Improvement on a Threshold Authenticated Encryption Scheme

Zuowen Tan

1.School of Information Technology, Jiangxi University of Finance and Economics,
Nanchang City 330013,Jiangxi Province, P.R. China
2.Key Lab of Network Security and Cryptology, School of Mathematics and Computer Science,
Fujian Normal University, Fuzhou 350007,Fujian Province, P.R. China
Email: tanzyw@yahoo.com.cn

***Abstract*—The authenticated encryption scheme allows one signer to generate an authenticated cipher-text so that no one except the designated verifier can recover the message and verify the message. In a (t, n) threshold authenticated encryption scheme, any t or more signers can generate an authenticated encryption for a message and send it to the designated verifier. Compared with the conventional encryption-then-signature schemes, threshold authenticated encryption schemes can meet more security requirements, including robustness, confidentiality, unforgeability, integrity, authenticity and non-repudiation. Based on Tseng and Jan's authenticated encryption scheme and elliptic curve cryptosystem, Chung et al. [2] recently proposed an efficient (t, n) threshold authenticated encryption scheme which can reduce the load of the signers by applying a division-of-labor signature technique. However, the paper demonstrates that there exists a design defect, the threshold authentication signature scheme cannot resist against insider attack and the scheme is not robust. Then, an improved authenticated encryption scheme based on elliptic curve cryptosystem is proposed. The novel authenticated encryption scheme removes the above-mentioned weaknesses.**

***Index Terms*—-signature, authenticated encryption scheme, elliptic curve cryptosystem, threshold cryptography**

I. INTRODUCTION

The authenticated encryption scheme is first introduced by Nyberg and Rueppel [3,4]. Such schemes incorporate the characteristics of both message encryption and the digital signature; that is, after a signer generates a signature on a message, only the specified verifier can recover the message, authenticate the sender of the message and verify the integrity of the message. Since the authenticated encryption schemes can meet more security requirements than traditional encryption and digital signature schemes, it has been extensively studied [5,6,7,8]. More focuses are on reducing the communication and operation costs [5, 6]. In order to ensure that message can be recovered from the signature, a message always is hashed in the signatures. Hashing a message can also reduce its size in the signature schemes. However, for authentication encryption schemes, hashing a message can not reduce the size of the authenticated cipher-text since message must be recovered. For an over-large message, two techniques to reduce the communication and operating costs are proposed. One of the techniques is like this: message is first divided into message blocks, then some redundant bits which demonstrate the linkage of the message are added into each block, and the signer encrypts and signs each block. The other technique is adding message linkage and adding the secret for the (i-1)-th message block into the generated signature in the i-th message block [6,7,8]. However, these techniques have some flaws. The former will increase communication costs. For the latter, if the (i-1)-th signature block is altered, then the i-th message block cannot be recovered. So, the verifier cannot proceed with the recovery of the message blocks until the verifier receives all the signature blocks. Obviously, such schemes cannot be applied in message flow transmission [9].

Based on threshold cryptosystems [10,11] and Tseng and Jan's [1] authenticated encryption scheme, Chung et al. [2] recently proposed an efficient (t, n) threshold authenticated encryption scheme. Chung et al. introduced a concept of labor division to reduce the workload of every signer in the threshold scheme. The main idea of the concept is that the message is divided into a few readable message blocks such that each signer only needs to examine and sign the message block assigned to him [2], then all sub-signatures on all the message blocks are combined into one group signature for the whole message.

Compared with the conventional encryption-then-signature schemes, threshold authenticated encryption schemes can meet more security requirements [16, 22, 23, 24, 25], such as robustness, integrity, confidentiality, unforgeability, authenticity and non-repudiation.

–Robustness. In a (t, n) threshold signature scheme ($1 \le t \le n$), if at least t signers in the group follow honestly the protocol, then a valid signature can be generated.

Manuscript received July 18, 2009; revised August 28, 2009; accepted October 1, 2009.
Supported by the National Natural Science Foundation of China (10961013).
Corresponding author: Zuowen Tan

doi:10.4304/jsw.5.7.697-704

–Integrity. A modification on message or signature during the transmission can be identified by the designated receiver.
–Confidentiality. Any information cannot be derived from the authenticated cipher-text by any one except the designated verifier.
–Unforgeability. The authenticated signature is not forgeable.
–Authenticity. The designated verifier can identify the signer group of a given threshold signature.
–Nonrepudiation. A valid signature can be generated only by t or more signers. The signer group cannot deny that the signature is generated by the group.

Based on the elliptic curve cryptosystems [12,13], the (t, n) threshold authenticated encryption scheme in [2] combines the characteristics of both message linkage and division-of-labor. After a detailed performance and security analysis, Chung et al. claimed that their scheme can reach high security with low computational cost. For simplicity, the scheme is called CHC scheme hereafter.

However, the paper demonstrates that there exists a design defect, the threshold authentication signature scheme cannot resist against insider attack and the scheme is not robust. An improved authenticated encryption scheme based on elliptic curve cryptosystem is proposed. The novel authenticated encryption scheme removes all the above-mentioned weaknesses.

The rest of the paper is organized as follows. CHC scheme is briefly reviewed in Section 2 and the analysis of CHC scheme is shown in Section 3. Section 4 and Section 5 propose a novel authenticated signature scheme and give a detailed analysis of the novel scheme, respectively. Section 6 concludes.

