A Multi-Receiver ID-Based Generalized Signcryption Scheme

Caixue Zhou*

School of Information Science and Technology, University of Jiujiang, JiuJiang 332005, China

ABSTRACT

Generalized signcryption(GSC) can adaptively work as an encryption scheme, a signature scheme or a signcryption scheme with only one algorithm. In this paper, the formal definition and security notions of multi-receiver identity-based generalized signcryption (MID-GSC) are defined. A concrete scheme is also proposed and proved to be confidential under the Bilinear Diffie-Hellman (BDH) assumption and existential unforgeable under the Computational Diffie-Hellman(CDH) assumption in the random oracle model, which only needs one pairing computation to generalized signcrypt a single message for n receivers using the randomness re-use technique. Compared with other multi-receiver ID-based signcryption schemes, the new scheme is also of high efficiency.

Keywords: Multi-receiver identity-based generalized signcryption; Bilinear pairing; Provable security; Randomness re-use; Selective identity security; Random oracle model

1. Introduction

Identity based(ID-based) cryptosystem was introduced by Shamir[1] in 1984. Its main idea is that public keys can be derived from arbitrary strings while private keys can be generated by the trusted Private Key Generator(PKG). This removes the need for senders to look up the receiver's public key before sending out an encrypted message. ID-based cryptography is supposed to provide a more convenient alternative to conventional public key infrastructure.

Signcryption, first proposed by Zheng[2], is a cryptographic primitive that performs signature and encryption simultaneously, at lower computational costs and communication overheads than those required by the traditional sign-then-encrypt approach. Due to its advantages, there have been many signcryption schemes proposed after Zheng's publication. However, in some applications, sometimes people need both confidentiality and authentication and sometimes they just need confidentiality or authentication separately. For that case, applications must often contain at least three cryptographic primitives: signcryption, signature, and encryption, 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.[3] proposed the concept of GSC which can implement the separate or joint encryption and signature functions in a single primitive, meanwhile

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

they gave a GSC scheme based on ECDSA[4]. Wang et al.[5] gave the first security model for a GSC scheme and modified the scheme proposed in [3]. The first ID-GSC scheme along with a security model was proposed by Lal and Kushwah[6] in 2008. However, Yu et al.[7] show that the security model proposed in [6] is not complete. They modified the security model and proposed a concrete scheme which is secure in this model. In 2010, Kushwah and Lal[8] simplified the security model proposed in [7] and gave an efficient ID-GSC scheme.

However, all the above GSC schemes consist of only one receiver. In 2000, Bellare et al.[9], and Baudron et al.[10] 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. Later a novel technique called randomness re-use[11] was presented to enhance the efficiency and bandwidths. Bellare et al.[12,13] investigated the property of randomness reusing-based multi-recipient encryption schemes (RR-MRES) and found that some RR-MRES keep the high security for the differences of the distinct recipient's public keys. They proved that if the underlying base scheme is reproducible and semantically secure, then the corresponding RR-MRES is semantically secure too. These results give a solution to construct a secure MRES with a semantically secure base scheme. Particularly, randomness re-use is a novel technique that can be used to reduce overheads of batch encryption. In PKC2005, baek et al.[14] first proposed an ID-based MRES which used the technique of randomness re-use, where only one pairing computation is needed to encrypt a single message for n receivers. In 2006, Duan et al.[15] first proposed an ID-based multi-receiver signcryption scheme which also used the technique of randomness re-use, where only one pairing computation is needed to signcrypt a single message for n receivers too. Since then, many ID-based multi-receiver signcryption schemes were proposed[16-19]. In GSC aspects, Han[20] first proposed a multi-receiver GSC scheme, but his scheme is a trivial n-recipient scheme that runs GSC repeatedly n times, which obviously is very inefficient. In 2008, Yang et al.[21] proposed a multi-receiver GSC scheme which used the technique of randomness re-use. In 2009, Han and Gui[22] proposed a multi-receiver GSC scheme which also used the technique of randomness re-use. However their schemes are not identity based ones. To the best of our knowledge, there has been no MID-GSC scheme proposed in the literature till date.

