Cryptanalysis of Publicly Verifiable Authenticated Encryption*

Ting-Yi Chang[‡] Chou-Chen Yang[†] Min-Shiang Hwang[†] $_{Member}$

Department of Management Information System[†]
National Chung Hsing University
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.
Email: mshwang@cyut.edu.tw
Fax: 886-4-23742337

Department of Computer and Information Science[‡]
National Chiao Tung University
1001 Ta Hsueh Road, Hsinchu, Taiwan, R.O.C.

February 17, 2004

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC91-2213-E-324-003.

Cryptanalysis of Publicly Verifiable Authenticated Encryption

Abstract

Recently, Ma and Chen proposed a new authenticated encryption scheme with public verifiability. The signer can generate a signature with message recovery for a specified recipient. With a dispute, the recipient has ability to convert the signature into an ordinary one that can be verified by anyone without divulging her/his private key and the message. However, we point out that any adversary can forge a converted signature in this article.

Keywords: Authenticated encryption scheme, discrete logarithms, signcryption.

1 Introduction

Authenticated encryption schemes [1, 3, 5, 8] and the signcryption schemes [2, 7, 9] fulfill both the functions of digital signature and public key encryption simultaneously. The signer can generate a signature with message recovery for a specified recipient. With a dispute, the recipient has ability to convert the signature into an ordinary one that can be verified by anyone (such as a judge). To avoid revealing the message and the recipient's private key, Ma and Chen proposed a publicly verifiable authenticated encryption scheme [6]. Their scheme is as efficient as the Zheng's scheme [9] with respect to both communication costs and the communication overhead. Their scheme also provides an efficient method for converting the original signature without using the zero-knowledge proof in Zheng's scheme.

However, in this article, a security flaw in Ma and Chen's scheme is presented. Any adversary can forge a converted signature to the judge. Therefore, the judge will misconceive the forged signature is generated by the original signer.

2 Review of Ma and Chen's Scheme

Initially, a trusted third party publicly chooses two large prime numbers p and q such that q divides $p-1$. Let g be a generator with order q in the Galois field $GF(p)$; x_A $(\in Z_q^*)$ and x_B $(\in Z_q^*)$ be Alice's and Bob's private key, respectively; y_A $(= g^{x_A} \bmod p)$ and y_B $(= g^{x_B} \bmod p)$ be Alice's and Bob's public key, respectively. Assume that Alice is the singer and Bob is the recipient. To sign a message $m \in Z_p^*$, Alice performs the following steps.

Step 1. Choose a random number $k \in Z_q^*$.

Step 2. Compute $c = m \cdot (H((g \cdot y_B)^k \bmod p))^{-1} \bmod p$. Here, $H(\cdot)$ denotes a one-way hash function [4].

Step 3. Compute $r = H((g \cdot y_B)^k \bmod p) \bmod q, H(m))$.

Step 4. Compute $s = k - x_A \cdot r \bmod q$.

Step 5. Send (c, r, s) to Bob.

After receiving (c, r, s), Bob performs the following steps to derive the message and verify the signature.

Step 1. Derive the message $m = c \cdot H((g \cdot y_B)^s \cdot y_A^{r\cdot(x_B+1)} \bmod p) \bmod p$.

Step 2. Verify $r = H(((g \cdot y_B)^s \cdot y_A^{r\cdot(x_B+1)} \bmod p) \bmod q, H(m))$.

For public verification, Bob computes $J = (y_B^s \cdot y_A^{r \cdot x_B} \bmod p) \bmod q$. Then, he sends $(H(m), J, r, s)$ to the judge. To verify that Alice is the originator signer of the hashed message $H(m)$, the judge checks whether the equation $r = H((g^s \cdot y_A^r \cdot J \bmod p) \bmod q, H(m))$ is hold or not. If it holds, the judge believes that Alice is the original signer.

3 Cryptanalysis of Ma and Chen's Scheme

Next, we show that an adversary can forge Alice's converted signature ($H(m')$, J', r', s') in Ma and Chen's scheme. The adversary performs the following steps.

Step 1. Choose a random number $s' \in Z_q^*$ and the forged message m'.

Step 2. Compute $r' = H((g^{s'} \bmod p) \bmod q, H(m'))$.

Step 3. Compute $J' = (y_A^{r'})^{-1} \bmod p$.

Step 4. Send $(H(m'), J', r', s')$ to the judge.

After receiving $(H(m'), J', r', s')$, the equation $r' = H((g^{s'} \cdot y_A^{r'} \cdot J' \bmod p) \bmod q, H(m'))$ checked by judge will be hold as follows.

$$
\begin{aligned}
& H((g^{s'} \cdot y_A^{r'} \cdot J' \bmod p) \bmod q, H(m')) \\
= \; & H((g^{s'} \cdot y_A^{r'} \cdot (y_A^{r'})^{-1} \bmod p) \bmod q, H(m')) \\
= \; & H((g^{s'} \bmod p) \bmod q, H(m')) \\
= \; & r
\end{aligned}
$$

Hence, the adversary can forge Alice's converted signature. The reviewer points out that a parenthesis of the hash function is not enough in Step 3 in Section 2. It harms the security of Ma and Chen's Scheme as we presented.

4 Conclusion

In this article, we have showed that there is a security flaw in Ma and Chen's scheme. Any adversary can use victim's public keys to forge the converted signatures.

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] W. H. He and T. C. Wu, "Cryptanalysis and improvement of Petersen-Michels signcryption scheme," *IEE Proceedings - Computers and Digital Techniques*, vol. 146, no. 2, pp. 123–124, 1999.

[3] P. Horster, M. Michels, and H. Petersen, "Authenticated encryption schemes with low communication costs," *Electronics Letters*, vol. 30, no. 15, p. 1212, 1994.

[4] 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.

[5] Wei-Bin Lee and Chin-Chen Chang, "Authenticated encryption schemes without using a one way function," *Electronics Letters*, vol. 31, no. 19, pp. 1656–1657, 1995.

[6] Changshe Ma and Kefei Chen, "Publicly verifiable authenticated encryption," *Electronics Letters*, vol. 39, no. 3, pp. 281–282, 2003.

[7] H. Petersen and M. Michels, "Cryptanalysis and improvement of signcryption schemes," *IEE Proceedings - Computers and Digital Techniques*, vol. 145, no. 2, pp. 149–151, 1998.

[8] 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.

[9] Y. Zheng, "Signcryption and its applications in efficient public key solutions," in *Information Security Workshop (ISW'97)*, pp. 291–312, New York, 1997.