SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks (2013)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.758

RESEARCH ARTICLE

Secure secret reconstruction and multi-secret sharing schemes with unconditional security

Lein Harn*

Department of Computer Science Electrical Engineering, University of Missouri-Kansas City, Kansas City, MO, U.S.A.

ABSTRACT

In Shamir's (t, n) secret sharing (SS) scheme, the secret s is divided into n shares by a dealer and is shared among n shareholders in such a way that any t or more than t shares can reconstruct this secret; but fewer than t shares cannot obtain any information about the secret s. In this paper, we will introduce the security problem that an adversary can obtain the secret when there are more than t participants in Shamir's secret reconstruction. A *secure secret reconstruction scheme*, which prevents the adversary from obtaining the secret is proposed. In our scheme, *Lagrange components*, which are linear combination of shares, are used to reconstruct the secret. Lagrange component can protect shares unconditionally. We show that this scheme can be extended to design a multi-secret sharing scheme. All existing multi-secret sharing schemes are based on some cryptographic assumptions, such as a secure one-way function or solving the discrete logarithm problem; but, our proposed multi-secret sharing scheme is unconditionally secure. Copyright © 2013 John Wiley & Sons, Ltd.

KEYWORDS

Shamir's scheme; secret reconstruction; multiple secrets; unconditional security; Lagrange component

***Correspondence**

Lein Harn, Department of Computer Science Electrical Engineering, University of Missouri-Kansas City, Kansas City, MO , U.S.A.
Email: harnl@umkc.edu

1. INTRODUCTION

Secret sharing (SS) schemes were introduced by both Blakley [2] and Shamir [16] independently in 1979 as a solution for safeguarding cryptographic keys and have been studied extensively in the literature. In Shamir's (t, n) SS scheme, the secret s is divided into n shares by a dealer and is shared among n shareholders in such a way that any t or more than t shares can reconstruct the secret; but fewer than t shares cannot obtain any information about the secret s.

Shamir's (t, n) SS scheme is based on a linear polynomial and is unconditionally secure. The security of cryptographic schemes/protocols can be classified into two types, computational security and unconditional security. Computational security assumes that the adversary has bounded computing power that limits the adversary solving hard mathematical problem, such as factoring a large composite integer into two primes. Unconditional security means that the security holds even if the adversary has unbounded computing power. Research on developing cryptographic schemes/protocols with unconditional security has received wide attention recently.

Although Shamir's secret reconstruction scheme is very simple; but in practical applications, possible threats make the secret reconstruction very complicated. In fact, adversaries who do not own valid shares may impersonate to be shareholders participated in the secret reconstruction. Most secret reconstruction schemes assume that participants in the secret reconstruction are all shareholders. One straightforward approach to ensure that all participants are shareholders is to use a conventional user authentication scheme at the beginning of the secret reconstruction. However, this approach adds additional complexity because user authentication is a one-to-one process. Furthermore, in a SS scheme, only the dealer needs to know who are legitimate shareholders and distribute private share(s) to each shareholder initially. In the secret reconstruction, shareholders may not know each other. Whether the secret can be reconstructed successfully, they should depend only on their shares; but not on their identities. If all released shares are valid shares, the secret can be reconstructed. On the other hand, if there is any fake share, the secret cannot be reconstructed. In 1985, Chor *et al*. [3] proposed the notion of verifiable secret sharing (VSS). Using VSS, shareholders are able to verify that their shares are valid without revealing their shares. There are vast research papers on VSS [5,10,11,14] in the literature. However, VSS is a complicated process, which requires additional information and processing time.