II. Review of CHC Scheme

In CHC scheme [2], $\{u_1, u_2, \cdots, u_n\}$ denotes the signer group with n signers where u_i is the i-th signer (i=1,2,$\cdots$,n). Each signer u_i has its public information x_i. An over-large message is divided into t readable message blocks among the actual signer group of t members. Each participant in the actual signer group only needs to sign the message block assigned to him. U_v is the designated verifier. CHC scheme consists of three phases.

A. System initialization phase

The trusted system authority (SA) first selects a large prime integer p, a finite field F_p, the point group E(F_p) of an elliptic curve E over F_p and a generator point $G \in$ E(F_p) with the large prime order q. SA makes a one-way hash function h() public. Then, SA generates the users' private keys.

(1) Choose randomly a (t-1) -degree secret polynomial in the polynomial ring $F_p[x]$:

$$f(x) = e_0 + e_1 x + e_2 x^2 + \cdots + e_t x^{t-1}. \quad (1)$$

(2) Take e_0 as the signer group's private key and compute $Y_s = e_0 G$ as the signer group's public key.

(3) Compute the private keys $f(x_i)$ and the public keys $Y_i = f(x_i)G$ of all signers u_i in the group.

(4) Take x_v as the designated verifier U_v's private key and compute U_v's the public key $Y_v = x_v G$.

B. Signature generation phase

Without loss of generality, assume that t signers $\{u_i | i=1,2, \ldots,t\}$ jointly sign a message m. The t signers collaborate to divide the message into t connected message blocks $\{m_1, m_2, \ldots, m_t\}$, where $m_i \in [1, p\text{-}1]$ (i=1,2, …,t). Each m_i has some redundancy to protect the scheme against a possible forgery attack [14, 15]. Each u_i (i=1,2, …,t) individually generates the signature for the message block m_i by taking the following steps.

(1) Select a random integer b_i in F_q^* and compute

$$B_i = b_i G = (x_{B_i}, y_{B_i}).$$

(2) Compute z_i :

$$z_i = (b_i \cdot x_{B_i}) Y_v = (x_{z_i}, y_{z_i}).$$

(3) Send B_i and z_i to the other participants via a secure channel.

(4) Compute B and the session key Z using all the pairs (B_i, z_i)(i=1,2, $\cdots$,t).

$$B = \sum_{i=1}^{t} B_i = (x_B, y_B),$$

$$Z = \sum_{i=1}^{t} z_i = (x_Z, y_Z). \quad (2)$$

(5) Compute the sub-signature (r_i, s_i) for the message block m_i and publishes it in the actual signer group:

$$r_i = m_i h(i \| x_Z) \mod p,$$

$$s_i = x_{B_i} \cdot b_i - r_i \cdot f(x_i) \cdot \prod_{j=1, j\neq i}^{t} \frac{0 - x_j}{x_i - x_j} \mod q. \quad (3)$$

When the clerk receives the sub-signatures, the clerk can verify the validity of the sub-signatures and then generates the threshold authenticated encryption signature on the message m.

(1) Verify the validity of each sub-signature (r_i, s_i) by checking whether the equality holds:

$$x_{B_i} B_i \stackrel{?}{=} s_i G + (r_i \cdot \prod_{j=1, j\neq i}^{t} \frac{0 - x_j}{x_i - x_j}) Y_i. \quad (4)$$

(2) Combine all the sub-signatures into a threshold authenticated encryption signature.

$$r = \sum_{i=1}^{t} r_i \mod p,$$

$$s = \sum_{i=1}^{t} s_i \mod q. \quad (5)$$

(3) Send the threshold authenticated encryption signature (r, s, r_1, r_2, $\cdots$,) for the whole message to the designated verifier U_v via a public channel.

C. Message recovery phase

After receiving the signature (r,s, r_1, r_2,$\cdots$, r_t), the verifier U_v recovers the message blocks $\{m_1, m_2, \cdots, m_t\}$ by performing the following steps.

(1) Compute the session key Z shared with the actual signer group $\{u_i \mid i=1,2,\cdots,t\}$.

$$Z = sY_v + (r \cdot x_v)Y_s = (x_Z, y_Z). \quad (6)$$

(2) Recover the message blocks $\{m_1, m_2,\ldots, m_t\}$

$$m_i = r_i \cdot h(i \| x_Z)^{-1} \bmod p \text{ for } i=1,2,\ldots,t. \quad (7)$$

(3) Validate the redundancy attached to all the message blocks m_i. If they are valid, then the authenticated signature is valid and the message blocks can be combined into the whole message.

III. ANALYSIS OF CHC SCHEME

Although Chung et al. discussed security of CHC scheme, the scheme is not as secure as claimed. In the following, a design defect and some security weaknesses of CHC scheme will be shown.

A. Correctness analysis

There is a design error in CHC scheme. Even if all the actual signers follow the protocol, Eq. (6) would not hold. The proof of Theorem **1** in [2] is also wrong. So, the verifier U_v can not recover the right message m_i (i=1,2, …,t) through Eq. (7).

