TELKOMNIKA, Vol. 11, No. 7, July 2013, pp. 3789 ~ 3797
e-ISSN: 2087-278X

A General Threshold Signature and Authenticated Encryption Scheme Based on ElGamal System

Yulian Shang[1, a], Wuyuan Jia[2, b], Lanhua Zhang[1, 3, c], and Yufei Zhang[1, d]
[1]College of Information and Engineering, Taishan Medical University, Taian, Shandong 271016 China
[2]College of Chemistry and Chemical Engineering, Taishan Medical University, Taian, Shandong 271016 China
[3]Institute of Neuroinformatics, Dalian University of Technology, Dalian, Liaoning 116024 China
Corresponding author, e-mail: shangyulian@163.com[a], jiawuyuan@163.com[b], Lhzhang @tsmc.edu.cn[c], yfzhang@tsmc.edu.cn[d]

Abstract

Based on ElGamal system, a group-oriented threshold signature and authenticated encryption scheme was put forward. After being signed by a signer group employing (t,n) threshold signature scheme, the message m was transmitted to a particular verifier group, and then the signature was verified through the cooperation of k ones from the verifier group with l members. Similarly, a general authenticated encryption scheme characterized by (k,l) joint verification was put forward through integrating (t,n) threshold signature scheme and message recovery technique together; After being encrypted singed by any t ones from a group with n members, the message m was transmitted to a particular verifier group with l members, and then recovered through the cooperation of any k ones from the verifier group. The security of this scheme is based on Shamir threshold scheme and ElGamal system. It realized the directional transmission of message between different groups and enjoyed the characteristics of reduced communication load and lowered calculation complexity, etc.

Keywords: *ElGamal system, threshold signature, authentication encryption, group oriented, interpolation polynomial*

1. Introduction

The research is based on the following facts in digital contracts:

A contract between two groups will be signed and verified. It cannot be exposed to any outsider, otherwise it will have been altered and forged risk. In other words, the signer group and verifier group must be regulated under a pre-stipulated security environment.

It's also the example above. Suppose that several managers on behalf of the group signed a contract with other group. They have not only to verify the authenticity of the contract signed, but also to ensure that only they can see the contents of the contract and other people are unable to see it.

In view of the above facts, a threshold signature scheme characterized by (k,l) joint verification for (t,n) signature was put forward to solve the first problem. It's stipulated that there are n members in a signer group, and only through the cooperation of at least t members can some message be effectively signed; on the other hand, only through the cooperation of at least k ones from a verifier group with l members can the signature be verified. Through integrating (t,n) threshold signature scheme and message recovery technique together, a general authenticated encryption scheme characterized by (k,l) joint verification was put forward to solve the second problem. It's stipulated that there are n members in a signer group, and only through the cooperation of at least t members can some message be effectively encrypted signed; on the other hand, only through the cooperation of at least k ones from a verifier group with l members can the signature be recovered. Thus, the schemes [1-0] before cannot meet practical needs. Therefore, there shall be a general scheme [11, 12] in which the signer group and verifier group (or recovery group) can be regulated under

Received January 27, 2013; Revised April 18, 2013; Accepted May 5, 2013

a pre-stipulated security environment. The security of this scheme is based on the intractability of discrete logarithm calculation in an infinite field [13], and it can be deemed as a revised ElGamal scheme which enjoys wider application in practice.

As a caveat: what we described in this paper is based on [14], some points of our paper has published in Applied Mechanics and Materials with title of "Research on Company-oriented General Authenticated Encryption Threshold Scheme", on Vols. 263-266 (2013), pp: 2953-2957, at Guangzhou, including some figures and tables and so on.

2. Description of the Scheme

2.1. Group-oriented General Threshold Signature Scheme

There are three parts in the whole scheme, i.e., shared distribution center (SDC), signer group,and verifier group. The scheme includes three stages, i.e., generation of parameters, generation and verification of private signatures, and generation and verification of group signatures.

