International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-3, Issue-11, November 2015

A Study on Improvement of Multi-receiver Generalized Signcryption Scheme

Deepa Mishra, Dr. Snigdh singh

***Abstract*— This Multi-receiver signcryption is a new cryptographic primitive that simultaneously fulfils both the functions of signature and multi-receiver encryption. Generalized Multi-Receiver signcryption can provide authenticity or confidentiality separately under specific inputs.**

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 an improved scheme, which can be proved to be IND-CCA2 secure and existentially unforgeable-adaptive chosen message attack (EUF-CMA) under computational Diffie-Hellman (CDH) assumption.

***Index Terms*— Generalized signcryption, Multi-receiver generalized signcryption, Adaptive chosen cipher text attack, Adaptive chosen message attack, randomness reusing.**

I. 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. In Asiacrypt 2011, Paterson et al. [2] revisited the problem where a single keypair is used for both encryption and signature primitives. This usage can reduce storage requirements, the cost of key certification and the time taken to verify certificates. These savings may be critical in embedded systems and low-end smart card applications.However, there is the question of whether it is secure to use the same keypair in two or more different primitives. The formal study of the security of key reuse was initiated by Haber et al. [3] in 2001, and followed by [4, 5, 6, 7]. Paterson et al. [8] gave examples, where encryption and signature schemes are individually secure but become completely insecure when a keypair is shared between them. They concluded that such scheme must be designed specially, and they gave a general construction and a more efficient concrete construction based on pairings, where encryption and signature schemes share the same keypair. They also proposed a scheme implementing the functionality of signcryption, signature and encryption using a single keypair. However, sometimes we need confidentiality and authenticity simultaneously, and sometimes we just need them separately. To achieve this special requirement, we can naively use three different schemes: an encryption scheme, a signature scheme, and a signcryption scheme. Nevertheless, the naive approach needs three keypairs, thus increases the burdens of the key management.

In order to realize signcryption, signature, and encryption functions by using one keypair and one algorithm, so as to save storage spaces and simplify key management, Han et al. [9] in 2006 introduced a new concept of generalized signcryption (GSC). GSC scheme can produce the specific outputs according to the inputs of identities of the sender and the receiver adaptively, that is, if the input of the sender is vacant, it becomes an encryption scheme, if the input of the receiver is vacant, it becomes a signature scheme, if the inputs of the sender and the receiver are not vacant, it becomes a signcryption scheme, if the inputs of the sender and the receiver are all vacant,it takes no secure policy. Its main merit is the storage requirements for three schemes (signcryption, encryption and signature) and three key pairs can be reduced to one scheme and one key pair. Thus, it can realize using one keypair and one algorithm in three different cryptographic primitives. It is very suitable for storage constrained environments, like the embedded systems, smart cards and wireless sensor networks.

Based on ECDSA [10] Han et al. [9] first proposed an efficient GSC scheme. Wang et al. [11] gave the first security model and revised Han et al.'s [9] scheme. In 2008, Lal et al. [12] gave the first identity-based generalized signcryption (ID-GSC) scheme and a security model of ID-GSC. In 2010, Yu et al. [13] pointed out Lal et al.'s [12] security model is not complete, and they improved it and proposed a new scheme which is secure in this model. Later, Kushwah et al. [14] simplified Yu et al.'s [13] security model and proposed another efficient ID-GSC scheme. Moreover, a lot of other GSC schemes have also been given out, including PKI-based (public key infrastructure) schemes [15, 16, 17], identity-based schemes [18, 19], certificateless schemes [20, 21, 22, 23], multi-PKG (private key generator) scheme [24, 25] and schemes in the standard model [24, 22, 26]. However all of the above mentioned schemes are suitable for one receiver scenario. Baudron et al. [27] and Bellare et al. [28] 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 n times, obviously it is inefficient. Later, a novel technique called randomness reuse [29] was presented to enhance the

