Digital Signature with Message Recovery and Its Variants Based on Elliptic Curve Discrete Logarithm Problem *

Yuan-Liang Tang[‡] Shiang-Feng Tzeng[‡] Min-Shiang Hwang[†]

Graduate Institute of Networking and Communication Engineering[†]
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Email: mshwang@mail.cyut.edu.tw
Fax: 886-4-23742337

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

April 4, 2003

*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

Digital Signature with Message Recovery and Its Variants Based on Elliptic Curve Discrete Logarithm Problem

Abstract

In this article, we shall adopt the concepts of elliptic curve cryptosystems and self-certified public keys to build a novel digital signature scheme with message recovery. The public key and the identity of the user can be authenticated simultaneously in recovering the message. In addition, we shall also present three extended digital signature schemes based on the proposed scheme. The first is an authenticated encryption scheme that only allows a designated verifier to retrieve and verify the message. The second is an authenticated encryption scheme with message linkages used to deliver a large message. And the third is for in message flows. The authenticated encryption scheme with message linkages for message flows allows the verifier to recover partial message blocks before obtaining the whole signature. Some possible attacks will be considered, and our security analysis will show that none of them can successfully break any of the proposed schemes.

Keywords: Authenticated encryption, cryptography, digital signature, message recovery, self-certified public key.

1 Introduction

Most digital signature schemes currently available are based on well-known public key systems, such as the RSA system [4, 6, 11, 22] and the ElGamal system [7, 10]. Moreover, using digital signature schemes with message recovery is more important for many small message applications. The aim of the digital signature scheme with message recovery is to enable the signer to send only a signature for a message to the verifier. After receiving the signature, the verifier can recover and verify the message from the signature.

In general, the existed digital signature schemes with message recovery are classified into two types: RSA-based schemes and discrete logarithm-based schemes (include elliptic curve-based schemes). PSS-R [2] and ISO/IEC 9796-2 are RSA-based, and the Nyberg-Rueppel [19, 20, 21], ISO/IEC 9796-3, 9796-4 and Miyaji [17] are signature schemes with message recovery based on discrete logarithms.

In 1994, Horster et al. [9] presented an authenticated encryption scheme which is a modified version of Nybery and Rueppel's scheme. In this scheme, only the designated verifier can retrieve and verify a message from the received signature. Hence, the scheme can be regarded as a combination of the data encryption scheme and the digital signature scheme. The scheme requires a smaller bandwidth for data communications to achieve privacy, integrity and authentication of information.

For the message to be recovered from the signature, the length of message is not reduced by the hash function. Usually, the content of the message is so large that the message has to be divided into many message blocks. Therefore, each message block contains some redundancy so that the message blocks can be correctly linked together. But these processes raise communication cost. Without increasing communication cost, Hwang et al. [12] proposed an authenticated encryption scheme with message linkages based on Horster et al.'s scheme. Since then, several efficient authenticated encryption schemes have been proposed [1, 14, 26] to improve the performance.

In all the schemes mentioned above, the message blocks can be recovered only after all the signature blocks have been received. Tseng et al. [24] proposed a novel scheme for message flows that allows the verifier to recover some of the message blocks before receiving the whole signature. That is, the verifier can carry out the receiving and the recovering processes simultaneously.

In 1991, Girault [8] first presented the concept of self-certified public keys. A public key is obtained from the signature of the user's private key with her/his identity signed by a system authority. The public key of each user does not need to be accompanied by a separate certificate to be authenticated by other users. The proof of the public key can implicitly be completed with the signature verification. Therefore, the storage space and computations normally required can been reduced by using self-certified public keys. Besides, the system authority does not know the user's private key, which is chosen by the user. Since 1991, many digital signature schemes using self-certified public keys have been proposed and discussed [5, 23, 25].

In the mid-1980s, Miller [16] and Koblitz [13] introduced elliptic curves into cryptography. Since that time, elliptic curves have played a more and more important role in many cryptographic situations. The security of the elliptic curves cryptography (ECC) rests on the difficulty of the elliptic curve discrete logarithm problem (ECDLP). Among existing signature schemes, ECC provides greater efficiency than both integer factorization systems and discrete logarithm systems, including key sizes and bandwidth for schemes of relative security [3, 15]. For reducing the size of messages, one of the appropriate signature schemes with message recovery is elliptic curve-based. Up to now, however, there exists no elliptic curve-based signature scheme with message recovery using self-certified public keys.

