Efficient Identity-Based Generalized Ring Signcryption Scheme

Caixue Zhou, Zongmin Cui, Guangyong Gao
School of Information Science and Technology, University of Jiujiang
JiuJiang, 332005, JiangXi, China
[e-mail: charlesjjjx@126.com]
*Corresponding author: Caixue Zhou

Received October 4, 2015; revised December 8, 2015; revised January 20, 2016; accepted October 6, 2016; published December 31, 2016

Abstract

In this paper, we introduce a new concept called generalized ring signcryption (GRSC), which can achieve ring signature and ring signcryption functions with only one key pair and one algorithm. It is very useful for a system which has a large number of users, or has limited storage space, or whose function requirements may be changed later. We give a formal definition and a security model of GRSC and propose a concrete scheme based on bilinear pairings. In the random oracle model, the scheme's confidentiality can be proved under the GBDH assumption, and its unforgeability can be proved under GDH' assumption, and what is more, this scheme also allows unconditional anonymity. Compared with other identity-based ring signcryption schemes that use bilinear pairings as well, our scheme is a highly efficient one.

Keywords: Ring signature, ring signcryption, bilinear pairing, random oracle model, identity-based cryptography

This research is supported by the National Nature Science Foundation of China under Grant Nos. 61462048, 61362032, 61562047 and 61662039, the Natural Science Foundation of Jiangxi Province, China (Grant Nos. 20151BAB207003 and 20161BAB202036). We express our thanks to Ms. Yan Di who checked our manuscript.

http://dx.doi.org/10.3837/tiis.2016.12.022 **ISSN : 1976-7277**

1. Introduction

Identity-based public key cryptosystem was first introduced by Shamir [1] in 1984. Its main purpose is to simplify the public key certificate management in the traditional public key cryptosystem. It uses the user's name or his/her IP address, etc. as his/her public key so that the public key certificate is no longer needed. Then a trusted third party called the private key generator (PKG) generates all users' private keys, which brings a new problem called the private key escrow problem. But it is still very useful in the scenario where the PKG is trusted absolutely.

In general, we use encryption to realize confidentiality and signature to realize authentication. When both are needed at the same time, the traditional method would involve two steps, that is, the sign-then-encrypt approach. Signcryption is a cryptographic primitive that performs both confidentiality and authentication in a single logic step, and compared with the traditional approach, it can greatly reduce computational costs and communicational overheads.

Ring signature was first introduced by Rivest et al. [2] in 2001. When a signer wants to sign a document in an anonymous way, he/she can conscript other n-1 persons to form a ring and sign the document with his/her private key and the others' public keys. Any verifier can be convinced that the signature is made by one member of the ring but does not know exactly who the signer is, nor do they know whether two signatures are issued by the same signer. A similar concept is the group signature [3]. In a group signature scheme, there exists a group manager who can revoke the anonymity, and this group manager must manage users' joining and leaving. However, in the ring signature scheme, the anonymity is irrevocable, no group manager is needed and the ring is ad hoc. The other n-1 persons are even unaware that their public keys have been included in the ring. The ring signature has been found in many practical applications since its introduction, such as whistle blowing [2], ad hoc network authentication [4], e-voting [5], e-auction [6], concurrent signature [7], and designated verifier signature [8].

The ring signature allows an actual signer to sign a document in an anonymous way. But sometimes we do not want everyone to see the document. For example, in e-auction, we just want the auction manager to see the document. In order to address this situation, Huang et al. [9] extended ring signature to ring signcryption in 2005, which allows someone anonymously sign a document but only the receiver can see it.

However, under some circumstances, we may sometimes want to use the ring signature and sometimes the ring signcryption, so we must hold two key pairs and use two algorithms - one for ring signature and the other for ring signcryption. But is there a way to use only one key pair and one algorithm to realize both these functions?

From the perspective of efficiency, using only one key pair and one algorithm to realize both functions will not only save storage space, simplify key management and reduce the cost of key verification, but simplify system deployment as well.

Haber et al. [10] were the first to study the subject of encryption and signature sharing the same key pair in the PKI (public key infrastructure) setting in 2001, which they called the combined public key cryptosystem. They concluded that one key pair being shared between an encryption and a signature is not necessarily safe, so they gave some concrete schemes where it is secure for both encryption and signature to share one key pair.

At the same time, Han et al. [11] also introduced the concept of generalized signcryption,

which is a natural extension of Zheng's signcryption. Generalized signcryption can realize encryption, signature and signcryption with only one key pair and one algorithm. Its purpose is to save the storage space of keys and programs, simplify key management and system deployment and reduce the time spent on verifying the keys, which is consistent with what the combined public key cryptosystem is created for.

The combined public key cryptosystem considered sharing the same key pair between different cryptographic primitives, but failed to consider sharing the same algorithm. If we can share the same algorithm, we will be able to further save the storage space of the system, and reduce the costs arising from changes in system functions, and simplify the system implementation. For example, previously a system could only perform encryption. Due to some reason, it is required to perform the signature function as well. If a combined public key cryptosystem is already used, the new requirement will not result in more keys, but with the new signature function added, the system has to be re-programmed and re-deployed. On the other hand, generalized signcryption considered sharing the same key pair and algorithm between encryption, signature and signcryption. However, it included encryption in its system, making it difficult to extend it to the ring cryptosystem, as we do not have the ring encryption. In this paper, we extend the generalized signcryption to ring cryptosystem without encryption. In other words, we explore the possibility of sharing the same key pair and algorithm between the ring signature and the ring signcryption, which we call the generalized ring signcryption.

We give a formal definition and a security model of GRSC in the identity-based setting, and propose a concrete scheme in the random oracle model by using bilinear pairings. Our scheme is highly efficient as it only needs a constant number of pairing computations, while in many ring signature and ring signcryption schemes in the literature, the pairing computations often grow linearly with the ring size n. Then we prove the confidentiality of our scheme under the GBDH assumption and the unforgeability of ours under the $GDH^{'}$ assumption, and also demonstrate that ours allows unconditional anonymity. Through efficiency analysis, we show that our scheme is highly efficient. Finally, we give an application example.

The rest of the paper is organized as follows. In Section 2, we review previous works on the combined public key cryptosystem, generalized signcryption, ring signature and ring signcryption. In Section 3, we introduce the concept of bilinear pairing, some complexity assumptions and the algorithm constitution and a security model of identity-based GRSC. In Section 4, we propose an efficient identity-based GRSC scheme in the random oracle model. In Section 5, we discuss the security and efficiency of the proposed scheme and give an application example. We conclude the paper in Section 6.

2. Related Work

Harber and Pinkas studied the subject of one key pair being shared between an encryption and a signature in 2001, and gave some secure schemes. Later, Coron et al. [12] proved that the PSS [13] scheme can be used for encryption and signature with the same key pair in 2002. Komano et al. [14] gave a scheme with a tighter security reduction in 2003. Vasco et al. [15] discussed the combined public key cryptosystem in the identity-based setting in 2008, and gave an example that an IND-CCA2 (indistinguishability of ciphertexts under adaptive chosen ciphertext attacks) secure public key encryption scheme and an EUF-CMA (existential unforgeability against chosen message attacks) secure signature scheme are no longer secure when they share the same key pair. Paterson et al. [16] revisited the combined public key cryptosystem in 2011, and gave a general construction and a concrete construction in the standard model respectively. Further they gave a scheme where encryption, signature and

signcryption share the same key pair. Degabriele et al. [17] discussed the combined public key cryptosystem in the EMV (Europay, MasterCard and VISA) card setting in 2012. In the same year, Chen et al. [18] discussed the combined public key cryptosystem in the attribute-based cryptosystem setting. Bellare et al. [19] introduced the key-versatile signature in 2014, which allows one to sign with keys already in use for another purpose.

