Security Flaw of an ECC-based Signcryption Scheme with Anonymity

Hu Xiong[1,2,3], Jianbin Hu[3], and Zhong Chen[3]

(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
Key Lab of Network Security and Cryptology & Fujian Normal University[2]
No. 8, Shangsan Road, Cangshan District, Fuzhou, Fujian, 350007, China
Institute of Software, School of Electronics Engineering and Computer Science & Peking University[3]
No. 5 Yiheyuan Road Haidian District, Beijing, 100085, China
(Email: xionghu.uestc@gmail.com)

(Received Dec. 23, 2010; revised and accepted Mar. 26, 2011)

Abstract

Signcryption is a cryptographic primitive that performs digital signature and public key encryption simultaneously, at lower computational costs and communication overhead than signing and encrypting separately. Recently, Chung *et al.* proposed an anonymous ECC-based signcryption scheme. We show that their scheme is not secure even against a chosen-plaintext attack.

Keywords: Anonymous, chosen plaintext attack, ECC-based cryptosystem, Signcryption

1 Introduction

Confidentiality, integrity, non-repudiation and authentication are the important requirements for many cryptographic applications. A traditional approach to achieve these requirements is to sign-then-encrypt the message. Signcryption, first proposed by Zheng in 1997 [25], is a cryptographic primitive that performs digital signature and public key encryption simultaneously, at lower computational costs and communication overheads than the signature-then-encryption approach. Several efficient signcryptionZheng2007 schemes have been proposed since 1997 [3, 10, 11, 13, 14, 17, 18, 23, 26]. The original scheme in [25] is constructed on the discrete logarithm problem but no security proof is given. Zheng's original construction [25] was only proven secure in 2002 by Baek et al. [2] who described a formal security model in a multi-user setting.

In 2002, Malone-Lee [12] proposed the first ID-based signcryption scheme using the bilinear pairings along with a security model. This model deals with notions of privacy and unforgeability. In 2003, Libert and Quisquater [15] pointed out that Malone-Lee's scheme [12] is not semantically secure and proposed three provably secure ID-based signcryption schemes. Unfortunately, the properties of public verifiability and forward security are mutually exclusive in the their schemes. Chow et al. [8] proposed an ID-based signcryption scheme that provides both public verifiability and forward security. However, Chow et al.'s scheme [8] needs two private keys. One is private signcryption key, the other is private decryption key. Boyen [5] developed the Malone-Lee's model [12] and added three new security notions: ciphertext unlinkability, ciphertext authentication and ciphertext anonymity. Boyen's scheme [5] is very useful in applications that require unlinkability and anonymity. In 2005, Chen and Malone-Lee [7] improved Boyen's scheme [5] in efficiency. In [4], Barreto et al. constructed the most efficient ID-based signcryption scheme to date.

Ring signature, initially formalized by Rivest *et al.* [16] in 2001, received a lot of concern since its introduction [1, 22, 24]. Due to its attracting feature of anonymity and spontaneity, ring signatures have been used in different scenarios such as electronic auction protocols [20, 21], vehicular ad hoc networks [19] and concurrent signatures [6].

Recently, Chung *et al.* [9] proposed an anonymous ECC-based signcryption scheme by combining the notion of ring signature with signcrytion together. They claimed that their scheme reaching the characteristic of confidentiality. However, in this paper, we show that it is not even secure against chosen-plaintext attacks.

The rest of this paper is organized as follows. In Section 2, we define the indistinguishability against adaptive chosen plaintext attacks for signcryption. Chung *et al.*'s anonymous ECC-based signcryption scheme has been reviewed and analyzed in Section 3 and Section 4, respectively. Finally, the conclusions are given in Section 5.

2 Formal Model of Anonymous Signcryption Schemes

We provide only those definitions relevant to our attack; see [2] for additional background and definitions.

2.1 Generic Scheme

A generic ring signcryption scheme consists of the following three algorithms.

- **Setup:** Given a security parameter k, the algorithm generates public/private key pairs. The public and private key pairs for the ring signers and the verifier are $(Q_1, d_1), \cdots, (Q_n, d_n), (Q_V, d_V)$.
- **Signcrypt:** To send a message m to the receiver whose identity is ID_V, user $Q_i (i \in \{1, \cdots, n\})$ chooses some other users to form a group $\mathcal{U}$ including herself and computes $\mathbf{Signcrypt}(m, \mathcal{U}, Q_V, d_i)$ on behalf of the group $\mathcal{U}$ to obtain the ciphertext σ.
- **Unsigncrypt:** When receiving σ, ID_V computes $\mathbf{Unsigncrypt}(\sigma, \mathcal{U}, d_V)$ and obtains the plaintext m or the symbol $\perp$ if σ is an invalid ciphertext between the group $\mathcal{U}$ and ID_V.

