A Robust Collaborative Threshold Authenticated Encryption Scheme Based on Message Blocking

Zhen Chen*†, Wenfang Zhang*† and Xiaomin Wang*
*School of Information Science and Technology, Southwest Jiaotong University
†Key Laboratory of Information Security and National Computing Grid, Southwest Jiaotong University
Chengdu, China
Email:bk20092301@my.swjtu.edu.cn

***Abstract*—In recent years, some collaborative threshold authenticated encryption schemes were put forward to ease the workloads of the individual signers. Unfortunately, the original scheme was found to have design flaws in its signature generation phase, however the improvements of the original one are all proved to be inefficient. In order to remedy the security flaws and improve the performance, a novel robust collaborative threshold authenticated encryption scheme is proposed in this paper. Based on the elliptic curve cryptography and the message linkage technology, this scheme can realize efficient encryption and authentication of large messages. Analysis shows that the proposed scheme is theoretically correct and has better performance. The scheme can be further applied into distributed environments, such as cloud storage and computing networks, dynamic alliance of enterprises and virtual organizations.**

***Keywords*-Authenticated encryption; Threshold signature; Elliptic curve cryptography; Message linkage;**

I. INTRODUCTION

In 1993, Nyberg and Rueppel [1] presented the authenticated encryption scheme firstly based on the difficulty of resolving the discrete logarithm problem. In this scheme, the message sender generates an authenticated cipher-text and only the specified recipient can verify the signature and recover the original message from the cipher-text. Subsequently, several authenticated encryption schemes were presented [2], [3]. As compared with the traditional digital signature and encryption schemes, the authenticated encryption schemes can simultaneously provide both confidentiality and authenticity for the transmitted messages and have higher efficiency with respect to communication and computation costs.

In some group-oriented application environments, the secret sharing technology was introduced into the authenticated encryption schemes, and correspondingly, the (*t, n*) threshold authenticated encryption schemes were put forward [4]. In such threshold schemes, to generate a group authenticated cipher-text, every participant signer should individually encrypt and generate his partial signature on the whole message. This makes the signers total workload heavier since each participant may have different responsibilities and may not be capable of examining the entire message. In order to decrease the workload of each participant, Chung et al. [5] proposed a specific (*t, n*) threshold authentication encryption scheme based on the techniques of labor-division and message linkage as well as the elliptic curve cryptosystem (ECC)[6]. Each participant just needs to sign the message block allocated to him, and the group signature is generated by combining all the individual signatures together. However, Chung et al.'s scheme is not theoretically correct owing to its flaws in the designing of the message recovery formulas. Additionally, the Chung's scheme fails to resist some security attacks such as the malicious signer attack mentioned in the literature [7]. In order to remedy the flaws exited in the Chung's scheme, Tan successively proposed two improved schemes [7], [8]. Tan's first scheme in [7] (for convenience, it will be denoted as Tan's scheme 1 hereafter) is based on the hardness of resolving the discrete logarithm problem over GF(p) (DLP), and his second scheme [8] (for convenience, it will be denoted as Tan's scheme 2 hereafter) is based on the hardness of resolving the discrete logarithm problem over elliptic curve (ECDLP). These two schemes can overcome the design flaws in Chung's scheme by modifying the signature and verification equations. However, the signers' workload and the overall computation and communication costs are increased.

In this paper, a more efficient and secure (*t, n*) threshold authenticated encryption scheme using collaborative signature and message linkage technology is proposed. Security analysis and performance evaluation show that the proposed scheme is theoretically correct and can resist all the existing attacks. Furthermore, it needs less communication and computation costs than the former schemes in [5], [7], [8]. This new scheme can be applied to realize large messages' encryption and authentication in distributed environments, such as cloud storage and computing networks, dynamic alliance of enterprises and virtual organizations.

This paper is composed of four sections. Section 1 gives the introduction. Section 2 proposes a new robust collaborative threshold authenticated encryption scheme. Section 3 analyses the correctness, performance and security of the proposed scheme. Section 4 gives the conclusions.

