Improvement of Authenticated Encryption Schemes with Message Linkages for Message Flows*

Min-Shiang Hwang[†] Member Jung-Wen Lo[‡§] Shu-Yin Hsiao[¶]

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

Department of Information Management[‡]
National Taichung Institute of Technology
129 Sec. 3, San-min Rd., Taichung, Taiwan 404, R.O.C.

Institute of Computer Science[§]
National Chung Hsing University
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.

Graduate Institute of Networking and Communication Engineering[¶]
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.

Improvement of Authenticated Encryption Schemes with Message Linkages for Message Flows

Abstract

An authenticated encryption scheme provides a mechanism of signing and encrypting simultaneously, and furthermore, the receiver can verify and decrypt the signature at the same time. Tseng et al. proposed two efficiently authenticated encryption schemes which can check the validity of the sent data before message recovery, but in fact their schemes cannot achieve completely the function. In this article, we point out the flaw and propose an improved scheme of revision.

Keywords: Authentication, cryptography, digital signature, encryption.

1 Introduction

In 1993, Nyberg and Rueppel proposed a digital signature scheme with message recovery based on discrete logarithms [9, 10]. For reducing the communication cost of Nyberg and Rueppel's schemes, Horster et al. proposed an authenticated encryption scheme afterward [2], and there have actually been quite a lot of efficient authenticated encryption schemes presented since then [4, 5, 8, 11, 13]. In these schemes, the signer produces a signature for a message and then sends the signature to a specific receiver. After receiving the signature, only the receiver can recover and verify the message.

In an authenticated encryption scheme, signer may split a message into several blocks. Therefore, with approach of encryption and signature for individual message, the authenticated encryption scheme demands efficient computing and the less use of bandwidth for data communication. So far, a number of authenticated encryptions with message linkage protocols have been proposed

[8, 12]. Tseng et al.'s schemes [12] are the most efficient in terms of the communication and computation cost than all other schemes proposed previously.

In this paper, we show that Tseng et al.'s scheme suffers from message flows destroyed by an adversary but the receiver is unconscious of the wrong flaws. In addition, we propose an improved scheme which modifies some aspects of Tseng et al.'s scheme.

The remainder of this article is organized as follows. In the next section, a brief review of Tseng et al.'s schemes and cryptanalysis of their schemes are given. In Section 3, we propose an improved scheme. The security analysis of the proposed scheme is discussed in Section 4. Finally, the conclusion is given in Section 5.

2 The Weakness of Tseng et al.'s Scheme

Tseng et al. proposed two efficiently authenticated encryption schemes: basic scheme and generalized scheme [12]. The former scheme is suitable for all-or-nothing flow encryption. It is more efficient than all other proposed schemes in the costs of communication and computation. However, this scheme has a drawback that the receiver must wait for the arrival of the whole signature blocks. Therefore, Tseng et al. proposed the generalized scheme in order to avoid this weakness. In other words, the receiver can receive and recover a message in the meantime.

2.1 Review of Tseng et al's Basic Scheme

The basic scheme Tseng et al. proposed contains three phases: the system initialization, the signature generation, and the message recovery phases. The scheme has a system authority SA, a signer U_a and a receiver U_b. In the system initialization phase, SA publishes system parameters including p, q, g and f. The parameter p is a large prime number and the parameter q is a large prime factor of $p-1$. Let g be a generator with order q in $GF(p)$, and f be a one-way hash function. A user U_i chooses a private key x_i and calculates one's public key $y_i = g^{x_i} \bmod p$.

In the signature generation phase, the message M is separated into M_1, M_2, $\cdots$, M_n, where $M_i \in GF(p)$ and $i \in 1, \cdots, n$. When U_a wants to send a message M to the receiver U_b, U_a first sets up $r_0 = 0$, chooses a random number $k \in GF(q)$, and then calculates r_i, r, and s as follows:

$$\begin{aligned} r_i &= M_i \cdot f(r_{i-1} \oplus y_b^k) \bmod p \quad \text{for} \ \ i = 1, 2, \cdots, n, \\ r &= f(r_1 \parallel r_2 \parallel \cdots \parallel r_n), \\ s &= k - r \cdot x_a \bmod q. \end{aligned}$$

Afterward, U_a sends $(r, s, r_1, r_2, \cdots, r_n)$ to U_b.