Generation of Parameters: in this stage, the parameters of the system are listed as follows:

(1) Public information in SDC: $P, q, g, h()$; where, P and q are big prime numbers and $q \mid (P-1)$; the order of generation factor g in $GF(P)$ is q; $h()$ is an irreversible hash function.

(2) Secret information in SDC:

$$f_s(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \cdots + a_1 x + a_0 \bmod q$$
$$f_v(x) = c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + \cdots + c_1 x + c_0 \bmod q$$
$$f_b(x) = b_{t-1b}x^{t-1} + b_{t-2}x^{t-2} + \cdots + b_1 x + b_0 \bmod q \qquad a_i, c_j, b_i \in [1, q-1], 1 \le i \le t-1, 1 \le j \le k-1;$$

Where, $f_s(x), f_v(x)$ are respectively randomly-selected interpolation polynomials of the signer group G_s and the verifier group G_v; $f_b(x)$ is the interpolation polynomial selected for the signer group G_s to generate group signatures.

(3) Public information of members: x_{si} (or x_{vj}) $\in [1, q-1]$, y_{si} (or y_{vj}), y_{bi}, $1 \le i \le n, 1 \le j \le l$; where, x_{si} (or x_{vj}) are the randomly-selected integral number for every member of the signer group (or the verifier group) in SDC; $y_{si} = g^{f_s(x_{si})} \bmod P$ (or $y_{vj} = g^{f_c(x_{vj})} \bmod P$) are their public key, and $y_{bi} = g^{f_b(x_{si})} \bmod P$ are the public key of the signer group.

(4) Secret information of members: $f_s(x_{si})$ (or $f_v(x_{vj})$), $f_b(x_{si})$

(5) Public information of the groups: Y_s (or Y_v), Y_b; where, $Y_s = g^{f_s(0)} \bmod P, Y_v = g^{f_v(0)} \bmod P$, $Y_b = g^{f_b(0)} \bmod P$

(6) Secret information of the groups: $f_s(0) = a_0, f_v(0) = c_0$

Generation and Verification of Private Signatures: According to the security strategy, any t members are allowed to sign a piece of message on behalf of the group in this scheme, and the members can simultaneously and independently sign the message. Without loss of generality, the t members for signing are expressed as $u_{s1}, u_{s2}, \cdots,$ and u_{st}. Every member $u_{si}, 1 \le i \le t$, carries out the following calculation with its own private key $f_s(x_{si})$ and the public key of the verifier group Y_v.

$$r_{si} = (Y_v)^{f_s(x_{si}) \prod_{j=1, j \ne i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}}} \bmod P \tag{1}$$

The result $\{r_{si}\}$ is transmitted to the members participating in signing through security channel, and every member calculates r as follows:

$$r = \prod_{i=1}^{t} r_{si} \bmod P \tag{2}$$

Then, every member u_{si} signs the message m using his private key $f_s(x_{si})$ and the session key $f_b(x_{si})$ through ElGamal signature scheme, i.e., calculates his private signature with the following formula:

$$s_i = h(m) f_s(x_{si}) \prod_{j=1, j\neq i}^{t} \frac{0-x_{si}}{x_{si}-x_{sj}} - r f_b(x_{si}) \prod_{j=1, j\neq i}^{t} \frac{0-x_{sj}}{x_{si}-x_{sj}} \bmod q \quad (3)$$

To verify the validity of private signature s_i, one member is randomly selected as the secretary to be responsible for the verification of private signatures and calculation of group signatures. Following formula is employed to verify private signatures by the secretary:

$$y_{si}^{h(m)\cdot \prod_{j=1, j\neq i}^{t} \frac{0-x_{sj}}{x_{si}-x_{sj}}} \stackrel{?}{=} g^{s_i} y_{bi}^{r\cdot \prod_{j=1, j\neq i}^{t} \frac{0-x_{sj}}{x_{si}-x_{sj}}} \bmod P \quad (4)$$