Deepa Mishra, Computer science and Engineering ,Acropolis Institute of Technology and Research Bhopal, Bhopal, India.
Dr Snigdh singh, Computer science and Engineering, Acropolis Institute of Technology and Research Bhopal, Bhopal, India.

efficiency. Randomness reuse is a novel technique to improve the efficiency of a multireceiver encryption scheme, but not all randomness reuse-based multi-receiver encryption schemes are secure. Bellare et al. [30, 32] proved that if the underlying basic scheme is reproducible and semantically secure, then the corresponding randomness reuse based multi-receiver encryption scheme is semantically secure too. Randomness reuse technique is also introduced to signcryption [33] and generalized signcryption [35] scenarios. Han et al. [34] proved if the underlying basic GSC scheme is reproducible and semantically secure, then the corresponding randomness reuse-based multi-receiver GSC scheme is semantically secure too.

In multi-receiver GSC setting, Han [15] 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. [35] proposed a multi-receiver GSC scheme which used the technique of randomness reuse, but they did not give the security proof of their scheme. In 2009, Han et al. [34] proposed a multi-receiver GSC scheme, their scheme is very efficient and they applied it for secure multicast in wireless network. In 2014, Zhou [36] proposed the first time an identity-based multi-receiver GSC scheme which also used the technique of randomness reuse.

In this paper, we will show that Han et al.'s [34] multi-receiver GSC scheme are insecure, their basic GSC scheme is not IND-CCA2 [37] 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.

II. 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: $\sigma \leftarrow (M, SK_k, PK_{R1}, PK_{R2,.....,}PK_{Rn})$ is a probabilistic algorithm, and takes the private key SK_s of the sender S, the public keys PK_{Ri} (i = 1,..,n) of the receivers and messages $M = m_i$, (i = 1,..,n) σ. There are 5 scenario in this algorithm:

a. Pure Signcrytpion mode: If the sender and all the receivers are determined, it runs in this mode, the ciphertext is $\sigma \leftarrow GSC(M, SK_S, PK_{R1}, PK_{R2,.....,}PK_{Rn}) = signcrypt(M, SK_S, PK_{R1}, PK_{R2,.....,}PK_{Rn})$.

b. Pure Signature Mode: If all the receiver are vacant and the sender is determined, it runs in this mode, the ciphertext is $\sigma \leftarrow GSC(M, SK_S, \phi_{R1}, \phi_{R2,.....,}\phi_{Rn}) = sign(M, SK_S)$. Here ϕ means the user is vacant.

c. Pure Encryption Mode: If the sender is vacant and all of the receivers are determined, it runs in this mode, the ciphertext is $\sigma \leftarrow GSC(M, \phi_S, PK_{R1}, PK_{R2,.....,}PK_{Rn}) = encrypt(M, PK_{R1}, PK_{R2,.....,}PK_{Rn})$.

d. Hybrid Signcryption Mode: If some of the receivers are vacant, and the rest of receivers are determined, it runs in this mode. For the determined receivers, the ciphertext σ is a signcryption ciphertext and for the vacant receivers, the ciphertext σ is a signature.

e. Hybrid Encryption Mode: If some of the receivers and sender are vacant, it runs in this mode. For the determined receivers, the ciphertext σ is an encryption ciphertext and for the vacant receivers, the ciphertext σ is a plain text, it takes no secure policy.

3. De-generalized Signcryption Algorithm: $m_i \cup \perp \leftarrow DGSC(\sigma_i, SK_R, PK_S)$ is a deterministic de- generalized signcryption algorithm and takes the public key PK_S of the sender S, the private key SK_R, of the receiver R_i, and the ciphertext $\sigma_i \in \sigma(i= 1,..n)$, to return the message m_i or an valid symbol ⊥. There are five scenario in this algorithm:

a. Pure Signcryption Mode: $DGSC(\sigma_i, SK_{Ri}, PK_S) = unsigncrypt(\sigma_i, SK_{Ri}, PK_S)$.

