ELSEVIER

Information Processing Letters 58 (1996) 189–194

Information Processing Letters

Authenticated encryption schemes with message linkage

Shin-Jia Hwang [a,*], Chin-Chen Chang [b,1], Wei-Pang Yang [a]

[a] *Institute of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan 300, ROC*

[b] *Institute of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan 621, ROC*

Received 15 August 1995; revised 15 January 1996

Communicated by S.G. Akl

Abstract

Authenticated encryption schemes need redundancy schemes to link up the message blocks; however, these redundancies increase communication costs. To construct links without increasing communication costs, we propose a general solution for all the authenticated encryption schemes based on the discrete logarithm problem. Because the computation cost to construct links is small, the improved scheme adopting our solution is almost as efficient as the original one. Moreover, by our solution, the recipient can easily determine the missing message blocks, and then acknowledge the sender to send only these blocks again. The communication cost will be also reduced. Adopting our solution, we also propose two new authenticated encryption schemes with message linkage.

Keywords: Authenticated encryption; Message recovery; Public key cryptography; Safety/security in digital systems

1. Introduction

Authenticated encryption schemes are useful for transmitting confidential data in insecure networks since they provide the data confidence, authentication and integrity, simultaneously. Based on the discrete logarithm problem, Nyberg and Ruppel [4] proposed the first authenticated encryption schemes. To reduce the communication cost of Nyberg and Rupple's schemes, Horster et al. [2] proposed their improved schemes. However, Horster et al.'s schemes need the aid of additional one-way functions to provide the encryption function. To remove additional one-way functions, Hwang et al. [3] proposed another authenticated encryption scheme without any additional one-way function.

However, there still exists a common disadvantage for the above authenticated encryption schemes. Usually, the length of the message is so long that the message must be divided into many message blocks first. Then the sender encrypts and signs these message blocks into the corresponding ciphertext blocks, respectively. Finally, the sender sends these ciphertext blocks out. Despite deriving no message block from the ciphertext block, an eavesdropper could remove some blocks from the ciphertext blocks. The recipient cannot detect this removal since the authenticated encryption schemes cannot use one-way hash functions. This removal is usually detected by a redundancy scheme on messages. That is, each mes-

* Corresponding author. Email: hwangsj@winston.cis.nctu.edu.tw.

[1] Email: ccc@cs.ccu.edu.tw.

PII S0020-0190(96)00032-4

Table 1
The original signature equations for the authenticated encryption scheme

Signature equation	The computation of $y_B^{k_i} \bmod P$
(1) $s_i \times k_i \equiv 1 + r_i \times x_A \pmod{Q}$	$y_B^{k_i} = (y_B \times y_{AB}^{r_i})^{(s_i)^{-1}} \bmod P$
(2) $r_i \times k_i \equiv 1 + s_i \times x_A \pmod{Q}$	$y_B^{k_i} = (y_B \times y_{AB}^{s_i})^{(r_i)^{-1}} \bmod P$
(3) $k_i \equiv s_i + r_i \times x_A \pmod{Q}$	$y_B^{k_i} = y_B^{s_i} \times y_{AB}^{r_i} \bmod P$
(4) $s_i \times k_i \equiv r_i + x_A \pmod{Q}$	$y_B^{k_i} = (y_B^{r_i} \times y_{AB})^{(s_i)^{-1}} \bmod P$
(5) $r_i k_i \equiv s_i + x_A \pmod{Q}$	$y_B^{k_i} = (y_B^{s_i} \times y_{AB})^{(r_i)^{-1}} \bmod P$
(6) $k_i \equiv r_i + s_i \times x_A \pmod{Q}$	$y_B^{k_i} = (y_B^{r_i} \times y_{AB}^{s_i}) \bmod P$

sage block contains the redundant bits to link up message blocks, but these redundancies increase communication cost.

To link up the message blocks without increasing communication cost, we propose a general solution for the authenticated encryption schemes based on the discrete logarithm problem in the next section. In Section 3, by integrating our solution into Horster et al.'s scheme, we propose our first authenticated encryption scheme, Scheme 1. To remove the additional one-way function from Scheme 1, we propose Scheme 2, in Section 4. The final section states our conclusions.

2. Our general solution

In this section, we describe our general solution to link up message blocks without increasing communication cost for the authenticated encryption schemes based on the discrete logarithm problem. To link up message blocks, we ought to construct the link between any two successive message blocks, but the construction of links will increase the computation cost to encrypt (or decrypt) ciphertext blocks. To reduce the cost, we have to utilize the computed item that is also authenticated by the recipient.