We make the consistency constraint that if $\sigma = \mathbf{Signcrypt}(m, \mathcal{U}, Q_V, d_i)$, then $m = \mathbf{Unsigncrypt}(\sigma, \mathcal{U}, d_V)$.

2.2 Security Notions

Definition 1. *An anonymous signcryption scheme is said to have the indistinguishability against adaptive chosen plaintext attacks property (IND-ASC-CPA) if no polynomially bounded adversary has a non-negligible advantage in the following game.*

1) *The challenger $\mathcal{C}$ runs the* **Setup** *algorithm with a security parameter k to produce public/secret key pairs $(Q_1, d_1), \cdots, (Q_n, d_n)$ for the ring members and verifier. After that, $\mathcal{C}$ keeps $(d_1, \cdots, d_n)$ secret and provides $\mathcal{A}$ with the public key $(Q_1, \cdots, Q_n)$.*
2) *The adversary $\mathcal{A}$ performs a polynomially bounded number of Signcryption queries as follows: $\mathcal{A}$ produces a set of users $\mathcal{U}$, a public key Q_j and a plaintext m. $\mathcal{C}$ randomly chooses a user $Q_i \in \mathcal{U}$ and acts as Q_i on behalf of $\mathcal{U}$. Then $\mathcal{C}$ sends the result of* $\mathbf{Signcrypt}(m, \mathcal{U}, Q_j)$ *to $\mathcal{A}$.*
3) *$\mathcal{A}$ generates two equal length plaintexts m_0, m_1, a user set $\mathcal{U}_A$ and a public key Q_V on which he wants to be challenged. He cannot have asked the private key corresponding to Q_V in the first stage.*
4) *$\mathcal{C}$ takes a bit $b \in_R \{0, 1\}$ and computes $\sigma =$* $\mathbf{Signcrypt}(m_b, \mathcal{U}_A, Q_V)$ *which is sent to $\mathcal{A}$.*
5) *$\mathcal{A}$ can ask a polynomially bounded number of queries adaptively again as in the first stage. Obviously, he cannot ask the secret key of Q_V and cannot make an unsigncryption query on σ to obtain the corresponding plaintext.*
6) *Finally, $\mathcal{A}$ produces a bit b' and wins the game if $b' = b$.*

The advantage of $\mathcal{A}$ is defined as $Adv(\mathcal{A}) = |2P[b' = b] - 1|$, where $P[b' = b]$ denotes the probability that $b' = b$.

3 Review of the Chung *et al.*'s Scheme

Setup. Let q denote a large prime number, E denote an elliptic curve, P denote a base point on the elliptic curve E with order q, and H denote a one-way hash function for resisting collision, where q, E, P, and H are public parameters, and Z_q is a finite field with q elements.

Let a group member set be $A = \{U_1, U_2, \cdots, U_n\}$ under the ECC, the private keys of $Q_1, Q_2, \cdots, Q_n$ are $d_1, d_2, \cdots, d_n$ respectively. The corresponding public keys $Q_1, Q_2, \cdots, Q_n$ satisfies $Q_i = d_i P$, where $i = 1, 2, \cdots, n$. The private and public keys of verifier U_v are d_v and $Q_v = d_v P$, respectively.

Signcrypt. Let a member U_i in A send the signcryption text of message m to verifier U_v. U_i executes the process of generating signcryption text as follows.

1) Randomly select $k \in_R [1, q-1]$ and $r \in_R [1, q-1]$;
2) Calculate $(x_i, y_i) = T_i = kP$, $(x_r, y_r) = R = rP$, and $(x_e, y_e) = T_e = rQ_v$;
3) Select $s_t \in_R [1, q-1]$, where $t = i+1, i+2, \cdots, n, 1, \cdots, i-1$ for $t-1 = n$ when $t = 1$;
4) Calculate $c_t = H(m \parallel x_{t-1})$ and $(x_t, y_t) = T_t = s_t P + c_t Q_t$, where $t = i+1, i+2, \cdots, n, 1, \cdots, i-1$ for $t-1 = n$ when $t = 1$;
5) Calculate $c_i = H(m \parallel x_{i-1})$ and $s_i = k - d_i c_i \pmod q$;
6) Encrypt the message m following $m' = E_{x_e}(m)$ using the symmetric secret key x_e;
7) Send the encrypted text $\sigma = (m', c_1, s_1, s_2, \cdots, s_n, R)$ to the verifier U_v.