If the equation is right, the private signature of the message is legitimate.
It's testified as follows:
It's known from (3) that

$$h(m) f_s(x_{si}) \prod_{j=1, j\neq i}^{t} \frac{0-x_{sj}}{x_{si}-x_{sj}} = s_i + r f_b(x_{si}) \prod_{j=1, j\neq i}^{t} \frac{0-x_{si}}{x_{si}-x_{sj}} \bmod q \quad (5)$$

substituted to (4):

$$\begin{aligned} & y_{si}^{h(m)\cdot \prod_{j=1, j\neq i}^{t} \frac{0-x_{sj}}{x_{si}-x_{sj}}} \stackrel{?}{=} g^{s_i} y_{bi}^{r\cdot \prod_{j=1, j\neq i}^{t} \frac{0-x_{sj}}{x_{si}-x_{sj}}} \bmod P \\ & = g^{s_i + r f_b(x_{si}) \prod_{j=1, j\neq i}^{t} \frac{0-x_{si}}{x_{si}-x_{sj}}} \\ & = g^{s_i} y_{bi}^{r\cdot \prod_{j=1, j\neq i}^{t} \frac{0-x_{sj}}{x_{si}-x_{sj}}} \bmod P \end{aligned} \quad (6)$$

Generation and Verification of Group Signatures: after t private signatures are verified, the secretary calculates the group signature.

$$s = \sum_{i=1}^{t} s_i \bmod q \quad (7)$$

The group signature of message m is transmitted to the verifier group G_v, and any k ones of the l members in group G_v can cooperate to verify the validity of the signature. Every member u_{vi}, $1 \le i \le k$, carries out the following calculation with its own private key $f_v(x_{vi})$ and the public key of the signer group Y_s.

$$r_{vi} = (Y_s)^{f_v(x_{vi}) \prod_{j=1, j\neq i}^{k} \frac{0-x_{vj}}{x_{vi}-x_{vj}}} \bmod P \quad (8)$$

Similarly, a secretary is randomly selected in the verifier group and he calculates:

$$r = \prod_{i=1}^{k} r_{vi} \bmod P \quad (9)$$

Then, the group signature can be verified as follows:

$$Y_s^{h(m)} \stackrel{?}{=} g^s \cdot Y_b^r \bmod P \tag{10}$$

Theorem 1.1 if (10) is right, message m is verified.
It's testified as follows:
Substituted (1) to (2), it's known that:

$$\begin{aligned} r &= (Y_v)^{\sum_{i=1}^{t} f_s(x_{si}) \prod_{j=1, j\neq i}^{t} \frac{0-x_{sj}}{x_{si}-x_{sj}}} \bmod P \\ &= (g^{f_v(0)})^{f_s(0)} \bmod P \end{aligned} \tag{11}$$

Multiplied by both sides for $i = 1,2,\cdots,t$, it's known from (4) that:

$$\prod_{i=1}^{t} y_{si}^{h(m)\cdot \prod_{j=1, j\neq i}^{t} \frac{0-x_{sj}}{x_{si}-x_{sj}}} = \prod_{i=1}^{t} g^{s_i} y_{bi}^{r\cdot \prod_{j=1, j\neq i}^{t} \frac{0-x_{sj}}{x_{si}-x_{sj}}} \bmod P \tag{12}$$

From Lagrange interpolation polynomials, it's can determine a $t-1$ degree polynomial utterly

$$f(x) = \sum_{i=1}^{t} y_i \cdot \prod_{j=1, j\neq i}^{t} \frac{x - x_j}{x_i - x_j} \tag{13}$$

The left of (7) can be rewrited by

$$\begin{aligned} &g^{\sum_{i=1}^{t} h(m) f_s(x_{si}) \cdot \prod_{j=1, j\neq i}^{t} \frac{0-x_{sj}}{x_{si}-x_{sj}}} \bmod P \\ &= (g^{f_s(0)})^{h(m)} \bmod P = (Y_s)^{h(m)} \bmod P \end{aligned} \tag{13}$$

