Authenticated Encryption Schemes: Current Status and Key Issues

Min-Shiang Hwang[1] and Chi-Yu Liu[2]
(Corresponding author: Min-Shiang Hwang)

Department of Management Information Systems, National Chung Hsing University[1],
250 Kuo Kuang Rd., Taichung, Taiwan 402, R.O.C. (Email: mshwang@nchu.edu.tw)
Graduate Institute of Networking and Communication Engineering, Chaoyang University of Technology[2],
168 Gifeng E. Rd., Wufeng Taichung County, Taiwan, R.O.C.

(Invited Paper)

Abstract

Nyberg and Ruppel first proposed a signature scheme with message recovery based on DSA in 1993, and the authenticated encryption scheme is a special application of their scheme. Afterward, there are many papers proposed about the authenticated encryption schemes. The signature scheme can reduce the transmitted cost, because the message has been contained in the signature of the message and the signer does not necessary to send the receiver the message and the signature. The scheme is very suitable for the key agreement application, because a key is a small amount of a message. In order to comprehend and interpret the authenticated encryption schemes overall, we discuss the evolution and the existed problems of authenticated encryption schemes.

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

1 Introduction

Two signature schemes have received widespread attention which are RSA signature [20] and Digital Signature Algorithm (DSA for short) [19]. In RSA signature scheme, the verifier can use two modes to verify the signer's signature. One of the mode is the text hashing method and the other is message recovery method. If the signer uses the text hashing method and transmits the signature of a message and a hash message to the verifier, the verifier can hash the received message and compares with the hash value received from the signer. Then, the verifier can ensure the correctness of the signature and the integrity of the message. If the signer uses the message recovery method, he/she should agree with the receiver on the message format in advance. Then, the verifier can also verify the correctness of the signature. DSA only provides the text hashing method to verify the signature of a message.

Nyberg and Ruppel first proposed a signature scheme with message recovery based on DSA in 1993 [17], and the authenticated encryption scheme is a special application of their scheme. Afterward, there are many papers proposed about the authenticated encryption schemes. The signature scheme can reduce the transmitted cost, because the message has been contained in the signature of the message and the signer does not necessary to send the receiver the message and the signature. The scheme is very suitable for the key agreement application, because a key is a small amount of a message. In order to comprehend and interpret the authenticated encryption schemes overall, we discuss the evolution and the exited problems of authenticated encryption schemes.

1.1 Briefly Review

In 1993, Nyberg and Rueppel [17] proposed a signature with message recover based on the discrete logarithm problem. In this scheme, there are some advantages which the application without a hash function is possible to be achieved, such as smaller bandwidth for signatures of small messages , and direct use in other schemes like identity-based public key systems or key agreement protocols. In 1994, Horster, Michels, and Petersen [5] (HMPs for short) proposed an authenticated encryption scheme based on message recover method which is the modification of Nyberg-Rupple's scheme [17]. In their scheme, a sender does not to have to transmit a message to the receiver. Then, the receiver not only could verify the message authentication and the message integrity, but he/she could also get the original message from the information that he/she has received. Although HMPs provided the confidentiality, this scheme was not secure in use because it suffers from "known ciphertext-plaintext attack". Lee

and Chang proposed an improved scheme in 1995 [10]. Then, Wu and Hsu [25] pointed out Lee and Chang's scheme [10] was not perfect when a dispute occurred, and they proposed a scheme to make up for the disadvantage in 2002. In 2003, Ma and Chen [13] proposed a new application in AES. Their scheme could provide the third party to verify the signature without knowing plaintext, except the sender and the receiver.

All of above basic authenticated encryption schemes are based on discrete logarithm. There is some researches of the authenticated encryption schemes which is based on elliptic curve discrete logarithm problem (ECDLP). Miller [15] and Kobitz [9] introduced the elliptic curve into cryptosystem in mid-1980s. Elliptic curve cryptosystem provides greater efficiency than both integer factorization systems and discrete logarithm systems, including key sizes and bandwidth for schemes of relative security [2, 14]. In the researches of the authenticated encryption scheme, Tzeng et al. proposed an authenticated encryption scheme based on ECDLP [22].

Although the basic authenticated encryption schemes can reduce transmitted cost efficiently, there still existed a common disadvantages for above schemes. When the transmitted message is so long that the message must be divided into many message blocks. Then, the signer must sign and encrypt each message block, and sends them to a receiver. That will result in the burst of the computation cost and transmission cost. Therefore, Hwang et al. [8] proposed an authenticated encryption scheme with message linkage to solve the leak. In 1997, Lee and Chang [11] pointed out that Hwang et al.'s scheme exited a disadvantage that the message block should be transmitted one by one in order. Therefore, they proposed an improvement to solve the drawback. In 2003, Tseng et al. thought that Lee and Chang's scheme was not applicable for message flows. They proposed an authenticated encryption scheme with message linkage for message flows [21]. Although Tseng et al.'s scheme can reduce the communication cost and computation cost, the security of the scheme has been broken. Their scheme was pointed out that does not achieve integrity, authentication and non-repudiation by Chen [3] and Zhang et al. [26].

In 1998, Hsu and Wu [**?**] thought that only one signer and one verifier can use the most existing authenticated encryption schemes. Therefore, they proposed a (t, n) threshold signature with authenticated encryption scheme to extend the capability of verification which is addressed to one signer and a group of verifiers. In 2000, Wang et al. [**?**] extended the Hsu and Wu's scheme to propose a (t, n) threshold authenticated encryption scheme which is addressed to a group of signers and a group of verifiers, and claimed their scheme can prevent the message revealing to an outsiders. Although Wang et al.'s scheme provided great concept, Hsu et al. [**?**] pointed out that their scheme is not secure that an attacker can solely validate the group signature and recover the message from the group signature without the assistance of other verifiers in the verifying group.

1.2 Requirements

According to the above description of the development of the authenticated encryption schemes, we can infer that an authenticated encryption scheme corresponds with the following properties:

(1)Confidentiality: it must ensure that the secret information can only be obtained, by the sender and the receiver, but not anyone else.

(2)Authentication: it must ensure the sender and the receivers' identities, and avoid the adversary to send a malicious message. The other hand, the scheme only allows a designate receiver to verify the signature for giving message.

(3)Non-repudiation: it must confirm the sender's identity, and the sender could not repudiate his signature and message.

(4)Message recovery: When the recipient received the signed and encrypted message, he/she can verify and decrypt the message simultaneously.

All of the above are the basic requirements of the authenticated encryption scheme (AES for short). If the proposed scheme satisfies those characteristics, it will be called an authenticated encryption scheme. There is an additional requirement which was proposed by Wu and Hsu [25] in 2002.

(5) Convertibility: When a dispute occurred between the sender and the receiver, the kind of authenticated encryption schemes should provide a mechanism to convert the signature to a original signature that can be verified by the other third party.

The remainder of this article is organized as follows. In Section 2, we briefly review the related article about authenticated encryption schemes that include schemes that consider the general length message (basic type), schemes that consider the linkages of a huge message, or message linkage with message flows, and the schemes based on elliptic curve discrete logarithm. In Section 3, we analyze all the mentioned schemes in Section 2 for the requirements, performance and the security. In Section 4, we indicate some research topics in the future about the authenticated encryption schemes. Finally, we make a conclusion for this article.

2 Related Works

In this article about authenticated encryption scheme, it is a special application of message recovery scheme proposed by Nyberg and Rueppel [17, 18]. There are many papers about the application with message recovery proposed in the past, and we can classify those papers by based on different of difficulties.

In illustration 1 is showed the classification of authenticated encryption schemes and then we briefly explain

it. In message recovery scheme, there two major applications which are authenticated encryption schemes and key distribution schemes.

