An Identity-Based Ring Signcryption Scheme

Gaurav Sharma, Suman Bala and Anil K. Verma

Abstract Signcryption enables a user to perform digital signature for providing authenticity and public key encryption for providing message confidentiality simultaneously in a single logical step with a cost lesser than sign-then- encrypt approach. As the concept of ring signcryption emerged, various practical applications like electronic transaction protocol and key management protocols, felt the requirement of signer's privacy, which was lacking in normal signcryption schemes. Without revealing the users' identity of the ring signcryption can provide confidentiality and authenticity both. In this paper, we present a new ID-based ring signcryption scheme, motivated to the scheme provided by Zhu et al. [1]. Selvi et al. [2] and Wang et al. [3] found some security flaws in the Zhu's scheme [1], which is being considered and repaired in this paper. The proposed scheme is proven to be secure against adaptive chosen ciphertext ring attacks (IND-IDRSC-CCA2) and secure against an existential forgery for adaptive chosen message attacks (EF-IDRSC-ACMA).

Keywords Identity-based ring signcryption · Identity based cryptography · Ring signcryption · Confidentiality · Anonymity · Unforgeability · Bilinear pairing

G. Sharma (✉) · S. Bala · A. K. Verma
Computer Science and Engineering Department, Thapar University, Patiala, India
e-mail: gaurav.sharma@thapar.edu

S. Bala
e-mail: suman.bala@thapar.edu

A. K. Verma
e-mail: akverma@thapar.edu

K. J. Kim and K.-Y. Chung (eds.), *IT Convergence and Security 2012*,
Lecture Notes in Electrical Engineering 215, DOI: 10.1007/978-94-007-5860-5_18,

1 Introduction

The idea behind Identity-based Ring Signcryption is a collaboration of different security techniques, such as Identity Based Cryptography, Ring Signature and Signcryption. Identity based cryptography provides a variant to Certificate based public key cryptography; ring signature provides anonymity along with the authenticity in such a way that even verifier does not know who has signed the message but he can verify that one of the ring member has signed it, while signcryption provides the encryption and signature in a single logical step to obtain confidentiality, integrity, authentication and non-repudiation.The concept of identity-based cryptography was introduced by Shamir [4] in 1984, to remove the need of certification of the public keys, which is required in the conventional public key cryptography setting. But, Shamir only proposed ID-based signature and left the ID-based encryption as an open problem. Boneh and Franklin [5] presented the first Identity Based Encryption scheme that uses bilinear maps (the Weil or Tate pairing) over super singular elliptic curves. Rivest et al. [6] introduced ring signature which is a group oriented signature with privacy concerns: a user can anonymously sign a message on behalf of a group of spontaneously conscripted users, without managers including the actual signer. The first ID-based ring signature scheme with bilinear parings, was proposed by Zhang and Kim [7]. Yuliang Zheng [8] introduced the concept of public key signcryption which fulfils both the functions of digital signature and public key encryption in a logically single step, and with a cost lower than that required by the sign-then- encrypt approach. However, Zheng didn't prove any security notions which was further proposed by Baek et al. [9], described a formal security model in a multi-user setting.

Xinyi Huang [10] combined the concepts of ID-based ring signature and signcryption together as identity-based ring signcryption. They provided a formal proof of their scheme with the chosen ciphertext security (IND-IDRSC-CCA) under the Decisional Bilinear Diffie-Hellman assumption. However, Huang et al.'s [10] scheme is computationally inefficient, since the number of pairing computations grows linearly with the group size. Huang et al.'s scheme needs $n + 4$ pairing computations, where n denotes the size of the group. The scheme lacks anonymity and had a key escrow problem as the scheme was based on ID-PKC. Wang et al. [11] eliminated the key escrow problem in [10] by proposing a verifiable certificateless ring signcryption scheme and gave a formal security proof of the scheme in random oracle model. But this scheme also needs $n + 4$ pairing computations. The problem of ID-based ring signcryption schemes is that they are derived from bilinear pairings, and the number of pairing computations grows linearly with the group size. Zhu [1] solved the above problem; they proposed an efficient ID-based ring signcryption scheme, which only takes four pairing operations for any group size. Zhu [12] proposed an ID-based ring signcryption scheme, which offers savings in the ciphertext length and the computational cost.