Unsigncrypt. On receiving the encrypted text $\sigma = (m', c_1, s_1, s_2, \cdots, s_n, R)$, the verifier U_v performs the following steps to verify.

1) Let $(x_r, y_r) = R$, calculate $(x_d, y_d) = d_v R$ and $m'' = E_{x_d}(m')$;
2) For $t = 1, 2, \cdots, n-1$, calculate $(x_t, y_t) = T_t = s_t P + c_t Q_t$ and $c_{t+1} = H(m'' \parallel x_t)$;

3) Calculate $(x_n, y_n) = T_n = s_nP + c_nQ_n$ and $c'_1 = H(m'' \parallel x_n)$;

4) With $c'_1 = c_1$, confirm that $\sigma = (m', c_1, s_1, s_2, \cdots, s_n, R)$ is a valid anonymous signcryption text from the group $A = \{U_1, U_2, \cdots, U_n\}$; otherwise, reject the encrypted text.

4 Cryptanalysis of the Chung *et al.*'s Scheme

In this section, we show that the Chung *et al.*'s anonymous signcryption scheme is not even secure against chosen plaintext attacks. When $\mathcal{A}$ receives the challenge ciphertext $\sigma^* = (m'^*, c_1^*, s_1^*, s_2^*, \cdots, s_n^*, R^*)$. $\mathcal{A}$ first makes a "wild guess" of b to be 0. Then, $\mathcal{A}$ goes as follows:

1) For $t = 1, 2, \cdots, n-1$, calculate $(x_t^*, y_t^*) = T_t^* = s_t^*P + c_t^*Q_t$ and $c_{t+1}^* = H(m_b \parallel x_t^*)$;

2) Calculate $(x_n^*, y_n^*) = T_n^* = s_n^*P + c_n^*Q_n$ and $c_1'^* = H(m_b \parallel x_n^*)$;

3) Checking whether the equation $c_1^* = c_1'^*$ holds.

If the above equations hold, then $\mathcal{A}$ knows that m_0 is the plaintext for the challenge ciphertext. If the above equations do not hold, $\mathcal{A}$ knows that m_1 is the plaintext for the challenge ciphertext. So Chung *et al.*'s anonymous signcryption scheme is not secure against the chosen plaintext attacks. The basic reason is that signcryption is achieved by using *Encrypt-then-Sign* paradigm in this scheme. This scheme lacks the binding between the encryption and signature; namely, the output of the encryption is not used as input in the hash of message, which is used for generating the signature. Informally, $\mathcal{A}$ is able to distinguish the ciphertext because, $\mathcal{A}$ knows that m_b is either m_0 or m_1 which were produced to $\mathcal{C}$ during the challenge phase by $\mathcal{A}$. Hence, $\mathcal{A}$ can find t' without having access to the private key of the receiver and this led to the proposed attack.

5 Conclusions

Chung *et al.* [9] proposed an anonymous ECC-based signcryption scheme and claimed that their scheme reaching the characteristic of confidentiality. However, we show that it is not even secure against chosen-plaintext attacks.

Acknowledgements

The authors thank the editors and the anonymous referees for their valuable comments and suggestions. This work is partially supported by National Natural Science Foundation of China under Grant No. 61003230, Open fund from Key Lab of Network Security and Cryptology, National key scientific and technological special project of China under Grant No. 2011ZX03002-002-03, Fundamental Research Funds for the Central Universities under Grant No. ZYGX2011J063.

References

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

[2] J. Baek, R. Steinfeld, and Y. Zheng, "Formal proofs for the security of signcryption," in *Public Key Cryptography*, vol. LNCS 2274, pp. 80–98. Springer-Verlag, 2002.

[3] F. Bao and R.H. Deng, "A signcryption scheme with signature directly verifiable by public key," in *Public Key Cryptography*, vol. LNCS 1431, pp. 55–59. Springer-Verlag, 1998.

[4] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Advances in Cryptology-Asiacrypt '05*, vol. LNCS 3788, pp. 515–532. Springer-Verlag, 2005.

[5] X. Boyen, "Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography," in *Advances in Cryptology-Crypto '03*, vol. LNCS 2729, pp. 383–399. Springer-Verlag, 2003.

[6] L. Chen, C. Kudla, and K. Paterson, "Concurrent signatures," in *Eurocrypt '04*, vol. LNCS 3027, pp. 287–305. Springer-Verlag, 2004.

[7] L. Chen and J. M. Lee, "Improved identity-based signcryption," in *Public Key Cryptography*, vol. LNCS 3386, pp. 362–379. Springer-Verlag, 2005.