To find the computed and authenticated item, we reconsider the signature equation. In an authenticated encryption scheme based on the discrete logarithm problem, the sender adopts a signature equation to generate the ciphertext block (r_i, s_i) for the ith message block. In the signature equation, there are three important items r_i, k_i, and x_A, where k_i is the secret random number selected by Sender A and x_A is the secret key of Sender A. Besides the ith message block, k_i is also authenticated by (r_i, s_i). Moreover, k_i is the function of the ith message block. Therefore, k_i is the most suitable one to construct links among message blocks.

To construct the links, our general solution is to add the secret k_{i-1} for the $(i-1)$th message block into the signature equation for the ith message block. If the original equation contains the constant item, the constant item can be removed. Then, the recipient uses (r_i, s_i) and β_{i-1} as the authentication parameters of the ith message block, where $\beta_{i-1} = y_B^{k_{i-1}} \bmod P$ and y_B is the public key of the recipient. Consequently, we have built the link between the ith and $(i-1)$th message blocks. Since β_{i-1} has been computed before the ith message block is

Table 2
The six modified signature equations to link up message blocks

Signature equation	The computation of $y_B^{k_i} \bmod P$
(1) $s_i \times k_i \equiv \boldsymbol{k_{i-1}} + r_i \times x_A \pmod{Q}$	$y_B^{k_i} = (y_B^{k_{i-1}} \times y_{AB}^{r_i})^{(s_i)^{-1}} \bmod P$
(2) $r_i \times k_i \equiv \boldsymbol{k_{i-1}} - s_i \times x_A \pmod{Q}$	$y_B^{k_i} = (y_B^{k_{i-1}} \times y_{AB}^{s_i})^{(r_i)^{-1}} \bmod P$
(3) $k_i \equiv \boldsymbol{k_{i-1}} + s_i + r_i \times x_A \pmod{Q}$	$y_B^{k_i} = y_B^{k_{i-1}} \times y_B^{s_i} \times y_{AB}^{r_i} \bmod P$
(4) $s_i \times k_i \equiv \boldsymbol{k_{i-1}} + r_i + x_A \pmod{Q}$	$y_B^{k_i} = (y_B^{k_{i-1}} \times y_B^{r_i} \times y_{AB})^{(s_i)^{-1}} \bmod P$
(5) $r_i k_i \equiv \boldsymbol{k_{i-1}} + s_i + x_A \pmod{Q}$	$y_B^{k_i} = (y_B^{k_{i-1}} \times y_B^{s_i} \times y_{AB})^{(r_i)^{-1}} \bmod P$
(6) $k_i \equiv \boldsymbol{k_{i-1}} + r_i + s_i \times x_A \pmod{Q}$	$y_B^{k_i} = (y_B^{k_{i-1}} \times y_B^{r_i} \times y_{AB}^{s_i}) \bmod P$

verified, we also reduce computation costs for the construction of links.

In Table 2, the six signature equations of Nyberg and Rupple [4] have been modified. Meanwhile Table 1 shows the original equations of Nyberg and Rupple [4]. To compare Table 2 with Table 1, we find that there is no additional computation cost for Eqs. (1) and (2). The additional computation cost for Eqs. (3)–(6) in Table 2 are all one multiplication modulo P and one addition modulo Q. The computation cost of our general solution is so small that the authenticated encryption scheme with message linkage is almost as efficient as the original one.

Since our solution links up message blocks, our method can detect which message block is missing. When some message blocks are missing, the recipient can find them and tell the sender to send the correct ones again. Comparing with the one-way hash functions, although the one-way hash function can also detect whether or not the recovered message is incomplete, it cannot point out which is the missing message block. Here the incomplete message is the message in which some information is lost. The sender must send all of the sent message blocks again. Upon detecting lost message blocks, our solution is better than the one-way hash function. Our solution also avoids paying the heavy communication cost to overcome the problem of missing message blocks.

3. A new authenticated encryption scheme

3.1. Review of Horster et al.'s scheme

We give a brief description of Horster et al.'s scheme in the following. A trusted center first publishes two large primes P and Q, where $Q|(P-1)$, the element α of order Q modulo P, and one secure one-way function $F: \mathrm{GF}(P) \to \mathrm{GF}(P)$. Each user, say A, chooses his secret key x_A and then computes his public key $y_A = \alpha^{x_A} \bmod P$.

