Cryptanalysis and Improvement of a Multi-Receiver Generalized Signcryption Scheme

Caixue Zhou*
School of Information Science and Technology, University of Jiujiang, JiuJiang 332005, P. R. China

Abstract. Generalized signcryption (GSC) scheme can adaptively work as an encryption scheme, a signature scheme or a signcryption scheme with only one algorithm. It is very suitable for storage-constrained environments. In this paper, we analyze a multi-receiver GSC scheme, and show that it cannot achieve indistinguishability-adaptive chosen ciphertext attack (IND-CCA2) secure in the pure encryption mode and hybrid encryption mode. We further propose a revised version of the scheme, which resolves the security issues of the original scheme without sacrificing its high efficiency and simple design. Our improved scheme can be proved to be IND-CCA2 secure and existentially unforgeable-adaptive chosen message attack (EUF-CMA) under computational Diffie-Hellman (CDH) assumption.

Keywords: generalized signcryption, multi-receiver generalized signcryption, adaptive chosen ciphertext attack, adaptive chosen message attack, random oracle model, randomness reusing

1. Introduction

In 1997, Zheng [1] proposed a novel concept named signcryption. The purpose of signcryption is to perform encryption and signature simultaneously, at lower computational costs and communication overheads than the usual sign-then-encrypt approach. Since then, many signcryption schemes have been proposed. However, in some applications, sometimes only message confidentiality or authenticity is needed. In this case, in order to ensure privacy or authenticity separately, signcryption must preserve sign module or encryption module, which will definitely increase the corresponding computation and implementation complexity and even will be infeasible in some resources-constrained environments such as embedded systems, sensor networks, and ubiquitous computing. Motivated by this, in 2006, Han et al. [2] proposed a new primitive called generalized signcryption, which can provide signcryption function when security and authenticity are required together, and can also provide encryption or signature function when one of them is required separately. Meanwhile they gave a GSC scheme based on ECDSA [3]. Wang

Corresponding author. E-mail address: charlesjjjx@126.com. Postal Address: School of Information Science and Technology, University of Jiujiang, JiuJiang 332005, China.

et al. [4] gave the first security model and improved the scheme proposed by [2]. The first identity-based generalized signcryption (ID-GSC for short) scheme along with a security model was proposed by Lal and Kushwah [5] in 2008. However, in 2010, Yu et al. [6] showed that the security model proposed by [5] is not complete, and they modified the security model and proposed a concrete scheme which is secure in this model. Later Kushwah and Lal [7] simplified the security model proposed by [6] and gave an efficient ID-GSC scheme. In addition, many other GSC schemes [8-17] have been proposed too, including PKI-based (public key infrastructure) schemes [8-10], identity-based schemes [11-12,17], certificateless schemes [13-16], multi-PKG (private key generator) scheme [17] and schemes in the standard model [15,17].

However all of the above mentioned schemes are suitable for one receiver scenario. In 2000, Bellare et al. [18], and Baudron et al. [19] independently formalized the concept of multi-receiver public key encryption. Their main result is that the security of public key encryption in the single-receiver setting implies the security in the multi-receiver setting. Hence, one can construct a semantically secure multi-receiver public key encryption scheme by simply encrypting a message under n different public keys of a semantically secure single-receiver public key encryption scheme. But the multi-receiver schemes of such structure will have n times computational costs than that of the base scheme. Later a novel technique called randomness reusing [20] was presented to enhance the efficiency. Randomness reusing is a novel technique to improve the efficiency of a multi-receiver encryption scheme, but not all randomness reusing-based multi-receiver encryption schemes are secure. Bellare et al. [21-22] proved that if the underlying base scheme is reproducible and semantically secure, then the corresponding randomness reusing-based multi-receiver encryption scheme is semantically secure too. Randomness reusing technique is also introduced to signcryption [23] and generalized signcryption [24] scenarios. Han and Gui [25] proved if the underlying base GSC scheme is reproducible and semantically secure, then the corresponding randomness reusing-based multi-receiver GSC scheme is semantically secure too.

In multi-receiver GSC setting, Han [8] first proposed a multi-receiver GSC scheme, but his scheme is a trivial n-receiver scheme that runs GSC repeatedly n times, which obviously is very inefficient. In 2008, Yang et al. [24] proposed a multi-receiver GSC scheme which used the technique of randomness reusing, but they did not give the security proof of their scheme. In 2009, Han and Gui [25] proposed a multi-receiver GSC scheme, their scheme is very efficient and they applied it for secure multicast in wireless network. In 2011, Zhou [26] proposed the first time an identity-based multi-receiver GSC scheme which also used the technique of randomness reusing.

In this paper, we show that Han and Gui's [25] base GSC scheme and

multi-receiver GSC scheme are insecure, their base GSC scheme is not IND-CCA2 [27] secure in the pure encryption mode, and thus their multi-receiver GSC scheme is not IND-CCA2 secure in the pure encryption mode and hybrid encryption mode. Then we give an improvement of their scheme, interestingly, the improved scheme is more secure than the original one while still maintaining its efficiency. The confidentiality and existential unforgeability of the improved scheme can be proved under the CDH assumption. Compared with other multi-receiver signcryption schemes, our improved scheme enjoys shorter ciphertext length and less operation costs like the original scheme.

In the next section, some preliminaries are reviewed. In section 3, we start with the description of Han-Gui's scheme, and give an attack on the scheme. In Section 4, we give an improvement of their scheme, and the security and performance analysis of the improved scheme. We conclude the paper in Section 5.

2. Preliminaries

2.1. Some definitions

Definition 1. Bilinear pairings.
Let $k \in N$ be a security parameter and q be a k bits prime. We consider groups G_1 and G_2 of the same prime order q. A bilinear map $e: G_1 \times G_1 \to G_2$ 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 $e(P, Q)$, for all $P, Q \in G_1$.

Definition 2. The Computational Diffie-Hellman problem.
The Computational Diffie-Hellman problem (CDH) in G_1 is to compute abP from $< P, aP, bP >$ for unknown randomly chosen $a, b \in Z_q$.

The advantage of any probabilistic polynomial time(PPT) algorithm G in solving CDH problem in G_1 is defined to be: $ADV_G^{CDH} = \Pr[G(P, aP, bP) = abP : a, b \in Z_q^*]$.

CDH assumption: For every PPT algorithm G, ADV_G^{CDH} is negligible.

