Digital Signature with Message Recovery Based on Factoring and Discrete Logarithm

Min-Shiang Hwang[1,2], Shih-Ming Chen[1] and Chi-Yu Liu[1]

(Corresponding author: Min-Shiang Hwang)

Department of Computer Science and Information Engineering, Asia University, Taiwan, ROC.[1]

Department of Medical Research, China Medical University Hospital, China Medical University[2]

(Email: mshwang@nchu.edu.tw)

June 18, 2015

Abstract

There are two applications in digital signature schemes with message recovery based on a discrete logarithm problem. One is an authenticated encryption scheme, and the other is a key agreement scheme. Considering that the cryptographic assumptions will be broken in the future, the digital signature scheme with message recovery should also be designed based on two assumptions. Besides the digital signature scheme with message recovery, the authenticated encryption scheme with message linkages should also be redesigned to deal with the problem when any one of the factoring and discrete logarithm assumptions is broken. In this paper, we propose a digital signature with message recovery based on factoring and discrete logarithm and show that the scheme is secure. In comparison with Zhang et al.'s scheme, our proposed scheme is the most efficient one in terms of communication cost and computation complexity.

Keywords: Authenticated encryption scheme, cryptography, factoring and discrete logarithm, message recovery, security.

1 Introduction

In order to prove the effectiveness of a document, before the holder of the document is delivered to his partner, he must sign the document so that he is in charge of it. Thus it can be seen that the signature is very important [11, 13, 16]. Traditionally, we use a hand-written signature to manifest the validity of a document and the identity of a signer. Nowadays, we use a digital signature instead of the traditional hand-written signature for the convenience of the transactions in the public network.

Nyberg and Rueppel [20] first proposed a digital signature scheme with message recovery based on a discrete logarithm problem. They applied their scheme in two applications where one is an authenticated encryption scheme, and the other is a key agreement scheme. In 1994, Horster et al [6] improved the authenticated encryption scheme proposed by Nyberg and Rueppel to claim their scheme was more efficient. Then Lee and Chang pointed out that the scheme proposed by Horster et al would suffer from "known-ciphertext-plaintext attack", so they proposed the other improvement [15]. Afterwards, many related schemes were proposed [1, 2, 23].

According to the previous schemes, we can conclude some requirements of a digital signature scheme with message recovery and the requirements of an authenticated encryption scheme [17, 21]. First, the digital signature scheme with message recovery must conform to three requirements such as authentication, non-repudiation, and message recovery [3, 9, 25]. But the authenticated encryption scheme should add the confidentiality, besides the above three requirements required by the digital signature scheme with message recovery.

In the past, the security of each public-key cryptosystem is based on one of two cryptographic assumptions that are discrete logarithm assumption [7] and factoring assumption. Some savants thought that if an efficient algorithm is developed in the future to break one or more of the assumptions, all of the related cryptosystem become insecure. Therefore, in 1994, Harn [4] first proposed a public-key cryptosystem based on factoring and discrete logarithm. Thereafter, there were many papers about the signature schemes based on two difficulties simultaneously [5, 12, 14, 22].

Considering that the cryptographic assumptions will be broken in the future, a digital signature scheme with message recovery should also be designed based on two assumptions. Besides the digital signature scheme with message recovery, the authenticated encryption scheme with message linkages should also be redesigned to deal with the problem where any one of the factoring and discrete logarithm assumptions is broken [10, 24]. Thus we design three schemes in this paper. The detail of the schemes is described in next section.

In the first section, we introduce the development of a message recovery scheme and its variants. In the next section, we propose three algorithms based on discrete logarithm and factoring, that are a message recovery scheme, its variants' authenticated encryption scheme, and authenticated encryption scheme with message linkage. Next, some of security is analyzed in Section 3. Then, we inspect the three schemes and their corresponding requirements, and discuss their performance in Section 4. Finally, a brief conclusion is presented in Section 5.

2 The Proposed Scheme

In this section, we propose a new signature scheme with message recovery based on factoring and discrete logarithm, the variants that are authenticated encryption scheme, and authenticated encryption scheme with message linkages. The three schemes all include the system initialization phase predefined and choose the system parameters for three participants including a trusted authority, a sender and a verifier.