Han et al. [11] introduced the concept of generalized signcryption in 2006, and proposed a concrete scheme in the PKI setting. Wang et al. [20] pointed out some security flaws in scheme [11] and improved it, giving a security model for generalized signcryption schemes for the first time in 2007. Lal and Kushwah [21] gave a security model of the identity-based generalized signcryption and a concrete scheme in 2008. Yu et al. [22] pointed out that the security model introduced in [21] is not complete, and gave a new security model and a concrete provably secure scheme in 2010. In the same year, Kushwah and Lal [23] simplified the security model introduced in [22], and proposed a more efficient identity-based generalized signcryption scheme. Han and Gui [24] proposed a multi-receiver generalized signcryption scheme in 2009. Ji et al. [25] gave for the first time a certificateless generalized signcryption scheme and security model in 2010. In the same year, Kushwah and Lal [23] pointed out that the scheme [25] is insecure and proposed a new one. Zhou et al. [26] proposed a new certificateless generalized signcryption scheme which is secure against the malicious-but-passive key generation center attack in 2014. Wei et al. [27] proposed an identity-based generalized signcryption scheme in the standard model in 2015. In the same year, Zhou [28] pointed out that the multi-receiver generalized signcryption scheme [24] is insecure and improved it, and Han et al. [29] proposed a generalized signcryption scheme in the attribute-based setting.

Ring signature was first introduced by Rivest et al. [2] in 2001. Abe et al. [30] proposed a ring signature scheme which uses RSA-type keys and DL-type keys to form a ring in 2002. Lv et al. [31] introduced the verifiable ring signature in 2003. In the verifiable ring signature, the actual signer can prove that he/she is the actual signer at a later stage. Liu et al. [32] introduced the linkable ring signature in 2004. In the linkable ring signature, two ring signatures can be linked if they are produced by the same signer. In the same year, Liu et al. [33] introduced three kinds of security models and two kinds of attacks called group-changing-attack and multiple-known-signature existential forgery to ring signature schemes. In the same year, Herranz et al. [34] introduced the ring forking lemma for the security proof of ring signatures. Bender et al. [35] introduced the strongest security models for the ring signature schemes by considering insider corruption attacks in 2006. In addition, the identity-based ring signature [36], certificateless ring signature [37], proxy ring signature [38] and blind ring signature [39], etc. were also proposed.

Huang et al. [9] extended ring signature to ring signcryption and proposed a concrete scheme in the identity-based setting in 2005, but the ciphertext of their scheme is too long. Zhu et al. [40] proposed an efficient identity-based ring signcryption scheme to reduce the ciphertext size in 2008. In the same year, Zhang et al. [41] introduced an identity-based ring signcryption scheme in which the actual signcrypter can prove that he/she is the actual signcrypter in a later stage. But unfortunately, Li et al. [42] pointed out that scheme [41] is insecure and improved it. Zhang et al. [43] proposed an efficient identity-based ring signcryption scheme to improve the efficiency of existing schemes in 2009. Deng et al. [44] proposed an identity-based ring signcryption scheme in 2014. But the pairing computations required in their scheme is linear with the ring size n. Other schemes proposed include the certificateless ring signcryption [45], the attribute-based ring signcryption [46] and the threshold ring signcryption [47], etc.

3. Preliminaries

3.1 Bilinear pairing

Let G_1 and G_2 be two multiplicative cyclic groups of prime order q and g be a generator of G_1. The map $e: G_1 \times G_1 \to G_2$ is said to be an admissible bilinear pairing if the following three conditions hold.

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

(2) Non-degeneracy: $e(g,g) \neq 1_{G_2}$.

(3) Computability: for all $P,Q \in G_1$, there exists an efficient algorithm to compute $e(P,Q)$.

3.2 Complexity assumption

(1) Bilinear Diffie-Hellman (BDH) Problem:

Given $(P,aP,bP,cP) \in G_1^4$ for unknown $a,b,c \in Z_q$, one must compute $e(P,P)^{abc}$.

The advantage of any probabilistic polynomial time (PPT) algorithm A in solving the BDH problem in (G_1,G_2,e) is defined to be: $ADV_A^{BDH} = \Pr[A(P,aP,bP,cP) = e(P,P)^{abc}, a,b,c \in Z_q]$.

BDH assumption: for every PPT algorithm A, ADV_A^{BDH} is negligible.

(2) Decisional Bilinear Diffie-Hellman (DBDH) Problem:

Given $(P,aP,bP,cP,T) \in G_1^4 \times G_2$ for unknown $a,b,c \in Z_q$, one must decide whether $T = e(P,P)^{abc}$.

The advantage of any PPT algorithm A in solving the DBDH problem in (G_1,G_2,e) is defined to be:

$$ADV_A^{DBDH} = \Pr[A(P,aP,bP,cP,T) = 1, a,b,c \in Z_q] - \Pr[A(P,aP,bP,cP,e(P,P)^{abc}) = 1, a,b,c \in Z_q].$$

DBDH assumption: for every PPT algorithm A, ADV_A^{DBDH} is negligible.

(3) Gap Bilinear Diffie-Hellman (GBDH) Problem [48]:

Given $(P,aP,bP,cP) \in G_1^4$ for unknown $a,b,c \in Z_q$, one must compute $e(P,P)^{abc}$ with the help of a DBDH oracle.

The advantage of any PPT algorithm A in solving the GBDH problem in (G_1,G_2,e) is defined to be: $ADV_A^{GBDH} = \Pr[A^o(P,aP,bP,cP) = e(P,P)^{abc}, a,b,c \in Z_q]$, where o denotes a DBDH oracle.

GBDH assumption: for every PPT algorithm A, ADV_A^{GBDH} is negligible.

(4) Computational Diffie-Hellman (CDH) Problem:

Given $(P,aP,bP) \in G_1^3$ for unknown $a,b \in Z_q$, one must compute abP.

The advantage of any PPT algorithm A in solving the CDH problem in G_1 is defined to be:

$$ADV_A^{CDH} = \Pr[A(P,aP,bP) = abP, a,b \in Z_q].$$

CDH assumption: for every PPT algorithm A, ADV_A^{CDH} is negligible.

(5) Gap Diffie-Hellman (GDH') Problem [48]:

Given $(P,aP,bP) \in G_1^3$ for unknown $a,b \in Z_q$, one must compute abP with the help of a DBDH oracle.

The advantage of any PPT algorithm A in solving the GDH' problem in (G_1,G_2,e) is defined to be: $ADV_A^{GDH'} = \Pr[A^o(P,aP,bP) = abP, a,b \in Z_q]$, where o denotes a DBDH oracle.

GDH' **assumption**: for every PPT algorithm A, $ADV_A^{GDH'}$ is negligible.

3.3 Definition of the identity-based generalized ring signcryption

An identity-based GRSC scheme consists of the following four algorithms, involving the ring $L=(ID_1,ID_2,...,ID_n)$, the sender ID_s ($s\in\{1,2,...,n\}$), and the receiver ID_r (ID_r may be null):

(1) $Setup(1^k)$: Given a security parameter 1^k, the PKG generates a master secret key s and a common parameter $params$. $params$ are public to all. PKG keeps the secret key s private.

(2) $Extract(params,s,ID)$: On input of $params$ and a user's identity ID, the PKG uses s to generate a private key D_{ID}, and then sends it to the user securely.

(3) $GRSC$: This algorithm has two modes: the ring signature mode and the ring signcryption mode.

$Ring-signature \bmod e(Params,m,L,D_{ID_s},ID_r)$: If the input of the receiver's identity ID_r is null, it runs in this mode. Other inputs are the message m, the $params$, the ring $L=(ID_1,ID_2,...,ID_n)$ and the actual signer's private key D_{ID_s} ($s\in\{1,2,...,n\}$). It generates a ring signature σ on (m,L).

$Ring-signcryption \bmod e(Params,m,L,D_{ID_s},ID_r)$: If the input of the receiver's identity ID_r is not null, it runs in this mode. Other inputs are the message m, the $params$, the ring $L=(ID_1,ID_2,...,ID_n)$, the sender's private key D_{ID_s} ($s\in\{1,2,...,n\}$). It generates a ring signcryption σ on (m,L).