In message recovery phase, when U_b receives the whole signature blocks, U_b calculates r' as follows:

$$r' = f(r_1 \parallel r_2 \parallel \cdots \parallel r_n) \tag{1}$$

If $r' = r$ holds, then U_b calculates y_b^k and M_i as follows:

$$y_b^k = y_b^s \cdot y_{ab}^r \bmod p, \quad \text{where} \ \ y_{ab} = y_a^{x_b} \bmod p, \tag{2}$$

$$M_i = r_i \cdot f(r_{i-1} \oplus y_b^k)^{-1} \bmod p, \quad \text{for} \ \ i = 1, 2, \cdots, n \ \ \text{and} \ \ r_0 = 0. \tag{3}$$

2.2 Cryptanalysis of Tseng et al.'s Scheme

In Tseng et al.'s scheme, the purpose of Equation (1) is to ensure that signature blocks are not falsified by someone, but it is unable to achieve the goal. Herein, we assume that someone attempts to destroy the message flow with the following procedures:

Step1. Generate an incorrect r_i'.

Step2. Obtain r' from $r' = f(r_1' \parallel r_2' \parallel \cdots \parallel r_n')$.

Step3. Delivery $(r', s, r_1', r_2', \cdots, r_n')$ to U_b.

The receiver must check the correctness of the message flow to assure that the signature blocks are not falsified or lost while obtaining the message flow of signature. Therefore, the receiver U_b executes Equations (1)$\sim$(3). U_b calculates r'' as $f(r'_1 \parallel r'_2 \parallel \cdots \parallel r'_n)$. It is obvious that r'' is equal to the forged r'. Therefore, U_b recovers the message blocks as follows:

$$\begin{aligned} y_b^{k'} &= y_b^s \cdot y_{ab}^{r'} \bmod p, \quad \text{where} \quad y_{ab} = y_a^{x_b} \bmod p, \\ M'_i &= r'_i \cdot f(r'_{i-1} \oplus y_b^{k'})^{-1} \bmod p, \quad \text{for} \quad i = 1, 2, \cdots, n \quad \text{and} \quad r_0 = 0. \end{aligned}$$

As the result, the receiver cannot discover that the recovery message is not the same as the original message M. Tseng et al.'s generalized scheme is designed for package switch networks, but it still has the same problem.

3 The Proposed Scheme

To avoid message flows altered by attackers and the receiver's unawareness, we propose an improvement of Tseng et al.'s scheme. The basic concept is the same as that of Tseng et al.'s scheme, including parameters (p, q, g, $f(\cdot)$, x_a, y_a, x_b, y_b, m) and three phases. We go into the proposed scheme as follows.

Signature Generation Phase:

The message M is separated into M_1, M_2, $\cdots$, M_n, where $M_i \in GF(p)$. While U_a wants to send a message M to U_b, U_a executes the following processes to produce the signature blocks:

Step1. Set $r_0 = 0$ and choose a random number $k \in GF(q)$. Then compute y_b^k and $t = g^k \bmod p$.

Step2. Compute the values r_i, r, and s as follows:

$$\begin{aligned} r_i &= M_i \oplus f(r_{i-1} \oplus y_b^k) \bmod p, \quad \text{for} \quad i = 1, \cdots, n, \\ r &= f(r_1 \parallel r_2 \parallel \cdots \parallel r_n) \\ s &= k - r \cdot x_a \bmod q \end{aligned}$$

Afterward, U_a sends $(t, s, r_1, r_2, \cdots, r_n)$ to U_b.

Message Recovery Phase:

When U_b receives the whole signature blocks, U_b recovers the message blocks as follows. U_b checks the following equation whether it is equal or not:

$$t^{x_b} = y_b^s \cdot y_{ab}^{r'} \bmod p. \tag{4}$$

If the above equation holds, U_b calculates r' and recovers the message blocks M_i as follows:

$$\begin{aligned} r' &= f(r_1 \parallel r_2 \parallel \cdots \parallel r_n) & (5)\\ M_i &= r_i \oplus f(r_{i-1} \oplus t^{x_b})^{-1} \bmod p, \quad \text{for} \quad i = 1, \cdots, n \quad \text{and} \quad r_0 = 0. & (6) \end{aligned}$$

The proposed scheme is also appropriate for conducting Tseng et al.'s generalized scheme in the similar way.

4 Security Analysis

The security of the proposed scheme is based on the difficulties of one-way hash function [3, 6] and discrete logarithms [1, 7, 14]. In this section, we analyze some possible attack situations and prove that the proposed scheme can successfully withstand these possible attacks.