In this paper, we first propose a new digital signature scheme with message recovery using self-certified public keys based on ECDLP. After that, we present three kinds of applications based on the proposed digital signature scheme with message recovery. The public key of the proposed schemes is cooperatively determined by system authority and user. It is computationally infeasible for the system authority to calculate the private key of the user.

Both the public key and the identity of the user can be authenticated when recovering the message.

In the next section, the authors shall present a novel digital signature scheme with message recovery using self-certified public keys based on ECDLP. After that, we shall show several extended digital signature schemes from the proposed digital signature scheme with message recovery. The security analysis of the proposed schemes will be discussed in section 4. Finally, a summary will be given in the last section.

2 Digital Signature Scheme with Message Recovery

In this section, we shall propose a novel digital signature scheme with message recovery which uses the concept of self-certified public keys. The proposed scheme is composed of three phases: the system initialization phase, the signature generation phase, and the message recovery phase.

System Initialization Phase:

In the system initialization phase, a trusted system authority (SA) is responsible for creating the system parameters. First, SA selects an elliptic curve E defined over Z_p where p is a prime. Let $G \in E(Z_p)$ be a base point of order n which is a prime. The elliptic curve E, the primes p and n, and the point G are made public. SA randomly selects an integer $a \in [1, n-1]$ and calculates $b = aG$, where a is kept secret and b is published. SA also publishes a one-way hash function $h(\cdot)$ with collision resistance, such as SHA-1 [18].

When a user U_i with identity ID_i wants to join the system, U_i selects a random integer $c_i \in [1, n-1]$ and calculates $d_i = c_i G$. Then U_i sends (d_i, ID_i) to SA for registration. After receiving (d_i, ID_i), SA selects a random integer $k_i \in [1, n-1]$, computes the public key for U_i as $y_i = k_i G + d_i$, and finds s_i in

user		system authority
select a random integer $c_i \in [1, n-1]$		
$d_i = c_i G$		
	$\xrightarrow{(d_i, ID_i)}$	
		select a random integer $k_i \in [1, n-1]$
		$y_i = k_i G + d_i$
		$s_i = k_i + ((y_i)_x + ID_i)a \bmod n$
	$\xleftarrow{(y_i, ID_i, s_i)}$	
$x_i = s_i + c_i \bmod n$		
check $x_i G = y_i + ((y_i)_x + ID_i)b$		

Figure 1: The System Initialization Phase

the following equation:

$$s_i = k_i + ((y_i)_x + ID_i)a \bmod n,$$

where $(\cdot)_x$ denotes the x-coordinate of the point $(\cdot)$ on E. Then SA returns (y_i, ID_i, s_i) to U_i, who calculates her/his private key as $x_i = s_i + c_i \bmod n$. Later on, U_i can verify the correctness of y_i by checking that

$$x_i G = y_i + ((y_i)_x + ID_i)b. \tag{1}$$

The flow chart for the system initialization phase is illustrated in Figure 1.

Signature Generation Phase:

Suppose that a signer U_a wants to sign a message M. The signature generation process is as follows. U_a first selects a random integer $k \in [1, n-1]$. Then U_a calculates the signature (r, s) for message M as follows:

$$r = M + (kG)_x \bmod n, \tag{2}$$

$$s = k - h(r)x_a \bmod n, \tag{3}$$

Finally, U_a delivers the digital signature (r, s) to the verifier.

Message Recovery Phase:

After receiving the digital signature (r, s), any verifier can use U_a's public key y_a and identity ID_a to recover message M as follows:

$$M = r - (sG + h(r)(y_a + ((y_a)_x + ID_a)b))_x \bmod n. \tag{4}$$

The flow chart of the signature generation phase and message recovery phase is illustrated in Figure 2.

signer		verifier
select a random integer $k \in [1, n-1]$		
$r = M + (kG)_x \bmod n$		
$s = k - h(r)x_a \bmod n$	$\xrightarrow{(r,s)}$	
		$M = r - (sG + h(r)(y_a + ((y_a)_x + ID_a)b))_x \bmod n$

Figure 2: Digital Signature Scheme with Message Recovery

By proving the following theorem, we can prove that the proposed scheme works correctly.

