates the corresponding entry in L_1. Note that if $b_i = 1$, then the public key of the receiver has been replaced and in this case, the challenger asks A for (T_i, V_i) and uses it in place of the old value stored in the entry. Finally, add $(Z_s, ID_s, S, X, ID_{Ri}, F_i, T_i, V_i, b_i)$ in L_2 (C fails if H_2 is already defined on any of such entries, but this happens only with probability $\frac{t \cdot q_{sc} + q_{H_2}}{2^{G_2}}$). At last, C sends $\sigma = (S, Y, Z, W_1, W_2, ..., W_t, L)$ to A.

Verify queries. When A submits a ciphertext $\sigma = (S, Y, Z, W_1, W_2, ..., W_t, L)$, a receiver's identity ID_R and a sender's identity ID_s, C extracts (S, Y, Z, W_i, L) from σ. If $ID_R \notin L^*$, then C knows the secret key of ID_R and hence designcrypts σ using the De-signcrypt Algorithm. Otherwise, C searches all entries (Y, $\cdot$, ID_s, $\cdot$, L, $\cdot$, Z) in L_1, and if no such entries exist, the symbol $\perp$ is returned to indicate that the ciphertext is invalid. Meanwhile, C searches the entry (Z, ID_s, S, X, ID_s, F_s, T_s, V_s, b_s) in L_2, and if it is not found, C rejects the ciphertext σ. If the ciphertext σ passes the above verification, C computes $Y' = F_s(S), S' \| X' = F_i^{-1}(W_i)$ and $m' = Z \oplus H_2(ID_s, S', X')$. If $Y' = Y$ and $S' = S$hold, and (m', X') passes the verification test, then C accepts σ; otherwise, C rejects σ. Note that a valid ciphertext is rejected with probability at most $\frac{q_{dsc}}{2^{G_2 - 1}}$.

Forge. After a polynomial-bounded number of queries, the adversary A outputs forged ciphertext $\sigma = <S, Y, Z, W_1, W_2, ..., W_t, L>$ (a receiver list $L = \{ID_{R1}, ID_{R2}, \ldots, ID_{Rt}\}$, and at least one $ID_{Ri} \notin L^*$) and the sender's identity $ID_s \in L^*$.

According to the above discussion, we know that as long as the simulation of the attacker's environment is perfect, the probability that A asks the value of (T_s, V_s) by the H_2 oracle is the same as the probability in a real attack. C fetches a random entry (Z_i, ID_s, S, X, ID_i, F_i, T_i, V_i, b_i) from L_2. With probability $\frac{1}{t(t \cdot q_{sc} + q_{H_2})}$ (as L_2 contains no more than $t \cdot q_{sc} + q_{H_2}$ elements by our construction, and C chooses ID_s with probability $1/t$), the chosen entry contains the right element (T_s, V_s). C returns (T_s, V_s) as the solution to the IP problem.

Now, we analyze the probability of C's success. Let E be the event that the forged ciphertext passes verifications.

Simulation fails if any of the following events occurs:

E_1: Extract Secret Key query is executed for some chosen challenge identity.

E_2: Both sender and at least one of receivers belong to the challenge set in some Signcrypt query.

E_3: The H_2 oracle collides in Signcrypt queries.

E_4: C rejects a valid ciphertext in Verify queries.

According to the above discussion, we know that $Pr[E] = \varepsilon$, where E implies that E_1 and E_2 never occur, that is, $\neg E_1 \wedge \neg E_2$. Also, we have $Pr[E_3] \leq \frac{q_{sc} \cdot (t \cdot q_{sc} + q_{H_2})}{2^{G_2}}$, since A conducts a total of q_{sc} Signcrypt queries and there are at most $t \cdot q_{sc} + q_{H_2}$ entries in L_2. $Pr[E_4] \leq \frac{q_{dsc}}{2^{G_2 - 1}}$ represents the probability of rejection of valid ciphertexts.

