Multi-Recipient Signcryption for Secure Wireless Group Communication[*]

Yiliang Han[†] Xiaolin Gui Xu ản Wang

Department of Computer Science and Technology, Xi'an Jiaotong University, Xi'an 710049, China
Department of Electronic Technology, Engineering College of Armed Police Force, Xi 'an 710086, China

Abstract

Secure group communication is significant for wireless and mobile computing. Overheads can be reduced efficiently when a sender sends multiple messages to multiple recipients using multi-recipient signcryption schemes. In this paper, we proposed the formal definition and security model of multi-recipient signcryption, presented the definition of reproducible signcryption and proposed security theorems for randomness reusing based multi-recipient signcryption schemes. We found that a secure reproducible signcryption scheme can be used to construct an efficient multi-recipient signcryption scheme which has the same security level as the underlying base signcryption scheme. We constructed a multi-recipient scheme which is provable secure in random oracle model assuming that the GDH problem is hard, based on a new BLS-type signcryption scheme. Overheads of the new scheme are only $(n+1)/2n$ times of traditional ways when a sender sends different messages to n distinct recipients. It is more efficient than other known schemes. It creates a possibility for the practice of the public key cryptosystem in ubiquitous computing.

Key words

secure group communication; signcryption; multi-recipient signcryption; reproducible signcryption;

1. Introduction

Security problem is significant for wireless and mobile communication systems. Data privacy and integrity, source authenticity are the main tasks to strengthen information systems. To achieve confidentiality and authenticity simultaneously, encryption and signature (message authenticated code) are often combined in sequence. The traditional way is infeasible with the disadvantages: (1) heavy overheads; (2) lack of security. Zheng proposed a novel conception named *signcryption* to perform the encryption and signature in a single primitive [1]. It fixed the above problems. It is an active and fruitful area in the past years. Bao and Deng improved it and gave a signcryption that can be verified publicly in 1998 [2]. DSA (Digital Signature Algorithm) based signcryption scheme SC-DSA [3], RSA based signcryption scheme RSA-TBOS (two birds one stone) [4], ECDSA based signcryption scheme [5] and Identity-based signcryption [6] were proposed in the past years. At the same times, some generic structures for signcryption and secure model were presented also [7,8]. We proposed generalized signcryption to achieve more functions with one primitive [9]. However, Zheng's conception is unpractical for increasingly popular ubiquitous communications.

In common scenario, message is delivered between a single sender and a single recipient. Users may encrypt (sign) the message to protect it. When message will be delivery to several recipients, a message will be encrypted for several times independently using an encryption algorithm with different parameters (recipients' public key will be also included in public key setting). As a matter of fact, most of the messages are communicated in multiple users setting. Especially, applications in wireless and mobile computing need multi-user communication, such as secure routing, data aggregation, multi-cast in WSN (wireless sensor networks), manet (mobile ad hoc networks), overlay networks and so on. The naïve method is that sender produces and issues messages one by one, which is inefficient and insecure, especially in wireless and energy constrained networks. Broadcasted message will awake idle nodes and consume their power. The expensive computation and data sending will exhaust sender nodes' energy quickly. To enhance the totally performance, we should resolve the following problems. (1) Reducing broadcast. (2) Reducing the data amount. (3) Reducing the computational overheads on sender nodes. So, signcryption have to be extended to the multi-user setting in order to enhance the performance.

[*] Supported by the National Natural Science Foundation of China under Grant No.60273085; the Program for New Century Excellent Talents in University of China under Grant No.NCET-05-0829

[†] Correspond to: Yiliang Han, Department of Electronic Technology, Engineering College of Armed Police Force, Xi'an, Shaanxi, 710086, China. yilianghan@hotmail.com.

Our work is motivated by above problems. Our goal is to provide a theoretic model and a feasible scheme for secure group communications in wireless and mobile computing. The remainder of the paper is organized as follows. We reviewed the related works and preliminary in section 2 and section 3. In section 4, we proposed the definition and model of multi-recipient signcryption. Two security theorems about multi-recipient signcryption by randomness reusing were proposed and proved. What's more, we constructed an efficient multi-recipient signcryption scheme based on bilinear paring in section 5. This scheme is semantic secure and unforgeable, which is more efficient than others. It is the unique one that can send multiple messages to distinct recipients. We conclude the whole paper in section 6.

2. The state-of-art Research

2.1. Multi-recipient Encryption

How to produce and transfer messages to multiple recipients is the task of MRES (multi-recipient encryption scheme). In SM-MR (single message-multi-recipient) scheme, a sender sends a single message to different receivers. While in MM-MR (multi-message-multi-recipient) schemes, a sender sends different messages to different receivers. Obviously, SM-MR is a special case of MM-MR. In a MRES, overheads are from computation and communication. The totally computational overheads include encryption operation of sender and decryption operations of multiple receivers. While, the totally communication overheads include the broadcasted ciphertext. So, an efficient MRES is a scheme with low computational cost and shortened broadcast message.

To send encrypted message to multiple receivers, the natural way is trivial n-recipient which produces and sends a ciphertext for each one. Because that some schemes are not secure in multi-user setting, trivial n-recipient scheme is simple but infeasible, for example, Håstad have found that RSA may leak message[10]. In 2000, Baudron et al. [11] and Bellare et al.[12] independently proved the secure condition for MRES. They found that the trivial n-recipient scheme is secure (in the sense of indistinguishability) if the base scheme is secure (in the sense of indistinguishability). The nice result can be used to test the security of some encryption schemes. But the secure trivial n-recipient schemes have n times overheads more than that of underlying base scheme. Kurosawa [13] presented a technology called randomness reusing to enhance the efficiency of multi-recipient encryption schemes based on ElGamal [14] and Cramer-Shoup[15]. The length of resulted ciphertext is half of the trivial n-recipient scheme. In general, randomness reusing will cause serious secure problems. But Kurosawa's result showed that randomness can be reused without sacrificing security in some cases. Bellare et al.[16] [17] investigated the property of randomness reusing schemes and presented the reproducibility theorem to verify the security.

2.2. Multi-recipient signcryption

In one-to-many scenarios, such as secure broadcast/multicast, privacy and authenticity can be achieved with signcryption simultaneously. But the trivial n-recipient signcryption is unpractical. We should extend signcryption to many users setting to enhance its efficiency, and evaluate its security accurately.

In the last few years, some SM-MR schemes were proposed. These schemes can send a single message to different recipients. Firstly, Zheng designed a scheme for multiple receivers [1]. It encrypts message with a random number k which is signcrypted to receivers by trivial n-recipient method. The totally overheads are about n+1 times than base scheme. This scheme is inefficient even if it is secure. We also designed a similar scheme for generalized signcrypiton [9]. In 2003, Boyen designed a multipurpose identity-based signcryption scheme which can be used in multiple receivers setting [18]. His method is carry out the sign operation once, and then performs the encrypt operation independently for each receiver, based on the output from sign operation. The n bilinear paring computations made the scheme very slow. In 2006, Duan et al. proposed a multi-receiver identity-based signcryption scheme which includes 1 paring operation in signcryption and 4n paring in designcryption [19]. In 2007, the scheme of Yu et al. [20], which includes 3n paring in designcryption, is on the basis of Chen and Malone-Lee's identity based signcryption [7]. In 2008, using a different way, Li et al. proposed a similar one which reduces the communication overheads slightly [21].

It is easy to see, MM-MR is more useful than SM-MR in wireless and mobile networks. It is used not only to broadcast messages, but also to communicate with distinct users simultaneously. For example, in data aggregation, the sink node often communicates with distinct sense nodes. Unfortunately, there are neither theoretic achievements including the model, definition and secure notions, nor practical scheme. To sum up, researches are imperfect, without general definition and secure model. Moreover, there is no theoretic basis for how to construct efficient and secure scheme, which hold back the efficiency of group communications.

3. Preliminary

3.1. Signcryption

Signcryption is a logical combination of encryption and signature. A common signcryption scheme is a two-party cryptographic protocol. The syntax is presented as follows [22].

Definition 1 (Signcryption). A signcryption scheme Σ=(Gen, SC, DSC) consists of three algorithms. Gen, the randomized keys generation algorithm, takes input a security parameter l and generates a pair of keys for user U. We write (SDK_U, VEK_U) ← Gen(U, 1^l). SDK is a secret key. VEK is a public key. Signcryption algorithm SC is a probabilistic algorithm. It takes the private key of the sender A, the public key of the recipient B and a message $m \in M$ to return a signcrypted text w. We write $w \leftarrow$ SC(m, SDK_A, VEK_B). Decryption algorithm DSC is a deterministic algorithm. It takes the public key of the sender A, the private key of the recipient B, and a signcryption text w, to return the message m or a invalid notation ⊥. We write $m \cup \{\perp\} \leftarrow$DSC($w$, SDK_B, VEK_A). For a fixed message $m \in M$, we say that the signcryption scheme Σ=(Gen, SC, DSC) is correct if and only if DSC(SC(m, SDK_S, VEK_R), SDK_R, VEK_S)=m.