Suppose that User A wants to transmit User B the message $m \in \mathrm{GF}(P)$ within a suitable redundancy scheme. User A first selects a random integer k from the range $[1, Q]$ and computes $r = m \times F(y_B^k)^{-1} \bmod P$. Then he constructs s satisfying the signature equation $s \equiv k - r \times x_A (\bmod Q)$. Finally, User A sends the ciphertext (r, s) to User B. User B first computes $y_B^k \equiv y_B^s \times y_{AB}^r (\bmod P)$, where the session key $y_{AB} = (y_A)^{x_B} \bmod P$. Then User B recovers $m = r \times F(y_B^k) \bmod P$ and checks if m satisfies the redundancy scheme.

The redundancy scheme has to deal with the links among the message blocks because the authenticated encryption scheme does not provide the link function. Next, the one-way function F is necessary for the encryption function; otherwise, an eavesdropper first derives the session key from $y_B^k \bmod P$ and then could recover any message block from the corresponding ciphertext block [2].

3.2. The description of our scheme

Now we present our authenticated encryption scheme, Scheme 1, which can link up the message blocks. Suppose that the parameters constructed by the trusted center and the users are the same as the ones in Horster et al.'s scheme. Suppose that User A wants to transmit the message M to User B. First, User A partitions M into t message blocks $\{m_1, m_2, \ldots, m_t\}$, where $m_i \in \mathrm{GF}(P)$ within a suitable redundancy scheme for $i = 1, 2, \ldots, t$. Here the redundancy scheme does not need to provide the function to link up message blocks. User A performs the following steps to encrypt and sign each message block.

Step 1. Select t distinct random integers $k_1, k_2, \ldots, k_t$ from the range $[1, Q]$.

Step 2. Compute $\beta_i = y_B^{k_i} \bmod P$ and $r_i = m_i \times F(\beta_i)^{-1} \bmod P$ for $i = 1, 2, \ldots, t$.

Step 3. Construct s_i satisfying the signature equation $s_i + k_{i-1} \equiv k_i - r_i \times x_A (\bmod Q)$ for $i = 1, 2, \ldots, t$, where $k_0 = 0$.

Finally, User A sends a set of ciphertext blocks $\{(r_1, s_1), (r_2, s_2), \ldots, (r_t, s_t)\}$ to User B. User B executes the following steps to recover all message blocks and checks whether the recovered message blocks are sent by User A.

Step 4. Compute $\beta_i \equiv y_B^{k_i} \equiv y_B^{k_{i-1}} \times y_B^{s_i} \times y_{AB}^{r_i} (\bmod P)$ for $i = 1, 2, \ldots, t$, where the session key $y_{AB} = (y_A)^{x_B} \bmod P$.

Step 5. Recover $m_i = r_i \times F(\beta_i) \bmod P$ and check whether m_i satisfies the redundancy scheme

for $i = 1, 2, \ldots, t$. If m_i does not satisfy the redundancy scheme, then he tells the sender to send m_i again.

Since User B obtains and verifies all message blocks, he recovers and verifies the message M. In Step 5, the recipient can also determine whether there exists missing message blocks after m_{i-1}. Theorem 1 shows the recipient has the ability to obtain the correct message block m_i from (r_i, s_i).

Theorem 1. *The message block m_i is obtained by $m_i = r_i \times F(y_B^{k_{i-1}} \times y_B^{s_i} \times y_{AB}^{r_i} \bmod P) \bmod P$ for $i = 1, 2, \ldots, t$, where $k_0 = 0$.*

Proof. First, we show that the recipient recovers the correct value β_1, where $\beta_1 = y_B^{k_1} \bmod P$. Because

$$s_1 \equiv k_1 - r_1 \times x_A - k_0 \equiv k_1 - r_1 \times x_A - 0 (\bmod Q),$$

we have

$$\beta_1 \equiv y_B^{k_1} \equiv y_B^{s_1} \times y_{AB}^{r_1} (\bmod P),$$

where $y_{AB} = (y_A)^{x_B} \bmod P$. Consequently, the recipient recovers the correct value β_i, for $i = 2, 3, \ldots, t$ by computing

$$\beta_i \equiv y_B^{k_i} \equiv y_B^{k_{i-1}} \times y_B^{s_i} \times y_{AB}^{r_i} \bmod P$$

for $i = 2, 3, \ldots, t$, since $k_i = k_{i-1} + r_i \times x_A + s_i \bmod Q$, where $\beta_i = y_B^{k_i} \bmod P$. Therefore the ith message block m_i can be obtained by

$$m_i = r_i \times F\left(y_B^{k_{i-1}} \times y_B^{s_i} \times y_{AB}^{r_i} \bmod P\right) \bmod P$$
$$= m_i \times F(\beta_i)^{-1} \times F(\beta_i) \bmod P. \quad \square$$