2.2. Framework of multi-receiver generalized signcryption scheme

A multi-receiver GSC scheme consists of the following three algorithms.

(1) Setup algorithm: Given a secure parameter k, it generates the system public parameters. $(SK_X, PK_X) \leftarrow Gen(X, 1^k)$ is a key generation algorithm and produces the private key SK_X and the public key PK_X for the user X.

(2) Generalized signcryption algorithm: $\sigma \leftarrow GSC(M, SK_S, PK_{R_1}, PK_{R_2}, ..., PK_{R_n})$ is a probabilistic algorithm, and takes the private key SK_S of the sender S, the public keys $\{PK_{R_i}, i = 1, ..., n\}$ of the receivers and messages $M = \{m_i, i = 1, ..., n\}$

σ.

This algorithm has 5 scenarios:

- Pure signcryption mode: if the sender and all of the receivers are determined, it runs in this mode, the ciphertext is $\sigma \leftarrow GSC(M, SK_S, PK_{R_1}, PK_{R_2}, ..., PK_{R_n}) = signcrypt(M, SK_S, PK_{R_1}, PK_{R_2}, ..., PK_{R_n})$.
- Pure signature mode: if all of the receivers are vacant and the sender is determined, it runs in this mode, the ciphertext is $\sigma \leftarrow GSC(M, SK_S, \phi_{R_1}, \phi_{R_2}, ...\phi_{R_n}) = sign(M, SK_S)$. ϕ means the user is vacant.
- Pure encryption mode: if the sender is vacant and all of the receivers are determined, it runs in this mode, the ciphertext is $\sigma \leftarrow GSC(M, \phi_S, PK_{R_1}, PK_{R_2}, ..., PK_{R_n}) = encrypt(M, PK_{R_1}, PK_{R_2}, ..., PK_{R_n})$.
- Hybrid signcryption mode: if some of the receivers are vacant, and the rest of receivers and the sender are determined, it runs in this mode. For the determined receivers, the ciphertext σ is a signcryption ciphertext; for the vacant receivers, the ciphertext σ is a signature.
- Hybrid encryption mode: if some of the receivers and the sender are vacant, it runs in this mode. For the determined receivers, the ciphertext σ is an encryption ciphertext; for the vacant receivers, the ciphertext is a plaintext, it takes no secure policy.

(3) De-generalized signcryption algorithm: $m_i \cup \{\perp\} \leftarrow DGSC(\sigma_i, SK_{R_i}, PK_S)$ is a deterministic designcryption algorithm and takes the public key PK_S of the sender S, the private key SK_{R_i} of the receiver R_i, and a ciphertext $\sigma_i \in \sigma (i = 1, ..., n)$, to return the message m_i or an invalid symbol $\perp$.

This algorithm has 5 scenarios:

- Pure signcryption mode: $DGSC(\sigma_i, SK_{R_i}, PK_S) = unsigncrypt(\sigma_i, SK_{R_i}, PK_S)$.
- Pure signature mode: $DGSC(\sigma_i, \phi_{R_i}, PK_S) = verify(\sigma_i, PK_S)$.
- Pure encryption mode: $DGSC(\sigma_i, SK_{R_i}, \phi_S) = decrypt(\sigma_i, SK_{R_i})$.
- Hybrid signcryption mode: For the determined receivers, $DGSC(\sigma_i, SK_{R_i}, PK_S) = unsigncrypt(\sigma_i, SK_{R_i}, PK_S)$; for the vacant receivers, $DGSC(\sigma_i, \phi_{R_i}, PK_S) = verify(\sigma_i, PK_S)$.
- Hybrid encryption mode: For the determined receivers, $DGSC(\sigma_i, SK_{R_i}, \phi_S) = decrypt(\sigma_i, SK_{R_i})$; for the vacant receivers, the ciphertext is the plaintext, it takes no secure policy.

For consistency, we require $DGSC(GSC(M, SK_S, PK_{R_1}, PK_{R_2}, ..., PK_{R_n}), SK_{R_i}, PK_S) = m_i$ for $i = 1, 2, ..., n$. $M = \{m_i, i = 1, ..., n\}$.

If all of the identities are vacant, it takes no secure policy. Above five modes are transparent to applications, namely, the algorithm can produce the specific outputs according to identities of the sender and the receivers adaptively. Applications need not care about which mode should be taken.

2.3 Security model of multi-receiver generalized signcryption scheme

The security notions for signcryption scheme are indistinguishability against adaptive chosen ciphertext attack (IND-SC-CCA2) and existential unforgeability against adaptive chosen message attack (EUF-SC-CMA). We

modify these definitions to adapt for the multi-receiver GSC scheme. Namely, a multi-receiver GSC scheme should satisfy confidentiality (IND-MGSC-CCA2) and unforgeability (EUF-MGSC-CMA).

Definition 3. A multi-receiver GSC scheme is said to be IND-MGSC-CCA2 secure if no probabilistic polynomial time adversary A has a non-negligible advantage in the following game.

(1) The challenger C runs Setup algorithm to generate the system public parameters and to generate multiple key pairs $(SK^*_{U_i}, PK^*_{U_i})(i=1,...,n)$. $SK^*_{U_i}$ is kept secret while $PK^*_{U_i}$ is given to adversary A. These key pairs are the challenge key pairs. (Note: some of the key pairs can be null, it means the user is vacant. At least one key pair is not null.)

(2) **Phase 1:** A makes polynomially bounded number of queries to the following oracles.

(a) GSC Oracle — A produces messages $M=\{m_i, i=1,...,n\}$ and n arbitrary public keys $PK_{R_i}(i=1,...,n)$ and requires the result of the operation $\sigma = GSC(M, SK^*_{U_j}, PK_{R_1},...,PK_{R_n})$ for an attacked user's private key $SK^*_{U_j}(j\in[1,n])$. Challenger C runs GSC algorithm and returns the output σ to A.

(b) DGSC Oracle — A produces a ciphertext σ, an arbitrary public key PK_S of the sender and requires the result of $DGSC(\sigma, SK^*_{U_j}, PK_S)$ for the attacked users's private key $SK^*_{U_j}(j\in[1,n])$. C runs $DGSC$ algorithm and returns the output of $DGSC$ to A.

Thses queries can be asked adaptively.

