Computing and Informatics, Vol. 24, 2005, 529–541

A *(T, N)* THRESHOLD SECRET SHARING SYSTEM WITH EFFICIENT IDENTIFICATION OF CHEATERS

Iuon-Chang Lin

Department of Management Information Systems
National Chung Hsing University
250 Kuo-Kuang Rd., Taichung, 402 Taiwan
e-mail: iclin@nchu.edu.tw

Chin-Chen Chang

Department of Information Engineering and Computer Science
Feng Chia University Taichung, Taiwan
e-mail: ccc@cs.ccu.edu.tw

Manuscript received 19 February 2004; revised 4 August 2005
Communicated by Peter Vojtáš

Abstract. In this paper, we propose a new (t, n) threshold scheme. The scheme allows a user to divide portions of a secret among the designated group. Any t or more participants from a designated group of n members can cooperate to reconstruct the secret while $(t-1)$ or less participants can not. Furthermore, the scheme provides an efficient mechanism to detect and identify cheaters. From the security analysis, we conclude that any participant does not have the ability to deceive other participants to obtain their portion of the secret. Therefore, this scheme is very practical for a broad spectrum of applications.

Keywords: Cheater identification, information security, secret sharing system

1 INTRODUCTION

Secret sharing is a technique that is used to share a secret among a group of participants. In real world, there are many applications that require a group of participants

to share a secret such as launching a nuclear missile, opening a bank vault, authenticating an electronic fund transaction, and others [6]. The simplest way to share a secret among a group of n participants is dividing the secret into n shadows, with each participant holding one shadow. When the n participants present their shadows honestly, the correct secret can be reconstructed. However, if one of the shadow-holders dies, we can never reconstruct the secret. In order to prevent a shadow from being lost, destroyed, or modified, a flexible way to share a secret is required.

The (t, n) threshold secret sharing technique not only provides a good solution to this problem but also fits various practical situations. The main concept of the (t, n) threshold scheme is to divide the shared secret into n shadows and only more than t out of n shadow-holders can cooperate to reconstruct the shared secret. All the possible subsets of a group that includes more than t participants are defined to be qualified subsets. Therefore, the (t, n) threshold scheme should be able to satisfy the following properties [8].

1. A dealer distributes the shadows to each participant.
2. The participants from one of the qualified subsets can reconstruct the shared secret easily using their shadows.
3. The participants from all the other unqualified subsets reveal no knowledge of the shared secret.

The secret sharing scheme also can be considered to be the key management process, and all the qualified subsets are called access structures in a cryptosystem.

In 1979, Shamir [11] first proposed a threshold secret sharing scheme. In the scheme, we assume that all participants will present their shadows honestly when they cooperate to reconstruct the shared secret. However, in the real world, the participants may be dishonest. A dishonest shadow-holder may submit false shadows to deceive other participants during the reconstruction of the shared secret. The dishonest participant is also called a cheater. By cheating, only the cheater has a chance to reconstruct the true secret. This is an important issue we have to concern in the application of the secret sharing technique. Therefore, how to detect and identify a cheater becomes an important topic in the area of secret sharing.

So far, many works have been published concerning (t, n) threshold secret sharing with cheater detection [2, 3, 13, 14]. In these schemes, we can detect whether there are cheaters during the reconstruction of a shared secret, but we cannot accurately identify who the cheaters are. In order to deal with this problem and provide higher reliability, some cheater identification schemes have been proposed [4, 7, 9]. These schemes can exactly identify who is presenting a false shadow. Therefore, a secret sharing scheme with a cheater identification scheme is more useful than one with a cheater detection scheme.

In this paper, we propose a (t, n) threshold secret sharing scheme based on Shamir's secret sharing concept [11]. Furthermore, our scheme provides a practical cheaters identification method. The rest of this paper is organized as follows. In Section 2, the proposed (t, n) threshold secret sharing scheme with cheater identi-

fication is described. In Section 3, a simple example is presented to illustrate the scheme. In Section 4, the security of the scheme and the required computations and communications are analyzed. In Section 5, a brief conclusion of this paper is made.