The detailed analysis is as follows. Note that

$$Z=\sum_{i=1}^{t} z_i = (x_z, y_z) = \sum_{i=1}^{t} (x_{B_i} \cdot b_i)Y_v \quad \text{(by Eq.(2))}$$

$$= \sum_{i=1}^{t} (s_i + r_i \cdot f(x_i) \cdot L_i)Y_v \quad \text{(by Eq.(3))}$$

$$= \left[\sum_{i=1}^{t} s_i + \sum_{i=1}^{t} (r_i \cdot f(x_i) \cdot L_i)\right] Y_v .$$

where $L_i = \prod_{j=1, j\neq i}^{t} \frac{0-x_j}{x_i - x_j}$ is Lagrange coefficient.

From the above equations, we obtain

$$Z \neq sY_v + [r \cdot x_v \cdot f(0)]G. \quad (8)$$

The verifier cannot obtain the right session key from Eq. (6). So U_v cannot recover the message m. In fact, at the beginning of signature generation phase in CHC scheme, the actual signer u_i (i=1,2, …,t) should calculate $r = \sum_{i=1}^{t} r_i$, then the actual signer u_i produces the sub-signature on message m_i as follows:

$$s_i = x_{B_i} \cdot b_i - r \cdot f(x_i) \cdot \prod_{j=1, j\neq i}^{t} \frac{0-x_j}{x_i - x_j} \bmod q. \quad (9)$$

The validity of the sub-signature is verified by the following formula:

$$x_{B_i} B_i \overset{?}{=} s_i G + (r \cdot \prod_{j=1, j\neq i}^{t} \frac{0-x_j}{x_i - x_j})Y_i . \quad (10)$$

B. Security analysis

However, even if CHC scheme is improved as in Section 3.1 and satisfies correctness, it will still have the following weaknesses.

- CHC scheme is not robust.

If one signer deviates the protocol during signature generation phase, then CHC scheme will fail. Without loss of generality, assume that u_i for some $i \in \{1,2,\cdots,t\}$ is the malicious signer. After t signers collaborate to divide the message into t connected message blocks $\{m_1, m_2,\cdots, m_t\}$, the malicious signer u_i generates the signature for the message block m_i by taking the following steps.

(1) Select a random integer b_i in F_q^* and compute:

$$B_i = b_i G = (x_{B_i}, y_{B_i}).$$

(2) Compute z_i':

$$z_i' = (b_i' \cdot x_{B_i}')Y_v = (x_{z_i}', y_{z_i}'),$$

where $b_i' \cdot x_{B_i}' \neq b_i \cdot x_{B_i}$.

(3) Send B_i and z_i' to the other signers via a secure channel.

(4) Compute B and the session key Z using all the B_j's and z_j's (j=1,2,$\cdots$,t):

$$B = \sum_{i=1}^{t} B_i = (x_B, y_B),$$

$$Z = \sum_{j=1, j\neq i}^{t} z_j + z_i' = (x_Z, y_Z).$$

(5) Compute the sub-signature (r_i, s_i) for the message block m_i and publish it in the actual signer group:

$$r_i = m_i h(i \| x_Z) \bmod p,$$

$$s_i = x_{B_i} \cdot b_i - r_i \cdot f(x_i) \cdot \prod_{j=1, j\neq i}^{t} \frac{0-x_j}{x_i - x_j} \bmod q.$$

It is not hard to check that the sub-signature (r_i, s_i) can pass the sub-signature verification equation (4). So, the clerk can generate the threshold authenticated encryption signature $(r, s, r_1, r_2, \cdots, r_t)$ on message m.

However, when the verifier U_v computes the right session key using the signature and the private key x_v through the equation (6), he/she will obtain a session key Z' rather than Z.

This is because:

$$Z' = \sum_{j=1}^{t} x_{B_j} \cdot b_j G$$

$$\neq \sum_{j=1, j\neq i}^{t} x_{B_j} \cdot b_j G + x_{B_i}' \cdot b_i' G$$

$$= Z .$$

Therefore, the verifier U_v can not recover the right message m through the equation (7). Moreover, any other participants in the scheme can not identify who the malicious signer is.

In fact, the very reason why the scheme cannot tolerate any malicious signer is that during the signature generation phase the linkage between B_i and z_i is not verified.

- CHC scheme suffers from the inside attack.

Assume that the signer u_j in the actual signer group is an inside malicious signer who wants to impersonate the signer u_k to sign the message block m_k. During the signature phase, after the signer u_k declared its sub-signature, the signer u_j impersonates u_k and requires that u_j and u_k need to restart their sub-signatures. u_j impersonates u_k to re-sign m_k as follow.

(1) Select a random integer b_k' in F_q^* and computes

$$B_k' = b_k' G = (x_{B_k'}, y_{B_k'}),$$
$$B_k'' = B_k + B_k' = (x_{B_k''}, y_{B_k''}).$$

(2) Compute

$$z_k'' = z_k + (b_k' \cdot x_{B_k'}) Y_v.$$

(3) Send both B_k'' and z_k'' to the other participants except u_k and himself in the actual signer group via a secure channel.

(4) Compute s_k' and publish the sub-signature (r_k, s_k') for the message block m_k in the actual signer group:

$$s_k' = s_k + x_{B_k'} \cdot b_k' \bmod q.$$

(5) Compute and send (B_j' , z_j') to the other participants except u_k and himself via a secure channel.

$$B_j' = B_j - B_k',$$
$$z_j' = z_j - (b_k' \cdot x_{B_k'}) Y_v.$$

(6) Compute s_j' and publishes the sub-signature (r_j, s_j') for the message block m_j in the actual signer group:

$$s_j' = s_j - b_k' \cdot x_{B_k'} \bmod q.$$

It is not hard to check both the sub-signature (r_k, s_k') and (r_j, s_j') is valid. But it will violate the claim in [2] that the sub-signature (r_k, s_k') is actually generated by the participant u_k. As a matter of fact, u_j can impersonate some actual signers at one time in the same way as mentioned above.