In the authenticated encryption schemes, we divide those schemes into four classifications: (1) factoring difficulty, (2) discrete logarithm difficulty, (3) elliptic curve, (4) factoring and discrete logarithm difficulties. In the classification of each authenticated encryption scheme based on different difficulties, there are two subclasses that are classified by the transmitted message length, and one is general message length and the other is linkage message.

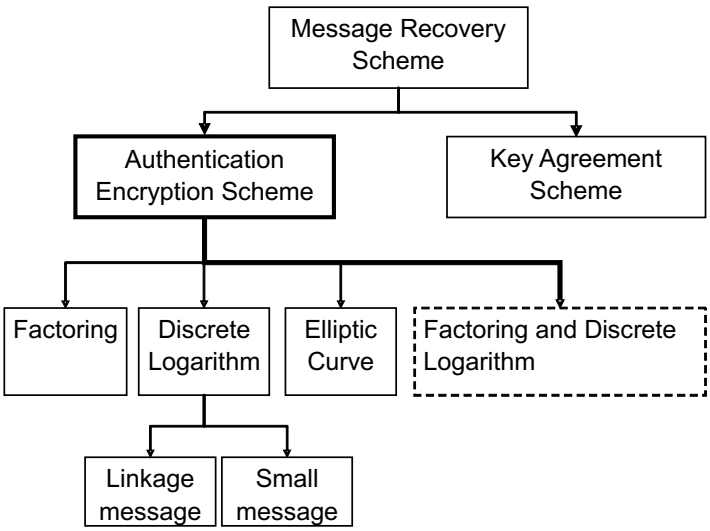

Figure 1: The classification of authenticated encryption scheme

Actually, there are the other extended applications of authenticated encryption schemes that are AES with message linkages and threshold authenticated encryption scheme.

2.1 Authenticated Encryption Schemes

I. Nyberg and Rueppel's signature scheme with message recovery

A new type of digital signature scheme providing message recovery was proposed by Nyberg and Rueppel [17, 18]. They proposed two applications of message recovery. One is that they combine ElGamal encryption and the message recovery which was called authenticated encryption scheme. The other is that they securely integrated the DSA into Diffie-Hellman key exchange. Before introduce the two applications, we should pre-define the notations which will be used.

Assume that A is the sender, and B is the receiver. Let p be a large prime such that $p-1$ has a large prime factor with order q in the Galosis field $GF(p)$. Each participant has his own secret key x_i in $GF(p)$, and a corresponding public key $y_i = g^{x_i} \bmod p$, where g is a generator of $GF(p)$. Then, the two applications are described as the follows.

A. Signing and Encrypting

It could be called authenticated encryption scheme. Let M be a message. The details of the scheme is the follows, and it can be divided into two phases: signed and encrypted phase, and recovered and verified phase. If Alice wants to send Bob the encryption and signature of the giving message, she can randomly select two values t, k and then calculates r, s with $r = Mg^{-k} \bmod p$, and $s = k - x_A r) \bmod q$. Then, she computes (C_1, C_2, C_3) by computing $C_1 = g^t \bmod p$, $C_2 = Mg^{-k} y_B^t \bmod p$, and $C_3 = s$. Finally, she sends Bob (C_1, C_2, C_3) which is the signed of encryption of the message. As Bob received the signature of encryption of the message M, (C_1, C_2, C_3), he will verify and recover message as the follows. First, he computes $r = C_1^{x_B} C_2 \bmod p$, and then recovers message and verifies with Alic's public key as $M = g^s y_A^r r$. (Figure 2)

B. Securely Integrate the DSA to Key Distribution

The other application of the message recovery is key distribution protocol. If users Alice and Bob want to built a session key $g^t modp$, they can perform the procedures as the follows. Alice first randomly selects two values t, k, and calculates signature r', s by computing $r = y_B^t g^{-k} \bmod p$, $r' = r \bmod q$ as in the DSA, and $s = k^{-1}(1 + x_A r') \bmod q$. Finally, she sends Bob the results (r', s). When Bob received r, s, he can with his secret key x_A, and Alice's public key to generate a session key in this session. He should do the procedures as the follows. Bob first computes $g^k = g^{s^{-1}} y_A^{s^{-1}} r' \bmod p$, and then computes $y_B^t = rg^k \bmod p$. Finally, he computes their session key with the equation $(y_B^t)^{x_B^{-1}}$. The procedures are as Figure 3.

II. Authenticated encryption schemes based on discrete logarithm

According to the concept of Nyberg and Rueppel's message recovery scheme [17, 18], there are many related papers have been proposed in the recently years. Thereinafter, we will review some of well-known authenticated encryption schemes based on the difficultly of discrete logarithm. Some of system parameters should be pre-defined before introducing those schemes.

Let p be a large prime such that $p-1$ has a large prime factor with order q in the Galosis field $GF(p)$. Each participant has his own secret key x_i in $GF(p)$,

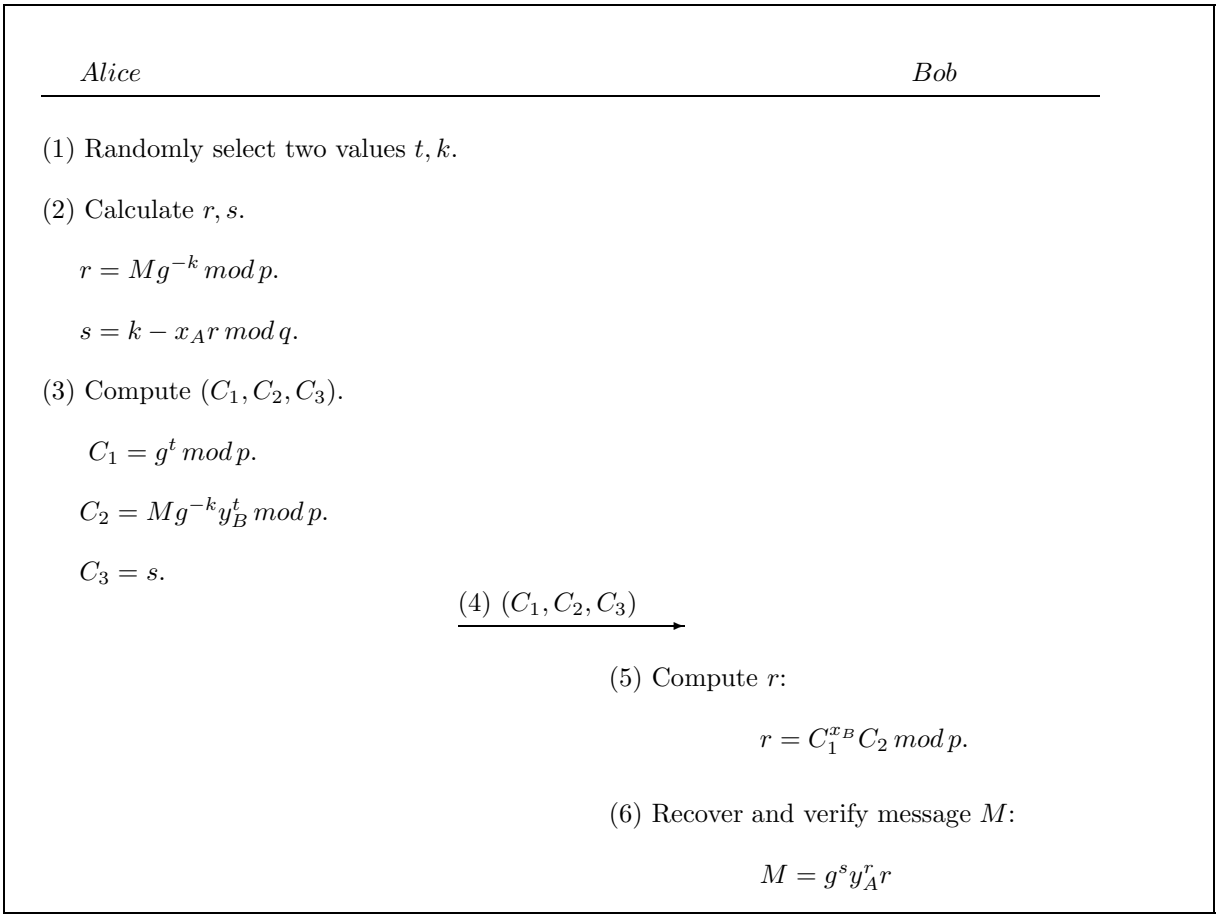

Figure 2: Nyberg and Rueppel's Signing and Encrypting Scheme

and a corresponding public key $y_i = g^{x_i} \bmod p$, where g is a generator of $GF(p)$. $H(.)$ denotes a one way hash function.