First, the trusted authority chooses four large prime numbers p_1, q_1, p_2, and q_2 where $p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$ and let the parameter $p = 4p_1q_1 + 1$ a prime number. It also computes a composite variant $n = p_1q_1$ and selects an integer g which is order of p_1p_2. The trusted authority should keep the system parameter p secret, and publish n, p, g and a one-way hash function $H(\cdot)$ to all users. Each user selects his/her private key X_i in Z_n, where $\gcd(X^2, n) = 1$, and $i = \{i|A, B\}$, and then compute his/her own public key $Y_i = g^{X_i^2} \bmod p$. The notation "$\oplus$" denotes the exclusive operator, and " $\|$ " denotes concatenation operator.

2.1 Signature Scheme with Message Recovery

The scheme can be divided into two phases: signature generation, and message recovery phases. In signature generation phase, the sender A creates a signature of message M which contains redundancy with his/her private key X_A, and delivers the signature R, S to the verifier B. After receiving R, S, user B verifies the signature and recovers the message with A's public key Y_A.

- Signature Generation Phase:
  The user A should first selects a random number T in Z_n such as $\gcd(T^2, n) = 1$, and then creates the signature of the message M that he/she wants to send. Finally, he sends R, S, M to the verifier B.

$$\begin{cases} R &= Mg^{-T^2} \bmod p \\ S &= T^2 - X_i^2 H(R) \bmod n \end{cases} \tag{1}$$

- Message Recovery Phase:
  In this phase, the verifier B can use the following equation to recover the message M:

$$M = Rg^S (Y_A)^{H(R)} \bmod p.$$

  And then check the format which is published by the trusted party of the message M. If the message format is correct, the verifier accepts the message to ensure the legitimacy of the signature of the source.

The scheme allows anyone to verify the signature R, S, and know the content of the message M.

2.2 Authenticated Encryption Scheme

In message recovery schemes, there is one special application called authenticated encryption scheme. Those schemes can provide the confidentiality of a message where the plaintext is only known between the sender and the verifier. The principal concept is described in the following. The sender can use the verifier's public key Y_B to encrypt the message M, besides signing the message which is same as the mentioned signature scheme with message recovery.

- Signature Generation Phase:
  First, the sender should select a random number T in Z_n such as $\gcd(T^2, n) = 1$. Then he/she creates the ciphertext of the signature R, S of the message M as follows:

$$\begin{cases} R &= MY_B^{-T^2} \bmod p \\ S &= T^2 - X_A^2 H(R) \bmod n \end{cases} \tag{2}$$

- Message Recovery Phase:
  In this phase, the verifier can decrypt and recover the message M with his/her secret key X_B, and the sender's public key Y_A is as follows:

$$\begin{aligned} M &= R(g^S Y_A^{H(R)})^{X_B^2} \bmod p. \\ &= R(g^{S\cdot X_B^2} Y_A^{H(R)\cdot X_B^2}) \bmod p. \end{aligned} \quad (3)$$

  He/She checks whether the format of the message is correct or not, and then decides whether to accept or reject it.

2.3 Authenticated Encryption Scheme with Message Linkage

The basic authenticated encryption scheme is only applied to a smaller message. A huge message has to be divided into many message blocks first, and then be signed and encrypted. For some disadvantages of the above mentioned basic scheme, it should be noted that the message blocks have been reordered, modified, deleted or replicated during transmission. We attempt to solve the above drawbacks, so a scheme is proposed to link up each message block. There are still three phases in this scheme: the system initialization phase, signature and encryption generation phase, and message recovery and decryption phase. The first phase has been defined in the first paragraph of this section, and the other phases are described as follows.