2 *(T, N)* THRESHOLD SECRET SHARING SCHEME FOR IDENTIFYING CHEATERS

Before describing the proposed scheme, some notations are defined first. We assume that U is a set that contains n participants $U_1, U_2, \ldots, U_n$, such that $U = \{U_1, U_2, \ldots, U_n\}$, and $\mathrm{ID}_1, \mathrm{ID}_2, \ldots, \mathrm{ID}_n$ are the identities of the n participants. Each member of U shares a secret K and holds a secret shadow S_i, where $1 \leq i \leq n$. Let Γ be the set that contains all the qualified subsets γ of U, i.e. $\Gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_l\}$. The qualified subset γ satisfies $|\gamma_i| \geq t$, where $|x|$ denotes the number of participants in γ and t is the threshold value in this system. Therefore, all the qualified subsets γ_i's can reconstruct the shared secret.

The proposed scheme consists of four phases: the shadow generation phase, the verification phase, the secret reconstruction phase, and the cheater identification phase. In the shadow generation phase, a dealer generates the shadows and sends them to all the participants in U to share a secret K. In the verification phase, each member in U can verify whether the shadows sent by the dealer and the other members are true or false. When the participants of any qualified subset in Γ give their approval to show their shadows, the shared secret K can be reconstructed in the secret reconstruction phase. If the reconstructed secret is not valid, we can identify in the cheater identification phase who the cheater is. These phases are described as follows.

2.1 The Shadow Generation Phase

Assume that a dealer wants to share a secret K among the n members in U. First, the dealer specifies the threshold value t freely within the range $1 \leq t \leq n$. Then the dealer chooses three system parameters p, q, and g, where p is a large prime, q is a prime factor of $p-1$, and g is a primitive root of the prime number p. That is, if g is a primitive root of the prime number p, then the numbers $g \mod P$, $g^2 \mod p$, ..., $g^{p-1} \mod p$, are distinct and consist of the integers from 1 through $p-1$ in some permutation. The parameters should be chosen to satisfy the standard ANSI X.930 [1] or FIPS186 [5]. Furthermore, the dealer has to generate the secret shadow for each participant in U and publish the information. The dealer generates the shadows and makes the information public as follows.

1. The dealer randomly generates n different polynomials f_i's of degree $t-1$, such that

$$f_i(X) = a_{(i,0)} + a_{(i,1)}X + \ldots + a_{(i,t-1)}X^{t-1} \bmod q, \tag{1}$$

where $a_{(i,1)}$, $a_{(i,2)}$, ..., $a_{(i,t-1)}$ are selected from $GF(q)$ for $i = 1, 2, \ldots, n$, and the coefficients $a_{(1,0)}$, $a_{(2,0)}$, ..., $a_{(n,0)}$ have to satisfy

$$a_{(1,0)} + a_{(2,0)} + \ldots + a_{(n,0)} \bmod q = K. \tag{2}$$

Note that all calculations of these polynomials are done in $GF(q)$, so the coefficients $a_{(i,1)}$, $a_{(i,2)}$, ..., $a_{(i,t-1)}$ and the secret K must be in the range from 1 to $q-1$.

2. The dealer sends the polynomial $f_i(X)$ to U_i through a secure channel.
3. For each participant U_i in U, the dealer computes

$$A_{(i,l)} = g^{a_{(i,l)}} \bmod p, \tag{3}$$

where $l = 0, 1, \ldots, t-1$. Then the dealer publishes all the $A_{(i,l)}$'s in a public bulletin board.

2.2 The Verification Phase

After receiving the polynomial from the dealer, each participant has to compute the shadows for the other participants in U. The participant can verify whether the received shadows are valid. The details of the verification phase are described as follows.

1. Each participant U_i computes

$$S_{(i,j)} = f_i(ID_j) = a_{(i,0)} + a_{(i,1)}ID_j + \ldots + a_{(i,t-1)}ID_j^{t-1} \bmod q, \tag{4}$$

where $ID_j \in GF(q)$, $j = 1, 2, \ldots, n$, and $i \neq j$.