IV. Improvement on CHC Scheme

In the section, an improved threshold authentication signature scheme is proposed. In the novel scheme, an over-large message is still divided into t readable message blocks among the actual signer group and each actual signer only needs to sign the message block assigned to him. Assume that $\{u_1, u_2, \ldots, u_n\}$ are the signer group. Each u_i has its public information x_i. U_v is the designated verifier. The proposed scheme is composed of the three phases.

A. System initialization phase

SA generates the system parameters: a large prime integer p, a finite field F_p, the point group $E(F_p)$ of an elliptic curve E over F_p, a one-way hash function $h()$ and a generator point G in $E(Fp)$ with the large prime order q. Then, *SA* generates the users' public/private keys as in CHC scheme.

B. Signature generation phase

Without loss of generality, assume that t signers $\{u_i | i=1,2,\cdots,t\}$ jointly sign a message m. First, the message m is divided into t connected message blocks $\{m_1, m_2, \cdots, m_t\}$ among the t signers.

The signature generation phase is subdivided into two phases: the sub-signature generation phase and the signature combination phase.

- **Sub-signature generation phase**

In the phase, each signer u_i (i=1,2, …,t) generates the signature for the message block m_i by performing the following operations.

(1) Select a random integer b_i in F_q^* and compute

$$B_i = b_i G = (x_{B_i}, y_{B_i}),$$
$$z_i = (b_i \cdot x_{B_i}) Y_v = (x_{z_i}, y_{z_i}). \quad (11)$$

(2) Select a random integer k_i in F_q^* and compute

$$R_i = k_i G,$$
$$R_{vi} = k_i Y_v, \quad (12)$$
$$s_i' = k_i - h(R_i \| R_{vi} \| B_i \| z_i) x_{B_i} b_i \bmod q. \quad (13)$$
$$s_i'' = k_i - h(i \| R_i \| R_{vi} \| B_i \| z_i) f(x_i) \bmod q. \quad (14)$$

(3) Send $(B_i, z_i, R_i, R_{vi}, s_i', s_i'')$ to the other signers via a secure channel.

(4) Check if the following holds:

$$s_i' G \stackrel{?}{=} R_i - h(R_i \| R_{vi} \| B_i \| z_i) x_{B_i} B_i, \quad (15)$$
$$s_i' Y_v \stackrel{?}{=} R_{vi} - h(R_i \| R_{vi} \| B_i \| z_i) z_i, \quad (16)$$
$$s_i'' G \stackrel{?}{=} R_i - h(i \| R_i \| R_{vi} \| B_i \| z_i) Y_i. \quad (17)$$

If the above equations hold, u_i goes to the following steps.

(5) Compute the session key Z

$$Z = \sum_{i=1}^{t} z_i = (x_Z, y_Z). \quad (18)$$

(6) Compute the sub-signature r_i for the message block m_i and publishes it in the actual signer group:

$$r_i = m_i h(Y_s \| i \| x_Z) \bmod p. \quad (19)$$

(7) Compute all the sub-signature s_i in the actual signer group:

$$s_i = x_{B_i} \cdot b_i - h(r_1 \| r_2 \| \cdots \| r_t) \cdot f(x_i) \cdot \prod_{j=1, j \neq i}^{t} \frac{0 - x_j}{x_i - x_j} \bmod q. \quad (20)$$

(8) Send the authenticated signature (r_i, s_i) to the clerk via a secure channel.

Note that when a certain signer u_i requires to re-sign its message block, the signer must run all the steps during sub-signature generation phase. That is, u_i must generate a new six-tuple $(B_i, z_i, R_i, R_{vi}, s_i', s_i'')$.

- **Signature combination phase**

When the clerk receives the sub-signatures, he/she first verifies the validity of the sub-signatures and then combines them into a threshold authenticated encryption signature on m.

(1) Check the validity of (r_i, s_i) by checking whether the equality holds:

$$x_{B_i} B_i \stackrel{?}{=} s_i G + (h(r_1 \| r_2 \| \cdots \| r_t) \cdot \prod_{j=1, j\neq i}^{t} \frac{0 - x_j}{x_i - x_j}) Y_i \cdot \quad (21)$$

(2) Combine all sub-signatures into a threshold authenticated encryption signature.

$$s = \sum_{i=1}^{t} s_i \ . \quad (22)$$

(3) Send the threshold authenticated encryption signature $(s, r_1, r_2, \ldots, r_t)$ to the designated verifier U_v via a public channel.

C. Message recovery phase

After the verifier U_v receives the signature $(s, r_1, r_2, \ldots, r_t)$, U_v recovers the message blocks $\{m_1, m_2, \ldots, m_t\}$ by performing the following steps.