Attack 1: An adversary attempts to derive the user's private key x_i from the available public information.

Analysis of Attack 1: Assume that an adversary wants to derive U_i's private key x_i from the corresponding public key $y_i = g^{x_i} \bmod p$. It is as difficult as breaking discrete logarithms to obtain U_i's private key x_i. With the knowledge of signature $(t, s, r_1, r_2, \cdots, r_n)$, the adversary has no ability to disclose the secret key x_a, which is based on the digital signature algorithm. The adversary also cannot derive secret value k through Equation (4), since the equation has two unknown variables k and x_i where the k is also under the protection of discrete logarithms.

Attack 2: An adversary tries to forge an authenticated encryption signature $(t, s, r_1, r_2, \cdots, r_n)$.

Analysis of Attack 2: Generating a valid signature must utilize the private key of signer. We have proven that an adversary cannot derive U_a's private key x_a on Attack 1. Thereupon, an adversary is incapable of forging any valid signature without knowing x_a, and any forged signature cannot pass the verification via Equation (4).

Attack 3: An adversary attempts to recover the message M from an authenticated encryption signature.

Analysis of Attack 3: From Equation (4), the message M can be recovered by anyone who has the private key x_b and is capable to compute y_b^k. Similar to Attack 1, it is difficult to break discrete logarithms to obtain a user's private key.

Attack 4: An adversary upsets message flows and the receiver does not recognize.

Analysis of Attack 4: If an adversary upsets message flows, the incorrect messages will be detected by the receiver. The receiver can verify whether the signature blocks are destroyed or lost by recomputing r' and s in Equations (4)∼(6). Similar to Attack 2, it is too difficult to obtain U_i's private key x_i by breaking discrete logarithms. Furthermore, an adversary cannot find some another values r_i' ($r_i' \neq r_i$) satisfying $r' = f(r_1 \parallel r_2 \parallel \cdots \parallel r_n)$. The r is under the protection of one-way hash function.

5 Conclusion

In this article, we enhance the security of Tseng et al.'s scheme. The proposed scheme also can apply to the generalized scheme of Tseng et al.'s scheme. The proposed scheme not only satisfies requirements of Tseng et al.'s scheme and protects user's private data certainly, but also achieves the security we mentioned above. Furthermore, we also analyze the security of our scheme in previous section. Our scheme can not only resist any adversary's attacks, but also detect the correctness of signature blocks. The proposed scheme is more secure than Tseng et al.'s scheme.

References

[1] Amit K Awasthi, "On the Authentication of the User from the Remote Autonomous Object," *International Journal of Network Security*, vol. 1, no. 3, pp. 166–167, 2005.

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

[3] 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.

[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] 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, 2005.

[6] Minho Kim and Cetin Kaya Koc, "A Simple Attack on a Recently Introduced Hash-based Strong-password Authentication Scheme," *International Journal of Network Security*, vol. 1, no. 2, pp. 77–80, 2005.

[7] Cheng-Chi Lee, Min-Shiang Hwang, and Li-Hua Li, "A new key authentication scheme based on discrete logarithms," *Applied Mathematics and Computation*, vol. 139, no. 2, pp. 343–349, 2003.

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

[9] K. Nyberg and R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery," in *1st ACM Conference on Computer and Communications Security*, pp. 58–61, Fairfax, Virginia, Nov. 1993.

[10] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm," in *Advances in Cryptology, EUROCRYPT'94*, pp. 175–190, 1994.

[11] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm," *Designs, Codes and Cryptography*, vol. 7, no. 1-2, pp. 61–81, 1996.

[12] Yuh-Min Tseng, Jinn-Ke Jan, and Hung-Yu Chien, "Authenticated encryption schemes with message linkages for message flows," *Computers and Electrical Engineering*, vol. 29, no. 1, pp. 101–109, 2003.

[13] Tzong-Sun Wu, Tzong-Chen Wu, and Wei-Hua He, "Authenticated encrption schemes with double message linkage," in *Proceeding of* 9^{th} *National Conference on Information Security, R.O.C.*, pp. 303–308, 1999.

[14] Chou-Chen Yang, Ting-Yi Chang, and Min-Shiang Hwang, "A new anonymous conference key distribution system based on the elliptic curve

discrete logarithm problem," *Computer Standards & Interfaces*, vol. 25, no. 2, pp. 141–145, 2003.