II. Proposed collaborative (t, n) threshold authenticated encryption scheme

A new robust threshold authenticated encryption scheme is presented in this section. In the new scheme, $u_1, u_2, \ldots, u_n$ indicates a group of n signer where u_k is the *k*-th signer (*k*=1, 2,..., *n*) with a corresponding identifier x_k, and U_v denotes the specified recipient. The proposal is composed of three phases: system initialization phase, authenticated signature generation phase, and message recovery phase which will be described in detail as follows.

A. System initialization phase

A trusted system authority called SA selects the required parameters: two large prime integers *p* and *q* where *q* is a factor of *p*-1, a finite field F_p, a *q*-ordered point group G_1 of an elliptic curve *E* over F_p with its generator point *P*, and a one-way hash function $h() : \{0,1\}^* \rightarrow F_p^*$. Then, SA generates the participants' public key and the private key by the following steps.

1) : Chooses an integer group G_2 of order *q* and generates a corresponding bilinear pairing $e : G_1 \times G_1 \rightarrow G_2$.

2) : Selects a secret polynomial in a polynomial ring $F_p[x]$ randomly:

$$f(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1} \tag{1}$$

where *t* is the threshold value. Then SA takes $f(0) = a_0$ as the signer group's private key and computes the corresponding public key $Y_s = a_0 P$.

3) : Computes the private key $f(x_k)$ and the corresponding public key $Y_k = f(x_k)P$ for each participant.

4) : Selects a random number x_v as the private key of the specified recipient and computes his public key $Y_v = x_v P$. The parameters $p, q, E, G_1, G_2, e, h, Y_s, Y_k$, and Y_v are then declared publicly.

B. Authenticated signature generation phase

Suppose that the actual signer group U_s consists of *t* individuals such as $u_1, u_2, \ldots, u_t$ and there is a message *m* waiting to be signed. Each signer u_k of the group U_s takes the subsequent steps to sign the message.

1) : Cooperates with other signers to divide the message *m* into *t* sub-blocks as $m_1, m_2, \ldots, m_t$, where $m_k \in [1, p-1](k = 1, 2, \ldots, t)$. Note that each block m_k should have a certain redundancy in sequence so as to resist the possible forgery attack[9].

2) : Selects an integer b_k in F_q^* randomly and computes the values of B_k, z_k as follows:

$$B_k = b_k P = (x_{B_k}, y_{B_k}) \tag{2}$$

$$z_k = (b_k \cdot x_{B_k}) Y_v = (x_{z_k}, y_{z_k}) \tag{3}$$

3) : Sends both B_k and z_k secretly to the other signers in U_s.

4) : Generates the session key *Z* between the signer group U_s and the verifier U_v by the following equation:

$$Z = \sum_{k=1}^{t} z_k = (x_Z, y_Z) \tag{4}$$

5) : Computes the signature (r_k, s_k) of the message block m_k as follows:

$$r_k = m_k \cdot h(k||x_Z) \ mod \ p \tag{5}$$

$$s_k = x_{B_k} \cdot b_k - (r_k + f(x_k) \cdot \prod_{\substack{i=1 \\ i \neq k}}^{t} \frac{0 - x_i}{x_k - x_i}) \ mod \ q \tag{6}$$

where $||$ denotes the concatenation operator. Then broadcasts (r_k, s_k) to the other signers.

6) : Sends both r_k and s_k to the clerk u_c. The clerk could be anyone of the signer group.

Once receiving all the signature blocks (r_k, s_k) and the corresponding (B_k, z_k), u_c can check the validity of each block and then combines all blocks into a cipher-text as follows.

1) : Checks if the following equality holds after receiving (B_k, z_k):

$$e(P, z_k) \stackrel{?}{=} e(B_k, x_{B_k} Y_v) \tag{7}$$

Once the above equality holds, u_c goes to the next step.

