Improvement of Convertible Authenticated Encryption Schemes

Ting-Yi Chang, Chou-Chen Yang, and Min-Shiang Hwang

[1] Graduate Institute of e-Learning, National Changhua University of Education, No. 1, Jin-De Road, Changhua City, Taiwan, R.O.C.
[2] Department of Management Information Systems, National Chung Hsing University, 250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
[3] Department of Computer Science and Information Engineering, Asia University, Taiwan, R.O.C.
* Corresponding author: mshwang@asia.edu.tw

Abstract. A convertible authenticated encryption scheme simultaneously provides the functions of integration, authentication, confidentiality, and non-repudiation. In this paper, we first separately point out that any adversary can forge a converted signature in Araki's scheme and Ma-Chen's scheme. Moreover, we further improve the weakness in Wu- Hsu's scheme, which is to convert the signature into an ordinary one should divulge the message. Our improved scheme not only solves the weakness but also reduces the computational complexities in both sides of signer and recipient.

Key words: Authenticated encryption scheme, discrete logarithm problem, one-way hash function, signcryption

1 Introduction

Paper work is rapidly being replaced as e-mail, electronic commerce, and electronic money, etc. become more widespread. In many of these new forms of communication, a digital signature is essential. A digital signature such as RSA [2, 4, 10, 11, 14, 17] and ElGamal [9, 15, 22] signature schemes provides the functions of integration, authentication, and non-repudiation, which anyone can verify signature by using the signer's public key. However, there are some situations should be considered. In some applications, it is unnecessary for anyone to verify the validity of the signature. The signature only needs to be verified by some specified recipient while keeping the message secret. For example, the use of electronic money only needs to be verified by the bank and keep electronic money secret. Therefore, the confidentiality should be affiliate with the properties of digital signatures. Some authenticated encryption schemes [5, 6, 12, 13, 19, 20] and signcryption schemes [18, 24] are proposed to achieve the above purpose.

In 1999, Araki et al. [1] proposed a convertible limited verifier signature scheme, which is more efficient than Boyar et al.'s scheme [3]. In their scheme, the signer generates a signature by using her/his private key and the recipient's

public key. It is similar to fulfill both functions of digital signature and public key encryption simultaneously. Only has the corresponding private key of the recipient's public key can recover the message and verify the signature. If the signer denies that she/he has never signed the message, the recipient can further convert the signature into an ordinary one that can be verified by anyone (such as judge) without divulging the recipient's private key. Later, in 2002, Wu and Hsu [21] proposed a new convertible authenticated encryption scheme which can easily convert the original signature without the cooperation of the signer. Moreover, it is more efficient than Araki et al.'s scheme in term of the computation complexities and the communication costs. However, Zhang and Kim [23] pointed out that the original signature generated by the signer could be forged in Araki et al.'s scheme.

Recently, in 2003, in order to avoid divulging the message, Ma and Chen [16] propose a publicly verifiable authenticated encryption scheme. When the recipient converts the original signature, he/she does not reveal not only the private key but also the message. Their scheme is as efficient as the Zheng's scheme [24] with respect to both communication costs and the communication overhead. In additionally, they provide an efficient method for converting the original signature than that using the zero-knowledge proof in Zheng's scheme.

However, in this paper, we will show that Araki et al.'s scheme suffer from not only a forgery original signature attack but also a forgery converted signature attack, that is, any one can forge a valid converted signature of a signer on an arbitrary message. The forgery converted signature attack can also successfully break the security of Ma-Chen's scheme. Certainly, the secure requirement against the forgery converted signature attack should also be concerned about. At the same time, we will propose an improved scheme which modifies some aspects of Wu and Hsu's scheme. The improved scheme can protect the message revealed for converting the original signature to the judge and reduces the computational complexities in both sides of signer and recipient.

2 Cryptanalysis of Araki et al.'s Scheme

In this section, we will show that scheme proposed by Araki et al. is not secure by presenting the forgery converted signature attack. For presenting our attack on Araki et al.'s scheme, we briefly review their scheme along with our attack in the following subsections, respectively.