- Signature and Encryption Generation Phase:
  Before signing and encrypting, the sender should divide the message M into n a sequence message blocks $\{M_1, M_2, \cdots, M_w\}$, where $M_i \in GF(n)$ for $i = 1, 2, \cdots, w$. Then he/she first sets an initial value $r_0 = 0$, and selects a random number T in Z_n such as $\gcd(T^2, n) = 1$. He/She obtains the ith ciphertext r_i by computing t as follows:

$$\begin{aligned} t &= Y_B^{T^2} \bmod p \quad (4) \\ r_i &= M_i H(r_{i-1} \oplus t) \bmod p. \end{aligned}$$

  In order to avoid the problems where the message blocks are deleted, reordered, or modified, the sender should compute a value R applied it to examine the completeness of the message M. Finally, he/she can generate the signature S of the message with his/her private key X_A as follows:

$$\begin{cases} R &= H(r_1 \parallel r_2 \parallel \cdots \parallel r_w) \\ S &= T^2 - X_A^2 R \bmod n \end{cases} \quad (5)$$

  After the above procedures, the sender should transmit $(n+2)$ signed and encrypted blocks $R, S, r_1, r_2, \cdots, r_w$ to the verifier B in a public way.

- Message Recovery Phase:
  After receiving those message blocks, the verifier executes the following procedure to recover and verify the message M. First, he/she calculates the verified value R' and checks whether R' is equal to R, and R is received from the sender or not:

$$\begin{cases} R' &= H(r_1 \parallel r_2 \parallel \cdots \parallel r_w) \\ R' &\stackrel{?}{=} R \end{cases} \quad (6)$$

  If the result is not equal, he rejects the message and requires the sender to retransmit those blocks. If it is equal, he/she continues the message recovering. He/She acquires the value g^{T^2} and then obtains t with g^{T^2} and his/her secret X_B:

$$\begin{aligned} g^{T^2} &= g^S Y_i^R \\ t &= (g^{T^2})^{X_B^2} \bmod p \\ &= (g^S Y_i^R)^{X_B^2} \bmod p \\ &= g^{S\cdot X_B^2} Y_i^{R\cdot X_B^2} \bmod p. \end{aligned} \quad (7)$$

  Finally, he/she recovers the ith message block M_i as follows:

$$M_i = r_i H(r_{i-1} \oplus t)^{-1} \bmod p.$$

  The verifier performs M_i until all message blocks are recovered.

3 Security Analysis

In this section, we examine whether our proposed three schemes are corresponded to security criterions or not. There are some general security requirements such as the security of a private key, the validity of a signature, the confidence of a ciphertext. Besides the above mentioned securities, we also assume that the well-known assumption such as the difficulty of discrete logarithm or factoring being broken, and our proposed scheme whether to keep the security or not.

1) An intruder impersonates the sender's signature without knowing the sender's private key.

   In the first proposed scheme, an intruder can know the signature R, S, the sender's public key Y_A and the message M. If he tries to invent the sender's signature, he can select a random number T' and a message M'. Although he can generate R' by computing $R' = M'g^{-T^2} \bmod p$, he cannot obtain S'. Because he does not know the sender's private key X_A, he cannot execute the equation $S' = T^2 - X_A^2 H(R) \bmod n$. It is not impossible that an intruder invents the sender's signature without knowing his/her private key. In the authenticated encryption scheme and the third scheme, an intruder only knows R, S and Y_A, so this scheme will face more difficulty than the first scheme.

2) The verifier forges the sender's signature without knowing the sender's private key.

   In the first scheme, the verifier can know R, S, M and Y_A, but he cannot know the sender's private key X_A. On those conditions, he cannot forge the sender's signature. The description is described as the first security attack. In the second and the third proposed scheme, the verifier holds R, S, M and the sender's public key Y_A, but he cannot create a fake signature, because he still doesn't know the sender's private key X_A.

3) An opponent reveals the sender's private key from his/her signature.

   An opponent wants to get the sender's private key from the sender's signature R and S in the message recovery scheme, he should first obtain R, S and T, and then he obtains $X_A^2 \bmod n$ by computing $X_A^2 = H(R)^{-1}(T^2 - S) \bmod n$. Since the random number T is secret, the opponent cannot get the sender's private key X_A. Even if he has the random number T, he must solve the difficulty of factoring to obtain X_A from the $X_A^2 \bmod n$. In the second scheme and the third scheme, the opponent still face the same difficulty as the first scheme.

4) An adversary derives the content of the ciphertext without knowing the verifier's secret key.

