International Journal of Security and Its Applications
Vol.9, No.1 (2015), pp.191-204
http://dx.doi.org/10.14257/ijsia.2015.9.1.20

A (n,t,n) Verifiable Multi-secret Sharing Scheme with Secure Secret Reconstruction

Li Meng[1], Qu Shaoyun[2], Xun Tiantian[1] and Yu Jia[1,3*]

[1]*College of Information Engineering, Qingdao University, 266071 Qingdao, China*
[2] *Software Technology College, Qingdao University, 266071 Qingdao, China*
[3]*Shandong provincial Key Laboratory of Computer Network, 250014 Jinan, China*
Email: given210@126.com, dqqsy@163.com, xuntian0412@163.com, yujia@qdu.edu.cn

Abstract

In a verifiable multi-secret sharing scheme, multiple secrets can be shared in one process and the shares can be verified. We propose a novel verifiable multi-secret sharing scheme in this paper. The scheme has the following advantages: (i) A mutually trusted dealer is no longer needed to distribute shares; (ii) shares can be verified by shareholders both in the secret generation and reconstruction phases; and (iii) any adversary without providing a valid share cannot recover the real secrets in the secret reconstruction phase. A secret sharing scheme with above-mentioned advantages is also described as a stepping stone, before we propose the multi-secret sharing scheme. We give the definition of a (n,t,n) verifiable (multi-)secret sharing scheme with secure secret reconstruction, which both of the proposed schemes meet. The security analysis of the proposed two schemes and the comparisons among the proposed multi-secret scheme and some other ones are also represented.

Keywords: *Multi-secret sharing; Secure secret reconstruction; Verifiability;* (n,t,n) *scheme*

1. Introduction

The concept of secret sharing scheme was first developed by Shamir [1] and Blakley [2] independently in 1979 as a solution to safeguard cryptographic keys. After that, secret sharing schemes have been extensively studied in many literatures [3-4]. In Shamir's (t,n) threshold secret sharing scheme [1], a secret is divided into n shares by a mutually trusted dealer and the n shares are distributed to n shareholders respectively, so that any t or more than t shareholders can recover this secret; but fewer than t shareholders cannot recover the secret. However, in Shamir's scheme [1], the dealer must stay honest and make no mistakes while distributing shares to shareholders, and the shareholders should unconditionally trust the shares from the dealer are valid. In order to solve the problem that shareholders cannot verify their shares, Chor e*t al.* [5] presented a verifiable secret sharing scheme by extending Shamir's scheme [1]. In a verifiable secret sharing scheme, shareholders are able to verify if the shares they received from the dealer are consistent or not.

In addition, the need of a mutually trusted dealer in Shamir's scheme [1] is another problem, because a trusted dealer might be impossible in some applications, such as wireless multimedia sensor networks and ad hoc networks. Ingemarsson and Simmons [6] tried to overcome the restriction and considered a secret sharing scheme without the assistance of a

* Corresponding author: yujia@qdu.edu.cn

ISSN: 1738-9976 IJSIA

mutually trusted dealer. Then Pedersen [7] proposed a joint (n, t, n) secret sharing scheme. The three parameters n, t, n refer to the number of dealers, the value of the threshold and the number of shareholders respectively. In Pedersen's (n, t, n) scheme, n shareholders, which are considered as dealers as well, generate and share a master secret in a joint way. Each shareholder first selects a random sub-secret, then shares the sub-secret with the other shareholders by utilizing Shamir's scheme [1]. And the master secret recovered in the reconstruction phase is the sum of all sub-secrets. As a result, the secret shared among shareholders is actually determined by all shareholders jointly.

In all above schemes, only one secret can be shared during each sharing process. The secret sharing scheme was designed as a key ingredient in the standard distributed cryptosystem. So did it happen to the multi-secret sharing scheme, which became a key tool when designing a multi-policy distributed cryptosystem. A multi-secret sharing scheme is supposed to distribute many different secrets among the shareholders in one process. As a trivial solution, a secret sharing scheme can be executed several times to accomplish this desire. In this case, the length of each secret share depends on the number of secrets. So the length of share may be unacceptable, when a great number of secrets are shared in one process. Obviously, the trivial way is not an ideal solution to share multiple secrets. Then He and Dawson proposed two nontrivial schemes [8-9] to share multiple secrets in one process. Since then, multi-secret sharing schemes have been studied in many papers [12-23]. Recently, Lein Harn [11] proposed a secure multi-secret sharing scheme, utilizing the linear combination of shares to protect the secrets from adversaries. Harn's scheme [11] solved the problem that shared secrets could be obtained by an adversary who provides no share in the situation that there are more than t shareholders participating in the secret reconstruction phase. However, this scheme depends on a mutually trusted dealer and the shares cannot be verified. But a mutually trusted dealer is not always available in many applications and verifiability is a quite significant property for secret sharing schemes. Especially in a (n, t, n) scheme, all shareholders participant in the secret generation phase and they are mutually distrusted. Consequently, it is even more desirable to possess the verifiable property in (n, t, n) secret sharing schemes.

