A Fair (*t*,*n*) Threshold Secret Sharing Scheme

Minhong Xing
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Beijing, China
buptxingminhong@163.com

Wenmin Li
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Beijing, China
liwenmin02@gmail.com

***Abstract*—The cloud service provider offers various storage services for mass data. However, for safety and recovery concern, the provider distributes the components of the data file on different servers. Therefore it is important to design appropriate secret sharing scheme. In this paper, we hide the real secret value in a sequence of pseudo secrets in order to decrease the probability of the cheater achieving a successful guess. We also use the multiple secret sharing techniques to realize efficient distribution and reconstruction, which reduce the storage burden of the user. Furthermore, we also make some analyses of our scheme and do some comparisons. Our scheme provides better secret reconstruction and helps improve the fairness of the existing scheme.**

Keywords—secret sharing; secret reconstruction; multiple secret sharing; fairness

I. INTRODUCTION

Cloud storage is a promising technology that alters the traditional storage habits of users. People could share photos, music or synchronize data files on the cloud. In the cloud storage environment, the service provider distributes the data file on different storage nodes, in order to ensure the security of the secret information. The secret sharing schemes could offer approaches to solve the issues. Thus it is of great importance to study the secure and highly efficient secret sharing scheme.

In 1979, Shamir [1] and Blakeley [2] firstly proposed the secret sharing schemes based on the Lagrange interpolation polynomial and projective geometry concepts respectively. Since then the secret sharing scheme has become an important research project. The secret sharing algorithm consists of secret distribution and secret reconstruction. Many discussions on designing secret sharing schemes have been proposed, such as verifiable secret sharing schemes [3], multiple secret sharing [4] and secret sharing without a mutually trusted party [5]. However, the secret reconstruction scheme needs to be further studied since the unfair sharing in the traditional mechanism has to be solved.

Tompa and Woll [6] were the first to propose a fair reconstruction policy. Their idea is to conceal the real secret value s in a sequence of random values so that the cheater has to guess the correct position of s. However, the policy requires that all the participants should release their shadows synchronically which is impractical if there is no other protocol supporting it. Lin and Harn[7] proposed the first fair secret construction protocol, which we will call LH scheme for short in the following. It is also designed as hiding real secret value in a random sequence. Their scheme is not forced to synchronize and could combine with other secret sharing scheme in order to realize any secret sharing policy. However, if the sequence is short, the cheater will gain a great advantage to achieve a successful guess. In 2013, Tian et al. [8] proposed a scheme, which we will call TMPJ scheme for short in the following. They gradually release the information to realize the fairness of secret sharing. However, in 2014, Harn [9] pointed out that TMPJ scheme still had some security problems.

In TMPJ scheme, the participants have to store multiple pseudo secret shadows in each round of construction, which increases the storage burden of the participant. The multiple secret sharing schemes can solve this issue. In 2008, Pang [10] proposed a multiple secret sharing scheme using a two-variable one-way function, in which participants could reuse their secret shadows. The dealer just needs to change one parameter and each participant needs to hold only one shadow.

In this paper, we proposed a fair (t,n) threshold secret sharing scheme. We first devise a modified scheme using the two-variable one-way function, which is based on TMPJ scheme. In our modified scheme the participants only hold one piece of secret shadow and just reuse it in each round of reconstruction. Then we use the improved TMPJ scheme to design a new secret sharing scheme and improve the fairness. Our scheme could ensure better fairness and reduce the storage cost of the user.

This work is supported by NSFC (Grant Nos. 61300181, 61202434), the Fundamental Research Funds for the Central Universities (Grant No. 2015RC23).

II. PRELIMINARIES

A. Shamir's Secret Sharing Scheme

The scheme consists of three phases [1].

(1) Parameter Selection

Choose a prime p which is greater than all the possible secrets and shadows. S denotes the secret value. There are n members in the system and at least t participants could recover S. And the dealer distributes the shadows to the participants.

(2) Secret Distribution

Randomly chooses $t-1$ numbers $s_1, s_2, ..., s_{t-1}$ to construct the polynomial:

$s(x) = S + s_1 x + ... + s_{t-1} x^{t-1} (\text{mod } p)$, where $s(0) \equiv S \bmod p$.

Randomly chooses n numbers $x_1, x_2, ..., x_n$ which are no less than p and calculates $y_i \equiv S(x_i) \bmod p$ to construct the pair (x_i, y_i).

The dealer distributes the n pairs (x_i, y_i) to the participants, where $i = 1, 2, ..., n$.

(3) Secret Reconstruction

Assume that t participants, with pair (x_i, y_i) each, work together to recover S. They firstly compute $f(x) \equiv \sum_{k=1}^{t} y_k \prod_{j=1, j\neq k}^{t} \frac{x - x_j}{x_k - x_j} (\text{mod } p)$. Set $x = 0$ and get $f(0)$, which is the secret S.

