

A Threshold Authenticated Encryption Scheme Based on Elliptic Curve Cryptosystem

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—A (t,n) threshold authenticated encryption scheme allows more than t signers to generate an authenticated cipher-text for a message and only the designated verifier can verify the message. Recently, Chung et al. [1] proposed a (t, n) threshold authenticated encryption scheme by applying a division-of-labor signature technique. However, we showed that the scheme has a design flaw. Then, we proposed a new authenticated encryption scheme based on elliptic curve cryptosystem. The new authenticated encryption scheme is more efficient.

Index Terms—encryption, authentication, threshold signature, elliptic curve cryptosystem

I. INTRODUCTION

The authenticated encryption scheme is first introduced by Nyberg and Rueppel [2]. 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 [3,4]. More focuses are on reducing the communication and operation costs [5, 6].

Based on threshold cryptosystems [7,8] and Tseng and Jan's [9] authenticated encryption scheme, Chung et al. [1] 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 [1], then all sub-signatures on all the message blocks are combined into one group signature for the whole message.

Based on the elliptic curve cryptosystems [10,11], the (t, n) threshold authenticated encryption scheme in [1] combines the characteristics of both message linkage and division-of-labor.

Manuscript received July18, 2009; revised August 28, 2009; accepted October 1, 2009.

Supported by the National Natural Science Foundation of China (10961013 and 10701040).

Corresponding author: Zuowen Tan

However, the paper demonstrates that there exists a design defect. An improved authenticated encryption scheme based on elliptic curve cryptosystem is proposed.

The rest of the paper is organized as follows. Chung et al.'s scheme is briefly reviewed and analyzed in Section 2. Section 3 and Section 4 propose a new authenticated signature scheme and give a detailed analysis of the new scheme, respectively. Section 5 concludes.

II. REVIEW AND ANALYSIS OF CHUNG ET AL.'S SCHEME

By $\{u_1, u_2, \dots, u_n\}$, we denotes the signer group with n signers where u_i is the i -th signer ($i=1,2, \dots, n$). 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. Chung et al.'s 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 $F_p[x]$:

$$f(x) = e_0 + e_1x + e_2x^2 + \dots + e_{t-1}x^{t-1}. \quad (1)$$

- (2) Take e_0 as the signer group's private key and compute $Y_s = e_0G$ 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 $\{u_i | i=1,2, \dots, t\}$ jointly sign a message m . The t signers collaborate to divide the message into t connected message blocks $\{m_1, m_2, \dots, m_t\}$, where $m_i \in [1, p-1]$ ($i=1,2, \dots, t$). Each m_i has some redundancy to protect the scheme against a possible forgery attack [12, 13]. Each u_i ($i=1,2, \dots, t$) 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 $z_i = (b_i \cdot x_{B_i}) Y_v = (x_{z_i}, y_{z_i})$.

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

(4) Compute B and the session key Z

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

(5) Compute and publish the sub-signature (r_i, s_i)

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

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.

$$r = \sum_{i=1}^t r_i \pmod p, s = \sum_{i=1}^t s_i \pmod q. \quad (5)$$

(3) Send the signature (r, s, r_1, r_2, \dots) to the designated verifier U_v via a public channel.

C. Message recovery phase

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

(1) Compute the session key Z shared with the actual

signer group $\{u_i | i=1, 2, \dots, t\}$.

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

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

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

(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.

Although Chung et al. discussed security of Chung et al.'s scheme, there is a design error in Chung et al.'s scheme. Even if all the actual signers follow the protocol, Eq.(6) would not hold. The proof of Theorem 1 in [1] is also wrong. So, the verifier U_v can not recover the right message $m_i (i=1, 2, \dots, t)$ 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

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

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 Chung et al.'s scheme, the actual signer $u_i (i=1, 2, \dots, t)$ 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:

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

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

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

III. IMPROVEMENT ON CHUNG ET AL.'S 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 $\{u_1, u_2, \dots, u_n\}$ 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 $E(F_p)$ with the large prime order q . Then, SA generates the users' public/private keys as in Chung et al.'s scheme.

B. Signature generation phase

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

Each signer $u_i (i=1, 2, \dots, t)$ generates the signature for 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

$$R_i = k_i G, R_{vi} = k_i Y_v, \quad (12)$$

$$s_i' = k_i - h(R_i \| R_{vi} \| B_i \| z_i) x_{B_i} b_i \pmod q. \quad (13)$$

$$s_i'' = k_i - h(i \| R_i \| R_{vi} \| B_i \| z_i) f(x_i) \pmod q. \quad (14)$$

(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:

$$s_i' G = R_i - h(R_i \| R_{vi} \| B_i \| z_i) x_{B_i} B_i, \quad (15)$$

$$s_i' Y_v = R_{vi} - h(R_i \| R_{vi} \| B_i \| z_i) z_i, \quad (16)$$

$$s_i'' G = R_i - h(i \| R_i \| R_{vi} \| B_i \| z_i) Y_i. \quad (17)$$

If the 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:

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

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

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

(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:

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

(2) Combine all sub-signatures into a threshold authenticated encryption signature $s = \sum_{i=1}^t s_i$.