We first give the definition of a (n, t, n) verifiable (multi-)secret sharing scheme with secure secret reconstruction and the security requirements. Then a secret sharing scheme is given as a stepping stone. We propose a multi-secret sharing scheme by extending the given secret sharing scheme. As desired, our schemes are verifiable, can execute without a mutually trusted dealer, and have the good property of secure secret reconstruction. The security of the verification phase is based on the hardness of computation Diffie-Hellman problem. Without the help of a mutually trusted dealer makes our schemes more flexible. And our schemes can resist the attacks from the adversaries who try to obtain secrets but provide no valid shares. As far as we know, there have not been any secret sharing schemes that possess the three properties at the same time until now.

We organize the rest of this paper as follows. Some preliminaries about our schemes, inclu ding Shamir's (t, n) secret sharing scheme, Pedersen's (n, t, n) secret sharing scheme and Harn's secure secret reconstruction scheme, are provided in the next section. A definition and the security requirements are represented in section 3. The proposed two schemes are elaborat ed in section 4 and section 5 respectively. In section 6, the comparisons among the proposed multi-secret scheme and some other multi-secret schemes are discussed. Section 7 includes th e conclusion of this work.

2. Preliminaries

In this section we briefly describe three previous schemes, Shamir's (t, n) secret sharing scheme, Pedersen's (n, t, n) secret sharing scheme and Harn's secure secret reconstruction scheme.

2.1. Shamir's (t, n) Secret Sharing Scheme [1]

Secret S is divided into n shares by a mutually trusted dealer and shared among n shareholders $P = \{P_1, \cdots, P_n\}$. n and t represent the number of shareholders and the threshold of the scheme respectively. p is a large prime, and all operations are performed in the finite field $GF(p)$. Shamir's scheme has two algorithms: share generation and secret reconstruction.

(1) Share generation

Firstly, the dealer D selects a random polynomial $f(x)$ of degree $t-1$: $f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} \bmod p$, where $a_1, \cdots, a_{t-1} \in GF(p)$ and $a_0 = S$. D computes shares $S_i = f(i)(i = 1, \cdots, n)$ and distributes each share S_i to shareholder P_i secretly.

(2) Secret reconstruction

Suppose the secret S is recovered by the subset P_{RE} of P, where $|P_{RE}| \geq t$. Then participants of P_{RE} reconstruct S using the Lagrange interpolating formula:

$$S = \sum_{P_i \in P_{RE}} S_i \prod_{P_j, P_j \in P_{RE}, i \neq j} \frac{j}{j - i} \bmod p .$$

2.2. Pedersen's (n, t, n) Secret Sharing Scheme [7]

The master secret S, which is shared among n shareholders, is the sum of the sub-secrets selected by shareholders. There is no dealer in the scheme, and each shareholder does the job the dealer is supposed to do. Intuitively, each shareholder in this scheme participates to generate and share the master secret. This scheme consists of four algorithms: master secret generation, sub-share generation, master share generation and master secret reconstruction.

(1) Master secret generation

Each shareholder P_i selects a random sub-secret S_i independently and the master secret S is the sum of all the sub-secrets: $S = \sum_{i=1}^{n} S_i = S_1 + \cdots + S_n$.

(2) Sub-share generation

P_i selects a random polynomial $f_i(x)$ of degree $t-1$, such that $f_i(0) = S_i$, and generates sub-shares $s_{ij} = f_i(x_j)(j = 1, \cdots, n)$ for other shareholders using Shamir's secret sharing scheme. P_i sends s_{ij} to shareholder $P_j (j = 1, \cdots, n)$ secretly. After all sub-shares are sent, each shareholder P_i has n sub-shares $s_{ji} (j = 1, \cdots, n)$.