(1) Compute the session key Z.

$$Z = sY_v + (h(r_1 \| r_2 \| \cdots \| r_t) \cdot x_v) Y_s = (x_Z, y_Z) \cdot \quad (23)$$

(2) Recover the message blocks $\{m_1, m_2, \ldots, m_t\}$.

$$m_i = r_i \cdot h(Y_s \| i \| x_Z)^{-1} \bmod p. \quad (24)$$

(3) Validate the redundancy attached to the message blocks m_i's. If they are valid, then all the message blocks can be combined into the whole message m.

V. ANALYSIS OF THE PROPOSED SCHEME

In the following, we will make some analysis on the propose scheme. On one hand, we will show that our scheme is designed correctly. On the other hand, some cryptanalysis demonstrate that the scheme meets the security properties.

A. Correctness analysis

We show the correctness of the proposed scheme through Theorem 1.

Theorem 1. In the proposed authentication signature scheme, the clerk can verify the sub-signature (r_i, s_i) using Eq. (21) during the signature combination phase.

Proof. From Eq. (20) , we have

$$x_{B_i} \cdot b_i = s_i + h(r_1 \| r_2 \| \cdots \| r_t) \cdot f(x_i) \cdot \prod_{j=1, j\neq i}^{t} \frac{0 - x_j}{x_i - x_j} \bmod q. \quad (25)$$

Thus, we can obtain

$$x_{B_i} \cdot b_i G = s_i G + h(r_1 \| r_2 \| \cdots \| r_t) \cdot f(x_i) \cdot \prod_{j=1, j\neq i}^{t} \frac{0 - x_j}{x_i - x_j} G,$$

$$= s_i G + (h(r_1 \| r_2 \| \cdots \| r_t) \cdot \prod_{j=1, j\neq i}^{t} \frac{0 - x_j}{x_i - x_j}) Y_i \cdot$$

From Eq. (13), we have $x_{B_i} \cdot b_i G = x_{B_i} B_i$. Therefore, Eq. (21) holds. □

Theorem 2. If all the participants in the scheme follow the protocol, the designated verifier U_v can recover all the message blocks via Eq. (24).

Proof. Multiplying Eq. (25) with Y_v, we obtain

$$x_{B_i} \cdot b_i Y_v = s_i Y_v + h(r_1 \| r_2 \| \cdots \| r_t) \cdot f(x_i) \cdot \prod_{j=1, j\neq i}^{t} \frac{0 - x_j}{x_i - x_j} Y_v,$$

$$\sum_{i=1}^{t} x_{B_i} b_i Y_v = \sum_{i=1}^{t} s_i Y_v + h(r_1 \| r_2 \| \cdots \| r_t) \cdot [\sum_{i=1}^{t} f(x_i) \prod_{j=1, j\neq i}^{t} \frac{0 - x_j}{x_i - x_j}] \cdot Y_v$$

From Eq. (13), we have

$$\sum_{i=1}^{t} Z_i = \sum_{i=1}^{t} s_i Y_v + h(r_1 \| r_2 \| \cdots \| r_t) \cdot [\sum_{i=1}^{t} f(x_i) \prod_{j=1, j\neq i}^{t} \frac{0 - x_j}{x_i - x_j}] \cdot Y_v$$

Thus, through Eq. (18), we can obtain

$$Z = \sum_{i=1}^{t} s_i Y + h(r_1 \| r_2 \| \cdots \| r_t) \cdot [\sum_{i=1}^{t} f(x_i) \prod_{j=1, j\neq i}^{t} \frac{0 - x_j}{x_i - x_j}] \cdot Y_v \cdot$$

From Eq. (1), we have

$$Z = sY + h(r_1 \| r_2 \| \cdots \| r_t) \cdot e_0 Y_v \cdot$$

Therefore, the session key Z can be computed through Eq. (23):

$$Z = sY_v + (r \cdot x_v) Y_s = (x_Z, y_Z) \cdot$$

From Eq.(19), it is easy to know that the message blocks can be recovered through Eq. (24). □

B. Security analysis

We first review two assumptions.

Definition 1 Consider a point group $E(F_p)$ of an elliptic curve E over F_p and a generator point $G \in E(F_p)$ with the large prime order q. Given $aG \in E(F_p)$, to compute the discrete logarithm a is difficult, which is called Discrete Logarithm (DL) Assumption of the elliptic curve.

Definition 2 Consider a point group $E(F_p)$ of an elliptic curve E over F_p and a generator point $G \in E(F_p)$ with the large prime order q. The assumption that the following two probability distributions are computationally indistinguishable is called Decisional Diffie-Hellman (DDH) assumption of the elliptic curve.

- (aG, bG, abG), where a and b are randomly and independently chosen from Z_q^*
- (aG, bG, cG), where a,b,c are randomly and independently chosen from Z_q^*.

Then, we show that the proposed scheme is secure under discrete logarithm assumption (DL) of the elliptic curve [12,13,17,18] and Decisional Diffie-Hellman assumption (DDH). The improved scheme inherits the security features of CHC scheme. Therefore, the proposed authenticated signature scheme can resist all the five attacks mentioned in [2]. In the following, we show that the novel scheme can satisfy robustness, confidentiality, unforgeability, integrity, authenticity and non-repudiation.