B. Two-Variable One-Way Function

We consider a function as a two-variable one-way function [10] if it satisfies the following properties.

(1) Given r and x, $f(r, x)$ will be easily computed.

(2) Given x and $f(r, x)$, it is hard to obtain r.

(3) For any r, it is hard to compute $f(r, x)$, without knowing x.

(4) Given r and $f(r, x)$, it is hard to obtain x.

(5) Given x, it is hard to find two different r_1 and r_2 so that $f(r_1, x) = f(r_2, x)$.

(6) Given pairs of r_i and $f(r_i, x)$, it is hard to compute $f(r', x)$ when $r' \neq r_i$.

III. OUR CONSTRUCTION

A. Improved Scheme of TMPJ

Phase 1: Parameter selection

$P_1, \ldots, P_n$ respectively denote n participants. $s \in GF(p)$ denotes the secret to be distributed. p denotes a prime greater than n. $s' \in GF(p)$ is chosen randomly as the stop indicator. The random value α_i is chosen as the identification of participant P_i. And $f(r, x)$ is a two-variable one-way function.

Phase 2: Secret distribution

The dealer runs the following algorithm.

(1) The dealer randomly chooses n numbers, $x_1, \ldots, x_n$, as the secret shadows for the participants $P_1, \ldots, P_n$.

(2) The dealer randomly chooses k numbers, $a_{10}, \ldots, a_{(l-1)0}, a_{l0}, \ldots, a_{k0}$, $(l \in [1, k])$. Set the value of $a_{(l-1)0}$ and a_{l0} as $a_{(l-1)0} = s - \sum_{i=1}^{l-2} a_{i0}$, $a_{l0} = s'$.

(3) For each a_{i0}, the dealer randomly chooses an integer r_i, and calculates the two-variable one-way function $f(r_i, x_i)$ for each secret shadow x_j of participant P_j.

(4) For each a_{i0}, the dealer uses $(0, a_{i0})$ and $(u_j, f(r_i, x_j))$ $(j = 1, \ldots, n)$ to construct the n th polynomial $g_i(x) = a_{i0} + a_{i1} x + \ldots + a_{n1} x^n$.

(5) The dealer chooses $n+1-t$ minimum integers d_{ji} $(j = 1, \ldots, n+1-t)$ from the set $[1, p-1] \setminus \{\alpha_j \mid j = 1, \ldots, n\}$ and then calculates $g(d_{ji})$.

(6) Release system parameters p, s' and parameter $(r_i, g(d_{1i}), g(d_{2i}), \ldots, g(d_{(n+1-t)i}))$.

Phase 3: Secret reconstruction

Every m $(m > t)$ participants could cooperate to recover the secret value s. Here we suppose the first m participants will succeed.

(7) In the first round, participant P_j firstly computes the pseudo secret shadow $s_{j2} = f(r_2, x_j)$ and sends the pseudo secret shadow to the other participants. Otherwise, halt the protocol, which means, the protocol should be executed in order.

(8) In the i th round, participant P_j computes the pseudo secret shadow $s_{jI} = f(r_i, x_j)$ and sends s_{ji} to the other participants.

(9) In the i th round, all the sub-secrets of $i-1$ th round released by the other participants have been received by participant P_j. If the sequence of sub-secrets is $(s_{1i}, ..., s_{(j-1)i}, s_{(j+1)i}, ..., s_{mi})$, the reconstruction algorithm continues. Otherwise, participant P_j announces that there is a malicious participant in the system and halts the protocol.

(10) Still in the i th round, we set $T_i = \{T_{i1}, ..., T_{iu}\}$, where $u = \binom{m}{t}$. The participant picks t pseudo secret shadows from $\{s_{1i}, ..., s_{mi}\}$ and sets them as the elements in T_i. Use the t pseudo secret shadows in T_{ii} and α_i to construct (α_i, s_{ji}). Then the participant chooses $n+1-t$ minimum integers d_{ji} from set $[1, p-1] \setminus \{\alpha_j \mid j = 1, \ldots, n\}$ and constructs $(d_{ji}, g(d_{ji}))$ according to the public parameters $g(d_{ji})$. The above $n+1$ tuples could be denoted as (X_c, Y_c) $(c = 1, 2, \ldots, n+1)$. The β th degree polynomial $g_i(x)$ can be calculated as $g_i(x) = \sum_{c=1}^{n+1} Y_c \prod_{d=1, d\neq c}^{n+1} \frac{x - X_j}{X_i - X_j} = a_{i0} + a_{i1}x + \ldots + a_{n1}x^n$.

