On the Security of A Provably Secure Certificate Based Ring Signature Without Pairing

Ji Geng[1], Hu Xiong[1,2], Fagen Li[1], and Zhiguang Qin[1]
(Corresponding author: Hu Xiong)

School of Computer Science and Engineering, University of Electronic Science and Technology of China[1]
No. 4, North Jianshe Road, Chenghua District, chengdu, Sichuan 610054, China
State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences[2]
No. 19 Yuquan Road, Shijingshan District, Beijing 100190, China
(Email: xionghu.uestc@gmail.com)
(Received Feb. 11, 2014; revised and accepted Nov. 6, 2014)

Abstract

Featured with anonymity and spontaneity, ring signature has been widely adopted in various environments to offer anonymous authentication. To simplify the certificate management in traditional public key infrastructure (PKI) and solve the inherent key escrow problem in the Identity-based cryptography, Qin *et al.* propose a pairing-free ring signature scheme in the certificate-based cryptosystem recently. Unfortunately, we demonstrate that their scheme is not secure against the malicious certificate authority (CA) and key replacement attacks by giving concrete attack. Concretely, a malicious certificate authority (CA) can forge a signature on arbitrary message in name of any user's identity and a uncertified user is also able to forge a message.

Keywords: Certificate-based signature, forgery attack, ring signature

1 Introduction

Ring signature [19], which allows a user to issue a signature on behalf of a group of possible signers (ring), has been introduced by Rivest *et al.* in Asiacrypt 2001. The resulting ring signature can convince a verifier that one member in the ring indeed signed the message without revealing the real identity of the actual signer. Different from group signature [4], there is not group manager in the ring signature to handle the enrollment and revocation of the ring members. Specifically, the actual signer can conscript the other ring members to form the ring without their consent. Featured with anonymity and spontaneity, ring signature has been widely adopted to offer anonymous authentication in various scenarios. As a representative example, portable devices or mobile applications in the infrastructure-less mobile ad hoc networks (MANETs) can share data with the other participants to behave in intelligent manners. It is challenging to secure MANETs due to the openness and lack of the central authority. Taking MANETs as an example, there are several security requirements a practical system must satisfy, including:

- **Authenticity**: In the situation of MANETs, the data sent from the other participants would be misleading if it is forged by adversaries. Thus, it is desirable to authenticate the receiving data to resist the attacks mounted by the outside adversaries;
- **Anonymity**: The shared data in MANETs contains vast information of users, from which one can extract the location of the target users, etc. Therefore, any failures with regard to the privacy preserving may lead to the reluctance from the users to share data with others;
- ***Ad hoc***: In the MANETs, the formation of a group where the actual user hidden from is spontaneous due to the lack of central authority; and
- **Efficiency**: Taking the huge number of users in MANETs into account, a practical system must lower the computation and communication overhead as much as possible.

Ring signature can be viewed as an efficient solution on the aforementioned situation where the data authenticity and anonymity are expected. In addition to the data sharing in the MANETs (instantiated as Vehicular *ad hoc* networks [21] and wireless sensor networks [11]), ring signature can also be deployed in other environments such as routing protocol [16] and electronic auction protocol [22, 23]. Furthermore, ring signatures can also be viewed as the building block of concurrent signatures [5, 7] and optimistic fair exchange [12]. The survey of ring signatures can be found in [6, 25].