   If an adversary attempts to derive the ciphertext with the known information R, S, and M in the authenticated encryption scheme, he must know the verifier's private key X_B or the random number T. In the authenticated encryption scheme with message linkage, he can get R, S, and $r_1, r_2, \cdots, r_w$. If he wants to decrypt the ith ciphertext block, he must know the verifier's private key X_B to compute the value t. The adversary will fail to get the content of the message block.

5) An intruder reorders, modifies, deletes or replicates the message blocks.

   If an intruder wants to reorder, modify, delete or replicate any message block, he should also modify the signature S by computing Equation (5). If he cannot execute the modification, reordered, modified, deleted or replicated, message blocks will not pass the verification in Equation (6).

6) Suppose the difficulty of computing discrete logarithm problems has been broken.

   If an attacker can break the discrete logarithm problem, he knows R, S, M, and the sender's public key Y_A, so that he can derive the exponent T^2 from Equation (1). If he wants to get the sender's private key X_A from Equation (1), he must break the difficulty of factoring simultaneously. It is difficult that the attacker gets the sender's private key X_A by computing $X_A^2 = H(R)^{-1}(T^2 - S) \bmod n$ where n is composed of two large prime numbers. In the second scheme and the third scheme, the attacker also faces the same difficulty as described in the above.

7) Suppose the difficulty of computing the factoring problem has been broken.

   Assume that the attacker can break the difficulty of the factoring problem. He could obtain any inverse of any value easily. Therefore, he can undertake the calculation of Equations (1), (2), or (5) which is related to the factoring assumption. Although an attacker can solve the difficulty of factoring, he cannot still get the sender's private key X_A from the equation, because all the equations contain two unknown variables T^2, and X_A^2.

4 Requirements and Performance Analysis

4.1 Requirements Analysis

In this subsection, we mainly discuss whether our scheme achieves the requirements of signature scheme with message recovery, authenticated encryption scheme or not.

(1) Confidentiality: The property is only provided by the authenticated encryption scheme. In the authenticated encryption scheme, only the verifier can derive the message M by calculating Equation (3) with his/her secret key X_B. In the scheme, the confidentiality of the message can be kept. In the authenticated encryption scheme with message linkages, the confidentiality is also same as above.

(2) Authentication: In signature scheme with message recovery, the recovery can verify the sender's identity with the sender's public key Y_A, and then checks the format of the message M which is pre-agreed with the sender. If the format of the message is corresponding to the rule, the verifier can authenticate the sender's identity. In the authenticated encryption scheme and authenticated encryption scheme with message linkages, the verifier can also authenticate the sender's identity with the sender's public key and the format of the message. The disparity of the signature scheme with message recovery is that the verifier must decrypt the message to verify the sender with his/her secret key X_B.

(3) Non-repudiation: The three proposed schemes are all provided with the property. The sender has his/her private key X_A, and only he/she can construct the signature R, S of the message M. As he/she created a signature, the property of the non-repudiation is in operation immediately.

(4) Message Recovery: The message can be recovered from the signature with the sender's public key. In the signature scheme with message recovery, the verifier can recover the message M by calculating Equation (2), and he/she can also verify the sender's identity. In the other two schemes, they can also achieve the requirement.

4.2 Performance Analysis

In this subsection, we will analyze the performance of our three schemes. For convenience, we should pre-define some notations: T_{mul} is the time for multiplication; T_h is the time for executing hash function; T_{exp} is the time for exponentiation with modulo p; and T_{inv} is the time for inversion modulo p. Actually, many other factors also affect the performance of an algorithm, but we only consider those T_h, T_{exp}, T_{mul}, and $Tinv$, computational heavily cost here.

Table 1: Performance analysis

	Computation Cost				Communication Cost
	T_{exp}	T_{inv}	T_h	T_{mul}	
Signature scheme with message recovery	3	1	2	7	$\|p\| + \|n\|$
Authenticated encryption scheme	3	1	2	8	$\|p\| + \|n\|$
Authenticated encryption scheme with message linkages	3	w	2w+2	2w+7	$w\|p\| + 2\|n\|$

In Table 1, there are two parts to be considered, computation cost and communication cost. The computation cost is aimed at how much time the system will spend to calculate, and the communication cost means that when the sender transmits the signature of the message M, he may send the maximum size of the information.