a. Horster et al.'s AES with low communication costs The authors [5] claimed that their scheme has low communication costs than the basic authenticated encryption scheme [18]. The scheme is divided into two phases, generation of signature and encryption phase, and recovery message and verification phase. If Alice wants to sign and encrypt message M, she can perform the procedures. First, she randomly selects a value k, and computes c, r, s by computing $c = MH(y_B^k)^{-1} \bmod p$, $r = c \bmod q$, and $s = k - x_A r \bmod q$. Next, she transmits c, s to Bob. As Bob receives the signed of encryption of giving message, he should do as the follows to decrypt and verify the message. First, he computes $r = c \bmod q$, and then recover and verify the message M with $M = H(y_B^s y_A^{r x_B}) c \bmod p$. The algorithm is shown Figure 4.

b. Wu and Hsu's convertible AES In 1999, Araki et al. proposed a convertible limited verified signature scheme which can be recognized as a new type of authenticated encryption scheme [1]. In their scheme, if any third party wants to recover the message and then verifies the signature, the receiver should require a parameter obtained from the sender to convert the signature to original signature. However, Wu and Hsu thought that the sender may not be willing to cooperate [25], and they proposed the other solution. And the other hands, they considered a situation that when the sender and the receiver dispute about the message, it should be judged by a just third party.

The proposed scheme can be divided into three phases, signing and encrypting, recovering and verifying, and judging phases. In the scheme, it contains signing and encrypting, and recovering and verifying phases. As the signer repudiates the signature, the recipient can reveal the converted signature $(r2, s)$, and the message M. Anyone signature can verify its validity with equation $r_2 = H(M, (g^s y_A^{r_2}) \bmod p) \bmod p$. In generation of signature and encryption phase, Alice first selects a random value k, and computesr_1, r_2, s by calculating $r_1 = MH(y_B^k \bmod p)^{-1} \bmod p$,

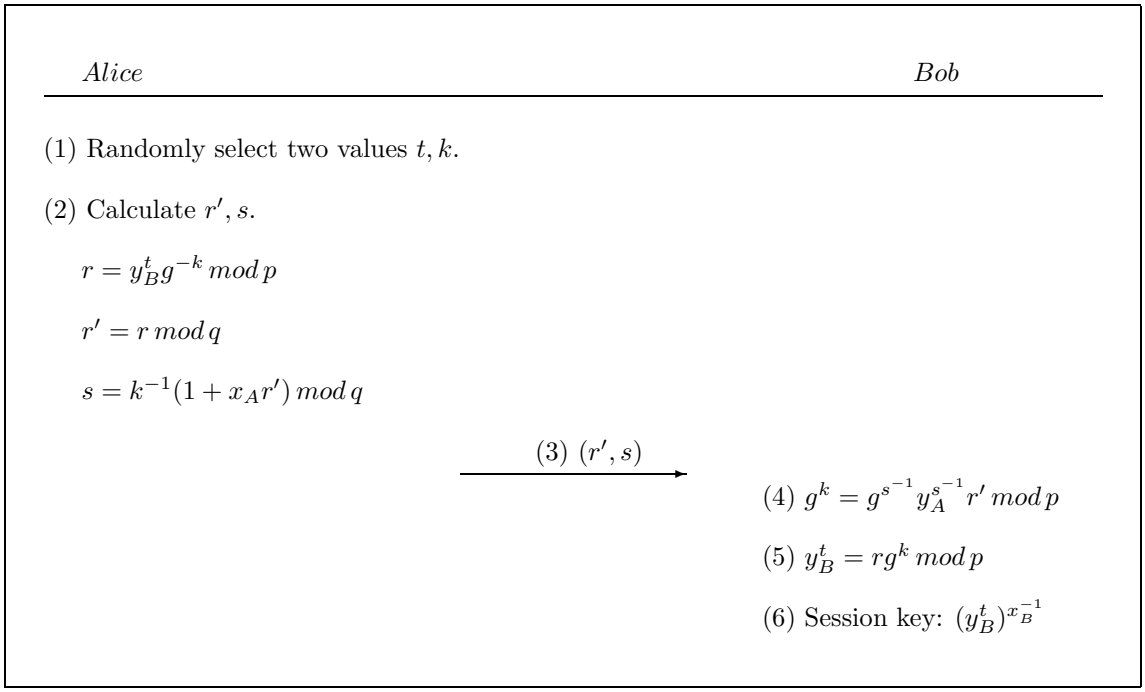

Figure 3: Nyberg and Rueppel's Securely Integrate the DSA to Key Distribution

$r_2 = H(M, H(g^k \, mod \, p)) \, mod \, q$, and $s = k - x_A r_2 \, mod \, q$. Then, she transmits r_1, r_2, s to Bob. As Bob receiving, he can recover message M with $M = r_1 H((g^s y_A^{r_2})^{x_B}) \, mod \, p$, and verify the signature with $r_2 \stackrel{?}{=} H(M, H(g^s y_A^{r_2} \, mod \, p) \, mod \, q$. The procedures can be showed as 5.

III. Authenticated encryption schemes based on elliptic curve cryptosystem

In 2004, Tzeng and Hwang [22] introduced a new digital signature scheme with message recovery based on ECC. They utilized the characteristic of ECC to propose their scheme and in addition to ECC, they also use self-certified public key which first be proposed by Girault in 1991. In this paper, it includes two parts which one is digital signature scheme with message recovery, and the other is authenticated encryption scheme and it's variants.

Digital signature scheme with message recovery

The proposed scheme can be divided into three phases: the system initialize phase, the signature generation phase, and the message recovery phase.
System initialized phase:
There is a trusted system authority (SA) is responsible for creating the system parameters. SA first 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. SA makes E, p, n, and G public. SA calculates $b = aG$, where $a \in [1, n-1]$ is a random number, and is secret. A user i require to join the system, and he should first choose a random number $c_i \in [1, n-1]$. Then he computes $di = ciG$, and send SA (d_i, IDi), where ID_i is user i's identity. After receiving (d_i, IDi), SA selects a random number k_i and computes user i's public key $y_i = k_i G + d_i$, and finds s_i with $s_i = k_i + ((y_i)_x + ID_i)a \, mod \, n$, where $(.)_x$ denotes the x-coordinate of the point $(.)$ on E. SA replies (y_i, ID_i, s_i) to user i, and user i can calculate his private key $x_i = s_i + c_i$ and verify the corresponding public key y_i with $x_i G = y_i + ((y_i)_x + ID_i)b$.
Signature generation phase: Alice wants to sign a message M, and she should perform the signature procedures as the follows.

Step 1. Choose a random number $k \in [1, n-1]$.

Step 2. Compute the signature (r, s) of the message M with $r = M + (kG)_x \, mod \, n$, and $s = k - H(r)x_A$.

Message recovery phase: After receiving (r, s), Bob can recover and verify the message M with $M = r - (sG + H(r)(y_A + ((y_A)_x + ID_A)b))_x \, mod \, n$.