Shamir's SS scheme requires a large data expansion (i.e., t shares are needed to reclaim one secret). Therefore, this scheme is inefficient as a conveyor of information. Multi-secret sharing scheme allows multiple secrets to be shared and reconstructed in different sessions using the same shares obtained initially. To achieve the objective of multi-secret sharing scheme, we need two security requirements to be met: (i) shares need to be protected in the secret reconstruction; otherwise, shares cannot be reused for reconstructing multiple secrets and (ii) each recovered secret will not compromise the secrecy of any uncovered secret; otherwise, fewer shares may be needed to reconstruct any uncovered secret (i.e., the threshold of uncovered secrets is decreased). All existing multi-secret sharing schemes can be classified into two categories: (i) schemes based on a one-way function [7–9] or a two-variable one-way function [4,12,19] and (ii) schemes based on some cryptographic assumptions, such as solving the discrete logarithm problem [6,15] or the Ron Rivest, Adi Shamir, and Leonard Adleman assumption [13]. There are other approaches to protect shares and secrets, for example, using a multi-party zero-knowledge interactive proof protocol [17], or a shuffling method [20]. The drawback of using a zero-knowledge interactive proof protocol is the computational complexity of the multi-party zero-knowledge interactive proof protocol.

In this paper, we propose the notion of *secure secret reconstruction*, which prevents adversaries from obtaining the secret. We use the linear combination of shares to protect the privacy of shares so the adversary cannot take advantage by releasing his value last in the secret reconstruction. This scheme is a simple modification of Shamir's (t, n) SS scheme, which can be extended to design a multi-secret sharing scheme with unconditional security. In the proposed scheme, multiple secrets can be recovered in different sessions. All existing multi-secret sharing schemes are based on some cryptographic assumptions, but, our proposed multi-secret sharing scheme is unconditionally secure.

The rest of this paper is organized as follows. In the next section, we introduce some preliminaries. In Section 3, we describe models of our proposed schemes including adversaries, communication networks, and security requirements. In Section 4, we analyze Shamir's (t, n) secret reconstruction and show that Shamir's secret reconstruction is a secure secret reconstruction when there are exact t participants; but, it is not a secure secret reconstruction when there are more than t participants. We propose a secure secret reconstruction scheme in Section 5. A secure multi-secret sharing scheme is proposed in Section 6. Conclusion is included in Section 7.

2. PRELIMINARIES

In this section, we introduce some fundamental backgrounds.

2.1. Shamir's (t, n) secret sharing scheme [16]

In Shamir's (t, n) SS scheme based on a linear polynomial, there are n shareholders, $U = \{U_1, U_2, \ldots, U_n\}$ and a dealer D. The scheme consists of two algorithms as indicated in Figure 1. Shamir's (t, n) SS scheme satisfies security requirements of the secret sharing scheme, that are, (i) the master secret can be reconstructed with any t or more than t shares and (ii) no information about the master secret can be obtained with fewer than t shares. Shamir's scheme is unconditionally secure because the scheme satisfies these two requirements without making any computational assumption. For more information on this scheme, readers can refer to the original paper [16].

2.2. Secret sharing homomorphism

Benaloh [1] introduced the property of the secret sharing homomorphism. Let S be the domain of the secret and T be the domain of shares corresponding to the secret. The function $F_I: T \rightarrow S$ is an induced function of the (t, n) SS. This function defines the secret s based on any subset containing t shares, $\{s_{i_1}, s_{i_2}, \ldots, s_{i_t}\}$, as $s = F_I(s_{i_1}, s_{i_2}, \ldots, s_{i_t})$, where $I = \{s_{i_1}, s_{i_2}, \ldots, s_{i_t}\}$.

Definition 1: ***Homomorphism of the secret sharing [1].*** *Let $\oplus$ and $\otimes$ be two functions on elements in sets S and T, respectively. We say that a (t, n) SS has the ($\oplus$,$\otimes$)-homomorphic property if for any subset I and $s = F_I(s_{i_1}, s_{i_2}, \ldots, s_{i_t})$, $s' = F_I(s'_{i_1}, s'_{i_2}, \ldots, s'_{i_t})$, then $s \oplus s' = F_I(s_{i_1} \otimes s'_{i_1}, s_{i_2} \otimes s'_{i_2}, \ldots, s_{i_t} \otimes s'_{i_t})$.*

We note that shares generated by Shamir's (t, n) SS scheme satisfy (+,+)-homomorphism property. In other words, the sum of shares of two polynomials, $f(x)$ and $g(x)$, is the share of additive polynomial, $f(x) + g(x)$.

3. MODEL

In this section, we describe models of our proposed schemes including adversary and security requirements.