(3) **Challenge**: A produces two message vectors $M^*_0=\{m^*_{0i}, i=1,...,n\}$, $M^*_1=\{m^*_{1i}, i=1,...,n\}$, an arbitrary private key SK^*_S, B flips a coin $b\leftarrow\{0,1\}$ to compute a ciphertext $\sigma^* = GSC(M^*_b, SK^*_S, PK^*_{U_1},...,PK^*_{U_n})$ under the attacked users's public keys $PK^*_{U_j}(j\in[1,n])$. B returns σ^* to A as a challenge.

(4) **Phase 2:** A is allowed to make polynomially bounded number of new queries as in phase 1 with the restriction that A should not query the $DGSC(\sigma^*, SK^*_{U_j}, PK^*_S)(j\in[1,n])$.

(5) **Guess**: At the end of this game, A outputs a bit b_0. A wins the game if $b_0 = b$.

The advantage of the adversary A is defined as follows: $Adv^{IND-MGSC-CCA2}(A) := 2\Pr[b_0 = b]-1$.

Note: In confidentiality game, it is only need to consider pure encryption mode, hybrid encryption mode, pure signcryption mode and hybrid signcryption mode with determined receivers. In the above challenge stage, the sender S can be vacant. In this case, algorithm runs in pure encryption mode or hybrid encryption mode, otherwise it runs in pure signcryption mode or hybrid signcryption mode. Because in the hybrid signcryption mode with vacant receivers, only signatures are made, it needs not to consider the IND-MGSC-CCA2 security. So these modes share the same game except in the hybrid signcryption mode with vacant receivers.

Definition 4. A multi-receiver GSC scheme is said to be EUF-MGSC-CMA secure if no probabilistic polynomial time adversary A has a non-negligible advantage in the following game.

(1) The challenger C runs Setup algorithm to generate the system public parameters and to generate a key pair (SK_S^*, PK_S^*). SK_S^* is kept secret while PK_S^* is given to adversary A. The key pair can not be null and is considered as the challenge key pair. Because in the pure signature mode, pure signcryption mode or hybrid signcryption mode, the sender can not be vancant.

(2) **Attack:** A can adaptively perform queries to the same oracles as those defined in Definition 3.

(3) **Forgery:** At the end of the game, A produces a ciphertext σ^* and n arbitrary receivers's key pairs $(SK_{R_i}^*, PK_{R_i}^*)(i = 1,...,n)$. A wins the game if the result of $DGSC(\sigma^*, PK_S^*, SK_{R_i}^*)(i \in [1,n])$ is a valid message m_i^* under the attacked user's public key PK_S^* and the i-th receiver's secret key $SK_{R_i}^*$, and σ^* is not the output of $GSC(M^*, SK_S^*, PK_{R_1}^*,..., PK_{R_n}^*)$, $M^* = \{m_1^*, m_2^*,..., m_n^*\}$. A's advantage is its probability of victory.

Note: In unforgeability game, it is only need to consider pure signature mode, pure signcryption mode and hybrid signcryption mode. In the above forgery stage, part or all of the receivers R_i^* can be vacant. In that case, algorithm runs in hybrid signcryption mode or pure signature mode, otherwise it runs in pure signcryption mode, so these modes share the same game.

3. Han-Gui's scheme and its security analysis

According to the result of Bellare et al. [21-22], if the underlying base scheme is reproducible and semantically secure, then the corresponding randomness reusing-based multi-receiver encryption scheme is semantically secure too. Han-Gui [25] extended the result to multi-receiver GSC setting, and proved that if the underlying base GSC scheme is reproducible and semantically secure, then the corresponding randomness reusing-based multi-receiver GSC scheme is semantically secure too. So, Han-Gui presented an underlying base GSC scheme first, and then they proved the base GSC scheme is reproducible and semantically secure, and concluded their multi-receiver GSC scheme is semantically secure.

3.1. Han-Gui's base generalized signcryption scheme.

The base scheme is a GSC scheme suitable for one receiver and comes from the BLS signature [28]. The base scheme is given as follows.

Parameters: Let k be a secure parameter, q be a k bits prime, and G_1 be a bilinear group with order q. P is a generator of group G_1. Elements on G_1 have the length of l bits. $H_1 : \{0,1\}^z \times G_1 \to G_1$ and $H_2 : G_1^3 \to \{0,1\}^{z+l}$ are two hash functions that can be regarded as random oracles.

Identification function: To identify the different cases and get adaptive outputs, we define the identification function $f(P)$. When $P = O$, $f(P) = 0$, else $f(P) = 1$, where $P \in G_1$ is a user's public key. $O \in G_1$ is the zero element.

Gen: It takes the secure parameter k and users' identities to produce keys. For the sender S, his keys are $(x_S, Y_S) \leftarrow Gen(S, 1^k)$, where $x_S \in_R Z_q$ and

$Y_S = x_S P \in G_1$. For the receiver R, his keys are $(x_R, Y_R) \leftarrow Gen(R, 1^k)$, where $x_R \in_R Z_q$ and $Y_R = x_R P \in G_1$. If $S \in \phi$ (an vacant user), $(0, O) \leftarrow Gen(S, 1^k)$. If $R \in \phi$, $(0, O) \leftarrow Gen(R, 1^k)$.

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

1. Picks a random coin $r \in_R Z_q$ and computes $U = rP \in G_1$.
2. Computes $V = x_S H_1(m, rY_R) \in G_1$.
3. Computes $Z = (m \| V) \oplus (H_2(U, Y_R, rY_R) f(Y_R)) \in \{0,1\}^{z+l}$.

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

DGSC: When receiving $\sigma = (U, Z)$, the receiver R performs the steps below.

1. Computes $H_2(U, Y_R, x_R U) \in \{0,1\}^{z+l}$.
2. Computes $(m \| V) = Z \oplus (H_2(U, Y_R, x_R U) f(Y_R))$.
3. If $V = O$, returns the message m, else computes $h = H_1(m, x_R U) \in G_1$ and then checks if $e(Y_S, h) = e(P, V)$. If this condition does not hold, rejects the ciphertext.