2. Each participant U_i sends $S_{(i,j)}$ to the other participants U_j's in U over a secure channel. Therefore, each participant U_i can obtain $n-1$ shadows $S_{(j,i)}$'s from the other participants U_j's in U.
3. After receiving the shadows $S_{(j,i)}$'s, each participant U_i checks whether the following equation holds:

$$g^{S_{(j,i)}} \bmod p = \prod_{l=0}^{t-1} {A_{(j,l)}}^{ID_i^l} \bmod p. \tag{5}$$

If the above equation holds, the participant can believe the received shadows are true.

2.3 The Secret Reconstruction Phase

Assume that the participants $U_1, U_2, \ldots, U_r$ of any qualified subset in Γ want to cooperate to reconstruct the shared secret K. They can perform the following steps to determine the shared secret K.

1. Each actual participant U_i in the qualified subset can compute his/her own shadow using

$$S_{(i,i)} = f_i(ID_i) = a_{(i,0)} + a_{(i,1)}ID_i + \ldots + a_{(i,t-1)}ID_i^{t-1} \bmod q. \tag{6}$$

2. According to the computed shadow $S_{(i,i)}$ and the received shadows $S_{(j,i)}$'s, $j = 1, 2, \ldots, n$, and $j \neq i$, the actual participant U_i can obtain a value S_i' by computing the following equation:

$$\begin{aligned} S_i' &\equiv f_1(ID_i) + f_2(ID_i) + \ldots + f_n(ID_i) \bmod q \\ &\equiv \sum_{j=1}^{n} a_{(j,0)} + \sum_{j=1}^{n} a_{(j,1)}ID_i + \sum_{j=1}^{n} a_{(j,2)}ID_i^2 + \ldots + \sum_{j=1}^{n} a_{(j,t-1)}ID_i^{t-1} \bmod q \\ &\equiv F(ID_i). \end{aligned} \tag{7}$$

3. Each actual participant U_i sends S_i' to the other participants in the qualified subset.
4. For each received S_j' $(j \in \gamma; j \neq i)$, U_i knows t points on the curve $F(x)$

$$(ID_i, F(ID_i)) = (ID_i, S_i'), i \in \gamma.$$

Each actual participant can apply the Lagrange interpolation formula to determine the shared secret K from the t different points (ID_i, S_i'), thus

$$\begin{aligned} K &\equiv \sum_{i \in \gamma} (S_i' \times L_i) \bmod q \\ &\equiv F(0) \\ &\equiv a_{(1,0)} + a_{(2,0)} + \ldots + a_{(n,0)} \bmod q, \end{aligned} \tag{8}$$

where

$$L_i = \prod_{i,j \in \gamma, j \neq i} \frac{-ID_j}{ID_i - ID_j} \bmod q. \tag{9}$$

2.4 The Cheater Identification Phase

If the reconstructed secret is not correct, each participant can identify who the cheater is by using the following steps.

1. After reconstructing the shared secret K, the participants can check whether the reconstructed secret is true by using the following equation:

$$\begin{aligned} g^K &\equiv \prod_{i=1}^{n} A_{(i,0)} \bmod p \\ &\equiv g^{a_{(1,0)} + a_{(2,0)} + \ldots + a_{(t,0)}} \bmod p \end{aligned} \tag{10}$$

2. If the above equation holds, we believe that all the participants are honest. Otherwise, each participant can verify the received S_i' by using the following equation:

$$g^{S_i'} \equiv \prod_{j=1}^{n} A_{(j,0)} \times \prod_{j=1}^{n} A_{(j,1)}^{ID_i} \times \ldots \times \prod_{j=1}^{n} A_{(j,t-1)}^{ID_i^{t-1}} \bmod p. \tag{11}$$

If the verification does not pass, it means that the participant U_i did not present a true S_i', i.e. U_i is dishonest. Therefore, we can accurately identify the cheater in this case.

3 A SIMPLE EXAMPLE

In this section, we give a simple example to illustrate the proposed scheme. Consider $(3, 5)$ threshold scheme in which 3 out of 5 participants can reconstruct the secret. Assume that a dealer selects $p = 73$, $q = 72$, and $g = 7$ and he/she wants to share the secret $K = 27$ among the 5 participants U_1, U_2, U_3, U_4, and U_5 with the unique identities 1, 2, 3, 4, and 5, respectively.