3.1. Adversaries

The adversaries in the secret reconstruction can be classified into two types, the outside adversaries and the inside adversaries. The outside adversaries are attackers who do not own valid shares generated by the dealer initially. We will discuss the security when outside adversaries participate in Shamir's secret reconstruction and try to obtain the master secret. We will show that when there are more than t participants in Shamir's secret reconstruction scheme, the outside adversary can still obtain the secret. We present the notion of a secure secret reconstruction scheme.

Share generation

Dealer D picks a random polynomial $f(x)$ of degree $t-1$: $f(x)=a_0+a_1x+...+a_{t-1}x^{t-1} \bmod p$, such that the secret is $s=f(0)=a_0$, and all coefficients, a_i, $i=0,1,...,t-1$, are in the finite field $GF(p)$ with $p>s$ and p is a prime. D computes n shares, $y_r=f(x_r)$, $r=1,2,...,n$, where x_r is the public information associated with shareholder U_r. Then, the dealer distributes each share y_r to corresponding shareholder U_r secretly.

Secret reconstruction

Assume that t shareholders, $\{U_1,U_2,...,U_t\}$, want to recover the secret, s. Shareholders release their shares and use the Lagrange interpolating formula, $s=f(0)=\sum_{l=1}^{t} f(x_l)\prod_{v=1,v\neq l}^{t}\frac{-x_v}{x_l-x_v} \bmod p$, to recover the secret.

Figure 1. Shamir's (*t, n*) secret sharing scheme.

Definition 2: ***Secure secret reconstruction scheme.*** *This scheme ensures that the secret can only be recovered by participants who present valid shares. In other words, if any outside adversary participated in the secret reconstruction, the adversary cannot obtain the secret.*

When there are more than t participants in the secret reconstruction, most papers suggest taking only t shares to recover the secret. This approach can cause a security problem because the outside adversary can impersonate to be a shareholder participated in the reconstruction and does not contribute any share. Because only t shares are needed to recover the secret, the adversary can still obtain the master secret in the secret reconstruction. In other words, a conventional user authentication scheme or a VSS scheme is needed at the beginning of the secret reconstruction to ensure that all participants have valid shares. This approach adds additional complexity because most user authentication scheme authenticates one user at a time and most VSS scheme verifies one share at a time. Furthermore, whether the secret can be reconstructed successfully, they should depend only on the shares; but not on the knowledge of who are shareholders. In Section 5, we propose a secure secret reconstruction scheme using a simple modification of Shamir's (*t*, *n*) SS scheme.

The inside adversaries are shareholders who own valid shares obtained from the dealer initially. In the multi-secret sharing scheme, we analyze the security whether $t-1$ inside adversaries can collude together to reveal the last uncovered secret if other secrets have already been recovered.

During the secret reconstruction, inside adversaries (also called "cheaters") can fool honest shareholders by presenting invalid shares. In this way, inside adversaries can recover the secret exclusively; but honest shareholders obtain nothing but a fake secret. Tompa and Woll [18] proposed a scheme to detect cheaters. There are many research papers addressing the problem of cheater detection and/or identification. For example, VSS scheme can be used to detect and/or identify cheaters. In this paper, we will not consider this type of attack.

3.2. Security requirements

Our proposed multi-secret sharing scheme has the following security properties.

Secrets. Every secret can only be recovered by any t or more than t participants who are shareholders; but cannot be obtained by any outside adversary.

Shares. In a multi-secret sharing scheme, shares of shareholders can be reused to reconstruct multiple secrets in different sessions. Thus, shares need to be protected in the reconstruction; otherwise, shares cannot be reused to reconstruct uncovered secrets. In the security analysis, we will examine the security of shares under the scenario that gives any outside adversary the most information to recover shares. The adversary tries to obtain the shares in the process to reconstruct the last secret, and the adversary is the last one to release his component. Furthermore, we assume that there are n shares released in the reconstruction of each secret.