- Pure signcryption mode: If the sender and the receiver are determined, it runs in this mode. Now, $x_S \neq 0,\ f(Y_R) = 1$, the *GSC* and *DGSC* algorithms are the same as above.
- Pure encryption mode: If the sender is vacant and the receiver is determined, it runs in this mode. Now, $x_S = 0,\ f(Y_R) = 1$, so, $V = x_S H_1(m, rY_R) = O$, $Z = (m \| O) \oplus H_2(U, Y_R, rY_R)$, message m can be recovered by $(m \| O) = Z \oplus H_2(U, Y_R, x_R U)$.
- Pure signature mode: If the receiver is vacant and the sender is determined, it runs in this mode. Now, $x_S \neq 0,\ f(Y_R) = 0$, so, $V = x_S H_1(m, O)$, $Z = (m \| V) \oplus (H_2(U, Y_R, rY_R) f(Y_R)) = m \| V$, the signature can be verified by checking $e(Y_S, H_1(m, O)) = e(P, V)$.

If all of the identities are absent, it takes no secure policy. The three modes are transparent to applications, namely, the algorithm can produce the specific outputs according to the identities of the sender and the receiver adaptively. Applications need not care about which mode should be taken.

3.2. Han-Gui's multi-receiver generalized signcryption scheme

A sender S sends z bits message vector $M = \{m_i \mid m_i \in \{0,1\}^z, i = 1, ..., n\}$ to intended receivers $R_i (i = 1, ..., n)$, and then broadcasts the aggregated signcryption text. A receiver R_i gets his signcryption text and designcrypts it.

Parameters and **Identification function** are the same as above.

Gen: It takes the secure parameter k and users' identities to produce keys. For the sender S, his keys are $(x_S, Y_S) \leftarrow Gen(S, 1^k)$, where $x_S \in_R Z_q$ and $Y_S = x_S P \in G_1$. For the receiver $R_i (i = 1, ..., n)$, his keys are $(x_{R_i}, Y_{R_i}) \leftarrow Gen(R_i, 1^k)$, where $x_{R_i} \in_R Z_q$ and $Y_{R_i} = x_{R_i} P \in G_1$. If $S \in \phi$ (an vacant user), $(0, O) \leftarrow Gen(S, 1^k)$. If $R_i \in \phi$, $(0, O) \leftarrow Gen(R_i, 1^k)$.

GSC: To signcrypt message vector $M = \{m_i \mid m_i \in \{0,1\}^z, i = 1, ..., n\}$, S performs the following operations.

1. Picks a random coin $r \in_R Z_q$ and computes the commitment $U = rP \in G_1$.

2. For $i = 1,...,n$

(a) Computes $V_i = x_S H_1(m_i, rY_{R_i}) \in G_1$.

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

EndFor

3. The ciphertext vector is given by $\sigma = (U, Z_1, ..., Z_n)$ which is sent to the group via a broadcast channel.

DGSC: When receiving σ, the receiver R_i gets his signcryption text $\sigma_i = (U, Z_i)$ and performs the following steps.

1. Computes $H_2(U, Y_{R_i}, x_{R_i} U)$.

2. Computes $(m_i \| V_i) = Z_i \oplus (H_2(U, Y_{R_i}, x_{R_i} U) f(Y_{R_i}))$.

3. If $V_i = O$, returns the message m_i, else computes $h_i = H_1(m_i, x_{R_i} U) \in G_1$ and then checks if $e(Y_S, h_i) = e(P, V_i)$. If this condition does not hold, rejects the ciphertext.

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

- Pure signcryption mode: If the sender and all of the receivers are determined, it runs in this mode. Now, $x_S \neq 0,\ f(Y_{R_i}) = 1$, the ciphertext vector $\sigma = (U, Z_1, ..., Z_n)$ is a signcryption ciphertext vector, the *GSC* and *DGSC* algorithms are the same as above.
- Pure encryption mode: If the sender is vacant and all of the receivers are determined, it runs in this mode. Now, $x_S = 0,\ f(Y_{R_i}) = 1$, so, $V_i = x_S H_1(m_i, rY_{R_i}) = O$, $Z_i = (m_i \| O) \oplus H_2(U, Y_{R_i}, rY_{R_i})$, the ciphertext vector $\sigma = (U, Z_1, ..., Z_n)$ is a encryption ciphertext vector, message m_i can be recovered by $(m_i \| O) = Z_i \oplus H_2(U, Y_{R_i}, x_{R_i} U)$.
- Pure signature mode: If all of the receivers are vacant and the sender is determined, it runs in this mode. Now, $x_S \neq 0,\ f(Y_{R_i}) = 0$, so, $V_i = x_S H_1(m_i, O)$, $Z_i = (m_i \| V_i) \oplus (H_2(U, Y_{R_i}, rY_{R_i}) f(Y_{R_i})) = m_i \| V_i$, the ciphertext vector $\sigma = (U, Z_1, ..., Z_n)$ is a signature vector, the signature can be verified by checking $e(Y_S, H_1(m_i, O)) = e(P, V_i)$.
- Hybrid signcryption mode: If some of the receivers are vacant, and the rest of receivers and the sender are determined, the scheme runs in this mode. For the determined receivers, $x_S \neq 0,\ f(Y_{R_i}) = 1$, the ciphertext vector $\sigma = (U, Z_i),\ for\ f(Y_{R_i}) = 1$ is a signcryption ciphertext vector, and the procedure is the same as pure signcryption mode; for the vacant receivers, $x_S \neq 0,\ f(Y_{R_i}) = 0$, the ciphertext vector $\sigma = (U, Z_i),\ for\ f(Y_{R_i}) = 0$ is a signature vector, the procedure is the same as pure signature mode.
- Hybrid encryption mode: If some of the receivers and the sender are vacant, it runs in this mode. For the determined receivers, $x_S = 0,\ f(Y_{R_i}) = 1$, the ciphertext vector $\sigma = (U, Z_i),\ for\ f(Y_{R_i}) = 1$ is a encryption ciphertext vector, and the procedure is the same as pure encryption mode; for the vacant receivers, $x_S = 0,\ f(Y_{R_i}) = 0$, the ciphertext vector $\sigma = (U, Z_i)$,

$for\ f\ Y_{R_i} =$ is a plaintext vector, it takes no secure policy.

The five modes are transparent to applications, namely, the algorithm can produce the specific outputs according to identities of the sender and the receivers adaptively. Applications need not care about which mode should be taken.

3.3 An attack on Han-Gui's base GSC scheme running in the pure encryption mode

The security of Han-Gui's multi-receiver GSC scheme relies on their base GSC scheme. In the following, we will prove that Han-Gui's base GSC scheme is not IND-CCA2 secure in the pure encryption mode. So their multi-receiver GSC scheme is insecure. Now we give an attack on the base GSC scheme running in the pure encryption mode as follows.