Theorem 2.1 *The message M can be recovered correctly from the digital signature (r, s) through Equation (4).*

Proof. From Equation (3), we have $k = s + h(r)x_a \bmod n$. Raising both sides of the above equation by multiplying them by the base point G, we have

$$\begin{aligned} kG &= (s + h(r)x_a)G, \\ &= sG + h(r)x_aG, \end{aligned}$$

From Equation (1), we can rewrite the above equation as

$$kG = sG + h(r)(y_a + ((y_a)_x + ID_a)b). \tag{5}$$

According to Equation (2) and (5), the message M can be obtained by calculating

$$\begin{aligned} M &= r - (kG)_x, \\ &= r - (sG + h(r)(y_a + ((y_a)_x + ID_a)b))_x \bmod n. \end{aligned}$$

This theorem is thus proven. By the above theorem, we see that the proposed scheme is workable. *QED.*

3 The Extended Digital Signature Schemes

In this section, we shall present three extended digital signature schemes from the proposed scheme in the preceding section. First, there is an authenticated encryption scheme that only allows a designated verifier to retrieve and confirm the message. The other two schemes are suitable for a large message such that the message has to be divided into a sequence of message blocks with each message block being encrypted and signed as a signature block individually. One of the two schemes uses an authenticated encryption scheme with message linkages as a basic scheme, in which only a random integer is used so that the communication cost is low. The other uses an authenticated encryption scheme with message linkages for message flows as a generalized scheme. The generalized scheme allows the designated verifier to retrieve individual blocks and use them before the whole signature has been derived.

Each of the extended digital signature schemes is also composed of three phases: the system initialization phase, the signature generation phase, and the message recovery phase. The system initialization phase is the same as that of the scheme in the preceding section. Therefore, we only describe the other two phases.

3.1 Authenticated Encryption Scheme

In this subsection, we shall present an authenticated encryption scheme that is a combination of the data encryption scheme and the digital signature scheme. In other words, the signer can create a digital signature for a message M and then deliver it to a designated verifier. Upon receiving the digital signature, only the designated verifier U_b can retrieve and verify the message M. The other verifiers are unable to do it. The flow chart of the authenticated encryption scheme is illustrated in Figure 3. Details of the signature generation phase and the message recovery phase are described as follows.

Signature Generation Phase:

Assume that U_a wants to create a signature for message M and send it to U_b. The signature generating procedure is stated as follows. First, U_a selects a random integer $k \in [1, n-1]$. Then U_a calculates the digital signature (r, s) for message M, where

$$r = M + (k(y_b + ((y_b)_x + ID_b)b))_x \bmod n, \quad (6)$$

$$s = k - h(r)x_a \bmod n. \quad (7)$$

Finally, U_a delivers the digital signature (r, s) to U_b.

Message Recovery Phase:

After receiving the digital signature (r, s), U_b can recover the message M by using her/his private key x_b and the public values y_a and ID_a as follows:

$$M = r - ((sG + h(r)(y_a + ((y_a)_x + ID_a)b))x_b)_x \bmod n. \quad (8)$$

By checking the following theorem, we will prove the correctness of this scheme.

Theorem 3.1 *The designated verifier U_b can correctly recover the message M from the digital signature (r, s) by Equation (8).*

signer (U_a)		verifier (U_b)
select a random integer $k \in [1, n-1]$		
$r = M + (k(y_b + ((y_b)_x + ID_b)b))_x \bmod n$		
$s = k - h(r)x_a \bmod n$	$\xrightarrow{(r,s)}$	
		$M = r - ((sG + h(r)(y_a + ((y_a)_x + ID_a)b))x_b)_x \bmod n$

Figure 3: Authenticated Encryption Scheme

Proof. For Equation (7), we have $k = s + h(r)x_a \bmod n$. Raising both sides of the above equation by multiplying them by the base point G, we have

$$\begin{aligned} kG &= (s + h(r)x_a)G, \\ &= sG + h(r)x_aG. \end{aligned}$$

From Equation (1), we can rewrite the above equation as

$$kG = sG + h(r)(y_a + ((y_a)_x + ID_a)b).$$

Only U_b has the private key x_b. Thus, she/he can calculate

$$\begin{aligned} k(y_b + ((y_b)_x + ID_b)b) &= k \cdot x_bG, \\ &= kG \cdot x_b, \\ &= (sG + h(r)(y_a + ((y_a)_x + ID_a)b))x_b. \end{aligned} \tag{9}$$

According to Equation (6) and (9), the message M can be derived by calculating

$$\begin{aligned} M &= r - (k(y_b + ((y_b)_x + ID_b)b))_x, \\ &= r - ((sG + h(r)(y_a + ((y_a)_x + ID_a)b))x_b)_x \bmod n. \end{aligned}$$

This theorem is thus proven. *QED.*

3.2 Authenticated Encryption Scheme with Message Linkages

Assume that the message is huge and therefore has to be divided into a sequence of message blocks. In this subsection, the proposed scheme can link up the message blocks without increasing the communication cost. Furthermore, the verifier can know whether the message blocks have been reordered, modified, deleted or replicated. The flow chart for the authenticated encryption scheme with message linkages is illustrated in Figure 4. Details in the signature generation phase and the message recovery phase are as follows.