2.1 Review of Araki et al.'s Scheme

Initially, a trust authority publicly chooses two large prime numbers p and q such that $p = 2q + 1$, a generator g of order q over the Galois field $GF(p)$. Assume that Alice is the signer and Bob is the recipient, which separately own the private keys $x_A \in Z_q^*$ and $x_B \in Z_q^*$. The corresponding public keys are $y_A = g^{x_A} \bmod p$ and $y_B = g^{x_B} \bmod p$, which are certified by the trusted third

party. Their scheme is divided into the signing and verification phase, and the conversion phase, which are descript as follows.

The Signing and Verification Phase:
To sign the message m which contains some redundancy [7], Alice performs the following steps.

Step 1. Choose a random number $k \in Z_q^*$.
Step 2. Compute $r_1 = y_B^{k+H(k)} \bmod p$ and $r_2 = m \cdot (r_1 + g)^{-1} \bmod p$, where $H(\cdot)$ is a one-way hash function [8].
Step 3. Check whether $r_1 + g = 0$ and $r_2 > q$ is hold or not. If it holds, comes back to Step 1. Otherwise, continues to Step 4.
Step 4. Compute $J = g^{H(k)} \bmod p$ and $s = (r_2 \cdot k - 1 - r_2) \cdot (1 + x_A)^{-1} \bmod q$.
Step 5. Send $\{r_2, s, J\}$ to Bob.

After receiving $\{r_2, s, J\}$, Bob derives the message m by computing $m = (y_B^{(1+r_2+s)\cdot r_2^{-1}} \cdot (y_A^{s \cdot r_2^{-1}} \cdot J)^{x_B} + g) \cdot r_2 \bmod p$ and checks the redundancy contained in m.

The Conversion Phase:
With a dispute, Bob converts the signature into an ordinary one (substitute for providing his secret key x_B), Alice is requested to release a parameter $u = s \cdot x_A \cdot r_2^{-1} + H(k) \bmod q$. Then, Bob verifies its validity with checking $g^u = y_A^{s \cdot r_2^{-1}} \cdot J \bmod p$. If it holds, Bob can convert the original signature into $\{m, r_2, s, J, u\}$. To verify the signature, the judge checks the equations $g^u = y_A^{s \cdot r_2^{-1}} \cdot J \bmod p$ and $m = (y_B^{(1+r_2+s)\cdot r_2^{-1} + u} + g) \cdot r_2 \bmod p$. If two equations hold, the judge believes that the signature $\{m, r_2, s, J, u\}$ is generated by Alice.

2.2 The Forgery Converted Signature Attack

Next we show that the adversary forges Alice's converted signature $\{m', r_2', s', J', u'\}$ in the conversion phase. It will lead to Alice gets erroneous judgment from the judge. The adversary performs the following steps.

Step 1. Choose an arbitrary message m' and a random number $s' \in Z_q^*$.
Step 2. Compute the values r_2', u', and J' as follows.

$$r_2' = (1 + g)^{-1} \cdot m' \bmod p \tag{1}$$
$$u' = -(1 + r_2' + s') \cdot r_2'^{-1} \bmod q \tag{2}$$
$$J' = (y_A^{s' \cdot r_2'^{-1}})^{-1} \cdot g^{u'} \bmod p \tag{3}$$

Step 3. Send $\{m', r_2', s', J', u'\}$ to the judge.

After receiving $\{m', r_2', s', J', u'\}$, the equations $g^{u'} = y_A^{s' \cdot r_2'^{-1}} \cdot J' \bmod p$ and $m' = (y_B^{(1+r_2'+s') \cdot r_2'^{-1} + u'} + g) \cdot r_2' \bmod p$ checked by judge will be hold as follows.