b. Pure Signature Mode: $DGSC(\sigma_i, \phi_{Ri}, PK_S) = verify(\sigma_i, PK_S)$.

c. Pure Encryption Mode: $DGSC(\sigma_i, SK_R, \phi_S) = decrypt(\sigma_i, SK_{Ri})$.

d. Hybrid Signcryption Mode: For the determined receivers, $DGSC(\sigma_i, SK_{Ri}, PK_S) = unsigncrypt(\sigma_i, SK_{Ri}, PK_S)$ and for the vacant receivers, $DGSC(\sigma_i, \phi_{Ri}, PK_S) = verify(\sigma_i, PK_S)$.

e. Hybrid Encryption Mode: For the determined receivers, $DGSC(\sigma_i, SK_{Ri}, \phi_S) = decrypt(\sigma_i, SK_{Ri})$ and for the vacant receivers, the ciphertext is plain text, it takes no secure policy .

For consistency, we require $DGSC(GSC(M, SK_S, PK_{R1}, PK_{R2,.....,}PK_{Rn}) SK_R, PK_S) = m_i$, for i=1,..,n, M= m_i.

If all 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 the inputs of identities of the sender and the receivers adaptively. Applications need not care about which mode should be taken.

III. Han et al's Multi-receiver General Signcryption Scheme

A Sender S sends a 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.

Setup: 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. $H_1: \{0,1\}^z X G_1 \rightarrow G_1$ and $H_2 : G_1^3 \rightarrow \{0,1\}^{z+1}$ are two hash functions, where z is the bit length of message m. In order to get adaptive outputs, they defined a special 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.

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

a) Picks a random coin $r \in_R Z_q$ and computes the commitment $U=rP \in G_1$.
b) For i = 1,..,n
   i. Computes $V_i = x_S H_1(m_i,rY_{R1}) \in G_1$.
   ii. Computes $Z_i = (m_i \| V_i) \oplus (H_2(U, Y_{Ri}, rY_{Ri})f(Y_{Ri})) \in \{0,1\}^{z+1}$.
   EndFor
c) 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:

a) Computes $H_2(U, Y_R, x_{Ri}U)$.
b) Computes $(m_i \| V_i) = Z_i \oplus (H_2(U, Y_{Ri}, x_{Ri}U)f(Y_{Ri}))$.
c) If $V_i = O$, returns the message m_i, else computes $h_i = H_2(m_i, x_{Ri}U) \in G_1$ 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 $x_{Ri}U = r Y_{Ri} = x_{Ri}r P$ and $(m_i \| V_i)$ is decrypted correctly. Thus $e(P, V_i) = e(P,x_Sh_i) = e(x_SP, h_i) = e(Y_s, h_i)$ holds.

Pure Signcryption Mode: If the sender and all of the receivers are determined, it runs in this mode. Now, $x_S \neq 0$ and $f(Y_{Ri})=1$,(i = 1,..,n), the ciphertext vector $\sigma = (U, Z_1,..., Z_n)$ is a signcryption ciphertext vector, the GSC and DGSC algorithm are same as above.

Pure Encryption Mode: If the sender is vacant and all of the receivers are determined, it runs in this mode. Now, $x_S=0$ and $f(Y_{Ri})=1$,(i = 1,..,n), so, $V_i = x_SH_1(m_i, r Y_{Ri}) = O$, $Z_i = (m_i \| O) \oplus H_2(U, Y_{Ri}, rY_{Ri})$, the ciphertext vector $\sigma = (U, Z_1,..., Z_n)$ is a encryption ciphertext vector, message m_i can be recovered by $(m_i \| O) = Z_i \oplus H_2(U, Y_{Ri}, x_{Ri}U)$.

