Cryptanalysis of publicly verifiable authenticated encryption

Ren-Junn Hwang
Department of Computer Science and Information Engineering, TamKang University
victor@mail.tku.edu.tw

Chih-Hua Lai
Department of Computer Science and Information Engineering, TamKang University
ericlay@seed.net.tw

Jui-Chu Peng
Department of Computer Science and Information Engineering, TamKang University
u8192476@tknet.tku.edu.tw

Abstract

In 2003, Ma and Chen proposed a new authenticated encryption scheme with public verification. This paper shows a method that anybody can forge the sender’s signature, although he does not know the sender’s private key. The Ma and Chen’s scheme does not provide unforgeability and non-repudiation. These two security functions are very important for an authenticated encryption scheme.

Keywords：Cryptanalysis, Authenticated encryption

1. Introduction

An authenticated encryption scheme provides a method to deliver secret and to authenticate message with low computation and communication overhead. It must provide three secure properties [1]:

(1) Unforgeability: It is computational infeasible that anybody wants to forge signature of sender for any message without sender’ s private key.

(2) Non-repudiation: It is computational feasible that trusted third party can judge sender’ s signature of message or not when dispute occurs. Nobody except sender can reproduce another sender’ s signature for the message.

(3) Confidentiality: It is computational infeasible that anybody wants to decrypt cipher text without any secret information between sender and recipient.

Ma and Chen [2] proposed a new authenticated encryption scheme with public verifiability. They claim that their scheme is computationally feasible for the trusted third party (TTP for short) to verify the sender’ s signature without divulging the recipient’ s private key.

This paper shows that Ma-Chen’ s scheme doesn’ t provide the unforgeability and non-repudiation. We will point out a method that anybody without the private key of sender can forge the signature of any message *m*’. He can profess that sender has sent this message *m*’ to him. However, the TTP will judge that sender has sent this message *m*’ to the adversary in the Ma-Chen’ s scheme.

2. Review of Ma and Chen’ s scheme

The Ma-Chen’ s scheme contains four phases: the system initialization phase, the signature generation phase, the message recovery phase, and the public verification phase. We briefly describe these four phases as follows.

2.1 Initialization phase

Trusted third party (TTP for short) randomly selects and publishes p, q and g. Both p and q are two large primes and $q|p$-1. g is a generator with order q over GF(p). TTP also publishes a public one-way hash function H. Each user i randomly chooses his private key $x_i \in Z_q^*$ and public key $y_i = g^{x_i} \bmod p$. Each user also should apply the certification of his public key.

2.2 Signature generation phase

To introduce Ma-Chen’ s scheme clearly, we assume that sender A wants to send message m to recipient B. In this phase, sender A will generate and send digital signature (r, s) and cipher text c to recipient B by the following steps.

Step 1: confirms recipient B’s public key y_B by using his certificate

Step 2: picks a random integer $k \in Z_q^*$

Step 3: computes $v = (g \cdot y_B)^k \bmod p$ and $e = v \bmod q$

Step 4: computes $c = m \cdot (H(v))^{-1} \bmod p$

Step 5: computes $r = H(e, H(m))$

Step 6: computes $s = k - x_A \cdot r \bmod q$

Step 7: sends (c, r, s) to recipient B

2.3 Message recovery phase

In this phase, recipient B decrypts and verifies cipher text c as follows:

Step 1: confirms recipient A's public key y_A by using his certificate
Step 2: computes $v = (g \cdot y_B)^s \cdot y_A^{r \cdot (x_B+1)}$ mod p and $e = v$ mod q
Step 3: recovers the message $m = c \cdot H(v)$ mod p
Step 4: If r is equal to $H(e, H(m))$ then m is the real plain text sent by sender A; otherwise, it is incorrect.

2.4 Public verification phase

For public verification, recipient B should compute K_1 = ($y_B{}^{s} \cdot y_A{}^{r \cdot x_B}$ mod p) mod q and forward ($H(m)$, K_1, r, s) to TTP. TTP performs the following steps to judge that sender A has sent the message m to recipient B.

Step 1: confirms recipient A's public key y_A by using his certificate
Step 2: computes $e = (g^s \cdot y_A{}^r \cdot K_1$ mod $p)$ mod q
Step 3: If r is equal to $H(e, H(m))$ then TTP judges m is sent by sender A; otherwise, it is incorrect.

3. Cryptanalysis on Ma-Chen's scheme

We show the method that anybody can forge sender's signature of any message without knowing sender's private key. The TTP can not find out the signature is fake. We describe these two phases as follows.

3.1 Forge signature phase

This section shows that Ma-Chen's publicly verifiable authenticated encryption scheme does not provide unforgeability and non-repudiation. Both of these two secure properties are necessary for authenticated encryption scheme. In Ma-Chen's scheme, the adversary C does not get the private key of sender A, but he can forges ($H(m')$, K_1', r', s') and profess that sender A has sent message m' to him. The TTP will judge that sender A has sent message m' to adversary C by performing public verification phase of Ma-Chen's scheme. The adversary C forges the ($H(m')$, K_1', r', s') by the following steps.

Step 1: computes $H(m')$ using the public one -way hash function for any message m'
Step 2: randomly select integer $s' \in Z_q^*$
Step 3: computes $e' = (g^{s'}$ mod $p)$ mod q
Step 4: computes $r' = H(e', H(m'))$
Step 5: computes $K_1' = ((\, y_A{}^{r'})^{-1}$ mod p) mod q
Step 6: professes sender A has sent m' to him and forwards ($H(m')$, K_1', r', s') to TTP.

3.2 Public verification phase

In the public verification phase of Ma-Chen's scheme, TTP performs the following steps to judge that sender A has sent message m' to the adversary C.

Step 1: confirms recipient A's public key y_A by using his certificate
Step 2: computes e'

$$= (g^{s'} \cdot y_A{}^{r'} \cdot K_1' \bmod p) \bmod q$$
$$= (g^{s'} \cdot y_A{}^{r'} \cdot (y_A{}^{r'})^{-1} \bmod p) \bmod q$$
$$= (g^{s'} \bmod p) \bmod q$$

Step 3: verifiable equation $r' = H(e', H(m'))$ is always valid

It is clearly that the adversary C forges the ($H(m')$, K_1', r', s') to profess that sender A has sent the message m' and its signature (r', s') to him successfully. However, the adversary C does not get the private key of sender A. Therefore, Ma-Chen's scheme does not satisfy the unforgeability and non-repudiation.

4. Conclusions

This paper shows that Ma-Chen's publicly verifiable authenticated encryption does not satisfy the unforgeability and non-repudiation properties of the authenticated encryption scheme. Anybody without sender's private key of sender A can make a fake report that sender A has sent the message m' to him easily. The TTP cannot judge that it is true or false. Therefore, sender A also can repudiate signature for any message.

5. References

[1] P. Horster, M. Michels, and H. Petersen, "Authenticated encryption scheme with low communication costs," *IEE Electronic Letters*, vol. 30, no. 15, pp. 1212-1213, 1994.

[2] C. Ma and K. Chen, "Publicly verifiable authenticated encryption," *IEE Electronic Letters*, vol. 39, no. 3, pp. 281-282, 2003.