(3) Master share generation

P_i computes the master share s_i with the n received sub-shares s_{ij} :

$$s_i = \sum_{j=1}^{n} s_{ji} = \sum_{j=1}^{n} f_j(x_i).$$

(4) Master secret reconstruction

When t or more than t shareholders release their master shares to reconstruct the master secret, the master secret S can be reconstructed by using the Lagrange interpolating formula.

2.3. Harn's Secure Secret Reconstruction Scheme [11]

A secret reconstruction scheme is secure when it makes sure that anyone without a valid sh are cannot reconstruct the real secret. It means that neither an outside adversary[1] nor an insid e adversary[2] can obtain the real secret without providing a valid share in a secure reconstructi on scheme. Sometimes there might be more than t shareholders participating in the secret re construction. When it happens, most papers suggest taking t of them to recover the secret. H owever, this approach causes a security problem that outside adversaries may pretend as share holders participating in the reconstruction but provide no share at all. As only t shares are n eeded to recover the secret, the adversaries can still obtain the secret when being aware of t valid shares from honest shareholders. In addition, inside adversaries (colluded shareholders) may collude trying to recover the secret. Harn's scheme can prevent the attacks from outside adversaries and colluded shareholders. Here are the two algorithms of Harn's secure secret re construction scheme.

(1) Share generation

D selects $k(i.e., kt > t-1)$ random polynomials $F_l(x)(l = 1, \ldots, k)$ with degree $t-1$, and generates shares $F_l(x)(l = 1, \ldots, k)$ for each shareholder P_r.

For the secret S, there are always integers $w_l, d_l(l = 1, \cdots, k) \in GF(p)$, such that $S = \sum_{l=1}^{k} d_l f_l(w_l)$, where $w_i \neq w_j$ and $w_i \notin \{x_1, \ldots, x_n\}$ (x_r is the public information of P_r). $w_l, d_l(l = 1, \ldots, k)$ are publicly known.

(2) Secret reconstruction

There are $j(i.e., t \leq j \leq n)$ participants $\{P_1, \ldots, P_j\}$ involving in the secret reconstruction. Each participant $P_r(1 \leq r \leq j)$ uses his shares $F_l(x_r)(l = 1, \ldots, k)$ to compute and release one Lagrange component C_r to other participants secretly:

$$C_r = \sum_{l=1}^{k} d_l f_l(x_r) \prod_{v=1, v \neq r}^{j} \frac{w_l - x_v}{x_r - x_v} \bmod p.$$

Thus, each participant in the reconstruction can recover the secret $S = \sum_{r=1}^{j} C_r \bmod p$ with the knowledge of $C_r(r = 1, \ldots, j)$. Any released Lagrange component C_r cannot be used to derive

[1] The outside adversary is an attacker who does not have valid shares generated initially and aims to get the master secret.
[2] The inside adversary has two types: the cheater who has valid shares, but tries to defraud valid shares from other shareholders by releasing fake shares; and the colluded shareholder who colludes to recover the secret with other colluded shareholders. The number of colluded shareholders should be less than the value of threshold.

new private shares $F_l(x_r)(r = 1,\dots, j)$, which guarantee that no outside adversaries can obtain the secret.

3. Definition and Security Requirements

Definition 1. ((n,t,n) verifiable (multi-)secret sharing scheme with secure secret reconstruction). A (multi-)secret sharing scheme is called a (n,t,n) verifiable (multi-)secret sharing scheme with secure secret reconstruction if it does not need any mutually trusted dealer, and ensures that no shareholder can provide fake shares to others and that the secret(s) can only be reconstructed by honest participants.

A (n,t,n) verifiable (multi-)secret sharing scheme with secure secret reconstruction should satisfy the following security properties. These properties are elaborated as the ways to counter several major possible attacks in a (multi-)secret sharing scheme.

Property 1. Shareholder-cheating resistance

We call the action that inside adversaries intend to provide wrong or fake sub-shares to other participants in the secret reconstruction phase is the shareholder-cheating attack. A scheme is called shareholder-cheating resistance, as long as the scheme can perform normally when honest participants in the reconstruction are t or more than t. In addition, the property of shareholder-cheating resistance also keeps the scheme's threshold value consistent and makes the scheme robust.

Property 2. Conspiracy resistance

The conspiracy attack is assumed that $t-1$ or fewer colluded shareholders attempt to reconstruct some secret (note that the last secret may be the easiest one to obtain in the multi-secret sharing scheme). A conspiracy resistant scheme should ensure that the reconstructions of recovered secrets reveal no information about uncovered secrets.