Notice that in the pure encryption mode, $V = O$. Now assume that given the challenge receiver's public key Y_R^*, the adversary A chooses two equal length messages m_0^* and m_1^* and sends them to the challenger. The challenger then chooses a random $b \in \{0,1\}$ and computes the challenge ciphertext of the message m_b^* as $\sigma^* = (U^*, Z^*)$ under the challenge public key Y_R^*. Upon receipt of the challenge ciphertext $\sigma^* = (U^*, Z^*)$, A chooses a random message $\overline{m}$, whose length is equal to that of m_0^*, and computes $\overline{Z} = Z^* \oplus (\overline{m} \| O)$. Finally, the adversary A sends the ciphertext $\overline{\sigma} = (U^*, \overline{Z})$ to the challenger for decryption, obviously the challenger will return $\overline{m} \oplus m_b^* \| O$ as the response, knowing the $\overline{m}$, A can get the m_b^*. Therefore, the base GSC scheme is not IND-CCA2 secure in the pure encryption mode and thus the Han-Gui's multi-receiver GSC scheme is not IND-CCA2 secure in the pure encryption mode and hybrid encryption mode.

4 An improved multi-receiver generalized signcryption scheme

4.1. An improved base generalized signcryption scheme

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

1. Computes $f(Y_S), f(Y_R)$.
2. Picks a random coin $r \in_R Z_q$ and computes $U = rP \in G_1$.
3. Computes $H = H_1(m, rY_R) \in G_1, V = x_S H \in G_1$.
4. If $f(Y_S) = 0$, computes $Z = (m \| H) \oplus (H_2(U, Y_R, rY_R) f(Y_R)) \in \{0,1\}^{z+l}$
   else computes $Z = (m \| V) \oplus (H_2(U, Y_R, rY_R) f(Y_R)) \in \{0,1\}^{z+l}$.

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

DGSC: When receiving $\sigma = (U, Z)$, the receiver R performs the steps below.

1. Computes $f(Y_S), f(Y_R)$.
2. If $f(Y_S) = 0$, computes $(m \| H) = Z \oplus (H_2(U, Y_R, x_R U) f(Y_R))$;
   else computes $(m \| V) = Z \oplus (H_2(U, Y_R, x_R U) f(Y_R))$

3. Computes $h = H_1(m, x_R U) \in G_1$

4. If $f(Y_S) = 0$, checks if $H = h$;

if this condition does not hold, rejects the ciphertext;

else returns m;

else checks if $e(Y_S, h) = e(P, V)$;

if this condition does not hold, rejects the ciphertext;

else returns m.

4.2 An improved multi-receiver generalized signcryption scheme

GSC: To signcrypt message vector $M = \{m_i \mid m_i \in \{0,1\}^z, i = 1,...,n\}$, S performs the following operations.

1. Computes $f(Y_S)$, $f(Y_{R_i})$, $i = 1,...n$.

2. Picks a random coin $r \in_R Z_q$ and computes the commitment $U = rP \in G_1$.

3. For $i = 1,...n$

(a) Computes $H_i = H_1(m_i, rY_{R_i}) \in G_1, V_i = x_S H_i \in G_1$.

(b) If $f(Y_S) = 0$, computes $Z_i = (m_i \| H_i) \oplus (H_2(U, Y_{R_i}, rY_{R_i}) f(Y_{R_i})) \in \{0,1\}^{z+l}$.

else computes $Z_i = (m_i \| V_i) \oplus (H_2(U, Y_{R_i}, rY_{R_i}) f(Y_{R_i})) \in \{0,1\}^{z+l}$

EndFor

4. The ciphertext vector is given by $\sigma = (U, Z_1, ..., Z_n)$ which is sent to the group via a broadcast channel.

DGSC: When receiving σ, the receiver R_i gets his signcryption text $\sigma_i = (U, Z_i)$ and performs the following steps.

1. Computes $f(Y_S), f(Y_{R_i})$, $i \in [1, n]$.

2. If $f(Y_S) = 0$, computes $(m_i \| H_i) = Z_i \oplus (H_2(U, Y_{R_i}, x_{R_i} U) f(Y_{R_i}))$

else computes $(m_i \| V_i) = Z_i \oplus (H_2(U, Y_{R_i}, x_{R_i} U) f(Y_{R_i}))$.

3. Computes $h_i = H_1(m_i, x_{R_i} U) \in G_1$

4. If $f(Y_S) = 0$, checks if $H_i = h_i$;

if this condition does not hold, rejects the ciphertext;

else returns m_i;

else checks if $e(Y_S, h_i) = e(P, V_i)$;

if this condition does not hold, rejects the ciphertext;

else returns m_i.

4.3 Security analysis

We have showed Han-Gui's underlying base GSC scheme is not semantically secure in paragraph 3.3, so their multi-receiver GSC scheme is not semantically secure either. The essence of their base GSC scheme being insecure is as follows. Note that in the pure signcryption mode of their base GSC scheme, the V part is not null, which intuitively makes it achives IND-CCA2 secure in the confidentiality game, and in the pure encryption mode, the V part is null, so the attacker can modify the challenge ciphertext to dechipher oracle to get the plaintext. In the improved base GSC scheme, we

use the H part to replace V part to concatenate message m in the pure encryption mode, which intuitively can make it achives IND-CCA2 secure.

About the security of the improved multi-receiver GSC scheme, we have the following two theorems. In proving the following two theorems, we reference the method adopted by [23,29-31]. Their schemes all use the randomness reusing technique and they directly demonstrate their multi-receiver signcryption schemes rather than rely on a base signcryption scheme. This method is different from Han and Gui's [25].

Theorem 1. In the random oracle model with secure parameter k, if an adversary A has non-negligible advantage ε against the IND-MGSC-CCA2 security of the improved multi-receiver GSC scheme running in the pure encryption mode, hybrid encryption mode, pure signcryption mode or hybrid signcryption mode with determined receivers, A runs in time t and performs q_{GSC} GSC queries, q_{DGSC} $DGSC$ queries and q_{H_i} queries to oracles $H_i (i = 1,2)$, then there exists an algorithm B that solves the CDH problem in G_1 with a probability $\varepsilon' \geq \varepsilon - (q_{H_2} q_{DGSC} / 2^k)$ in a time $t' \leq t + (2q_{DGSC} + 2q_{H_2})t_e$, where t_e denotes the time required for one pairing computation.