Threshold. The recovered secret should not compromise the secrecy of any uncovered secret. Because each recovered secret is a function of share(s), shareholders can establish equation of shares on the basis of each recovered secret. This additional equation should not compromise the secrecy of shares and uncovered secrets; otherwise, the threshold of uncovered secrets can be reduced. In the security analysis of the threshold, we will examine the security of threshold under the scenario that gives the most information to the adversary. We assume that there are $t-1$ colluded shareholders (i.e., inside adversaries) trying to recover the last secret after all other secrets having been reconstructed. In the processing to recover the last secret, these colluded adversaries are the last ones to release their values.

4. ANALYSIS OF SHAMIR'S SECRET RECONSTRUCTION SCHEME

It is obvious that when there are exact t participants including an adversary in Shamir's secret reconstruction, the adversary cannot obtain the secret because the adversary does not have enough number of valid shares to recover

the secret. Thus, Shamir's secret reconstruction scheme is a secure secret reconstruction scheme when there are exact t shares. However, when there is more than t participants in Shamir's secret reconstruction, most papers suggest taking only t shares to recover the secret. This approach may cause a security problem because the outside adversary can impersonate to be a shareholder participated in the reconstruction and does not contribute any share. Because only t shares are needed to recover the secret, the adversary can still obtain the secret. One solution to avoid this security problem is to use a VSS before secret reconstruction. The VSS can allow participants to verify that all participants have valid shares. This approach can prevent any adversary participated in the secret reconstruction. But, VSS is a complicated process and it causes significant overhead in the secret reconstruction.

There is one simple way to prevent the outside adversary to obtain the secret. The dealer splits the secret s into two pieces, s_1 and s_2 such that $s = s_1 + s_2$. The dealer distributes s_1 to all shareholders and uses Shamir's (t, n) SS scheme to distribute shares of s_2 to shareholders. Because the outside adversary does not have s_1, the outside adversary cannot obtain the secret. However, in this approach, the threshold of the secret s_1 is 1. This contradicts to the objective of a (t, n) SS scheme, which the threshold should be t. In other words, the outside adversary only needs to compromise one copy of the secret s_1, the outside adversary can still obtain the master secret when there are more than t shares presented in the secret reconstruction.

Shamir's secret reconstruction scheme can be generalized to take more than t shares. For example, when there are j (i.e., $t \le j \le n$) shareholders with their shares, $\{f(x_1), f(x_2), \ldots, f(x_j)\}$, participated in the secret reconstruction, the secret can be recovered as $s = f(0) = \sum_{r=1}^{j} f(x_r) \prod_{v=1, v\neq r}^{j} \frac{-x_v}{x_r - x_v} \bmod p$. In this generalization, each participant needs to contribute one share in the secret reconstruction. If there is any invalid share, the reconstructed secret is different from the real secret. However, this generalization is not a secure secret reconstruction scheme because the adversary only needs t valid shares (i.e., the degree of the polynomial $f(x)$ is $t-1$) to recover the secret. If there are j (i.e., $t \le j \le n$) shares in the secret reconstruction, the adversary can take only t out of j shares to obtain the master secret. In the next section, we propose a secure secret reconstruction scheme using this generalization. The proposed scheme uses linear combination to protect the secrecy of shares. This scheme is a simple modification of Shamir's secret reconstruction scheme.

5. SECURE SECRET RECONSTRUCTION SCHEME

In this section, we propose a secure secret reconstruction scheme. The basic idea is that the dealer in Shamir's (t, n) SS scheme selects k (i.e., $kt > n-1$, e.g, if $t=2$, $n=5$, then $k=3$. We will prove this condition in Theorem 1) random polynomials, $f_l(x)$, $l = 1, 2, \ldots, k$, having degree $t-1$ each, and generates shares, $f_l(x_r)$, $l = 1, 2, \ldots, k$, for each shareholder, U_r. For any secret, s, the dealer can always find integers, $w_l, d_l, l = 1, 2, \ldots, k$, in $GF(p)$, such that $s = \sum_{l=1}^{k} d_l f_l(w_l)$, where $w_i \neq w_j$, and $w_i \notin \{x_1, x_2, \ldots, x_n\}$, for every pair of i and j, x_r is the public information for shareholder, U_r. The dealer makes these integers, $w_l, d_l, l = 1, 2, \ldots, k$, publicly known.