[8] S. S. M. Chow, S. M. Yiu, L. C. K. Hui, and K. P. Chow, "Efficient forward and provably secure id-based signcryption scheme with public verifiability and public ciphertext authenticity," in *Information Security and Cryptology*, vol. LNCS 2971, pp. 352–369. Springer-Verlag, 2004.

[9] Y. F. Chung, Z. Y. Wu, and T. S. Chen, "Ring signature scheme for ecc-based anonymous signcryption," *Computer Standards & Interfaces*, vol. 31, pp. 669–674, 2009.

[10] C. Gamage, J. Leiwo, and Y. Zheng, "Encrypted message authentication by firewalls," in *Public Key Cryptography*, vol. LNCS 1560, pp. 69–81. Springer-Verlag, 1999.

[11] H. Y. Jung, D. H. Lee, J. I. Lim, and K.S. Chang, "Signcryption schemes with forward secrecy," in *Proceedings of the Information Security Application (WISA 2001)*, pp. 463–475, Seoul, Korea, 2001.

[12] J. M. Lee. "Identity based signcryption,". tech. rep., Cryptology ePrint Archive, Report 2002/098, 2002. http://eprint.iacr.org/2002/098.

[13] J. M. Lee and W. Mao, "Two birds one stone: signcryption using RSA," in *Proceedings of the Topics in*

Cryptology-CT-RSA 2003, vol. LNCS 2612, pp. 211–226. Springer-Verlag, 2003.

[14] F. Li, X. Xin, and Y. Hu, "Id-based signcryption scheme with (t,n) shared unsigncryption," *International Journal of Network Security*, vol. 3, no. 2, pp. 155–159, 2006.

[15] B. Libert and J.J. Quisquater, "A new identity based signcryption schemes from pairings," in *Proceedings of the 2003 IEEE Information Theory Workshop*, pp. 155–158, Paris, France, 2003.

[16] A. Shamir R. L. Rivest and Y. Tauman, "How to leak a secret," in *Advances in Cryptology-Asiacrypt '01*, vol. LNCS 2248, pp. 552–565. Springer-Verlag, 2001.

[17] J. B. Shin, K. Lee, and K. Shim, "New dsa-verifiable signcryption schemes," in *Proceedings of the Information Security and Cryptology (ICISC 2002)*, vol. LNCS 2587, pp. 35–47. Springer-Verlag, 2003.

[18] M. Toorani and A. A. B. Shirazi, "Cryptanalysis of an elliptic curve-based signcryption scheme," *International Journal of Network Security*, vol. 10, no. 1, pp. 51–56, 2010.

[19] H. Xiong, K. Beznosov, Z. Qin, and M. Ripeanu, "Efficient and spontaneous privacy-preserving protocol for secure vehicular communication," in *ICC 2010*, p. 2010, 1-6.

[20] H. Xiong, Z. Chen, and F. Li, "Bidder-anonymous english auction protocol based on revocable ring signature," *Expert System with Applications*, vol. 39, no. 8, pp. 7062–7066, 2012.

[21] H. Xiong, Z. Qin, and F. Li, "An anonymous sealed-bid auction protocol based on ring signature," *International Journal of Network Security*, vol. 8, no. 2, pp. 236–243, 2009.

[22] H. Xiong, Z. Qin, and F. Li, "A certificateless proxy ring signature scheme with provable security," *International Journal of Network Security*, vol. 12, no. 2, pp. 113–127, 2011.

[23] D. H. Yum and P. J. Lee, "New signcryption schemes based on KCDSA," in *Proceedings of the Information Security and Cryptology (ICISC 2001)*, vol. LNCS 2288, pp. 305–317. Springer-Verlag, 2002.

[24] D. Zheng, X. Li, and K. Chen, "Code-based ring signature scheme," *International Journal of Network Security*, vol. 5, no. 2, pp. 154–157, 2007.

[25] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost (signature) + cost(encryption)," in *Advances in Cryptology-Crypto '97*, vol. LNCS 1294, pp. 165–179. Springer-Verlag, 1997.

[26] Y. Zheng and H. Imai, "How to construct efficient signcryption schemes on elliptic curves," *Information Processing Letters*, vol. 68, no. 5, pp. 227–233, 1998.

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

Jianbin Hu is an associate professor in Peking University (PKU). He received his Ph.D degree from PKU, China, 2004. His research interests include: cloud computing and information security.

Zhong Chen is a professor in PKU. He received his Ph.D degrees in computer science from PKU, in 1989. His research interests lie in information security and software engineering.