The three schemes can be divided into two phases, signature and ciphertext generation phase, and message recovery and verification phase. In the first scheme, the signature generation phase, the sender will perform $1T_{exp}$, $1T_{inv}$, $1T_h$, $5T_{mul}$ to achieve the processes of this phase. In the message recovery and verification phase, the verifier should perform $2T_{exp}$, $1T_h$, $2T_{mul}$ to complete the processes of this phase. The required communication cost of the scheme is $|p| + |n|$, where $|p|$ denotes the length of the prime number p, and $|n|$ denotes the length of the composite variant n.

In the second scheme, the signature and ciphertext generation phase, the sender will perform $1T_{exp}$, $1T_{inv}$, $1T_h$, $4T_{mul}$ to achieve the processes of this phase. In the message recovery and verification phase, the verifier should perform $2T_{exp}$, $1T_h$, $4T_{mul}$ to complete the processes of this phase. The required communication cost of the scheme is $|p| + |n|$ of which explanation is the same as the first scheme.

In the third scheme, if there are w message blocks, the computation cost is in the following. In the signature and ciphertext generation phase, the sender will perform $1T_{exp}$, $(w+1)T_h$, $(w+3)T_{mul}$ to achieve the processes of this phase. In the message recovery and verification phase, the verifier should perform $2T_{exp}$, wT_{inv}, $(w+1)T_h$, $(w+4)T_{mul}$ to complete the processes of this phase. In this scheme, the communication cost increases by the size of the message M. Therefore, the scheme will transmit a total of $w|p| + 2|n|$ information in a public channel.

5 Comparisons

Since the comparisons with other schemes, Li-Zhang-Wang [18] and Lv-Wang [19] schemes, had been reviewed in [26], we only compare our method with Zhang-Zhao-Ji's schemes [26] which is the newest authenticated encryption schemes (published in 2015), in terms of the length of signature, computation of signature generation, and computation of message recover and verification.

There are two schemes in [26]: Authenticated encryption scheme (AES) and authentication encryption scheme with message linkage (AES-ML). We are briefly reviewed below.

We first review Zhang-Zhao-Ji's AES as follows. There are two phases in Zhang-Zhao-Ji's AES: Authenticated encryption phase, and message recover and verification phase. In authenticated encryption phase, the signer generates the signature (r, s, v) as follows:

$$r = g^{-k} t_V^k \bmod p \tag{8}$$

$$s = k - h(r, M) x_S \bmod q \tag{9}$$

$$v = M \cdot (y_{V_1} y_{V_2})^k \bmod p. \tag{10}$$

Here, x_S (x_V) denotes the sender's (verifier's) private key; $y_{V_1} = g^{x_V} \bmod p$ denotes the verifier's public key; $y_{V_2} = g^{x_V^2} \bmod p$; M denotes a message; k denotes a random number.

In the message recover and verification phase, the verifier generates the message M' and verifies the signature (r, s, v) as follows:

$$M' = v \cdot r^{-x_V} \tag{11}$$

$$r \stackrel{?}{=} (g^s y_S^{h(r,M')})^{x_V - 1} \bmod p. \tag{12}$$

Here, y_S is the sender's public key. Table 2 shows the comparisons of Zhang-Zhao-Ji's AES and the proposed AES scheme in Section 2.2. In Table 2, there are three parts to be considered, length of signature, computation of signature generation, computation of message recover and verification. The length of signature or communication cost is the maximum size of the information will been transmitted by a sender. The computation of signature generation is aimed at how much time the system will spend to generate a digital signature for a message M. And the computation of message recover and verification is the computing time for message recover and verification.