For the member of verifier group u_{vi} can calculate r_{vi} from (8), multiplied by both sides for $i = 1,2,\cdots,t$, r' is known from (4) that:

$$\begin{aligned} r' &= (Y_s)^{\sum_{i=1}^{k} f_v(x_{vi}) \cdot \prod_{j=1, j\neq i}^{k} \frac{0-x_{vj}}{x_{vi}-x_{vj}}} \bmod P \\ &= (g^{f_s(0)})^{f_v(0)} \bmod P \end{aligned} \tag{14}$$

The value of r' is equal to r from (2). The group signature can be calculated from (10). On the other hand, the right of (15) can be rewrited by:

$$\begin{aligned} &g^{\sum_{i=1}^{t} s_i} \cdot g^{\sum_{i=1}^{t} r f_b(x_{si}) \cdot \prod_{j=1, j\neq i}^{t} \frac{0-x_{sj}}{x_{si}-x_{sj}}} \bmod P \\ &= g^s \cdot (g^{f_b(0)})^r \bmod P \\ &= g^s Y_b^r \bmod P \end{aligned} \tag{15}$$

2.2. Group-oriented General Authenticated Encryption Threshold Scheme

There are also three parts in the whole scheme, i.e., shared distribution center (SDC), signer group and verifier group. The scheme includes three stages, i.e., generation of parameters, encryption and signature, and message recovery.

Generation of Parameters: in this stage, the parameters of the system are listed as follows:
(1) Public information of SDC: P, q, g ; where, P and q are big prime numbers and $q \mid (P-1)$; the order of generation factor g in $GF(P)$ is q.
(2) Secret information of SDC:

$$f_s(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \cdots + a_1 x + a_0 \bmod q$$
$$f_v(x) = c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + \cdots + c_1 x + c_0 \bmod q$$
$$f_b(x) = b_{t-1b}x^{t-1} + b_{t-2}x^{t-2} + \cdots + b_1 x + b_0 \bmod q \qquad a_i, c_j, b_i \in [1, q-1], 1 \le i \le t-1, 1 \le j \le k-1;$$

Where, $f_s(x), f_v(x)$ are respectively randomly-selected interpolation polynomials of the signer group G_s and the verifier group G_v; $f_b(x)$ is the interpolation polynomial selected for the signer group G_s to generate group signatures.
(3) Public information of members: x_{si} (or $x_{vj}) \in [1, q-1]$, y_{si} (or y_{vj}), y_{bi}, $1 \le i \le n, 1 \le j \le l$; where, x_{si} (or x_{vj}) are the randomly-selected integral number for every member of the signer group (or the verifier group) in SDC; $y_{si} = g^{f_s(x_{si})} \bmod P$ (or $y_{vj} = g^{f_c(x_{vj})} \bmod P$) are their public key, and $y_{bi} = g^{f_b(x_{si})} \bmod P$ are the public key of the signer group.
(4) Secret information of members: $f_s(x_{si})$ (or $f_v(x_{vj})), f_b(x_{si})$
(5) Public information of the groups: Y_s (or $Y_v), Y_b$; where, $Y_s = g^{f_s(0)} \bmod P, Y_v = g^{f_v(0)} \bmod P$, $Y_b = g^{f_b(0)} \bmod P$
(6) Secret information of the groups: $f_s(0) = a_0, f_v(0) = c_0$

Encryption and signature: Suppose that after the secret message m is transmitted from the signer group G_s to the verifier group G_v and recovered, there is enough redundancy for validation in it. According to threshold signature scheme, any t members can represent the group to sign the message. Without loss of generality, the t members for signing are express as $u_{s1}, u_{s2}, \cdots, u_{st}$. Each member $u_{si}, 1 \le i \le t$ uses his/her own key $f_s(x_{si})$ and public key Y_v of the signer group to calculate:

$$z_{si} = (Y_v)^{f_s(x_{si}) \prod_{j=1, j \ne i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}}} \bmod P \tag{16}$$

and

$$r_i = (g)^{f_b(x_{si}) \prod_{j=1, j \ne i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}}} \bmod P \tag{17}$$