In the secret reconstruction, there is j (i.e., $t \le j \le n$) participants, $\{P_1, P_2, \ldots, P_j\}$. Each participant P_r uses his shares, $f_l(x_r), l = 1, 2, \ldots, k$, to compute and release one Lagrange component, $c_r = \sum_{l=1}^{k} d_l f_l(x_r) \prod_{v=1, v\neq r}^{j} \frac{w_l - x_v}{x_r - x_v} \bmod p$, to all other participants secretly. Thus, after knowing c_r, $r = 1, 2, \ldots, j$, each participant can recover the secret as $s = \sum_{r=1}^{j} c_r \bmod p$. If there is any outside adversary, because private share, $f_l(x_r), r = 1, 2, \ldots, j$, cannot be derived from any released Lagrange component c_r, the adversary cannot recover the secret. We outline this scheme, Scheme 1, in Figure 2.

Theorem 1. *Scheme 1 is a secure secret reconstruction scheme if $kt > n-1$, as we have defined in Section 3.1, where t is the threshold, n is the number of shares, and k is the number of secret polynomials.*

Proof **Secrets**. It is obvious that the secret can be successfully reconstructed in Scheme 1 if all participants are shareholders and act honestly to release their Lagrange components. In case there is any outside adversary who does not own any valid share, the adversary cannot release a valid Lagrange component. Thus, the recovered secret must be different from the real secret s. Furthermore, the adversary cannot derive any share, $f_l(x_r)$, from each released Lagrange component, $c_r = \sum_{l=1}^{k} d_l f_l(x_r) \prod_{v=1, v\neq r}^{j} \frac{w_l - x_v}{x_r - x_v} \bmod p$.

Shares. In the following discussion, we consider the scenario that gives an outside adversary the most information to recover shares. We assume that there are n participants in the secret reconstruction and the adversary is the last one to release his component. Since each released Lagrange component is a linear function of kt coefficients of polynomials, $f_l(x), l = 1, 2, \ldots, k$, having degree $t-1$, the adversary can obtain at most $n-1$ Lagrange components and form $n-1$ equations. Because $kt > n-1$ (i.e., kt is the number of unknown coefficients of polynomials, $f_l(x), l = 1, 2, \ldots, k$, having degree $t-1$ each), this condition prevents the adversary to solve the secret polynomials, $f_l(x)$, $l = 1, 2, \ldots, k$. Thus, the adversary cannot recover the secret in Scheme 1.

Share generation

The dealer D selects k (i.e., $kt > n-1$) random polynomials, $f_l(x), l=1, 2,...,k$, having degree $t-1$ each and generates shares, $f_l(x_r), l=1, 2, ..., k$, for each shareholder, U_r. For any secret, s, the dealer can always find integers, $w_l, d_l, l = 1,2,...,k$, in $GF(p)$, such that $s = \sum_{l=1}^{k} d_l f_l(w_l)$, where $w_i \neq w_j$ and $w_i \notin \{x_1, x_2, ..., x_n\}$, for every pair of i and j, x_i is the public information for shareholder, U_i. The dealer makes these integers, w_l, d_l, $l = 1,2,...,k$, publicly known.

Secret reconstruction

1. Each participant P_r uses his shares, $f_l(x_r)$, $l = 1,2,...,k$, to compute and release one Lagrange component, $c_r = \sum_{l=1}^{k} d_l f_l(x_r) \prod_{v=1, v\neq r}^{j} \frac{w_l - x_v}{x_r - x_v} \bmod p$, to all other participants secretly.
2. After knowing c_r, $r = 1,2,..., j$, each participant computes $s == \sum_{r=1}^{j} c_r \bmod p$.

Figure 2. Secure secret reconstruction scheme.