The other schemes include Li et al. [13], Yong et al. [14] and Zhang [15]. Selvi et al. [2] proved that Li et al. [16] and Zhu et al. scheme [1] are not secure against adaptive chosen ciphertext attack while Zhu's [12] scheme and Yong's [14] scheme are not secure against chosen plaintext attack. Qi's [17] proved that their scheme has the shortest ciphertext and is much more efficient than Huang's [10] and Selvi's [2] scheme. Selvi et al. [18] proved that Zhang et al. [19] scheme is insecure against confidentiality, existential unforgeability and anonymity attacks. Zhou [20] presented an efficient identity-based ring signcryption scheme in the standard model.

Roadmap: The remaining paper is organized as follows: Sect. 2 gives some preliminaries and basic definitions of Bilinear Pairing. The formal model has been discussed in Sect. 3. In Sect. 4, we propose our ID-based ring signcryption scheme; security analysis of the proposed scheme is discussed in Sect. 5. In Sect. 6, we concluded the remarks about the paper.

2 Preliminaries

2.1 Notations Used

The following notations have been made in common for all the existing schemes and Table 1 defines the description of the notations that have been used throughout the paper.

2.2 Basic Concepts on Bilinear Pairing

Let G_1 be a cyclic additive group generated by P of prime order q, and G_2 be a cyclic multiplicative group of the same order q. Let a and b be elements of Z_q^*. Assume that the discrete logarithm problem (DLP) in both G_1 and G_2 is hard. Let $\hat{e} : G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing with the following properties shown in Table 2.

Table 1 Notations used

k : security parameter	$\{0,1\}^l$: string with length l.
params : systems' public parameter generated by PKG	$\{0,1\}^*$: string with arbitrary length.
	$m \in_R M$: message, M: message space
t : secret key generated by PKG	$\hat{e} : G_1 \times G_1 \rightarrow G_2$is a bilinear pairing
G_1: cyclic additive group generated by P of prime order $q > 2^k$	ID_i: user identity
	S_i: private key of user i
G_2: cyclic multiplicative group generated by P of prime order $q > 2^k$	Q_i: public key of user i
	S : sender, R : receiver
$P \in G_1$: random generator	$\mathcal{L}$: group of ring members
P_{pub} public key of PKG	$\mathbb{C}$: signcrypted ciphertext
Z_q^*: multiplicative group modulo q.	$\mathcal{A}$: Adversary, $\mathcal{C}$: Challenger

Table 2 Properties of bilinear mapping

Bilinearity	$\forall P, Q, R \in_R G_1$, $\hat{e}(P+Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$, $\hat{e}(P, Q+R) = \hat{e}(P, Q)\hat{e}(P, R)$. In particular, for any $a, b \in Z_q^*$ $\hat{e}(aP, bP) = \hat{e}(P, P)^{ab} = \hat{e}(P, abP) = \hat{e}(abP, P)$
Non-degeneracy	$\exists P, Q, \in G_1 \ni \hat{e}(P, Q) \neq I_{G_2}$, where $I_{G_2}$is the identity of G_2
Computability	$\forall P, Q \in G_1$, there is an efficient algorithm to compute$\hat{e}(P, Q)$.

3 Formal Model of Identity Based Ring Signcryption

A generic ID-based ring signcryption scheme consists of five algorithms Setup, Keygen, Signcrypt, Unsigncrypt and Consistency. The description of these algorithms has been provided in Table 3.