Robustness: In CHC scheme, when a certain signer u_i wants to deviate the protocol during signature generation phase, u_i must select a random integer b_i in F_q^* and computes $B_i = b_i\ G = (x_{B_i}, y_{B_i})$. If u_i uses a different integer b_i' in F_q^* to compute z_i' as in Section 3.2, ($x_{B_i}B_i$, Y_v, z_i') will not be an example of Diffie-Hellman distribution. Under DDH assumption, any actual signer in CHC scheme cannot find that ($x_{B_i}B_i$, Y_v, z_i') is not an example of Diffie-Hellman distribution. However, in the proposed scheme, any actual signer can identify that ($x_{B_i}B_i$, Y_v, z_i') is not an example of Diffie-Hellman distribution. This is because during the sub-signature generation phase, when u_i publishes (B_i, z_i) in the actual signer group, u_i has to send (B_i, z_i, R_i, R_{vi}, s_i') to the other signers. From Eq. (15) and Eq. (16), it is easy to know that (B_i, z_i, R_i, R_{vi}, s_i') is a variant of the Schnorr signature [19] on (B_i, z_i). On discrete logarithm assumption (DL), it is secure against forgery attack in the random oracle model [20]. Moreover, Eq.(15) and Eq. (16) show that ($x_{B_i}B_i$, Y_v, z_i) must come from the Diffie-Hellman distribution. Thus, the proposed scheme can resist the first attack of Section 3.2. In fact, if any signer can identify that ($x_{B_i}B_i$, z_i) have the same discrete logarithms on the generator element G. So another suggested measure to resist the first attack of Section 3.2 is that all the actual signer use non-interactive knowledge proof of the equality of discrete logarithms [21] to demonstrate $x_{B_i}B_i$ with basis G and z_i with Y_v have the same discrete logarithm. Obviously, it will add some more workload.

So, any signer who deviates from the protocol can be identified. The proposed scheme is robust.

Confidentiality: If an attacker obtains the authenticated signature (s, r_1, r_2, …, r_t), it is computational infeasible to get any information about message blocks m_i with the secure hash function h(). The proposed scheme is still secure against chosen message attacks. Because every time the actual signers use random integer b_i to produce the session key Z in Eq.(13). So different sessions have different X_z's. Even if the attacker can get some X_z's. But the attacker cannot use X_z's to recover the message in other sessions.

Now consider known message blocks attack against the proposed scheme. Because the proposed scheme applies the division-of-labor signature technique, it is necessary that we consider chosen message block attack in the proposed scheme. For example, the attacker obtains the i-th message block m_i and r_i. Although the attacker can work out $h(i||X_z)=r_i/m_i$, the attacker still cannot recover another message block. The attacker only use r_j and $h(j||X_z)$ and can recover the j-th message block m_j. However, $h(i||X_z) \neq h(j||X_z)$. Moreover, the attacker cannot compute $h(j||X_z)$ from $h(i||X_z)$.

The analysis demonstrates that any information cannot be derived from the authenticated cipher-text by any one except the designated verifier.

Unforgeability: In the propose scheme, any signers who deviate from the protocol will be identified by other signers. In a similar analysis of confidentiality, the proposed scheme is secure against chosen message attack. In addition, the improved scheme can resist the insider attack in Section 3.2. When a certain signer u_i requires that he wants to re-sign its message block and impersonate other signer u_j, the signer must run all the steps during the sub-signature generation phase and generate s_j''. In essence, s_j'' is also a variant of the Schnorr signature on (B_j, z_j). When u_i produces s_j'', s_j'' will not satisfy the signature verification equation Eq. (16). Therefore, the impersonation attack will fail.

Integrity: In the proposed scheme, the designated verifier can identify if the message is valid. After the verifier recovers the message blocks, he can validate them by the redundancy attached to the message blocks m_i. Next, if an attacker intercepts the authenticated signature, changes the order of the r_i's and sends them to the designated verifier, the verifier can determine whether the signature blocks have been rearranged by the redundancy associated with the message blocks.

Authenticity: After the designated verifier recovers the message blocks $\{m_1, m_2, \ldots, m_t\}$, if the redundancy shows that the message blocks m_i's are valid, the designated verifier is sure that the signer group with public key Y_s is the actual signer group.

Nonrepudiation: The authenticity and unforgeabilitiy of the proposed scheme imply that the proposed scheme satisfies nonrepudiation.

C. Performance analysis

In [2], the author considered these authentication encryption schemes by Tseng and Jan [1], Hwang et al. [7] and Lee and Chang [8]. The detailed analysis showed that the authentication encryption scheme [2] had better properties. Since the proposed authentication encryption scheme is based on CHC scheme, it holds the same advantages over those schemes in [1], [7] and [8]. We omitted the similar analysis here.

In the following, we use these notations to analyze the efficiency of the proposed authentication encryption scheme. We will ignore some light-weight operations such as modular addition and subtraction in F_q^* and F_p^*.

This is because these operations cost much less time than the following operations.

- $|\bullet|$: the bit length.
- T_H: the time of executing the one-way hash function h().
- T_F: the time of executing the one-way hash function F().
- T_{MUL}: the time of modulus multiplication operation in F_p^* or F_q^*.
- T_{EXP}: the time of modulus exponentiation operation in F_q^* or F_p^*.
- T_{INV}: the time of modulus inverse element operation in F_q^* or F_p^*.
- $T_{EC\text{-}MUL}$: the time of modulus multiplication operation in the elliptic curve point group.
- $T_{EC\text{-}ADD}$: the time of modulus addition operation in the elliptic curve point group.