Property 3. Outside-attack resistance

Assume the outside attack is that outside adversaries try to reconstruct the secrets by faking valid components. In order to make a scheme outside-attack resistant, the shares cannot be revealed in secret reconstructions or reused in different sessions.

4. The Proposed Secret Sharing Scheme

A verifiable (n,t,n) secret sharing scheme with secure secret reconstruction and its security analysis are elaborated in this section.

4.1. Notations

The notations of the proposed scheme are represented in Table 1.

Table 1. The Notations in the Proposed Secret Sharing Scheme

Notation	Meaning
n	The number of shareholders
t	The threshold of the scheme

p	A big prime
g	A generator of field $GF(p)$
P	The set of shareholders
P_i	The $i\text{-}th$ shareholder
S	The master secret
k	The number of polynomials each shareholder selects
S_i	The sub-secret selected by P_i
K_{ir}	The sub-share from P_i to P_r
x_r	The ID information of P_r
m	The number of participants in the secret reconstruction phase
$\overline{P}$	The set of dishonest shareholders
P_{RE}	The set of participants in the secret reconstruction phase
C_r	The Lagrange component released by P_i

4.2. Description

In order to construct a novel multi-secret sharing scheme, we propose the secret sharing scheme as a stepping stone. In the secret sharing scheme, the master secret S, which is determined jointly by all shareholders, is shared among n shareholders $P = \{P_1, \ldots, P_n\}$. There are three algorithms in the scheme: share generation, share verification and secret reconstruction.

4.3. Algorithms

(1) Share generation

In the share generation phase, each shareholder $P_i (i = 1, \ldots, n)$ generate kn (k can be considered as security parameter) sub-shares and distributes them to all shareholders by the following steps:

i) selects $k (i.e., k > 1)$ random polynomial with $t-1$ degree each:

$$F_{il}(x) = \sum_{j=0}^{t-1} a_{ilj} x^j \bmod p \ (l = 1, \ldots, k), a_{ilj} \in GF(p).$$

ii) generates sub-shares $K_{ilr} = F_{il}(x_r)$, which would be secretly sent to shareholders $P_r (r = 1, \ldots, n)$ respectively (x_r is the ID information of P_r).

iii) computes $E_{ilj} = g^{a_{ilj}} \bmod p$ as commitments that would be released publicly for other shareholders to verify the sub-shares they have received from P_i.

iv) randomly selects $S_i \in GF(p)$ as his sub-secret and finds two integers w_{il} and d_{il} in $GF(p)$, such that $S_i = \sum_{l=1}^{k} d_{il} F_{il}(w_{il}) \bmod p$, where $w_i \notin \{x_1, \cdots, x_n\}$ and $w_{i\alpha} \neq w_{i\beta} (1 \le \alpha, \beta \le k \cap \alpha \neq \beta)$ [11].

Each shareholder P_i makes w_{il} and d_{il} publicly known. And the master secret is determined by the sum of the sub-secrets from all shareholders:

$$S = \sum_{i=1}^{n} S_i .$$

(2) Share verification

Each shareholder P_r can verify the received sub-shares by computing the following equations:

$$g^{K_{ilr}} = \prod_{j=0}^{t-1} E_{ilj}^{x_r^j} \left(i = 1, \ldots, n, l = 1, \ldots, k\right).$$

P_r regards the sub-share K_{ilr} valid if it has passed the verification; otherwise P_r publishes K_{ilr} for other shareholders to verify it. P_i is added to $\overline{P}$, which is empty initially, after the other shareholders have an agreement that the sub-share K_{ilr} from P_i is invalid. And none in $\overline{P}$ is admitted to participate in the secret reconstruction.

(3) Secret reconstruction

The set of participants involving in the secret reconstruction of is denoted as $P_{RE} = \{P_1, \ldots, P_m\}$, where $m \geq t$ and $P_{RE} \cap \overline{P} = \phi$. And each shareholder $P_r \in P_{RE}$ uses all the received sub-shares $K_{ilr}\left(i = 1, \ldots, n, l = 1, \ldots, k\right)$ to compute and release one Lagrange component $C_r = \sum_{i=1}^{n} C_{ir} \bmod p$ to the other participants in the reconstruction phase, where C_{ir} is the sub-Lagrange component:

$$C_{ir} = \sum_{l=1}^{k} d_{il} K_{ilr} \prod_{v=1, v \neq r}^{m} \frac{w_{il} - x_v}{x_r - x_v} \bmod p$$

With all $C_r\{r \mid P_r \in P_{RE}\}$, each participant in P_{RE} can recover the master secret S:

$$S = \sum_{r=1}^{m} C_r \bmod p.$$

4.4. Security Analysis

Theorem 1. Our proposed secret sharing scheme is a (n, t, n) verifiable secret sharing scheme with secure secret reconstruction scheme.

