Cryptanalysis of an Authenticated Encryption Scheme Using Self-Certified Public Keys*

Chwei-Shyong Tsai† Shu-Chen Lin‡ Min-Shiang Hwang†

Department of Management Information System†
National Chung Hsing University
250 Kuo Kuang Road,
402 Taichung, Taiwan, R.O.C.
Email: mshwang@nchu.edu.tw

Department of Information Management‡
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.

October 31, 2012

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

†Responsible for correspondence: Prof. Min-Shiang Hwang.

Cryptanalysis of an Authenticated Encryption Scheme Using Self-Certified Public Keys

Abstract

Recently, Tseng et al. proposed an authenticated encryption scheme using self-certified public keys. In their scheme, only the specified receiver can verify and recover the message. In this article, we will demonstrate their scheme cannot withstand the known plaintext-ciphertext attack. The intruder has ability to expose every message sent between the signer and the specified receiver.

Keywords: Authenticated encryption, digital signature, self-certified public key

1 Introduction

Nyberg and Rueppel proposed the signature scheme which gives the message recovery based on the discrete logarithm [7]. Horster et al. proposed an application of the Nyberg-Rueppel's scheme for authenticated encryption [3]. In the authentication encryption scheme, the signer generates the signature for a message and sends it to the specified receiver. Only the specified receiver has ability to recover and verify the message. They proposed the authentication encryption scheme based on the discrete logarithm which has lower communication costs. Later, a number of schemes have been proposed to reduce communication costs and improve the performance [5, 6].

Above schemes are proposed based on well-known public key system [1, 4, 8]. In these scheme, each user publishes the public key which must to be authenticated, and keeps his/her secret key. To authenticate public keys, there are three approaches: the certificate-based, the identity-based and the self-certified approaches. In the certificate-based approach, each user selects his/her secret key and computes the public key which is authenticated by a certificate generated by the system authority. The system authority is trusted by all users and needs large storage to store each user's public key. In the identity-based approach, the user's public key is his/her unique identity. However, the system authority can impersonate any user at any moment [2].

In the self-certified approach, each user's public key is derived from the signature of the user's secret key. His/Her secret key includes his/her identity and only been kept by himself. Tseng et al. propose their authenticated encryption scheme using self-certified public key [10]. However, their scheme cannot withstand the known plaintext-ciphertext attack [5]. We will show that the intruder can expose every message sent between the signer and the specified receiver.

The remainder of our paper is organized as follows. In Section 2, we briefly review Tseng et al.'s authenticated encryption scheme. An attack on Tseng et al.'s authenticated encryption scheme is proposed in Section 3. Finally, we give a brief conclusion in Section 4.

2 Review of Tseng et al.'s Scheme

Tseng et al. proposed an authenticated encryption scheme [10] that only the specified receiver can verify and recover the message. The scheme contains three phases: initialization phase, signature generation and message recovery phases. Three phases are described in the following subsections, respectively.

2.1 Initialization Phase

There is a trusted authority that generates system parameters as follows: N denotes the product of two large primes p and q, where $p = 2p' + 1$ and $q = 2q' + 1$, with themselves prime; g denotes a base element of order $p' \times q'$; $h(\cdot)$ denotes a public one-way function. After generating these parameters, the trusted authority publishes $\{N, g\}$ and keeps $\{p, q, p', q'\}$ secret.

Assume each user has a unique identity ID. When a user Alice wants to compose her public key. Alice randomly select an integer x_i as her secret key and computes $p_i = g^{x_i} \bmod N$. Then, she sends p_i and her unique identity ID_i to the trusted authority. Upon receiving p_i and ID_i, the trusted authority computes and publishes Alice's public key $y_i = (p_i - ID_i)^{(h(ID_i))^{-1}} \bmod N$. Alice can verify the public key y_i by computing the following equation:

$$y_i^{h(ID_i)} + ID_i = g^{x_i} \bmod N. \tag{1}$$

2.2 Signature Generation Phase

Suppose that Alice wants to send an authenticated message M to Bob (whose identity is ID_j). She first chooses a random integer k and computes the signature $\{r, s\}$ for message M, where

$$\begin{cases} r &= M \cdot (y_j^{h(ID_j)} + ID_j)^{-k} \bmod N, \\ s &= k - x_i \cdot h(r). \end{cases}$$

Next, Alice sends $\{r, s\}$ to the Bob.

2.3 Message Recovery Phase

After receiving $\{r, s\}$, Bob uses his secret key x_j to recover the message M. Thus, the message can be recovered by computing the following equation.

$$M = r \cdot (g^s \cdot (y_i^{h(ID_i)} + ID_i)^{h(r)})^{x_j} \bmod N. \tag{2}$$

The message M must be correctly recovered and verified by checking the validity of the redundancy.