Pure Signature Mode: If all of the receivers are vacant and the sender is determined, it runs in this mode. Now, $x_S \neq 0$ and $f(Y_{Ri})=0$, (i = 1,..,n), so, $V_i = x_SH_1(m_i, O)$, $Z_i = (m_i \| V_i) \oplus (H_2(U, Y_{Ri}, rY_{Ri}) f(Y_{Ri})) = m_i \| V_i$, 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 the receivers and senders are determined, the scheme runs in this mode. For the determined receivers, $x_S \neq 0$ and $f(Y_{Ri})=1$, the ciphertext vector $\sigma = (U, Z_i)$ is a signcryption ciphertext vector, and the procedure is the same as pure signcryption mode and for the vacant receivers, $x_S \neq 0$ and $f(Y_{Ri})=0$, the ciphertext vector $\sigma = (U, Z_i)$ is a signature vector, and the procedure is the same as pure signature mode.

Hybrid Encryption Mode: If some of the receivers and senders are vacant, it runs in this mode. For the determined receivers, $x_S = 0$ and $f(Y_{Ri}) = 1$, the ciphertext vector $\sigma = (U, Z_i)$ is a encryption ciphertext vector, and the procedure is the same as pure encryption mode and for the vacant receivers, $x_S = 0$ and $f(Y_{Ri}) = 0$, the ciphertext vector $\sigma = (U, Z_i)$ is a planetext vector, it takes no secure policy.

The five 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.

IV. 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:

a) Computes $f(Y_s)$, $f(Y_{Ri})$,i=1,..,n.
b) Picks a random coin $r \in_R Z_q$ and computes the commitment $U = rP \in G_1$.
c) For i = 1,..,n
   i. Computes $H_i = H_1(m_i,rY_{Ri}) \in G_1$, $V_i = x_SH_i$.
   ii. If $f(Y_s)=0$, Computes $Z_i = (m_i \| H_i) \oplus (H_2(U, Y_{Ri}, rY_{Ri})f(Y_{Ri})) \in \{0,1\}^{z+1}$,
   else computes $Z_i = (m_i \| V_i) \oplus (H_2(U, Y_{Ri}, rY_{Ri})f(Y_{Ri})) \in \{0,1\}^{z+1}$;
   EndFor
d) 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:

a) Computes $f(Y_s)$, $f(Y_{Ri})$,i∈[1,n].
b) If $f(Y_s) = 0$, Computes $(m_i \| H_i) = Z_i \oplus (H_2(U, Y_{Ri}, x_{Ri}U)f(Y_{Ri}))$,else computes $(m_i \| V_i) = Z_i \oplus (H_2(U, Y_{Ri}, x_{Ri}U)f(Y_{Ri}))$.
c) Computes $h_i = H_1(m_i, x_{Ri}U) \in G_1$.
d) If $f(Y_s) = 0$, checks if $H_i = h_i$; if this condition does not hold, rejects the ciphertext; relse return m_i; else checks if $e(Y_S,h_i) = e(P,V_i)$, if this condition does not hold, reject the ciphertext; else return m_i.

V. 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 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 improved is. The authors of the original schemes compared their scheme with other multi-receiver signcryption schemes including Duan et al's multi-receiver signcryption [33], Yu et al's signcryption [38], Li et al's identity based broadcast signcryption [39] and Boyens

Schemes	Communication Overheads	Computational Overheads					
		Pairing		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
Improved Scheme	(n+1)|G| +|m|	0	2n	n+1	n	0	0

multipurpose identity-based signcryption [40]. They considered the costly operations including pairing evaluation (Pairing), modular exponentiation (Exp), and modular inverse(Inv). Though the comparison, they concluded their scheme is the most efficient one. There our improved scheme is the most efficient one too. Now, we give the comparison in above table, which shows that the computation time and ciphertext size of improved scheme are both the shortest like the original scheme's.