If $\beta = n$, then the reconstruction algorithm continues. Otherwise, participant P_j announces that there is malicious participants in the system and halts the protocol.

(11) If there exists a pseudo secret shadow $s_{ei} \in \{s_{1i}, ..., s_{mi}\} \setminus T_{ii}$ does not satisfy the polynomial $g_i(x)$, namely $s_{ie} \neq g_i(e)$, it means that there is a malicious participant and the protocol will be halted. Otherwise, it means that all the participants act honestly in this round.

Participant P_j will compute and send the next pseudo secret $s_{ji} = f(r_i, x_j)$ to the other participants.

(12) If every step in (7)~(12) could be executed correctly, then $X = g_i(0)$ will be calculated. If $X \neq s'$, this means that all the participants act honestly in this round of reconstruction. P_j will compute and send the next pseudo secret to the other participants.

(13) According to the above description, when $X = s'$, the participant obtains all the secret shadows used for construction. Therefore, the secret value can be recovered as $s = \sum_{i=1}^{l-1} g_i(0) = \sum_{i=1}^{l-1} a_{i0}$.

B. A new fair (t,n) threshold secret sharing scheme

Phase 1: Parameter selection

$P_1, \ldots, P_n$ respectively denote n participants. $s \in GF(p)$ denotes the secret to be distributed. p denotes a prime greater than n. $s^* \in GF(p)$ is the location indicator of s. $s' \in GF(p)$ is chosen randomly as the stop indicator.

Phase 2: Secret distribution

The dealer runs the following algorithm.

(1) The dealer randomly chooses $k+1$ unique numbers to form a $(k+1)$ -elements sequence $S = \{s_1, \cdots, s_k\}$. Set $s_{J+1} = s^*$, $s_L = s - s_J$, $s_{L+1} = t^*$, where $J < L \in [1, k-1]$

(2) For each $s_i \in S$, in the distribution phase of s_i, the protocol in section Ⅲ-A will be executed correctly. As in the improved scheme of TMPJ, the Dealer distributes the secret shadows of different sub-secrets by changing parameter r in the two-variable one-way function $f(r_i, x_i)$. Participant P_j will receive $x_j^{(i)}$ as his secret shadow.

(3) Release the parameters p, s^*, t^*, s'.

Phase 3: Secret reconstruction

(4) In order to reconstruct each element in S, the algorithm is executed correctly as the protocol described in section Ⅲ-A. In the r th round, each participant P_j presents his pseudo secret share $s_{jr}^{(i)}$. Until the $(l-1)$ th round, all the participants recover the constant term s' of the polynomial, and they can finally get s_i.

(5) When all the participants of any qualified subset reconstruct the secret value, they have to reconstruct $s_1, s_2, \ldots, s_{L-1}$, s_L, and s_{L+1} accordingly until they obtain s_{J+1} and s_{L+1}. Then verify that $s_{J+1} = s^*$ and $s_{L+1} = t^*$.

(6) The participants now could assure the previously derived value s_J and s_L are what they need. They add s_J and s_L together to obtain the secret value s.

IV. COMPARISONS

A. Fairness

In LH scheme, the dealer conceals the real secret value s in the k -elements sequence and uses an indicator to point out the location of s. However, if the dishonest participant successfully guesses the correct location of s, he will exclusively obtain s, while the other participants cannot, and the probability is $1/k$. Assume the case that k is very small, such as $k = 2$, the dishonest participants will obtain s with the probability of $1/2$. This largely decreases the security level of this scheme.

In TMPJ scheme, the dealer breaks the secret shadow of the participants into sub-secrets. The scheme is novel and decreases the probability of the dishonest participant obtaining s to $1/C_k^{l-1}$. However, after $l-1$ round computations, the dishonest participant can use the secret shadow derived in each round to reconstruct s. The fairness of the scheme still needs to be improved.

Our scheme is inspired by LH scheme and TMPJ scheme. We improve both of the two schemes and construct a fair (t, n) threshold secret sharing scheme. In our scheme, the probability of a dishonest participant exclusively obtaining s is not greater than $\frac{1}{k^2 \cdot (C_k^{l-1})^2}$.