4 Proposed Scheme

In this section, we propose our new Identity-Based Ring signcryption Scheme. Our scheme has four following algorithms:

1. *Setup* (k): Given a security parameter k, a trusted private key generator (PKG) generates the system's public parameters *params* and the corresponding master secret key t that is kept secret by PKG.
   a. The trusted authority randomly chooses $t \in_R Z_q^*$ keeps it as a master key and computes the corresponding public key $P_{pub} = tP$.
   b. Let $(G_1, +)$ and $(G_2, *)$ be two cyclic groups of prime order $q > 2^k$ and a random generator $P \in G_1$.
   c. $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing.
   d. Choose Hash Functions

$$H_1 : \{0,1\}^* \rightarrow G_1, H_2 : G_2 \rightarrow \{0,1\}^l, H_3 : \{0,1\}^* \rightarrow Z_q^*, H_4 : \{0,1\}^* \rightarrow \{0,1\}^l$$

Table 3 Generic identity based ring signcryption scheme

Setup	For a given parameter k, a trusted private key generator generates system's public parameters *params* and its corresponding master secret key t, which is kept secret.
Keygen	For a given user identity ID_i, PKG computes private key S_i by using *params* and $t$and transmits $S_i$to ID_i via secure channel.
Signcrypt	For sending a message m from sender to a receiver with identity ID_R, senders' private key S_S, and a group of ring members $\{U_i\}_{i=1 \mathrm{to} n}$ with identities $\mathcal{L} = \{ID_1, \ldots, ID_n\}$, sender computes a ciphertext.
Unsigncrypt	For retrieving a message m, if $\mathbb{C}$is a valid ring signcryption of $m$from the ring $\mathcal{L}$to ID_R or 'invalid', if $\mathbb{C}$ is an invalid ring signcryption.
Consistency	An identity based ring signcryption scheme is said to be consistent if $\Pr[\mathbb{C} \leftarrow signcrypt(m, \mathcal{L}, S_S, ID_R), m \leftarrow unsigncrypt(\mathbb{C}, \mathcal{L}, S_R)] = 1$

e. The public parameters are:$params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3, H_4\}$.

2. *Keygen* (ID_i): Given a user identity ID_i of user U_i, the PKG, using the public key computes the parameters *params* and the master secret key t, computes the corresponding private key S_i, and transmits it to ID_i in a secure way as follows.

a. The public key is computed as $Q_i = H_1(ID_i)$.
b. The corresponding private key $S_i = tQ_i$.
c. PKG sends S_i to user U_i via a secure channel.

3. *Signcrypt*: Let $\mathcal{L} = \{ID_1, \ldots, ID_n\}$ be a set of n ring members, such that $ID_S \in \mathcal{L}$. ID_R may or may not be in $\mathcal{L}$. The sender runs this algorithm to send a message $m \in M$, where M is a message space, to a receiver with identity ID_R, the senders private key S_S, outputs a ring signcryption $\mathbb{C}$ as follows:

a. Choose a random number $r \in_R Z_q^*$ and $m^* \in_R M$.And compute $R_0 = rP$, $R = e(rP_{pub}, Q_R)$, $k = H_2(R)$, $\mathbb{C}_1 = m^* \oplus k$
b. Choose $R_i \in G_1 \, \forall \, i = \{1, 2, \ldots, n\} \backslash \{S\}$ and compute $h_i = H_3(m||\mathcal{L}|| R_i||R_0)$.
c. Choose $r_S \in_R Z_q^* \, \forall \, i = S$ Compute $R_S = r_S Q_S - \sum_{i \neq S} (R_i + h_i Q_i)$, $h_S = H_3 (m||\mathcal{L}||R_S||R_0)$, $V = (h_S + r_S) S_S$, $\mathbb{C}_2 = (m||r_S||V) \oplus H_4(m^*||R_0)$.
d. Finally the sender outputs the ciphertext as $\sigma = (\mathcal{L}, R_0, R_1, \ldots, R_n, \mathbb{C}_1, \mathbb{C}_2)$to the receiver.