(4) $UN-GRSC$: This algorithm also has two modes: the ring signature verification mode and the ring un-signcryption mode.

$Ring-signature\ verification \bmod e(Params,\sigma,L,ID_r)$: If the input of the receiver's identity ID_r is null, it runs in this mode. Any person can verify the validity of the ring signature σ. If it is correct, the ring signature is accepted.

$Ring-un-signcryption \bmod e(Params,\sigma,L,ID_r,D_{ID_r})$: If the input of the receiver's identity ID_r is not null, it runs in this mode. The receiver ID_r uses his private key D_{ID_r} to recover the message m and verify the validity of the ring signcryption σ. If it is correct, the ring signcryption is accepted.

For consistency, we require if $\sigma=GRSC(Params,m,L,D_{ID_s},ID_r)$, then $UN-GRSC(Params,\sigma,L,ID_r)=true$ for ID_r is null or $UN-GRSC(Params,\sigma,L,ID_r,D_{ID_r})=m$ for ID_r is not null.

3.4 Security model of identity-based generalized ring signcryption

To be secure, an identity-based generalized ring signcryption scheme must be confidential (in the ring signcryption mode), unforgeable (in both modes), and signer ambiguous (in both modes).

Definition 1 (confidentiality)

An identity-based GRSC scheme is semantically secure against the adaptive chosen ciphertext and chosen id attacks (IND-ID-GRSC-CCA for short) in the ring signcryption mode if no PPT adversary A has a non-negligible advantage in the following game:

(1) $Setup$: The challenger C runs the setup algorithm to generate a master secret key s and a common parameter $params$. C gives $params$ to A and keeps s secret.

(2) *Phase* 1: A can make the following polynomially bounded number of queries adaptively.

(a) *Extract queries*: A produces an identity ID to query for its private key. C runs the extract algorithm to produce a D_{ID} and returns it to A.

(b) *GRSC queries*: A produces a message m, a ring $L=(ID_1,ID_2,...,ID_n)$, and a receiver's identity ID_r. Here if ID_r is null, it is equal to a ring signature query or else it is equal to a ring signcryption query. C randomly selects an index s from L, extracts its private key D_{ID_s}, and then runs the GRSC algorithm and returns the output σ to A.

(c) *UN – GRSC queries*: A produces a σ, a ring $L=(ID_1,ID_2,...,ID_n)$, and a receiver's identity ID_r. Here if ID_r is null, it is equal to a ring signature verification query or else it is equal to a ring un-signcryption query. If it is a ring signature verification query, C runs the UN-GPSC algorithm to return true or false to A. If it is a ring un-signcryption query, C first extracts the private key of ID_r, and then runs the UN-GPSC algorithm to return the plaintext m or an invalid symbol $\perp$ to A;

(3) *Challenge*: The attacker A selects two equal-length but different messages m_0, m_1, a ring $L^*=(ID_1^*,ID_2^*,...,ID_n^*)$, and a challenge identity ID_r^* (ID_r^* must not be null). Here A is not allowed to make the extraction query to identity ID_r^*. C randomly selects a bit $b\in\{0,1\}$ and an index s from L^*, extracts its private key $D_{ID_s^*}$, and computes $\sigma^*=GRSC(m_b,L^*,D_{ID_s^*},ID_r^*)$. Then C gives σ^* to A.

(4) *Phase* 2: The attacker A can adaptively make a series of queries like in Phase 1, but he cannot make an extraction query of identity ID_r^* and cannot make a UN-GRSC query to (σ^*,L^*,ID_r^*).

(5) *Guess*: When the attacker A wants to end the game, he/she must give his/her guess $b'\in\{0,1\}$. If $b'=b$, he/she wins the game.

The advantage of the adversary A is defined as: $Adv^{IND-ID-GRSC-CCA}(A):=2\Pr[b'=b]-1$.

Note: We allow the attacker A to make queries about the secret keys of the ring L^* in the challenge stage, but these insider attackers cannot breach the security of the scheme.

Definition 2 (unforgeability)

An identity-based GRSC scheme is existentially unforgeable against the adaptive chosen message and chosen id attacks (EUF-ID-GRSC-CMA for short) in the ring signature mode or ring signcryption mode if no PPT adversary A has a non-negligible advantage in the following game:

(1) *Setup*: it is the same as in the confidentiality game.

(2) *Attack*: the attacker A can issue the same queries as in the confidentiality game.

(3) *Forgery*: The attacker A outputs a forged ciphertext σ^* (which may be a ring signature or ring signcryption) on message m^* and ring $L^*=(ID_1^*,ID_2^*,...,ID_n^*)$, and the receiver is ID_r^* (ID_r^* may be null). The ciphertext σ^* is not the output of GRSC query. A does not make extraction queries of any users in the ring $L^*=(ID_1^*,ID_2^*,...,ID_n^*)$, and σ^* can pass through the validity of UN-GRSC.

A's advantage is its probability of victory.

Note: We allow the attacker A to make a query about the secret key of the receiver ID_r^* (if ID_r^* is not null) in the forgery stage, but the insider attacker ID_r^* cannot breach the security of the scheme.

Note: In the above forgery stage, ID_r^* may be null. If ID_r^* is null, it runs in the ring signature mode or else it runs in the ring signcryption mode. So the two modes share the same game.

Definition 3 (signer ambiguity)

An identity-based generalized ring signcryption scheme is unconditionally signer-ambiguous if for any ciphertext $\sigma^* = GRSC(Params, m^*, L^*, D_{ID_s^*}, ID_r^*)$ (which may be a ring signature or a ring signcryption), where $L^* = (ID_1^*, ID_2^*, ..., ID_n^*)$ and $s \in \{1,2,...,n\}$, any verifier A even with unbounded computing resources, cannot identify the actual signer or signcrypter with a probability better than a random guess. In othwe words, A can only output the actual signer or signcrypter ID_s with a probability no better than $1/n$ ($1/(n-1)$ if A is in the signers set).

4. An Efficient Identity-Based Generalized Ring Signcryption Scheme

4.1 The concrete scheme

Setup：Given a security parameter 1^k, the PKG selects two cyclic groups $(G_1,+)$ and $(G_2,\cdot)$ of prime order q, a generator P of G_1, a bilinear map $e: G_1 \times G_1 \to G_2$, and three hash functions: $H_1: \{0,1\}^* \to G_1$, $H_2: \{0,1\}^* \to \{0,1\}^l$, $H_3: \{0,1\}^* \to Z_q^*$. l represents the bit length of a message. Then the PKG randomly selects $s \in Z_q^*$ as the master secret key, and sets $P_{pub} = sP$ as the master public key. In addition, the PKG defines a special function f. If the receiver's identity ID_r is null then $f(ID_r) = 0$; else $f(ID_r) = 1$. The system public parameters are $\{e, G_1, G_2, q, P, P_{pub}, H_1, H_2, H_3, f\}$.

Extract: Let ID_u be a user's identity. The PKG computes his private key as $D_{ID_u} = s \cdot Q(ID_u)$, $Q(ID_u) = H_1(ID_u)$.

GRSC: Let $L = \{ID_1, ID_2, ..., ID_n\}$, $m \in \{0,1\}^l$, and ID_r be the receiver. The actual signer's private key is D_{ID_s}, $1 \le s \le n$. He/she produces the generalized ring signcryption $\sigma = \{c, R, U_1, U_2, ..., U_n, V\}$ as follows:

(1) Computes $f(ID_r)$.

(2) Randomly chooses $t \in Z_q^*$, and computes $R = f(ID_r) \cdot tP$, $w = e(P_{pub}, Q_{ID_r})^{t \cdot f(ID_r)}$, $c = f(ID_r) \cdot H_2(w, R, Q_{ID_1}, Q_{ID_2}, ..., Q_{ID_n}) \oplus m$.