Proof

Property 1. Shareholder-cheating resistance

Analysis: The share verification phase makes sure that the sub-shares released by shareholders must be valid, so it can prevent the attacks from the cheaters. And according to the hardness of computation Diffie-Hellman problem, the commitments $E_{ilj} = g^{a_{ilj}} \bmod p$ reveal no information about sub-shares. Consequently, the secret reconstructed by any adversary who provides a wrong or fake component is not the same with the real one.

Property 2. Conspiracy resistance

Analysis: For security analysis, the adversaries are given an ultimate ability they supposed to have, i.e., there are $t-1$ colluded shareholders attempting to reconstruct the master secret, and they can release their components after all the other participants' releasements in the secret reconstruction. The master secret $S = \sum_{i=1}^{n} S_i$ is a linear combination of points on n polynomials $F_{il}(x)(i = 1, \ldots, n, l = 1, \ldots, k)$, with $t-1$ degree each. So in order to obtain the master secret, ktn coefficients are needed. However, the $t-1$ colluded shareholders know $kt(t-1)$ of the needed ktn coefficients. As a result, they need to get the other $kt(n-t+1)$ unknown coefficients from the available information. Each colluded shareholder has $(n-t+1)k$ sub-shares from the honest shareholders, so the $t-1$ colluded shareholders can form at most

$k(t-1)(n-t+1)$ equations using their received sub-shares. Furthermore, they can also form $(n-t+1)$ equations from the Lagrange components released by the honest shareholders (we assume there are n shareholders participating in the secret reconstruction). Totally, the colluded shareholders can construct $(kt-k+1)(n-t+1)$ equations, however, the condition $k>1$ makes sure that $(kt-k+1)(n-t+1)<kt(n-t+1)$. Obviously, the proposed scheme can prevent the conspiracy attack of $t-1$ colluded shareholders.

Property 3. Outside-attack resistance

Analysis: For the security analysis, we assume that there are n shareholders participating in the secret reconstruction and the outside adversary can be the last one to release his component. Each released Lagrange component C_r is a linear function of polynomials $F_{il}(x)(i=1,\ldots,n, l=1,\ldots,k)$, with $t-1$ degree each. So in order to forge a valid component, an adversary should solve the function of nkt coefficients. But the adversary can form $n-1$ equations at most from the released $n-1$ Lagrange components. It is obvious that $nkt>n-1$, so the secret polynomials $F_{il}(x)(i=1,\ldots,n, l=1,\ldots,k)$ cannot be solved by the adversary. As a result, the outside adversary cannot construct a valid component or recover the master secret without providing a valid component.

5. The Proposed Multi-secret Sharing Scheme

We design a multi-secret sharing scheme by extending the secret sharing scheme presenting in section 4. The security analysis of the proposed multi-secret scheme is represented at the end of this section.

5.1. Notations

The notations of the proposed multi-secret sharing scheme are represented in Table 2.

Table 2. The Notations in the Proposed Multi-secret Sharing Scheme

Notation	Meaning
n	The number of shareholders
t	The threshold of the scheme
h	The number of secrets
p	A big prime
g	A generator of field $GF(p)$
P	The set of shareholders
P_i	The $i\text{-}th$ shareholder
S_{MUL}	The set of secrets
S_u	The $u\text{-}th$ secret
k	The number of polynomials each shareholder selects
K_{ilr}	The sub-share of $l\text{-}th$ polynomial from P_i to P_r
x_r	The ID information of P_r

S_{i-u}	The sub-secret of S_u selected by P_i
m	The number of participants in the secret reconstruction phase
$\overline{P}$	The set of dishonest shareholders
P_{RE-u}	The set of participants in the secret reconstruction phase of S_u
C_{r-u}	The Lagrange component of S_u released by P_i

5.2. Description

There are h secrets are shared among n shareholders $P = \{P_1, \ldots, P_n\}$. The set of the secrets is denoted as $S_{MUL} = \{S_1, \ldots, S_h\}$. This multi-secret sharing scheme is designed by extending the scheme in section 4, so it has all the good properties of that scheme but can share multiple secrets in each single process. This scheme also has three algorithms: share generation, share verification and secret reconstruction.