Each member calculates the public session key z after the result $\{z_{si}, r_i\}$ is transmitted to all signers by security channels.

$$z = (\prod_{i=1}^{t} z_{si} \bmod P) \bmod q \tag{18}$$

Then u_{si} uses his/her key and session key $f_b(x_{si})$ to sign the message according to the revised ElGamal signature scheme. Member u_{si} calculates the stipulated value r and private signature s_i, in conformity to the following formula.

$$r = m(\prod_{i=1}^{t} r_i^{z}) \cdot g^{z} \bmod P \tag{19}$$

$$s_i = zf_b(x_{si}) \prod_{j=1, j\neq i}^{t} \frac{0 - x_{si}}{x_{si} - x_{sj}} - rf_s(x_{si}) \prod_{j=1, j\neq i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}} \bmod q \quad (20)$$

A member is randomly elected as a full-time secretary with responsibility for the validation of private signatures and the calculation of group signatures. After the private signatures are received, the secretary will validate the private signature using the following formula:

$$r_i^z \stackrel{?}{=} g^{s_i} y_{si}^{r \cdot \prod_{j=1, j\neq i}^{t} \frac{0-x_{sj}}{x_{si}-x_{sj}}} \bmod P \quad (21)$$

If the equation is right, the private signature s_i of the message m is valid.
Then the secretary calculates the group signature as follows:

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

Finally the group signature of message m is transmitted to the verifier group.

Message recovery: When the group signature of message m is transmitted to the verifier group G_v, k ones of the l members in group G_v must cooperate to recover the message. Without loss of generality, we express k validation members as $u_{v1}, u_{v2}, \cdots, u_{vk}$. Firstly, each member $u_{vj}, 1 \le j \le k$ uses signature (r, s) to calculate $g^{zf_b(0)}$:

$$g^{zf_b(0)} = g^s \cdot Y_s^r \bmod P \quad (23)$$

Then each verifier uses key $f_v(x_{vj})$ and public key Y_s of the signer group to calculate the value of z_{vi}:

$$z_{vi} = (Y_s)^{f_v(x_{vi}) \prod_{j=1, j\neq i}^{k} \frac{0-x_{vj}}{x_{xi}-x_{vj}}} \quad (24)$$

Public session key can be determined by the verifier group through combining k $z_{vi}, i = 1,2,\cdots,k$, as below:

$$z = (\prod_{i=1}^{k} z_{vi} \bmod P) \bmod q \quad (25)$$

So message m can be recovered by the values of $g^{zf_b(0)}$ and z.

$$m = r \cdot (g^{zf_b(0)})^{-1} \cdot g^{-z} \bmod P \quad (26)$$

Finally, the recovered m is authenticated through checking the validity of its interior redundancy.

Theorem 2.2 If (r, s) is the signature pair generated during the stage of signature encryption, message m can be decrypted precisely during the stage of message recovery.
It's testified as follows:

During the stage of signature encryption, each user $u_{si}, 1 \le i \le t$ calculates z_{si} and r_i in conformity to formula (16) and formula (17), then the signer group calculate public session key z :

$$z = ((Y_v)^{\sum_{i=1}^{t} f_s(x_{si}) \prod_{j=1, j\neq i}^{t} \frac{0-x_{sj}}{x_{si}-x_{sj}}} \bmod P) \bmod q$$
$$= ((g^{f_v(0)})^{f_s(0)} \bmod P) \bmod q$$

The (r, s) signature can be got from formula (19) and formula (22), and then transmitted to the verifier group. On the other hand, member $u_{vj}, 1 \le j \le k$ of the verifier group calculates $g^{zf_b(0)}$ with formula (23) and z_{vi} with formula (24).Then the k members can cooperate to get the public session key using formula (25).

$$z' = ((Y_s)^{\sum_{i=1}^{k} f_v(x_{vi}) \prod_{j=1, j\neq i}^{t} \frac{0-x_{sj}}{x_{si}-x_{sj}}} \bmod P) \bmod q$$
$$= ((g^{f_v(0)})^{f_s(0)} \bmod P) \bmod q$$