In the shadow generation phase, the dealer randomly generates 5 polynomials,

$$\begin{aligned} f_1(X) &= 5 + 11X + 8X^2 \bmod 72, \\ f_2(X) &= 4 + 3X + 26X^2 \bmod 72, \\ f_3(X) &= 6 + 9X + 14X^2 \bmod 72, \\ f_4(X) &= 7 + 19X + 6X^2 \bmod 72, \ \textit{and} \\ f_5(X) &= 5 + 22X + 2X^2 \bmod 72, \end{aligned}$$

where the shared secret $K = 5+4+6+7+5 = 27$. The dealer delivers $f_1(X)$, $f_2(X)$, ..., $f_5(X)$ to $U_1, U_2, \ldots, U_5$, respectively. Then, using Equation (2), the dealer computes the public information such that $A_{(1,0)} = 17$, $A_{(1,1)} = 52$, $A_{(1,2)} = 64$, $A_{(2,0)} = 65$, $A_{(2,1)} = 51$, $A_{(2,2)} = 49$, $A_{(3,0)} = 46$, $A_{(3,1)} = 10$, $A_{(3,2)} = 24$, $A_{(4,0)} = 30$, $A_{(4,1)} = 43$, $A_{(4,2)} = 46$, $A_{(5,0)} = 17$, $A_{(5,1)} = 3$, and $A_{(5,2)} = 49$. He/She publishes these parameters in a public bulletin board.

In the verification phase, U_1 computes and sends $S_{(1,2)} = f_1(2)$, $S_{(1,3)} = f_1(3)$, $S_{(1,4)} = f_1(4)$, and $S_{(1,5)} = f_1(5)$ to U_2, U_3, U_4, and U_5, respectively. U_2 computes and sends $S_{(2,1)} = f_2(1)$, $S_{(2,3)} = f_2(3)$, $S_{(2,4)} = f_2(4)$, and $S_{(2,5)} = f_2(5)$ to U_1, U_3, U_4, and U_5, respectively. U_3 computes and sends $S_{(3,1)} = f_3(1)$, $S_{(3,2)} = f_3(2)$, $S_{(3,4)} = f_3(4)$, and $S_{(3,5)} = f_3(5)$ to U_1, U_2, U_4, and U_5, respectively. U_4 computes and sends $S_{(4,1)} = f_4(1)$, $S_{(4,2)} = f_4(2)$, $S_{(4,3)} = f_4(3)$, and $S_{(4,5)} = f_4(5)$ to U_1, U_2, U_3, and U_5, respectively. U_5 computes and sends $S_{(5,1)} = f_5(1)$, $S_{(5,2)} = f_5(2)$, $S_{(5,3)} = f_5(3)$, and $S_{(5,4)} = f_5(4)$ to U_1, U_2, U_3, and U_4, respectively. After receiving the shadows from the other participants, each participant U_i checks whether the received shadows are valid by using Equation (4), such as

$$\begin{aligned} g^{S_{(1,2)}} &\equiv A_{(1,0)} \times A_{(1,1)}^{ID_2} \times A_{(1,2)}^{ID_2^2} \bmod p \\ &\equiv 17 \times 52^2 \times 64^{2^2} \bmod 73 \\ &\equiv 7^{59} \bmod 73 \\ &\equiv 52, \end{aligned}$$

and so on.

If all the verifications pass, the participants can cooperate to reconstruct the shared secret. Now, suppose that U_1, U_2, and U_3 want to cooperate to reconstruct the secret K. Using the received $S_{(2,1)}$, $S_{(3,1)}$, $S_{(4,1)}$, and $S_{(5,1)}$, U_1 can compute S_1' from Equation (6). Similarly, U_2 can compute S_2' and U_3 can compute S_3'. After that, U_1 sends S_1' to U_2 and U_3; U_2 sends S_2' to U_1 and U_3; U_3 sends S_3' to U_1 and U_2. After receiving S_2' and S_3', U_1 can reconstruct the secret by computing

$$\begin{aligned} K &\equiv (S_1' \times L_1) + (S_2' \times L_2) + (S_3' \times L_3) \bmod q \\ &\equiv (3 \times 3) + (19 \times 69) + (3 \times 1) \bmod 72 \\ &\equiv 27. \end{aligned}$$