VI. Conclusion

Generalized signcryption scheme can adaptively work as an encryption scheme, a signature scheme or a signcryption scheme with only one algorithm and one key pair, thus it can realize using one keypair in three different cryptographic primitives. It is very suitable for storage-constrained environments. By using the randomness reuse technology, Han et al. 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 et al's multi-receiver GSC scheme is not secure in the pure encryption mode and hybrid encryption mode and an adversary can modify the challenge ciphertext and then can get the plaintext. To remedy this security flaw, an improvement of this scheme is given, which is more secure than the original one while still maintaining its efficiency.

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] K. G. Paterson, J. C. N. Schuldt, M. Stam, and S. Thomson, "On the joint security of encryption and signature, revisited," in Proceedings of Asiacrypt'11,pp. 161-178, 2011.

[3] S. Haber and B. Pinkas, "Securely combining public-key cryptosystems," in ACM Conference on Computer and Communications Security, pp. 215-224,2001.

[4] J. S. Coron, M. Joye, D. Naccache, and P. Paillier,"Universal padding schemes for rsa," in Proceedings of Crypto'02, pp. 226-241, 2002.

[5] J. P. Degabriele, A. Lehmann, and K. G. Paterson,"On the joint security of encryption and signature in emv," in Proceedings of CT-RSA'12, pp. 116-135,2012.

[6] Y. C. Komano and K. Ohta,"Efficient universalvpadding techniques for multiplicative trapdoor one-way permutation," in Proceedings of CRYPTO'03,pp. 366-382, 2003.

[7] M. I. G. Vasco, F. Hess, and R. Steinwandt,"Combined (identity-based) public key schemes," Cryptology ePrint Archive, 2008.

[8] K. G. Paterson, J. C. N. Schuldt, M. Stam, and S. Thomson, "On the joint security of encryption and signature, revisited," in Proceedings of Asiacrypt'11,pp. 161-178, 2011.

[9] Y. L. Han and X. Y. Yang, "Ecgsc: Elliptic curve based generalized signcryption," in The 3rd International Conference on Ubiquitous Intelligence and Computing (UIC'06), pp. 956-965, 2006.

[10] X9.62 ANSI, "The elliptic curve digital signature algorithm (ECDSA)," 1999.

[11] X. A. Wang, X. Y. Yang, and Y. L. Han, "Provable secure generalized signcryption," Cryptology ePrintArchive, 2007.

[12] S. Lai and P. Kushwah, "Id-based generalized signcryption," Cryptology ePrint Archive, 2008.

[13] G. Yu, X. X. Ma, Y. Shen, and W. B. Han, "Provable secure identity based generalized signcryption scheme," Theoretical Computer Science, vol. 411, no. 40-42, pp. 3614{3624, 2010.

[14] P. Kushwah and S. Lal,"Efficient generalized signcryption schemes," Cryptology ePrint Archive, 2010.

[15] Y. L. Han, "Generalization of signcryption for resources-constrained environments," Wireless Communications and Mobile Computing, vol. 7, no. 7,pp. 919-931, 2007.

[16] Y. L. Han and X. L. Gui, "Bpgsc: Bilinear paring based generalized signcryption scheme," in Eighth International Conference on Grid and Cooperative Computing, pp. 76-82, 2009.

[17] C. R. Zhang and Y. Q. Zhang, "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'10), pp. 466-469, 2010.

[18] P. Kushwah and S. Lal, "An efficient identity based generalized signcryption scheme," Theoretical Computer Science, vol. 412, no. 45, pp. 6382-6389, 2011.

[19] S. Lai and P. Kushwah, "Generalization of barreto et al id based signcryption scheme," Cryptology ePrintArchive, 2009.

[20] H. F. Ji, W. B. Han, and L. Zhao, "Certificateless generalized signcryption," Cryptology ePrint Archive, 2010.

[21] P. Kushwah and S. Lal, \Provable secure certificateless generalized signcryption scheme," International Journal of Computer Technology and Applications,vol. 3, no. 3, pp. 925-939, 2012.