In this paper, by reference to the design method of multi-receiver identity-based signcryption of [15], based on the variant signature scheme of Sakai-Ogishi-Kasahara(V-SOK)[23], we propose an efficient MID-GSC scheme that only requires one pairing computation to generalized signcrypt a single message for n receivers. We provide formal security notions for MID-GSC schemes based on the selective identity attack model in which an attacker outputs ahead of time the identities of multiple receivers that it wishes to be challenged[24]. We then prove that our scheme is confidential under the BDH[25] assumption and existential unforgeable under the

CDH[26] assumption in the random oracle model[27]. The paper is organized as follows: in the next section, we give the definition of bilinear pairings and related computational hard problems. The definition and the security model of MID-GSC are given in Section 3. In Section 4 we give the concrete MID-GSC scheme. The efficiency is analyzed in Section 5. Section 6 concludes the paper.

2. Preliminary

Definition 1 (Bilinear pairings)
Let G_1 be a cyclic additive group, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order. Let $\hat{e}: G_1 \times G_1 \to G_2$ be a mapping with the following properties:
(1). Bilinearity: $\hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$ for all $P,Q \in G_1$, $a,b \in Z_q$.
(2). Non-degeneracy: There exists $P,Q \in G_1$ such that $\hat{e}(P,Q) \neq 1_{G2}$.
(3). Computability: There exists an efficient algorithm to compute $\hat{e}(P,Q)$, for all $P,Q \in G_1$.
Definition 2. (BDH problem)
The BDH problem is, given $P, aP, bP, cP \in G_1$, for unknown $a,b,c \in Z_q^*$, to compute $\hat{e}(P,Q)^{abc}$.
The advantage of any probabilistic polynomial time(PPT) algorithm G in solving BDH problem in G_1 is defined to be: $ADV_G^{BDH} = \Pr[G(P,aP,bP,cP) = \hat{e}(P,P)^{abc} : a,b,c \in Z_q^*]$.
BDH assumption: For every PPT algorithm G, ADV_G^{BDH} is negligible.
Definition 3. (CDH problem)
The CDH problem is, given $P, aP, bP \in G_1$ for unknown $a,b \in Z_q^*$, to compute abP.
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

3. MID-GSC and its security notions

3.1 Syntax

In the setting of MID-GSC, either a single message or multiple messages can be generalized signcrypted. In our context, we assume that a single message is generalized signcrypted to multiple receivers. Actually, it's very easy to modify our scheme to become a multi-message multi-receiver scheme.
Definition 4 (MID-GSC):
An MID-GSC scheme =($Setup, Extract, GSC, UGSC$) consists of four algorithms.
Setup: Given a security parameter 1^k, the PKG generates a master key s and a common parameter $params$. $params$ is given to all interested parties while s is kept secret.
Extract: This is the user key generation algorithm. Providing an identity ID received from a user and its master key s as input, the PKG runs this algorithm to generate a private key associated with ID, denoted by D_{ID}.
GSC: This is a probabilistic algorithm. This algorithm takes the private key D_A of

the sender A, the multiple receivers' identities $ID_1,...,ID_n$ and message m to return ciphertext $\sigma = GSC(m, D_A, ID_1,...,ID_n)$.

UGSC: This is a deterministic algorithm. The receiver ID_i computes $UGSC(\sigma, ID_A, ID_i)$ with the corresponding private key D_{IDi}, obtains m or an invalid symbol $\perp$.

For consistency, we require $UGSC(GSC(m, D_A, ID_1,...,ID_n), ID_A, ID_i) = m$.

