On the Security of A Publicly Verifiable Authenticated Encryption[1]

Hung-Min Sun and Cheng-Ta Yang*

Department of Computer Science
National Tsing Hua University, Hsinchu, Taiwan 30055
E-mail: hmsun@cs.nthu.edu.tw

*Department of Computer Science and Information Engineering
National Cheng Kung University, Tainan, Taiwan 70101

Abstract

Recently, Ma and Chen proposed an efficient authenticated encryption with public verifiability in which the receiver's private key and the message are not divulged during the public verifiability. In this paper, we show that Ma and Chen's scheme does not actually achieve the non-repudiation property.

Keywords: Cryptanalysis, Authenticated Encryption, Public Variability

1. Introduction

Public key cryptography has revolutionized the way for people to conduct secure and authenticated communications. Horster, Michels and Peterson[1] first proposed an authenticated encryption scheme that achieves message authenticity as well as message confidentiality.

An authenticated encryption scheme is a message transmission scheme, which sends messages in a secure and authentic way. Basically, an authenticated encryption scheme should satisfy the following property[2][3][4][6]:

- Confidentiality: it is computationally infeasible for an adaptive attacker to find out any secret information from a ciphertext.
- Unforgeability: it is computationally infeasible for an adaptive attacker to masquerade as the sender in sending a message.
- Non-repudiation: it is computationally feasible for a third party to settle a dispute between the sender and the recipient in an event where the sender denies the fact that he is the originator of the message.

Recently, Ma and Chen[5] proposed a new efficient public verifiable authenticated encryption scheme. It was claimed that the receiver's private key and the message are not divulged during the public verifiability. In this paper, we show that Ma and Chen's scheme

[1]This research was supported in part by the Communications Software Technology project of Institute for Information Industry and sponsored by MOEA, R.O.C. and by the National Science Council, Taiwan, R.O.C., under contract NSC-91-2520-S-007-010.

does not actually achieve the non-repudiation property.

The paper is organized as follows. In Section 2, we briefly review Ma and Chen's public verifiable authenticated encryption scheme. In Section 3, we show the insecurity of Ma and Chen's scheme. Finally, we conclude the paper in Section 4.

2. Review of Ma and Chen's scheme

We first review Ma and Chen's scheme in the following. From now on, we assume that Alice is the sender and Bob is the recipient.

Initial setting

1. Two large primes p and q with $q|(p-1)$.
2. An element $g \in Z_p^*$ of order q.
3. $x_A \in Z_q^*$ is Alice's secret key; and $y_A \equiv g^{x_A} \bmod p$ is Alice's public key.
4. $x_B \in Z_q^*$ is Bob's secret key; and $y_B \equiv g^{x_B} \bmod p$ is Bob's public key.
5. One way hash function H with $|H| < |p|$, where $|p|$ denotes the number of bits in p and $|H|$ denotes the number of bits in the output value of hash function H.

Alice: in order to send a message $m \in Z_p^*$, Alice does the following:

1. Picks a random number $k \in Z_q^*$.
2. Computes $v \equiv (g \cdot y_B)^k \bmod p$ and $e \equiv v \bmod q$.
3. Computes $c \equiv m(H(v))^{-1} \bmod p$.
4. Computes $r = H(e, H(m))$.
5. Computes $s \equiv k - x_A \cdot r \bmod q$.
6. Sends *(c, r, s)* to Bob.

Bob: in order to recover the message m from *(c, r, s)*, Bob does the following:

1. Computes $v \equiv (g \cdot y_B)^s \cdot y_A^{r(x_B+1)} \bmod p$ and $e \equiv v \bmod q$.
2. Recovers the message $m \equiv c \cdot H(v) \bmod p$.
3. Verifies $r ? = H(e, H(m))$.
4. For public verification, Bob computes $K_1 \equiv (y_B^k \bmod p) \bmod q \equiv (y_B^s \cdot y_A^{r \cdot x_B} \bmod p) \bmod q$ and forwards $(H(m), K_1, r, s)$ to an arbitrary trusted third party. In order to verify whether Alice is the originator of the encryption and signature, the trusted third party checks the validity of $(H(m), K_1, r, s)$ as follows:
5. Computes $e \equiv (g^s \cdot y_A^r \cdot K_1 \bmod p) \bmod q$.
6. Verifies $r ? = H(e, H(m))$.

Ma and Chen claimed that the proposed scheme has an efficient non-repudiation procedure without using zero-knowledge proof. In next section, we will show that their scheme does not actually achieve the non-repudiation property.

3. Cryptanalysis

In the section, we show that in Ma and Chen's scheme, the trusted third party cannot correctly verify the actual originator of the encryption and signature. A forgery attack against Ma and Chen's scheme is demonstrated below.

1. Bob holds Alice's public key y_A and chooses *e'*, *m'* and *s'*.
2. Computes *r'=H(e', H(m'))*.
3. Computes $K_1' \equiv (e' \cdot g^{-s'} \cdot y_A^{-r'} \bmod p) \bmod q$.

It can be seen that given *e'*, *m'* and *s'*, Bob knows y_A and then can easily obtain K_1'. Therefore, Bob can easily forge a valid message $(H(m'), K_1', r', s')$, and send it to an arbitrary trusted third party. The trusted third party will authenticate that Alice is the originator of the encryption and signature.

From the above analysis, Ma and Chen's scheme violates the non-repudiation property.

4. Conclusions

In this paper, we have shown that the publicly verifiable authenticated encryption scheme proposed by Ma and Chen violates the non-repudiation property. We can easily forge a message, which passes the trusted third party's verification. Further research can be made to design a secure authenticated encryption scheme with public verifiability and non-repudiation property.

Reference

[1] Horster P, Michels M, Petersen H., "Authenticated encryption schemes with low communication costs", Electronic Letters; 30(15): 1212 1994.
[2] Lee WB, Chang CC, "Authenticated encryption schemes without using a one way function", Electronic Letters; 31(19): 1656--7 1995.
[3] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) ≤ cost (signature) + cost (encryption)", In Advances in Cryptology - CRYPTO'97, LNCS 1294, Springer-Verlag, pp.165-179, 1997.
[4] Y. Zheng, "Signcryption and its applications in efficient public key solutions". In Information Security Workshop (ISW '97), LNCS 1397, Springer-Verlag, pp.291-312, 1998.
[5] C. Ma, K. Chen, "Public verifiable authenticated encryption", Electronic Letters; 39(3): 281--2 2003.
[6] H. Petersen and M. Michels, "Cryptanalysis and improvement of signcryption schemes", IEE Proceedings on Computers and Digital Techniques, 145:149--151, 1998.