Threshold. In the following discussion, we consider the scenario that $t-1$ colluded shareholders (i.e., inside adversaries) trying to recover the secret from their shares. The secret, $s = \sum_{l=1}^{k} d_l f_l(w_l)$, is a linear combination of points on k polynomials, $f_l(x)$, $l = 1, 2, \ldots, k$, having degree $t-1$ each. We assume that these colluded shareholders have their shares, $f_l(x_r)$, $l = 1, 2, \ldots, k$, $r = 1, 2, \ldots, t-1$. These colluded shareholders can use their $k(t-1)$ shares to construct $k(t-1)$ equations. Because $kt > k(t-1)$ (i.e., kt is the number of unknown coefficients of polynomials, $f_l(x), l = 1, 2, \ldots, k$, having degree $t-1$ each), this condition prevents the colluded shareholders to solve the secret polynomials, $f_l(x), l = 1, 2, \ldots, k$. Thus, the colluded shareholders cannot recover the secret in Scheme 1. The security of Scheme 1 is unconditionally secure because we have made no computational assumption in previous discussion.

Remark 1. For any secret, s, the dealer needs to select $w_i \neq w_j$, for every pair of i and j and the secret is $s = \sum_{l=1}^{k} d_l f_l(w_l)$. If $w = w_i = w_j$, for every pair of i and j, the adversary can still recover the secret after knowing t Lagrange components. This is because in this case the secret, $s = \sum_{l=1}^{k} d_l f_l(w)$, is a share of the additive sum of polynomials, $\sum_{l=1}^{k} d_l f_l(x)$, having degree $t-1$. Each P_i needs to use his shares to compute and release the Lagrange component, $c_r = \sum_{l=1}^{k} d_l f_l(x_r) \left\{ \prod_{v=1, v\neq r}^{j} \frac{w - x_v}{x_r - x_v} \right\} \bmod p$. The adversary can recover the additive sum of shares, $\sum_{l=1}^{k} d_l f_l(x_r)$, from each released Lagrange component c_i. Thus, after knowing t additive sum of shares, the adversary can recover the additive sum of polynomials, $\sum_{l=1}^{k} d_l f_l(x)$, and obtain the secret. In the next section, we will extend Scheme 1 to design a multi-secret sharing scheme.

Remark 2. In Shamir's (t, n) SS scheme, each shareholder has only one share; but, in Scheme 1, the number of shares of each shareholder is expanded by a factor of $O(k)$ and the number of public parameters is also of size $O(k)$, where $kt > n-1$. However, shares in Scheme 1 can be used to prevent outside adversary to obtain the secret without invoking any additional VSS scheme. It is a time-consuming process to use VSS scheme to verify multiple shares because all VSS schemes verify one share at a time.

6. SECURE MULTI-SECRET SHARING SCHEME

In a secure multi-secret sharing scheme, two security requirements need to be satisfied: (i) shares need to be protected; otherwise, shares cannot be reused for reconstructing other secrets and (ii) each recovered secret should not compromise the secrecy of uncovered secrets; otherwise, the threshold is reduced for other secrets.

Scheme 1 can be modified to share h secrets in the following way. The basic idea is that the dealer in Shamir's (t, n) SS scheme selects k (i.e., $\{kt > h(n+1) - 2\} \cap \{k > (h-1)(n-t+2)\}$, for example, if $t = 2$, $n = 5$, $h = 2$, then $k = 6$. We will prove this condition in Theorem 2) random polynomials, $f_l(x)$, $l = 1, 2, \ldots, k$, having degree $t-1$ each, and generates shares, $f_l(x_r)$, $l = 1, 2, \ldots, k$, for each shareholder, U_r. For any secret, s_i, the dealer finds integers, $w_l, d_{i,l}, l = 1, 2, \ldots, k$, in $GF(p)$, such that $s_i = \sum_{l=1}^{k} d_{i,l} f_l(w_l)$,

where $w_i \neq w_j$ and $w_i \notin \{x_1, x_2, \ldots, x_n\}$, for every pair of i and j, x_r is the public information for shareholder, U_r, and all $(d_{i,1}, d_{i,2}, \ldots, d_{i,k})$ are linearly independent vectors, $i = 1, 2, \ldots, h$. The dealer makes these integers, $w_l, d_{i,l}$, $l = 1, 2, \ldots, k$, and $i = 1, 2, \ldots, h$, publicly known.