(3) Randomly chooses $U_i \in G_1$ and computes $h_i = H_3(c, L, U_i, Q_{ID_r})$ for $i \in \{1,...,n\} \setminus \{s\}$.

(4) Randomly chooses $r_s \in Z_q^*$, and computes $U_s = r_s P - \sum_{i=1, i \ne s}^{n} (h_i Q_{ID_i} + U_i)$, $h_s = H_3(c, L, U_s, Q_{ID_r})$, and $V = r_s P_{pub} + h_s D_{ID_s}$.

UN-GRSC: Given a generalized ring signcryption ciphertext $\sigma = \{c, R, U_1, U_2, ..., U_n, V\}$ on (m,L). The verifier does the following.

If $R = O$ (O represents the point at infinity), σ is a ring signature.

(1) Computes $h_i = H_3(c, L, U_i, Q_{ID_r})$, for $i \in \{1,2,...,n\}$.

(2) Verifies whether $e(P, V) = e(P_{pub}, \sum_{i=1}^{n} (h_i Q_{ID_i} + U_i))$.

If $R \ne O$, σ is a ring signcryption.

(1) Computes $h_i = H_3(c, L, U_i, Q_{ID_r})$, for $i \in \{1,2,...,n\}$.

(2) Verifies whether $e(P,V) = e(P_{pub}, \sum_{i=1}^{n}(h_i Q_{ID_i} + U_i))$.

(3) If the above equation holds true, he/she computes $w = e(R, D_{ID_r})$, $m = H_2(w, R, Q_{ID_1}, Q_{ID_2}, ..., Q_{ID_n}) \oplus c$.

4.2 Adaptation :

The scheme is an adaptive scheme that can switch to two different modes according to the receiver's identity ID_r. If the input of the receiver's identity ID_r is null, then it works in the ring signature mode or else it works in the ring signcryption mode. So these two modes share the same algorithm, and we can use the same key pair to ring-sign or ring-signcrypt a document.

5. Analysis of the Proposed Scheme

5.1 Correctness

(1) $e(P,V) = e(P, r_s P_{pub} + h_s D_{ID_s}) = e(P_{pub}, r_s P + h_s Q_{ID_s})$

$$= e(P_{pub}, U_s + \sum_{i=1, i\neq s}^{n}(h_i Q_{ID_i} + U_i) + h_s Q_{ID_s})$$

$$= e(P_{pub}, \sum_{i=1}^{n}(h_i Q_{ID_i} + U_i))$$

(2) $w = e(P_{pub}, Q_{ID_r})^t = e(tP, sQ_{ID_r}) = e(R, D_{ID_r})$

5.2 Confidentiality

Theorem 1. In the random oracle model, if there is a PPT attacker A having non-negligible advantage ε against the IND-ID-GRSC-CCA security of our scheme running in the ring signcryption mode when running in time T and performing at most q_{GRSC} GRSC queries, $q_{UN-GRSC}$ UN-GRSC queries, q_{H_1} H_1 queries, q_{H_2} H_2 queries, q_{H_3} H_3 queries and q_E extraction queries, then GBDH problem can be solved with a probability of $\varepsilon' \geq \varepsilon \cdot 1/q_{H_1} \cdot (1-1/q_{H_1}) \cdot (1-q_{UN-GRSC}/2^k)$ in a time $T' \leq T + O((((q_{GRSC} + q_{UN-GRSC}) \cdot n) + q_E) \cdot t_m + q_{GRSC} \cdot t_e + (q_{GRSC} + q_{UN-GRSC}) \cdot t_p)$, where t_m, t_e and t_p represent the time for a scalar multiplication on G_1, an exponentiation on G_2 and a pairing operation respectively.

Proof. Our proof is partially similar to scheme [48]. Let's suppose the challenger C is given $(P, A = aP, B = bP, C = cP) \in G_1^4$ for random $a,b,c \in Z_q^*$. C does not know the values of a, b and c, and is asked to compute $e(P,P)^{abc}$ with the help of a DBDH oracle. To utilize the adversary A, the challenger C will simulate extraction oracle, GRSC oracle, UN-GRSC oracle, H_1 oracle, H_2 oracle and H_3 oracle to provide responses to A's queries. C maintains three lists L_1, L_2 and L_3, which are initially empty. We assume all queries in the following are distinct and A

will ask for $H_1(ID)$ before ID is used in any other queries. In the beginning, C gives the system parameters $params$ to A with $P_{pub}=aP$ and he randomly selects a number $\theta \in \{1,2,...,q_{H_1}\}$.

H_1 **queries:** On the i-th query ID, if $i \neq \theta$ C randomly selects $x \in Z_q^*$ and repeats the process until x is not in the list L_1 and sets $Q_{ID}=xP$. Then C stores (i,ID,x) in the list L_1 and returns Q_{ID} to A. Otherwise, C stores $(\theta,ID,-)$ in the list L_1 and returns $Q_{ID_\theta}=bP$ to A.

H_2 **queries:** A supplies an item $(w,R,Q_{ID_1},Q_{ID_2},...,Q_{ID_n})$. C does the following.

(1) C checks if the DBDH oracle returns 1 when queried with the tuple (aP,bP,cP,w). If it is, C returns w and stops.

(2) Otherwise, C goes through the list L_2 with entries $(*,R,Q_{ID_1},Q_{ID_2},...,Q_{ID_n},h_2)$, so that for different values of h_2, the DBDH oracle returns 1 when queried on the tuple (aP,bP,R,w). If such a tuple exists, C returns h_2 and replaces the symbol * with w.

(3) Otherwise, C randomly selects $h_2 \in \{0,1\}^l$ and repeats the process until h_2 is not in the list L_2. C stores the item $(w,R,Q_{ID_1},Q_{ID_2},...,Q_{ID_n},h_2)$ in the list L_2, and returns h_2 to A.

H_3 **queries:** A supplies an item (c,L,U_i,Q_{ID_r}). C randomly selects $h_3 \in Z_q^*$ and repeats the process until h_3 is not in the list L_3. C stores the item (c,L,U_i,Q_{ID_r},h_3) in the list L_3, and returns h_3 to A.

Extract queries: A supplies an identity ID, C searches in the list L_1 on ID and obtains (i,ID,x). If $i=\theta$ then C outputs failure and aborts. Otherwise, C returns $x(aP)$.

GRSC queries: A produces a message m, a ring $L=(ID_1,ID_2,...,ID_n)$, and a receiver's identity ID_r. Here if ID_r is null, it is equal to a ring signature query or else it is equal to a ring signcryption query. C randomly selects an index s from L.

(1) $ID_s \neq ID_\theta$. C runs the GRSC algorithm as normal because C can get the private key of ID_s.

(2) $ID_s = ID_\theta$. C produces the GRSC ciphertext as follows.

(a) Computes $f(ID_r)$.

(b) Randomly selects $t \in Z_q^*$ and computes $R=f(ID_r)\cdot tP$, $w=e(P_{pub},Q_{ID_r})^{t\cdot f(ID_r)}$ and $c=f(ID_r)\cdot H_2(w,R,Q_{ID_1},Q_{ID_2},...,Q_{ID_n})\oplus m$.

(c) Randomly selects $U_i \in G_1$ and computes $h_i=H_3(c,L,U_i,Q_{ID_r})$ for $i \in \{1,...,n\}\setminus\{s\}$.

(d) Randomly selects $z,h_s \in Z_q^*$ and computes $U_s=zP-h_sQ_{ID_s}-\sum_{i=1,i\neq s}^{n}(h_iQ_{ID_i}+U_i)$.

(e) Saves item (c,L,U_s,Q_{ID_r},h_s) to the list L_3. If a collision occurs in the list L_3, C repeats the step (d).

(f) Computes $V=z(aP)$ and outputs the GRSC ciphertext $\sigma=\{c,R,U_1,U_2,...,U_n,V\}$.