The event E_5 implies that C chooses the correct entry from L_2 in the last Verify Phase. And we know that $Pr[E_5] \leq \frac{1}{t(t \cdot q_{sc} + q_{H_2})}$. So, the advantage ε' of C is defined as:

$$\varepsilon' = Pr[E \wedge \neg E_1 \wedge \neg E_2 \wedge \neg E_3 \wedge \neg E_4 \wedge E_5] \quad (7)$$

Therefore, we obtain

$$\varepsilon' > \frac{\varepsilon}{t(t \cdot q_{sc} + q_{H_2})} \left(1 - \frac{q_{sc} \cdot (t \cdot q_{sc} + q_{H_2})}{2^{G_2}}\right) \left(1 - \frac{q_{dsc}}{2^{G_2 - 1}}\right) \quad (8)$$

Theorem 5. Unforgeability under the attack of Type 2. In the random oracle model, if an SUF-CLMSC-CMA-2 adversary A has a non-negligible advantage ε against the security of our scheme when performing q_{H_i} queries to random oracles H_i ($i = 1, 2$), q_{ske} Extract Secret Key queries, q_{pke} Extract Public Key queries, q_{sc} Signcrypt queries and q_{ver} Verify queries, then there exists an algorithm C that can solve the IP problem with an advantage ε' defined as:

$$\varepsilon' > \frac{\varepsilon}{t(t\cdot q_{sc}+q_{H_2})}(1-\frac{q_{sc}\cdot(t\cdot q_{sc}+q_{H_2})}{2^{G_2}})(1-\frac{q_{dsc}}{2^{G_2-1}}) \quad (9)$$

where t is the number of receivers in the challenge set and G_2 denotes the bit length of the element over G^n.

The attacker has access to the master key, but cannot perform public key replacement under the attack of Type 2. The proof is similar to that of Theorem 4.

2.4 Backward Secrecy. Each time Alice sends a message m to receivers, she chooses $r \in G^n$ randomly as the session key. Even though she sends the same message m, the corresponding ciphertext σ will be different in different sessions. So the new receiver who joins the group later does not have the previous value $X = \bar{F}(r)$ which is computed for the message m, and thus he/she can not obtain the previous message m. Therefore, our scheme is backward secure.

2.5 Forward Secrecy. Forward secrecy means that the members who have quitted the group are not able to know the later session keys. In our scheme, the session key r is randomly chosen in each session. When some member of the group quits the group, the sender will compute the partial key for the rest members again, which guarantees that the members who have quitted the group cannot obtain the plaintext message from the later ciphertext. So our scheme is forward secure.

2.6 Non-repudiation. According to Theorem 4 and Theorem 5, our scheme is unforgeable. Suppose that Alice signcrypts a message m. If others want to repudiate her signature S, they have to solve the MQ problem to get the secret key of Alice, and it is computationally infeasible because the MQ problem is an NP-hard problem. Therefore, only Alice knows her secret key and others can not repudiate her behavior of signcrypting the message m. So our scheme is non-repudiation.

2.7 Public Verifiability. The proposed scheme provides public verifiability of ciphertext source, which is an important requirement in broadcast communications. Any third party can be convinced of the sender of the ciphertext σ by recovering Y' in the second step of the de-signcryption phase and checking whether the equation $Y' = Y$ holds. This is in fact due to the unforgeability of the signature. This verification procedure does not involve the knowledge of messages or the receiver's secret key but only the ciphertext σ. Hence, our scheme supports public verifiability.

3 Performance Comparison

In this section, we shall compare our scheme with the existing schemes [8–10,12] in performance. We mainly consider the computation and communication cost.

The proposed scheme does not involve any bilinear pairing operations, exponentiation operations and multiplications in groups. In the signcryption phase, it needs only two hash operations, (t+2) MQ-mapping (it means the mapping operation on the multivariate quadratic equations) operations and one XOR operation, while in the de-signcryption phase, it needs two hash operations, two MQ-mapping operations and one XOR operation. The MQ-mapping operations are linear operations and have much lower computation complexity than bilinear pairing operations and exponentiation operations. According to the above analysis, the computation complexity of our scheme is $O(t+4)$. The ciphertext of our scheme is $(t+1)G_1+(t+1)G_2+|m|$ bits in length, where t is the number of receivers, G_2 is the bit length of the element over G^n, and G_1 is the bit length of the element over G^{n+p}. Compared with the representative CLMSC scheme [12], the new scheme has lower computation complexity without bilinear pairing operation needed. We also compare our scheme with the naive extension of schemes [8–10] for multi-receiver setting in Table 1, in which par denotes pairing operation, exp denotes exponentiation operation and ciphertext-size denotes the bit length of the ciphertext. The comparisons are summarized in Table 1.