The security notions of signcryption were presented by Zheng firstly [1]. But for a verifiable publicly signcryption scheme, we say that it is secure if the following conditions are satisfied [9]:

Unforgeability. It is computationally infeasible for an adaptive foreger, who may be a dishonest Bob and allowed to query Alice's signcryption algorithm, to masquerade Alice in creating an authentic signcrypted text.

Confidentiality. It is computationally infeasible for an adaptive attacker to gain any partial information on the contents of a signcrypted text. The adaptive attacker may be any party other than Alice and Bob.

Now, we give the formal version of the above secure notions.

Definition 2 (Confidentiality). A signcryption scheme Σ=(Gen, SC, DSC) is semantic secure against IND-CCA2 (indistinguishability against adaptive chosen ciphertext attacks), if there is no probabilistic polynomial time attacker A can perform the attack experiment CCAExp with non-negligible advantage. For secure parameter $k \in N$, we consider the experiment CCAExp as follows.

Experiment $\mathbf{CCAExp}_{\Sigma,\mathbf{A}}^{\mathbf{ind\text{-}cca2}}(k)$

(1) $I \leftarrow \mathbf{G}(1^k)$; $(st) \leftarrow$A(select, I)

(2) (VEK_S, SDK_S) ← $\mathbf{K}$ (I)

(3) (VEK_R, SDK_R) ← $\mathbf{K}$ (I)

(4) (m_0, m_1, st)$\leftarrow \mathrm{A}^{SC(.),\ RO(.),\ DSC}$(find, st), ($|m_0|=|m_1|$)

(5) $\underline{b} \leftarrow \{0, 1\}$; $w \leftarrow$SC($m_{\underline{b}}$)

(6) $d \leftarrow \mathrm{A}^{SC(.),\ RO(.),\ DSC(.)}$ (guess, w, st)

(7) If $d \leftarrow \underline{b}$, and w was never queried to DSC(.), then return 1

Else return 0.

In the random oracle model [23] with secure parameter k, an adversary A runs in time t and performs q_{SC} signcryption queries, q_{DSC} de-signcryption queries and q_H queries to oracle RO(.), has the advantage $\mathbf{Adv}_{\Sigma,\mathbf{A}}^{\mathbf{ind\text{-}cca2}}(k) = \max\{\Pr[\mathbf{CCAExp}_{\Sigma,\mathbf{A}}^{\mathbf{ind\text{-}cca2-0}}(k) = 0]$ $- \Pr[\mathbf{CCAExp}_{\Sigma,\mathbf{A}}^{\mathbf{ind\text{-}cca2-1}}(k) = 0]\}$.

Notes. A is an adaptive attacker and runs in three stages. In the selecting stage, the attacker is given some initial information and outputs a state information st. In the finding stage, A selects two messages with equal length and submits to signcryption subroutine after querying to RO(.), SC(.) and DSC(.). In the guessing stage, A continues to get the help from these oracles.

Definition 3 (Unforgeability). A signcryption scheme Σ=(Gen, SC, DSC) is existentially unforgeable against adaptive insider CMA (chosen message attacks), if there is no probabilistic polynomial time forger E can perform the forge experiment ForgeExp with non-negligible advantage. For secure parameter $k \in N$, we consider the experiment ForgeExp as follows.

Experiment $\mathbf{ForgeExp}_{\Sigma,\mathbf{E}}^{\mathbf{cma}}(k)$

(1) $I \leftarrow \mathbf{G}(1^k)$; $(st) \leftarrow$E(select, I)

(2) (VEK_S, SDK_S) ← $\mathbf{K}$ (I)

(3) (VEK_R, SDK_R) ← $\mathbf{K}$ (I)

(4) If $\mathrm{E}^{SC(.)RO(.)}$(VEK_S,VEK_R, SDK_R) outputs (m, w) such that

(a) $\mathrm{DSC}^{RO(.)}$ (w, SDK_R, VEK_S) = m

(b) m was never queried to SC(.)

Return 1 else return 0.

The forger E runs in time t and performs q_{SC} signcryption queries and q_H queries to oracle RO(.), has the advantage $\mathbf{Adv}_{\Sigma,\mathbf{E}}^{\mathbf{cma}}(k) = \max\{\Pr[\mathbf{ForgeExp}_{\Sigma,\mathbf{E}}^{\mathbf{cma}}(k) = 1]\}$.

3.2. Bilinear Pairings and GDH Problem

Definition 4 (Bilinear Pairings). Let k be a security parameter and q be a k bit prime number. We consider groups G_1 and G_2 of the same prime order q. A bilinear map e: $G_1 \times G_1 \rightarrow G_2$ satisfies the following properties.

1. Bilinearity: $e(aP, bQ) = e(P,Q)^{ab}$ for all P, $Q \in G_1$, a, $b \in Z_q$.

2. Non-degeneracy: $e(P,Q) \neq 1$ for any P, $Q \in G_1$.

3. Computability: it is feasible to compute $e(P,Q)$, P, $Q \in G_1$.

**Definition 5 (GDH, the Gap Diffie-Hellman

problem). The GDH problem is to solve a given instance (P, aP, bP) of the CDH (Computational Diffie-Hellman) problem with the help of a DDH (Decisional Diffie-Hellman) problem oracle, that is able to decide whether (P, aP, bP, cP) is such that $c = ab \pmod q$ by checking the equation $e(P, cP) = e(aP, bP)$. Where, the CDH problem is given (P, aP, bP) to compute $abP \in G_1$ for unknown $a, b \in Z_q$. The DDH in G_1 is given (P, aP, bP, cP) to decide whether $ab \equiv c \pmod q$ for unknown $a, b, c \in Z_q$.

Assumption 1 (GDH assumption)**.** For the secure parameter $k \in N$, a probabilistic polynomial time attacker A will resolve the GDH problem on G_1 with order q and generator P. His advantage $\mathbf{Adv}_{\mathbf{GDH,A}}(k) = \max\{\Pr[\mathbf{A}(P, aP, bP) = abP, a, b \in Z_q^*]\}$ is negligible.

4. MM-MR Signcryption

As mentioned above, MM-MR is a secure primitive with potential practice in ubiquitous computing. In this section, we will propose the theoretic basis for MM-MR.

4.1. Model

Our model considers the MM-MR scenario. A sender issues several different messages $m_1,\ldots,m_t$ to several receivers P_i, i=1… t simultaneously. The receiver takes and designcrypts his signcryption text from the broadcasted message. MM-MR is a generic primitive of multi-recipient signcryption. Base signcryption scheme and SM-MR are both of special cases of MM-MR. We can easily find that, MM-MR signcryption scheme will become a SM-MR scheme when $m_1=\ldots= m_t =m$, and will become a base signcryption scheme when t=1. A formal definition of MM-MR signcryption scheme as follows.

Definition 6(Multi-recipient). A multi-recipient signcryption scheme MΣ=(Gen, MSC, DSC) consists of three algorithms. Gen is a keys generation algorithm as above. Signcryption algorithm MSC is a probabilistic algorithm. It takes the private key of the sender A, the public keys $\mathrm{VEK}_P = \{\mathrm{VEK}_{Pi}, i=1,\ldots, t\}$ of the recipient $P=\{P_i, i=1\ldots t\}$ and messages $M=\{m_i, i=1,\ldots, t, m_i \in M\}$ to return a signcryption text $W \leftarrow \mathrm{MSC}(M, \mathrm{SDK}_S, \mathrm{VEK}_P)$. DSC is a deterministic algorithm. It takes the public key of the sender A, the private key of the recipient P_i and a ciphertext w_i, to return the message m_i or $\perp$. We write $m_i \cup \{\perp\} \leftarrow \mathrm{DSC}(w_i, \mathrm{SDK}_{Pi}, \mathrm{VEK}_A)$. For a fixed message $M \in M$, we say that the multi-recipient signcryption scheme MΣ=(Gen, MSC, DSC) is correct if and only if $\mathrm{DSC}(\mathrm{SC}(M, \mathrm{SDK}_S, \mathrm{VEK}_P), \mathrm{SDK}_P, \mathrm{VEK}_S) = M$.

4.2. Security notions

Signcryption aims to establish secure and authorized communication. Zheng pointed out that a secure signcryption scheme should achieve confidentiality, unforgeability and non-repudiation [1]. But for any verifiable signcryption scheme, the unforgeability implies the non-repudiation. So, confidentiality and unforgeability are sufficient for a verifiable scheme. Now, we give the definitions of confidentiality and unforgeability for a multi-recipient signcryption scheme.