Obviously the value of z' is equal to the value z in formula (18). So message m can be recovered by formula (26).

$$m = r \cdot (g^{zf_b(0)})^{-1} \cdot g^{-z} \bmod P$$
$$= m(\prod_{i=1}^{t} r_i^z) g^z (g^{zf_b(0)})^{-1} \cdot g^{-z} \bmod P$$
$$= m \bmod P$$

3. Results and Analysis

3.1. Security Assessment and Performance Analysis of the General Threshold Signature Scheme

Thinking that the signature s_i is drawn from ElGamal signature scheme [1] and can be deemed as a revised ElGamal scheme, the security of this scheme is based on ElGamal scheme. On the private signature stage, message m is transformed into $h(m)$ through an irreversible hash function with its randomness increased to prevent ElGamal attacks.

In this scheme, if the verifier group is arranged in particular, Harn's scheme comes to be under a condition of $k = l = 1$ in the verifier group. In Harn's scheme, there are two parameters (r, s) transmitted to the verifiers as group signatures, whereas, in our scheme, the agreed value r can be put forward by the signer group and the verifier group respectively through applying a secret sharing scheme [10], therefore, there will be only one parameter s needs to be transmitted to the verifier group. The Table 1 list the comparison of communication cost.

Table 1. Character Comparision of our scheme and Harn's scheme

Comparision \ Method	Harn's scheme	Our scheme
Message redundancy	$Sig(m) = (r, s)$	$Sig(m) = (s)$
	2	1
Communication cost	$\|m\| + \|P\| + \|q\|$	$\|m\| + \|q\|$
Time complexity of signature generation	$TE + (3t+1)TM + (t-1)TI$	$TE + (3t+2)TM + (t-1)TI$
Time complexity of signature verification	$2TE + TM$	$2TE + TM$

The signature transmission in Harn's scheme is $|m|+|P|+|q|$, and that in our scheme is reduced to $|m|+|q|$; on signature generation stage, time complexity of signature calculation is $TE+(3t+2)TM+(t-1)TI$, and that on verification stage is $2TE+TM$. Table 1 shows that, in our scheme, message redundancy and communication cost are both reduced, with only an extra TM added on signature stage.

3.2. Security Assessment and Performance Analysis of the General Authenticated Encryption Threshold Scheme

The scheme we put forward is originated from [12], so the security of this scheme depends on the intractability of the discrete logarithm in an infinite field. This scheme can resist the plaintext attack, equation attack, disguise attack and conspiracy attack.

The authentication encryption scheme offered by Nyberg and Rueppel in [4] is a combination of digital signature with message recovery and data encryption, which limits to one signer and one verifier. Then the sharing authentication encryption scheme [5] presented by Hsu and Wu extends it to one signer and a group of verifiers. Through integrating the threshold signature and authentication encryption scheme, we present a general authentication encryption scheme which is oriented to a signer group and a verifier group. So, the two schemes above can be deemed as special conditions of the scheme we put forward.

Our scheme turns into Hsu & Wu's scheme when the signer group only contains one member, i.e. $n=t=1$.First, when Hsu & Wu's scheme creates signature pairs (r,s) of message m, the pairs are encrypted to cryptograph (c_1,c_2,c_3), seeing the signature extended to three parameters. Our scheme handles message encryption and signature simultaneously, and there are two message extensions of signature pairs. Furthermore, the cryptograph length of message in Hsu & Wu's scheme is $2|P|+|q|$, and the message recovery cost of communication is $(k+2)|P|+|q|$. In our scheme the signature length of message is $|P|+|q|$, and the message recovery cost of communication is $(k+1)|P|+|q|$. Thus the bandwidth and communication cost are all reduced in our scheme.

