IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 25, 2019, accepted January 7, 2020, date of publication January 13, 2020, date of current version January 21, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2965978

Certificateless Broadcast Multisignature Scheme Based on MPKC

HUIFANG YU, SHUAIFENG FU, YIXIAN LIU, AND SHUAI ZHANG
School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

Corresponding author: Huifang Yu (yuhuifang@xupt.edu.cn)

This work was supported in part by the Doctoral Foundation of Xi'an University of Posts and Telecommunications under Grant 101-205020019, and in part by the Chunhui Project of Ministry of Education under Grant Z2017052.

ABSTRACT Broadcast multisignature allows multiple signers to sign the same message, which can be used in many areas, such as electronic contract signing, educational administration management system and grade management system. At present, the security of most broadcast multisignature schemes mainly depends on the intractability of large integer factoring (LIF) or discrete logarithm (DL) problem. Thus, broadcast multisignature schemes will suffer from the potential threat of the quantum computing attacks. Hence, it is an important problem how to solve the quantum computing attacks in traditional broadcast multisignature. In this paper, we construct the first certificateless broadcast multisignature scheme based on multivariate public key cryptosystem (MPKC-CLBMSS), whose security is based on the hardness of the isomorphism of polynomials (IP) problem. MPKC-CLBMSS not only solves the problem of quantum computing attacks, but also avoids the key escrow issue in IB-PKC along with the certificate management problem in traditional PKI. In MPKC-CLBMSS, the signature length is as same as that of the partial signature, regardless of the number of signers; the verification time of signature is as same as for a partial signature. MPKC-CLBMSS has higher computational efficiency than the existing broadcast multisignature scheme. Moreover, the security proof shows that MPKC-CLBMSS satisfies the unforgeability in the random oracle model.

INDEX TERMS Multivariate public key cryptosystem, certificateless public key technique, broadcast multisignature, post-quantum cryptography.

I. INTRODUCTION

Identity-based public key cryptosystem (IB-PKC) [1] can solve the certificate management problem in the traditional public key infrastructure (PKI) [2]. In IB-PKC, the public key of user is identity information such as telephone number and e-mail address. The user's private key is generated by a private key generator (PKG). It is obvious that the public key of user no longer requires authentication. However, a malicious PKG can disguise as any lawful user because the private key of every user in the system is known to the PKG. Hence, IB-PKC causes the private key escrow problem. In 2003, Al-Riyami and Paterson [3] presented certificateless public key cryptography (CL-PKC), where the user's full private key includes the partial private key of user generated by a key generation center (KGC) and a secret value chosen by this user, this shows that the KGC does not know the user's secret value. Because the certificate use in PKI and the key escrow problem in IB-PKC are removed in CL-PKC, the applications of CL-PKC are becoming more widespread. Certificateless multisignature is one of the important applications.

Multisignature is a group-oriented signature that allows multiple users to sign the same message. Multisignature is classified into the sequential multisignature and broadcast multisignature. Sequential multisignature requires the user to sign in a specific sequence, while broadcast multisignature does not require the order. Itakura [4] proposed the concept of multisignature and Micail *et al.* [5] gave the security model of multisignature. Liang *et al.* [6] introduced the idea of multisignature into CL-PKC, and constructed a concrete certificateless multisignature scheme from bilinear pairings. Since later, certificateless multisignature schemes [7]–[9] have been widely studied by scholars. In 2009, Zhang et al. [10] designed a certificateless multisignature scheme based on the computational Diffie-Hellman (CDH) problem, but its compactness was not satisfied and the signature length increased with the number of users. In 2012, Islam and Biswas [11] devised a compact certificateless multisignature scheme with

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

strong designated verifier using bilinear pairings, but this scheme did not provide the security proof in the random oracle model and had the disadvantage of low computational efficiency. In 2014, Islam and Biswas [12] presented a certificateless short sequential and broadcast multisignature scheme based on bilinear pairings and proved its security in the random oracle model. In 2017, Islam *et al.* [13] devised a certificateless multisignature scheme with low complexity using elliptic curve.

As far as we know, most of certificateless broadcast multisignature schemes are based on the traditional public key cryptosystem, whose security mainly depends on the intractability of large integer factoring (LIF) or discrete logarithm (DL) problem. With the emergence of Shor algorithm [14], the security of certificateless broadcast multisignature schemes under the hardness assumption of algebraic number theory will suffer from the threat of quantum computing attacks. Therefore, it is very important to construct new anti-quantum certificateless broadcast multisignature scheme. As one of the major candidates of post-quantum cryptography, the security of multivariate public key cryptosystem (MPKC) mainly depends on the intractability of multivariate quadratic (MQ) and the isomorphism of polynomials (IP) problems. MPKC has high computational efficiency and can realize strong secure communication on low-end devices. Signature and encryption schemes based on MPKC are widely studied [15]–[18]. At present, there is no certificateless broadcast multisignature scheme based on MPKC.