Authenticated encryption scheme

The proposed scheme is extended from above digital signature scheme with message recovery. It allows a designated receiver to decrypt and verify the giving message. The system initialization phase is the same as the above scheme. The remainder of two phases

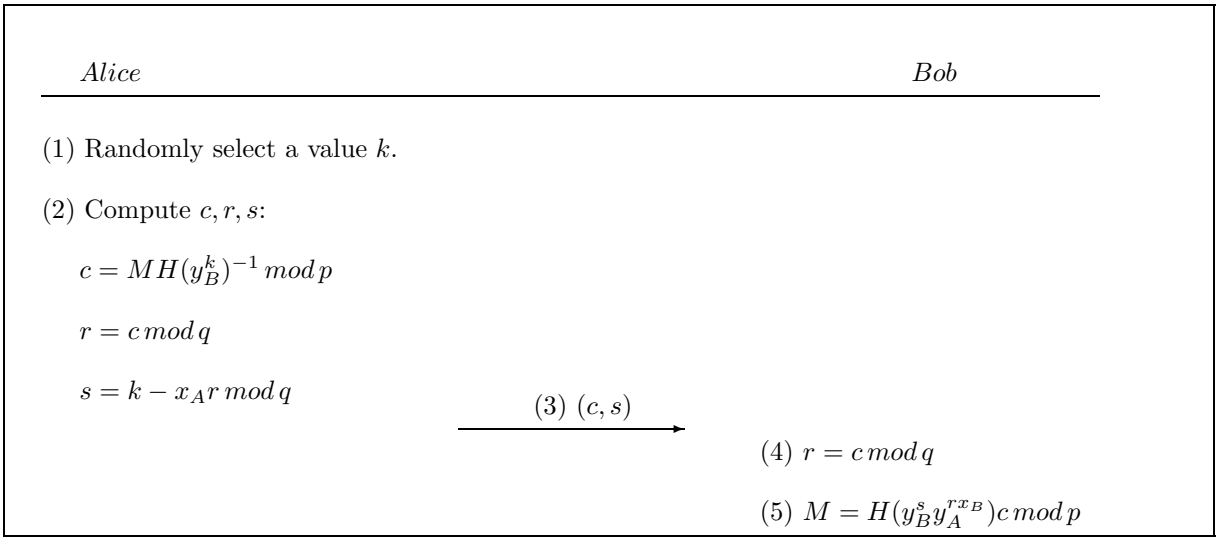

Figure 4: Horster et al.'s authenticated encryption scheme

are is described as the follows.
Signature generation phase: If Alice wants to sign a message M and sends it to Bob, she can perform the following procedures.

Step 1. Select a random integer $k \in [1, n-1]$.

Step 2. Compute the signature of the message M, r and s.
$r = M + (kG)_x \, mod \, n$, $s = k - H(r)x_A \, mod \, n$

Step 3. Send (r, s) to Bob.

Message recovery and verification phase: After receiving (r, s), Bob can verify and recover the message with $M = r - (sG + H(r)(y_A + ((y_A)_x + ID_A)b))_x \, mod \, n$.

Authenticated encryption scheme with message linkages

The authors considered that when a message is huge and has to be divided into a sequence of message blocks. They also proposed an solution to achieve the requirements of the huge message. In the scheme, it is claimed that if the message blocks have been reordered, modified, deleted or replicated, the receiver can detect them. The detailed procedures is as the follows.
Signature generation phase: If Alice wants to generate a signature for the message M, she should first divides the message M into $m_1, \cdots, m_n$, where $m_i \in E(Z_p)$ for $i = 1, 2, \cdots, n$. The steps are as the follows.

Step 1. Setup a initial value $r_0 = 0$, and select a random integer $k \in [1, n-1]$.

Step 2. Compute the signatures of each message block with
$r_i = M_i + H(r_{i-1} \bigoplus (k(y_B + ((y_B)_x + ID_B)b))_x) \, mod \, n$,
$r = H(r_1 \parallel r_2 \parallel \cdots \parallel r_n)$, and
$s = k - rx_A \, mod \, n$.

Step 3. Send $(r, s, r_1, r_2, \cdots, r_n)$ to Bob.

Message recovery phase: As Bob receives $(r, s, r_1, r_2, \cdots, r_n)$ from Alice, he first computes $r' = H(r_1 \parallel r_2 \parallel \cdots \parallel r_n)$ and then confirms that $r' = r$ is true. Finally, he recovers the message block m_i by computing $m_i = r_i - H(r_{i-1} \bigoplus ((sG + r(y_A + ((y_A)_x + ID_A)b))x_B)_x) \, mod \, n$.

Authenticated encryption scheme with message linkages for message flows

The scheme allows the verifier to retrieval individual blocks and use them before all the signature blocks are obtained. The signature generation phase and message recovery phase are described as follows.
Signature generation phase: When Alice wants to generate a signature for the message M, she should set the message components as the sequence $m_1, \cdots, m_n$. Let t blocks form a segment. 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 Alice creates $\lceil n/t \rceil$ signature for all segments.

Step 1. Setup two initial values $r_0 = 0$, $r_{i0} = r_{i-1}$ and select a random integer $k_i \in [1, n-1]$.

Step 2. Compute the signatures of each message block with
$r_{ij} = M_{ij} + H(r_{i(j-1)} \bigoplus (k_i(y_B + ((y_B)_x + ID_B)b))_x) \, mod \, n$,
$r_i = H(r_{i1} \parallel r_{i2} \parallel \cdots \parallel r_{it})$, and
$s_i = k_i - r_i x_A \, mod \, n$.

Step 3. Send $(r_i, s_i, r_{i1}, r_{i2}, \cdots, r_{it})$ to Bob.

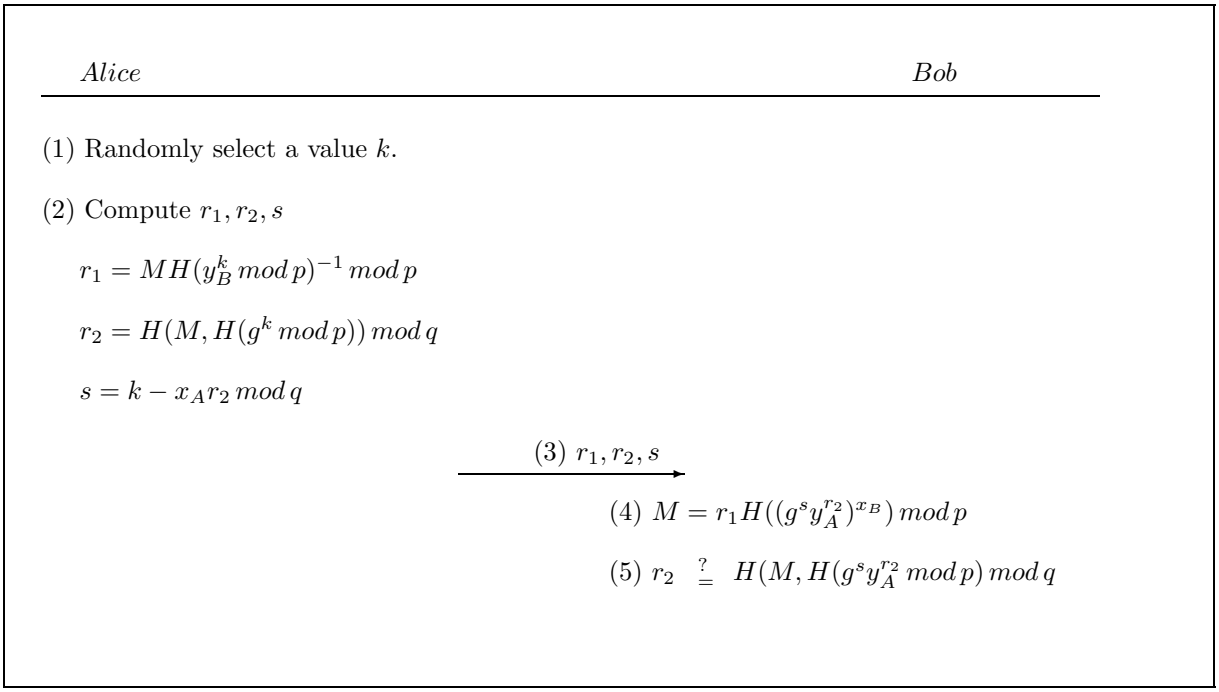

Figure 5: Wu and Hsu's convertible authenticated encryption scheme

Message recovery phase: After receiving $(r_i, s_i, r_{i1}, r_{i2}, \cdots, r_{it})$, Bob can verify and recover ith segment and then use it. The steps are described as the follows. First, Bob should calculate $r_i^{'} = H(r_{i1} \parallel r_{i2} \parallel \cdots \parallel r_{it})$, and then confirms that $r_i^{'} = r_i$ is true. Finally, he obtains the segment by computing $M_{ij} = r_{ij} - H(r_{i(j-1)} \bigoplus((k_i(y_B + ((y_B)_x + ID_B)b))x_B)_x) \bmod n$.