Table 2: Comparisons of Zhang-Zhao-Ji's AES and the proposed AES scheme

	Zhang-Zhao-Ji's AES	The proposed AES
Length of signature	$2\|q\| + \|p\|$ (i.e., 3072 bits)	$\|n\| + \|p\|$ (i.e., 2048 bits)
Computation of signature generation	$3T_{exp}$	$1T_{exp}$
Computation of message recover and verification	$3T_{exp}$	$2T_{exp}$

The length of signature of Zhang-Zhao-Ji's AES is $2|q| + |p|$. The sender needs to send the signature (r, s, v) to verifier. The lengths of (r, s, v) are $|p|$, $|q|$, $|p|$, respectively. For security sake, the lengths of $|p|$ and $|q|$ are 1024 bits. Therefore, the total length of signature of Zhang-Zhao-Ji's AES is 3072 bits. The length of the proposed AES is $|n|+|p|$. The sender needs to send the signature (R, S) to verifier (see the Signature Generation Phase in Section 2.2). The lengths of (R, S) are $|p|$, $|n|$, respectively. For security sake, the lengths of $|n|$ and $|p|$ are 1024 bits. Therefore, the total length of signature of the proposed AES is 2048 bits.

The computation cost of Zhang-Zhao-Ji's AES [26] and the proposed AES schemes can be divided into two phases, signature generation phase, and message recovery and verification phase. We can ignore multiplication, hash function, inversion, and exclusion (XOR) operations since the exponentiation operation spends more than these operations 1000 times. In Table 2, T_{exp} denotes the time for exponentiation operation. In the signature generation phase of

Zhang-Zhao-Ji's AES, the sender will perform $3T_{exp}$, two T_{exp}s for Equation (8) and one T_{exp} for Equation (10), to achieve the processes of this phase. In the signature generation phase of the proposed AES, the sender will perform one T_{exp} for Equation (2) to achieve the processes of this phase. The T^2 and X_A^2 in Equation (2) is only required 2 multiplications but not exponentiation operation.

In the message recovery and verification phase, the verifier should perform $3T_{exp}$, one T_{exp} for Equation (11) and two T_{exp}s for Equation (12), to complete the processes of this phase. In the message recovery and verification phase of the proposed AES, the verifier should perform $2T_{exp}$ for Equation (3), one for $g^{SX_B^2}$ and one for $Y_A^{H(R)X_B^2}$ in Equation (3), to complete the processes of this phase.

Next, we review Zhang-Zhao-Ji's AES with message linkage (AES-ML) as follows. There are also two phases in Zhang-Zhao-Ji's AES-ML: Authenticated encryption phase, and message recover and verification phase. In authenticated encryption phase, the signer generates the signature $(r, r_1, r_2, \cdots, r_w, s, v)$ as follows:

$$r_i = M_i \cdot f(r_{i-1} \oplus M_{i-1} \oplus (y_{V_1} y_{V_2})^k) \quad \text{for } i = 1, 2, \cdots, w \tag{13}$$
$$r = g^{-k} t_{R_1}^k \bmod p \tag{14}$$
$$s = k - h(r||r_1||r_2|| \cdots ||r_w, M) x_S \bmod q \tag{15}$$
$$v = M_1 \cdot (y_{V_1} y_{V_2})^k \bmod p. \tag{16}$$

Here, M denotes a message; M_1 is the first block of M; f is a one-way function. Other symbols are the same as in the Zhang-Zhao-Ji's AES and the proposed scheme.

In the message recover and verification phase, the verifier generates the message M' and verifies the signature $r, r_1, r_2, \cdots, r_w, s, v$ as follows:

$$M_1' = v \cdot r^{-x_V} \tag{17}$$
$$M_i' = r_i \cdot f(r_{i-1} \oplus M_{i-1} \oplus (y_{V_1} y_{V_2})^k)^{-1} \quad \text{for } i = 1, 2, \cdots, w \tag{18}$$
$$r \stackrel{?}{=} (g^s y_S^{h(r,M')})^{x_V - 1} \bmod p. \tag{19}$$

Table 3 shows the comparisons of Zhang-Zhao-Ji's AES with message linkage and the proposed AES with message linkage scheme in Section 2.3. In Table 3, there are also three parts to be considered, length of signature, computation of signature generation, computation of message recover and verification.