3 Attack on Tseng et al.'s Scheme

In this section, we will show that Tseng et al.'s authenticated encryption scheme cannot withstand the known plaintext-ciphertext attack. Assume Alice wants to sign and encrypt the message to a specified receiver Bob. First, Alice computes the signature $\{r, s\}$ for the message M. Upon receiving $\{r, s\}$, Bob uses his secret key x_j to recover the message M. However, an intruder has ability to recover the message without Bob's secret key. From Equation (2), it can be derived as follows:

$$\begin{aligned} M &= r \cdot (g^s \cdot ((y_i^{h(ID_i)} + ID_i)^{h(r)})^{x_j} \bmod N \\ &= r \cdot (g^{x_j})^s \cdot ((y_i^{h(ID_i)} + ID_i)^{x_j})^{h(r)} \bmod N. \end{aligned} \tag{3}$$

If an intruder collects (M_1, r_1, s_1) and (M_2, r_2, s_2), then he/she can obtain the following two equations as Equation 3.

$$\begin{cases} M_1 &= r_1 \cdot (g^{x_j})^{s_1} \cdot ((y_i^{h(ID_i)} + ID_i)^{x_j})^{h(r_1)} \bmod N \\ M_2 &= r_2 \cdot (g^{x_j})^{s_2} \cdot ((y_i^{h(ID_i)} + ID_i)^{x_j})^{h(r_2)} \bmod N. \end{cases} \tag{4}$$

From Equation (4), it can be seen that

$$\begin{cases} ((y_i^{h(ID_i)} + ID_i)^{x_j})^{h(r_1)} \bmod N &= M_1 \cdot (r_1 (g^{x_j})^{s_1})^{-1} \\ ((y_i^{h(ID_i)} + ID_i)^{x_j})^{h(r_2)} \bmod N &= M_2 \cdot (r_2 (g^{x_j})^{s_1})^{-1}. \end{cases} \tag{5}$$

If the value $h(r_1)$ and $h(r_2)$ are relatively prime, the intruder can find two numbers a and b such that $ah(r_1) + bh(r_2) = 1$ by the Euclidean algorithm [9]. Let the value $(y_i^{h(ID_i)} + ID_i)^{x_j}$ be the value X. From Equation (5), the value X can be revealed by computing the following equations:

$$\begin{aligned} (X^{h(r_1)})^a \cdot (X^{h(r_2)})^b &= (M_1 \cdot (r_1 (g^{x_j})^{s_1})^{-1})^a \cdot (M_2 \cdot (r_2 (g^{x_j})^{s_2})^{-1})^b \bmod N \\ X^{ah(r_1)+bh(r_2)} &= M_1^a M_2^b r_1^{-a} r_2^{-b} (g^{x_j})^{-(as_1+bs_2)} \bmod N \\ X &= M_1^a M_2^b r_1^{-a} r_2^{-b} (g^{x_j})^{-(as_1+bs_2)} \bmod N. \end{aligned}$$

From Equation 1, an intruder can obtain g^{x_j} by computing $y_i^{h(ID_i)} + ID_i \bmod N$, where y_i, $h(ID_i)$, and ID_i are public. Since all of M_1, M_2, a, b, r_1, r_2, s_1, s_2, and g^{x_j} are known, the intruder can easy to obtain X (i.e., $(y_i^{h(ID_i)} + ID_i)^{x_j}$).

Since the intruder can obtain the value $(y_i^{h(ID_i)} + ID_i)^{x_j}$, he/she can expose the next message sent between Alice and Bob. Therefore, Tseng et al.'s authenticated encryption scheme cannot fulfill their opinion of security requirement.

To remedy this weakness, every $h(r_i)$s cannot relatively prime with other $h(r_j)$s. If $h(r_i)$ is relatively prime with other $h(r_j)$s, then the signer need to rechoose an integer k_i in Signature Generation Phase such that $\gcd(h(r_i), h(r_j)) \neq 1$ for all generated r_js.

4 Conclusion

We have shown that Tseng et al.'s authenticated encryption scheme cannot fulfill their opinion of security requirement. Their scheme cannot withstand the known plaintext-ciphertext attack. Hence, the intruder has ability to expose every message sent between the signer and the specified receiver.

References

[1] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, pp. 469–472, July 1985.

[2] M. Girault, "Self-certified public keys," in *Advances in Cryptology, EUROCRYPT'91*, pp. 491–497, Lecture Notes in Computer Science, 1991.

[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, "An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445–446, 2002.

[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] Wei-Bin Lee and Chin chen Chang, "Authenticated encryption schemes with linkages between message blocks," *Information Processing Letters*, vol. 63, no. 5, pp. 247–250, 1997.

[7] Kaisa Nyberg and Rainer A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm," *Designs, Codes Cryptography*, vol. 7, pp. 61–81, 1996.

[8] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.

[9] Bruce Schneier, *Applied Cryptography, 2nd Edition.* New York: John Wiley & Sons, 1996.

[10] Yuh-Min Tseng, Jinn-Ke Jan, and Hung-Yu Chien, "Digital signature with message recovery using self-certified public keys and its variants," *Applied Mathematics and Computation*, vol. 136, pp. 203–214, 2003.