MID-GSC is an adaptive scheme which implies three modes in this case. If the sender and all of the receivers are determined, it runs in signcryption mode. If all of the receivers are vacant and the sender is determined, it runs in signature mode. If the sender is vacant and all of the receivers are determined, it runs in encryption mode. Other inputs are not allowed. The three modes are transparent to applications, namely, the algorithm can produce the specific outputs according to the inputs of identities of the sender and the receivers adaptively. Applications need not care about which mode should be taken.

3.2 Security model for MID-GSC

Now we present security notions for MID-GSC schemes. Recall that the selective identity attack means that an adversary commits ahead of time to the identity on which it will be challenged. We extend this notion to MID-GSC setting. Thus in our models, the adversary is assumed to output ahead of time multiple identities that it wishes to attack. Besides, due to the identity based nature, we should assume that the adversary may obtain any private key other than those of the multiple target identities. Note that in the description of the models, we often equate a user with its identity. With respect to confidentiality, the widely accepted notion is indistinguishability of ciphertexts under chosen ciphertext attacks. we adapt it to the MID-GSC setting and refer to it as indistinguishability of ciphertexts under selective multi-ID generalized signcryption, chosen ciphertext attacks (IND-sMIDGSC-CCA). Analogously, existential unforgeability under selective multi-ID generalized signcryption, adaptive chosen message attacks is UF-sMIDGSC-CMA for short.

In our security models, by reference to the simplified security models of [8] and the security models of [17], we give out the MID-GSC security models.

Definition 5 (confidentiality)

An MID-GSC scheme is IND-sMIDGSC-CCA if no probabilistic polynomial time adversary A has a non-negligible advantage in the following game.

(1) ***Setup*** : The challenger C runs the Setup algorithm to generate a master key and a common parameter ($s, Params$). C gives $Params$ to A while he keeps s secret from A. After receiving the system parameters , the adversary A outputs the set of target identities $S^* = \{ID_1^*,...,ID_n^*\}$.

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

(a) Extract Oracle — A produces an identity ID and queries for the secret key of ID. The Extract Oracle returns D_{ID} to A provided $ID \notin S^*$.

(b) GSC Oracle — A produces a message m, n receivers' identities $ID_1, ID_2,..., ID_n$, the sender's identity ID_A. The challenger C returns $\sigma = GSC(m, ID_A, ID_1, ID_2,..., ID_n)$ to A. Here if the sender and all of the receivers are not vacant, it equals to signcryption oracle, if all of the receivers are vacant, it equals to signature oracle, if the sender is vacant, it equals to encryption oracle.

(c) UGSC Oracle — A produces a ciphertext σ, the receiver's identity ID_i, $i \in [1,n]$, the sender's identity ID_A. The challenger C returns $UGSC(\sigma, ID_A.ID_i) = m \text{ or } \perp$ to A. Here if the sender and all of the receivers are not vacant, it equals to un-signcryption oracle, if all of the receivers are vacant, it equals to signature verify oracle, if the sender is vacant, it equals to decryption oracle.

(3) ***Challenge***: A produces two equal length different plaintexts m_0, m_1, an arbitrary sender ID_A^*, n receivers' identities $ID_1^*,...,ID_n^* \in S^*$. B flips a coin b←{0, 1} to compute a ciphertext $\sigma^* = GSC(m_b, ID_A^*, Q_1^*,...,Q_n^*)$ 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 restrictions that it should not query the $UGSC(\sigma^*, ID_A^*, ID_i^*)$ and the extract oracle for the secret keys of $ID_i^* \in S^*$ $(i = 1,...,n)$.

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

We define the advantage of the adversary A as: $Adv^{IND-sMIDGSC-CCA}(A) := 2\Pr[b_0 = b] - 1$.

Note: In the above challenge stage, the sender ID_A^* can be vacant. In this case, algorithm runs in encryption mode otherwise it runs in signcryption mode, so encryption mode and signcryption mode share the same game.

Definition 6 (unforgeability)

An MID-GSC scheme is UF-sMIDGSC-CMA if no probabilistic polynomial time adversary A has a non-negligible advantage in the following game.