The time complexity of signature encryption computing is $3(TE+TM)$ at the stage of signature encryption, and the time complexity is $3TE+(2k+2)TM+(k+1)TI$ for verifier. Table 1 is the comparison of Harn's scheme, Hsu &Wu's scheme and ours'. Our scheme performs better in bandwidth and communication cost. Yet in our scheme, there are two more TI calculation values and one TM calculation value in the total time complexity compared with Hsu and Wu's scheme. In other words, communication cost and time complexity are mutually restricted.

Table 2. Contrast of the three schemes

Comparision \ Method	Harn's Scheme	Hsu & Wu's Scheme	Our Scheme
Message redundancy	$Sig(m)=(c_1,c_2,c_3,c_4)$ 4	$Sig(m)=(c_1,c_2,c_3)$ 3	$Sig(m)=(r,s)$ 2
Cryptograph length	$3\|P\|+\|q\|$	$2\|P\|+\|q\|$	$\|P\|+\|q\|$
Communication cost of message recovery	$2k\|P\|+\|q\|+\|m\|$	$(k+2)\|P\|+\|q\|$	$(k+1)\|P\|+\|q\|$
Time complexity of encryption	$3(TE+TM)+2TI$	$3(TE+TM)$	$3(TE+TM)$
Time complexity of message recovery	(2*k*+3)*TE*+*kTM*+(*k*-1)*TI*	3*TE*+(2*k*+1)*TM*+(*k*-1)*TI*	3*TE*+(2*k*+2)*TM*+(*k*+1)*TI*

4. Conclusion

The analysis above indicates that this scheme enjoys enough security, with message redundancy and communication costs both reduced, and the calculation complexity of verification algorithm also lowered. It not only has significant theoretical meaning in the

communication between different companies, such as commercial, military and municipal departments, but also finds wider applications in practice.

Acknowledgements

This work was financially supported in part by Institutes of Higher Education Science and Technique Foundation of Shandong Province (J10LC59), Scientific Research Tasks of Tainshan Medical University General Program (2011ZR060) and College Student Science and Technique Innovation Action Program of Taian (2010D2033, 2010D2034, 2011D1035, 2011D2035). The authors thank the College of Information and Engineering Taishan Medical University colleagues for manuscript comments. The authors are grateful to the anonymous referees for their valuable comments and suggestions.

References

[1] ElGamal T. *IEEE Transactions Information Theory*. 1985; 31(4): 469-472.
[2] Harn L. *IEEE Proceedings of Computers and Digital Technique*. 1994; 141: 307-313.
[3] Bin Wang and Jianhua Li. *Chinese Journal of Computers*. 2003; 26: 158l-1583.
[4] K Nyberg, RA Rueppel. Des., Codes,Cryptogr. 1996; 7: 61-68.
[5] CL Hsu, TC Wu. Inf. Process. Lett. 1996; 58: 189-194.
[6] R Tso, C Gu and T Okamoto. *Cryptology and Network Security*. 2007 (CANS 2007), LNCS 4857. Berlin: Springer-Verlag. 2007: 47-59.
[7] Y Ming and Y Wang. in Proceedings of the 2009 Fifth International Conference on Information Assurance and Security. Washington: IEEE Computer Society. 2009: 87-90.
[8] B Kang, J Park, and S Hahn. Topics in Cryptology-CT-RSA. 2004, LNCS 2964. Berlin: Springer-Verlag. 2004: 99-111.
[9] J Zhang. *Information Security Practice and Experience*. 2009, LNCS 5451. Berlin: Springer-Verlag. 2009: 47-58.
[10] SCHNEIERB: John Wiley & Sons, Inc. 1994.
[11] GENNAROR: Massachusetts Institute of Technology, Cambridge. 1996.
[12] Yulian Shang, Lanhua Zhang, Yufei Zhang. 7th International Conference on System of Systems Engineering. Italy:Genova. 2012; 16-19: 211-213.
[13] A Shamir. Communication of the ACM. 1979; 22:612-613.
[14] Yulian Shang, Guoqing Yang, Lanhua Zhang, Yufei Zhang. *Applied Mechanics and Materials*. Guangzhou. 2013; 263-266: 2953-2957.