A. CONTRIBUTIONS

In this paper, we construct a new certificateless broadcast multisignature scheme based on MPKC (MPKC-CLBMSS), which solves the certificate management problem in PKI and the key escrow problem in IB-PKC. In MPKC-CLBMSS, the signature length is as same as the length of the partial signature generated by every signer, and its verification time is fixed to the time demanded to verify a partial signature. Our MPKC-CLBMSS is proved to be unforgeable in the random oracle model. By performance comparison analysis, we find that MPKC-CLBMSS not only has the advantage of resisting quantum computing attacks, but also has higher computational efficiency than traditional broadcast multisignature schemes.

B. PAPER ORGANIZATION

The structure of this paper is organized as follows: the second section introduces the definitions of MPKC, multivariate signature scheme (MSS), MPKC-CLBMSS along with the formal security models of MPKC-CLBMSS. The third section introduces a concrete instance of MPKC-CLBMSS, and proves its correctness. The fourth section proves the security of MPKC-CLBMSS. In the fifth section, the efficiency and security of MPKC-CLBMSS are compared with those of the previous broadcast multisignature schemes. The sixth section is a summary of the whole paper.

TABLE 1. Notations and their meaning.

Notations	Meaning
q	a prime
K	finite field with prime order q
r	the number of equations
n	the number of variables
P	the equations of n elements r polynomials
m	arbitrary message
t	the number of signers
N_i	the signer, where $i=1,2,\cdots,t$
C	collector
V	verifier
B	challenger
k	a security parameter
s	the system master key
ppk	the system partial public key
psk	the system partial private key
ID_i	the identity information of N_i
pk_i	the public key of N_i
sk_i	the private key of N_i
σ_i	the partial signature
σ	the signature
$params$	a set of system parameters

II. PRELIMINARIES

In this section, the meaning of notations for this paper are defined in Table 1. Hereafter, we briefly describe some preliminaries required in this paper.

A. NOTATIONS

The meaning of notations for this paper are defined in Table 1.

B. MPKC

MPKC has large advantage of performance in anti-quantum algorithm attacks and one of the research hotpots.

Let K denote a finite field, r denote the number of equations, and n denote the number of variables. Let P denote the equations of n elements r polynomials, i.e.,

$$P = (p_1(x_1, x_2, \cdots, x_n), \cdots, p_r(x_1, x_2, \cdots, x_n)) \quad (1)$$

where $p_i (i = 1, 2, \cdots, r)$ are defined as follows:

$$p_i(x_1, x_2, \cdots, x_n) := \sum_{1\le j\le k\le n} \gamma_{ijk} x_j x_k + \sum_{j=1}^{n} \beta_{ij} x_j + \alpha_i \quad (2)$$

where the coefficients $\alpha, \beta, \gamma \in K$ and the variables $x \in K$.

Definition 1(MQ Problem): Given n elements r multivariate equations over finite field K:

$$\begin{aligned} p_1(x_1, x_2, \cdots, x_n) &= p_2(x_1, x_2, \cdots, x_n) \\ &= \cdots = p_r(x_1, x_2, \cdots, x_n) = 0 \end{aligned} \quad (3)$$

where the coefficients and variables of p_i are taken from the finite field K. The problem of solving the equations is called the multivariate quadratic (MQ) problem.

As shown in [19], the MQ problem is a difficult problem of nondeterministic polynomials (NP), even on the smallest finite field K_2.

Definition 2 (IP Problem): Let P and Q be multivariate equations of n variables r polynomials, where P and Q are randomly selected over the finite field K, moreover, P and Q are isomorphic. There exists $P = T \circ Q \circ S$, where T and S are two invertible affine maps. The problem of finding the (T, S) isomorphism from Q to P is called the IP problem.

The IP problem is proven to be NP hard [20].

C. DEFINITION OF MSS

A generic multivariate signature scheme (MSS) is defined as follows:

KEYGEN: Let K denote a finite field, Q denote an invertible map $K^n \rightarrow K^r$, T denote an invertible affine map over K^r and S denote an invertible affine map over K^n. The private key includes a central mapping Q together with two affine transformations T and S. The public key satisfies $P = T \circ Q \circ S$.

SIGN: Let $m \in K^r$ denote a message (or message digest) to be signed. The signer orderly computes $y = T^{-1}(m) \in K^r$, $x = Q^{-1}(y) \in K^n$, $\sigma = S^{-1}(x) \in K^n$. Finally, the signature σ of message m is sent to the verifier.

VERIFY: After receiving σ, the verifier computes $m' = T \circ Q \circ S(\sigma)$. If $m' = m$ holds, the verifier accepts σ and rejects it otherwise.

D. DEFINITION OF MPKC-CLBMSS

In a MPKC-CLBMSS, multiple signers are able to sign the same message. A MPKC-CLBMSS mainly includes the KGC, t signers $\mathrm{N}_i (i = 1, 2, \cdots, t)$, collector C and verifier V, where the primary responsibility of the collector C is verifies the validity of the partial signature σ_i generated by signer N_i, and generates the signature σ if the partial signature σ_i is valid. Usually, a MPKC-CLBMSS consists of five algorithms as follows.