Table 1: Notations

Notations	Descriptions
MANETs:	**M**obile **A**d hoc **NET**work**s**
PKI:	**P**ublic **K**ey **I**nfrastructure
ID-PKC:	**Id**entity-based **P**ublic **K**ey **C**ryptography
CB-PKC:	**C**ertificate-**B**ased **P**ublic **K**ey **C**ryptography
CA:	**C**ertificate **A**uthority
PKG:	**P**rivate **K**ey **G**enerator
ID_i:	The identity of the user i
(upk_{ID_i}, usk_{ID_i}):	The user public/secret key pair of the user i
(R, k_i):	The certificate of the user i
$L_{ID} = \{ID_1, \cdots, ID_n\}$:	The identity set of n ring members
$L_{upk} = \{upk_{ID_1}, \cdots, upk_{ID_n}\}$:	The public key set of n ring members
$\mathcal{G}$:	A multiplicative group with order q, where q is prime number.
g:	A random generator chosen from $\mathcal{G}$
π_{u_i}:	The proof-of-knowledge (PoK) such that $PK\{(u_i) : U_1 = g^{u_i} \wedge U_2 = X^{u_i}\}$
H:	Secure hash function such as $H : \{0,1\}^* \to \mathbb{Z}_q^*$

In traditional public key infrastructure (PKI), a semi-trusted certificate authority (CA) is involved to generate a digital certificate to bind the public key and the corresponding identity. The management overhead of the public key certificate is considered to be costly. To simplify the certificate management, the notion of Identity-based public key cryptography (ID-PKC) has been introduced [20]. In ID-PKC, the public key of user can be easily derived from its digital identity such as email address or telephone number. To enjoy the merits of ID-PKC, the notion of ID-based ring signature schemes along with the extensions have been extensively investigated [2, 8, 24]. Unfortunately, a fully-trusted private key generator (PKG) is needed to generate the private key for each user according to its respective identity in ID-PKC. Thus, the key escrow problem is introduced into ID-PKC.

To simplify the heavy certificate management in traditional PKI and solve the key escrow problem in ID-PKC, a new paradigm, certificate-based public key cryptography (CB-PKC), is proposed by Gentry [10]. In CB-PKC, each user will generate the public and private key pair itself and the CA will issue the certificate using the private key generation algorithm in ID-PKC. In this way, the certificate will be used as part of the private key and third-party queries on certificate status in traditional PKI has already been eliminated in CB-PKC. Au *et al.* [1] introduce the notion of ring signature in the CB-PKC setting to enjoy the merits of CB-PKC and ring signature together, and further proposed a concrete certificate based ring signature based on bilinear pairing.

In order to remove the costly bilinear pairing operation, Qin *et al.* [18] proposed a pairing free certificate-based ring signature recently. Furthermore, they claimed that their scheme is provably secure in the random oracle model assuming the Discrete Logarithm assumption holds. Unfortunately, in this paper, we show that their scheme cannot achieve the claimed security by demonstrating two forgery attacks. Concretely, a malicious CA equipped with the master secret key can forge a valid signature on arbitrary message. In addition, a uncertified entity without a certificate issued by CA can also forge a valid signature on arbitrary message but replacing the public keys.

The rest of this paper is organized as follows. In Section 2, we review Qin *et al.*'s pairing-free certificate based ring signature scheme. In Section 3, we show that Qin *et al.*'s scheme is not secure and analyze the basic reason for the attack. Finally, the conclusions are given in Section 4.

2 Review of Qin et al.'s Scheme

Qin *et al.*'s certificate based ring signature scheme [18] is based on certificate-based signature scheme in [17] and ID-based ring signature scheme in [13]. The notation used in [18] is listed in Table 1 to improve the readability and we review Qin *et al.*'s scheme as follows.

1) Setup: Let $\mathcal{G}$ be a multiplicative group with order q. The CA selects a random generator $g \in \mathcal{G}$ and randomly chooses $x \in_R \mathbb{Z}_q^*$ as the master secret key. It sets $X = g^x$. Let $H : \{0,1\}^* \to \mathbb{Z}_q^*$ be a cryptographic hash function. The public parameters are given by params$=(\mathcal{G}, q, g, X, H)$ The multiplicative group can be implemented on the Elliptic curve cryptography (ECC). According to [3], to achieve the comparable level of security to 1024-bits RSA, the Koblitz elliptic curve $y^2 = x^3 + ax^2 + b$ defined on $\mathbb{F}_{2^{163}}$ providing ECC group can be adopted. Here, a is equal to 1 and b is a 163-bit random prime. Thus, the size of the element in group $\mathcal{G}$ (the master public key and the user public key) is assumed to be 163-bit.