2.2 The Extended Applications

I. Authenticated encryption schemes with message linkages

a. Hwang et al.'s AES with message linkage

Although the proposed authenticated encryption scheme provided great guidelines for the security and the authentication, Hwang et al. thought that those scheme still existed a common disadvantage [8]. Usually, for the long message must be divided into many message blocks before transmitting. To avoiding a eavesdropper replacing any message block without being detected by the recipient, each message block should contain the redundant bits to link up message blocks, but the redundancies increase communication cost. Hwang et al. considered the problem, and they proposed a solution for the authenticated encryption scheme. The scheme is still divided into two phases, generation of signature and encryption phase, and recovery message and verification phase. If Alice wants to sign and encrypt a huge message M with the scheme, she should first divide long message M to t blocks as $M = m_1, m_2, \cdots, m_t$. Next, she randomly selects t values $k_1, k_2, \cdots, k_t$, and computes $ß_i, r_i$ by the equations $ß_i = y_B^{k_i} \bmod p$, and $r_i = m_i H(ß_i)^{-1} \bmod p$. Then, she signs each block with $s_i + k_{i+1} = k_i - x_A r_i) \bmod q$. Finally, she transmit the signature of all message blocks $(r_1 s_1), (r_2, s_2), \cdots, (r_t, s_t)$ to Bob. As Bob received those message, he can first computes $ß_i = y_B^{k_i} = y_B^{k_i^{-1}} y_B^{s_i} y_A^{r_i x_B} \bmod p$. Then, he recovers and verifies m_i with $m_i = r_i H(ß_i) \bmod p$. Finally, if he complete all message blocks recovery, he can combine all blocks to the ordinary message M.

In this paper, the authors proposed another authenticated encryption scheme for long message. They removed the additional one-way functions, and proposed the following algorithm to correspond to the requirements of Lee and Cheng's scheme. The details are as the follows. In this scheme, the equation $r_i = m_i H(ß_i)^{-1} \bmod p$ is modified to $r_i = m_i g^{-ß_i} \bmod p$, and then s_i is also modified to $s_i = k_i - k_{i+1} - x_A r_i \bmod q$. After Bob receives $(r_1 s_1), (r_2, s_2), \cdots, (r_t, s_t)$, he can computes $ß_i = y_B^{k_i} = y_B^{k_i^{-1}} y_B^{s_i} y_A^{r_i x_B} \bmod p$, and recovers and verifies m_i with $m_i = r_i g^{ß_i \bmod q} \bmod p$. (Figure 7)

b. Tseng et al.'s AES with message linkages for message flows

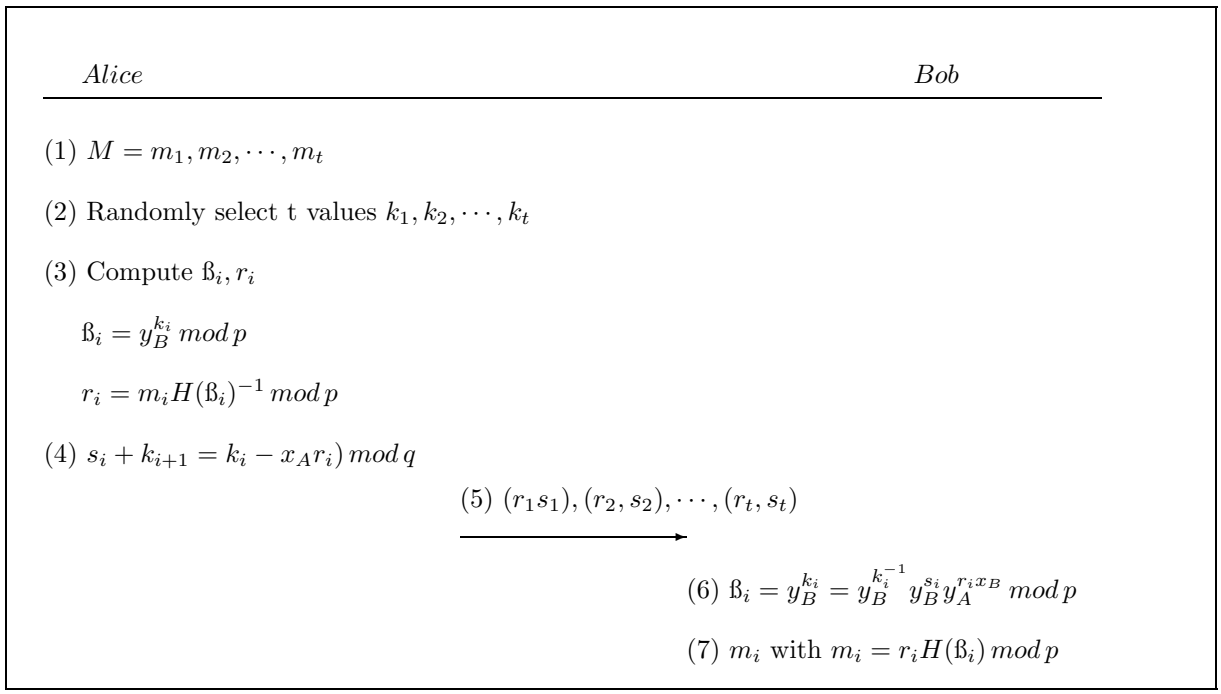

Figure 6: Hwang et al.'s AES with message linkage

In practical implement, there are many kinds of message flow such as digitized audio, stock quote, news, or whatever that all belong to "all-or-nothing flow" [4, 16, 24]. Actually, there is not "all-or-nothing" message flow. According to the kind of message, a receiver can recover individual blocks and use them before the entire message blocks are received. In 2003, Tseng et al. proposed a scheme [21] according to the requirements of the type of the message flow. They proposed two schemes, basic scheme and generalized scheme and we just introduce the basic scheme and the generalized scheme can refer to [21]. In basic scheme, the scheme is divided into three phases: the system initialization phase, the signature generation phase, and message recovery phase. In the system initialization phase, the parameters is defined same as above which contains $p, q, g, H(.)$, and each user's key pair (x_i, y_i). Then remainder phases are described as the follows.

Generation of signature phase:

Step 1. The sender Alice divides long message M to t blocks: $M = m_1, m_2, \cdots, m_n$.

Step 2. She setups $r_0 = 0$ and chooses a ransom number $k \in GF(q)$.

Step 3. Alice computes $r_i = m_i H(r_{i-1} \bigoplus y_B^k) \, mod \, q$ for $i = 1, \cdots, n$, where "$\bigoplus$" denotes the exclusive operator.

Step 4. Alice computes $s = k - r x_A \, mod \, q$, where $r = H(r_1 \parallel r_2 \parallel \cdots \parallel r_n \parallel n)$, and the "$\parallel$" denotes the concatenation operator.

Step 5. Alice transmits $n + 1$ signature blocks $r, s, r_1, \cdots, r_n$ to Bob.