Of the authentication encryption schemes, Tseng and Jan's scheme [1] has less communication and lower computational complexity. Now, we compare our proposed scheme in terms of performance efficiency with Tseng and Jan's scheme.

As mentioned in Section II, F_p is a finite field with a large prime order p, $E(F_p)$ is a point group of an elliptic curve E over F_p and a generator point $G \in E(F_p)$ with the large prime order q. For convenience, we further assume that the system parameters are set up as follows: p is a 1024-bit prime, q is a 160-bit integer and the modulus exponentiation is about 160-bit integer. Tseng and Jan's scheme is based on an exponentiation operation, while the proposed scheme is based on the elliptic curve multiplication and addition operations. Therefore, in order to estimate the efficiency in performance of the two schemes, the three operation units, T_{EXP}, $T_{EC\text{-}MUL}$, and $T_{EC\text{-}ADD}$, must be simplified to the unit of the modulus multiplication operation. Performance simulation results in literature demonstrate that the different operation units can be changed into the modulus multiplication one: one T_{EXP} is about 240 times of one T_{MUL}, one $T_{EC\text{-}MUL}$ is about 29 times of one T_{MUL} and one $T_{EC\text{-}ADD}$ is times of one 0.12 T_{MUL}.

Now, we first consider the communication cost. In Tseng and Jan's scheme, the signature blocks are defined as $(r, s, r_1, r_2, \cdots, r_t)$, while the communication cost is $|q|+(t+1)|p|$. Although the signer in the improved scheme is a group, the authenticated encryption blocks are less one element than that of Tseng and Jan's scheme. In essence, the signature blocks in our scheme are signature $(s, r_1, r_2, \ldots, r_t)$ and the communication cost is $|q|+t|p|$. In other words, the communication cost of our scheme does not increase as the number of the signers increases.

Next, consider the computational complexities of the signature generation phase and the message recovery phase. As we know, the signer is a group in our scheme. However, when we compare the computational complexities of the signature generation phase and the message recovery phase in the two authenticated encryption schemes, the required amount of computation in the signature generation phase and the message recovery phase will be compared only for every message block m_i.

TABLE I. PERFORMANCE COMPARISONS

	Tseng and Jan's scheme	The proposed scheme
Signature generation phase (in different operation form)	$1T_{EXP}+2\ T_{MUL}+1\ T_H+1T_F$	$4\ T_{MUL}+4\ T_H+7\ T_{EC\text{-}MUL}$
Message recovery phase(in different operation form)	$3T_{EXP}+3\ T_{MUL}+1\ T_H+1T_F+1T_{INV}$	$2\ T_{MUL}+1\ T_H+2\ T_{EC\text{-}MUL}+1T_{INV}+1T_{EC\text{-}ADD}$
Signature generation phase (in one unit form)	$2\ 42T_{MUL}+1\ T_H+1T_F$	$207T_{MUL}+4\ T_H$
Message recovery phase (in one unit form)	$722T_{MUL}+1\ T_H+1T_F+1T_{INV}$	$60.12\ T_{MUL}+1\ T_H+1T_{INV}$
Total time complexity	$964T_{MUL}+2\ T_H+2T_F+1T_{INV}$	$267.12\ T_{MUL}+5\ T_H+1T_{INV}$

Table I demonstrates the performance comparisons between our proposed scheme and Tseng and Jan's scheme in terms of the computational costs for the signature generation phase, the message recovery phase and the total time complexity, respectively. From Table I, it is obvious that our scheme has better performance in comparison with Tseng and Jan's scheme.

Then, we compare our scheme with CHC scheme in terms of the communication cost and the computational costs. In CHC scheme, the signature blocks are defined as $(r, s, r_1, r_2, \cdots, r_t)$, while in the proposed scheme, the signature blocks are signature $(s, r_1, r_2, \ldots, r_t)$. The communication cost of the proposed scheme is less one $|p|$ bits than that of CHC scheme. As for the signature generation phase, our scheme adds 3 T_h and 5 $T_{EC\text{-}MUL}$ more than CHC scheme. However, CHC scheme suffers from some weaknesses mentioned in Section III. Our scheme has the same time complexity as CHC scheme in the message recovery phase. Moreover, the proposed scheme overcomes the security weaknesses of CHC scheme and meets all the properties of a secure authentication encryption signature scheme.

VI. CONCLUSION

A (t, n) threshold authenticated encryption scheme allows any t or more signers to generate an authenticated encryption on a message so that only the designated verifier can recover the message and verify the message. Compared with the conventional encryption-then-signature schemes, threshold authenticated encryption schemes hold more performance and security properties. Recently, Chung et al. [2] proposed an efficient (t, n) threshold authenticated encryption scheme by applying a division-of-labor signature technique. Chung et al.'s

authenticated encryption scheme is more efficient than the previous authenticated encryption schemes. However, the paper demonstrates that there exists a design defect in Chung et al.'s scheme. Moreover, Chung et al.'s scheme is not robust. Based on elliptic curve cryptosystem and Chung et al.'s scheme, an improved authenticated encryption scheme is proposed. A detailed analysis shows that the proposed authenticated encryption scheme removes the above-mentioned weaknesses and the proposed scheme is secure. Moreover, compared to Tseng and Jan's scheme, our scheme is more efficient.

