

## Short Paper

---

# An Efficient Authenticated Encryption Scheme With Message Linkages and Low Communication Costs

YUH-MIN TSENG\* AND JINN-KE JAN

*\*Department of Information Management  
Nan-Kai College of Technology and Commerce  
Nantou, 542 Taiwan  
Institute of Applied Mathematics  
National Chung Hsing University  
Taichung, 402 Taiwan*

An efficient authenticated encryption scheme with message linkages is proposed. For achieving both privacy and integrity in data communications, the proposed scheme requires smaller bandwidth and computational time when compared to previously proposed authenticated encryption schemes with message linkages. Moreover, the proposed scheme allows the verifier to recover and verify the message blocks simultaneously, and hence, the message recovery phase could be speeded up. The security of the proposed scheme is based on the authenticated encryption scheme as well as the one-way hash cryptographic function assumption.

**Keywords:** cryptography, authentication, encryption, message linkage, signature

## 1. INTRODUCTION

In [6] Nyberg and Rueppel presented the first signature scheme based on the discrete logarithm problem that gives message recovery. They also proposed in [7] a general procedure on how to modify all previously proposed signature schemes based on the discrete logarithm problem to allow message recovery. Later, Horster et al. [2] proposed an authenticated encryption scheme modified from Nyberg-Rueppel's scheme. Authenticated encryption scheme can be regarded as the combination of data encryption scheme and digital signature scheme. In the authenticated encryption scheme, the signer may make a signature-ciphertext for a message and then send it to a specified receiver. And, only the receiver has the ability to recover and verify the message. It can be seen that, compared to the straightforward approach employing the encryption and the signature schemes for a message, authenticated encryption scheme requires a smaller bandwidth for data communications to achieve privacy, integrity and authentication of information.

---

Received November 25, 1999; revised April 11, 2000; accepted May 3, 2000.  
Communicated by Hsu-Chun Yen.

In order to recover the message from the signature, the message cannot be hashed to reduce the message size. If the message is large, it must be divided into a sequence of message blocks, and each message block is encrypted and signed individually. Unfortunately, this approach has a disadvantage: An intruder can reorder or delete some signature blocks so that the recipient does not know whether the message blocks have been rearranged or deleted. This disadvantage can be remedied by employing a redundancy mechanism to construct the linkages among message blocks [2], but it increases the communication costs.

To reduce the communication costs for employing a redundancy mechanism, Hwang et al. [3] proposed an authenticated encryption scheme with message linkages based on that of Horster et al.'s scheme. In Hwang et al.'s scheme, the signer adds the  $(i - 1)$ th secret for  $(i - 1)$ th message block into the signature for the  $i$ th message block, allowing the message linkages to be constructed. Recently Lee and Chang [5] also proposed another scheme with message linkages based on Lee-Chang's scheme [4] in which the communication costs and computational complexity are low in comparison to Hwang et al.'s scheme.

In this paper, we propose an efficient authenticated encryption scheme with message linkage and low communication costs based on Horster et al.'s scheme. The proposed scheme has lower communication costs and less computational complexity than those mentioned above, and the security of the proposed scheme is the same as that of those previously proposed schemes.

The remainder of this article is organized as follows. In the next section, the proposed system is described. Section 3 presents the security analysis of the proposed system. In Section 4, we present the performance for our system and compare it with the previous work. Section 5 gives our conclusions.

## 2. OUR SCHEME

Our scheme consists of three phases: system initialization, signature generation, and message recovery. We describe these in detail here.

### System initialization phase

The system authority (SA) chooses a large prime number  $p$  such that  $p - 1$  has a large prime factor  $q$ . Let  $g$  be a generator with order  $q$  in  $GF(p)$ . SA also selects a one-way hash function  $f$ [8]. Then, SA publishes  $p$ ,  $q$ ,  $g$  and  $f$ . Each user in the system,  $U_i$ , selects a secret key  $x_i$  in  $Z_q$  and computes the corresponding public key  $y_i = g^{x_i} \bmod p$ .