4.2.1. Confidentiality

For a multi-recipient signcryption scheme, confidentiality means that information of any plaintext could not be leaked to any others. In a SM-MR signcryption scheme, only outsider adversary wants to get the underlying message, since all of the receivers have the same one. While in a MM-MR signcryption scheme, recipients who want to get messages for any others are potential adversaries, because each recipient receives the different message. So, we take into account a scenario called *insider attacks*. We adapt the attacker model similar to insider attacker in [17]. Besides his own key pairs, the adversary has the ability to corrupt some fraction of other users and possession of their secret keys. We assume that adversary B attacking MΣ has corrupted n-l receivers. Uncorrupted users are numbered as 1,…, l. B runs in three stages: (1) in selecting stage, B is given the number of users n and outputs state information st and a integer l, ($1 \le l \le n$); (2) in finding stage, B is given a common parameter I, state information st and public keys of l uncorrupted users $\{\mathrm{VEK}_1, \ldots, \mathrm{VEK}_l\}$, outputs two l-victors $\boldsymbol{M}_\mathbf{0}$, $\boldsymbol{M}_\mathbf{1}$ of messages; (3) in guessing stage, B returns a bit d as his guess of the challenge bit b. In all of the stages, signcryption oracle $MSC(.)$ signcrypts all of message submitted by B except for the challenge message vector M^*. At the same time, designcryption oracle $DSC(.)$ designcrypts all of signcryption text submitted by B except for the challenge text vector W^*.

Definition 7 (confidentiality). Let MΣ=(Gen, MSC, DSC) be a MM-MR signcryption scheme. Let B be an adaptive adversary which runs in three stages. For atk Î {cpa, cca}, b Î {0, 1}, $k \in N$. Consider following experiment.

Experiment $\mathbf{Exp}^{\mathbf{mr\text{-}atk\text{-}b}}_{\mathbf{M\Sigma,B,n(.)}}(k)$

(1) $I \leftarrow \mathbf{G}(1^k)$; $(1^l, st) \leftarrow \mathrm{B}(\mathrm{select}, n, I)$ $(1 \le l \le n)$

(2) $(\mathrm{VEK}_S, \mathrm{SDK}_S) \leftarrow \mathbf{K}(I)$

(2) For i=1,…, l do $(\mathrm{VEK}_i, \mathrm{SDK}_i) \leftarrow \mathbf{K}(I)$ EndFor

(3) $(\boldsymbol{M}_0, \boldsymbol{M}_1, \boldsymbol{M}, \mathrm{coins}, st) \leftarrow \mathrm{B}^{MSC(.), RO(.), O^{1}(.), \ldots, O^{l}(.)}(\mathrm{find}, pk, st)$

$|\boldsymbol{M}_0|=|\boldsymbol{M}_1|=l$; $|\boldsymbol{M}|=n\text{-}l$; $|\mathrm{VEK}|=l$; $|\mathrm{coins}|= n(k)\text{-}l$

(4) For $i=l+1,\ldots, n$ do $(\mathrm{VEK}_i', \mathrm{SDK}_i') \leftarrow \mathrm{K}$ (I,

```
coins$_i$) EndFor
    (5) VEK$_P$ ←(VEK$_1$, …, VEK$_l$, VEK$_{l+1}'$, …, VEK$_n'$)
    (6) $M$*←($m_{b1}$,…, $m_{bl}$, $m_1$,…, $m_{n-l}$)
    (7) $W$*=MSC($M$*, SDK$_S$,VEK$_P$)
    (8) $d$←B$^{MSC(.), RO(.), O^1(.), …, O^l(.)}$(guess, $W$*, $st$)
    (9) Return $d$
```

The advantage of an attacker for ind-atk is defined as follows:

$$\mathrm{Adv}^{\mathrm{mr\text{-}atk}}_{\mathrm{M\Sigma, B, n}}(k,t,q_{RO},q_{MSC},q_{DSC}) = \max\{\Pr[\,\mathrm{Exp}^{\mathrm{mr\text{-}atk\text{-}0}}_{\mathrm{M\Sigma, B, n}}(k)=0] - \Pr[\,\mathrm{Exp}^{\mathrm{mr\text{-}atk\text{-}1}}_{\mathrm{M\Sigma, B, n}}(k)=0]\}.$$

The MM-MR signcryption scheme **MS** is said to be IND-CPA (indistinguishability against chosen plaintext attacks) secure (or IND-CCA secure) if the function $\mathrm{Adv}^{\mathrm{mr-cpa}}_{\mathrm{M\Sigma, B, n}}(k,t,q_{RO},q_{MSC},q_{DSC})$ (or $\mathbf{Adv}^{\mathbf{mr-cca}}_{\mathbf{M\Sigma, B, n}}(k,t,q_{RO},q_{MSC},q_{DSC})$)is negligible for any probabilistic polynomial time attacker B who runs in time t, using q_{RO} queries to its random oracles, q_{MSC} queries to its signcryption oracle and q_{DSC} queries to its designcryption oracle.

4.2.2. Unforgeability

For a multi-recipient signcryption scheme, unforgeability means that any users have no ability to forge a signcrypted text from the sender (who is a signer also). Outsider adversary has to forge a signcrypted text to pass the verifying operation. While, the legitimate recipient has more powerful ability to win the forge attacks. He can forge a valid signcryption text as long as he forges a signature of sender. We adapt the forger model including insider attacker. Moreover, there is no need for any forger to forger signcryption text W on M, but w on any m. A scheme is secure against any forger, if it is secure against insider forger.

Definition 8 (unforgeability). Let MΣ=(Gen, MSC, DSC) be a multi-recipient MM-MR signcryption scheme, and F be a forger. For any $k \in N$, consider the following experiment:

Experiment $\mathrm{ForgeExp}^{\mathrm{mr\text{-}cma}}_{\mathrm{M\Sigma,F,n}}(k)$

```
    Experiment $\mathbf{ForgeExp}^{\mathbf{mr\text{-}cma}}_{\mathbf{M\Sigma,F,n}}(k)$
    (1) $I$ ← G (1$^k$); ($st$) ←F(select, $n$, $I$)
    (2) (VEK$_S$, SDK$_S$) ← K ($I$)
    (3) For $i$=1,…, $n$ do (VEK$_i$, SDK$_i$) ← K ($I$, coins$_i$) EndFor
    (4) If F$^{MSC(.)RO(.)}$ outputs ($m_i$, $w_i$), $m_i \in M$, $w_i \in W$
        (a) DSC$^{RO(.)}$ ($w$, SDK$_{Pi}$, VEK$_S$) = $m_i$
        (b) $m_i$ is never queried to MSC
    Return 1 else return 0.
```

The advantage of a forger is defined as follows:

$$\mathrm{Adv}^{\mathrm{cma}}_{\mathrm{M\Sigma, F, n(.)}}(k,t,q_{RO},q_{MSC}) = \max\{\Pr[\,\mathrm{ForgeExp}^{\mathrm{cma}}_{\mathrm{M\Sigma, F, n}}(k)=1]\}$$

The MM-MR signcryption scheme MΣ is said to be strongly existentially unforgeable against chosen-message attacks (SC-SUF-CMA) if the function $\mathrm{Adv}^{\mathrm{cma}}_{\mathrm{M\Sigma, F, n(.)}}(k,t,q_{RO},q_{MSC})$ is negligible for any random polynomial time forger F who runs in time t, using q_{RO} queries to its random oracles, q_{MSC} queries to its signcryption oracle.

4.3. Randomness Reusing and Reproducible Signcryption Scheme

RR (randomness reusing) is a novel technology to improve efficiency of MRES. Generally, randomness reusing may cause serious problem for some encryption schemes. Kurosawa's result [13] shows that some encryption schemes with randomness reusing is secure for multiple recipients setting, while keeping lower communication overheads. The schemes based randomness reusing can be marked as RR-MRES. Not all of RR-MRES are secure, even they are efficient. Bellare et al. pointed out that some RR-MRES keep high security for the differences of the distinct recipient's public keys [17]. They proposed a condition for secure RR-MRES: if the base scheme is reproducible, then the corresponding RR-MRES is secure too.

Though signcryption is a type of public key primitive, it still differs to public key encryption. The signcryption algorithm takes as input a secret key of sender, a public key of receiver and a message to be transmitted. The designcryption algorithm takes as input a public key of sender, a secret key of receiver and a signcryption text. While, public encryption algorithm takes receiver's public key and a message, decryption algorithm takes receiver's secret key and ciphertext. The reproducibility of signcryption scheme is different to that of public key encryption scheme. We present the definition of reproducible signcryption scheme as follows.

Definition 9 (Reproducible Signcryption Scheme). Fix a signcryption S=(Gen, SC, DSC). Let **R** be an randomized polynomial-time algorithm that takes as input a secret key of sender, a public key of receiver, signcryption text of a random message, another secret key of sender, a pair of keys of receiver, and another random message, returns a signcryption text. We say that S is reproducible if exists a **R** such that SC (m', SDK$_S'$, VEK$_R'$, v)=**R**(I, VEK$_R$, SDK$_S$, w, m', VEK$_R'$, SDK$_R'$, SDK$_S'$).