SETUP: The KGC selects a security parameter k as input, and outputs a set of system parameters *params*.

EXTRACT: The KGC generates the system master key s. Then KGC takes *params* and s as input, and outputs the system partial public/private key *ppk*/*psk*.

KEYGEN: The signer N_i takes *params*, *ppk*/*psk* and ID_i as input, and outputs the public/ private key pk_i/sk_i.

SIGN: The signer N_i takes *params*, ID_i, sk_i and a message m as input, and outputs the corresponding partial signature σ_i. The collector C takes *params*, m, ID_i, pk_i and σ_i as input, and outputs the signature σ if the partial signature σ_i is valid.

VERIFY: The verifier V takes *params*, m, σ, ID_i and pk_i as input, and accepts or rejects σ by checking whether the verification condition is true.

E. SECURITY MODELS OF MPKC-CLBMSS

Generally, there are two types of attacks in MPKC-CLBMSS. (1) Type I attack: the adversary A_1 does not know the system master key s, but A_1 can substitute the public key of any signer. (2) Type II attack: the adversary A_2 knows the system master key s, but A_2 cannot substitute the signer's public key.

Through the game between the adversary $\mathrm{A}_1(\mathrm{A}_2)$ and challenger B, we define the security models of MPKC-CLBMSS. In the following, we define an unforgeability attack game.

Setup: B runs the setup algorithm to generate a set of system parameters *params*, and runs the extraction algorithm to generate the system master key s. Then B sends *params* to A_1, and sends *params* and s to A_2.

Attack: In the game, the above two types of adversaries can conduct a series of queries:

H queries: When $\mathrm{A}_1(\mathrm{A}_2)$ queries for hash function, B returns the corresponding hash function value to $\mathrm{A}_1(\mathrm{A}_2)$.

Public key queries: When A_1 (A_2) queries for the public key of signer's ID_i, B runs the key extraction algorithm to obtain pk_i, and outputs pk_i to A_1 (A_2).

Public key replacement: A_1 can replace the public key of any signer with any value in a specific range.

Private key queries: When $\mathrm{A}_1(\mathrm{A}_2)$ queries for the private key of signer's ID_i, B obtains sk_i by running the key extraction algorithm, and outputs sk_i to A_1 (A_2). If the corresponding public key of signer is substituted, A_1 (A_2) cannot perform this queries.

Signature queries: When A_1 (A_2) submits a signature queries for the signer's ID_i and message m, B obtains σ by a call to the signature algorithm and outputs the signature σ to A_1 (A_2).

Forgery: A_1 (A_2) outputs a forged signature σ^*. If σ^* is valid, A_1 (A_2) succeeds; otherwise, it fails.

Definition 3 (Unforgeability): A MPKC-CLBMSS has the existential unforgeability against adaptive chosen-message attacks (EUF-CMA) if no polynomial bounded adversary A_1 wins the EUF-CMA game with a non-negligible advantage.

Definition 4 (Unforgeability): If no polynomial bounded adversary A_2 wins the EUF-CMA game with a non-negligible advantage, a MPKC-CLBMSS has the EUF-CMA security.

III. CONCRETE INSTANCE of MPKC-CLBMSS

In this section, we construct a concrete instance of MPKC-CLBMSS by referring to the thoughts of certificateless signcryption algorithms from MPKC [15]. The processes of signature and verification are shown in Figure 1. MPKC-CLBMSS can resist quantum computing attacks and solve the key escrow issue together with certificate management problem. MPKC-CLBMSS comprises of several polynomial time algorithms as follows:

A. SETUP

This algorithm is run by the KGC as follows.

(1) take a security parameter k as input and generate a finite field $K = \mathrm{GF}(q)$ of order q with $q = p^l$, where p is a prime;