### Signature generation phase

Without loss of generality, assume that signer  $U_a$  wants to send a message  $M$  to a specified receiver  $U_b$ . Message  $M$  is made up of the sequence  $\{M_1, M_2, \dots, M_n\}$ , where  $M_i \in GF(p)$ . Thus, signer  $U_a$  carries out the following procedure to generate the signature blocks for message  $M$ .

- (1) Let  $r_0 = 0$  and choose a random number  $k \in GF(q)$

- (2) Compute  $r_i = M_i \cdot f(r_{i-1} \oplus y_b^k) \bmod p$  for  $i = 1, \dots, n$ , where “ $\oplus$ ” denotes the exclusive operator.
- (3) Compute  $s = k - r \cdot x_a \bmod q$ , where  $r = h(r_1 \| r_2 \| \dots \| r_n)$ ,  $h$  is a one-way hash function [8] and “ $\|$ ” denotes concatenation.

Finally,  $U_a$  sends  $n + 1$  signature blocks  $(r, s, r_1, r_2, \dots, r_n)$  to  $U_b$  in a public way. Note that  $r_i$  is used as a linking parameter to generate the  $i$ th and  $(i + 1)$ th message blocks.

### Message recovery phase

After receiving the set  $(r, s, r_1, r_2, \dots, r_n)$ ,  $U_b$  performs the verification procedure to recover the message blocks  $\{M_1, M_2, \dots, M_n\}$ .

- (1) Compute  $r' = h(r_1 \| r_2 \| \dots \| r_n)$  and check that  $r' = r$  holds.
- (2) Compute  $y_b^k = y_b^s \cdot y_{ab}^r \bmod p$ , where  $y_{ab} = y_a^{x_b} \bmod p$ .
- (3) Recover the message blocks  $\{M_1, M_2, \dots, M_n\}$  as follows.

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

In the following theorem, we show that message blocks  $\{M_1, M_2, \dots, M_n\}$  can be correctly recovered and verified.

**Theorem:** Message block  $\{M_1, M_2, \dots, M_n\}$  can be obtained by computing  $M_i = r_i \cdot f(r_{i-1} \oplus y_b^k)^{-1} \bmod p$ , where  $i = 1, \dots, n$  and  $r_0 = 0$ .

**Proof:** Since  $s = k - r \cdot x_a \bmod q$  and  $r = h(r_1 \| r_2 \| \dots \| r_n)$ , we have

$$\begin{aligned} & y_b^s \cdot y_{ab}^r \bmod p \\ &= y_b^{k - r \cdot x_a} \cdot y_{ab}^r \bmod p \\ &= y_b^k \cdot y_b^{-r \cdot x_a} \cdot y_{ab}^r \bmod p, \text{ where } y_{ab} = y_a^{x_b} \bmod p. \\ &= y_b^k \bmod p \end{aligned}$$

Since  $r_i = M_i \cdot f(r_{i-1} \oplus y_b^k) \bmod p$ ,  $M_i$  can be obtained by  $M_i = r_i \cdot f(r_{i-1} \oplus y_b^k)^{-1} \bmod p$ .  $\square$

## 3. SECURITY ANALYSIS

The security of our scheme is primarily based on the authenticated encryption scheme of [2] and the same one-way hash function assumptions as the previously proposed schemes. Note that the adopted one-way hash function is Secure Hash Function (SHS) [8], uses a 160-bit hash value. This makes the known birthday attack even harder. Besides, as for strengthening the security, the modular exponentiation function can also be considered the one-way hash function. So the security is based on the difficulty of computing the discrete logarithm problem [2, 7].

In the following, some security problems are considered.