Proof: We show how to build an algorithm B that solves the CDH problem by running the adversary A as a subroutine. On input $(P, aP, b_i P), (i = 1,2,...,n)$, B's goal is to compute one of the $ab_i P, (i = 1,2,...,n)$. B sets $Y_{R_i}^* = b_i P$ as the challenge public keys, and gives these public keys to adversary A. Here some of the key pairs can be null, namely, $b_i = 0, Y_{R_i}^* = O$ for some i, it means the user is vacant. At least one key pair is not null.

Phase 1: A performs a first series of queries of the following kinds that are handled by B as explained below:

Simulator: H_1, H_2

B maintains lists L_1, L_2, which keep track of the answers given to oracle queries on H_1, H_2. Upon a query on H_i, B first scans in the list L_i to check whether H_i is already defined for that input. If it is, the previously defined value is returned. Otherwise, B picks a random element from the output range of H_i, returns it to A and stores the input and output values in L_i.

Simulator: $GSC(M, x_S, Y_{U_1}, Y_{U_2}, ..., Y_{U_n})$

A produces a message vector $M = \{m_i, i = 1,...,n\}$ and n arbitrary public keys $Y_{U_i} (i = 1,...,n)$ and requires the result of the operation $\sigma = GSC(M, x_S, Y_{U_1}, ..., Y_{U_n})$.

- If the public key of the sender Y_S is not one of the target public keys $b_i P, i \in [1,n]$, B just runs GSC algorithm as nomal because B knows the private key of the sender.
- If the public key of the sender Y_S is one of the target public keys $b_i P, i \in [1,n]$, then B proceeds as follows:
  - Computes $f(Y_S)$, $f(Y_{U_j})$, $j = 1,...,n$.
  - Chooses $r \in_R Z_q$, computes $U = rP$.
  - Queries $h_{1j} P = O_{H_1}(m_j, rY_{U_j})$, computes $V_j = x_S h_{1j} P = h_{1j} b_i P$ for $j = 1,...,n$.

- Queries $h_{2j} = O_{H_2}(U, Y_{U_j}, rY_{U_j})$.
- If $f(Y_S) = 0$, computes $Z_j = (m_j \| h_{1j}P) \oplus (h_{2j} f(Y_{U_j}))$ for $j = 1,...,n$. Else $Z_j = (m_j \| V_j) \oplus (h_{2j} f(Y_{U_j}))$ for $j = 1,...,n$.
- The ciphertext vector is $\sigma = (U, Z_1,..., Z_n)$, which is returned to A.

Simulator: $DGSC(\sigma, x_{R_i}, Y_S)$

A produces a ciphertext $\sigma = (U, Z_1,..., Z_n)$, an arbitrary public key Y_S of the sender and requires the result of $DGSC(\sigma, x_{R_i}, Y_S)$ for $i \in [1,n]$.

- If the public key of the receiver Y_{R_i} is not the target public key $b_i P$, $i \in [1,n]$, B just runs the $DGSC$ algorithm as nomal because B knows the private key of the receiver.
- If the public key of the receiver Y_{R_i} is the target public key $b_i P$, $i \in [1,n]$, then B proceeds as follows:
  - Computes $f(Y_S)$, $f(Y_{R_i})$, $i \in [1,n]$.
  - If $f(Y_S) = 0$, B iterates in L_2 for each item h_2, computes $(m_i \| H_i) = Z_i \oplus (h_2 f(Y_{R_i}))$, then checks if m_i is in L_1; if not, moves to the next item of L_2 and begins again, else retrieves $h_{1i}P$, and checks if $H_i = h_{1i}P$; if not, move to the next item of L_2 and begins again, else returns m_i and stop. If going through L_2, no m_i returns, then returns an invalid symbol $\perp$.
  - If $f(Y_S) = 1$, B iterates in L_2 for each item h_2, computes $(m_i \| V_i) = Z_i \oplus (h_2 f(Y_{R_i}))$, then checks if m_i is in L_1; if not, moves to the next item of L_2 and begins again, else retrieves $h_{1i}P$, and checks if $e(Y_S, h_{1i}P) = e(P, V_i)$; if not, move to the next item of L_2 and begins again, else returns m_i and stop. If going through L_2, no m_i returns, then returns an invalid symbol $\perp$.

Challenge: A produces two message vectors $M_0 = \{m_{0_i}, i = 1,...,n\}$, $M_1 = \{m_{1_i}, i = 1,...,n\}$, an arbitrary private key x_S^*, and requires the GSC ciphertext on one of the two message vectors with the receiver public keys are the challenge public keys $b_i P$, $i = 1,...,n$. B then sets $U^* = aP$, chooses $\{Z_1^*, Z_2^*,..., Z_n^*\} \in_R \{0,1\}^{z+l}$ and sends the challenge ciphertext $\sigma^* = (U^*, Z_1^*,..., Z_n^*)$ to A.

Phase 2: A performs new queries as in phase 1 with the restriction that A should not query the $DGSC(\sigma^*, x_{R_i}^*, Y_S^*)$.

At the end of the game, A returns a guess. A cannot realize that σ^* is not a valid ciphertext unless A asks for one of the hash value $H_2(U^*, Y_{R_i}^*, aY_{R_i}^*) = H_2(aP, b_i P, ab_i P)$, $(i = 1,2,...,n)$, for which $b_i \neq 0$. B ignores A's answer and looks into the list L_2 for tuples of the form $(aP, b_i P, X, .)$. For each of them, B checks whether $e(P, X) = e(aP, b_i P)$, if this relation holds, B stops and outputs X as the solution of the CDH problem. If no tuple of this kind satisfies the above equality, B stops and outputs invalid.

Now, we assess the probability that the simulation is not perfect. The only case where it can happen is when a valid ciphertext is rejected in a $DGSC$ query. It is easy to see that for every item in L_2, there is exactly one item in L_1 providing a valid ciphertext. The probability to reject a valid ciphertext is

thus not greater than $q_{H_2}/2^k$. Since A makes total q_{DGSC} queries during the attack, so we have $\varepsilon' \geq \varepsilon - (q_{H_2} q_{DGSC}/2^k)$. Moreover, the bound on B's computation time derives from the fact that every $DGSC$ query requires two pairing evaluations while the extraction of the solution from L_2 implies to compute at most $2q_{H_2}$ pairings.