[22] L. D. Liu, H. F. Ji, W. B. Han, and L. Zhao, "Certificateless generalized signcryption scheme without random oracles," Journal of Software (in Chinese),vol. 23, no. 2, pp. 394{410, 2012.

[23] C. X. Zhou, W. Zhou, and X. W. Dong, "Provable certificateless generalized signcryption scheme,"Designs Codes and Cryptography, vol. 71, no. 2,pp. 331-346, 2014.

[24] H. F. Ji, W. B. Han, and L. D. Liu, "Identity based generalized signcryption scheme for multiple pkgs in standard model," Journal of Electronics and Information Technology (in Chinese), vol. 33, no. 5,pp. 1204{1210, 2011.

[25] C. X. Zhou and Y. L. Han, "Identity-based multi-pkg generalized signcryption scheme," Journal of Chinese Computer Systems (in Chinese), vol. 34, no. 7,pp. 163-1636, 2013.

[26] G. Y. Wei, J. Shao, Y. Xiang, P. P. Zhu, and R. X.Lu, "Obtain confidentiality or/and authenticity in big data by ID-based generalized signcryption," Information Sciences, DOI: 10.1016/j.ins.2014.05.034,2014.

[27] O. Baudron, D. Pointcheval, and J. Stern, "Extended notions of security for multicast public key cryptosystems," in Proceedings of ICALP'00, pp. 499-511, 2000.

[28] M. Bellare, A. Boldyreva, and S. Micali, "Public-key encryption in a multi-user setting: Security proofs and improvements," in Proceedings of Eurocrypt'00, pp. 259-274, 2000.

[29] K. Kurosawa, "Multi-recipient public-key encryption with shortened ciphertext," in Proceedings of Public Key Cryptography, pp. 48-63, 2002.

[30] M. Bellare, A. Boldyreva, K. Kurosawa, and J. Staddon,"Multi-recipient encryption schemes: how to save on bandwidth and computation without sacrificing security," IEEE Transactions on Information Theory, vol. 53, no. 11, pp. 39273943, 2007.

[31] M. Bellare, A. Boldyreva, and S. Micali, "Public-key encryption in a multi-user setting: Security proofs and improvements," in Proceedings of Eurocrypt'00, pp. 259-274, 2000.

[32] M. Bellare, A. Boldyreva, and J. Staddon, "Random-ness re-use in multi-recipient encryption scheme," in Proceedings of Public Key Cryptography, pp. 85-99,2003.

[33] S. S. Duan and Z. F. Cao, "Efficient and provably secure multi-receiver identity-based signcryption," in Proceedings of ACISP'06, pp. 195-206, 2006.
[34] Y. L. Han and X. L. Gui, "Adaptive secure multicast in wireless networks," International Journal of Communication Systems, vol. 22, no. 9, pp. 1213-1239, 2009.
[35] X. Y. Yang, M. T. Li, L. X. Wei, and Y. L. Han, "New ecdsa-verifiable multi-receiver generalization signcryption," in The 10th IEEE International Conference on High Performance Computing and Communications, pp. 1042-1047, 2008.
[36] C. X. Zhou, "Provably secure and efficient multi-receiver identity-based generalized signcryption scheme," in 2014 Ninth Asia Joint Conference on Information Security, pp. 82-89, 2014.
[37] C. Racko and D. Simon,"Non-interactive zero knowledge proof of knowledge and chosen ciphertext attacks," in Proceedings of Crypto'91, pp. 433-444,1991.
[38] Y. Yu, B. Yang, X. Y. Huang, and M. W. Zhang, "Efficient identity-based signcryption scheme for multiple receivers," in Proceedings of ATC'07, pp. 13-21,2007.
[39] F. G. Li, X. J. Xin, and Y. P. Hu, "Indentity-based broadcast signcryption," Computer Standards and Interfaces, vol. 30, no. 2, pp. 89-94, 2008.
[40] X. Boyen, "Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography," in Proceedings of Crypto'03, pp. 383-399,2003.