- (1) An intruder tries to derive a user's secret key  $x_a$  from the corresponding public key  $y_a = g^{x_a} \bmod p$ . He will face the difficulty of computing the discrete logarithm [2, 7]. It is also difficult to derive the secret key  $x_a$  from  $s = k - r \cdot x_a \bmod q$ , because the equation has two unknown variables.
- (2) If an intruder knows one message block  $M_i$ , he may try to derive the common key  $y_{ab}$ . He first computes  $f(r_{i-1} \oplus y_b^k) = M_i^{-1} \cdot r_i \bmod p$ . If he can obtain  $y_b^k$ , then  $y_{ab}$  can be derived from  $y_b^k = y_b^s \cdot y_{ab}^r \bmod p$ . However,  $y_b^k$  is protected under the one-way hash function, so he cannot obtain it.
- (3) If an intruder knows one message block  $M_i$ , he may try to derive the remaining message blocks. Although he may obtain  $f(r_{i-1} \oplus y_b^k) = M_i^{-1} \cdot r_i \bmod p$ , he cannot derive  $y_b^k$ , because  $y_b^k$  is protected under the one-way hash function. Thus, our scheme can withstand the known-plaintext attack.
- (4) If any signature block is reordered, modified, deleted or replicated, then the signature equation  $s = k - r \cdot x_a \bmod q$  must be modified as well. Because  $r = h(r_1 \| r_2 \| \dots \| r_n)$ , it is guaranteed that it is hard to reorder, delete, modify or replicate.

#### 4. PERFORMANCE AND COMPARISONS

In this section, we will discuss the computational complexity and size of transmitted messages. For convenience the following notations are used to analyze the computational complexity and the communication costs:  $|m|$  denotes the bit length of  $m$ ;  $T_f$  and  $T_h$  are the times for executing the adopted one-way hash function  $f$  and  $h$ , respectively;  $T_{EXP}$  is the time for modular exponentiation;  $T_{INV}$  is the time for modular inverse;  $T_{MUL}$  is the time for modular multiplication. Note that the time for computing modular addition, subtraction and exclusive-or operation is ignored, since they are much smaller than  $T_{EXP}$ ,  $T_{INV}$ ,  $T_{MUL}$ ,  $T_f$  and  $T_h$ .

Let  $n$  be the number of message blocks and  $\{M_1, M_2, \dots, M_n\}$  be the set of signed message blocks. The size of signed message blocks  $\{M_1, M_2, \dots, M_n\}$  is bounded to  $n|p|$ . Generally, the chosen  $p$  and  $q$  is greater than  $2^{512}$  and  $2^{160}$ , respectively. In Hwang et al.'s scheme [3], the signer selects  $n$  distinct random numbers to generate  $r_i, i = 1, \dots, n$ . Then the signer adds the  $(i-1)$ th random number for the  $(i-1)$ th message block into the signature for the  $i$ th message block, and then the message linkages can be constructed, but each message block is signed individually using Horster et al.'s scheme [2]. The set of signature blocks is  $\{(r_1, s_1), (r_2, s_2), \dots, (r_n, s_n)\}$  and the size of the set is bounded to  $n|p| + n|q|$ . To reduce the communication costs, Lee and Chang [5] used fewer random numbers to generate signature blocks. In their scheme, the transmitted signature blocks for signing the message blocks  $\{M_1, M_2, \dots, M_n\}$  are  $\{r_1, r_2, \dots, r_n, s_1, s_2, \dots, s_t\}$ , where  $t = \lceil \log n \rceil$ . It is bounded to  $n|p| + t|q|$ . In our scheme, the set of signature blocks is  $(r, s, r_1, r_2, \dots, r_n)$ . Generally, the chosen  $p$  and  $q$  is greater than  $2^{512}$  and  $2^{160}$ , respectively. Note that the adopted one-way hash function  $h$  to compute  $r = h(r_1 \| r_2 \| \dots \| r_n)$  is SHS [8], it always produces a fixed-length (160 bits) output.

Therefore, the size of  $(r, s, r_1, r_2, \dots, r_n)$  is bounded to  $n|p| + 2|q|$  and the transmission efficiency is  $n|p| / (n|p| + 2|q|)$ .

For time complexity consideration, the computational complexity for the signature generation and message recovery are  $T_{EXP} + (n+1)T_{MUL} + nT_f + T_h$  and  $3T_{EXP} + nT_{INV} + (n+1)T_{MUL} + nT_f + T_h$ , respectively. From the viewpoint of the computational complexity for the signature generation and message recovery as well as the communication costs, we make comparisons among our scheme, Lee-Chang's scheme [5] and Hwang et al.'s scheme [3]. The comparisons are presented in Table 1. As shown in Table 1, it is obvious that our proposed scheme is more efficient than Hwang et al.'s scheme and Lee-Chang's scheme in the term of the communication costs.