(1) ***Setup***: The challenger C runs the Setup algorithm to generate a master key and a common parameter $(s, Params)$. C gives $Params$ to A while he keeps s secret from A. After receiving the system parameters , the adversary A outputs the target identity ID^* on which he would like to challenge.

(2) ***Attack***: A issues queries to the same oracles as those in the confidentiality game .

(3) ***Forgery***: A eventually produces a ciphertext σ and n arbitrary receivers' identities $ID_1, ID_2,..., ID_n$, A wins if the result of $UGSC(\sigma, ID^*, ID_i)$ for some $i \in [1,n]$ results in a valid message m, the private key of ID^* was not queried and σ was not the output of $GSC(m, ID^*, ID_1,..., ID_n)$.

Note: In the above forgery stage, all of the receivers $(ID_1,..., ID_n)$ can be vacant. In that case, algorithm runs in signature mode otherwise it runs in signcryption mode, so signature mode and signcryption mode share the same game.

4. Our scheme

4.1 Description of our scheme

Setup: Given the security parameter 1^k, this algorithm outputs: two cycle groups $(G_1, +)$ and $(G_2, \cdot)$ of prime order q, a generator $P \in G_1$, a bilinear map $\hat{e}: G_1 \times G_1 \to G_2$, three hash functions: $H_0: \{0,1\}^{n_1} \to G_1$, $H_1: \{0,1\}^{z+(n+1)\cdot n_1} \times G_1 \to G_1$, $H_2: G_2 \to \{0,1\}^{z+n_2}$.

Here n_1, n_2 and z are the number of bits required to represent an identity, an element of G_1 and a message respectively. H_0, H_2 needs to satisfy an additional property: $H_0(0) = \vartheta, H_2(1) = 0$, where ϑ denotes the infinite element in group G_1. PKG chooses s randomly from Z_q^* as his master key, and computes $P_{pub} = sP$ as his public key. The system parameters are $params = \{G_1, G_2, q, n_1, n_2, z, \hat{e}, P, P_{pub}, H_0, H_1, H_2\}$.

Define a special function $f(ID)$, where $ID \in \{0,1\}^{n_1}$. If identity is vacant, that is $ID \in \phi$, let $ID = 0$, $f(ID) = 0$; in other cases, $f(ID) = 1$.

Extract: Each user in the system with identity ID_U, his public key $Q_U = H_0(ID_U)$ is a simple transform from his identity. Then PKG computes private key $D_U = s \cdot Q_U$ for ID_U. If $ID_U \in \phi$, $(\vartheta, \vartheta) \leftarrow Gen(U, 1^k)$.

GSC: Suppose Alice with identity ID_A wants to send a message m to n different receivers $ID_i\ (i = 1\ to\ n)$: select any one ID_B from $ID_i\ (i = 1\ to\ n)$

- Computes $f(ID_A)$ and $f(ID_B)$ $(B \in [1, n])$
- Selects $k \in Z_q^*$, $Q_R \in G_1$ randomly, Computes $R = kP$
- Computes $H = H_1(m, R, ID_A, ID_1, ..., ID_n) \in G_1$
- Computes $S = f(ID_A) \cdot D_A + kH$
- Computes $Y = \hat{e}(P_{pub}, Q_R)^{k \cdot f(ID_B)}$
- Computes $C = (m \| S) \oplus H_2(Y)$
- Computes $U_i = k(Q_R + Q_{ID_i})$ $(i = 1, ..., n)$
- The ciphertext is $\sigma = (R, C, U_1, ..., U_n)$.

UGSC: Each receiver ID_i uses his private key D_{ID_i} to decrypts $\sigma = (R, C, U_1, ..., U_n)$:

- Computes $f(ID_i)$
- Computes $Y' = \hat{e}(P_{pub}, U_i)^{f(ID_i)} \hat{e}(R, D_{ID_i})^{-f(ID_i)}$
- Computes $m \| S = C \oplus H_2(Y')$
- Checks if $\hat{e}(S, P) = \hat{e}(Q_A, P_{pub})^{f(ID_A)} \hat{e}(H, R)$, where $H = H_1(m, R, ID_A, ID_1, ..., ID_n) \in G_1$.