Similarly, U_2 and U_3 can also compute the shared secret K by using Equation (7). U_1, U_2, and U_3 can verify the validity of the reconstructed secret by using Equation (9):

$$g^K \equiv A_{(1,0)} \times A_{(2,0)} \times A_{(3,0)} \times A_{(4,0)} \times A_{(5,0)} \bmod p. \tag{12}$$

If the verification holds, U_1, U_2, and U_3 accept the reconstructed secret as valid. Otherwise, at least one participant among U_1, U_2, and U_3 has presented a false S_i' to cheat the others. Similarly, to verify the shadow generated in Step 3 of the verification phase, we can use Equation (10) to check the validity of S_i'. If the verification does not pass, that means U_i is dishonest. Therefore, the cheater can be identified.

4 DISCUSSIONS

In this section, we shall examine the security of our proposed scheme. In addition, we shall also discuss the required computational and communicational overheads in our proposed scheme.

4.1 Security Analysis

In this section, we shall examine the security of our new scheme. The most important property of the (t, n) threshold secret sharing scheme is that only t or more participants can cooperate to reconstruct the shared secret. That means we have

to guarantee that $t-1$ or less participants cannot reconstruct the shared secret. In our proposed scheme, we apply the Lagrange interpolating polynomial to share the secret among a set of members. If the degree of the polynomial is $t-1$, that means we require t or more shadows for the reconstruction of the original polynomial. This ensures that we need t or more participants to reconstruct the shared secret $F(0) = K$.

In the following, we will show that any $t-1$ participants cannot recover the secret K.

In our scheme, the solutions for $\sum_{j=1}^{n} a_{(j,0)}$, $\sum_{j=1}^{n} a_{(j,1)}$, ..., $\sum_{j=1}^{n} a_{(j,t-1)}$ can be computed by the matrix form as follows:

$$\begin{bmatrix} 1 & \mathrm{ID}_1 & \mathrm{ID}_1^2 & \dots & \mathrm{ID}_1^{t-1} \\ 1 & \mathrm{ID}_2 & \mathrm{ID}_2^2 & \dots & \mathrm{ID}_2^{t-1} \\ \vdots & \vdots & \ddots & \vdots & \\ 1 & \mathrm{ID}_t & \mathrm{ID}_t^2 & \dots & \mathrm{ID}_t^{t-1} \end{bmatrix} \begin{bmatrix} \sum_{j=1}^{n} a_{(j,0)} \\ \sum_{j=1}^{n} a_{(j,1)} \\ \vdots \\ \sum_{j=1}^{n} a_{(j,t-1)} \end{bmatrix} = \begin{bmatrix} S_1' \\ S_2' \\ \vdots \\ S_t' \end{bmatrix}.$$

The coefficient matrix

$$\begin{bmatrix} 1 & \mathrm{ID}_1 & \mathrm{ID}_1^2 & \dots & \mathrm{ID}_1^{t-1} \\ 1 & \mathrm{ID}_2 & \mathrm{ID}_2^2 & \dots & \mathrm{ID}_2^{t-1} \\ \vdots & \vdots & \ddots & \vdots & \\ 1 & \mathrm{ID}_t & \mathrm{ID}_t^2 & \dots & \mathrm{ID}_t^{t-1} \end{bmatrix}$$

is called Vandermonde matrix and the determinant of the matrix is non-zero. Thus, the coefficients $(\sum_{j=1}^{n} a_{(j,0)}, \sum_{j=1}^{n} a_{(j,1)}, \dots, \sum_{j=1}^{n} a_{(j,t-1)})$ have a unique solution over the field Z_q.

If the $t-1$ participants $U_1, U_2, \dots, U_{t-1}$, attempts to recover the secret K, they obtain a system of $t-1$ linear equations with t unknowns such as

$$\begin{aligned} S_1' &= \sum_{j=1}^{n} a_{(j,0)} + \left(\sum_{j=1}^{n} a_{(j,1)}\right) \mathrm{ID}_1 + \left(\sum_{j=1}^{n} a_{(j,2)}\right) \mathrm{ID}_1^2 \\ &\quad + \dots + \left(\sum_{j=1}^{n} a_{(j,t-1)}\right) \mathrm{ID}_1^{t-1} \bmod q \\ S_2' &= \sum_{j=1}^{n} a_{(j,0)} + \left(\sum_{j=1}^{n} a_{(j,1)}\right) \mathrm{ID}_2 + \left(\sum_{j=1}^{n} a_{(j,2)}\right) \mathrm{ID}_2^2 \\ &\quad + \dots + \left(\sum_{j=1}^{n} a_{(j,t-1)}\right) \mathrm{ID}_2^{t-1} \bmod q \\ &\vdots \end{aligned} \tag{13}$$