Signature Generation Phase:

Without loss of generality, assume that U_a desires to create a signature for message M that is to be sent to U_b. The message is composed of the sequence $\{M_1, M_2, \cdots, M_n\}$, where $M_i \in E(Z_p)$ for $i = 1, 2, \cdots, n$. U_a fulfills the following steps to generate the signature blocks for the message M.

1. Make $r_0 = 0$ and select a random integer $k \in [1, n-1]$.

2. Calculate

$$r_i = M_i + h(r_{i-1} \oplus (k(y_b + ((y_b)_x + ID_b)b))_x) \bmod n, \tag{10}$$

for $i = 1, 2, \cdots, n$, where " $\oplus$ " denotes the exclusive-or operator.

3. Calculate

$$s = k - r x_a \bmod n, \tag{11}$$

where $r = h(r_1 || r_2 || \cdots || r_n)$, "$||$" denotes the concatenation operator.

U_a delivers the signature blocks $(r, s, r_1, r_2, \cdots, r_n)$ to U_b via a public channel. Note that r_i is used as a linking parameter between the ith and $(i+1)$th message block.

Message Recovery Phase:

After receiving the signature blocks $(r, s, r_1, r_2, \cdots, r_n)$, U_b can retrieve the message blocks $\{M_1, M_2, \cdots, M_n\}$ by the following steps.

1. Calculate $r' = h(r_1||r_2||\cdots||r_n)$ and confirm that $r' = r$ is true.

2. Recover the message blocks $\{M_1, M_2, \cdots, M_n\}$ as follows:

$$M_i = r_i - h(r_{i-1} \oplus ((sG + r(y_a + ((y_a)_x + ID_a)b))x_b)_x) \bmod n, \quad (12)$$

   for $i = 1, 2, \cdots, n$ and $r_0 = 0$.

signer (U_a)		verifier (U_b)
make $r_0 = 0$		
select a random integer $k \in [1, n-1]$		
$r_i = M_i + h(r_{i-1} \oplus (k(y_b + ((y_b)_x +$ $ID_b)b))_x) \bmod n$		
$r = h(r_1\|\|r_2\|\|\cdots\|\|r_n)$		
$s = k - rx_a \bmod n$		
	$\xrightarrow{(r, s, r_1, r_2, \cdots, r_n)}$	
		$r' = h(r_1\|\|r_2\|\|\cdots\|\|r_n)$
		confirm $r' = r$
		$M_i = r_i - h(r_{i-1} \oplus ((sG + r(y_a+$ $((y_a)_x + ID_a)b))x_b)_x) \bmod n$

Figure 4: Authenticated Encryption Scheme with Message Linkages

Let's prove that the proposed scheme works correctly by proving the following theorem.

Theorem 3.2 *In the message recovery phase, the designated verifier U_b can recover the message blocks $\{M_1, M_2, \cdots, M_n\}$ by using Equation (12).*

Proof. From Equation (11), we have $k = s + rx_a \bmod n$. Raising both sides of the above equation by multiplying them by the base point G, we have

$$\begin{aligned} kG &= (s + rx_a)G, \\ &= sG + rx_aG. \end{aligned}$$

From Equation (1), we can rewrite the above equation as

$$kG = sG + r(y_a + ((y_a)_x + ID_a)b).$$

Only U_b has the private key y_b. Thus, she/he can calculate

$$\begin{aligned} k(y_b + ((y_b)_x + ID_b)b) &= k \cdot x_bG, \\ &= kG \cdot x_b, \\ &= (sG + r(y_a + ((y_a)_x + ID_a)b))x_b. \end{aligned} \tag{13}$$

According to Equation (10) and (13), the message M_i can be achieved by computing

$$\begin{aligned} M_i &= r_i - h(r_{i-1} \oplus (k(y_b + ((y_b)_x + ID_b)b))_x), \\ &= r_i - h(r_{i-1} \oplus ((sG + r(y_a + ((y_a)_x + ID_a)b))x_b)_x \bmod n. \end{aligned}$$

Therefore, U_b can get the message M. This theorem is thus proven. QED.