2) UserKeyGen: User ID_i selects a secret value $u_i \in \mathbb{Z}_q^*$

as his secret key usk_{ID_i}, and computes his public key $upk_{ID_i} = (g^{u_i}, X^{u_i}, \pi_{u_i})$ where π_{u_i} is the following non-interactive proof-of-knowledge (PoK):

$$PK\{(u_i) : U_1 = g^{u_i} \wedge U_2 = X^{u_i}.\}$$

The subscript of u_i has been inadvertently omitted in [18]. This omission has been corrected to be consistent.

3) CertGen: Let $\tilde{h}_i = H(upk_{ID_i}, ID_i)$ for user ID_i with public key upk_{ID_i} and binary string ID_i which is used to identify the user. To generate a certificate for user ID_i, the CA randomly chooses $r \in_R \mathbb{Z}_q^*$, computes $R = g^r$ and $k_i = r^{-1}(\tilde{h}_i - xR) \bmod q$. The certificate is (R, k_i). Note that a correctly generated certificate should satisfy the following equality:

$$R^{k_i} X^R = g^{\tilde{h}_i}.$$

4) Ring-Sign: Suppose there is a group of n users whose identities form the set $L_{ID} = \{ID_1, \cdots, ID_n\}$, and their corresponding public keys form the set $L_{upk} = \{upk_{ID_1}, \cdots, upk_{ID_n}\}$. To sign a message $m \in \{0,1\}^*$ on behalf of the group, the actual signer, indexed by s using the secret key usk_{ID_s} and the certificate $cert_{ID_s}$, performs the following steps.

   a. For each $i \in \{1, \cdots, n\} \setminus \{s\}$, selects $y_i \in_R \mathbb{Z}_q^*$ uniformly at random and computes $Y_i = R^{-y_i}$.
   b. Compute $h_i = H(m \| L_{upk} \| L_{ID} \| Y_i)$ for $i \in \{1, \cdots, n\} \setminus \{s\}$.
   c. Choose $y_s \in_R \mathbb{Z}_q^*$, computes $Y_s = R^{-y_s} \prod_{i \neq s} (g^{u_i})^{h_i \tilde{h}_i} \prod_{i \neq s} (X^{u_i})^{-h_i R}$.
   d. Compute $h_s = H(m \| L_{upk} \| L_{ID} \| Y_s)$.
   e. Compute $z = (\sum_{i=1}^{n} y_i + h_s k_s u_s) \bmod q$.
   f. Output the ring signature on m as $\sigma = \{Y_1, \cdots, Y_n, R, z, \pi_{u_1}, \cdots, \pi_{u_n}\}$. Though $\{R, \pi_{u_1}, \cdots, \pi_{u_n}\}$ is needed in the Verify algorithm, it has been inadvertently omitted in the signature of [18]. This omission has been corrected to be consistent.

5) Verify: To verify a ring signature $\sigma = \{Y_1, \cdots, Y_n, R, z, \pi_{u_1}, \cdots, \pi_{u_n}\}$ on a message m with identities in L_{ID} and corresponding public keys in L_{upk}, the verifier performs the following steps.

   a. Check whether π_{u_i} is a valid PoK. If not, outputs $\perp$, Otherwise, run the next step.
   b. Compute $h_i = H(m \| L_{upk} \| L_{ID} \| Y_i)$ and $\tilde{h}_i = H(upk_{ID_i}, ID_i)$ for all $i \in \{1, \cdots, n\}$.
   c. Check whether

$$\prod_{i=1}^{n} (g^{u_i})^{h_i \tilde{h}_i} \stackrel{?}{=} R^z Y_1 \cdots Y_n \prod_{i=1}^{n} (X^{u_i})^{h_i R}$$

   d. Accept the ring signature as valid and outputs 1 if the above equation holds, otherwise, output 0.