2) : Verifies the validity of each signature block (r_k, s_k) by checking if the following equality holds:

$$x_{B_k} B_k \stackrel{?}{=} s_k P + r_k P + \prod_{\substack{i=1 \\ i \neq k}}^{t} \frac{0 - x_i}{x_k - x_i} Y_i \tag{8}$$

If the equality holds, the signature block is actually generated by the corresponding signer u_k. Then, u_c executes the next step.

3) : Generates a group signature for the whole message.

$$r = \sum_{k=1}^{t} r_k \ mod \ q \quad , \quad s = \sum_{k=1}^{t} s_k \ mod \ q \tag{9}$$

4) : Sends the signature $(r, s, r_1, r_2, \ldots, r_t)$ to the specified verifier U_v.

C. Message recovery phase

First of all, the verifier U_v verifies the validity of the signature $(r, s, r_1, r_2, \ldots, r_t)$, and then recovers the message *m* by the following steps:

1) : Calculates the session key *Z* shared with the actual signer group U_s by the following equation.

$$Z = sY_v + rY_v + x_v Y_s = (x_Z, y_Z) \tag{10}$$

2) : Retrieves the sub-message $m_1, m_2, \ldots, m_t$ as follows:

$$m_k = r_k \cdot h(k||x_Z)^{-1} \ mod \ p \tag{11}$$

3) : Checks the validity of all the message blocks by the redundancy. If all blocks are valid, then U_v combine all the sub-blocks into the complete message *m*.

III. Property analysis of the proposed scheme

We will analyze the proposed scheme in detail from three aspects: correctness, security and performance in this section.

A. Correctness analysis

Chung's scheme will fail even if all the actual signers follow the proposal because of the wrong proof of Theorem 1 as pointed in literature [5]. The authors make a mistake by equating $\sum_{k=1}^{t}(r_k \cdot f(x_k) \cdot \prod_{\substack{i=1 \\ i\neq k}}^{t} \frac{0-x_i}{x_k-x_i})$ and $\sum_{k=1}^{t} r_k \cdot \sum_{k=1}^{t} f(x_k) \cdot \prod_{\substack{i=1 \\ i\neq k}}^{t} \frac{0-x_i}{x_k-x_i})$. Our propose method resolves this issue. Now we will give a detailed proof of correctness as follows.

Theorem 1: The specified verifier U_v can retrieve the message block using (11).

Proof: At the signature generation stage, the actual signer group computes the session key shared with U_v by using (3) and (4), and determines the sub-signature by using (5) and (6). So U_v can decrypt the message correctly.

$$
\begin{aligned}
& Z = \textstyle\sum_{k=1}^{t} z_k = (x_Z, y_Z) && by(4) \\
\Leftrightarrow\ & Z = \textstyle\sum_{k=1}^{t}(b_k \cdot x_{B_k})Y_v && by(3) \\
\Leftrightarrow\ & Z = \textstyle\sum_{k=1}^{t}(s_k + r_k + f(x_k) \cdot \prod_{\substack{i=1 \\ i\neq k}}^{t} \frac{0-x_i}{x_k-x_i})Y_v && by(6) \\
\Leftrightarrow\ & Z = (\textstyle\sum_{k=1}^{t} s_k + \sum_{k=1}^{t} r_k + \sum_{k=1}^{t} f(x_k) \prod_{\substack{i=1 \\ i\neq k}}^{t} \frac{0-x_i}{x_k-x_i})Y_v \\
\Leftrightarrow\ & Z = (s + r + f(0))Y_v \\
\Leftrightarrow\ & Z = sY_v + rY_v + (f(0) \cdot x_v)P \\
\Leftrightarrow\ & Z = sY_v + rY_v + x_v Y_s
\end{aligned}
$$

■

Thus, the verifier U_v can get the session key Z by the above derivation and then recover all the sub-messages $\{m_1, m_2, \ldots, m_t\}$ by (11).

B. Security analysis

The security of our proposal depends on the difficulty of solving ECDLP, and it is sufficiently secure to resist the following attacks.