3.3 Authenticated Encryption Scheme with Message Linkages for Message Flows

The scheme to be proposed in this subsection is similar to that in Subsection 3.2. The scheme allows the verifier to retrieve individual blocks and use them before all the signature blocks are obtained. Therefore, this authenticated encryption scheme with message linkages is applicable to message flows. The flow chart of the authenticated encryption scheme with message linkages for message flows is illustrated in Figure 5. The signature generation phase and message recovery phase are described as follows.

Signature Generation Phase:

Assume that U_a wants to deliver a message M to U_b. The message M could be a large document or message flow. Assume the message M is a sequence $\{M_1, M_2, \cdots, M_n\}$, where $M_i \in E(Z_p)$. Let t blocks form a segment. Thus, the message M consists of $\lceil n/t \rceil$ segments. That is, a segment contains t sequential message blocks $\{M_{i1}, M_{i2}, \cdots, M_{it}\} \subset \{M_1, M_2, \cdots, M_n\}$. Then U_a fulfills the following process to create the signature blocks for segment i, where $i = 1, 2, \cdots, \lceil n/t \rceil$.

1. Make $r_{i0} = r_{i-1}$ and select a random integer $k_i \in [1, n-1]$.

2. Calculate

$$r_{ij} = M_{ij} + h(r_{i(j-1)} \oplus (k_i(y_b + ((y_b)_x + ID_b)b))_x) \bmod n \tag{14}$$

   for $i = 1, 2, \cdots, t$.

3. Calculate

$$s_i = k_i - r_i x_a \bmod n, \tag{15}$$

   where $r_i = h(r_{i1}||r_{i2}||\cdots||r_{it})$ and let $r_0 = 0$.

U_a sends signature blocks $(r_i,\ s_i,\ r_{i1},\ r_{i2},\ \cdots,\ r_{it})$ to U_b for each segment i, $i = 1, 2, \cdots, \lceil n/t \rceil$. Note that r_{ij} is used as a linking parameter between the jth and $(j+1)$th message block in segment i, and r_i is used as a linking parameter between the ith and $(i+1)$th segment.

Message Recovery Phase:

After receiving the signature blocks $(r_i,\ s_i,\ r_{i1},\ r_{i2},\ \cdots,\ r_{it})$, U_b can recover the message blocks $\{M_{i1}, M_{i2}, \cdots, M_{it}\}$ by following the steps below.

1. Calculates $r'_i = h(r_{i1}||r_{i2}||\cdots||r_{it})$ and confirm that $r'_i = r_i$ is true.

2. Use her/his private key x_b and public values y_a and ID_a to recover the message blocks $\{M_{i1}, M_{i2}, \cdots, M_{it}\}$ as follows:

$$M_{ij} = r_{ij} - h(r_{i(j-1)} \oplus ((s_iG + r_i(y_a + ((y_a)_x + ID_a)b))x_b)_x) \bmod n. \quad (16)$$

signer (U_a)		verifier (U_b)
make $r_0 = 0$, $r_{i0} = r_{i-1}$		
select a random integer $k_i \in [1, n-1]$		
$r_{ij} = M_{ij} + h(r_{i(j-1)} \oplus (k_i(y_b + ((y_b)_x$ $+ID_b)b))_x) \bmod n$		
$r_i = h(r_{i1}\|\|r_{i2}\|\|\cdots\|\|r_{it})$		
$s_i = k_i - r_ix_a \bmod n$		
	$\xrightarrow{(r_i, s_i, r_{i1}, r_{i2}, \cdots, r_{it})}$	
		$r'_i = h(r_{i1}\|\|r_{i2}\|\|\cdots\|\|r_{it})$
		confirm $r'_i = r_i$
		$M_{ij} = r_{ij} - h(r_{i(j-1)} \oplus ((s_iG + r_i(y_a$ $+((y_a)_x + ID_a)b))x_b)_x) \bmod n$

Figure 5: Authenticated Encryption Scheme with Message Linkages for Message Flows

By proving the following theorem, we shall prove that the message blocks $\{M_{i1}, M_{i2}, \cdots, M_{it}\}$ can be correctly recovered and verified.