Multi-recipient signcryption scheme can be constructed with randomness reusing to achieve computation and communication savings. In the sense of privacy, if underlying base signcryption scheme is reproducible and IND-CPA (IND-CCA) secure, then the associated multi-recipient signcryption scheme is RR-IND-CPA (RR-IND-CCA) secure also.

Theorem 1. Fix a signcryption scheme S=(Gen, SC, DSC) and a integrity n, MS=(Gen, MSC, DSC) is associated randomness reusing multi-recipient scheme. If S is reproducible, then for any randomized polynomial time attacker B_{atk}, there exists a randomized polynomial time attacker A_{atk}, atk Î {cpa, cca}, such that for any k $\mathbf{Adv}^{\mathbf{mr-atk}}_{\mathbf{M\Sigma,B_{atk},n}}(k) \leq n \cdot \mathbf{Adv}^{\mathbf{atk}}_{\mathbf{\Sigma,A_{atk}}}(k)$.

Proof.

We consider a hybrid experiment [17] and attackers described in definition 4 and definition 7.

For confidentiality of a signcryption scheme, IND-CCA2 is the strongest secure notion. A scheme semantic secure against IND-CCA2, implies IND-CCA and IND-CPA. We only consider the case of IND-CCA2.

```
  Experiment HybirdEXP H_j(k)=0 (0≤j≤n)
    (1) $I \leftarrow \mathbf{G}(1^k)$; $(1^l, st) \leftarrow$ B(select, $n$, $I$)  $(1\leq l\leq n)$
    (2) $(\mathrm{VEK}_S, \mathrm{SDK}_S) \leftarrow \mathbf{K}(I)$
    (3) For $i$=1,…, $l$ do $(\mathrm{VEK}_i, \mathrm{SDK}_i) \leftarrow \mathbf{K}(I)$ EndFor
    (4) $(M_0, M_1, M$, coins, $st) \leftarrow \mathrm{B}^{MSC(.), RO(.), DSC1(.), …, DSC\,l(.)}$(find, $st$)
    (5) For $i$=$l$+1,…, $n$ do $(\mathrm{VEK}_i', \mathrm{SDK}_i') \leftarrow$ K ($I$, coins$_i$) EndFor
    (6) $\mathrm{VEK}_P \leftarrow (\mathrm{VEK}_1,…,\mathrm{VEK}_l,\mathrm{VEK}_{l+1}', …,\mathrm{VEK}_n')$
    (7) If $j\leq l$ then $M^* \leftarrow (m_{01},…, m_{0j}, m_{1j+1}, m_{1l}, m_1,…, m_{n-l})$
          else $M^* \leftarrow (m_{01},…, m_{0l}, m_1,…, m_{n-l})$
    (8) $W^*$=MSC($M^*$, $\mathrm{SDK}_S$,$\mathrm{VEK}_P$)
    (9) $d \leftarrow \mathrm{B}^{MSC(.), RO(.), DSC1(.), …, DSC\,l(.)}$(guess, $W^*$, $st$)
    (10) Return $d$
```

Let p_j=Pr[$\mathrm{H}_j(k)$=0]. We claim that $\Pr[\mathbf{Exp}^{\mathbf{mr-cca-0}}_{\mathbf{M\Sigma,B,n}}(k)=0]=p_n$ and $\Pr[\mathbf{Exp}^{\mathbf{mr-cca-1}}_{\mathbf{M\Sigma,B,n}}(k)=0]=p_0$.

We can get $\mathbf{Adv}^{\mathbf{mr-cca}}_{\mathbf{M\Sigma,B,n}}(k)=p_n-p_0$.

Then， We construct an attacker A which runs B as a subroutine, against the base scheme Σ. A runs three stages too. In each stage, A gets information from B's outputs.

```
  A (select, $I$)
    (1) $I \leftarrow \mathbf{G}(1^k)$; $(1^l, st') \leftarrow$ B(select, $n$, $I$) $(1\leq l\leq n)$; $j \leftarrow \{1,…, l\}$
    (2) $st \leftarrow (st', l, j)$
    (3) Return $st$
  A (find, $I$, $\mathrm{VEK}_R$)
    (1) $(\mathrm{VEK}_S, \mathrm{SDK}_S) \leftarrow \mathbf{K}(I)$
    (2) If $j\leq l$ then For $i$=1,…, $j$-1,$j$+1,…,$l$ do $(\mathrm{VEK}_i, \mathrm{SDK}_i) \leftarrow \mathbf{K}(I)$; $\mathrm{VEK}_j = \mathrm{VEK}_R$ EndFor
        else For $i$=1,…,$l$ do $(\mathrm{VEK}_i, \mathrm{SDK}_i) \leftarrow \mathbf{K}(I)$ EndFor
    (3) $(M_0, M_1, M$, coins, $st') \leftarrow \mathrm{B}^{MSC(.), RO(.), DSC1(.), …, DSC\,l(.)}$(find, $st'$)
    (4) For $i$=$l$+1,…, $n$ do $(\mathrm{VEK}_i', \mathrm{SDK}_i') \leftarrow$ K ($I$, coins$_i$) EndFor
    (5) $\mathrm{VEK}_P \leftarrow (\mathrm{VEK}_1,…,\mathrm{VEK}_l,\mathrm{VEK}_{l+1}', …,\mathrm{VEK}_n')$
    (6) If $j > l$ then $m_{0j}=m_j$; $m_{1j}=m_j$
    (7) $st \leftarrow (st', l, j\, M_0, M_1, M, \mathrm{VEK}_P)$
    (8) Return $(m_{0j}, m_{1j}, st)$
  A (guess, $w$, $st$)
    (1) For $i$=1,…, $j$-1,$j$+1,…,$n$ do
          If $i$=$l$+1,…, $n$ then $m' \leftarrow m_i$
          If $i\leq j$ then $m' \leftarrow m_{0i}$
          Else $m' \leftarrow m_{1i}$
            $w_i \leftarrow$ RP($I$, $\mathrm{VEK}_R$, $\mathrm{SDK}_S$, $w$, $m'$, $\mathrm{VEK}_i$, $\mathrm{SDK}_i$, $\mathrm{SDK}_S$)
          EndFor
    (2) $W' \leftarrow \{w_1,…,w_{j-1}, w, w_{j+1},…,m_n\}$
    (3) $d \leftarrow \mathrm{B}^{MSC(.), RO(.), DSC1(.), …, DSC\,l(.)}$(guess, $W'$, $st'$)
    (4) Return $d$
```

We claim that $\Pr[\mathbf{Exp}^{\mathbf{cca-0}}_{\mathbf{\Sigma,A}}(k)=0]=\frac{1}{n}\sum_{i=1}^{n}p_i=\frac{p_n}{n}$ and $\Pr[\mathbf{Exp}^{\mathbf{cca-1}}_{\mathbf{\Sigma,A}}(k)=0]=\frac{1}{n}\sum_{i=1}^{n}p_{i-1}=\frac{p_0}{n}$.

Then, we can get $\mathbf{Adv}^{\mathbf{atk}}_{\mathbf{\Sigma,A}}(k)=\Pr[\mathbf{Exp}^{\mathbf{cca-0}}_{\mathbf{\Sigma,A}}(k)=0]-\Pr[\mathbf{Exp}^{\mathbf{cca-1}}_{\mathbf{\Sigma,A}}(k)=0]=\frac{1}{n}(p_n-p_0)$.

By taking the maximum, we obtain that $\mathbf{Adv}^{\mathbf{mr-atk}}_{\mathbf{M\Sigma,B_{atk},n}}(k) \leq n \cdot \mathbf{Adv}^{\mathbf{atk}}_{\mathbf{\Sigma,A_{atk}}}(k)$.

The overheads of A include B's overheads, picking the random number j, producing n-1 key pairs and RP's overheads. □

Theorem 2. Fix a signcryption scheme S=(Gen, SC, DSC) and a integrity n, MS=(Gen, MSC, DSC) is corresponding randomness reusing multi-recipient scheme. If S is reproducible, then for any randomized polynomial time forger F, there exists a randomized polynomial time attacker E. For any k:

$$\mathbf{Adv}^{\mathbf{mr-cma}}_{\mathbf{M\Sigma,F,n}}(k) \leq n \cdot \mathbf{Adv}^{\mathbf{cma}}_{\mathbf{\Sigma,E}}(k)$$

Proof.