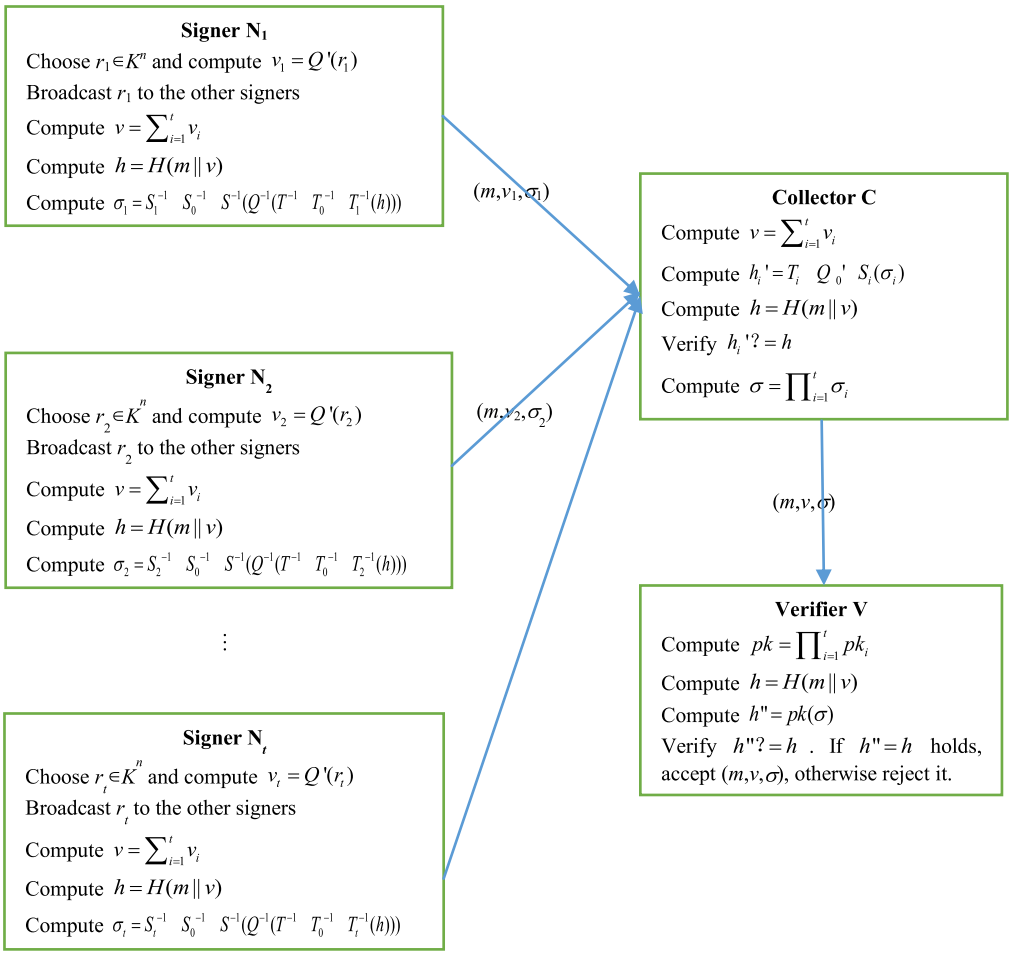


FIGURE 1. The processes of signature and verification.

(2) choose two positive integers r and n, where r is the number of multivariate equations and n is the number of variables;
(3) H: $\{0,1\}^* \times K^n \rightarrow K^n$ is cryptography hash function;
(4) publish a set of system parameters $params = (K, p, q, l, r, n, H)$.

B. EXTRACT

This algorithm is run by the KGC as follows.

(1) choose a multivariate encryption system with the core transformation Q that is invertible and quadric from K^n to K^n;
(2) choose two invertible affine maps $T:K^n \rightarrow K^n$ and $S:K^n \rightarrow K^n$ to compute $Q' = T \circ Q \circ S$, where Q' is the system public key and $s = \{T, Q, S\}$ is the system master key;
(3) randomly choose two invertible affine maps $T_0:K^n \rightarrow K^n$ and $S_0:K^n \rightarrow K^n$, then compute $Q'_0 = T_0 \circ Q' \circ S_0$. The partial public key is Q_0' and the partial private key is $\{T_0 \circ T, Q, S \circ S_0\}$;
(4) publish the system public key $Q' = T \circ Q \circ S$, and deliver the partial private key to the lawful signers via the private channel.

C. KEYGEN

Every signer N_i randomly chooses two affine maps $T_i:K^n \rightarrow K^n$ and $S_i:K^n \rightarrow K^n$, and computes $pk_i = T_i \circ Q'_0 \circ S_i$. The public key is pk_i and the private key is $sk_i = \{T^{-1} \circ T_0^{-1} \circ T_i^{-1}, Q^{-1}, S_i^{-1} \circ S_0^{-1} \circ S^{-1}\}$.

D. SIGN

Every signer N_i carries out the following steps.

(1) choose a random number $r_i \in K^n$ and compute $v_i = Q'(r_i)$;
(2) broadcast v_i to the other signers $N_j (j = 1, 2, \cdots, t; j \neq i)$;
(3) compute $v = \sum_{i=1}^{t} v_i$;
(4) compute $h = H(m||v)$;
(5) compute $\sigma_i = S_i^{-1} \circ S_0^{-1} \circ S^{-1}(Q^{-1}(T^{-1} \circ T_0^{-1} \circ T_i^{-1}(h)))$;
(6) output the partial signature (m, v_i, σ_i) to the collector C.

Then collector C carries out as follows.

(1) compute $v = \sum_{i=1}^{t} v_i$;
(2) compute $h'_i = T_i \circ Q'_0 \circ S_i(\sigma_i)$ and $h = H(m||v)$, then verify the individual signature (m, v_i, σ_i) by determining whether the equality $h'_i = h$ holds. C computes the

signature $\sigma = \prod_{i=1}^{t} \sigma_i$ if $h_i' = h$ holds and rejects (m, v_i, σ_i) otherwise;

(3) send the signature $(m, v, .\sigma)$ on the message m to the verifier V.