UN-GRSC queries: A produces a GRSC ciphertext $\sigma=\{c,R,U_1,U_2,...,U_n,V\}$, a ring $L=(ID_1,ID_2,...,ID_n)$, and a receiver's identity ID_r. Here if ID_r is null, it is equal to a ring signature verification query or else it is equal to a ring un-signcryption query. If it is a ring signature verification query, which just needs public parameters. If it is a ring un-signcryption query, consider two cases:

(1) $ID_r \neq ID_\theta$. C runs the UN-GRSC algorithm as normal because C can get the private

key of ID_r.

(2) $ID_r = ID_\theta$. C first runs the verification part of the UN-GRSC algorithm, which just needs public parameters. If the verification does not succeed, C returns $\perp$. Otherwise, it means the verification of the UN-GRSC algorithm is correct. In this situation, C checks if a tuple $(w, R, Q_{ID_1}, Q_{ID_2}, ..., Q_{ID_n}, h_2)$ exists in the list L_2, so that for some w, the DBDH oracle returns 1 when queried on (aP, bP, R, w). If such a tuple exists, C recovers the message m using the hash value h_2. Otherwise, C randomly selects $h_2 \in \{0,1\}^l$ and repeats the process until h_2 is not in the list L_2. C stores the item $(*, R, Q_{ID_1}, Q_{ID_2}, ..., Q_{ID_n}, h_2)$ in the list L_2 and recovers the message m using the hash value h_2. The symbol * denotes an unknown value of pairing.

At last, the attacker A outputs two equal-length but different messages m_0, m_1, a ring $L^* = (ID_1^*, ID_2^*, ..., ID_n^*)$ and a challenge identity ID_r^*. If $ID_r^* \neq ID_\theta$, C outputs failure and aborts; otherwise C proceeds to construct a challenge as follows. C sets $R^* = cP$, selects a random bit b, a random hash h_2^* and sets $c^* = h_2^* \oplus m_b$. C randomly selects $s \in \{1,2,...,n\}$ and makes an extraction query to get the private key $D_{ID_s^*}$ of ID_s^*. C randomly selects $U_i^* \in G_1$ and computes $h_i^* = H_3(c^*, L^*, U_i^*, Q_{ID_r^*})$ for $i \in \{1,...,n\} \setminus \{s\}$. C randomly selects $r_s^* \in Z_q^*$ and computes $U_s^* = r_s^* P - \sum_{i=1, i \neq s}^{n} (h_i^* Q_{ID_i^*} + U_i^*)$, $h_s^* = H_3(c^*, L^*, U_s^*, Q_{ID_r^*})$ and $V^* = r_s^* P_{pub} + h_s^* D_{ID_s^*}$. The challenge ciphertext $\sigma^* = \{c^*, R^*, U_1^*, U_2^*, ..., U_n^*, V^*\}$.

In the second stage of the confidentiality game, A can adaptively make a series of queries like before with the restrictions as in the confidentiality game. At last, A must give out its guess. A cannot find out that σ^* is not a valid ciphertext unless he/she asks for the hash value of $H_2(w^* = e(P,P)^{abc}, R^*, Q_{ID_1^*}, Q_{ID_2^*}, ..., Q_{ID_n^*})$. If this happens, C will solve the GDBH problem due to the first step of H_2 oracle.

Now we assess the probability of success. In the challenge stage, the probability of $ID_r^* = ID_\theta$ is $1/q_{H_1}$. The probability of A querying the private key of ID_θ is $1/q_{H_1}$. In the UN-GRSC queries, the probability of C rejecting a valid ciphertext does not exceed $q_{UN-GRSC}/2^k$.

The time complexity of C depends on the scalar multiplication on G_1, the exponentiation on G_2 and pairing operations needed in all above queries. The extraction queries need $O(1)$ scalar multiplications. The GRSC queries need $O(n)$ scalar multiplications, $O(1)$ exponentiations and $O(1)$ pairings. The UN-GRSC queries need $O(n)$ scalar multiplications and $O(1)$ pairings.

5.3 Unforgeability

Theorem 2. In the random oracle model, if there is a PPT attacker A having non-negligible advantage $\varepsilon \geq 7V_{q_{H_3},n}/2^k$ $(V_{q_{H_3},n} = q_{H_3}(q_{H_3}-1)...(q_{H_3}-n+1))$ against the EUF-ID-GRSC-CMA security of our scheme running in the ring signature mode or ring signcryption mode when running in time T and performing at most q_{GRSC} GRSC queries, $q_{UN-GRSC}$ UN-GRSC queries, q_{H_1} H_1 queries, q_{H_2} H_2 queries, q_{H_3} H_3 queries and q_E extraction queries, then GDH'

problem can be solved with a probability of $\varepsilon' \geq (\varepsilon^2/66V_{q_{H_3},n})\cdot 1/q_{H_1}\cdot(1-1/q_{H_1})\cdot(1-q_{UN-GRSC}/2^k)$ in a time $T' \leq T+O((((q_{GRSC}+q_{UN-GRSC})\cdot n)+q_E)\cdot t_m+q_{GRSC}\cdot t_e+(q_{GRSC}+q_{UN-GRSC})\cdot t_p)$, where t_m, t_e and t_p represent the time for a scalar multiplication on G_1, an exponentiation on G_2 and a pairing operation respectively.

Proof. Suppose the challenger C is given $(P, A=aP, B=bP)\in G_1^3$ for random $a,b\in Z_q^*$. C does not know the values of a and b, and is asked to compute abP with the help of a DBDH oracle. To utilize the adversary A, the challenger C will simulate extraction oracle, GRSC oracle, UN-GRSC oracle, H_1 oracle, H_2 oracle and H_3 oracle to provide responses to A's queries. C maintains three lists L_1, L_2 and L_3, which are initially empty. We assume all queries in the following are distinct and A will ask for $H_1(ID)$ before ID is used in any other queries. In the beginning, C gives the system parameters $params$ to A with $P_{pub}=aP$ and he/she randomly selects a number $\theta\in\{1,2,...,q_{H_1}\}$.

The H_1, H_3, GRSC, UN-GRSC and extraction queries are the same as in Theorem 1.

H_2 **queries:** A supplies an item $(w,R,Q_{ID_1},Q_{ID_2},...,Q_{ID_n})$. C does the following.

(1) C goes through the list L_2 with entries $(*,R,Q_{ID_1},Q_{ID_2},...,Q_{ID_n},h_2)$, so that for different values of h_2, the DBDH oracle returns 1 when queried on the tuple (aP,bP,R,w). If such a tuple exists, C returns h_2 and replaces the symbol * with w.

(2) Otherwise, C randomly selects $h_2\in\{0,1\}^l$ and repeats the process until h_2 is not in the list L_2. C stores the item $(w,R,Q_{ID_1},Q_{ID_2},...,Q_{ID_n},h_2)$ in the list L_2, and returns h_2 to A.

At last, A outputs a forged ciphertext $\sigma^*=\{c^*,R^*,U_1^*,U_2^*,...,U_n^*,V^*\}$ (it may be a ring signature or ring signcryption) on message m^*, ring $L^*=(ID_1^*,ID_2^*,...,ID_n^*)$ and the receiver ID_r^* (ID_r^* may be null). If σ^* can pass the validation of UN-GRSC algorithm and A does not violate the restrictions of Definition 2, according to the ring forking lemma [34], we can get two valid ring signatures $\{m^*,U_1^*,U_2^*,...,U_n^*,V^*\}$ and $\{m^*,U_1^*,U_2^*,...,U_n^*,V'\}$ so that $h_i^*\neq h_i'$ for some $i\in\{1,2,...,n\}$ and $h_j^*=h_j'$ for all $j\in\{1,2,...,n\}\setminus\{i\}$. If $ID_i=ID_\theta$, we can solve the GDH' problem as follows: $V^*-V'=(h_\theta^*-h_\theta')D_{ID_\theta}=(h_\theta^*-h_\theta')abP$, $abP=(V^*-V')(h_\theta^*-h_\theta')^{-1}$.