Table 3: Comparisons of Zhang-Zhao-Ji's AES with message linkage and the proposed scheme

	Zhang-Zhao-Ji's AES-ML	The proposed AES-ML Scheme
Length of signature	$3072 + 164Bw$	$1188 + 1024w$
Computation of signature generation	$4T_{exp}$	$1T_{exp}$
Computation of message recover and verification	$4T_{exp}$	$2T_{exp}$

The length of signature of Zhang-Zhao-Ji's AES-ML is $3072 + 164Bw$. The sender needs to send the signature $(r, r_1, r_2, \cdots, r_w, s, v)$ to verifier. The length of (r, s, v) is the same as in Table 2. The length of r_i is $|f| \times |M_i|$. $|f|$ denotes the length of the one way function f; $|M_i|$ denotes the length of the ith block of message M. Here, we use B to replace M_i as the length of a block. For SHA-1, the length of $|f|$ is 164 bits [8]. Therefore, the total length of signature of Zhang-Zhao-Ji's AES-ML is $3072 + 164wB$ bits. The length of the proposed AES-ML is $1188 + 1024w$. The sender needs to send the signature $(R, S, r_1, r_2, \cdots, r_w)$ to verifier (see the Signature Generation Phase in Section 2.3). The lengths of (R, S, r_i) are $|f|$, $|n|$, $|p|$, respectively. Therefore, the total length of signature of the proposed AES-ML is $1024(w + 1) + 164$ bits. In general, the length of a block is 1024 bits. Obviously, the proposed AES with message linkage is less than that of Zhang-Zhao-Ji's AES-ML scheme.

In the signature generation phase of Zhang-Zhao-Ji's AES-ML, the sender will perform $4T_{exp}$, one T_{exp} for Equation (13), two T_{exp}s for Equation (14), and one T_{exp} for Equation (16), to achieve the processes of this phase. In the signature generation phase of the proposed AES-ML, the sender will perform one T_{exp} for Equation (4) to achieve the processes of this phase.

In the message recovery and verification phase of Zhang-Zhao-Ji's AES-ML, the verifier should perform $4T_{exp}$, one T_{exp} for Equation (17), one T_{exp} for Equation (18), and two T_{exp}s for Equation (19), to complete the processes of this phase. In the message recovery and verification phase of the proposed AES-ML, the verifier should perform $2T_{exp}$ for Equation (7) to complete the processes of this phase.

From Tables 2 and 3, our proposed scheme is the most efficient than Zhang-Zhao-Ji's schemes in terms of communication cost and computation complexity.

6 Conclusions

In this article, we have introduced the development and the requirements of a digital signature scheme with message recovery scheme. In order to avoid the difficulty that the factoring or the discrete logarithm is broken one day, we have designed three schemes based on two difficulties of factoring and discrete logarithm simultaneously, which is suitable for the different requirement. If one of the two difficulties has been broken, the security of the schemes can be kept with the other of the two difficulties.

The signature scheme with message recovery can be applied to an electronic written acknowledgement for a debt where the size of the message content is smaller. The authenticated encryption scheme can be applied to the key agreement or other applications. The last scheme can be applied where the higher confidentiality and huge message are required. And we also have analyzed the security of the three schemes to avoid the sender's and the verifier's private keys from being obtained by an attacker.

Acknowledgments

This study was supported by the Ministry of Science and Technology, Taiwan (ROC) under grant MOST103-2221-E-468-026, MOST103-2622-E-468-001-CC2, and MOST103-2622-H-468-001-CC2.

References

[1] Ting-Yi Chang, Chou-Chen Yang, and Min-Shiang Hwang, "Cryptanalysis of publicly verifiable authenticated encryption," *IEICE Transactions on Foundations*, vol. E87-A, no. 6, pp. 1645–1646, 2004.

[2] M. Changshe and C. Kefei, "Publicly verifiable authenticated encryption," *Electronics Letters*, vol. 39, no. 3, pp. 281–282, 2003.

[3] L. Hernández Encinas, A. Martín del Rey, and J. Muñoz Masqué, "A weakness in authenticated encryption schemes based on Tseng et al.'s schemes," *International Journal of Network Security*, vol. 7, no. 2, pp. 157–159, 2008.

[4] L. Harn, "Public-key cryptosystem design based on factoring and discrete logarithms," *IEE Proceedings - Computers and Digital Techniques*, vol. 141, no. 3, pp. 193–195, 1994.

[5] Wei-Hua He, "Digital signature scheme based on factoring and discrete logarithms," *IEE Electronics Letters*, vol. 37, no. 4, pp. 220–222, 2001.