E. VERIFY

This algorithm is run by the verifier V.

1) compute $pk = \prod_{i=1}^{t} pk_i$;
2) compute $h = H(m||v)$;
3) compute $h" = pk(\sigma)$ and verify whether the equality $h" = h$ holds. If so, the verifier accept $(m, v, .\sigma)$ and rejects it otherwise.

F. CORRECTNESS ANALYSIS

The correctness of signature (m, v, σ) can be ensured in MPKC-CLBMSS.

Before we prove correctness, we will introduce the properties that we will use.

Property 1: Let K be a finite field, K^n be a linear space in the finite field, $L_1(x), L_2(x), \cdots, L_z(x)$ be z linearized polynomials on K^n, then the following eqality is true.

$$L_1(x) \times L_2(x) \times \cdots \times L_z(x) = L_1(L_2 \cdots (L_z(x))) \quad (4)$$

In addition, the equality (4) satisfies the commutative and associative property of multiplication, and the distributive property of ordinary addition [21], [22].

We can easily verify the following equality is true by using **property 1**. That is the proposed scheme satisfies the correctness.

$$\begin{aligned} h'' &= pk(\sigma) \\ &= \prod_{i=1}^{t} pk_i (\prod_{i=1}^{t} \sigma_i) \\ &= \prod_{i=1}^{t} pk_i (\prod_{i=1}^{t} sk_i(h)) \\ &= (\prod_{i=1}^{t} pk_i \prod_{i=1}^{t} sk_i) h(\text{Using} Property 1) = h \end{aligned} \quad (5)$$

IV. SECURITY ANALYSIS

Theorem 1: If an EUF-CMA adversary A_1 could forge a legal signature with non-negligible advantage ε (making at most q_{sk} private key queries and q_s signature queries), there is an algorithm B that can solve the IP problem with advantage ε', where

$$\varepsilon' \geq \frac{\varepsilon}{t(t \cdot q_s + q_{sk})} \frac{1}{1 + q_s} \left(1 - \frac{q_{sk})}{2^{|K^n|}}\right) \left(1 - \frac{q_s}{2^{|K^n|-1}}\right) \quad (6)$$

Proof: A_1 can replace any signer's public key, but does not know the system master key $s = \{T, Q, S\}$. For a random instance $(T_i \circ Q_0' \circ S_i, Q_0')$ of the IP problem, the goal of B is to obtain (T_i, S_i). B defines three lists L_H, L_k and L_s, which are employed to record the query-answer values for the H oracle, public/private key oracle and signature oracle, respectively. Each list is empty in the beginning.

(1) Setup

B runs the setup algorithm to produce a set of system parameters *params*, and runs the extraction algorithm to generate the system master key $s = \{T, Q, S\}$. Then B sends *params* to A_1, and keeps $s = \{T, Q, S\}$ secretly.

(2) Attack

H queries: A_1 queries for (m, v). If L_H contains (m, v, h), B outputs h to A_1; otherwise, B randomly returns a random number $h \in K^n$ to A_1 and adds the record (m, v, h) into L_H.

Public key queries: A_1 queries for the public key of arbitrary identity ID_i. B checks L_k at first, and it is necessary to consider the following two cases in response to this queries:

(1) If L_k contains the corresponding record (ID_i, pk_i), B outputs the public key pk_i to A_1.

(2) If L_k does not contain the corresponding record (ID_i, pk_i), B randomly selects $T_i, S_i \in K^n$ and computes pk_i by using the equality (7). Then B adds the record (ID_i, T_i, S_i, pk_i) into L_k and outputs pk_i to A_1.

$$pk_i = T_i \circ Q_0' \circ S_i \quad (7)$$

Public key replacement: A_1 randomly chooses $pk_i' \in K^n$ to replace any signer's public key pk_i. Then, C updates the list L_k with $(ID_i, *, *, pk_i')$.

Private key queries: A_1 queries a private key of the identity ID_i of arbitrary signer. B first checks L_k, and it is necessary to consider the following three cases in response to this queries:

(1) If L_k contains the corresponding record (ID_i, T_i, S_i, sk_i), B outputs the private key sk_i to A_1.

(2) If L_k does not contain the corresponding record (ID_i, T_i, S_i, sk_i) and the public key is not replaced, B executed the public key queries to obtain the corresponding record $(ID_i, T_i, S_i,)$ and computes the private key sk_i by using the equality (8). Then B adds the record (ID_i, T_i, S_i, sk_i) into L_k and outputs sk_i to A_1.

$$sk_i = \{T^{-1} \circ T_0^{-1} \circ T_i^{-1}, Q^{-1}, S_i^{-1} \circ S_0^{-1} \circ S^{-1}\} \quad (8)$$

(3) If L_k does not contain the corresponding record (ID_i, T_i, S_i, sk_i) and the public key is replaced, B cannot answer the private key sk_i of arbitrary identity ID_i. B aborts the game.