3.3. The security and performance considerations

Due to the following analysis, the user's secret key x, the session key between any two users, and the random integers k_i are secure. It is difficult to derive the secret key x and the random integer k_i from the public key y and r_i, respectively, because the derivations are equivalent to solving the discrete logarithm problem. The signature equations do not reveal the secret key and the random integers since the number of the unknown variables is more than the number of equations. Consequently, the session key y_{AB} between Users A and B is still secure based on the hardness of the Diffie and Hellman problem [1]. The intruder cannot derive the session key y_{AB} from β_i since β_i is also protected by the secure one-way function F.

Consider whether an intruder can forge (r_i', s_i') for $\beta_i' \equiv y_B^{k_i'} \bmod P$ and m_i'. To forge (r_1', s_1') for β_1' and m_1', (r_1', s_1') must satisfy $s_1' \equiv k_1' - r_1' \times x_A (\bmod Q)$. Since the secret key x_A is secure, the intruder cannot construct (r_1', s_1') from the $s_1' \equiv k_1' - r_1' \times x_A (\bmod Q)$. He is forced to forge (r_1', s_1') satisfying

$$\beta_1' \equiv y_B^{k_1'} \equiv y_B^{s_1'} \times y_{AB}^{r_1'} (\bmod P).$$

This work is equivalent to solving the discrete logarithm problem, so he cannot forge (r_1', s_1') for β_1' and m_1'. Now both k_1 and m_1 are authenticated and fixed after verifying the first message block m_1 since m_1 satisfies the redundancy scheme. In addition, k_1 is secret. Assume that k_{i-1} is an authenticated and secret integer after verifying the $(i-1)$th message block. If the intruder forges (r_1', s_1') for β_i' and m_i', he is faced with the same difficult work to forge (r_1', s_1'). The intruder cannot forge (r_i, s_i) for β_i and m_i.

The order of the message blocks is guaranteed by our message linkage in Scheme 1. Due to the above analysis, the intruder cannot forge (r_i, s_i) for β_i and m_i for $i = 1, 2, \ldots, t$. That is, the k_i's are authenticated by the recipient at the same time though the k_i's are secret. Consequently, the link constructed by k_i is also authenticated. Therefore, these links guarantee that the order of the message blocks is determined by the sender.

The encryption function of Scheme 1 is secure. The intruder cannot obtain β_i to decrypt the ith message block from the ciphertext block (r_i, s_i) since the session key y_{AB} is secure and secret in Scheme 1.

In Scheme 1, the Sender A performs one exponentiation modulo P and one inverse modulo P, then executes F once in Step 2. The Recipient B needs to compute two exponentiations modulo P in Step 4 and execute F once in Step 5. Comparing with the computation cost of Horster et al.'s scheme, the recipient performs one additional multiplication modulo P while the sender performs one additional

addition modulo Q. That is, the one multiplication modulo P and one addition modulo Q are the costs for integrating our general solution into Horster et al.'s scheme. Since the additional cost is small, our Scheme 1 is almost as efficient as Horster et al.'s scheme.

4. Another authenticated encryption scheme

4.1. The description of our other scheme

To remove the additional one-way functions in Scheme 1, we present another scheme, Scheme 2, which can also link up the message blocks. The parameters constructed by the trusted center and the users are the same as the ones in Scheme 1 excluding the one-way function F. Suppose that User A wants to transmit the message M to User B. User A first partitions M into a set of t message blocks $\{m_1, m_2, \ldots, m_t\}$, where $m_i \in \mathrm{GF}(P)$ within a redundancy scheme for $i = 1, 2, \ldots, t$. Replacing Step 2 in Scheme 1 by Step 2', User A executes Steps 1–3 in Scheme 1.