Note: In the above challenge stage, the sender S can be vacant. In this case, algorithm runs in pure encryption mode or hybrid encryption mode, otherwise it runs in pure signcryption mode or hybrid signcryption mode, so these modes share the same game except in the hybrid signcryption mode with vacant receivers. Because in the hybrid signcryption mode with vacant receivers, only signatures are made, it needs not to consider the IND-MGSC-CCA2 security.

Theorem 2. In the random oracle model with secure parameter k, if there exists a forger F with non-negligible advantage ε against the EUF-MGSC-CMA security of the improved multi-receiver GSC scheme running in the pure signature mode, pure signcryption mode or hybrid signcryption mode, F runs in time t and performs q_{GSC} GSC queries, q_{DGSC} $DGSC$ queries and q_{H_i} queries to oracles $H_i (i = 1,2)$, then there exists an algorithm B that solves the CDH problem in G_1 with a probability $\varepsilon' \geq \varepsilon - (q_{H_2} q_{DGSC}/2^k + 1/2^k)$ in a time $t' \leq t + (2q_{DGSC})t_e$, where t_e denotes the time required for one pairing computation.

Proof: We show how to build an algorithm B that solves the CDH problem by running the adversary F as a subroutine. On input (P, aP, bP), B's goal is to compute abP. B sets $Y_S^* = bP$ as the challenge public key, and gives the public key to adversary F. The value of b can not be zero, because in the pure signature mode, pure signcryption mode or hybrid signcryption mode, the sender can not be vancant.

Attack: F issues queries to the same oracles as those in the confidentiality game and all oracles are the same except oracle H_1.

Simulator: H_1

B maintains a list L_1, which keeps track of the answers given to oracle queries on H_1. Upon a query (m_i, P_{e_i}), B first scans in the list L_1 to check whether H_1 is already defined for that input. If it is, the previously defined value is returned. Otherwise, B picks a random element $h_{1i} \in Z_q^*$ and sets $H_{1i} = h_{1i} aP$, and stores $(m_i, P_{e_i}, h_{1i}, H_{1i})$ in L_1, output H_{1i} to adversary F.

Forgery: F eventually produces a ciphertext $\sigma^* = (U^*, Z_1^*, Z_2^*, ..., Z_n^*)$ and n arbitrary receivers's key pairs $(x_{R_i}^*, Y_{R_i}^*)(i = 1, ..., n)$, and the attacked user's public key Y_S^*. B runs $DGSC$ algorithm using the private keys $x_{R_i}^*$ and the attacked user's public key Y_S^* to get the m_i^*, V_i^*. If σ^* is valid, we have $e(Y_S^*, H_1(m_i^*, x_{R_i}^* U^*)) = e(P, V_i^*)$, then the list L_1 must contain an entry $(m_i^*, x_{R_i} U^*, h_{1i}^*, H_{1i}^*)$ with overwhelming probability (otherwise, B stops and outputs failure). Then $V_i^* = x_S^* H_{1i}^* = x_S^* (h_{1i}^* ap) = h_{1i}^* abP$, and that $(h_{1i}^*)^{-1} V_i^*$ is the solution of the CDH instance abP.

Now we assess B's probability of failure, F outputs a fake σ^* without

asking the corresponding $H_1(m_i^*, x_{R_i}U^*, h_{1i}^*, H_{1i}^*)$ query is at most $1/2^k$, The probability to reject a valid ciphertext is not greater than $q_{H_2}q_{DGSC}/2^k$. Finally, it comes that B's advantage is $\varepsilon' \geq \varepsilon - (q_{H_2}q_{DGSC}/2^k + 1/2^k)$. Moreover, the bound on B's computation time derives from the fact that every $DGSC$ query requires two pairing evaluations.

Note: In the above forgery stage, part or all of the receivers R_i can be vacant. In that case, algorithm runs in hybrid signcryption mode or pure signature mode, otherwise it runs in pure signcryption mode, so these modes share the same game.

4.4 Performance analysis

Since computation time and ciphertext size are two important factors affecting the efficiency, we present the comparison with respect to them. It is obvious that our improved scheme does not add any extra computation costs and the ciphertext size is the same as the original one, meaning they have the same efficiency, but the original one is not secure while ours is. The authors of the original scheme compared their scheme with other multi-receiver signcryption schemes including Duan and Cao's multi-receiver signcryption [23] (denoted by DC), Yu et al.'s signcryption [30] (denoted by YYHZ), Li et al.'s identity-based broadcast signcryption [32] (denoted by LXH) and Boyen's multipurpose identity-based signcryption [33] (denoted by Boyen). They considered the costly operations including pairing evaluation (Pairing), modular exponentiation (Exp), and modular inverse (Inv). Through the comparison, they concluded their scheme is the most efficient one. Therefore our improved scheme is the most efficient one too. Now, we give the comparison in Table 1, which shows that the computation time and ciphertext size of our improved scheme are both the shortest like the original scheme's.

Table 1. Overheads of multi-receiver signcryption schemes

Schemes	Communication overheads	Computational overheads					
		Paring		Exp		Inv	
		SC	DSC	SC	DSC	SC	DSC
DC	(n+3)|G|+|m|+|ID|	1	4n	n+5	n	0	2n
YYHZ	(n+3)|G|+|m|+|ID|	1	3n	n+5	n	0	n
LXH	(n+2)|G|+|m|+|ID|	1	3n	n+3	2n	0	0
Boyen	2n|G|+|m|+|ID|	n	4n	2n+2	2n	0	n
Original Scheme	(n+1)|G|+|m|	0	2n	n+1	n	0	0
Our Scheme	(n+1)|G|+|m|	0	2n	n+1	n	0	0

5. Conclusion

Generalized signcryption scheme can adaptively work as an encryption

scheme, a signature scheme or a signcryption scheme with only one algorithm, thus it is more widely applicable than signcryption scheme. By using the randomness reusing technology, Han-Gui proposed a multi-receiver GSC scheme, and used it for secure multicast in wireless network. Its main merits are to reduce overheads efficiently and avoid rekeying when membership changes. In this paper, we show that Han-Gui's multi-receiver GSC scheme is not IND-CCA2 secure in the pure encryption mode and the hybrid encryption mode, and an adversary can modify the challenge ciphertext and then can get the plaintext. To remedy this security flaw, we give an improvement of the scheme. Interestingly, the improved scheme is more secure than the original one while still maintaining its efficiency. Due to the computation of the pairing still being time-consuming, it is expected pairing-free multi-receiver GSC schemes are to be proposed in the future.