$$S'_{t-1} = \sum_{j=1}^{n} a_{(j,0)} + \left(\sum_{j=1}^{n} a_{(j,1)}\right) \mathrm{ID}_{t-1} + \left(\sum_{j=1}^{n} a_{(j,2)}\right) \mathrm{ID}_{t-1}^{2} + \ldots + \left(\sum_{j=1}^{n} a_{(j,t-1)}\right) \mathrm{ID}_{t-1}^{t-1} \bmod q.$$

Suppose that they hypothesize a value S_0 for the key and let $F(0) = S_0$ be the t^{th} equation. Thus, the coefficient matrix of t equations with t unknowns will be a unique solution. Therefore, for each hypothesized value S_0, there is a unique polynomial $F'(x)$ such that

$$S'_i = F'(\mathrm{ID}_i),$$

for $i = 1, 2, \ldots, t-1$, and such that $S_0 = F'(0)$. Thus, no information of the key can be ruled out [12].

To prevent cheating, our proposed scheme provides a cheater detection and identification method. When a dishonest participant modifies his/her own shadow and offers it, as if it were kept intact, for the reconstruction of the shared secret, it must pass the test in the cheater identification phase. However, the action will be detected in Step 1 and be identified in Step 2 of the cheater identification phase. The dishonest participant will fail the test in the cheater identification phase.

Furthermore, the coefficients $a_{(i,0)}$'s of the polynomial $f_i(X)$ is critical to the security of the scheme. Since the shared secret K equals the sum of all coefficients $a_{(i,0)}$'s, if they are compromised, anyone can easily derive the shared secret K. Therefore, we must ensure that coefficients $a_{(i,0)}$ can never be derived from other ways, such as using the public information $A_{(i,0)}$ to obtain it.

If an adversary attempts to determine the coefficients $a_{(i,0)}$ from the public information $A_{(i,0)}$, he/she has to solve the discrete logarithm problem to find the unique exponent $a_{(i,0)}$, such that $g^{a_{(i,0)}} \equiv A_{(i,0)} (\mathrm{mod}\ p)$. However, the discrete logarithm problem cannot be solved in polynomial-time. Currently, there is still no algorithm which can solve this problem efficiently. In other words, the existing algorithms for computing discrete logarithms are very time consuming such as exhaustive search for all possible values $g^{a_{(i,0)}}$ in $O(p)$.

4.2 Required Computational and Communicational Overheads

Considering the shadow generation phase in the proposed (t, n) secret sharing scheme, the dealer has to generate n polynomials of degree $t-1$ and transmit them to the n members in U. Each transmitted polynomial contains t coefficients $a_{(i,1)}$, $a_{(i,2)}$, …, $a_{(i,t-1)}$, the binary value of $\{a_{(i,1)}, a_{(i,2)}, \ldots, a_{(i,t-1)}\}$ is between 1 and $q-1$. That is, the size of each coefficient must be less or equal to $\log_2(q)$. Therefore, the amount of the transmitted bits for each polynomial is $t\lceil \log_2(q) \rceil$ bits. Furthermore, the dealer has to compute $A_{(i,l)} = g^{a_{(i,l)}} \bmod p$ for all $1 \le i \le n$ and $0 \le l \le t-1$ and publish them to public bulletin board.

In total, the following computations are required in the shadow generation phase:

- n polynomial generations, and
- nt modular exponential computations.

Furthermore, the following communications are required:

- transmitting n polynomials required $nt\lceil \log_2(q) \rceil$ bits, and
- broadcasting $A_{(i,l)}$.