Recovery message phase: After receiving those blocks, Bob can recover with the following procedures.

Step 1. Compute $r' == H(r_1 \parallel r_2 \parallel \cdots \parallel r_n \parallel n)$, and check if $r' = r$ or not.

Step 2. Compute $y_B^k = y_B^s y_{AB}^r \, mod \, p$, where $y_{AB} = y_A^{x_B} \, mod \, p$.

Step 3. Recover the message m_i with $m_i = r_i H(r_{i-1} \bigoplus y_B^k)^{-1} \, mod \, p$, for $i = 1, \cdots, n$.

Generalized scheme

Generation of signature phase:

Step 1. The sender Alice divides long message M to t blocks: $M = m_1, m_2, \cdots, m_n$.

Step 2. She setups $r_0 = 0$ and chooses a ransom number $k \in GF(q)$.

Step 3. Alice computes $r_i = m_i H(r_{i-1} \bigoplus y_B^k) \, mod \, q$ for $i = 1, \cdots, n$, where "$\bigoplus$" denotes the exclusive operator.

Step 4. Alice computes $s = k - r x_A \, mod \, q$, where $r = H(r_1 \parallel r_2 \parallel \cdots \parallel r_n \parallel n)$, and the "$\parallel$" denotes the concatenation operator.

Step 5. Alice transmits $n + 1$ signature blocks $r, s, r_1, \cdots, r_n$ to Bob.

Recovery message phase: After receiving those blocks, Bob can recover with the following procedures.

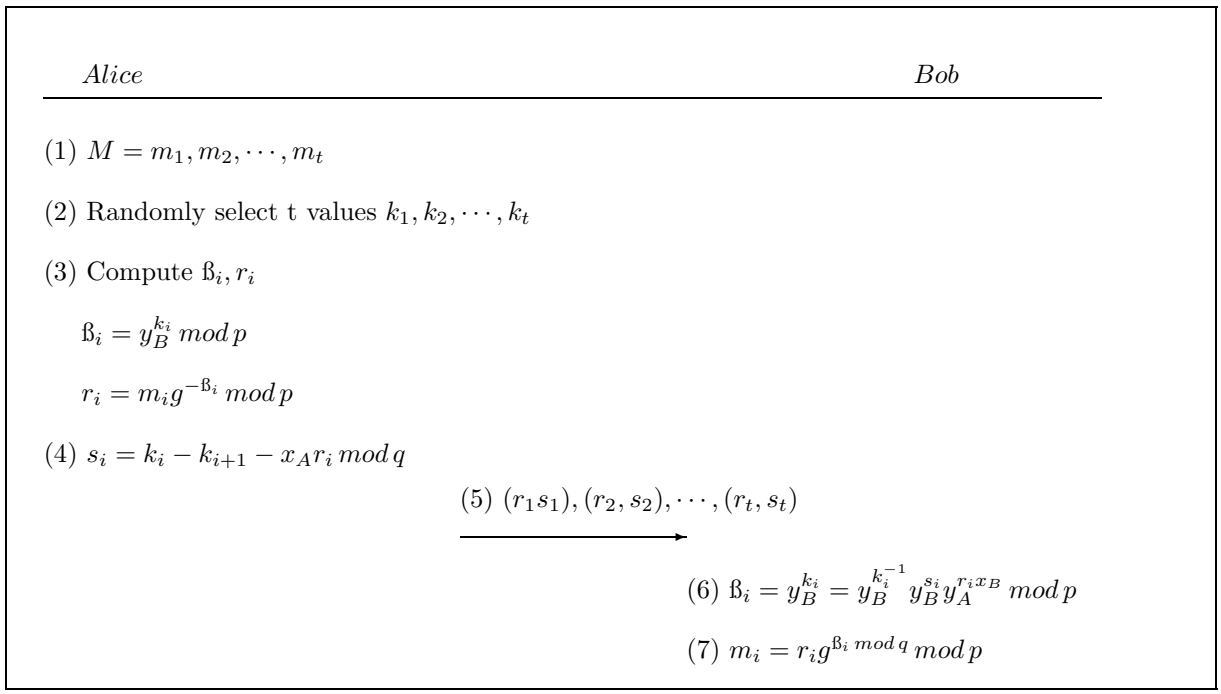

Figure 7: Hwang et al.'s AES with message linkage without hash function'

Step 1. Compute $r' == H(r_1 \parallel r_2 \parallel \cdots \parallel r_n \parallel n)$, and check if $r' = r$ or not.

Step 2. Compute $y_B^k = y_B^s y_{AB}^r \, mod \, p$, where $y_{AB} = y_A^{x_B} \, mod \, p$.

Step 3. Recover the message m_i with $m_i = r_i H(r_{i-1} \bigoplus y_B^k)^{-1} \, mod \, p$, for $i = 1, \cdots, n$.

II. (t, n) threshold authenticated encryption schemes In 1998, Hsu and Wu integrated the design concepts of the signature scheme with message recovery and the (t, n) threshold scheme based on discrete logarithm. They proposed the scheme to extend the capability of verification which is addressed to one signer and a group of verifiers. The scheme can be divided into four phases: system initiation, registration, signature encryption, and message recovery phases. In the system initiation phase, the system authority (SA) will pre-define the system parameters and publishes them. SA will selects two large prime numbers p, q and g where $q \mid p-1$ and g is a generator with order q in $GF(p)$. The registration, and signature encryption, and message recovery phases are described as the following.
Registration phase: S_A denotes a real signer and $G = \{U_1, U_2, \cdots, U_n\}$ denotes a group of n verifiers. Each verifier has his own identity ID_i which is corresponded with the verifier U_i.

Step 1. SA randomly selects a integer $x_a \in Z_q^*$ to be the private key of the real signer S_a.

Step 2. SA calculates the real signer's public key with computing $y_a = g^{x_a} \, mod \, p$.

Step 3. SA randomly selects a integer $x_G \in Z_q^*$ to be the private key of the group G.

Step 4. SA also calculates the corresponded public key with x_G of the group G.

Step 5. SA generates a $(t-1)$-degree polynomial $f(v) = x_G + a_1 v + a_2 v^2 + a_3 v^3 + \cdots + a_{t-1} v^{t-1} \, mod \, q$.

Step 6. SA computes each verifier's private key with $x_i = f(ID_i)$ and also computes his/her public key with $y_i = g^{x_i} \, mod \, p$.

Signature encryption phase: As the real signer S_a wants to transmit a secret message m to G. He/she can performs the following algorithm to protect the content of m.

Step 1. S_a selects a random number $k \in Z_q^*$.

Step 2. She/he generates the signature (r, s).
$r = m g^{-k} \, mod \, p$
$s = k - x_a r \, mod \, p$

Step 3. Then S_a selects a random number $d \in Z_q^*$.

Step 4. She/he generates the encryption c_1, c_2, c_3 of the message m.
$c_1 = m g^d \, mod \, p$
$c_2 = r y_G^{-d} \, mod \, p$
$c_3 = s$

As the signer generates the signature and encryption of the message m, she/he sends c_1, c_2, c_3 the group verifiers G. When G receives them, they can determine t verifiers to recover the message m from the signature and encryption. Message recovery phase:

$W = \{U_1, U_2, \cdots, U_t\}$ denotes a group of t verifiers of G. Then they can perform the following procedures to recovery the message and verify the signature of m.

Step 1. Every $U_i \in W$ computes $E_i = c_1^{x_i L_i \bmod p} \bmod p$, where $L_i = \prod_{j=1, i\neq j}^{t} -ID_j(ID_i - ID_j)^{-1} \bmod q$.

Step 2. They mutually cooperate to compute $E = \prod_{j=1}^{t} E_j \bmod p$.

Step 3. And they recompute the signature (r', s') of m with $r' = c_2 E \bmod p$ and $s' = c_3$.

Step 4. Finally, they recover the message with $m = g^s y_a^r r \bmod p$.