1) Attack 1: An attacker knows the public keys of all participants in the protocol and may derive the verifier's private key x_v, the group private key $f(0)$ or even the signers' private keys $f(x_k)$. Depending on the difficulty of resolving ECDLP, it is quite sufficient to resist this type of attacks. Besides, the attacker may derive the private key $f(x_k)$ of each signer by (6) in the signature phase. However, the attacker has to find the values of two secret parameters $f(x_k)$ and b_k to satisfy (6). Over all, a forcible deduction is nearly infeasible.

2) Attack 2: In the proposed scheme, suppose a malice signer u_k chooses two random integers b'_k and x'_{b_k} to compute z'_k which can satisfy the individual signature verification equation (8) but is independent from B_k. In Chung's scheme, the relevance between B_k and z_k is not checked in the signature generation phase, so the malicious participant can forge an incorrect z'_k corresponding to a correct B_k to sign the message. In such a case, the verifier cannot recover the right session key according to Theorem 1 in [5], and neither can he recover the message. On the contrary, in our proposal, the verification equation (7) based on bilinear pairings is used to establish the linkage between B_k and z_k, which can be further used to protect the scheme from the above issue.

3) Attack 3: An attacker may try to cheat the clerk u_c in the signature generation phase by randomly selecting a integer r_k and a point B_k to compute s_k satisfying (7). Such an attack that depends on resolving the ECDLP is unworkable.

4) Attack 4: Now consider the chosen sub-message attack against the proposal. Suppose an attacker acquires the value of r_k and the corresponding message block m_k. The attacker can calculate $h(k||x_Z) = r_k \cdot m_k^{-1} \ mod\ q$, but he cannot recover the value of x_Z owing to the one-way hash function. So, an attacker cannot infer any information from the authenticated cipher-text in this way.

5) Attack 5: If an attacker gets the group signature $(r, s, r_1, r_2, \ldots, r_t)$, he attempts to permute or tamper with the group signature. However, a specified verifier U_v can put in order each message block recovered from (11) by the redundancy associated with m_k. Also, the verifier can determine which message block has been tempered with using the redundancy.

C. Performance evaluation

In the following, we compare our scheme with Chung's scheme [5] and Tan's scheme 2 [8] on the performance efficiency. Time complexity is designed for estimating the required cost of executing operations. Hence, we give all related symbols which are described in Table I.

In Chung's scheme, the message owner is a group and the finally group signature to be sent to the specified verifier is $(r, s, r_1, r_2, \ldots, r_t)$. According to the protocol, the communication cost is $2|q| + t|p|$ in together. Compared to Chung's scheme, the communication cost of Tan's scheme 2 and our proposed scheme does not grow at all.

Table I
Definitions of operation symbols

Symbols	Definitions
T_{mul}	Time for modulus multiplication operation
T_{inv}	Time for modulus inverse element operation
T_{EC_mul}	Time for elliptic-curve multiplication operation
T_{EC_add}	Time for elliptic-curve addition operation
T_h	Time for executing the one-way hash function $h()$
T_{bp}	Time for executing a bilinear pairing operation

We hence compare the complexity of computations on the signature phase and the message recovery phase based on an

individual with a sub-message m_k. Assume that the value of t in all three schemes is equal to one. For estimating the performance of the three schemes, the various operation units should be exchanged into the modules multiplication unit according to the literature [10]: one T_h is approximately 0.4 times of T_{mul}, one T_{EC_mul} is about 29 times of T_{mul}, one T_{EC_add} is about 0.12 times of T_{mul} and one T_{bp} is about 75 times of T_{mul}. In summary, we conclude the required time complexity of processing the data which are shown in Table II.