Now we assess the probability of success. In the forgery stage, the probability of $ID_i=ID_\theta$ is $1/q_{H_1}$. The probability of A querying the private key of ID_θ is $1/q_{H_1}$. In the UN-GRSC queries, the probability of C rejecting a valid ciphertext does not exceed $q_{UN-GRSC}/2^k$. Combined with the ring forking lemma, the probability of C success is $\varepsilon' \geq (\varepsilon^2/66V_{q_{H_3},n})\cdot 1/q_{H_1}\cdot(1-1/q_{H_1})\cdot(1-q_{UN-GRSC}/2^k)$.

The time complexity of C is the same as in Theorem 1.

5.4 Signer ambiguity

Theorem 3. Our scheme allows unconditional signer ambiguity.

Proof. The proof is similar to scheme [49]. Since $U_i\in G_1$ for $i\in\{1,...,n\}\setminus\{s\}$, r_s, and t are randomly selected, hence $(U_1,U_2,...,U_n)$ and R are also uniformly distributed. c does not contain any information about the actual signer or signcrypter. It still needs to consider whether $V=r_sP_{pub}+h_sD_{ID_s}$ leaks information about the actual signer or signcrypter. Let us

consider the following equation:

$$\begin{aligned} e(P,V) &= e(P, r_s P_{pub} + h_s D_{ID_s}) \\ &= e(P_{pub}, r_s P + h_s Q_{ID_s}) \\ &= e(P_{pub}, r_s P) \cdot e(P_{pub}, h_s Q_{ID_s}) \\ &= e(P_{pub}, U_s + \sum_{i=1, i\neq s}^{n} (h_i \cdot Q_{ID_i} + U_i)) \cdot e(P_{pub}, h_s Q_{ID_s}) \end{aligned}$$

It seems that an attacker can check whether ID_j is the actual signer or signcrypter by checking whether the following equation holds:

$$e(P_{pub}, U_j + \sum_{i=1, i\neq j}^{n} (h_i \cdot Q_{ID_i} + U_i)) = \frac{e(P,V)}{e(P_{pub}, h_j Q_{ID_j})}.$$

However, the equation holds not only when j=s, but also when $\forall j \in \{1,2,...,n\} \setminus \{s\}$. i.e. the signature is symmetric.

Thus, for any fixed message m and fixed ring L, the distribution of $\sigma = \{c, R, U_1, U_2, ..., U_n, V\}$ is independent and uniformly distributed no matter who is the actual signer or signcrypter. An attacker has no advantage in identifying the actual signer or signcrypter over random guessing.

5.5 Comparison of performance

We compare our scheme in the ring signcryption mode with other identity-based ring signcryption schemes using bilinear pairings, including Zhu et al.'s scheme [40], Li et al.'s scheme [42], Zhang et al.'s scheme [43] and Deng's scheme [44]. The comparison is listed in **Table 1**. Pa, SM and Ex represent the pairing computation, scalar multiplication on G_1 and exponentiation on G_2 respectively. From **Table 1**, we can see that the pairing computations of scheme [44] is linear with the ring size n in the signcryption and un-signcryption stages, while others just need constant pairing computations. The scalar multiplication computations of our scheme are the least in the signcryption stage ($n \geq 2$) and are one of the least in the un-signcryption stage. The ciphertext sizes of all schemes are almost the same.

In order to understand the comparison more directly, we use PBC library [50] to give out the concrete experimental data. The hardware platform is an Inter Core i7-4510U CPU 2.0 GHz with 8 GB memory and the operating system is Windows 7 home basic 64-bit. The supersingular elliptic curve is $E/F_p : y^2 = x^3 + x$ with embedding degree 2, where q is a 160-bit Solinas prime $2^{159} + 2^{107} + 1$ and p a 512-bit prime satisfying $p + 1 = qh$ (h is a multiple of 12). Its security level is equivalent to 80-bit AES. In this experimental environment, the average computational time of a pairing, a scalar multiplication on G_1 and an exponentiation on G_2 is listed in **Table 2** (we have experimented it 100 times). By combining **Table 1** and **Table 2**, and letting the ring size n be 10, we get **Table 3**. Obviously, our scheme is highly efficient. In addition, our scheme uses only one key pair and one algorithm. Let the identity of a user be 160 bit, the bit length of G_1 be 512 bit and the EXE file be 273KB in the above situation. Thus, our scheme is able to save key pair storage by 1184 bit and one EXE file storage by almost 273KB.

In addition, we compare our scheme in the ring signcryption mode ($n = 1$) with Han et al.'s [11] scheme in the signcryption mode. The comparison is listed in **Table 4**. By combining **Table 4** and **Table 2**, and letting the ring size n be 1, we get **Table 5**. As the bilinear pairing is a very time consuming operation and scheme [11] is not pairing-based, the performance of scheme [11] is much better than ours. So designing pairing-free GRSC schemes will be our

next work. In addition, although scheme [11] is better than ours, it is not a ring signature/signcryption scheme, which means it does not allow anonymity.

Table 1. Comparison of performance I

Scheme	Signcryption	Un-signcryption	Signature-size
[40]	$Pa+(2n+3)\cdot SM$	$3\cdot Pa+n\cdot SM$	$\|m\|+(n+2)\cdot\|G_1\|$
[42]	$Pa+(2n+1)\cdot SM+Ex$	$3\cdot Pa+n\cdot SM$	$\|m\|+(n+2)\cdot\|G_1\|$
[43]	$Pa+(2n+4)\cdot SM$	$4\cdot Pa+n\cdot SM$	$\|m\|+(n+2)\cdot\|G_1\|$
[44]	$2n\cdot Pa+(2n+1)\cdot SM$	$(2n+1)\cdot Pa+2n\cdot SM$	$\|m\|+(n+1)\cdot\|G_1\|+\|q\|$
Ours	$Pa+(n+3)\cdot SM+Ex$	$3\cdot Pa+n\cdot SM$	$\|m\|+(n+2)\cdot\|G_1\|$

Table 2. Cryptographic operation time (milliseconds)

Pa	SM	Ex
15.58	7.62	1.8

Table 3. Comparison of performance II (milisecondes, n=10)

Scheme	Signcryption	Un-signcryption
[40]	190.84	122.94
[42]	177.4	122.94
[43]	198.46	138.52
[44]	471.62	479.58
Ours	116.44	122.94

Table 4. Comparison of performance III (n=1)

Scheme	Signcryption	Un-signcryption	Signature-size
[11]	$2\cdot SM$	$3\cdot SM$	$\|m\|+\|G_1\|+\|q\|+\|\mathrm{MAC}\|$
Ours	$Pa+4\cdot SM+Ex$	$3\cdot Pa+SM$	$\|m\|+3\cdot\|G_1\|$

Table 5. Comparison of performance IV (milisecondes, n=1)

Scheme	Signcryption	Un-signcryption
[11]	15.24	22.86
Ours	47.86	54.36

5.6 Application of the scheme

Generalized ring signcryption can be applied in many practical areas. In general, if a person wants to sign a document anonymously, he/she can use a ring signature. If he/she wants to sign a document anonymously while keeping the document confidential, he/she can use a ring signcryption. Using our generalized ring signcryption, he/she just needs to hold one key pair and use one algorithm to achieve both functions. In this way, the key management and system deployment will be simplified. In the following, we give a concrete example to show the advantages of the generalized ring signcryption.

In recent years, wireless body area networks (WBANs) have attracted much attention from both academia and industry. Multiple wearable or implanted intelligent physiological sensors will collect various vital signals in order to monitor the patient's health status, and these collected signals will be transmitted wirelessly to a controller (mobile phone or PDA). Then the controller will transmit all this information to a remote health server, so that this information will be shared and processed by many doctors. Meanwhile, the patient can consult

doctors remotely through the WBANs. The doctors only need to know the bio-information of the patient while all private information such as name and age, etc. must be kept secret; therefore, anonymity must be provided [51,52]. At the same time, confidentiality and/or authentication must also be guaranteed. Generalized ring signcryption is well suited to this scenario. For bio-information, the controller can transmit it by ring signcryption to the remote health server to guarantee confidentiality, authentication and anonymity. For consulting information, the controller can transmit it by ring signature to guarantee authentication and anonymity as ring signature requires less computation. Using our generalized ring signcryption scheme, the controller will need to hold one key pair and use one algorithm only. It can be illustrated in **Fig. 1**.