Output m if the above verification is true, or output $\perp$ if false.

Correctness: It is easy to see that the above **UGSC** algorithm is consistent if σ is a valid ciphertext, since:

$$
\begin{aligned}
Y' &= \hat{e}(P_{pub}, U_i)^{f(ID_i)} \hat{e}(R, D_{ID_i})^{-f(ID_i)} \\
&= \hat{e}(sP, kQ_R + kQ_{ID_i})^{f(ID_i)} \hat{e}(R, D_{ID_i})^{-f(ID_i)} \\
&= \hat{e}(kP, sQ_R + sQ_{ID_i})^{f(ID_i)} \hat{e}(R, D_{ID_i})^{-f(ID_i)} \\
&= \hat{e}(kP, sQ_R)^{f(ID_i)} \hat{e}(kP, sQ_{ID_i})^{f(ID_i)} \hat{e}(R, D_{ID_i})^{-f(ID_i)} \\
&= \hat{e}(kP, sQ_R)^{f(ID_i)} \hat{e}(R, D_{ID_i})^{f(ID_i)} \hat{e}(R, D_{ID_i})^{-f(ID_i)} \\
&= \hat{e}(kP, sQ_R)^{f(ID_i)} \\
&= \hat{e}(sP, kQ_R)^{f(ID_i)} \\
&= \hat{e}(P_{pub}, Q_R)^{k \cdot f(ID_i)} = Y. \qquad (as\ f(ID_i) = f(ID_B))
\end{aligned}
$$

$\hat{e}(S, P) = \hat{e}(f(ID_A) \cdot D_A + kH, P) = \hat{e}(f(ID_A) \cdot D_A, P) \hat{e}(kH, P) = \hat{e}(Q_A, P_{pub})^{f(ID_A)} \hat{e}(H, R)$.

Then receiver ID_i can decrypt the ciphertext and obtain the signed message.

4.2 Adaptation

MID-GSC is an adaptive scheme that can seamlessly switch to different modes according to the inputs of users' identities, applications need not care about all of these works. Note that the scheme seamlessly switches to three modes without any other additional operation.

Signcryption mode*:* when $ID_A \notin \phi$ and $ID_i\ (i = 1\ to\ n) \notin \phi$, then $f(ID_A) = 1$ and $f(ID_i) = 1$ $(i \in [1, n])$. Algorithm runs in signcryption mode.

Encryption mode*:* when $ID_A \in \phi$ and $ID_i\ (i = 1\ to\ n) \notin \phi$, then $f(ID_A) = 0$ and $f(ID_i) = 1$ $(i \in [1, n])$. Algorithm runs in encryption mode. In this case, $S = kH$, the check equation becomes: $\hat{e}(S, P) = \hat{e}(H, R)$, where $H = H_1(m, R, \phi, ID_1, ..., ID_n)$.

Signature mode*:* when $ID_A \notin \phi$ and $ID_i\ (i = 1\ to\ n) \in \phi$, then $f(ID_A) = 1$ and $f(ID_i) = 0$ $(i \in [1, n])$. Algorithm runs in signature mode. In this case, $Y = \hat{e}(P_{pub}, Q_R)^{k \cdot f(ID_i)} = 1$,

$C = (m \| S) \oplus H_2(Y) = (m \| S) \oplus H_2(1) = m \| S$, The ciphertext is $\sigma = (R, C, U_1, ..., U_n) = (R, m \| S, U_1, ..., U_n)$, namely (R, S) is the signature of m .