We construct a forger E to forge a base signcryption scheme running F as a subroutine. E attacks the signcryption scheme with sender S and recipient R. In F's experiment, R is P_j, for $j\in$ {1,…, n}.

```
  $\mathrm{E}^{SC(.)RO}$ ($\mathrm{VEK}_S$,$\mathrm{VEK}_R$, $\mathrm{SDK}_R$)
    (1) $I \leftarrow \mathbf{G}(1^k)$; $(st) \leftarrow$ F(select, $I$); $j \leftarrow \{1,…, n\}$
    (2) $(\mathrm{VEK}_S, \mathrm{SDK}_S) \leftarrow \mathbf{K}(I)$
    (3) For $i$=1,…, $j$-1, $j$+1,…, $n$ do
          $(\mathrm{VEK}_i, \mathrm{SDK}_i) \leftarrow \mathbf{K}(I$, coins$_i)$; $(\mathrm{VEK}_j, \mathrm{SDK}_j)=(\mathrm{VEK}_R, \mathrm{SDK}_R)$
          EndFor
    (4) If $(m_i, w_i) \leftarrow \mathrm{F}^{MSC(.)RO(.)}(\mathrm{VEK}_S,\mathrm{VEK}_P, \mathrm{SDK}_P)$ such that
          (a) $\mathrm{DSC}^{RO(.)}(w_i, \mathrm{SDK}_i, \mathrm{VEK}_S) = m_i$
          (b) $m_i$ was never queried on $MSC$(.)
            then $w_j \leftarrow$ RP($I$, $\mathrm{VEK}_R$, $\mathrm{SDK}_S$, $w_i$, $m_j$, $\mathrm{VEK}_R$, $\mathrm{SDK}_R$, $\mathrm{SDK}_S$)
            Return $(m_j, w_j)$
```

Forger E has to forge a signcryption text that can be verified by receiver $P_j(R)$ to win the experiment. While, forger F can win the experiment by forging a signcryption text that can be verified by any receiver.

After wining, F produces the signcryption text associated with receiver P_j using reproducing algorithm RP. It is easy to see that (m_j, w_j) is a valid message-signcryption text as well as (m_i, w_i).

In experiment $\mathbf{ForgeExp}^{\mathbf{cma}}_{\Sigma,\mathbf{E_i}}(k)$, E attacks the base signcryption scheme with sender S and recipient P_j.

Thus,

$$\mathrm{ForgeExp}^{\mathrm{cma}}_{\Sigma,\mathrm{E}_1}(k) = \mathrm{ForgeExp}^{\mathrm{cma}}_{\Sigma,\mathrm{E}_2}(k) \\ = \ldots \mathrm{ForgeExp}^{\mathrm{cma}}_{\Sigma,\mathrm{E}_n}(k) = \mathrm{ForgeExp}^{\mathrm{cma}}_{\Sigma,\mathrm{E}}(k) .$$

Obviously,

$$\Pr[\mathbf{ForgeExp}^{\mathbf{mr\text{-}cma}}_{\mathbf{M}\,\Sigma,\,\mathbf{F,n}}(k) = 1] \\ = \sum_{i=1}^{n} \Pr[\mathbf{ForgeExp}^{\mathbf{cma}}_{\Sigma,\,\mathbf{E_i}}(k) = 1] .$$

By taking the maximum, we obtain that $\mathbf{Adv}^{\mathbf{mr-cma}}_{\mathbf{M}\,\Sigma,\mathbf{F,n}}(k) \le n \cdot \mathbf{Adv}^{\mathbf{cma}}_{\Sigma,\mathbf{E}}(k)$.

The overheads of E include the running times of F, RP, picking the random number j and producing n-1 key pairs. □

5. An Efficient MM-MR Signcryption Scheme

5.1. SC-BLS: An Improved Signcyption Scheme based on BLS Signature

In this subsection, we will construct a signcryption scheme based on BLS signature scheme which was presented by Boneh, Lynn and Shacham in 2001 [24]. It is an efficient scheme based on any GDH group and be used broadly for its simplicity and low overheadss. In 2004, Libert and Quisquater proposed a signcryption scheme [35] based on BLS. The scheme wraps up the message and sender's public key. So receiver could perform designcryption operation without getting sender's public key beforehand. But the scheme is not secure since signature couldn't include receiver's private information and attackers have chance to forge a signcryption text that could be passed the verifying operation. In 2005, Tan pointed out that the scheme is neither semantic secure against chosen cipher attack nor key privacy [26]. At the same time, Yang et al. also found the problem and improved it [27]. Their improvement failed to grasp the essence and was broken by Tan [28]. Li et al. [29] presented another improved scheme which is secure against Tan's attack. In order to keep the sender's public key privacy, these schemes encrypted it together with message. In fact, public key privacy is not necessary for general applications. Recipient could get sender's identity information from network protocols directly. So, it is not practical to obtain the property while reducing communication bandwidth. Motivated by the base secure demand, we improved Li's scheme in this section. For a z-bits message, Li's scheme [29] produces z+3l bits signcryption text which could be reduced to z+2l bits in our scheme. We name the new scheme SC-BLS.

Let k be secure parameter, q is a k-bits prime, and G_1 is a bilinear group with order q. P is a generator. l is the length of elements on G_1. H_1: $\{0, 1\}^z \times G_1 \rightarrow G_1$and H_2: $G_1^{\,2} \rightarrow \{0, 1\}^{z+l}$ are two hash functions that can be regarded as random oracle. Notation ? $_{\mathrm{R}}$ means random selection. SC-BLS consists of three algorithm: *KeyGen*, *SC* and *DSC*.

Algorithm KeyGen. User U picks a random $x_u \leftarrow_{\mathrm{R}} Zq$ and sets his public key to $Y_u = x_u P \in G_1$. His private key is x_u. We will denote the sender and the receiver respectively by $U = S$ and U=R and their key pair by (x_S, Y_S) and (x_R, Y_R).

Algorithm SC. to signcrypt a plaintext $m \in \{0, 1\}^z$ intended to R, the sender S uses the following procedure:

1. Pick a random $r \leftarrow_{\mathrm{R}} Z_q$ and compute $U = rP \in G_1$.
2. Compute $V = x_S H_1(m, rY_R) \in G_1$.
3. Compute $Z = (m||V) \oplus H_2(U, Y_R, rY_R) \in \{0, 1\}^{z+l}$.

The ciphertext is given by $w = (U, Z) \in G_1 \times \{0, 1\}^{z+l}$.

Algorithm DSC. when receiving a ciphertext $w = (U, Z)$, the receiver R has to perform the steps below:

1. Compute $H_2\ (U, x_R U) \in \{0, 1\}^{n+l}$.
2. Compute $(m||V) = Z \oplus H_2(U, Y_R, x_R U)$.
3. Compute $H = H_1(m, x_R U) \in G_1$ and then check if $e(Y_S, h) = e(P, V)$. If this condition does not hold, reject the ciphertext.

Correctness. If $w = (U, Z)$ is a valid signcryption text, it is easy to see that $x_R U = rY_R = x_R rP$ and $(m||V)$ is decrypted correctly. Thus $e(P, V) = e(P, x_S h) = e(x_S P, h) = e(Y_S, h)$ is hold.

5.2. Multi-recipient Signcyrption Scheme

In this subsection, we will construct a multi-recipient scheme called MSC-BLS based on SC-BLS with randomness reusing. In this scheme, a sender S signcrypts messages $M = \{m_i | m_i \in \{0, 1\}^z, i=1, \ldots, n\}$ for n distinct receiver R_i, i=1, …, n, then broadcasts signcryption text. A receiver R_i gets his signcryption text and designcrypts it using base designcryption algorithm. MSC-BLS also consists of three algorithms: KeyGen, MSC and DSC.

Algorithm KeyGen: For a sender, his key pair is (x_S, Y_S), $x_S \leftarrow_{\mathrm{R}} Zq$, $Y_S = x_S P \in G_1$. For a receiver P_i, i=1, …, n, his key pair is (x_{Ri}, Y_{Ri}), $x_{Ri} \leftarrow_{\mathrm{R}} Zq$, $Y_{Ri} = x_{Ri} P \in G_1$.

Algorithm MSC: To signcrypt messages $M = \{m_i | m_i \in \{0, 1\}^z, i=1, \ldots, n\}$, S performs following operations.

1. Pick a random $r \leftarrow_{\mathrm{R}} Z_q$ and compute $U = rP \in G_1$.
2. For i=1,…,n
   (a) Compute $V_i = x_S H_1(m_i, rY_{Ri}) \in G_1$.

(b) Compute $Z_i = (m_i||V_i)\oplus H_2(U, Y_{Ri}, rY_{Ri})\in\{0, 1\}^{z+l}$.

EndFor

3. The ciphertext is given by $W = (U, Z_i) \in G_1\times \{0, 1\}^{n+l}$. $W = (U, Z_1,\ldots, Z_n)$

Algorithm DSC: When receiving *W*, the receiver R_i get his signcryption text w_i=(U, Z_i) and performs the steps below.

1. Compute $H_2(U, x_{Ri}U)\in\{0, 1\}^{z+l}$.
2. Compute $(m_i||V_i)=Z \oplus H_2(U, Y_{Ri}, x_{Ri}U)$.
3. Compute $h_i = H_1(m_i, x_{Ri}U)\in G_1$ and then check if $e(Y_S, h_i)= e(P, V_i)$. If this condition does not hold, reject the ciphertext.