[6] P. Horster, M. Michels, and H. Petersen, "Authenticated encryption schemes with low communication costs," *Electronics Letters*, vol. 30, no. 15, pp. 1212–1213, 1994.

[7] Min-Shiang Hwang, Chin-Chen Chang, 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.

[8] Min-Shiang Hwang and Iuon-Chung, *Introduction to Information and Network Security, 5th Ed.*, McGraw-Hill, 2015.

[9] 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.

[10] Min-Shiang Hwang, Jung-Wen Lo, Shu-Yin Hsiao, "Improvement of Authenticated Encryption Schemes with Message Linkages for Message Flows," *IEICE Transactions on Information and Systems*, vol. E89-D, no. 4, pp. 1575–1577, 2006.

[11] Min-Shiang Hwang, Shiang-Feng Tzeng, and Shu-Fen Chiou, "A non-repudiable multi-proxy multi-signature scheme," *Innovative Computing, Information and Control Express Letters*, vol. 3, no. 3, pp. 259–264, 2009.

[12] Min-Shiang Hwang, Chao-Chen Yang, and Shiang-Feng Tzeng, "Improved digital signature scheme based on factoring and discrete logarithms," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 5, no. 2, pp. 151–155, 2002.

[13] Cheng-Chi Lee, Tzu-Chun Lin, Shiang-Feng Tzeng, and Min-Shiang Hwang, "Generalization of proxy signature based on factorization," *International Journal of Innovative Computing, Information and Control*, vol. 7, no. 3, pp. 1039–1054, 2011.

[14] N. Y. Lee, "Security of Shao's signature schemes based on factoring and discrete logarithms," *IEE Proceedings - Computers and Digital Techniques*, vol. 146, no. 2, pp. 119–121, 1999.

[15] Wei-Bin Lee and Chin-Chen Chang, "Authenticated encryption scheme without using a one way function," *Electronics Letters*, vol. 31, no. 19, pp. 1656–1657, 1995.

[16] Chun-Ta Li, Min-Shiang Hwang, and Shih-Ming Chen, "A batch verifying and detecting the illegal signatures," *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 12, pp. 5311–5320, 2010.

[17] Xiangxue Li, Dong Zheng, and Kefei Chen, "LFSR-based signatures with message recovery," *International Journal of Network Security*, vol. 4, no. 3, pp. 266–270, 2007.

[18] Y. Li, J. Zhang, Y. Wang, "Improvement for forward-secure authenticated encryption scheme," *Journal of Southest University*, vol. 37, pp. 20–23, 2010.
[19] J. Lv, X. Wang, "Practical convertible encryption scheme using self-certified public keys," *Applied Mathematic Computation*, vol. 1699, no. 2, pp. 1285–1297, 2005.
[20] K. Nyberg and R. A.Rueppel, "A new signature scheme based on the dsa giving message recovery," in *ACM Computer & Communications Security*, vol. 1, pp. 58–61, 1993.
[21] R. Rajaram Ramasamy and M. Amutha Prabakar, "Digital signature scheme with message recovery using knapsack-based ECC," *International Journal of Network Security*, vol. 12, no. 1, pp. 7–12, 2011.
[22] Z. Shao, "Signature schemes based on factoring and discrete logarithms," *CIEE Proceedings - Computers and Digital Techniques*, vol. 145, no. 1, pp. 33–36, 1998.
[23] Shiang-Feng Tzeng and Min-Shiang Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem," *Computer Standards & Interface*, vol. 26, no. 2, pp. 61–71, 2004.
[24] Shiang-Feng Tzeng, Yuan-Liang Tang, Min-Shiang Hwang, "A New Convertible Authenticated Encryption Scheme with Message Linkages," *Computers and Electrical Engineering*, vol. 33, no. 2, pp. 133–138, 2007.
[25] Eun-Jun Yoon and Kee-Young Yoo, "On the security of signature scheme with message recovery and its application," *International Journal of Network Security*, vol. 3, no. 2, pp. 151–154, 2006.
[26] Jianhong Zhang, Xubing Zhao, Cheng Ji, "A novel authenticated encryption scheme and its extension," *Information Sciences*, vol. 317, pp. 196–201, 2015.