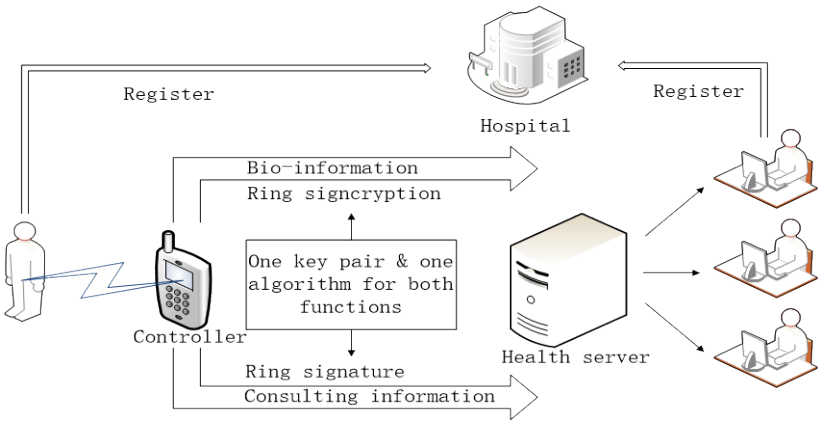

Fig. 1. Application of GRSC scheme in WBANs

Now, we will show in detail how our GRSC scheme is going to be applied in the WBANs. Firstly, the hospital runs the setup algorithm to produce the system public parameters $\{e,G_1,G_2,q,P,P_{pub},H_1,H_2,H_3,f\}$ and the master secret key s. Secondly, the patients and doctors get their private keys D_{ID_u} from the hospital. Thirdly, the sender patient spontaneously conscripts other n-1 patients to form a ring. For the Bio-information, he/she calls the GRSC algorithm in the ring signcryption mode to produce a ciphertext $\sigma=\{c,R,U_1,U_2,...,U_n,V\}$. For the consulting information, he/she calls the GRSC algorithm in the ring signature mode to produce a ciphertext $\sigma=\{c,R,U_1,U_2,...,U_n,V\}$. If $R=O$ (O represents the point at infinity), σ is a ring signature. The receiver doctor verifies $e(P,V)=e(P_{pub},\sum_{i=1}^{n}(h_iQ_{ID_i}+U_i))$. If it holds true, he/she accepts σ, or otherwise rejects σ. If $R\neq O$, σ is a ring signcryption. The receiver doctor verifies $e(P,V)=e(P_{pub},\sum_{i=1}^{n}(h_iQ_{ID_i}+U_i))$. If it holds true, he/she recovers the message $m=H_2(w,R,Q_{ID_1},Q_{ID_2},...,Q_{ID_n})\oplus c$.

6. Conclusion

In this paper, we introduce a new concept of generalized ring signcryption, which can perform ring signature and ring signcryption with only one key pair and one algorithm. It is very suitable for a system which has a large number of users, or has limited storage space, or whose

function requirements may be changed later. Then we give a formal definition and a security model of GRSC and propose a concrete scheme. Our scheme is secure under the GBDH assumption and $GDH^{'}$ assumption in the random oracle model and allows unconditional anonymity. Compared with other identity-based ring signcryption schemes that use bilinear pairings, ours is a highly efficient one. Future work is to design GRSC schemes without bilinear pairings.

References

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. of Crypto'1984*, pp. 47-53, Aug 19-22, 1984. Article(CrossRef Link)

[2] R. L. Rivest, A. Shamir and Y. Tauman, "How to leak a secret," in *Proc. of AsiaCrypt'2001*, pp. 552-565, Dec 9-13, 2001. Article(CrossRefLink)

[3] J. Y. Hwang, L. Q. Chen and H. S. Cho, "Short dynamic group signature scheme supporting controllable linkability," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1109-1124, 2015. Article(CrossRefLink)

[4] J. K. Liu, V. K. Wei and D. S. Wong, "Linkable spontaneous anonymous group signature for Ad Hoc groups (extended abstract)," in *Proc. of ACISP'2004*, pp. 325-335, Jul 13-15, 2004. Article(CrossRefLink)

[5] S. S. M. Chow, J. K. Liu and D. S. Wong, "Robust receipt-free election system with ballot secrecy and verifiability," in *Proc. of NDSS'2008*, pp. 81-94, Feb 8-11, 2008.

[6] H. Xiong, Z. Chen and F. G. Li, "Bibber-anonymous english auction protocol based on revocable ring signature," *Expert Systems with Applications*, vol. 39, no. 8, pp. 7062-7066, 2012. Article(CrossRefLink)

[7] L. Chen, C. Kudla and K. Paterson, "Concurrent signatures," in *Proc. of EuroCrypt'2004*, pp. 287-305, May 2-6, 2004. Article(CrossRefLink)

[8] F. Laguillaumie and D. Vergnaud, "Multi-designated verifiers signatures," in *Proc. of ICICS' 2004*, pp. 495-507, Oct 27-29, 2004. Article(CrossRefLink)

[9] X. Y. Huang, W. Susilo, Y. Mu and F. T. Zhang, "Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world," in *Proc. of AINA'2005*, pp. 649-654, Mar 28-30, 2005. Article(CrossRefLink)

[10] S. Haber and B. Pinkas, "Securely combining public-key cryptosystems," in *Proc. of CCS'2001*, pp. 215-224, Nov 6-8, 2001. Article(CrossRefLink)

[11] Y. L. Han, X. Y. Yang, P. Wei, Y. M. Wang and Y. P. Hu, "ECGSC: elliptic curve based generalized signcryption," in *Proc. of UIC 2006*, pp. 956–965, Sep 3-6, 2006. Article(CrossRefLink)

[12] J. S. Coron, M. Joye, D. Naccache and P. Paillier, "Universal padding schemes for RSA," in *Proc. of Crypto'2002*, pp. 226-241, Aug 18-22, 2002. Article(CrossRefLink)

[13] M. Bellare and P. Rogaway, "The exact security of digital signatures - How to sign with RSA and Rabin," in *Proc. of EuroCrypt'1996*, pp. 399-416, May 12-16, 1996. Article(CrossRefLink)

[14] Y. C. Komano and K. Ohta, "Efficient universal padding techniques for multiplicative trapdoor one-way permutation," in *Proc. of Crypto'2003*, pp. 366-382, Aug 17-21, 2003. Article(CrossRefLink)

[15] M. I. G. Vasco, F. Hess and R. Steinwandt, "Combined (identity-based) public key schemes," *Cryptology ePrint Archive*, Report 2008/466 (2008). Available at http://eprint.iacr.org/ 2008/466 [Accessed on 3 Feb 2009].