Correctness. If w_i=(U, Z_i) is a valid signcryption text, it is easy to see that $x_{Ri}U= rY_{Ri} = x_{Ri}rP$ and $(m_i||V_i)$ is decrypted correctly. Thus $e(P, V_i) =e(P, x_S h_i) =e(x_S P, h_i)= e(Y_S, h_i)$ is hold.

According to the definition in subsection 3.1, MSC-BLS is a general scheme. When m_1=, …,= m_n = m, MSC-BLS will become a SM-MR scheme. When n=1, it will become SC-BLS. It has the same KeyGen algorithm and DSC algorithm as that of SC-BLS.

5.3. Security Analysis

5.3.1. Reproducibility of SC-BLS

Lemma 1. Base signcryption scheme SC-BLS=(Gen, SC, DSC) is a reproducible scheme.

Proof.

Firstly, we run signcrytion SC(m', SDK$_S'$, VEK$_R'$, r), for given random coins r, a sender S' and a recipient R' on the message m'.

Algorithm SC(m', SDK$_S'$, VEK$_R'$, r)

1. Compute $U =rP\in G_1$.
2. Compute $V' = x_S'H_1(m', rY_R')\in G_1$.
3. Compute $Z'= (m'||V')\oplus H_2(U, rY_R')\in \{0, 1\}^{n+l}$.
4. Return $w' = (U, Z')\in G_1\times \{0, 1\}^{n+l}$ as cipher text.

Then, we run a polynomial time reproducing algorithm **RP**, which takes common parameters, a public key of recipient R, secret key of a sender S, signcryption text w=(U, Z)of a message m, another message m', key pair of another recipient R', and secret key of another sender S', outputs the corresponding signcryption text.

Algorithm RP(I, VEK$_R$, SDK$_S$, w, m', VEK$_R'$, SDK$_R'$, SDK$_S'$)

1. Compute $V' = x_S'H_1(m', rY_R')\in G_1$.
2. Compute $Z'= (m'||V')\oplus H_2(U, rY_R')\in \{0, 1\}^{n+l}$.
3. Return $w' = (U, Z')\in G_1\times \{0, 1\}^{n+l}$ as cipher text.

Obviously, SC(m', SDK$_S'$, VEK$_R'$, r)=**RP**(I, VEK$_R$, SDK$_S$, w, m', VEK$_R'$, SDK$_R'$, SDK$_S'$).

So, the base signcryption scheme is a reproducible scheme. □

5.3.2. Security of SC-BLS

In the random oracle model assuming that GDH problem is hard.

Lemma 2. In the random oracle model with secure parameter k, if an adversary A has non-negligible advantage e against the IND-CCA2 security of SC-BLS when running in time t and performing q_{SC} signcryption queries, q_{DSC} de-signcryption queries and q_{Hi} queries to oracles H_i, i=1,2, then there is an algorithm B that solves the GDH problem in G_1 with probability $e'\geq e - q_{DSC}(q_{H1} / 2^k+q_{H2} / 2^{z+l})$ and within running time $t'=t+(4q_{DSC} +2q_{H2})t_b+ q_{H2}t_e$. Where t_b denotes the time required for one pairing evaluation, t_e denotes the time required for exponention.

Proof.

For contradiction, we assume that an attacker A breaks IND-CCA2 of SC-BLS with probability greater than e that within time t. We show that using A, one can construct an attacker B for solving the GDH problem with the help of a DDH solver due to the bilinear pairing.

Suppose that B is given (P, aP, bP) as an instance of CDH. B runs A as a subroutine to find the solution of abP. A then adaptively performs hash queries, signcryption queries and de-signcryption queries. Firstly, $Y_U = bP\in G_1$ is given to B as a challenge public key. To handle A's queries, B maintains two lists L_1 and L_2 to keep track of the answers given to oracle queries on H_1 and H_2.

Hash queries are simulated as follows.

H_1 simulation. When a hash query H_1 (m, P_1) is received, B checks if the query tuple (m, P_1, h) is already in L_1. If it exists, the result of hP is returned. Else, B picks a random number $h\in Z_q$, inserts the tuple (m, P_1, h) into list L_1 and returns the result of hP.

H_2 simulation. When a hash query $H_2(P_1, P_2, P_3)$ is received, B checks if the query tuple (P_1, P_2, P_3, v) is already in L_2. If it exists, the existing result of v is returned. If it does not exist but $e(P_1, P_2)= e(P, P_3)$, B picks a random number $v\in\{0, 1\}^{z+l}$, inserts the tuple (P_1, P_2, P_3, v) into list L_2 and returns the number v. If (P_1, P_2, ·, t) exists in L_2, and $e(P_1, P_2)= e(P, P_3)$, then replace the "·" with P_3, and returns v, where "·" is a symbol to denote blank. Else, B picks $v\in\{0, 1\}^{z+l}$ randomly and returns it.

Signcryption and de-signcryption queries are simulated as follows.

SC simulation. For a signcryption query on (m, Y_R) choosed by A, B checks if $Y_R\notin G_1$or Y_R=Y_U, rejects it. Otherwise, B picks $r\in Z_q$ randomly, computes the result of $U =rP$. Then B simulates H_1 (m, rY_R) to obtain the returned value of hP. If (m, rY_R) does not exist, B picks a random number $h\in Z_q$, inserts the tuple (m, rY_R, h) into the list, and computes the result of $V = hY_U = h(bP)$. B simulates H_2 (U, Y_R, rY_R) and computes the result of $Z = (m||bhP)\oplus H_2(U, Y_R, rY_R)$, and returns w=(U, Z) as the signcryption text on a message m with the receiver's public key Y_R and the sender's public key Y_U.

DSC simulation. For a signcryption text (U, Z) choosed by A, B checks if (U, Y_U, Q_i, v_i) exists in L_2, $0\leq i \leq q_{h2}$, such that $(m_i||V_i)= Z\oplus v_i$, for the corresponding elements (m_i, Q_i, h_i) in L_1 is such that V_i=h_ibP, then records the tuple (m_i, U, Y_U, V_i, Q_i, h_i). If one of them satisfies $e(P, Q_i)= e(U, Y_U)$ and $e(Y_{Si}, h_i)= e(P, V_i)$, then returns ($m_i$, U, V_i) to A as a signature pair with then sender's public key Y_{Si}. Else returns with 0.

After completing the first stage, A chooses two z-bits messages m_0 and m_1 together with an arbitrary sender's private x_S, asks a challenge signcryption text produced by B under receiver's public key Y_U. B sets the challenge signcryption text as w=(U, Z), where U=aP, Z is selected from $\{0, 1\}^{z+l}$ randomly. Then B picks $\underline{b}\in\{0, 1\}$randomly, adds the tuple ($m_{\underline{b}}$, ·) into L_1, picks $h\in Z_q$ randomly, produdces and records hP as the result of H_1 ($m_{\underline{b}}$, ·). Then, B produces and records v=$Z\oplus$ ($m_{\underline{b}}$|| hbP) in the list as the result of H_2 (U, Y_U, ·), sets V= hbP. Where "·" is symble to denote blank, it will be replaced by T if A queries H_2 (U, Y_U, T) later. At the same time, the conrrespoding value in L_1 will also be replaced. B returns w=(U, Z) to A. A couldn't determine that w is not a valid signcryption text unless he have asked the value of H_2 (aP, bP, abP).

A outputs $\underline{b'}\in\{0, 1\}$ as his guess of $\underline{b}$ after performing new queries as above. A has privelege to query all of messages accept w. B looks for (aP, bP, T) in the list L_2, such that $e(P, T)= e(aP, bP)$. If B could find a proper (aP, bP, T), he returns T as the solution of CDH problem. Otherwise, B stops and returns 0.

Analysis. If the simulated attack is computationally indistinguishable form a real attack, we say that B's simulation of B H_1, H_2, SC and DSC are perfect. Let E be the event that abP is queried on H_2 by A. In a real attack game, the probability of A wins will be $\Pr[\underline{b}=\underline{b'}] \leq \Pr[\underline{b}=\underline{b'}|\neg E]+\Pr[E] = 1/2+1/2\Pr[E]$, namely $e = 2\Pr[\underline{b} = \underline{b}']-1\leq \Pr[E]$.

The only event that causes the simulation is not peferct is that a valid signcryption text be rejected in designcryption query stage. It is the result of simulation of H_1 and H_2. For the queries on H_1, the probability is no more than $q_{H1} / 2^k$. For the queries on H_2 , the probability is no more than $q_{H2} / 2^{z+l}$. The totally probability is no more than $q_{DSC}(q_{H1} / 2^k + q_{H2} / 2^{z+l})$ for q_{DSC} designcryption queries. Hence, the probability of B wins is $e'\geq e - q_{DSC}(q_{H1} / 2^k + q_{H2} / 2^{z+l})$.