Signature queries: A_1 queries a signature of the signer's ID_i. B checks L_s at first and it is necessary to consider the following three cases in response to this queries:

(1) If L_s contains the corresponding record (ID_i, m, σ_i), B outputs the partial signature σ_i to A_1.

(2) If L_s does not contain the corresponding record (ID_i, T_i, S_i, sk_i) and the public key is not replaced, B executed the public key queries to obtain the corresponding record (ID_i, T_i, S_i) and computes the private key sk_i and partial signature σ_i by using the equalities (8) and (9) respectively. Then B adds the record (ID_i, T_i, S_i, sk_i) into L_k and adds the record (ID_i, m, σ_i) into L_s. Finally, it outputs σ_i to A_1.

$$\sigma_i = S_i^{-1} \circ S_0^{-1} \circ S^{-1}(Q^{-1}(T^{-1} \circ T_0^{-1} \circ T_i^{-1}(h))) \quad (9)$$

(3) If L_s does not contain the corresponding record (ID_i, T_i, S_i, sk_i) and the public key is replaced, B cannot answer the partial signature σ_i of ID_i. B aborts the game.

TABLE 2. Notations and their descriptions of various time complexities (in milliseconds).

Notations	Descriptions
T_{BP}	Time complexity for executing the bilinear pairing operation, $1T_{BP}\approx 20.01$ms
T_{ME}	Time complexity for executing the modular exponentiation, $1T_{ME}\approx 55.20$ms
T_{EM}	Time complexity for executing the elliptic curve scalar point multiplication, $1T_{EM}\approx 6.38$ms
T_{EA}	Time complexity for executing the addition of two elliptic curve points, $1T_{EA}\approx 0.03$ms
T_{H}	Time complexity for executing the maptopoint hash function, $1T_{H}\approx 6.38$ms

TABLE 3. Comparison of performance.

Schemes	Signature cost	Verification cost	Signature length	NO-KEI	NO-CMP	RQCA
Literature [12]	$2(t\text{-}1)T_{BP}+tT_{EM}+2(t\text{-}1)T_{EA}$	$2T_{BP}$	$1\|G_q\|$	YES	YES	NO
Literature [13]	$3tT_{EM}+4tT_{EA}$	$3T_{EM}+2T_{EA}$	$2\|G_q\|$	YES	YES	NO
Literature [23]	$3tT_{ME}+tT_{EM}$	$2T_{ME}+2T_{EM}$	$3\|G_q\|$	NO	YES	NO
Literature [24]	$tT_{ME}+tT_{H}$	$3T_{BP}+2T_{H}$	$\{0,1\}^n+\|G_q\|$	YES	NO	NO
MPKC-CLBMSS	$(t+1)T_{H}$	T_{H}	$2\|K^n\|$	YES	YES	YES

(3) Forgery

After a sequence of the queries, A_1 outputs a forged signature σ^* on a message m^*.

From the queries above, if A_1 wants to successfully forge a signature, A_1 must obtain the full private key $sk_i = \{T^{-1} \circ T_0^{-1} \circ T_i^{-1}, Q^{-1}, S_i^{-1} \circ S_0^{-1} \circ S^{-1}\}$ through the queries above. Obtaining the full private key sk_i corresponding to the forged signature as the resolution of IP problem.

Let us estimate the probability of the challenger B solving the IP problem.

E_1: the event that B does not abort the game. This probability is

$$\Pr[E_1] \geq \frac{1}{1+q_s}\left(1-\frac{q_{sk}}{2^{|K^n|}}\right) \tag{10}$$

E_2: the event that B rejects a valid partial signature. This probability is

$$\Pr[E_2] \leq \frac{q_s}{2^{|K^n|-1}} \tag{11}$$

E_3: the event that B obtains the correct signature. This probability is

$$\Pr[E_3] \leq \frac{1}{t\,(t\cdot q_s+q_{sk})}. \tag{12}$$

In addition, $\Pr[E_4] = \varepsilon$ represents the advantage that adversary A_1 can successful forge a signature.

Based on the above analysis, the advantage of B in solving the IP problem is $\varepsilon' = \Pr[E_1 \wedge E_2 \wedge E_3 \wedge E_4]$. Because the events are independent of each other, there is $\varepsilon' = \Pr[E_1] \cdot \Pr[E_2] \cdot \Pr[E_3] \cdot \Pr[E_4]$, i.e.,

$$\varepsilon' \geq \frac{\varepsilon}{t\,(t\cdot q_s+q_{sk})\,(1+q_s)}\left(1-\frac{q_{sk})}{2^{|K^n|}}\right)\left(1-\frac{q_s}{2^{|K^n|-1}}\right) \tag{13}$$

Theorem 2: If an EUF-CMA adversary A_2 could forge a legal signature with non-negligible advantage ε (making at most q_{sk} private key queries and q_s signature queries), there is an algorithm B which can solve the IP problem with advantage ε', where

$$\varepsilon' \geq \frac{\varepsilon}{t\,(t\cdot q_s+q_{sk})\,(1+q_s)}\left(1-\frac{q_{sk})}{2^{|K^n|}}\right)\left(1-\frac{q_s}{2^{|K^n|-1}}\right) \tag{14}$$

Let A_2 be the type II of adversary of MPKC-CLBMS, which can obtain the system master key $s = \{T, Q, S\}$ but cannot replace the signer's public key. Referring to **Theorem 1**, it is easy to prove **Theorem 2**, here we will not repeat.