4. *Unsigncrypt*: This algorithm is executed by a receiver ID_R. This algorithm takes the ring signcryption σ, the ring members $\mathcal{L}$ and the private key S_R, as input and produces the plaintext m, if σ is a valid ring signcryption of m from the ring $\mathcal{L}$ to ID_R or 'invalid', if σ is an invalid ring signcryption as follows:

a. Compute $R' = e(R_0, S_R), k' = H_2(R'), m'^* = \mathbb{C}_1 \oplus k'$
b. Recover m', V' as $(m'||r_S||V') = \mathbb{C}_2 \oplus H_4(m'^*||R_0)$.
c. Compute $h'_i = H_3(m'||\mathcal{L}||R_i||R') \, \forall \, i = \{1, 2, \ldots, n\}$
d. Checks if $e(P, V') \stackrel{?}{=} e\left(P_{pub}, \sum_{i=1}^{n} (R_i + h_i Q_i)\right)$. If the check succeeds accept m, else return $\perp$.

5 Security Analyses of the Proposed Scheme

5.1 *Correctness*

In this section, a proof of correctness has been shown, that if the ciphertext $\mathbb{C}$ has been correctly generated, the verification equations will hold.

If $e(P, V') \stackrel{?}{=} e\left(P_{pub}, \sum_{i=1}^{n} (R_i + h_i Q_i)\right)$ holds.

Proof: $e(P,V) = e(P,(h_S + r_S)S_S) = e(P,(h_S + r_S)tQ_S) = e(tP, h_S Q_S + R_S + \sum_{i=1, i \neq s}^{n} (R_i + h_i Q_i)) = e\left(P_{pub}, \sum_{i=1}^{n} (R_i + h_i Q_i)\right)$

5.2 Security Analyses

5.2.1 Confidentiality

Theorem: If an IND-IRSC-CCA2 adversary $\mathcal{A}$ has an advantage ε against IRSC scheme, asking hash queries to random oracles $\mathcal{O}_{H_i}(i = 1, 2, 3, 4)$, q_e extract queries ($q_e = q_{e_1} + q_{e_2}$, where q_{e_1} and q_{e_2} are the number of extract queries in the first phase and second phase respectively), q_{sc} signcryption queries and q_{us} unsigncryption queries, then there exist an algorithm $\mathcal{C}$ that solves the CBDH problem with advantage $\varepsilon\left(\frac{1}{q_{H_1} q_{H_2}}\right)$.

5.2.2 Unforgeability

Theorem: An identity based ring signcryption scheme (IRSC) is said to be existentially unforgeable against adaptive chosen message attack (EUF-IRSC-CMA), against any polynomially bounded adversary $\mathcal{A}$ under the random oracle model if CDHP is hard.

6 Conclusion

Wang et al. [25] proved that the Zhu et al. scheme [1] to be insecure against anonymity and also does not satisfy the property of unforgeability. Selvi el al [2] also attacked and proved the scheme prone to confidentiality attack. Till now, a very few ID-based ring signcryption schemes have been proposed and most of them have been proved insecure. In this paper an efficient ID based ring signcryption scheme has been presented which has been proven secure against the primitive properties of signcryption: confidentiality, unforgeability and anonymity. The future work may include ring signcryption schemes in combination with ID-based threshold signcryption, ID-based proxy signcryption and id based hybrid signcryption schemes and certificate-less schemes in the standard model. Also, to reduce communication overhead, constant ciphertext size ring signcryption schemes can be improved.