3 Analysis of Qin *et al.*'s Scheme

It is non-trivial to devise secure certificate-based encryption/signature scheme since the certificate of the user will no longer be used to certify the corresponding public key instead it will be implicitly used as part of private key in the decryption/signing algorithm. In fact, several certificate-based encryption scheme [26] and certificate-based signature scheme [14, 17] have been shown to be insecure against the attacks mounted by an uncertified entity or malicious CA respectively [9, 15, 27]. Motivated by these attacks, we observe that Qin *et al.*'s certificate-based ring signature [18] is also insecure against the forgery attack. Comparing with the existing attack algorithms with respect to certificate based encryption/signature schemes [9, 15, 27], our work mainly focus on the insecurity of the certificate-based ring signature, where a large number of users are involved in the process of the signature generation.

According to [14, 15, 18, 27], two different types of attacks by the malicious CA and by an uncertified user should be considered in CB-PKC. On the one hand, the malicious CA, who has the master secret key, cannot obtain the user secret key and mount the public key replacement attack. On the other hand, the uncertified user can replace public keys of any entities in the system, but is not allowed to obtain the target user's certificate.

3.1 Malicious CA Attack on Qin *et al.*'s Scheme

Given a ring signature $\sigma = \{Y_1, \cdots, Y_n, R, z, \pi_{u_1}, \cdots, \pi_{u_n}\}$ with the identities in $L_{ID} = \{ID_1, \cdots, ID_n\}$ and corresponding public keys in $L_{upk} = \{upk_{ID_1}, \cdots, upk_{ID_n}\}$, the CA equipped with the master key x can forge a valid signature on arbitrary message m' as follows:

1) Randomly choose $j \in_R \{1, \cdots, n\}$.
2) Compute $\tilde{h}_j = H(upk_{ID_j}, ID_j)$.
3) Compute $R' = x^{-1}\tilde{h}_j$, where x is the master key.
4) For each $i \in \{1, \cdots, n\} \setminus \{j\}$, selects $y_i' \in_R \mathbb{Z}_q^*$ uniformly at random and computes $Y_i' = (R')^{-y_i'}$.
5) Compute $h_i' = H(m' \| L_{upk} \| L_{ID} \| Y_i')$ for $i \in \{1, \cdots, n\} \setminus \{j\}$.
6) Choose $y_j' \in_R \mathbb{Z}_q^*$, computes $Y_j' = (R')^{-y_j'} \prod_{i \neq j} (g^{u_i})^{h_i' \tilde{h}_i} \prod_{i \neq j} (X^{u_i})^{-h_i' R'}$.
7) Compute $z' = \sum_{i=1}^{n} y_i' \bmod q$.
8) Output the ring signature on m' as $\sigma = \{Y_1', \cdots, Y_n', R', z', \pi_{u_1}, \cdots, \pi_{u_n}\}$.

The following equations show that the signature $\sigma = \{Y_1', \cdots, Y_n', R', z', \pi_{u_1}, \cdots, \pi_{u_n}\}$ is valid.

$$\begin{aligned}\prod_{i=1}^{n}(g^{u_i})^{h_i\tilde{h}_i} &= \prod_{i\neq j}(g^{u_i})^{h_i'\tilde{h}_i} g^{xu_jh_j'x^{-1}\tilde{h}_j} \\ &= \prod_{i\neq j}(g^{u_i})^{h_i'\tilde{h}_i} g^{xu_jh_j'R'} \\ &= \prod_{i\neq j}(g^{u_i})^{h_i'\tilde{h}_i} X^{u_jh_j'R'} \\ &= (R')^{\sum_{i=1}^{n} y_i'} \prod_{i\neq j}(R')^{-y_i'} \cdot (R')^{-y_j'} \prod_{i\neq j}(g^{u_i})^{h_i'\tilde{h}_i} \\ &\quad \prod_{i\neq j}(X^{u_i})^{-h_i'R'} \prod_{i=1}^{n}(X^{u_i})^{h_i'R'} \\ &= (R')^{z'} Y_1' \cdot \cdots \cdot Y_n' \prod_{i=1}^{n}(X^{u_i})^{h_i'R'}.\end{aligned}$$