5.3. Algorithms

(1) Share generation

For $i = 1, \ldots, n$, shareholder $P_i \in P$ performs the following steps:

i) selects $k (i.e., \{nkt > nh + h - 2\} \cap \{(k-h)(n-t+1) > h-1\})$, we will prove this condition in the security analysis, random polynomials with $t-1$ degree each:

$$F_{il}(x) = \sum_{j=0}^{t-1} a_{ilj} x^j \bmod p (l = 1, \ldots, k), a_{ilj} \in GF(p).$$

ii) generates sub-shares $K_{ilr} = F_{il}(x_r)$, which would be secretly sent to shareholder $P_r (r = 1, \ldots, n)$ respectively.

iii) computes $E_{ilj} = g^{a_{ilj}} \bmod p (j = 0, \ldots, t-1, l = 1, \ldots, k)$, which would be released publicly as commitments for other shareholders to verify the sub-shares they have received from P_i.

iv) randomly selects $S_{i-u} \in GF(p)$ as his sub-secret of secret $S_u (u = 1, \ldots, h)$ and finds integers w_{il-u} and d_{il-u} in $GF(p)$, such that $S_{i-u} = \sum_{l=1}^{k} d_{il-u} F_{il}(w_{il-u})$, where $w_{il-u} \notin \{x_1, x_2, \cdots, x_n\}$ and $w_{i\alpha-u} \neq w_{i\beta-u} (1 \le \alpha, \beta \le k \cap \alpha \neq \beta)$.

Each shareholder P_i makes the integers w_{il-u} and d_{il-u} publicly known. And every secret going to be shared among P is determined by the sum of the corresponding sub-secrets selected by all shareholders:

$$S_u = \sum_{i=1}^{n} S_{i-u}.$$

(2) Share verification

The share verification process is the same with the share verification in section 4.3.

(3) Secret reconstruction

We denote the set of participants in the secret reconstruction as $P_{RE-u} = \{P_1, \ldots, P_m\}$, where $m \ge t$ and $P_{RE} \cap \overline{P} = \phi$. Each shareholder P_r in P_{RE-u} uses all received sub-shares $K_{ilr} (i = 1, \ldots, n, l = 1, \ldots, k)$ to compute a Lagrange component C_{r-u}, which would release to the other participants in the reconstruction:

$$C_{r-u} = \sum_{i=1}^{n} C_{ir-u} \bmod p ,$$

where C_{r-u} is the sub-Lagrange component:

$$C_{ir-u} = \sum_{l=1}^{k} d_{il-u} F_{il}(x_r) \prod_{v=1, v\neq r}^{m} \frac{w_{il-u} - x_v}{x_r - x_v} \bmod p .$$

After knowing all $C_{r-u}\{r \mid P_r \in P_{RE-u}\}$, each participant in P_{RE-u} could compute and recover all the shared secrets:

$$S_u = \sum_{r=1}^{m} C_{r-u} \bmod p (u = 1, \ldots, h).$$

5.4. Security Analysis

Theorem 2. The proposed multi-secret sharing scheme is a (n, t, n) verifiable multi-secret sharing scheme with secure secret reconstruction, if $\{ktn > h(n+1) - 2\} \cap \{kn > (h-1)(n-t+2)\}$, where t is the threshold, n and k are the number of shareholders and secret polynomials each shareholder selects respectively.

Proof

Property 1. Shareholder-cheating resistance

Analysis: Same as the analysis of property 1 in section 4.4.

Property 2. Conspiracy resistance

Analysis: Assuming $t-1$ colluded shareholders attempt to recover the last secret S_h after $h-1$ secrets having been recovered. They need $kt(n-t+1)$ coefficients to obtain S_h. And they can construct $h(n-t+1)$ and $h-1$ equations from released Lagrange components and recovered secrets respectively. Furthermore, they also can construct $k(t-1)(n-t+1)$ equations by using their received sub-secrets from honest shareholders. So the total number of equations they build is $(kt-k+h)(n-t+1)$. Then the condition $(k-h)(n-t+1) > h-1$ prevents the colluded shareholders from solving the secret polynomials $F_{il}(x)(i = 1, \ldots, n, l = 1, \ldots, k)$ and obtaining the last secret S_h. Thus, the threshold of the last uncovered secret is consistent with the original threshold value, which means our scheme can counter the conspiracy attack.