Then we evaluate the running time of B. We only consider the expensive operations, such as pairing evaluation and exponention. The running time of B includes that of A, 4 pairing evaluations in each designcryption query, 2 pairing evaluations and 2 exponentions in each signcryption query. It is easy to see, the running time of B is t'=t+$(4q_{DSC} +2q_{H2})t_b$+ $q_{H2}t_e$. Where t_b denotes the time required for one pairing evaluation, t_e denotes the time required for exponention. □

Lemma 3. In the random oracle model with secure parameter k, if there exists a forger F has non-negligible advantage r to forge a valid SC-BLS signcryption text when running in time t and performing q_{SC} signcryption queries and q_{Hi} queries to oracles H_i, i=1,2, then there is an algorithm E that solves the GDH problem in G_1 with probability $r' \geq r - (q_{H1}q_{SC} + 1)/2^k$ in time $t'=t + 2q_{SC}q_{H2}t_b+ (2q_{SC} + 2q_{SC}q_{H1})\, t_e$ Where t_b denotes the time required for one pairing evaluation, t_e denotes the time required for exponention.

Proof.

We assume that a forger F could forge a valid SC-BLS signcryption text with probability greater than r that within time t. We can construct an attacker E could solve the GDH problem. Suppose that E is given (P, aP, bP) as an instance of CDH. E runs F as a subroutine to find the solution of abP. F then adaptively performs hash queries, signcryption queries. To handle F's queries, E maintains two lists L_1 and L_2 to keep track of the answers given to oracle queries on H_1 and H_2.

Hash queries are simulated as follows.

H_1 simulation. When a hash query H_1 (m, P_1) is received, E checks if the query tuple (m, P_1, h) is already in L_1. If it exists, the result of hP is returned. Else, E picks a random number $h\in Z_q$, inserts the tuple (m, P_1, h) into list L_1 and returns the result of haP.

Hash oracle H_2 is simulated as in the proof of lemma 2.

Signcryption is simulated as follows.

SC simulation. For a signcryption query on (m, Y_R) choosed by F, E checks if $Y_R\notin G_1$or Y_R=Y_U, rejects it. Otherwise, E picks $r\in Z_q$ randomly, computes U =rP. Then E simulates H_1 (m, rY_R). If (m, rY_R) is aleady in L_1, E stops and outputs 0. Otherwise, E picks $h\in Z_q$ randomly, and sets the result of H_1 (m, rY_R) as hP. E simulates H_2 (U, Y_R, rY_R), computes the results of $V = hY_S$, $Z = (m||V)\oplus H_2(U, Y_R, rY_R)$, and returns w=(U, Z) as the signcryption text on a message m with the receiver's public key Y_R and the sender's public key Y_U.

After completing the first stage, F produces a signcryption text w'=(U', Z') and a pair of receipient's keys.

E performs the designcryption operation with secret key x_R. If w' is valid, E can recover the signature V', such that $e(P, V')$=$e(bP, haP)$. If F never query on the value of H_1 (m', rY_R) in the simulation process, namely (m', rY_R) is not in the list L_1, E

outputs 0 and stops. Otherwise, H_1 (m', rY_R, h) must exists in L_1, and be set as haP. It is easy to see $V'=tabP$. E can compute $abP=t^{-1}V$. E outputs abP and stops. Thus, E resolves the CDH problem.

Now we assess the probability of E's success. In signcryption query stage, the probability of E fails to responde is no more than $q_{H1}q_{SC}/2^k$, because each q_{SC} signcryption query includes q_{H1} queries. In designcryption stage, E has no chance to reject a valid signcrypiton text, because he performs a real designcryption operation. The probability of F produces a valid signcryption text without query is $1/2^k$. To sum up, the taltally probability of E solves abP is $r' \geq r - (q_{H1}q_{SC}+1)/2^k$.

The running time of E includes that of F, 2 exponentions in each signcryption query, 2 exponentions in H_1 query, 2 pairing evaluations in each H_2 query. Thus, the running time of E is $t'=t+2q_{SC}q_{H2}t_b+ (2q_{SC}+2q_{SC}q_{H1})t_e$. Where t_b denotes the time required for one pairing evaluation, t_e denotes the time required for exponention. □

5.3.3. Security of MSC-BLS

Theorem 4. In the random oracle model with secure parameter k, if an adversary B has non-negligible advantage against the IND-CCA2 security of n-recipient scheme MSC-BLS when running in time t and performing q_{SC} signcryption queries, q_{DSC} designcryption queries and q_{Hi} queries to oracles H_i, i=1,2, then there is an algorithm D that solves the GDH problem in G_1 with non-negligible probability. The advantage functions as follows.

$$\mathbf{Adv}^{\mathbf{mr-atk}}_{\mathbf{M\,\Sigma,B_{atk,}n}}(k) \leq n \cdot (\mathbf{Adv}^{\mathbf{GDH}}_{G_1,\mathbf{D}}(k) - q_{DSC}\,({q_{H1}}\big/{2^k} + {q_{H2}}\big/{2^{z+l}})$$

Theorem 4 can be proof by theorem1, lemma 1and lemma 2 easyly. Namely, MSC-BLS is semantic secure against IND-CCA2 in random oracle with assuming that the GDH problem is computational infeasible.

Theorem 5. In the random oracle model with secure parameter k, if there exists a forger F has non-negligible advantage to forge a valid SC-BLS signcryption text when running in time t and performing q_{SC} signcryption queries and q_{Hi} queries to oracles H_i, i=1,2, then there is an algorithm E that solves the GDH problem in G_1 with non-negligible probability. The advantage functions as follows.

$$\mathbf{Adv}^{\mathbf{mr-cma}}_{\mathbf{M\,\Sigma,F,n}}(k) \leq n \cdot (\mathbf{Adv}^{\mathbf{GDH}}_{G_1,\mathbf{E}}(k) - {(q_{H1}q_{SC}+1)}\big/{2^k}\ .$$

Theorem 5 can be proof by theorem 2, lemma 1 and lemma 3 directly. Namely, MSC-BLS is unforgeable against CMA in the random oracle with assuming that the GDH problem is computational infeasible.

5.4. Performance Analysis

The major advantage of multi-recipient signcryption scheme is cost(MΣ)<<$n$cost(Σ). Namely, it can reduce overheads efficiently, while keeping high level security.

We compared the major computational overheads and transmission overheads with other known schemes. In section 2.2, some known schemes are listed. All of them are SM-MR schemes. We evaluated the following schemes: Boyen's multipurpose identity-based signcryption [18] (denoted by Boyen), Duan and Cao's multi-receiver identity-based signcryption [19] (denoted by DC), Yu's identity-based signcryption [20] (denoted by YYHZ), Li's identity-based broadcast signcryption [21] (denoted by LXH). There are two MM-MR schemes as follows: trivial n-recipient scheme which runs SC-BLS repeatedly (denoted by n SC-BLS), and MSC-BLS. MM-MR schemes can also be used as SM-MR. We consider the costly operations which include pairing operation, exponentiation and inverse. Performances of above schemes sending 1 message to n recipients is listed in Table 1 and Table 2.

SM-MR has to perform n times when sending n different messages to n recipients. While, MM-MR just needs one time. Performances of above schemes sending n message to n recipients is listed in Table 3 and Table 4.

Table 1 Computational overheads comparison (1message-n recipients)

Schemes	Paring		Exp		Inv	
	SC	DSC	SC	DSC	SC	DSC
Boyen[18]	n^2	$4n^2$	$2n + 2n^2$	$2n^2$	0	n^2
DC[19]	n	$4n^2$	n^2+5n	n^2	0	$2n^2$
YYHZ[20]	n	$3n^2$	n^2+5n	n^2	0	n^2
LXH[21]	n	$3n^2$	n^2+3n	$2n^2$	0	0
n SC-BLS	0	$2n$	$2n$	n	0	0
MSC-BLS	0	$2n$	$n+1$	n	0	0

Table 2 Communication overheads comparison (1message-n recipients)

Schemes	Communication overheads
Boyen[18]	$2n\|G_1\|+\|m\|+\|ID\|$
DC[19]	$(n+3)\|G_1\|+\|m\|+\|ID\|$
YYHZ[20]	$(n+3)\|G_1\|+\|m\|+\|ID\|$
LXH[21]	$(n+2)\|G_1\|+\|m\|+\|ID\|$
n SC-BLS	$n(\|m\|+2\|G_1\|)$
MSC-BLS	$(n+1)\|G_1\|+\|m\|$

Table 3 Computational overheads comparison (n message-n recipients)