TABLE I. ADVANTAGE COMPARISON

Scheme	Efficiency
LH Scheme	$1/k$
TMPJ Scheme	$1/C_k^{l-1}$
Our Scheme	$1/k^2 \cdot (C_k^{l-1})^2$

TABLE II. EFFICIENCY COMPARISON

Scheme	Efficiency
LH Scheme	$(L+1)\cdot T_L(t)$
TMPJ Scheme	$l\cdot(T_L(t)+(m-t)T_p)$
Our Scheme	$(L+1)l\cdot(T_L(t)+(m-t)T_p)$

We assume that the dishonest participant and the other $t-1$ participants have reconstructed a sequence of values $s_1, s_2, \ldots, s_{L+1}$, namely that s_J and s_L have been recovered. In the process of recovering each value s_i in the sequence S, we use the improved TMPJ algorithm to do l round computation. By using the $l-1$ polynomials to reconstruct, the probability of the dishonest participant correctly guessing s_i is no greater than $1/C_k^{l-1}$. Moreover, like the LH scheme, the probability of the dishonest participant correctly guessing s_i in the k-elements sequence is no greater than $1/k$. Therefore, according to the secret sharing policy, the probability of a dishonest participant exclusively obtaining s is not greater than $\frac{1}{k^2 \cdot (C_k^{l-1})^2}$. The security and fairness of our scheme is highly improved as we can see in TABLE Ⅰ.

B. Efficiency

In our construction, we introduce the two-variable one-way function $f(r,x)$. For the case of multiple unique secret values, by changing the value of r, we distribute the secret shadow for each participant only once. Therefore the participants only need to store one piece of secret shadow each during the secret sharing process. We highly reduce the storage cost of the participants, while in TMPJ scheme multiple secret shadows need to be released.

We make a comparison of the efficiency in the secret reconstruction phase in TABLE Ⅱ, where $T_L(t)$ denotes the computational cost of the Lagrange interpolation polynomial with t points, and T_p denotes the computational cost of polynomial verification.

In LH scheme, for a k-elements sequence, t participants are cooperating to reconstruct the secret. There will be $L+1$ round operations, and in each operation, the computational cost of the Lagrange interpolation polynomial will be $T_L(t)$.

In TMPJ scheme, for a k-elements sequence, m $(m>t)$ participants are cooperating to reconstruct the secret. There will be l round operations. In each operation, the computational cost of the Lagrange interpolation polynomial will be $T_L(t)$ and the computational cost of polynomial verification will be $(m-t)T_p$.

In our scheme, we hide the real secret value s in the k-elements sequence S. When recovering each s_i in S, we use the improved TMPJ scheme which executes l round computations. And we will execute the operation $L+1$ times.

Although our scheme has some loss in efficiency, however, we improve the fairness and security. Therefore it is an applicable scheme.

V. CONCLUSIONS

In this paper, we study the fair reconstruction of the secret value. By using the two-variable one-way function, we improve the TMPJ scheme and realize multi-secret sharing. Based on our improvement, we propose a new fair secret sharing scheme. In the reconstruction phase, we use Lagrange interpolation polynomial and polynomial verification to detect whether there is a dishonest participant in the system. Once the cheater is detected, the protocol halts immediately. Moreover, we hide the real secret value in the sequence in order to decrease the probability of the cheater achieving a successful guess and improve the fairness.

ACKNOWLEDGMENT

This work is supported by NSFC (Grant Nos. 61300181, 61202434), the Fundamental Research Funds for the Central Universities (Grant No. 2015RC23).

REFERENCES

[1] Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613.

[2] Blakley, George Robert. "Safeguarding cryptographic keys." In Managing Requirements Knowledge, International Workshop on, pp. 313-313. IEEE Computer Society, 1899.

[3] Shao, Jun. "Efficient verifiable multi-secret sharing scheme based on hash function." Information Sciences 278 (2014): 104-109.

[4] Shyu, Shyong Jian, and Hung-Wei Jiang. "General constructions for threshold multiple-secret visual cryptographic schemes." Information Forensics and Security, IEEE Transactions on 8, no. 5 (2013): 733-743.

[5] Ingemarsson, Ingemar, and Gustavus J. Simmons. "A protocol to set up shared secret schemes without the assistance of a mutually trusted party." In Advances in Cryptology—EUROCRYPT'90, pp. 266-282. Springer Berlin Heidelberg, 1991.

[6] Tompa, Martin, and Heather Woll. "How to share a secret with cheaters." *journal of Cryptology* 1, no. 3 (1989): 133-138.

[7] Lin, Hung-Yu, and Lein Harn. "Fair reconstruction of a secret." Information Processing Letters 55, no. 1 (1995): 45-47.

[8] Tian, Youliang, Jianfeng Ma, Changgen Peng, and Qi Jiang. "Fair (t, n) threshold secret sharing scheme." Information Security, IET 7, no. 2 (2013): 106-112.

[9] Harn, Lein. "Comments on'fair (t, n) threshold secret sharing scheme'." Information Security, IET 8, no. 6 (2014): 303-304.

[10] Pang, Liaojun, Huixian Li, Ye Yao, and Yumin Wang. "A verifiable (t, n) multiple secret sharing scheme and its analyses." In Electronic Commerce and Security, 2008 International Symposium on, pp. 22-26. IEEE, 2008.