V. PERFORMANCE ANALYSIS

In this section, we analyze the efficiency of MPKC-CLBMSS and previous broadcast multisignature schemes in terms of the signature length together with the computation and verification cost of signature. According to the actual calculation results in literatures [11]–[13], we give the notations and descriptions of various time complexity in Table 2. In Table 3, we describe the performance comparison between MPKC-CLBMSS and previous broadcast multisignature schemes [12], [13], [23], [24]. In Table 3, t denotes the number of signers, $\{0,1\}^n$ denotes n bits, $|G_q|$ denotes the size of the element of cyclic group G of prime order q, $|K^n|$ denotes the size of the element of the n degree extension finite of K, NO-KEI denotes that the scheme can avoid the key escrow issue, NO-CMP denotes that the scheme can avoid the certificate management problem and RQCA denotes that the scheme can resist quantum computing attacks. According to Table 2 and Table 3, the signature cost efficiency comparison

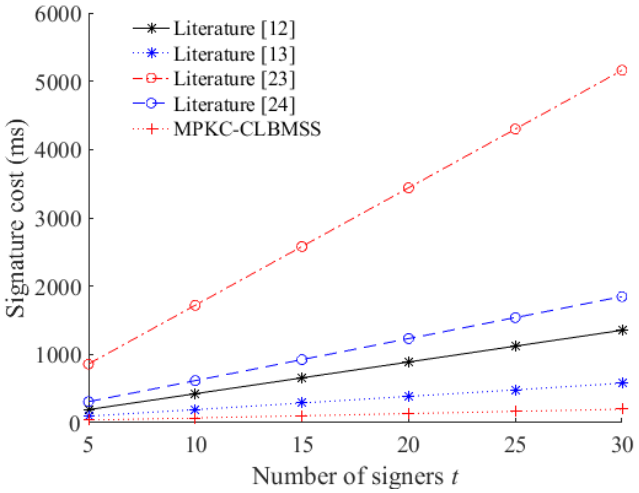


FIGURE 2. Comparison of signature cost.

of MPKC-CLBMSS and previous broadcast multisignature schemes is shown in Figure 2.

As shown in Table 3, we know that MPKC-CLBMSS does not include the bilinear pairing operations and modular exponentiation. Obviously, MPKC-CLBMSS has the advantages of small signature cost and low verification cost compared with literatures [12], [13], [23] and [24]. In addition, the signature length of MPKC-CLBMSS is shorter. In terms of security, MPKC-CLBMSS not only solves the problem of quantum computing attacks, but also avoids the key escrow issue in IB-PKC along with the certificate management problem in traditional PKI. As can be seen from Figure 2, MPKC-CLBMSS has obvious merit in signature cost.

VI. CONCLUSION

With the advent of quantum algorithms and the imminent birth of quantum computers, post-quantum cryptography is becoming more and more important research spots. As one of the primary candidates for post-quantum cryptography, MPKC is diffusely studied because of high computational efficiency and high security. In this paper, a new MPKC-CLBMSS is designed. Analysis shows that MPKC-CLBMSS is unforgeable against A_1 and A_2. In MPKC-CLBMSS, the signature length is as same as that of the partial signature, regardless of the number of signers. The verification time of signature is as same as for a partial signature. Also, MPKC-CLBMSS does not include bilinear pairing operations and modular exponentiation compared with other previous broadcast multisignature schemes, so it has the advantages of small computational cost and high computational efficiency. Moreover, the proposed scheme is based on the IP problem of MPKC, so it has the advantage of resisting quantum computing attacks. MPKC-CLBMSS is especially suitable for multiple user authorization to achieve specific functions. For example, the score of a subject requires the signature of multiple teachers to form the final score in the grade management system.