Theorem 3.3 *In the message recovery phase, the designated verifier U_b can recover the message blocks $\{M_{i1}, M_{i2}, \cdots, M_{it}\}$ by Equation (16).*

Proof. From Equation (15), we have $k_i = s_i + r_ix_a \bmod n$. Raising both sides of the above equation by multiplying them by the base point G, we have

$$\begin{aligned} k_iG &= (s_i + r_ix_a) \cdot G, \\ &= s_iG + r_ix_aG. \end{aligned}$$

From Equation (1), we can rewrite the above equation as

$$k_iG = s_iG + r_i(y_a + ((y_a)_x + ID_a)b).$$

Only U_b has the private key x_b. Thus, she/he can calculate

$$\begin{aligned} k_i(y_b + ((y_b)_x + ID_b)b) &= k_i \cdot x_bG, \\ &= k_iG \cdot x_b, \\ &= (s_iG + r_i(y_a + ((y_a)_x + ID_a)b))x_b. \end{aligned} \quad (17)$$

According to Equation (14) and (17), the message M_{ij} can be obtained by computing

$$\begin{aligned} M_{ij} &= r_{ij} - h(r_{i(j-1)} \oplus (k_i(y_b + ((y_b)_x + ID_b)b))_x), \\ &= r_{ij} - h(r_{i(j-1)} \oplus ((s_iG + r_i(y_a + ((y_a)_x + ID_a)b))x_b)_x \bmod n. \end{aligned}$$

Therefore, U_b can acquire the message $\{M_{i1}, M_{i2}, \cdots, M_{it}\}$. This theorem is thus proven. *QED.*

4 Discussions

4.1 Security Analysis

Let us discuss the security of the proposed schemes. Basically, the security of the proposed schemes is based on the difficulty of cryptographic assumptions as follows:

1. **OWHF assumption [18]:** Suppose that $h(\cdot)$ is a one-way hash function. For given arbitrary-length message m, it is easy to calculate $h(m)$. However, it is computationally infeasible to
   (a) Given an integer $h(m)$, it is difficult to find m.
   (b) Given an integer $h(m)$, it is difficult to derive another message m' such that $h(m) = h(m')$.

2. **ECDLP assumption [13, 16]:** Suppose that E is an elliptic curve. Given two points A and B on E, it is computationally infeasible to find k such that $B = kA$.

In the following paragraphs, a description of a number of attacks against the proposed schemes will be presented. Since the security of the authenticated encryption scheme with message linkages is similar to that of the authenticated encryption scheme with message linkages for message flows, we shall discuss the security of the two together. In this subsection, we shall consider some possible attacks against the proposed schemes. Attacks 1 and 2 are against all the proposed schemes. Attack 3 targets the authenticated encryption scheme. Attacks 4-6 are against the authenticated encryption scheme with message linkages for message flows. We shall prove that the proposed schemes can successfully withstand these possible attacks.

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

Analysis of attack 1: An adversary can derive $x_aG = y_a + ((y_a)_x + ID_a)b$ from Equation (1). However, it is as difficult as breaking ECDLP to obtain U_a's private key x_a. For the digital signature scheme with message recovery and the authenticated encryption scheme, the adversary can get x_a from $s = k - h(r)x_a \bmod n$. The equation has two unknown variables k and x_a. If the adversary somehow knows k from $r = M + (kG)_x \bmod n$ and $r = M + (k(y_b + ((y_b)_x + ID_b)b))_x \bmod n$, she/he still has to face the difficulty of solving ECDLP. For the authenticated encryption scheme with message linkages for message flows, the adversary can derive x_a from $s_i = k_i - r_i x_a \bmod n$ if she/he knows k_i. The adversary can use two approaches to get k_i. In the first approach, she/he must first obtain $k_i(y_b + ((y_b)_x + ID_b)b)$ from $r_{ij} = M_{ij} + h(r_{i(j-1)} \oplus (k_i(y_b + ((y_b)_x + ID_b)b))_x) \bmod n$ and then calculate

k_i from $k_i(y_b + ((y_b)_x + ID_b)b)$. However, this means she/he has to solve both the OWHF and ECDLP. In the other approach, the adversary can calculate k_i from $k_iG = s_iG + r_iy_a$, but she/he will also have to solve ECDLP.

Attack 2: An intruder, without U_a's private key x_a, attempts to forge the digital signature to impersonate U_a.