$$\begin{aligned} & y_A^{s' \cdot r_2'^{-1}} \cdot J' \bmod p \\ = & \, y_A^{s' \cdot r_2'^{-1}} \cdot (y_A^{s' \cdot r_2'^{-1}})^{-1} \cdot g^{u'} \bmod p \quad \text{(by Equation (3))} \\ = & \, g^{u'} \end{aligned}$$

and

$$\begin{aligned} & (y_B^{(1+r_2'+s') \cdot r_2'^{-1} + u'} + g) \cdot r_2' \bmod p \\ = & \, (y_B^{(1+r_2'+s') \cdot r_2'^{-1} - (1+r_2'+s') \cdot r_2'^{-1}} + g) \cdot r_2' \bmod p \quad \text{(by Equation (2))} \\ = & \, (1+g) \cdot r_2' \bmod p \\ = & \, (1+g) \cdot (1+g)^{-1} \cdot m' \bmod p \quad \text{(by Equation (1))} \\ = & \, m' \end{aligned}$$

Hence, with the knowledge of Alice public key y_A, the adversary can easily forge Alice's converted signature.

3 The Proposed Scheme

To avoid exposing the message m when convert the original signature to the judge, we make some modifications in Wu-Hsu's scheme [21]. The parameters $\{p, q, g, H(\cdot), x_A, x_B, y_A, y_B, m\}$ are also the same as those in Araki et al.'s scheme. The detail of two phases is as follows.

The Signing and Verification Phase:
To sign the message m, Alice performs the following steps.

Step 1. Choose a random number $k \in Z_q^*$.
Step 2. Compute r_1, r_2, and s as follows.

$$r_1 = m \cdot (y_B^k \bmod p)^{-1} \bmod p \tag{4}$$
$$r_2 = H(H(m), g^k \bmod p) \bmod q \tag{5}$$
$$s = k - x_A \cdot r_2 \bmod q \tag{6}$$

Step 3. Send $\{r_1, r_2, s\}$ to Bob.

After receiving $\{r_1, r_2, s\}$, Bob first derives the message m by computing

$$m = (g^s \cdot y_A^{r_2})^{x_B} \cdot r_1 \bmod p \tag{7}$$

and checks the redundancy contained in m. Then, he checks the validity of the signature with the following equation.

$$r_2 = H(H(m), g^s \cdot y_A^{r_2} \bmod p)) \bmod q \tag{8}$$

If it holds, the signature $\{r_1, r_2, s\}$ is indeed generated by Alice.

4 Conclusions

In this article, we have shown that security flaws in Araki et al.'s scheme and Ma-Chen's scheme. Moreover, we make some modifications in Wu-Hsu's scheme to avoid divulging the message. Though modifications were made, the original advantages are maintained and un-compromised. It further reduces the computational complexities in both sides of signer and recipient.

References

1. Shunsuke Araki, Satoshi Uehara, and Kyoki Imamura, "The limited verifier signature and its application," *IEICE Transactions on Fundamentals*, vol. E82-A, no. 1, pp. 63–68, 1999.
2. Feng Bao, Cheng-Chi Lee, Min-Shiang Hwang, "Cryptanalysis and Improvement on Batch Verifying Multiple RSA Digital Signatures," *Applied Mathematics and Computation*, vol. 172, no. 2, pp. 1195–1200, Jan. 2006.
3. J. Boyar, D. Chaum, and T. Pedersen, "Convertible undeniable signatures," in *Advances in Cryptology, Crypto'90*, pp. 189–205, 1990.
4. Chin-Chen Chang, Min-Shiang Hwang, "Parallel Computation of the Generating Keys for RSA Cryptosystems," *IEE Electronics Letters*, vo1. 32, no. 15, pp. 1365–1366, 1996.
5. Ting-Yi Chang, Chou-Chen Yang, Min-Shiang Hwang, "Cryptanalysis of Publicly Verifiable Authenticated Encryption," *IEICE Transactions on Foundations*, vol. E87-A, no. 6, pp. 1645-1646, June 2004.
6. L. H. Encinas, A. M. del Rey, and J. M. Masqué, "A Weakness in Authenticated Encryption Schemes Based on Tseng et al.'s Schemes," *International Journal of Network Security*, vol. 7, no. 2, pp. 157–159, 2008.
7. S. Goldwasser, S. Micali, and R. Rivest, "A secure digital signature scheme," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 281–308, 1988.
8. Min-Shiang Hwang, Chin-Chen Chang, and Kuo-Feng Hwang, "A watermarking technique based on one-way hash functions," *IEEE Transactions on Consumer Electronics*, vol. 45, no. 2, pp. 286–294, 1999.
9. Min-Shiang Hwang, Chin-Chen Chang, and Kuo-Feng Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445–446, 2002.
10. Min-Shiang Hwang, Cheng-Chi Lee, Yan-Chi Lai, "Traceability on RSA-Based Partially Signature with Low Computation," *Applied Mathematics and Computation*, vol. 145, no. 2-3, pp. 465–468, Dec. 2003.
11. Min-Shiang Hwang, Iuon-Chung Lin, and Kuo-Feng Hwang, "Cryptanalysis of the batch verifying multiple RSA digital signatures," *Informatica*, vol. 11, no. 1, pp. 15–19, 2000.
12. Min-Shiang Hwang and Chi-Yu Liu, "Authenticated Encryption Schemes: Current Status and Key Issues," *International Journal of Network Security*, vol. 1, no. 2, pp. 61-73, Sept. 2005.
13. Min-Shiang Hwang, Jung-Wen Lo, Shu-Yin Hsiao, "Improvement of Authenticated Encryption Schemes with Message Linkages for Message Flows," *IEICE Transactions on Information and Systems*, vol. E89-D, no. 4, pp. 1575-1577, 2006.