3.2 Key Replacement Attack on Qin *et al.*'s Scheme

In the following, we show that the scheme is not against an uncertified entity attack. Concretely, an entity without a certificate issued by CA can forge a valid signature on arbitrary message m' by replacing the public keys. The attack is depicted as follows:

1) Randomly choose $r \in_R \mathbb{Z}_q^*$ and compute $R' = g^r$.
2) Randomly choose $j \in_R \{1, \cdots, n\}$.
3) For each $i \in \{1, \cdots, n\} \setminus \{j\}$, selects $y_i' \in_R \mathbb{Z}_q^*$ uniformly at random and computes $Y_i' = g^{-y_i'}$.
4) Compute $h_i' = H(m' \| L_{upk} \| L_{ID} \| Y_i')$ for $i \in \{1, \cdots, n\} \setminus \{j\}$.
5) Choose $y_j' \in_R \mathbb{Z}_q^*$, computes $Y_j' = X^{-aR'} g^{-y_j'} \prod_{i\neq j}(g^{u_i})^{h_i'\tilde{h}_i} \prod_{i\neq j}(X^{u_i})^{-h_i'R'}$.
6) Compute $\tilde{h}_j = H(upk_{ID_j}, ID_j)$.
7) Compute $u_j = \frac{a}{\tilde{h}_j}$ as the secret key of user with identity ID_j, and set $upk_{ID_j} = (g^{u_j}, X^{u_j}, \pi_{u_j})$ as the public key of this user, where π_{u_j} is the following non-interactive proof-of-knowledge (PoK):
$$PK\{(u_j).: U_1 = g^{u_j} \wedge U_2 = X^{u_j}\}.$$
8) Compute $z' = \frac{ah_j'}{r} + \frac{\sum_{i=1}^{n} y_i'}{r} \bmod q$.
9) Output the ring signature on m' as $\sigma = \{Y_1', \cdots, Y_n', R', z', \pi_{u_1}, \cdots, \pi_{u_n}\}$.

The following equations show that the signature $\sigma = \{Y_1', \cdots, Y_n', R', z', \pi_{u_1}, \cdots, \pi_{u_n}\}$ is valid.

$$\begin{aligned}\prod_{i=1}^{n}(g^{u_i})^{h_i\tilde{h}_i} &= g^{u_j\tilde{h}_jh_j'} \prod_{i\neq j}(g^{u_i})^{h_i'\tilde{h}_i} \\ &= g^{\frac{a}{\tilde{h}_j}\tilde{h}_jh_j'} \prod_{i\neq j}(g^{u_i})^{h_i'\tilde{h}_i} \\ &= g^{ah_j'} \prod_{i\neq j}(g^{u_i})^{h_i'\tilde{h}_i} \\ &= g^{ah_j'} X^{-aR'} \prod_{i\neq j}(g^{u_i})^{h_i'\tilde{h}_i} X^{\frac{a}{h_j'}h_j'R'} \\ &= g^{ah_j'} X^{-aR'} \prod_{i\neq j}(g^{u_i})^{h_i'\tilde{h}_i} X^{u_jh_j'R'} \\ &= (g^r)^{\frac{ah_j'}{r} + \frac{\sum_{i=1}^{n} y_i'}{r}} \prod_{i\neq j} g^{-y_i'} X^{-aR'} g^{-y_j'} \\ &\quad \prod_{i\neq j}(g^{u_i})^{h_i'\tilde{h}_i} \prod_{i\neq j}(X^{u_i})^{-h_i'R'} \prod_{i=1}^{n}(X^{u_i})^{h_i'R'} \\ &= (R')^{z'} Y_1' \cdot \cdots \cdot Y_n' \prod_{i=1}^{n}(X^{u_i})^{h_i'R'}.\end{aligned}$$

4 Conclusions

In this paper, we have showed that the Qin *et al.* [18]'s certificate based ring signature scheme is not secure against the forgery attack. We consider pairing-free certificate based ring signature scheme along with provable security as an open problem and our future research work.