In the verification phase, each participant U_i has to compute and transmit $S_{(i,j)}$ to other $(n-1)$ members in U, each participant requires $n-1$ polynomial computations and $(n-1)\lceil \log_2(q) \rceil$ bit transmissions. After receiving $S_{(i,j)}$ for all $1 \leq j \leq n$, $i \neq j$, U_i, U_i has to confirm the validity of $S_{(i,j)}$ by checking whether or not $g^{S_{(j,i)}} \bmod p$ satisfies Equation (5). Each U_i performs the verification $n-1$ times and each verification requires t modular exponential computations and $t-1$ modular multiplications.

In total, each U_i requires the following computations in this phase:

- $n-1$ polynomial computations,
- $(n-1)t$ modular exponential computations, and
- $(n-1)(t-1)$ modular multiplications.

And, the communication is

- $(n-1)\lceil \log_2(q) \rceil$ bits.

In the secret reconstruction phase, each actual participant U_i computes $S_{(i,i)}$ and S_i' by using Equations (6) and (7), respectively. It requires 1 polynomial computation and $(n-1)$ modular additions. Then, each actual participant U_i transmits S_i' ($\lceil \log_2(q) \rceil$ bits) to the other participants in the qualified subset. Finally, each U_i in γ can recover the secret K by using Equation (8). It requires $t(t-1)$ modular multiplications and $t-1$ modular additions.

The total computations for each participant in γ in the secret reconstruction phase are listed below:

- 1 polynomial computation,
- $t(t-1)$ modular multiplications, and
- $(n-1)+(t-1)$ modular additions.

And, the communication is

- $(t-1)\lceil \log_2(q) \rceil$ bits.

In the cheater identification phase, each participant U_i performs Equation (10) to check the validity of the recovered secret K. It requires 1 modular exponential computation and $n-1$ modular multiplications. Furthermore, the actual participant

can perform Equation (11) to verify the validity of the received S_i'. It requires $n(t-1)+1$ modular exponential computations and $nt-1$ modular multiplications.

The information rate is used to measure the efficiency of secret sharing scheme. The information rate for $U_i \in U$ is $\rho_i = \frac{H(K)}{H(S_i)}$, where $H(K)$ is the entropy of the secret K and $H(S_i)$ is the entropy of the share assigned to U_i. The perfect secret sharing scheme is that the length of the secret equals the length of the share held by a participant, so $\rho_i = 1$ [10]. In our scheme, each participant holds a polynomial, which contains t coefficients, and $n-1$ shadows $S_{(j,i)}$'s from the other participants U_j's in U. The secret K, the coefficients $a_{(i,1)}$, $a_{(i,2)}$, ..., $a_{(i,t-1)}$, and the shadows $S_{(i,j)}$'s are all in $GF(q)$. Therefore, the information rate of our scheme is $\rho = \frac{1}{t+n-1}$.

5 CONCLUSIONS

In this paper, we presented a novel and secure (t, n) threshold secret sharing scheme with cheater identification. In summary, our scheme possesses the following three desirable features. They are (1) a flexible choice of the threshold value t, (2) a guarantee that t or more participants can reconstruct the shared secret, but $t-1$ or less cannot, and (3) identification of cheaters.

Acknowledgements

The authors wish to thank many anonymous referees for their suggestions to improve this paper.

REFERENCES

[1] American National Standards Institute: ANSI X9.30.1-1997: Public-Key Cryptography for the Financial Services Industry – Part 1: The Digital Signature Algorithm (DSA). American Bankers Association, 1997.

[2] Blakley, G. R.—Meadows, C.: Security of Ramp Schemes. Advance in Cryptology-Crypto '84, Lecture Notes in Computer Science, Vol. 196, 1984, pp. 242–268.

[3] Brickell, E. F.—Stinton, D. R.: The Detection of Cheaters in Threshold Schemes. Advance in Cryptology-Crypto '88, Lecture Notes in Computer Science, Vol. 403, 1988, pp. 564–577.

[4] Chang, C. C.—Hwang, R. J.: Efficient Cheater Identification Method for Threshold Schemes. IEE-Proceedings on Computer. Digit. Tech., Vol. 144, 1997, No. 1, pp. 23–27.

[5] Federal Information Processing Standards: FIPS 186: Digital Signature Standard (DSS), 1994.

[6] Hwang, R. J.—Chang, C. C.: An On-line Secret Sharing Scheme for Multi-secrets. Computer Communications, Vol. 21, 1998, No. 13, pp. 1170–1176.