5. Security and efficiency analyses of MID-GSC

5.1. Security of MID-GSC

Theorem 1. In the random oracle model, if an adversary A has non-negligible advantage ε against the IND-sMIDGSC-CCA security of our scheme running in signcryption mode or encryption mode when running in time t and performing q_{GSC} generalized signcryption queries, q_{UGSC} generalized un-signcryption queries and q_{H_i} queries to oracles H_i ($for\ i = 0,1,2$) , then there is an algorithm B that solves the BDH problem with probability $\varepsilon' \geq 1/q_{H_2}(\varepsilon - q_{H_2} \cdot q_{UGSC} / 2^k)$ and within running time $t' < t + (2q_{UGSC} + q_{GSC})/t_e$ where t_e denotes the time required for one pairing evaluation.

The corresponding proof will be given in the full version.

Theorem 2. In the random oracle model, if a forger F has non-negligible advantage ε against the UF-sMIDGSC-CMA security of our scheme running in signcryption mode or signature mode, then B can solve the CDH problem with probability $\varepsilon_B \geq \varepsilon - 1/2^k$.

The corresponding proof will be given in the full version.

5.2 Efficiency

As far as we know, there has been no MID-GSC scheme proposed in the literature till date. So, we compare the efficiency of our scheme with several multi-receiver ID-based signcryption schemes which also use randomness re-use technique. Since computation time and ciphertext size are two important factors affecting the efficiency, we present the comparisons with respect to them. Table 1 shows the comparisons. From table 1, we can conclude that the ciphertext size of our scheme is the shortest one, our scheme is of high efficiency.

Table 1 Efficiency comparisons with other schemes

	Scalar Mul in G1	Mul in G2	Pairing	Ciphertext size
Scheme[15]	n +5	0	5	(n+3)|G1|+|ID|+|m|
Scheme[16]	n+4	1	4	(n+2)|G1|+|G2|+|m|
Scheme[18]	n +4	1	5	(n+3)|G1|+|G2|+|m|
Our scheme	n+1	1	6	(n+2)|G1|+|m|

6. Conclusion

In this paper, we give the formal definition and security notions of multi-receiver Id-based generalized signcryption and propose a concrete scheme which needs only one pairing computation to generalized signcrypt a single message for n receivers and then prove its security in the random oracle model under the BDH and CDH assumptions. According to the comparisons with other multi-receiver ID-based signcryption schemes, the new scheme is of high efficiency. Further work is on the way to construct more efficient schemes than ours.

References

[1] A. Shamir, Identity-based cryptosystem and signature scheme, in: G. R. Blakley,D. Chaum (Eds.), Advances in Cryptology – CRYPTO' 84, Vol. 196 of Lecture Notes in Computer Science, International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1985, pp. 120-126.

[2] Y. Zheng, Digital signcryption or how to achieve cost (signature & encryption)<<cost(signature) + cost (encryption). In Advances in Cryptology—CRYPTO'1997, Lecture Notes in Computer Science, vol. 1294. Springer: Heidelberg, 1997; 165-179.

[3] Y. Han and X. Yang, ECGSC: Elliptic curve based generalized signcryption scheme. Cryptology ePrint Archive, Report 2006/126, 2006, http:/eprint.iacr.org/.

[4] ANSI X9.62. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1999.

[5] X. Wang, Y. Yang and Y. Han, Provable secure generalized signcryption. Cryptology ePrint Archive, Report 2007/173, 2007, http:/eprint.iacr.org/.

[6] S. Lal and P. Kushwah, ID based generalized signcryption. Cryptology ePrint Archive, Report 2008/84, http://eprint.iacr.org/ 2008/84.pdf, 2008.

[7] G. Yu, X. Ma, Y. Shen et al., Provable secure identity based generalized signcryption scheme . Theoretical Compute Science, 2010, 411(40-42): 3614-3624.

[8] P. Kushwah, S. Lai, Efficient generalized signcryption schemes. http://eprint.iacr.org/2010/346.pdf.

[9] M. Bellare, A. Boldyreva, S. Micali, Public-key Encryption in a Multi-User Setting: Security Proofs and Improvements, In Eurocrypt 2000, LNCS 1807, pp. 259-274, Springer-Verlag, 2000.