Table II
PERFORMANCE COMPARISONS

Items of contrast	**Signature generation phase**		**Message recovery phase**	
	Time complexity	***Rough estimation***	***Time complexity***	***Rough estimation***
Chung's scheme	$2T_{EC\_mul}+4T_{mul}+T_h$	$62.4T_{mul}$	$2T_{EC\_mul}+T_{EC\_add}+2T_{mul}+T_h+T_{inv}$	$60.52T_{mul}+T_{inv}$
Tan's scheme 2	$7T_{EC\_mul}+4T_{mul}+T_h$	$208.6T_{mul}$	$2T_{EC\_mul}+T_{EC\_add}+2T_{mul}+T_h+T_{inv}$	$60.52T_{mul}+T_{inv}$
The proposal	$2T_{EC\_mul}+4T_{mul}+T_{EC\_add}+T_h+T_{bp}$	$136.5T_{mul}$	$3T_{EC\_mul}+2T_{EC\_add}+T_{mul}+T_h+T_{inv}$	$88.64T_{mul}+T_{inv}$

Table II presents a comparison in terms of the computational cost between the schemes. Chung's scheme seems better because of the lower cost but there exit some design defects in the scheme. Also, Chung's scheme fails to resist Attack 2 shown in Section III.B. However, both Tan's scheme 2 and our proposal can overcome the above weaknesses, which inevitably increase the computational cost compared to Chung's scheme. In the signature generation phase, Tan's scheme 2 adds $3T_h$ and $5T_{EC\_mul}$ in the computational cost. In our proposal, we replaces $1T_{EC\_add}$ instead of $1T_{mul}$ and adds a bilinear pairing in signature generation phase to achieve adequate security. The calculation of bilinear pairing operation is much more than the modules multiplication operation. However, the total computational cost of our proposal in this phase is much lower than Tan's scheme 2, and the protocol procedure is simplified by using the bilinear pairing. In the message recovery phase, Tan's scheme 2 doesn't increase the computational cost compared to Chungs scheme. As for our proposal, it slightly increased by $1T_{EC\_mul}$ and $1T_{EC\_add}$. In summary, the proposed scheme can overcome all the security flaws exited in Chung's scheme and is totally more efficient than Tan's scheme 2.

IV. CONCLUSION

In this paper, we proposed a robust collaborative threshold authenticated encryption scheme. By using collaborative signature and message linkage technology, each signer just needs to sign one message block allocated to him, which reduces the signers workload dramatically. By using the elliptic curve cryptography and the bilinear pairing, our scheme is more robust and effective than the former similar schemes. The new scheme can be applied in distributed environments, such as cloud storage and computing networks, dynamic alliance of enterprises and virtual organizations.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (Grant No. 61003245, 61371098, 60903202), the Major Project for the Science and Technology Development of the railway ministry of China (Grant No. 2012X004-A), the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20090184120024), the Outstanding Youth Foundation of Sichuan Province, China (Grant No. 2011JQ0027), and the Fundamental Research Funds for the Central Universities of China (Grant No. SWJTU12CX099, SWJTU11CX041).

REFERENCES

[1] K. Nyberg and R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery," In: Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, VA, pp. 58-61, 1993.

[2] P. Horster, M. Michels and H. Petersen, "Authenticated encryption schemes with low communication costs," IEEE Electronics Letters, vol. 30(15), pp. 1212-1213, 1994.

[3] J. Zhang and Y. Wang, "Method of constructing elliptic curve authenticated encryption scheme," Applied Mathematics and Computation, vol. 168(1), pp. 146-151, 2005.

[4] C. L. Hsu and T. C. Wu, "Authenticated encryption scheme with (t, n) shared verification," IEE Proceedings-Computers and Digital Techniques, vol. 145(2), pp. 117-120, 1998.

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

[6] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, pp. 203-209, 1987.

[7] Z. W. Tan, "A new threshold authenticated encryption scheme using labor-division signature," Journal of Systems Science and Complexity, vol. 6(23), pp. 1183-1194, 2010.

[8] Z. W. Tan, "Improvement on a threshold authenticated encryption scheme," Journal of Software, vol. 7(5), pp. 697-704, 2010.

[9] C. C. Lin and C. S. Laih, "Cryptanalysis of Nyberg-Ruppels message recovery scheme," IEEE Communication Letters, vol. 4(7), pp. 231-232, 2000.

[10] W. S. Juang, "RO-cash: An efficient and practical recoverable pre-paid offline e-cash scheme using bilinear pairings," Journal of Systems and Software, vol. 83, pp. 638-645, 2010.