In this section, we introduce the representative papers of authenticated encryption scheme and the extended schemes.

3 Discussion

In this section, we can estimate the mentioned scheme which are introduced in Section 2. For the convenience, we use abbreviation to represent every proposed scheme. Horster et al.'s scheme is called "HMP_DL" [5], and Wu and Hus's scheme [25] is called "WH_DL" [25]. In 2004, Tzeng and Hwang [22] proposed a signature scheme with elliptic curve cryptosystem, "TH_ECC" for short. In the extended applications, Hwang et al.'s scheme [8] is called "HCY_ML". In 2003, Tseng et al. proposed a scheme [21] according to the requirements of the type of the message flow, "TSE_ML" for short. Finally, the Hsu and Wu [6] proposed a (t, n) threshold authenticated encryption scheme, "HW_T" for short.

3.1 Requirement Estimation

In Horster et al.'s scheme, it cannot ensure the confidentiality of a message M, because the scheme cannot withstand the known plaintext-ciphertext attack [10]. The scheme had no the function of the convertibility. Although Wu and Hsu's scheme provided the convertibility, it needed addition information u sent by the original signer. And the other weakness of Wu and Hsu's scheme was that if the signer did not cooperate with the receiver, the trusted third party cannot judge who was legal. Tzeng et al. proposed an authenticated encryption scheme based on ECDLP [22], and the scheme has no the convertibility requirements of an authenticated encryption scheme. Hwang et al. [8] proposed an authenticated encryption scheme with message linkage, and it cannot achieve the convertibility requirements of AES, too. Tseng et al.'s with message linkage for message flows [21] has been broken. It has been pointed out that does not achieve integrity, authentication and non-repudiation by Chen [3] and Zhang et al. [26]. Hsu and Wu's scheme [**?**] does not provide the convertibility function.

3.2 Performance Analysis

For the convenience, we use abbreviation to represent every proposed scheme. Horster et al.'s scheme is called "HMP_DL" [5], and Wu and Hus's scheme [25] is called "WH_DL" [25]. In 2004, Tzeng and Hwang [22] proposed an authenticated encryption scheme with message linkage based on elliptic curve cryptosystem, "TH_ECC" for short. In the extended applications, Hwang et al.'s scheme [8] is called "HCY_ML". In 2003, Tseng et al. proposed a scheme [21] that is authenticated encryption scheme with message linkage called "TSE_MF" by us, and they also proposed another scheme according to the requirements of the type of the message flow, "TSE_MF" for short. Finally, the Hsu and Wu [6] proposed a (t, n) threshold authenticated encryption scheme, "HW_T" for short. The "ML" denotes message linkage and the "MF" denotes message flows.

In efficiency property, we will focus on the performance of our scheme and to analyze the efficiency. For convenience, we first define some notations to denote the performance time: 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. We only consider those $T_h, T_{exp}, T_{mul}, Tinv$ computational heavily cost. In order to differentiate the computational complexity between the elliptic curve cryptosystem and the general discrete logarithm cryptosystem, we define the other notations to evaluate the performance of the authenticated encryption scheme based on ECDLP. T_{ec_mul} is the 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.

For the communication cost of the various schemes, we define some notation to denote the total size of the transmitted message. $|p|$ denotes the bit length of a prime number p, and $|q|$ denotes the bit length of a prime number q. $|h|$ denotes a bit length of a hashing value. If the message is large, it must be divided into n message blocks. $\lceil n/c \rceil$ denotes that a set of signature blocks is $(r_i, s_i, r_{i1}, \cdots, r_{ic})$ for each segment i, $i = 1, \cdots, \lceil n/c \rceil$. t denotes that t verifiers of a group of m verifiers such like that is defined in Hsu and Wu [6].

We could dispute the computational cost over two phases, signature generation phase, and message recovery phase. The signature generation phase of HMP_DL requires $T_{exp}+T_{inv}+2T_{mul}+T_h$ and the message recovery phase needs $2T_{exp}+T_h+3T_{mul}$. The signature generation phase of WH_DL requires $3T_h + T_{inv} + 2T_{mul} + 2T_{exp}$ and the message recovery phase needs $3T_h + T_{inv} + 3T_{exp}$. In the Tzeng and Hwang's AES based on ECDLP, the signature scheme with message recovery, the signature generation phase needs $T_{ec\_mul} + T_{mul} + T_h$, and the message recovery phase, it costs $2T_{ec\_mul}+T_{ec\_add}+T_h$. In their authenticated encryption scheme, the signature generation phase costs $2T_{ec\_mul}+T_{ec\_add}+T_{mul}+T_h$, and the message recovery phase, the verifier spends $4T_{ec\_mul}+2T_{ec\_add}+T_h$

Table 1: Requirement estimation

	HMP_DL	WH_DL	TH_ECC	HCY_ML	TSE_ML	HW_T
Confidentiality	No	Yes	Yes	Yes	Yes	Yes
Authentication	Yes	Yes	Yes	Yes	No	Yes
Non-repudiation	Yes	Yes	Yes	Yes	No	Yes
Convertibility	No	Yes	No	No	No	No
Message Recovery	Yes	No	Yes	Yes	Yes	Yes

to recover the message. In the authenticated encryption scheme with message linkages, assume that the message is divided into n message blocks. In the signature generation phase, it should spend $2T_{ec\_mul}+T_{ec\_add}+T_{mul}+(n+1)T_h$, and in the message recovery phase, the verifier must spend $4T_{ec\_mul} + 2T_{ec\_add} + (n+1)T_h$.

In Tseng et al.'s scheme, they proposed two scheme, basic scheme that only be used in message linkage and generalized scheme that can be used in message linkage and in message flows. In their basic scheme, the computation cost of the signature generation phase is $(n+1)(T_h + T_{mul}) + T_{exp}$ and the message recovery phase requires $(n+1)(T_h + T_{mul}) + 3T_{exp} + nT_{inv}$. In the generalized scheme, the computational complexity for the signature generation and message recovery are $\lceil n/c \rceil (T_{exp} + (t+1)(T_h + T_{mul}))$ and $\lceil n/c \rceil (n+1)(3T_{exp} + tT_{inv} + (t+1)(T_h + T_{mul}))$. In the Hsu and Wu's scheme [6], the signer generates a signature that the computational cost is $3T_{exp} + T_{mul}$, and the verifier recovers the message that will needs $3T_{exp} + (2t+1)T_{mul} + (t-1)T_{inv}$.

4 Future Works

In the future, some research topics can be indicated. In the past, there are many papers about authenticated encryption scheme [1, 5, 10, 13, 25] based on various difficulties such as discrete logarithm, factoring, or elliptic curve, etc. Several savants also armed at the linkages of a huge message or the message linkages for message flows to design a suitable algorithm with the concept of authenticated encryption scheme [3, 8, 11, 21, 26]. According to the group of verifiers, many papers have been proposed to suit the requirements of a authenticated encryption scheme with (t, n) shared verification such as [6, 7, 12, 23]. Actually, there are some subjects should be down in the future. The future works can be described as the below items.

1) In practical implement, when signer cannot sign message, the proxy behavior will happen. To consider the aspect of proxy signature, we will proposed a algorithm with the concept of AES.

2) In a mobile environment, short response time and efficient computation are very important. When a user requests a service to a provider with payment way, he will considerably care about the transmitted time and cost. Since it costs quite much of the computation of authentication encryption schemes more efforts should be made to improve the efficiency.

3) Actually, the other cryptosystem is developing gradually recently, Elliptic curve cryptosystem. It can provide more efficient performance, and keeps the same security as the traditional public cryptosystems. We maybe also combine the two difficulties which are factoring and elliptic curve to provide more efficient and more security protocol in the future.