Step 2'. Compute

$$\beta_i = y_B^{k_i} \bmod P \text{ and } r_i = m_i \times \alpha^{-\beta_i \bmod Q} \bmod P$$

for $i = 1, 2, \ldots, t$. Then the set of ciphertexts, $\{(r_1, s_1), (r_2, s_2), \ldots, (r_t, s_t)\}$, is sent to User B. Replacing Step 5 in Scheme 1 by Step 5', User B performs Steps 4 and 5 in Scheme 1.

Step 5'. Recover

$$m_i = r_i \times \alpha^{\beta_i \bmod Q} \bmod P$$

and check whether m_i satisfies the redundancy scheme for $i = 1, 2, \ldots, t$. If m_i does not satisfy the redundancy scheme, he tells the sender to send m_i again.

Finally, User B has recovered and verified the message M. The following theorem shows why the message block m_i obtained from (r_i, s_i) is correct.

Theorem 2. *The message block m_i is recovered by*

$$m_i = r_i \times \alpha^{(y_B^{k_{i-1}} \times y_B^{s_i} \times y_{AB}^{r_i} \bmod P) \bmod Q} \bmod P$$

for $i = 1, 2, \ldots, t$, where $k_0 = 0$.

Proof. Due to the same inference for β_i in the proof of Theorem 1, we also show that the recipient recovers the correct value β_i by

$$\beta_i \equiv y_B^{k_i} \equiv y_B^{k_{i-1}} \times y_B^{s_i} \times y_{AB}^{r_i} (\bmod P)$$

for $i = 1, 2, \ldots, t$, where $\beta_i = y_B^{k_i} \bmod P$ and $k_0 = 0$. Thus the recipient recovers m_i by

$$\begin{aligned} m_i &\equiv r_i \times \alpha^{(y_B^{k_{i-1}} \times y_B^{s_i} \times y_{AB}^{r_i} \bmod P) \bmod Q} \\ &\equiv m_i \times \alpha^{-\beta_i \bmod Q} \times \alpha^{\beta_i \bmod Q} (\bmod P). \end{aligned}$$

□

4.2. The security and performance considerations

Similar to the security analysis for Scheme 1, we find that the secret key x and all the random integers k_i are secure. The session key is still secure without the one-way function F since it is also difficult to derive the session key y_{AB} from

$$r_i = m_i \times \alpha^{(y_B^{k_{i-1}} \times y_B^{s_i} \times y_{AB}^{r_i} \bmod P) \bmod Q} \bmod P.$$

Due to the similar security analysis to forge (r_i', s_i') for $\beta_i' = y_B^{k_i'} \bmod P$ and m_i' in Scheme 1, an intruder cannot forge (r_i', s_i') for the β_i' and m_i' in Scheme 2. Since the session key y_{AB} is still secure in Scheme 2, the encryption function of Scheme 2 is secure, too. In Scheme 2, the order of the message blocks is authenticated by the recipient because all the k_i's are secret and authenticated.

In Scheme 2, the sender performs two exponentiations modulo P while the recipient performs three exponentiations modulo P. The computation cost to link up message blocks is also one multiplication modulo P and one addition modulo Q. It is still small. Scheme 2 is more efficient than Hwang et al.'s scheme, since the total commutation cost of Hwang et al.'s scheme is seven exponentiations modulo P.

5. Conclusions

In this paper, we propose a general solution to link up message blocks without increasing the communication cost for the authentication encryption schemes based on the discrete logarithm problem. The computation cost to construct the link between

successive message blocks is small, so the improved authenticated encryption scheme is almost as efficient as the original one. In addition, by our solution, the recipient can determine which message blocks are lost and then tell the sender to send only these lost ones again. This also reduces the communication costs caused by the missing problem of message blocks. Adopting our solution, we propose two authenticated encryption schemes: Schemes 1 and 2. Scheme 1 still needs additional one-way functions while Scheme 2 does not. In addition, our Scheme 2 is more efficient than Hwang et al.'s scheme [2].

References

[1] W. Diffie and M.E. Hellman New directions in cryptography, *IEEE Trans. Information Theory* **22** (1976) 644–654.

[2] P. Horster, M. Michels and H. Petersen, Authenticated encryption schemes with low communication costs, *Electronics Lett.* **30** (15) (1994) 1212–1212.

[3] S.J. Hwang, C.C. Chang and W.P. Yang, An encryption/signature scheme with low message expansion, *J. Chinese Inst. Engineers* (1995).

[4] K. Nyberg and R.A. Ruppel, Message recovery for signature scheme based on the discrete logarithm problem, in: *Preproceedings Eurocrypt '94*, Perugia, Italy (1994) 175–190.