[16] K. G. Paterson, J. C. N. Schuldt, M. Stam and S. Thomson, "On the joint security of encryption and signature, revisited," in *Proc. of AsiaCrypt'2011*, pp. 161-178, Dec 4-8, 2011. Article(CrossRefLink)

[17] J. P. Degabriele, A. Lehmann and K. G. Paterson, "On the joint security of encryption and signature in EMV," in *Proc. of CT-RSA'2012*, pp. 116-135, Feb 27-Mar 2, 2012. Article(CrossRefLink)

[18] C. Chen, J. Chen, H. W. Lim Z. F. Zhang and D. G. Feng, "Combined public-key schemes: the case of ABE and ABS," in *Proc. of ProvSec 2012*, pp. 53-69, Sep 26-28, 2012. Article(CrossRefLink)
[19] M. Bellare, S. Meiklejohn and S. Thomson, "Key-versatile signatures and applications: RKA, KDM and joint enc/sig," in *Proc. of EuroCrypt'2014*, pp. 496-513, May 11-15, 2014. Article(CrossRefLink)
[20] X. A. Wang, X. Y. Yang and Y. L. Han, "Provable secure generalized signcryption," Cryptology ePrint Archive, Report 2007/173 (2007). Available at http://eprint.iacr.org/2007/173 [Accessed on 21 May 2008].
[21] S. Lal and P. Kushwah, "ID based generalized signcryption," Cryptology ePrint Archive, Report 2008/084 (2008). Available at http://eprint.iacr.org/2008/084 [Accessed on 26 Feb 2008].
[22] G. Yu, X. X. Ma, Y. Shen and W. B. Han, "Provable secure identity based generalized signcryption scheme," *Theoretical Compute Science*, vol. 411, no. 40-42, pp. 3614-3624, 2010. Article(CrossRefLink)
[23] P. Kushwah and S. Lal, "Efficient generalized signcryption schemes," Cryptology ePrint Archive, Report 2010/346 (2010). Available at http://eprint.iacr.org/2010/346 [Accessed on 16 Jun 2010].
[24] 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. Article(CrossRefLink)
[25] H. F. Ji, W. B. Han and L. Zhao, "Certificateless generalized signcryption," Cryptology ePrint Archive, Report 2010/204 (2010). Available at http://eprint.iacr.org/2010/204 [accessed on 19 Apr 2010].
[26] 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. Article(CrossRefLink)
[27] G. 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*, vol. 318, pp. 111-122, 2015. Article(CrossRefLink)
[28] C. X. Zhou, "An improved multi-receiver generalized signcryption scheme," *International Journal of Network Security*, vol. 17, no. 3, pp. 340-350, 2015.
[29] Y. L. Han, Y. C. Bai, D. Y. Fang and X. Y. Yang, "The new attribute-based generalized signcryption scheme," in *Proc. of ICYCSEE'2015*, pp. 353-360, 2015. Article(CrossRefLink)
[30] M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n signatures from a variety of keys," in *Proc. of AsiaCrypt'2002*, pp.415-432, Dec 1-5, 2002. Article(CrossRefLink)
[31] J. Q. Lv and X. M. Wang, "Verifiable ring signature," in *Proc. of DMS'2003*, pp. 663–667, Sep, 2003.
[32] J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups (extended abstract)," in *Proc. of ACISP*, pp. 325-335, Jul. 13-15, 2004. Article(CrossRefLink)
[33] J. K. Liu and D. S. Wong, "On the security models of (Threshold) ring signature schemes," in *Proc. of ICISC*, pp. 204-217, Dec. 2-3, 2004. Article(CrossRefLink)
[34] J. Herranz and G. Saez, "New identity-based ring signature schemes," in *Proc. of ICICS'2004*, pp. 27–39, Oct 27-29, 2004. Article(CrossRefLink)
[35] A. Bender, J. Katz and R. Morselli, "Ring signatures: stronger definitions, and constructions without random oracles," in *Proc. of TCC*, pp. 60-79, Mar. 4-7, 2006. Article(CrossRefLink)
[36] M. H. Au, J. K. Liu, W. Susilo and J. Y. Zhou, "Realizing fully secure unrestricted ID-based ring signature in the standard model based on HIBE," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1909-1922, 2013. Article(CrossRefLink)
[37] L. Z. Deng, "Certificateless ring signature based on RSA problem and DL problem," *RAIRO-Theoretical Informatics and Applications*, vol. 49, no. 4, pp. 307-318, 2015. Article(CrossRefLink)
[38] M. R. Asaar, M. Salmasizadeh and W. Susilo, "A short identity-based proxy ring signature scheme from RSA," *Computer Standards & Interfaces*, vol. 38, pp. 144-151, 2015. Article(CrossRefLink)
[39] M. H. Au and W. Susilo, "Two-party (blind) ring signatures and their applications," in *Proc. of ISPEC*, pp. 403-417, May 5-8, 2014. Article(CrossRefLink)

[40] L. J. Zhu and F. T. Zhang, "Efficient id-based ring signature and ring signcryption schemes," in *Proc. of CIS'2008*, pp. 303-307, Dec 13-17, 2008. Article(CrossRefLink)
[41] M. W. Zhang, B. Yang, S. L. Zhu and W. Z. Zhang, "Efficient secret authenticatable anonymous signcryption scheme with identity privacy," in *Proc. of ISI 2008*, pp.126-137, Jun. 17, 2008. Article(CrossRefLink)
[42] F. G. Li, S. Masaaki and T. Tsuyoshi, "Analysis and improvement of authenticatable ring signcryption scheme," *Journal of Shanghai Jiaotong University (Science)*, vol. 13, no. 6, pp. 679-683, 2008. Article(CrossRefLink)
[43] J. H. Zhang, S. N. Gao, H. Chen and Q. Geng, "A novel ID-based anonymous signcryption scheme," in *Proc. of APWeb/WAIM 2009*, pp. 604-610, Apr 2-4, 2009. Article(CrossRefLink)
[44] L. Z. Deng, J. W. Zeng and S. W. Li, "A new identity-based ring signcryption scheme," *International Journal of Electronic Security and Digital Forensics*, vol. 6, no. 4, pp. 333-342, 2014. Article(CrossRefLink)
[45] H. Sun, "Efficient certificateless ring signcryption in the standard model," *Journal of Computational Information Systems*, vol. 10, no. 8, pp. 3181-3188, 2014.
[46] Z. Z. Guo, M. C. Li and X. X. Fan, "Attribute-based ring signcryption scheme," *Security and Communication Networks*, vol. 6, no. 6, pp. 790-796, 2013. Article(CrossRefLink)
[47] L. Z. Deng, S. W. Li and Y. F. Yu, "Identity-based threshold ring signcryption from pairing," *International Journal of Electronic Security and Digital Forensics*, vol. 6, no. 2, pp. 90-103, 2014. Article(CrossRefLink)
[48] M. Barbosa and P. Farshim, "Certificateless signcryption," in *Proc. of ASIACCS'2008*, pp. 369-372, Mar 18-20, 2008. Article(CrossRefLink)
[49] S. S. M. Chow, S. M. Yiu and L. C. K. Hui, "Efficient identity based ring signature," in *Proc. of ACNS 2005*, pp. 499-512, Jun 7-10, 2005. Article(CrossRefLink)
[50] PBC library. http://crypto.stanford.edu/pbc.
[51] J. W. Liu, Z. H. Zhang, X. F. Chen and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 332-342, 2014. Article(CrossRefLink)
[52] C. J. Wang and J. Liu, "Attribute-based ring signcryption scheme and its application in wireless body area networks," in *Proc. of ICA3PP 2015*, pp. 521-530, Nov 18-20, 2015. Article(CrossRefLink)

Caixue Zhou received the B.S. in Computer Science Department from Fudan University in 1988, Shanghai, China and the M.S. in Space College of Beijing University of Aeronautics and Astronautics in 1991, Beijing, China. He has been served as an Associate Professor in the School of Information Science and Technology, Jiujiang University, Jiujiang, China since 2007. He is a member of the CCF (China Computer Federation) and a member of CACR(Chinese Association for Cryptologic Research). His research interests include applied cryptography and security of computer networks .

Zongmin Cui received the B.E degree from Southeast University in 2002 and the M.S. degree from HuaZhong University of Science and Technology in 2006. He received the Ph.D. Degree from Huazhong University of Science and Technology in 2014. He is currently an associate professor with the School of Information Science and Technology, Jiujiang University, Jiujiang, China. His research interests include cloud security, authorization update, key management, access control, and publish/subscribe system.

Guangyong Gao received the Ph.D. Degree from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2012. Currently he is an associate professor with the School of Information Science and Technology, Jiujiang University, Jiujiang, China. His research interests include Multimedia Information Security, Digital Image Processing and Computer Networks Security.