[7] Hwang, R. J.—Lee, W. B.—Chang, C. C.: A Concept of Designing Cheater Identification Methods for Secret Sharing. The Journal of Systems and Software, Vol. 46, 1999, No. 1, pp. 7–11.

[8] Krawczyk, H.: Secret Sharing Made Short. Advance in Cryptology-Crypto '93, Lecture Notes in Computer Science, Vol. 773, 1993, pp. 136–146.

[9] Lee, W. B.—Chang, C. C.: A Dynamic Secret Sharing Scheme Based on the Factoring and Diffie-Hellman Problems. IEICE Transactions on Fundamentals, Vol. E81-A, 1998, No. 8, pp. 1170–1176.

[10] Pieprzyk, J.—Hardjono, T.—Seberry, J.: Fundamentals of Computer Security. Springer-Verlag, Chapters 9 and 10, 2003.

[11] Shamir, A.: How to Share a Secret. Communications of ACM, Vol. 22, 1979, No. 11, pp. 612–613.

[12] Stinson, D. R.: Cryptography Theory and Practice. CRC Press, Chapter 11, 1995.

[13] Sun, H. M.—Shieh, S. P.: Construction of Dynamic Threshold Schemes. Electronics Letters, Vol. 30, 1994, No. 24, pp. 2023–2024.

[14] Tompa, M.—Woll, H.: How to Share a Secret With Cheaters. Journal of Cryptology, Vol. 1, 1988, No. 2, pp. 133–138.

Iuon-Chang Lin received the B. Sc. in computer and information sciences from Tung Hai University, Taichung, Taiwan, Republic of China, in 1998; the M. Sc. in Information Management from Chaoyang University of Technology, Taiwan, in 2000. He received his Ph. D. in computer science and information engineering in March 2004 from National Chung Cheng University, Chiayi, Taiwan. He is currently an assistant professor of the Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan, ROC. His current research interests include electronic commerce, information security, cryptography, and mobile communications.

Chin-Chen Chang obtained his Ph. D. degree in computer engineering from National Chiao Tung University. His first degree is Bachelor of Science in applied mathematics and Master of Science in computer and decision sciences, from National Tsing Hua University. Dr. Chang served in National Chung Cheng University from 1989 to 2005. His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from February 2005.

Prior to joining Feng Chia University, Professor Chang was an associate professor in Chiao Tung University, professor in National Chung Hsing University, chair professor in National Chung Cheng University. He had also been Visiting Researcher and Visiting Scientist to Tokyo University and Kyoto University, Japan. During his service in Chung Cheng, Professor Chang served as Chairman of the Institute of Computer Science and Information Engineering, Dean of College of Engineering, Provost and then Acting President of Chung Cheng University and Director of Advisory Office in Ministry of Education, Taiwan.

Professor Chang's topics of research interests include, but are not limited to, data engineering, database systems, computer cryptography and information security. A researcher of acclaimed and distinguished services and contributions to his country and advancing human knowledge in the field of information science, Professor Chang has won many research awards and honorary positions by and in prestigious organizations both nationally and internationally. He is currently a Fellow of IEEE and a Fellow of IEE, UK. And since his early years of career development, he consecutively won Outstanding Youth Award of the R. O. C., Outstanding Talent in Information Sciences of the R. O. C., AceR Dragon Award of the Ten Most Outstanding Talents, Outstanding Scholar Award of the R. O. C., Outstanding Engineering Professor Award of the R. O. C., Chung-Shan Academic Publication Awards, Distinguished Research Awards of National Science Council of the R. O. C., Outstanding Scholarly Contribution Award of the International Institute for Advanced Studies in Systems Research and Cybernetics, Top Fifteen Scholars in Systems and Software Engineering of the Journal of Systems and Software, and so on. On numerous occasions, he was invited to serve as Visiting Professor, Chair Professor, Honorary Professor, Honorary Director, Honorary Chairman, Distinguished Alumnus, Distinguished Researcher, Research Fellow by universities and research institutes. He also published over 850 papers in information sciences. In the meantime, he participates actively in international academic organizations and performs advisory work to government agencies and academic organizations.