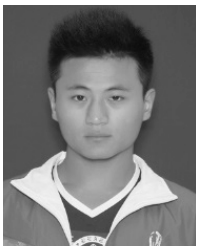
REFERENCES

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.
[2] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 196. 1984, pp. 47–53.
[3] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 2894. 2003, pp. 452–473.
[4] K. Itakura, "A public-key cryptosystem suitable for digital multisignatures," NEC Res. Dev. 71, 1983.
[5] S. Micali, K. Ohta, and L. Reyzin, "Accountable-subgroup multisignatures," in *Proc. 8th ACM Conf. Comput. Commun. Secur.*, New York, NY, USA, 2001, pp. 245–254.
[6] H. M. Liang, "A certificateless multisignature scheme," *J. Jimei Univ. (Nat. Sci.)*, vol. 13, no. 2, pp. 127–131, 2008.
[7] W. J. Luo and C. Y. Li, "Certificateless sequential multi-signature scheme without pairings," *Appl. Res. Comput.*, vol. 29, no. 4, pp. 1427–1429, 2012.
[8] Y. Qin and X. Wu, "Efficient certificateless sequential multi-signature scheme," *J. Commun.*, vol. 34, no. 7, pp. 105–110, 2013.
[9] V. C. Trinh, "A short server-aided certificateless aggregate multisignature scheme in the standard model," *Secur. Commun. Netw.*, vol. 2019, pp. 1–14, Mar. 2019.
[10] L. Zhang and F. Zhang, "A new certificateless aggregate signature scheme," *Comput. Commun.*, vol. 32, no. 6, pp. 1079–1085, Apr. 2009.
[11] S. H. Islam and G. P. Biswas, "Certificateless strong designated verifier multisignature scheme using bilinear pairings," in *Proc. Int. Conf. Adv. Comput., Commun. Inform.*, New York, NY, USA, 2012, pp. 540–546.
[12] S. H. Islam and G. Biswas, "Certificateless short sequential and broadcast multisignature schemes using elliptic curve bilinear pairings," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 26, no. 1, pp. 89–97, Jan. 2014.
[13] S. H. Islam, M. S. Farash, G. Biswas, M. K. Khan, and M. S. Obaidat, "A pairing-free certificateless digital multisignature scheme using elliptic curve cryptography," *Int. J. Comput. Math.*, vol. 94, no. 1, pp. 39–55, Jan. 2017.
[14] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Ann. Symp. Found. Comput. Sci.*, Santa Fe, NM, USA, 1994, pp. 124–134.
[15] X. H. Li, "Certificateless multi-receiver signcryption scheme based on multivariate public key cryptography," *Chin. J. Comput.*, vol. 35, no. 9, pp. 1881–1889, 2012.
[16] M. S. Chen, "From 5-pass MQ-based identification to MQ-based signatures," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 10032. 2016, pp. 135–165.
[17] M. S. Chen, "SOFIA: MQ-based signatures in the QROM," in *Public-Key Cryptography* (Lecture Notes in Computer Science), vol. 10770. 2018, pp. 3–33.
[18] S. Akleylek and M. Soysaldi, "A novel 3-pass identification scheme and signature scheme based on multivariate quadratic polynomials," *Turkish J. Math.*, vol. 43, no. 1, pp. 241–257, Jan. 2019.
[19] J. Patarin and L. Goubin, "Trapdoor one-way permutations and multivariate polynomials," in *Information and Communications Security* (Lecture Notes in Computer Science), vol. 1334. 1997, pp. 356–368.
[20] L. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms," in *Advances in Cryptology* (Lecture Notes in Computer Sciencee), vol. 1070. 1996, pp. 33–48.
[21] O. Ore, "On a special class of polynomials," *Trans. Amer. Math. Soc.*, vol. 35, no. 3, pp. 559–559, Mar. 1933.
[22] O. Ore, "Contributions to the theory of finite fields," *Trans. Amer. Math. Soc.*, vol. 36, no. 2, pp. 243–243, Feb. 1934.
[23] M. Mohammedi, "Cryptanalysis and improvement of identity-based multisignature scheme," in *Proc. 3rd Int. Conf. Future Netw. Distrib. Syst.*, Paris, France, no. 19, 2019.
[24] J. H. Park and Y.-H. Park, "A tightly-secure multisignature scheme with improved verification," *IEICE Trans. Fundam.*, vol. E99.A, no. 2, pp. 579–589, 2016.

HUIFANG YU was born in Qinghai, China. She received the Ph.D. degree in cryptography from Shaanxi Normal University. She is currently a Professor and a Master Supervisor with the Xi'an University of Posts and Telecommunications. She has completed more than 10 research projects, including a 973 Basic Research Project. She is the PI of more research projects, including the National Natural Science Foundation of China. She has published two books and more than 50 articles. She has ten national invention patents. Her main research interests include cryptography and information security. She is also a Senior Member of CACR.

SHUAIFENG FU was born in Shaanxi, China. She is currently pursuing the master's degree in cyberspace security with the Xi'an University of Posts and Telecommunications. She has two national invention patents. Her main research interests include post-quantum cryptography and information security.

YIXIAN LIU was born in Shaanxi, China. He is currently the Director of the Information Security and Countermeasure Experiment Teaching Center, Xi'an University of Posts and Telecommunications. His research interests are network security and information security assessment.



SHUAI ZHANG was born in Shandong, China. He is currently pursuing the master's degree in cyberspace security with the Xi'an University of Posts and Telecommunications. His research interests include multivariate public key cryptosystems and information security.