References

1. Zheng, Y. Digital signcryption or how to achieve cost (signature & encryption)<<cost(signature)+cost(encryption). In: Crypto'1997, Lecture Notes in Computer Science, Vol. 1294. Springer, Berlin, 1997, pp.165-179.
2. Han, Y., Yang, X. ECGSC: Elliptic curve based generalized signcryption. In: The 3rd International Conference on Ubiquitous Intelligence and Computing (UIC-2006), Lecture Notes in Computer Science, Vol. 4159. 2006, pp.956-965.
3. ANSI X9.62. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1999.
4. Wang, X., Yang, X., Han, Y. Provable secure generalized signcryption. http://eprint.iacr.org/2007/173. *Journal of Computers*, 2010, 5(5), 807-814.
5. Lai, S., Kushwah, P. ID-based generalized signcryption. http://eprint.iacr.org/2008 /084.
6. Yu, G., Ma, X., Shen, Y., et al. Provable secure identity based generalized signcryption scheme. *Theoretical Computer Science*, 2010, 411(40-42), 3614-3624.
7. Kushwah, P., Lal, S. Efficient generalized signcryption schemes. http://eprint.iacr.org/2010/346.
8. Han, Y. Generalization of signcryption for resources-constrained environments. *Wireless Communications and Mobile Computing*, 2007,7, 919-931.
9. Han, Y., Gui, X. BPGSC: Bilinear paring based generalized signcryption scheme. In: Eighth International Conference on Grid and Cooperative Computing, 2009, pp.76-82.
10. Zhang, C., Zhang, Y. Secure and efficient generalized signcryption scheme based on a short ECDSA. In: 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010, pp.466-469.
11. Lal, S., Kushwah, P. Generalization of Barreto et al ID based signcryption scheme. http://eprint.iacr.org/2009/193.
12. Kushwah, P., Lal, S. An efficient identity based generalized signcryption scheme. *Theoretical Computer Science*, 2011, 412, 6382-6389.

13. Ji, H., Han, W., Zhao, L. Certificateless generalized signcryption. http://eprint.iacr.org/2010/204.
14. Kushwah, P., Lal, S. Provable secure certificateless generalized signcryption scheme. *International Journal of Computer Technology and Applications*, 2010,3(3): 925-939.
15. Liu, L., Ji, H., Han, W., et al. Certificateless generalized signcryption scheme without random oracles. *Journal of Software*, 23(2), 2012, 394-410. (in chinese).
16. Zhou, C., Zhou, W., Dong, X. Provable certificateless generalized signcryption scheme. *Designs Codes and Cryptography*, 2012, DOI: 10.1007/s10623-012-9734-y.
17. Ji, H., Han, W., Liu, L. Identity based generalized signcryption scheme for multiple PKGs in standard model. *Journal of Electronics & Information Technology*, 2011, 33(5), 1204-1210. (in chinese)
18. Bellare, M., Boldyreva, A., Micali, S. Public-key encryption in a multi-user setting: Security proofs and improvements. In: Eurocrypt 2000, Lecture Notes in Computer Science, Vol.1807. Springer, Berlin, 2000, pp.259-274.
19. Baudron, O., Pointcheval, D., Stern, J. Extended notions of security for multicast public key cryptosystems. In: ICALP 2000, Lecture Notes in Computer Science, Vol.1853. Springer, Berlin, 2000, pp.499-511.
20. Kurosawa, K. Multi-recipient public-key encryption with shortened ciphertext. In: Public Key Cryptography 2002, Naccache D, Paillier P (eds). Springer, Berlin, 2002, pp.48-63.
21. Bellare, M., Boldyreva, A., Staddon, J. Randomness re-use in multi-recipient encryption scheme. In: Public Key Cryptography 2003, Desmedt YG (ed.). Springer, Berlin, 2003, pp.85-99.
22. Bellare, M., Boldyreva, A., Kurosawa, K., et al. Multi-recipient encryption schemes: how to save on bandwidth and computation without sacrificing security. *IEEE Transactions on Information Theory*, 2007, 53(11), 3927-3943.
23. Duan, S., Cao, Z. Efficient and provably secure multi-receiver identity-based signcryption. In: ACISP 2006, Batten, L.M., Safavi-Naini, R. (eds.). Lecture Notes in Computer Science, Vol. 4058. Springer, Berlin, 2006, pp.195-206.
24. Yang, X., Li, M., Wei, L., et al. New ECDSA-verifiable multi-receiver generalization signcryption. In: The 10th IEEE International Conference on High Performance Computing and Communications, 2008, pp.1042-1047.
25. Han, Y., Gui, X. Adaptive secure multicast in wireless networks. *International Journal of Communication Systems*, 2009, 22, 1213-1239.
26. Zhou, C. A multi-receiver ID-based generalized signcryption scheme. http://eprint.iacr.org/2011/601.
27. Racko, C., Simon, D. Non-interactive zero knowledge proof of knowledge and chosen ciphertext attacks. In: Crypto'91, Lecture Notes in Computer Science, Vol.576. 1991, pp. 433-444.
28. Boneh, D., Lynn, B., Shacham, H. Short signatures from the Weil pairing. In: Asiacrypt'2001, Boyd C (ed.). Lecture Notes in Computer Science, Vol. 2248. Springer, Berlin, 2001, pp.514-532.
29. Li, F., Hu, Y., Liu, S. Efficient and provably secure multi-receiver signcryption from bilinear pairings. *Wuhan University Journal of Nature Sciences*, 2007, 12(1), 17-20.

30. Yu, Y., Yang, B., Huang, X., et al. Efficient identity-based signcryption scheme for multiple receivers. In: ATC'2007, Xiao B et al. (eds). Lecture Notes in Computer Science, Vol. 4610. Springer, Berlin, 2007, pp.13-21.
31. Selvi, S.S.D., Vivek S.S., Gopalakrishnan, R., et al. On the provable security of multi-receiver signcryption schemes. http://eprint.iacr.org/2008/238.
32. Li, F., Xin, X., Hu, Y. Indentity-based broadcast signcryption. *Computer Standards and Interfaces*, 2008, 30(2), 89-94.
33. Boyen, X. Multipurpose identity-based signcryption: a swiss army knife for identity-based cryptography. In: Crypto'2003, Boneh D (ed.). Lecture Notes in Computer Science, Vol. 2729. Springer, Berlin, 2003, pp.383–399.