Acknowledgments

This work is partially supported by National Natural Science Foundation of China under Grant Nos. 61003230, 61370026, 61300191 and 61103206, the Fundamental Research Funds for the Central Universities under Grant No. ZYGX2013J073 and ZYGX2012J077, and the Applied Basic Research Program of Sichuan Province under Grant No. 2014JY0041.

References

[1] Man Ho Au, Joseph K. Liu, Willy Susilo, and Tsz Hon Yuen, "Certificate based (linkable) ring signature," in *3rd International Conference on Information Security Practice and Experience-ISPEC 2007*, pp. 79–92, Hong Kong, China, May 2007.

[2] Amit K Awasthi and Sunder Lal, "Id-based ring signature and proxy ring signature schemes from bilinear pairings," *International Journal of Network Security*, vol. 4, no. 2, pp. 187–192, 2007.

[3] Xuefei Cao, Weidong Kou, and Xiaoni Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," *In-*

formation Sciences, vol. 180, no. 15, pp. 2895–2903, 2010.

[4] David Chaum and Eugene van Hevst, "Group signature," in *Advances in Cryptology-EUROCRYPT 1991*, pp. 257–265, Brighton, UK, April 1991.

[5] Liqun Chen, Caroline Kudla, and Kenneth G. Paterson, "Concurrent signatures," in *Advances in Cryptology-EUROCRYPT 2004*, pp. 287–305, Interlaken, Switzerland, May 2004.

[6] Sherman S. M. Chow, Richard W. C. Lui, Lucas Chi Kwong Hui, and Siu-Ming Yiu, "Identity based ring signature: Why, how and what next," in *EuroPKI 2005*, pp. 144–161, Canterbury, UK, June 2005.

[7] Sherman S.M. Chow and WILLY Susilo, "Generic construction of (identity-based) perfect concurrent signatures," in *7th International Conference on Information and Communications Security-ICICS 2005*, pp. 194–206, Beijing, China, December 2005.

[8] Sherman S.M. Chow, Siu-Ming Yiu, and Lucas C.K. Hui, "Efficient identity based ring signature," in *3rd International Conference on Applied Cryptography and Network Security-ACNS 2005*, pp. 499–512, NY, USA, June 2005.

[9] David Galindo, Paz Morillo, and Carla Ràfols, "Breaking yum and lee generic constructions of certificate-less and certificate-based encryption schemes," in *3rd European PKI Workshop: Theory and Practice-EuroPKI 2006*, pp. 81–91, Turin, Italy, June 2006.

[10] Craig Gentry, "Certificate-based encryption and the certificate revocation problem," in *Advances in Cryptology-EUROCRYPT 2003*, pp. 272–293, Warsaw, Poland, May 2003.

[11] Daojing He, Jiajun Bu, Sencun Zhu, Sammy Chan, and Chun Chen, "Distributed access control with privacy support in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3472–3481, 2011.

[12] Qiong Huang, Guomin Yang, Duncan S. Wong, and Willy Susilo, "Efficient optimistic fair exchange secure in the multi-user setting and chosen-key model without random oracles," in *The Cryptographers' Track at the RSA Conference, CT-RSA 2008*, pp. 106–120, San Francisco, CA, USA, April 2008.

[13] Germán Sáez Javier Herranz, "New identity-based ring signature schemes," in *6th International Conference on Information and Communications Security-ICICS 2004*, pp. 27–39, Malaga, Spain, October 2004.

[14] Bo Gyeong Kang, Je Hong Park, and Sang Geun Hahn, "A certificate-based signature scheme," in *Topics in Cryptology-CT-RSA 2004*, pp. 99–111, CA, USA, February 2004.