ACKNOWLEDGMENT

The author would like to thank the support from the Opening Foundation of Key Lab of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University (09A003) and the National Natural Science Foundation of China (10961013 and 10701040). The author thanks the valuable suggestion from some reviewers and useful discussions with my colleagues.

REFERENCES

[1] Y. M. Tseng and J. K. Jan, "An efficient authenticated encryption scheme with message linkages and low communication costs," *Journal of information science and engineering*, 18(1), 2002, pp.41-46.

[2] Y. F. Chung, K. H. Huang, T. S. Chen, "Threshold authenticated encryption scheme using labor-division signature," *Computer Standards & Interfaces* 31(2), 2009, pp.300-304.

[3] K. Nyberg and R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery," in Proceeding 1st ACM conference on computer and communications security, Fairfax, VA, 1993, pp.58-61.

[4] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm," in *Advances in cryptology—EUROCRYPT'94*, Springer-Verlag, Berlin, 1994, pp.175-190.

[5] P. Horster, M. Michels, and H. Petersen, "Authenticated encryption schemes with low communication costs," *Electronics letters*, 30, 1994, pp.1212-1213.

[6] W. B. Lee and C. C. Chang, "Authenticated encryption scheme without using a one way Function," *Electronics letters*, 31, 1995, pp.1656-1657.

[7] S. J. Hwang, C. C. Chang, and W. P. Yang, "Authenticated encryption schemes with message linkage," *Information processing letters*, 58, 1996, pp.189-194.

[8] W. B. Lee and C. C. Chang, "Authenticated encryption schemes with linkage between message blocks," *Information processing letters*, 63, 1997, pp.247-250.

[9] Y. M. Tseng, J. K. Jan, and H. Y. Chien, "Authenticated encryption schemes with message linkages for message flows," *Computers and electrical engineering*, 29, 2003, 101-109.

[10] Y. Desmedt and Y. Frankel, "Threshold Cryptosystems," in *Proc. Advance in Cryptology—CRYPTO'89,* LNCS 435, Springer-Verlag, 1989, pp.307-315.

[11] T.P. Pedersen, "A threshold cryptosystem without a trusted party," in *Advances in Cryptology—EUROCRYPT'91*, LNCS 547, Springer-Verlag, 1991, pp. 522–526.

[12] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, 48, 1987, pp.203-209.

[13] V. Miller, "Uses of elliptic curves in cryptography," in *Advances in cryptology—CRYPTO'85*, Springer-Verlag, 1985, pp.417-426.

[14] K. Nyberg and R. A. Ruppel, "Message recovery for signature scheme based on the discrete logarithm problem," *Designs codes and cryptography*, 7,1996, pp.61-81.

[15] C. C. Lin and C. S. Laih, "Cryptanalysis of Nyberg-Ruppel's message recovery scheme," *IEEE communication letters*, 4(7), 2000, pp.231-232.

[16] C. M. Li, T. Hwang and N. Y. Lee, "Remark on the threshold RSA signature scheme," in *Advances in Cryptology—CRYPTO'93*, LNCS Vol. 773, Springer-Verlag, 1993, pp.413-420.

[17] N. Koblitz. *Algebraic aspects of cryptography*. Springer, New York, 1998.

[18] N. Koblitz, A. Menezes, S. Vanstone, "The state of elliptic curve cryptography," *Designs, Codes and Cryptography*, 19, 2000, pp.173-193.

[19] Schnorr, C.P. , "Efficient signature generation by smart cards," *Journal of Cryptology* 4(3), 1991, pp.161-174.

[20] Pointecheval, D., Stern, J., "Security of Proofs for Signatures," in *Advance in Cryptology–EUROCRYPTO'96*, LNCS 1070, Springer-Verlag, 1996, pp. 387-398.

[21] J. Camenisch, M. Stadler, "Efficient group signature schemes for large groups," in *Advances in Cryptology-CRYPTO'97*, Vol.1294, Springer Verlag, 1997, pp.410-424.

[22] W. B. Lee and C. C. Chang, "(t, n) threshold digital signature with traceability property," Journal of Information Science and Engineering 15(5), 1999, pp.669-678.

[23] C.T. Wang, C. H. Lin, C.C. Chang., "Threshold signature schemes with traceable signers in group communications," Computer Communications 21(8), 1998, pp.771-776.

[24] C. Park, K. Kurosawa, "New ElGamal type threshold digital signature scheme," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E79-A(1), 1996, pp.86-93.

[25] S. K. Langford, "Threshold DSS signature without a trusted party," in *Advances in Cryptology-CRYPTO'95*, Springer Verlag, 1995, pp.397-409.

Zuowen Tan, born in Yiyang, Hunan, P.R. China, 1967. He received the M.S. degree in Fundamental Mathematics from Xiangtan University in 2002, and the Ph.D. degree in Applied Mathematics from Institute of Systems Science, Academy of Mathematics and System Science, Chinese Academy of Sciences in 2005.

He is currently an associate professor at Department of Computer Science & Technology, School of Information Management, Jiangxi University of Finance & Economics. He has published over 30 papers on information security in some international conferences and journals. His current research interests include e-commerce security, information security and cryptography.

Dr. Tan was Committee members of some international conferences on information security and reviewers of some international journals. Dr. Tan has ever won the Dean Scholarship of Chinese Academy of Sciences and the Dean Scholarship of Academy of Mathematics and Systems Science, respectively.