[10] O. Baudron, D. Pointcheval, J. Stern, Extended Notions of Security for Multicast Public Key Cryptosystems, In ICALP 2000, LNCS 1853, pp. 499-511, Springer-Verlag, 2000.

[11] K. Kurosawa, Multi-recipient public-key encryption with shortened ciphertext. In Public Key Cryptography 2002, Naccache D, Paillier P (eds). Springer: Heidelberg, 2002; 48-63.

[12] M. Bellare, A. Boldyreva, J. Staddon, Randomness re-use in multi-recipient encryption scheme. In Public KeyCryptography 2003, Desmedt YG (ed.). Springer: Heidelberg, 2003; 85-99.

[13] M. Bellare, A. Boldyreva, K. Kurosawa 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. DOI: 10.1109/TIT.2007.907471.

[14] J. Baek, R. Safavi-Naini, W. Susilo, Efficient multi-receiver identity based encryption and its application to broad encryption. In: Vaudenay, S. (ed.) PKC 2005. LNCS, vol. 3386, pp. 380-397. Springer, Heidelberg (2005)

[15] S. Duan, Z. Cao, Efficient and provably secure multi-receiver identity-based signcryption. In: Batten, L.M., Safavi-Naini, R. (eds.) ACISP 2006. LNCS, vol. 4058, pp. 195-206. Springer, Heidelberg (2006)

[16] Y. Yu, B. Yang, X. Huang, et al., Efficient identity-based signcryption scheme for multiple receivers. In ATC, pages 13-21, 2007.

[17] S.S.D. Selvi, S.S. Vivek, R. Srinivasan, et al., An Efficient Identity-Based Signcryption

Scheme for Multiple Receivers. Cryptology ePrint Archive, Report 2008/341, http://eprint.iacr.org/2008/341.pdf, 2008.

[18] S. S. D. Selvi, S. S. Vivek, R. Gopalakrishnan, et al., On the provable security of multi-receiver signcryption schemes, Cryptology ePrint Archive, Report 2008/238, http://eprint.iacr.org/ 2008/238.pdf, 2008.

[19] F. Li, H. Xiong, and X. Nie, A new multi-receiver ID-based signcryption scheme for group communications. in Proc. International Conference on Communications, Circuits and Systems-ICCCAS 2009, San Jose, USA, pp. 296-300, 2009.

[20] Y. Han, Generalization of Signcryption for Resources-constrained Environments. Wireless Communication and Mobile Computing, pages. 919-931, 2007. DOI: 10.1002/wcm.504

[21] X. Yang, M. Li, L. Wei et al., New ECDSA-Verifiable Multi-Receiver Generalization Signcryption. The 10th IEEE International Conference on High Performance Computing and Communications, pages 1042-1047, 2008. DOI 10.1109/HPCC.2008.82

[22] Y. Han, X. Gui, Adaptive secure multicast in wireless networks. International Journal Of Communication Systems 2009; 22:1213-1239. DOI: 10.1002/dac.1023

[23] B. Libert, J. Quisquater, The exact security of an identity based signature and its applications . http://eprint.iacr.org/2004/102.pdf

[24] R. Canetti, S. Halevi, and J. Katz, A Forward-Secure Public-Key Encryption Scheme, Advances in Cryptology - In Eurocrypt 2003, LNCS 2656, pp. 255-271, Springer-Verlag, 2003.

[25] D. Boneh and M. Franklin, Identity-Based Encryption from the Weil Pairing, Advances in Cryptology - In Crypto 2001, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.

[26] D. Whitfield, H. Martin, New directions in cryptography. IEEE Transactions on Information Theory, 1976,22 (6):644-654

[27] M. Bellare and P. Rogaway, Random Oracles are Practical: A Paradigm for Designing Efficient Protocols, In ACM CCCS '93, pp. 62-73, 1993.