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

C. Message recovery phase

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

(2) Compute the session key Z .

$$Z = s Y_v + (h(r_1 \| r_2 \| \dots \| r_t) \cdot x_v) Y_s = (x_Z, y_Z). \quad (22)$$

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

$$m_i = r_i \cdot h(Y_s \| i \| x_Z)^{-1} \pmod p. \quad (23)$$

(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 .

IV. 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.

D. Correctness analysis

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

Proof. From Eq. (20), we have

$$x_{B_i} \cdot b_i = s_i + h(r_1 \| r_2 \| \dots \| r_t) \cdot f(x_i) \cdot \prod_{j=1, j \neq i}^t \frac{0 - x_j}{x_i - x_j} \pmod q. \quad (24)$$

Thus, we can obtain

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

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

Therefore, Eq. (21) holds. \square

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. (23).

Proof. Multiplying Eq. (24) with Y_v , we obtain

$$\begin{aligned} \sum_{i=1}^t x_{B_i} b_i Y_v &= \sum_{i=1}^t s_i Y_v + h(r_1 \| r_2 \| \dots \| r_t) \cdot \left[\sum_{i=1}^t f(x_i) \prod_{j=1, j \neq i}^t \frac{0 - x_j}{x_i - x_j} \right] Y_v, \\ \sum_{i=1}^t z_i &= \sum_{i=1}^t s_i Y_v + h(r_1 \| r_2 \| \dots \| r_t) \cdot \left[\sum_{i=1}^t f(x_i) \prod_{j=1, j \neq i}^t \frac{0 - x_j}{x_i - x_j} \right] Y_v. \end{aligned}$$

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

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

$$Z = s Y + h(r_1 \| r_2 \| \dots \| r_t) \cdot e_0 Y_v.$$

So, the session key Z can be computed through Eq. (22):

$$Z = s Y_v + (r \cdot x_v) Y_s = (x_Z, y_Z).$$

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

E. Performance analysis

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.

- $| \cdot |$: 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 $F()$.
- $T_{MUL}/T_{EXP}/T_{INV}$: the time of modulus multiplication/ exponentiation/ inverse operation in F_p^* or F_q^* .
- T_{EC-MUL}/T_{EC-ADD} : the time of modulus multiplication/ addition operation in the elliptic curve point group.

Now, we compare our proposed scheme in terms of performance efficiency with Tseng and Jan's scheme [9] which has less communication cost and lower computational complexity in the literature.

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-MUL} , and T_{EC-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-MUL} is about 29 times of one T_{MUL} and one T_{EC-ADD} is times of one $0.12 T_{MUL}$.

Now, we first consider the communication cost. In Tseng and Jan's scheme [9], the signature blocks are defined as $(r, s, r_1, r_2, \dots, r_t)$, 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 $(s, r_1, r_2, \dots, r_t)$ 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 . The total time cost of Tseng and Jan's scheme is $964T_{mul}+2 T_h+ 2T_F + 1T_{INV}$, while the total time of our

new scheme is about $267.12 T_{mul}+5 T_h+ 1T_{INV}$. So, our scheme has better performance.

V. 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. Chung et al. applied a division-of-labor signature technique and constructed an efficient (t,n) threshold authenticated encryption scheme. However, the paper demonstrates that there exists a design defect in their scheme. A new authenticated encryption scheme is proposed. The proposed authenticated encryption scheme removes the above-mentioned weaknesses and more efficient than Tseng and Jan's scheme.

REFERENCES

- [1] 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.
- [2] 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.
- [3] S. J. Hwang, C. C. Chang, and W. P. Yang, "Authenticated encryption schemes with message linkage," *Information processing letters*, 58, 1996, pp.189-194.
- [4] W. B. Lee and C. C. Chang, "Authenticated encryption schemes with linkage between message blocks," *Information processing letters*, 63, 1997, pp.247-250.
- [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] Y. Desmedt and Y. Frankel, "Threshold Cryptosystems," in *Proc. Advance in Cryptology—CRYPTO'89*, LNCS 435, Springer-Verlag, 1989, pp.307-315.
- [8] T.P. Pedersen, "A threshold cryptosystem without a trusted party," in *Advances in Cryptology—EUROCRYPT'91*, LNCS 547, Springer-Verlag, 1991, pp. 522-526.
- [9] 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.
- [10] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, 48, 1987, pp.203-209.
- [11] V. Miller, "Uses of elliptic curves in cryptography," in *Advances in cryptology—CRYPTO'85*, Springer-Verlag, 1985, pp.417-426.
- [12] 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.
- [13] C. C. Lin and C. S. Lai, "Cryptanalysis of Nyberg-Ruppel's message recovery scheme," *IEEE communication letters*, 4(7), 2000, pp.231-232.