According to the above analyses, the proposed scheme is more efficient than the existing ones, and it is also provably secure in the random oracle model. The proposed scheme is a very useful tool in multicast communication. With the rapid development of wireless networks, it is particularly important to transfer instruction data from the control center to multiple intelligent terminals securely [30]. The control center needs to encrypt the sensitive information to prevent it from being eavesdropped and cracked before sending it to intelligent terminals, while intelligent terminals need to judge whether the received instruction is from the trusted entity. To solve this security problem, we must take both the security requirements and the performance of the intelligent terminals into account, because intelligent terminals are generally characterized by low power consumption, low computing power and narrow communication bandwidth, which make the traditional identity-based scheme not suitable for them. Through the analyses about the security and performance of our scheme, it can be concluded that our scheme can better address these issues and it is in line with the characteristics of intelligent terminals.

Conclusions

As one of the alternative cryptosystems, multivariate public key cryptography can resist quantum attack, and has been researched by scholars extensively. In this paper, we employ multivariate public key cryptography to propose a new construction of the certificateless multi-receiver signcryption scheme, called a quantum attack-resistent certificateless multi-receiver signcryption scheme. The new scheme inherits the security of multi-variable cryptosystems that could resist quantum attack, and it avoids the certificate management and the key escrow problem. We proved its security under the hardness of the MQ problem and its unforgeability under the IP assumption in the random oracle model. In addition, the scheme also has security properties such as forward secrecy, backward secrecy, non-repudiation and public

Table 1. Comparison of our scheme and the existing ones.

scheme	MQ-mapping	par	exp	hash	ciphertext-size
Li et al.'s [8]	0	2	t+1	2t+2	2$t\|l\|+t\|m\|$
Selvi et al.'s [9]	0	0	5t+7	3t+3	2$t\|Z_q\|$+2$\|l\|$+ $t\|m\|$
Jing et al.'s [10]	0	0	3t+2	2t+2	2$t\|l\|+t\|m\|$
Selvi et al.'s [12]	0	2	2t+2	t+7	(2t+1)$\|Z_q\|+\|l\|$
Ours	t+4	0	0	4	$(t+1)G_1+(t+1)G_2+\|m\|$

t denotes the number of receivers, $|Z_q|$ denotes the bit length of elements in finite field Z_q, $|l|$ denotes the bit length of elements in group l, $|m|$ denotes the bit length of message m, G_1 denotes the bit length of elements in G^{n+p}, G_2 denotes the bit length of elements in G^n.

doi:10.1371/journal.pone.0049141.t001

verifiability. Analyses show that the proposed scheme is more efficient than the existing ones. Although our scheme is constructed by using PMI+, there are still some other multivariate cryptosystems like IPHFE suitable for our construction. In the future work, we will construct the multi-receiver signcryption scheme by using IPHFE or other better multivariate cryptosystem, and compare the performance of the new scheme with that of the scheme proposed in this paper.

Author Contributions

Analyzed the data: HL XC LP WS. Wrote the paper: HL XC LP WS. Conceived and designed the scheme: HL XC. Proved the security of the scheme: HL XC.