References

1. Zhu Z, Zhang Y, Wang F (2008) An efficient and provable secure identity based ring signcryption scheme. Computer standards & interfaces, pp 649–654
2. Selvi SSD, Vivek SS, Rangan CP (2009) On the security of identity based ring signcryption schemes. In: Proceedings of 12th International Conference on ISC 2009, Pisa, Italy, Sept 7–9, 2009, Proceedings of LNCS 5735, Springer, Berlin, pp 310–325
3. Wang H, Yu H (2008) Cryptanalysis of two ring signcryption schemes. In: Inscrypt 2008, LNCS-5487, Springer, Berlin, pp 41–46
4. Shamir A (1984) Identity-based cryptosystems and signature schemes. In: Proceedings of CRYPTO '84, LNCS 196, Springer, Berlin, pp 47–53
5. Boneh D, Franklin M (2001) Identity-based encryption from the weil pairing. In: Proceedings of CRYPTO '01, LNCS 2139, Springer, Berlin, pp 213–229
6. Rivest RL, Shamir A, Tauman Y (2001) How to leak a secret. In: Proceedings of advances in cryptology in asiacrypt 2001, LNCS 2248, Springer, Berlin, pp 552–565
7. Zheng F, Kim K (2002) Id-based blind signature and ring signature from pairings. In: Proceedings of Asiacrypt 02, LNCS 2501, Springer, Berlin, pp 533–547
8. Zheng Y (1997) Digital signcryption or how to achieve cost (signature and encryption) cost (signature) + cost(encryption)'. In: Proceedings of CRYPTO-97, pp 165–179
9. Baek J, Steinfeld R, Zheng Y (2002) Formal proofs for the security of signcryption. In: Proceedings of PKC—02, LNCS 2274, pp 81–98
10. Huang X, Susilo W, Mu Y, Zhang F (2005) Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world. In: Proceedings of AINA 05, Taipei, Taiwan, pp 649–654
11. Wang L, Zhang G, Ma C (2007) A secure ring signcryption scheme for private and anonymous communication. In: Proceedings of international conference NPC workshops, 2007
12. Zhu L, Zhang F (2008) Efficient identity based ring signature and ring signcryption schemes. In: Proceedings of international conference on CIS'08, vol 2, pp 303–307
13. Li F, Xiong H, Yu Y (2008) An efficient ID-based ring signcryption scheme. In: Proceedings of ICCCCAS 2008, Xiamen, pp 542–546
14. Yu Y, Li F, Xu C, Sun Y (2008) An efficient identity-based anonymous signcryption scheme. Wuhan Univ J Nat Sci 13(6):670–674
15. Zhang J, Gao S, Chen H, Geng Q (2009) A novel id-based anonymous signcryption scheme. In: Proceedings of APWeb/WAIM, LNCS 5446, Springer, Berlin, pp 604–610
16. Li F, Shirase M, Takagi T (2008) Analysis and improvement of authenticatable ring signcryption scheme. J Shanghai Jiaotong Univ (Sci) 13(6):679–683
17. Qi ZH, Yang G, Ren XY, Li YW (2010) An ID-based ring signcryption scheme for wireless sensor networks. In: Proceedings of IET International of Conference WSN, China, pp 368–373
18. Selvi SSD, Vivek SS, Rangan CP (2010) Identity based ring signcryption with public verifiability. In: Proceedings of SECRYPT—10, LNCS 2010
19. Zhang M, Zhong Y, Yang B, Zhang W (2009) Analysis and improvement of an id-based anonymous signcryption model. In: Proceedings of ICIC (1), LNCS 5754
20. Zhou J (2011) An efficient identity-based ring signcryption scheme without random oracles. In: Proceedings of international conference on computer and electrical engineering 4th (ICCEE—11), 2011
21. Huang XY, Zhang FT, Wu W (2006) Identity-based ring signcryption scheme. Proc Tien Tzu Hsueh Pao/Acta Electronica Sinica 34(2):263–266
22. Malone-Lee J (2002) Identity based signcryption. J Cryptol 2002/098
23. Chow SSM, Yiu SM, Hui LCK (2005) Efficient identity based ring signature. In: Proceedings of ACNS 2005, LNCS 3531, Springer, Berlin, pp 499–512