4) For the 3G/GSM, it needs more efficient transmission. Therefore, the authenticated encryption scheme can be applied in the environments. 3G/GSM has the key agreement protocol, and it can also be applied in them. Those protocols can be designed, and compare the designed protocol using authenticated encryption scheme with the 3G/GSM general protocols.

5 Conclusions

In this article, we have introduced related works in Section 2. In Section 3, we have discussed that if each proposed scheme has achieved the requirements of an authenticated encryption scheme, or not. Then, we have also analyzed the performance of each schemes which are introduced in Section 2. Nyberg and Rueppel's method could be apply to small message transmission such as ID-based system or key agreement system. The signature scheme with message recovery can be applied to a electronic written acknowledgement for a debt which the size of the message content is smaller.

Although the authenticated encryption scheme researches provide more efficient for the communication, they exit an potential problem which the security may be lower than the general signature and then encryption schemes. If the participators communicate with each other, they must pre-share a message format mutually that will reduce the security of secure message. The message format is public, and the parts of the secure message are known by everyone. If the length of a secure message is 1024 bits and it includes the pre-shared format 10 bits, it can be detected obviously that the secure bits is only 1014 bits. That may not cause serious security problem, but it is a fact that those scheme will reduce the security.

Table 2: Performance analysis

	ML	MF	Comm. cost	Signature generation	Message recovery
HMP_DL	No	No	$\|p\| + \|q\|$	$T_{exp} + T_{inv}$ $+2T_{mul} + T_h$	$2T_{exp} + T_h$ $+3T_{mul}$
WH_DL	No	No	$\|p\| + 2\|q\|$	$3T_h + T_{inv}$ $+2T_{mul} + 2T_{exp}$	$3T_h + T_{inv}$ $+3T_{exp}$
TH_ECC	Yes	No	$(n+1)\|p\| + \|h\|$	$2T_{ec\_mul} + T_{ec\_add}$ $+T_{mul} + (n+1)T_h$	$4T_{ec\_mul} + 2T_{ec\_add}$ $+(n+1)T_h$
HCY_ML	Yes	Yes	$n\|p\| + n\|q\|$	$n(T_h + T_{inv})$ $+n(T_{exp} + T_{mul})$	$n(T_h + 3T_{mul})$ $+(2n+1)T_{exp}$
TSE_ML	Yes	No	$n\|p\| + \|q\| + \|h\|$	$(n+1)(T_h + T_{mul})$ $+T_{exp}$	$(n+1)(T_h + T_{mul})$ $+3T_{exp} + nT_{inv}$
TSE_MF	Yes	Yes	$\lceil n/c \rceil (t\|p\| + \|q\|)$ $+\lceil n/c \rceil (\|h\|)$	$\lceil n/c \rceil (T_{exp}$ $+(t+1)(T_h + T_{mul}))$	$\lceil n/c \rceil (n+1)(3T_{exp} + tT_{inv}$ $+(t+1)(T_h + T_{mul}))$
HW_T	No	No	$(t+2)\|p\|$ $+2\|q\|$	$3T_{exp} + T_{mul}$	$3T_{exp} + (2t+1)T_{mul}$ $+(t-1)T_{inv}$

References

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

[2] William J Caelli, Ed Dawson, and S. Rea, "PKI, elliptic curve cryptography, and digital signatures," *Computers & Security*, vol. 18, no. 1, pp. 47–66, 1999.

[3] B. H. Chen, "Improvement of authenticated encryption schemes with message linkages for message flows," *Computers and Electrical Engineering*, vol. 30, no. 7, pp. 465–469, 2004.

[4] R. Gennaro and P. Rohatgi, "How to sign digital stream," in *Advances in Cryptology: Crypto'97*, pp. 180–197, 1997.

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

[6] C. L. Hsu and T. C. Wu, "Authenticated encryption scheme with *(t, n)* shared verification," *IEE Proceedings - Computers and Digital Techniques*, vol. 145, no. 2, pp. 117–120, 1998.

[7] C. L. Hsu, T. S. Wu, and T. C. Wu, "Improvements of generalization of threshold signature and authenticated encryption for group communications," *Information Processing Lettes*, vol. 81, no. 1, pp. 41–45, 2002.

[8] S. J. Hwang, C. C. Chang, and W. P. Yang, "Authenticated encryption schemes with message linkage," *Information Processing Letters*, vol. 58, no. 4, pp. 189–194, 1996.

[9] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203–209, 1987.

[10] W. B. Lee and C. C. Chang., "Authenticated encryption scheme without using a one way function," *IEEE Electronics Letters*, vol. 31, no. 19, pp. 1656–1657, 1995.

[11] W. B. Lee and C. C. Chang, "Authenticated encryption schemes with linkage between message blocks," *Information Processing Letters*, vol. 63, no. 5, pp. 247–250, 1997.

[12] J. Z. Lu and H. Y. Chen, "Improvement of authenticated encryption scheme with (t, n) shared verification," in *Computer Software and Applications Conference, 2000. COMPSAC 2000. The 24th Annual International*, pp. 445–448, Oct. 2000.

[13] C. Ma and K. Cheng, "Publicly verifiable authenticated encryption," *IEEE Electronics Letters*, vol. 39, no. 3, pp. 281–282, 2003.

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

[15] V. Miller, "Use of elliptic curves in cryptography," in *In Advances in Cryptology - CRYPTO'85*, vol. 218, pp. 417–426, 1985.

[16] S. Mittra and Thomas Y. C. Woo, "A flow-based approach to datagram security," in *ACM SIGCOMM Computer Communication Review*, vol. 27, pp. 221–234, Oct. 1997.

[17] 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.

[18] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm," in *Advance in Cryptology-EUROCRYPTO'94 proceedings, Lecture notes in computer science*, vol. 1, pp. 175–190, May 1994.

[19] National Institute of Standards and Technology (NIST), "The digital signature standard proposed by NIST," *Communications of the ACM*, vol. 35, no. 7, pp. 34–40, 1992.

[20] 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, 1978.
[21] Y. M. Tseng, J. K. Jan, and H. Y. Chien, "Authenticated encryption schemes with message linkages for message flows," *International Journal of Computers & Electrical Engineering*, vol. 29, no. 1, pp. 101–109, 2003.
[22] S. F. Tzeng and M. S. 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.
[23] C. T. Wang, C. C. Chang, and C. H. Lin, "Generalization of threshold signature and authenticated encryption for group communications," *IEICE Trans. Fundamentals*, vol. E83-A, no. 6, pp. 1228–1237, 2000.
[24] C. K. Wong and Simon S. Lam, "Digital signatures for flows and multicasts," *IEEE/ACM Transactions on Networking*, vol. 7, no. 4, pp. 502–513, 1999.
[25] T. S. Wu and C. L. Hsu, "Convertible authenticated encryption scheme," *The journal of Systems and Software*, vol. 39, no. 3, pp. 281–282, 2002.
[26] Z. Zhang, S. Araki, and G. Xiao, "Improvement of tseng et al.'s authenticated encryption schemes with message linkages," *Computers and Electrical Engineering*, vol. 162, no. 3, pp. 1475–1483, 2005.

Min-Shiang Hwang was born on August 27, 1960 in Tainan, Taiwan, Republic of China (ROC.). He received the B.S. in Electronic Engineering from the National Taipei Institute of Technology, Taipei, Taiwan, ROC, in 1980; the M.S. in Industrial Engineering from the National Tsing Hua University, Taiwan, in 1988; and a Ph.D. in Computer and Information Science from the National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at the National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also the chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He was a professor and chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002-2003. He obtained the 1997, 1998, 1999, 2000, and 2001 Outstanding Research Award of National Science Council of the Republic of China. He is currently a professor and chairman of the department of Management Information Systems, National Chung Hsing University, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 100 articles on the above research fields in international journals.

Chi-Yu Liu received the B.S. degree in Information Management and M.S. in Graduate Institute of Networking and Communication Engineering from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2002 and 2004, respectively. Her current research interests include cryptography, information security, and network security.