**Table 1. Comparisons of our scheme with those of Lee-Chang's scheme and Hwang et al.'s scheme.**

	Our scheme	Lee-Chang's scheme	Hwang et al.'s scheme
Size of signature blocks	$n p  + 2 q $	$n p  + t q $	$n p  + n q $
Transmission efficiency	$n p  / (n p  + 2 q )$	$n p  / (n p  + t q )$	$n p  / (n p  + n q )$
Time complexity of signature generation	$T_{EXP} + (n+1)T_{MUL} + nT_f + T_h$	$nT_{EXP} + T_h + (n+t)T_{MUL}$	$nT_{EXP} + nT_f + nT_{INV} + 2nT_{MUL}$
Time complexity of message recovery	$3T_{EXP} + nT_{INV} + nT_f + (n+1)T_{MUL} + T_h$	$(t+2)T_{EXP} + nT_{INV} + (3n+t)T_{MUL} + T_h$	$(2n+1)T_{EXP} + nT_f + 3nT_{MUL}$

Note that the linkage between  $M_{i-1}$  and  $M_i$  is achieved through  $r_{i-1}$  because  $M_i = r_i \cdot f(r_{i-1} \oplus y_b^k)^{-1} \bmod p$ , and hence, the  $i$ th message block can be recovered independently. Therefore, the proposed scheme allows the verifier to recover and verify the message blocks simultaneously. It can be seen that the message recovery phase could almost be speeded up  $n$  times.

## 5. CONCLUSIONS

We have proposed an efficient authenticated encryption scheme with messages linkage. Only a random number was used, but we have shown that the security of the proposed scheme is the same as one of the previously proposed schemes. In comparison with the all previously proposed schemes in terms of the communication costs and the computational complexity, we have demonstrated that our scheme performs better.

## REFERENCES

1. W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. 22, 1976, pp. 644-654.

2. P. Horster, M. Michels, and H. Petersen, "Authenticated encryption schemes with low communication costs," *Electronics Letters*, Vol. 30, 1994, pp. 1212.
3. S. J. Hwang, C. C. Chang, and W. P. Yang, "Authenticated encryption schemes with message linkages," *Information Processing Letters*, Vol. 58, 1996, pp. 189-194.
4. W. B. Lee and C. C. Chang, "Authenticated encryption scheme without using a one-way hash function," *Electronics Letters*, Vol. 31, 1995, pp. 1656-1657.
5. W. B. Lee and C. C. Chang, "Authenticated encryption schemes with linkage between message blocks," *Information Processing Letters*, Vol. 63, 1997, pp. 247-250.
6. K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm," *Advances in Cryptology – EUROCRYPT'94*, Springer-Verlag, 1994, pp. 175-190.
7. K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm," *Designs, Codes and Cryptography*, Vol. 7, 1996, pp. 61-81.
8. NIST FIPS PUB 180, "Secure hash standard," National Institute of Standards and Technology, U.S. Department of Commerce, DRAFT, 1993.

**Yuh-Min Tseng (曾育民)** received the B.S. degree in Computer Science and Engineering from National Chiao Tung University, Taiwan, Republic of China, in 1988; and the M.S. degree in Computer and Information Engineering from National Taiwan University in 1990 and the Ph.D. in Applied Mathematics from National Chung Hsing University in 1999. He is currently an Associate Professor of the Department of Information Management, Nan-Kai College of Technology and Commerce. He is a member of the Chinese Association for Information Security. His research interests include network security, cryptography, database security, and image encryption.

**Jinn-Ke Jan (詹進科)** was born in Taiwan in 1951. He received the B.S. degree in Physics from Catholic Fu Jen University, Taiwan, Republic of China, in 1974 and the M.S. degree in Information and Computer Science from Tokyo University in 1980. He studied Software Engineering and Human-Computer Interface at the University of Maryland, College Park, MD, during 1984-1986. He is presently a professor of the Department of Applied Mathematics at National Chung Hsing University, Taiwan. He is currently also a director of the Computer Center at National Chung Hsing University, the editor of Information and Education, and an executive member of the Chinese Association for Information Security. His research interests include computer cryptography, network security, human factors of designing software and information systems, database security, and coding theory.