Analysis of attack 2: Suppose an intruder wants to forge a valid signature for a given message M' that can pass the verification equation. If the intruder determines r first, she/he has to obtain the value of s by solving ECDLP. On the other hand, if the intruder fixes the integer s first, she/he will have to solve the OWHF to obtain the value of r. Therefore, the verification equation is secure against a forgery attack.

Attack 3: An opponent attempts to decrypt the message M from the digital signature (r, s) without U_b's private key x_b in the authenticated encryption scheme.

Analysis of attack 3: Since an opponent does not know x_b, she/he cannot obtain the correct message M by calculating $M = r - ((sG + h(r)(y_a + ((y_a)_x + ID_a)b))x_b)_x \bmod n$. The opponent attempts to find $k(y_b + ((y_b)_x + ID_b)b) = s(y_b + ((y_b)_x + ID_b)b) + h(r)x_a(y_b + ((y_b)_x + ID_b)b)$ from $s = k - h(r)x_a \bmod n$ and then calculates $M = r - (k(y_b + ((y_b)_x + ID_b)b))_x \bmod n$. Thus, she/he must also know the private key x_a. However, to find x_a, the opponent has to solve ECDLP.

Attack 4: In the authenticated encryption scheme with message linkages for message flows, an intruder attempts to decrypt one message M_{ij} for the signature (r_i, s_i, r_{i1}, r_{i2}, $\cdots$, r_{it}) without U_b's private key x_b.

Analysis of attack 4: As with attack 3, an intruder does not know U_b's private key x_b and therefore she/he cannot obtain the correct message M_{ij} by calculating Equation (16). The intruder might attempt to find the value $k_i(y_b + ((y_b)_x + ID_b)b)$ by computing $k_i(y_b + ((y_b)_x + ID_b)b) = s_i(y_b + ((y_b)_x + ID_b)b) + r_i x_a(y_b + ((y_b)_x + ID_b)b)$ from $s_i = k_i - r_i x_a \bmod n$ and then calculate $M_{ij} = r_{ij} - h(r_{i(j-1)} \oplus (k_i(y_b + ((y_b)_x + ID_b)b))_x) \bmod n$. Thus, she/he needs to know U_a's private key x_a. As with attack 1, the intruder has to solve ECDLP.

Attack 5: If an adversary knows one message block M_{ij}, the adversary might attempt to derive the other message blocks.

Analysis of attack 5: Although she/he may obtain $h(r_{i(j-1)} \oplus (k_i(y_b + ((y_b)_x + ID_b)b))_x) = r_{ij} - M_{ij} \bmod n$, she/he cannot derive $k_i(y_b + ((y_b)_x + ID_b)b)$, which is protected by the OWHF. Thus, the proposed scheme can withstand the known plaintext attack.

Attack 6: An opponent attempts to reorder, modify, delete or replicate the message blocks.

Analysis of attack 6: If any signature block is recorded, modified, deleted or replicated, then the signature equation $s_i = k_i - r_i x_a \bmod n$ must be changed as well. Thus, those signature blocks cannot pass the verification equations because the relationship $r_i = h(r_{i1}||r_{i2}|| \cdots ||r_{it})$ will no longer exist. Therefore, the verifier will detect the changes.

4.2 Performance Evaluation

In this subsection, let's evaluate the performance of the proposed schemes. The following notations are used to analyze the computational complexity: T_{EC-MUL} is the time for multiplying a number by a point on the elliptic curve; T_{EC-ADD} is the time for the adding one point to another on the elliptic curve; T_{MUL} is the time for the multiplication with modulo n; And T_h is the time for executing the one-way hash function. Note that the time for computing addition and subtraction is ignored.

In the digital signature scheme with message recovery, the signature generation phase requires $T_{EC-MUL} + T_{MUL} + T_h$. For recovering the message, a verifier has to spend $2T_{EC-MUL} + T_{EC-ADD} + T_h$. In the authenticated encryption scheme, the signer requires $2T_{EC-MUL} + T_{EC-ADD} + T_{MUL} + T_h$ to generate the signature. And the time required by the designated verifier to recover the message is $4T_{EC-MUL} + 2T_{EC-ADD} + T_h$.