Property 3. Outside-attack resistance

Analysis: We assume the outside adversary tries to obtain the last secret S_h after $h-1$ secrets having been recovered and he can be the last one to release the Lagrange component. We also assume there would be n Lagrange components released in each reconstruction. The Lagrange component C_{r-u} released by each shareholder during the reconstruction of S_u is a linear function of polynomials $F_{il}(x)(i = 1, \ldots, n, l = 1, \ldots, k)$, with $t-1$ degree each. So an adversary has to solve the function having ktn coefficients in order to forge a valid component and obtain the secret eventually. The adversary can form $(h-1)+(h-1)n$ from the recovered $(h-1)$ secrets and the released $(h-1)n$ Lagrange components of recovered secrets. Furthermore, the adversary can construct another $(n-1)$ equations using the released Lagrange components of S_h. So the total number of the equations formed by the adversary adds up to $(h-1)+(h-1)n+(n-1)$. The condition $nkt > nh + h - 2$ ensures that any adversary cannot forge a valid component. So our proposed scheme is outside-attack resistant.

6. Comparison

In this section we give the comparisons among the proposed multi-secret sharing scheme and three other ones [11, 19, 14] in Table 3. It can be seen form the table that the scheme in [11] is a multi-secret sharing scheme with secure secret reconstruction that satisfies unconditional security. However, a mutually trusted dealer is needed and shares cannot be verified in this scheme. As we have stated the need of a dealer is a bottleneck when secret sharing schemes are designed for many applications, and the verifiability is more significant than unconditional security in a (n,t,n) secret sharing scheme. And the shares can be verified in the schemes of [14, 19]. Moreover, the scheme in [19] can execute without the help of a dealer. But it does not have the property of secure secret reconstruction.

Table 3. The Comparisons among Four Multi-secret Schemes

Property	Our scheme	The scheme in [11]	The scheme in [19]	The scheme in [14]
The dealer distributes the shares	No	Yes	No	Yes
Verify the cheating action among shareholders	Yes	No	Yes	Yes
Prevent conspiracy attacks	Yes	Yes	Yes	Yes
Resist outside-adversary attacks	Yes	Yes	Yes	Yes
Recover multiple secrets by Lagrange interpolating polynomial	Yes	Yes	Yes	Yes
The shares are reusable	Yes	Yes	Yes	Yes
Shareholder do not need to follow a specific order	Yes	Yes	No	No
Recover multiple secrets parallelly	Yes	Yes	No	No
Has secure secret reconstruction property	Yes	Yes	No	No
Security is based on Shamir's scheme and discrete logarithm	Yes	No	Yes	Yes
Has unconditional security property	No	Yes	No	No

7. Conclusion

Aim at solving the existing problems of multi-secret sharing schemes, a verifiable (n,t,n) multi-secret sharing scheme with secure secret reconstruction is proposed in this paper. A mutually trusted dealer is no longer needed in our proposed multi-secret sharing scheme, and the adversaries without providing valid shares cannot obtain real secrets even in the situation that there are more than t shareholders participating in the secret reconstruction. These properties make our scheme more flexible and reliable. A secret sharing scheme with the same properties is also given as a stepping stone. Both of the proposed schemes can resist the

attacks from outside and inside adversaries, including cheaters and colluded shareholders. In addition, the security analysis and the comparisons among the proposed multi-secret scheme and three other ones are also represented.

Acknowledgments

This research is supported by National Natural Science Foundation of China (61272425, 61402245), Qingdao science and technology development project(12-1-4-2-(16)-jch, 13-1-4-151-jch), Huawei Technology Fund(YB2013120027), Minsheng Project of Huangdao District in Qingdao, and Shandong provincial Key Laboratory of Computer Network (SDKLCN-2013-03).