The secret reconstruction is the same as Scheme 1. If there are j (i.e., $t \leq j \leq n$) participants, $\{P_1, P_2, \ldots, P_j\}$, to recover the secret s_i, each participant P_r uses his shares, $f_l(x_r), l = 1, 2, \ldots, k$, to compute and release one Lagrange component, $c_r = \sum_{l=1}^{k} d_{i,l} f_l(x_r) \prod_{v=1, v \neq r}^{j} \frac{w_l - x_v}{x_r - x_v} \bmod p$, to all other participants secretly. After knowing, $c_r, r = 1, 2, \ldots, j$, each participant computes $s_i = \sum_{r=1}^{j} c_r \bmod p$. We outline this scheme, Scheme 2, in Figure 3.

Theorem 2 *The proposed scheme is a multi-secret sharing scheme to share h secrets with properties as we have described in Section 3.2 if* $\{kt > h(n+1) - 2\} \cap \{k > (h-1)(n-t+2)\}$, *where t is the threshold, n is the number of shares, k is the number of secret polynomials, and h* is the number of secrets.

Proof **Secrets**. We have proven this property in Theorem 1.

Shares. Because each released Lagrange component, $c_r = \sum_{l=1}^{k} d_{i,l} f_l(x_r) \prod_{v=1, v \neq r}^{j} \frac{w_l - x_v}{x_r - x_v} \bmod p$, of shareholder U_r is a linear combination of k shares, $f_l(x_r)$, $l = 1, 2, \ldots, k$, shares are protected unconditionally from each released component.

In the following discussion, we consider the scenario that gives any outside adversary the most information to recover shares. The adversary tries to obtain the shares in the process to reconstruct the last secret s_h and the adversary is the last one to release his component. In this case, $h-1$ secrets, s_i, $i = 1, 2, \ldots, h-1$, have already been recovered. We assume that n Lagrange components are used to recover each secret including the current secret s_h. Because each released Lagrange component and each secret is a linear function of kt coefficients of polynomials, $f_l(x), l = 1, 2, \ldots, k$, having degree $t-1$ each, the adversary can construct at most $(h-1)n + n - 1$ equations from Lagrange components (i.e., $(h-1)n$ equations from previously released Lagrange components of recovered secrets and $n-1$ from components of the current secret s_h) and $n-1$ equations from previously recovered secrets. In total, the adversary can form $(h-1)n + (n-1) + (h-1)$ equations. Because $kt > (h-1)n + (n-1) + (h-1) \rightarrow kt > h(n+1) - 2$ (i.e., kt is the number of unknown coefficients of polynomials, $f_l(x), l = 1, 2, \ldots, k$, having degree $t-1$ each), this condition prevents the adversary to solve the secret polynomials, $f_l(x), l = 1, 2, \ldots, k$. Thus, the adversary cannot recover the shares. The security of polynomials used to generate shares is unconditionally protected.

Threshold. In the following discussion, we consider the scenario that gives multiple inside adversaries the most information to change the threshold value. We assume that there are $t-1$ colluded shareholders trying to recover the last secret s_h after $h-1$ secrets, $s_i, i = 1, 2, \ldots, h-1$, having been recovered. Firstly, we show whether or not s_h can be recovered by a linear combination of previously recovered secrets, s_i, $i = 1, 2, \ldots, h-1$. Because each secret is $s_i = \sum_{l=1}^{k} d_{i,l} f_l(w_l)$, where $w_i \neq w_j$, for every pair of i and j, and all $(d_{i,1}, d_{i,2}, \ldots, d_{i,k})$ are linearly independent vectors, $i = 1, 2, \ldots, h$, it is impossible to obtain

Share generation

To share h secrets, s_i, $i = 1,2,\ldots,h$, the dealer D selects k (i.e., $\{kt > h(n+1) - 2\} \cap \{k > (h-1)(n-t+2)\}$,) random polynomials, $f_l(x)$, l=1, 2,...,k, and each polynomial has degree $t-1$, and generates shares, $f_l(x_r)$, $l = 1,2,\ldots,k$, for each shareholder, U_r. For any secret, s_i, the dealer finds integers, $w_l, d_{i,l}$, $l = 1,2,\ldots,k$, in *GF(p),* such that $s_i = \sum_{l=1}^{k} d_{i,l} f_l(w_l)$, where $w_i \neq w_j$ and $w_i \notin \{x_1, x_2, \ldots, x_n\}$, for every pair of i and j, x_r is the public information for shareholder, U_r, and all $(d_{i,1}, d_{i,2}, \ldots, d_{i,k})$ are linearly independent vectors, $i = 1,2,\ldots,h$. The dealer makes these integers, $w_l, d_{i,l}$, $l = 1,2,\ldots,k$, and $i = 1,2,\ldots,h$, publicly known.