In addition, assume there is a large message to deliver. The message is divided into w message blocks. In the authenticated encryption scheme with message linkages, the set of signature blocks is $(r, s, r_1, r_2, \cdots, r_n)$. Therefore, the signer requires $2T_{EC-MUL} + T_{EC-ADD} + T_{MUL} + (w + 1)T_h$ to generate the message blocks, while verifying and retrieving the message blocks requires $4T_{EC-MUL} + 2T_{EC-ADD} + (w + 1)T_h$. In the authenticated encryption scheme with message linkages for message flows, the set of signature blocks is $(r_i, s_i, r_{i1}, r_{i2}, \cdots, r_{it})$ for each segment i, where $i = 1, 2, \cdots, \lceil n/t \rceil$. Therefore, the computational complexities for the signature generation and message recovery are $\lceil n/t \rceil (2T_{EC-MUL} + T_{EC-ADD} + T_{MUL} + (w+1)T_h)$ and $\lceil n/t \rceil (4T_{EC-MUL} + 2T_{EC-ADD} + (w + 1)T_h)$.

5 Conclusion

In this article, we presented a digital signature scheme with message recovery using self-certified public keys based on the elliptic curve discrete logarithm problem. In addition, we also proposed three extended digital schemes from the proposed digital signature scheme with message recovery. These schemes propose that the user's public key and identity can be authenticated simultaneously when recovering the message is being recovered. In the authenticated encryption scheme, the signer is able to generate a signature for a message and then transmit it to a designated verifier. Only the designated verifier can recover and verify the message. The authenticated encryption scheme with message linkages is suitable for the delivery of large messages providing the linkages among signature blocks. In order to enable the receiving procedure and the recovery process to proceed simultaneously, we have offered an authenticated encryption scheme with message linkages applicable to message flows. All the proposed schemes preserve the main merits of elliptic curve cryptography and self-certified public keys. To break our schemes is as difficult as breaking the one-way hash function and the elliptic curve discrete logarithm problem.

References

[1] Shunsuke Araki, Satoshi Uehara, and Kyoki Imamura, "The limited verifier signature and its application," *IEICE Transactions on Fundamentals*, vol. E82-A, no. 1, pp. 63–68, 1999.

[2] M. Bellare and P. Rogaway, "The exact security of digital signatures: How to sign with rsa and rabin," in *Advances in Cryptology, Eurocrypt'96*, pp. 399–416, 1996.

[3] William J. Caelli, Edward P. Dawson, and Scott A. Rea, "Pki, elliptic curve cryptography, and digital signatures," *Computers & Security*, vol. 18, no. 1, pp. 47–66, 1999.

[4] Chin-Chen Chang and Min-Shiang Hwang, "Parallel computation of the generating keys for RSA cryptosystems," *IEE Electronics Letters*, vol. 32, no. 15, pp. 1365–1366, 1996.

[5] Yun-Shihng Chang, Tzong-Chen Wu, and Shih-Chan Huang, "ElGamal-like digital signature and multisignature schemes using self-certified public keys," *The Journal of Systems and Software*, vol. 50, pp. 99–105, Feb. 2000.

[6] S. Wesley Changchien, Min-Shiang Hwang, and Kuo-Feng Hwang, "A batch verifying and detecting multiple RSA digital signatures," *International Journal of Computational and Numerical Analysis and Applications*, vol. 2, no. 3, pp. 303–307, 2002.

[7] 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.

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

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

[10] 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.

[11] Min-Shiang Hwang, Cheng-Chi Lee, and Yan-Chi Lai, "Traceability on RSA-based partially signature with low computation," *Applied Mathematics and Computation*, 2002.

[12] Shin-Jia Hwang, Chin-Chen Chang, and Wei-Pang Yang, "Authenticated encryption schemes with message lingage," *Information Processing Letters*, vol. 58, no. 4, pp. 189–194, 1996.

[13] K. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[14] 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.

[15] A. Menezes and S. Vanstone, "Elliptic curve systems," *Proposed IEEE P1363 Standard*, pp. 1–42, 1995.

[16] Victor S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology, CRYPTO'85*, pp. 417–426, Lecture Notes in Computer Science, Vol. 218, 1985.

[17] A. Miyaji, "A message recovery signature scheme equivalent to DSA over elliptic curves," in *Advances in Cryptology, Asiacrypt'96*, pp. 1–14, 1996.

[18] NITS. "Secure hash standard,". Tech. Rep. FIPS 180-1, NITS, US Department Commerce, April 1995.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] Z. Shao, "Cryptographic system using a self-certified public key based on discrete logarithms," *IEE Proceedings - Computer Digital Technology*, vol. 148, no. 6, pp. 233–237, 2001.

[24] 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.

[25] 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, no. 2-3, pp. 203–214, 2003.

[26] 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.