References

[1] A. Shamir, "How to share a secret", Communications of the ACM, vol. 22, no. 11, **(1979)**, November, pp. 612-613.
[2] G. R. Blakley, "Safeguarding cryptographic keys", Proc. AFIPS 1979 National Computer Conference, **(1979)** June 4-7, pp. 313-317.
[3] E. F. Brickell, "Some ideal secret sharing schemes", Proceedings of the Eurocrypt'89, vol. 434, **(1990)**, pp. 468-475.
[4] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing", Proceedings of 28th IEEE Symposium on Foundations of Computer Science, **(1987)** October 12-14, pp. 427-438.
[5] B. Chor, S. Goldwasser, S. Micali and B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults", Proceedings of the 26th IEEE Symposium on Foundations of Computer Science, **(1985)** October 21-23, pp. 383-395.
[6] I. Ingemarsson and G. J. Simmons, "A protocol to set up shared secret schemes without the assistance of a mutually trusted party", Proceedings of the Eurocrypt'90, vol. 473, **(1990)** May 21-24, pp. 266-282.
[7] T. P. Pedersen, "A threshold cryptosystem without a trusted party", Proceedings of the Eurocrypt'91, vol. 547, **(1991)** April 8-11, pp. 522-526.
[8] J. He and E, Dawson, "Multistage secret sharing based on one-way function", Electronics Letter, vol. 30, no. 19, **(1994)** September, pp. 1591-1592.
[9] J. He and E. Dawson, "Multi secret-sharing scheme based on one-way function", Electronics Letter. vol. 31, no. 2, **(1995)** January, pp. 93-95.
[10] L. Harn, "Efficient sharing (broadcasting) of multiple secrets", IEEE Proceedings on Computers and Digital Techniques, vol. 142, no. 3, **(1995)** May, pp. 237-240.
[11] L. Harn, "Secure secret reconstruction and multi-secret sharing schemes with unconditional security", Security and Communication Networks, vol. 7, no. 3, **(2014)** March, pp. 567-573.
[12] R. J. Hwang and C. C. Chang, "An on-line secret sharing scheme for multi-secrets", Computer Communications, vol. 21, no. 13, **(1998)** September, pp. 1170-1176.
[13] H. Y. Chien, J. K. Jan and Y. M. Tseng, "A practical (t, n) multi-secret sharing scheme. IEICE Transactions on Fundamentals of Electronics, Communications and Computer, vol. E83-A, no. 12, **(2000)** December, pp. 2762-2765.
[14] J. Shao and Z. F. Cao, "A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme", Applied Mathematics and Computation, vol. 168, no. 1, **(2005)** September, pp. 135-140.
[15] J. J. Zhao, J. Z. Zhang and R. Zhao, "A practical verifiable multi-secret sharing scheme" Computer Standards & Interfaces, vol. 29, no. 1, **(2007)** January, pp. 138-141.
[16] M. H. Dehkordi and S. Mashhadi, "New efficient and practical verifiable multi-secret sharing schemes", Information Science, vol. 178, no. 9, **(2008)** May, pp. 2262-2274.
[17] Z. Eslami and J. Z. Ahmadabadi, "A verifiable multi-secret sharing scheme based on cellular automata", Information Science, vol. 180, no.15, **(2010)** August, pp. 2889-2894.
[18] Y. K. Chen, J. Yu, X. G. Cheng, R. Hao and H. Y. Liu, "Verifiable Multi-secret sharing scheme based on Homogeneous Linear Recursion", Acta Scientiarum Naturalium Universitatis Pekinensis, vol. 46, no. 5, **(2010)**, pp. 709-714.
[19] L. Harn and C. L. Lin, "Strong (n, t, n) verifiable secret sharing scheme", Information Science, vol. 180, no. 16, **(2010)** August, pp. 3059-3064.

[20] C. Q. Hu, X. F. Liao and X. Z. Cheng, "Verifiable multi-secret sharing based on LFSR sequences", Theoretical Computer Science, vol. 445, no. 3, **(2012)** August, pp. 52-62.
[21] H. Zhao, J. Z. Sun, F. Y. Wang and L. Zhao, "A finite equivalence of multisecret sharing based on Lagrange interpolating polynomial", Security Communication Networks, vol. 6, no. 9, **(2013)** September, pp. 1169-1175.
[22] Y. F. Wu, L. P. Huang, X. Wang and N. Yu, "An extensible cheat-proofing multi-secret sharing scheme with low computation complexity", Security Communication Networks, vol. 7, no. 6, **(2014)** June, pp. 1042-1048.
[23] J. Herranz, A. Ruiz and G. Sáez, "New results and applications for multi-secret sharing schemes", Designs, Codes and Cryptography, vol. 73, no. 3, **(2013)** May, pp. 841-864.