References

1. Zheng Y (1997) Digital signcryption or how to achieve cost (signature & encryption)<<cost (signature)+cost (encryption). In: Proc. 17th Annual International Cryptology Conference on Advances in Cryptology. 165–179.
2. Luo M, Wen Y, Zhao H (2008) A certificate-based signcryption scheme. In: Proc. International Conference on Computer Science and Information Technology. 17–23.
3. Pang LJ, Gao L, Pei QQ, Cui JJ, Wang YM (2013) A new ID-based multi-recipient public-key encryption scheme. Chinese Journal of Electronics 1: 89–92.
4. AI-Riyami SS, Paterson KG (2003) Certificateless public key cryptography. In: Proc. 9th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2003). 452–473.
5. Barbosa M, Farshim P (2008) Certificateless signcryption. In: Proc. ACM Symposium on Information, Computer and Communications Security. 369–372.
6. Barreto PSLM, Deusajute AM, Cruz ES, Pereira GCF, Silva RR (2008) Toward efficient certificateless signcryption from (and without) bilinear pairings. http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03_03_artigo.pdf.
7. Li F, Shirase M, Takagi T (2009) Certificateless hybrid signcryption. In: Proc. 5th International Conference on Information Security Practice and Experience. 112–123.
8. Li PC, He MX, Li X, Liu WG (2010) Efficient and provably secure certificateless signcryption from bilinear pairings. Journal of Computational Information Systems 6: 3643–3650.
9. Selvi SSD, Vivek S, Rangan CP (2009) Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing. In: Proc. 5th international conference on Information security and cryptology (Inscrypt'09). 75–92.
10. Jing XF (2011) Provably secure certificateless signcryption scheme without pairing. In: Proc. International Conference on Electronic and Mechanical Engineering and Information Technology. 4753–4756.
11. Selvi SSD, Vivek SS, Shukla D, Chandrasekaran PR (2008) Efficient and provably secure certificateless multi-receiver signcryption. In: Proc. 2nd International Conference on Provable Security. 52–67.
12. Selvi SSD, Vivek SS, Rangan CP (2009) A note on the certificateless muli-receiver signcryption scheme. IACR Cryptology ePrint Archive. 308–308.
13. Miao SQ, Zhang FT, Zhang L (2010) Cryptanalysis of a certificateless multi-receiver signcryption scheme. In: Proc. International Conference on Multimedia Information Networking and Security. 593–597.
14. Shor PW (1994) Algorithms for quantum computation: discrete logarithms and factoring. In: Proc. 35th Symposium on Foundations of Computer Science. 124–134.
15. Dubois V, Fouque FA, Shamir A, Stern J (2007) Cryptanalysis of the SFLASH signature scheme. In: Proc. 3rd International SKLOIS Conference on Information Security and Cryptology (Inscrypt 2007). 1–4.
16. Billet O, Robshaw MJB, Peyrin T (2007) On building hash functions from multivariate quadratic equations. In: Proc. 12th Australasian conference on Information security and privacy (ACISP'07). 82–95.
17. Patarin J, Goubin L (1997) Trapdoor one-way permutations and multivariate polynomials. In: Proc. first International Conference on Information and Communications Security. 356–368.
18. Patarin J (1996) Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric. In: Proc. International Conference on the Theory and Application of Cryptographic Techniques. 33–48.
19. Bouillaguet C, Faugère JC, Fouque PA, Perret L (2011) Practical cryptanalysis of the identification scheme based on the isomorphism of polynomial with one secret problem. In: Proc.14th International Conference on Practice and Theory in Public Key Cryptography. 473–493.
20. Ding JT, Gower JE (2006) Inoculation multivariate schemes against differential attacks. In: Proc. 9th International Conference on Theory and Practice in Public-Key Cryptography. 290–301.
21. Hashimoto Y, Takagi T, Sakurai K (2012) General fault attacks on multivariate public key cryptosystems. In: Proc. 4th International Workshop on Post-Quantum Cryptography. 1–18.
22. Faugère JC, Perret L (2006) Polynomial equivalence problems: algorithmic and theoretical aspects. In: Proc. 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. 30–47.
23. Bouillaguet C, Faugère P, Perret L (2009) Differential algorithms for the isomorphism of polynomials problem. http://eprint.iacr.org/2009/583.pdf.
24. Tang SH, Xu LL (2012) Proxy signature scheme based on isomorphisms of polynomials. In: Proc. 6th International Conference on Network and System Security. 113–125.
25. Ding JT, Schmidt D (2005) Cryptanalysis of HFEv and internal perturbation of HFE. In: Proc. 10th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2005). 288–301.
26. Dubois V, Granboulan L, Stern J (2007) Cryptanalysis of HFE with Internal Perturbation. In: Proc. 10th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2007). 249–265.
27. Dubois V, Gama N (2010) The degree of regularity of HFE Systems. In: Proc. 16th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2010). 557–576.
28. Ding JT, Hodges TJ (2011) Inverting HFE systems is quasi-polynomial for all fields. In: Proc. 31th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO 2011). 724–742.
29. Ding JT, Kleinjung T (2012) Degree of Regularity of HFE minus. Journal of Math-for-Industry. 2012, Vol 4, 97–104.
30. Pang LJ, Li HX, Pei QQ (2012) Improved multicast key management of Chinese wireless local area network security standard. IET Communications 6: 1126–1130.