[15] Jiguo Li, Xinyi Huang, Yi Mu, Willy Susilo, and Qianhong Wu, "Certificate-based signature: Security model and efficient construction," in *EuroPKI 2007*, pp. 110–125, Palma de Mallorca, Spain, June 2007.

[16] Xiaodong Lin, Rongxing Lu, Haojin Zhu, Pin-Han Ho, Xuemin (Sherman) Shen, and Zhenfu Cao, "Asrpake: An anonymous secure routing protocol with authenticated key exchange for wireless ad hoc networks," in *Proceedings of IEEE International Conference on Communications, ICC 2007*, pp. 1247–1253, Scotland, UK, June 2007.

[17] Joseph K. Liu, Joonsang Baek, Willy Susilo, and Jianying Zhou:, "Certificate-based signature schemes without pairings or random oracles," in *11th International Conference on Information Security-ISC 2008*, pp. 285–297, Taipei, Taiwan, September 2008.

[18] Zhiguang Qin, Hu Xiong, and Fagen Li, "A provably secure certicate based ring signature without pairing," *International Journal of Network Security*, vol. 16, no. 3, pp. 244–251, 2014.

[19] Ronald L. Rivest, Adi Shamir, and Yael Tauman, "How to leak a secret," in *Advances in Cryptology-AsiaCrypt 2001*, pp. 552–565, Gold Coast, Australia, December 2001.

[20] Adi Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology-Crypto 1984*, pp. 47–53, California, USA, August 1984.

[21] Hu Xiong, Konstantin Beznosov, Zhiguang Qin, and Matei Ripeanu, "Efficient and spontaneous privacy-preserving protocol for secure vehicular communication," in *Proceedings of IEEE International Conference on Communications, ICC 2010*, pp. 1–6, Cape Town, South Africa, May 2010.

[22] Hu Xiong, Zhong Chen, and Fagen Li, "Bidder-anonymous english auction protocol based on revocable ring signature," *Expert Systems with Applications*, vol. 39, no. 8, pp. 7062–7066, 2012.

[23] Hu Xiong, Zhiguang Qin, and Fagen Li, "An anonymous sealed-bid electronic auction based on ring signature," *International Journal of Network Security*, vol. 8, no. 3, pp. 235–242, 2009.

[24] Hu Xiong, Zhiguang Qin, and Fagen Li, "A certificateless proxy ring signature scheme with provable security," *International Journal of Network Security*, vol. 12, no. 2, pp. 92–106, 2011.

[25] Hu Xiong, Zhiguang Qin, and Fagen Li, "A taxonomy of ring signature schemes: Theory and applications," *IETE Journal Of Research*, vol. 59, no. 4, pp. 376–382, 2013.

[26] Dae Hyun Yum and Pil Joong Lee, "Identity-based cryptography in public key management," in *1st European PKI Workshop: Research and Applications-EuroPKI 2004*, pp. 71–84, Samos Island, Greece, June 2004.

[27] Jianhong Zhang, "On the security of a certificate-based signature scheme and its improvement with pairings," in *5th International Conference on Information Security Practice and Experience-ISPEC 2009*, pp. 47–58, Xi'an, China, April 2009.

Ji Geng is a professor in the School of Computer Science and Engineering, University of Electronic Science and Technology of China. He received his M.S. degree from

Southwest Jiaotong University in 1990. His research interests include: information security and system software.

Hu Xiong is an associate professor at University of Electronic Science and Technology of China (UESTC). He received his Ph.D degree from UESTC in 2009. His research interests include: cryptography and network security.

Fagen Li received his Ph.D. degree from Xidian University in 2007. He is now an associate professor in the School of Computer Science and Engineering, University of Electronic Science and Technology of China. His recent research interests include cryptography and network security.

Zhiguang Qin is the dean and professor in the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC). He received his PH.D. degree from UESTC in 1996. His research interests include: information security and computer network.