Schemes	Paring		Exp		Inv	
	SC	DSC	SC	DSC	SC	DSC
Boyen[18]	n	$4n$	$2+2n$	$2n$	0	n
DC[19]	1	$4n$	$n+5$	n	0	$2n$
YYHZ[20]	1	$3n$	$n+5$	n	0	n
LXH[21]	1	$3n$	$n+3$	$2n$	0	0
n SC-BLS	0	$2n$	$2n$	n	0	0
MSC-BLS	0	$2n$	$n+1$	n	0	0

Table 4 Communication overheads comparison (n message-n recipients)

Schemes	Communication overheads
Boyen[18]	$n[2n\|G_1\|+\|m\|+\|ID\|]$
DC[19]	$n[(n+3)\|G_1\|+\|m\|+\|ID\|]$
YYHZ[20]	$n[(n+3)\|G_1\|+\|m\|+\|ID\|]$
LXH[21]	$n[(n+2)\|G_1\|+\|m\|+\|ID\|]$
n SC-BLS	$n(\|m\|+2\|G_1\|)$
MSC-BLS	$(n+1)\|G_1\|+\|m\|$

Notes: 1. Paring denotes pairing operation, Exp denotes exponentiation, Inv denotes inverse, SC denotes signcryption operation, DSC denotes designcryption operation. 2. $|G_1|$ denotes the length of elements in G_1, $|m|$ denotes the length of message, $|ID|$ denotes the length of identity. 3. In EEH scheme, |KH| denotes the length of hash function KH, the length of block cipher is equal to $|m|$.

Remark 1. MSC-BLS compared with n SC-BLS. Overheads of MSC-BLS are reduced efficiently as n growing. In signcryption operation, computation overheads of MSC-BLS are half of that of n SC-BLS, communication overheads of MSC-BLS are 2/3 of that of n SC-BLS. The two schemes have the same totally computational overheads in designcryption operation. The two schemes have the same computational overheads and communication overheads as the underlying base signcryption scheme when n=1.

Remark 2. MSC-BLS compared with other identity-based schemes. In above schemes, Boyen, DC, LL, YYHZ and LXH are identity-based signcryption schemes which include plenty of paring operations. Obviously, MSC-BLS has few pairing operations, exponentiation and inverse operations. Thus, MSC-BLS is more efficient than others. When sending 1 message to n recipients, the communication overheads of MSC-BLS are slightly greater than others. But, when sending n messages, overheads of other schemes are n times than that of the schemes when sending 1 message. MSC-BLS has the same overheads when sending 1 message or n messages.

To sum up, MSC-BLS is the most efficient scheme as we known, especially used in the applications that sends different messages to distinct recipients.

6. Conclusion

In this paper, we investigated the efficiency and security of secure group communication. We present the result which provides a simple and reliable method to construct an efficient group communication scheme. If underlying base signcryption scheme is reproducible and semantic secure and unforgeable, then the corresponding randomness reusing multi-recipient signcryption scheme is secure too.

MSC-BLS proposed in this paper is a good scheme of MM-MR. It creates a possibility for the practice of the public key cryptosystem in ubiquitous computing.

References

1 Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) << cost(signature) + cost(encryption). In: Kaliski Jr. B.S. ed. Advances in Cryptology – CRYPTO' 1997. LNCS1294, Heidelberg: Springer-Verlag,1997, 165-179

2 Bao F, Deng RH. A signcryption scheme with signature directly verifiable by public key. In: Imai H., Zheng Y. ed. Public Key Cryptography' 98, LNCS 1431, Heidelberg: Springer-Verlag,1998, 55-59

3 Shin JB, Lee K, Shim K. New DSA-Verifiable signcryption schemes. In: Lee PJ, Lim CH eds. Proc. of ICISC'2002, Heidelberg: Springer-Verlag, 2003, 35-47

4 Malone-Lee J, Mao W. Two birds one stone: signcryption using RSA. In: Joye M ed. CT-RSA'2003. LNCS2612, Heidelberg: Springer-Verlag, 2003, 211-226

5 Han YL, Yang XY. New ECDSA-verifiable generalized signcryption, Chinese Journal of Computer, 2006, 29(11): 2003-2012 (in Chinese with English abstract).

6 Chen L, Malone-Lee J. Improved identity-based signcryption. In: Vaudenay S ed. Public Key Cryptography 2005, LNCS 3386, Heidelberg: Springer-Verlag, 2005, 362-379.

7 An JH, Dodis Y, Rabin T. On the security of joint signature and encryption. In: Knudsen L ed. Advances in Cryptology – EUROCRYPT' 2002, LNCS 2332, Heidelberg: Springer-Verlag, 2002, 83-107

8 Baek J, Steinfeld R, Zheng Y. Formal proofs for the security of signcryption. Journal of Cryptology, 2007, 20(2): 203-235

9 Han YL. Generalization of signcryption for resources-constrained environments. Wireless Communication and Mobile Computing, 2007, 7(7): 919-931

10 Håstad J. Solving simultaneous modular equations of low degree. SIAM J. on Computing, 1988, 17(2): 336-341

11 Baudron D, Stern JP. Extended notions of security for multicast public key cryptosystems. In: Montanari U, Rolim JDP, Welzl E eds. Proc. of the 27th International Colloquium on Automata, Languages and Programming (ICALP' 2000), LNCS 1853, Heidelberg: Springer-Verlag, 2000, 499-511

12 Bellare M, Boldyreva A, Micali S. Public-key encryption in a multi-user setting: Security proofs and improvements. In: Preneel B ed. Advances in Cryptology – EUROCRYPT' 2000, LNCS1807, Heidelberg: Springer-Verlag, 2000, 259~274

13 Kurosawa K. Multi-recipient public-key encryption with shortened ciphertext. In: Naccache D, Paillier P eds. Public Key Cryptography 2002, Heidelberg: Springer-Verlag, 2002, 48-63

14 ElGamal T. A public key cryptosystem and signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory, 1985, 31(4): 469-472

15 Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk H ed. Advances in Cryptology—CRYPTO' 98, LNCS 1462, Heidelberg: Springer-Verlag, 1998, 13-25

16 Bellare M, Boldyreva A, Staddon J. Randomness re-use in multi-recipient encryption scheme. In: Desmedt YG ed. Public Key Cryptography 2003, Heidelberg: Springer-Verlag, 2003, 85-99

17 Bellare M, Boldyreva A, Kurosawa Kand Staddon J. Multi-recipient encryption schemes: how to save on bandwidth and computation without sacrificing security. IEEE Transactions on Information Theory. 2007, 53(11), 3927-3943

18 Boyen X. Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography. In: Boneh D ed. Advances in Cryptology -CRYPTO'2003. LNCS 2729, Heidelberg: Springer-Verlag, 2003, 383-399

19 Duan SS, Cao ZF. Efficient and provably secure multi-receiver identity-based signcryption. In: Batten LM, Safavi-Naini R eds. ACISP' 2006. LNCS 4058, Heidelberg: Springer-Verlag, 2006, 195-206

20 Yu Y, Yang B, Huang XY, and Zhang MW. Efficient identity-based signcryption scheme for multiple receivers. In: Xiao B. et al. eds. ATC' 2007, LNCS 4610, Heidelberg: Springer-Verlag, 2007, 13~21

21 Li FG, Xin XJ, Hu YP. Indentity-based broadcast signcryption. Computer Standards & Interfaces. 2008, 30 (2): 89-94

22 Dodis Y. Signcryption(short survey). In: Tilborg V. Henk CA eds. Encyclopedia of Cryptography and Security, Berlin: Spinger-verlag, 2005

23 Bellare M, Rogaway P. Random oracle are practical: a paradigm for designing efficient protocols. In: Denning D, Pyle R, Ganesan R, Sandhu R and Ashby V eds. Proc. of the First ACM Conference on Computer and Communication Security, ACM, 1993, 62-73

24 Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing. In: Boyd C ed. ASIACRYPT'2001. LNCS 2248, Heidelberg: Springer-Verlag, 2001, 514-532

25 Libert B, Quisquater JJ. Efficient signcryption with key privacy from gap Diffie-Hellman groups. In: Bao F, Deng RH, Zhou J eds. PKC2004. LNCS 2947, Heidelberg: Springer-Verlag, 2004, 187-200

26 Tan CH. On the security of signcryption scheme with key privacy. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 2005, E88-A(4), 1093-1095

27 Yang G, Wong DS, Deng X. Analysis and improvement of a signcryption scheme with key privacy. In: Zhou J, Lopez J, Deng RH and Bao F eds. ISC'2005. LNCS 3650, Heidelberg: Springer-Verlag, 2005, 218-232

28 Tan CH. Analysis of improved signcryption scheme with key privacy. Information Processing Letters, 2006, 99(4):135-138

29 Li CK, Yang G, Wong DS, Deng X and Chow SM. An Efficient Signcryption Scheme with Key Privacy. In: Lopez J, Samarati P, Ferrer JL eds. EuroPKI'2007, LNCS 4582, Heidelberg: Springer-Verlag, 2007, 78-93