14. Min-Shiang Hwang, Eric Jui-Lin Lu, Iuon-Chang Lin, "A Practical (t, n) Threshold Proxy Signature Scheme Based on The RSA Cryptosystem," *IEEE Transactions on Knowledge and Data Engineering*, vol. 15. no. 6, pp. 1552–1560, Nov./Dec. 2003.
15. Cheng-Chi Lee, Min-Shiang Hwang, Shiang-Feng Tzeng, "A New Convertible Authenticated Encryption Scheme Based on the ElGamal Cryptosystem," *International Journal of Foundations of Computer Science*, Vol. 20, Iss. 2, pp. 351-359, 2009
16. Changshe Ma and Kefei Chen, "Publicly verifiable authenticated encryption," *Electronics Letters*, vol. 39, no. 3, pp. 281–282, 2003.
17. K. Singh and S. G. Samaddar, "Enhancing Koyama Scheme Using Selective Encryption Technique in RSA-based Singular Cubic Curve with AVK," *International Journal of Network Security*, vol. 14, no. 3, pp. 164–172, 2012.
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. Chwei-Shyong Tsai, Shu-Chen Lin, Min-Shiang Hwang, "Cryptanalysis of an Authenticated Encryption Scheme Using Self-Certified Public Keys," *Applied Mathematics and Computation*, vol. 166, no. 1, pp. 118-122, July 2005.
20. Shiang-Feng Tzeng, Yuan-Liang Tang, Min-Shiang Hwang, "A New Convertible Authenticated Encryption Scheme with Message Linkages," *Computers and Electrical Engineering*, vol. 33, no. 2, pp. 133-138, Mar. 2007.
21. Tzong-Sun Wu and Chien-Lung Hsu, "Convertible authenticated encyption scheme," *The Journal of Systems and Software*, vol. 62, no. 3, pp. 205–209, 2002.
22. Chou-Chen Yang, Ting-Yi Chang, Jian-Wei Li, Min-Shiang Hwang, "Simple Generalized Group-oriented Cryptosystems Using ElGamal Cryptosystem," *Informatica*, vol. 14, no. 1, pp. 111-120, 2003.
23. Fangguo Zhang and Kwangjo Kim, "A universal forgery on araki et al.'s convertible limited verifier signature scheme," *IEICE Trans. Fundamentals*, vol. E86-A, no. 2, pp. 515–516, 2003.
24. Y. Zheng, "Signcryption and its applications in efficient public key solutions," in *Information Security Workshop (ISW'97)*, pp. 291–312, New York, 1997.