Secret reconstruction We consider the situation to reconstruct the secret, s_i.

1. Each participant P_r uses his shares, $f_l(x_r)$, $l = 1,2,\ldots,k$, to compute and release one Lagrange component, $c_r = \sum_{l=1}^{k} d_{i,l} f_l(x_r) \prod_{v=1, v \neq r}^{j} \frac{w_l - x_v}{x_r - x_v} \bmod p$.
2. After knowing, c_r, $r = 1,2,\ldots,j$, each participant computes $s_i = \sum_{r=1}^{j} c_r \bmod p$.

Figure 3. Secure multi-secret sharing scheme with h secrets.

DOI: 10.1002/sec

s_k from a linear combination of previously recovered secrets, Then, we examine whether or not s_h can be recovered from the combined knowledge of their shares, previously recovered $h-1$ secrets, s_i, $i=1, 2,\ldots, h-1$, and released Lagrange components of other shareholders. We assume that n Lagrange components are used to recover each secret, $s_i, i=1, 2, \ldots, h-1$. Because each released Lagrange component and each secret is a linear function of kt coefficients of polynomials, $f_l(x), l=1, 2, \ldots, k$, having degree $t-1$ each, the colluded shareholders can construct $(h-1)(n-(t-1))+(h-1)$ equations (i.e., $(h-1)(n-(t-1))$ equations from released Lagrange components of other shareholders and h-1 equations from previously recovered secrets). Furthermore, these colluded shareholders can use their $k(t-1)$ shares to construct $k(t-1)$ equations. In total, they can form $(h-1)(n-(t-1))+(h-1)+k(t-1)$ equations. Because $kt > (h-1)(n-(t-1))+(h-1)+(k(t-1) \rightarrow k > (h-1)(n-t+2)$ (i.e., kt is the number of unknown coefficients of polynomials, $f_l(x)$, $l=1, 2, \ldots, k$, having degree $t-1$ each), this condition prevents the colluded shareholders to solve the secret polynomials, $f_l(x)$, for $l=1, 2, \ldots, k$, and then to obtain the last secret s_h. Thus, the threshold of the uncovered secrets remains the same as the original value. The security of polynomials used to generate secrets is unconditionally protected.

7. CONCLUSION

In this paper, we introduce the model of adversaries and security requirement of the secret reconstruction schemes. Then, we analyze Shamir's secret reconstruction scheme and show that an adversary can obtain the secret when there are more than t participants in Shamir's secret reconstruction. We propose a secure secret reconstruction scheme and use it to design a secure multi-secret sharing scheme with unconditional security. Our proposed schemes are simple modification of Shamir's (t, n) secret sharing scheme.

REFERENCES

1. Benelux JC. Secret sharing homomorphisms: keeping shares of a secret secret. *Advances in Cryptology - Crypto '86*, LNCS 263, Springer-Verlag: 1987; 251–260.
2. Blakley GR. Safeguarding cryptographic keys. *Proceedings of AFIPS'79 Nat. Computer Conf.* 1979; **48**: 313–317, AFIPS Press.
3. Chor B, Goldwasser S, Micali S, Awerbuch B. Verifiable secret sharing and achieving simultaneously in the presence of faults. *Proceedings of 26th IEEE Symp. on Foundations of Computer Science* 1985; 383–395.
4. Chien HY, Jan JK, Tseng YM. A practical (t, n) multi-secret sharing scheme. *IEICE Transactions on Fundamentals -A* 2000; (12): 2762–2765.
5. Feldman P. A practical scheme for non-interactive verifiable secret sharing. *Proceedings of 28th IEEE Symp. on Foundations of Computer Science* 1978; 427–437.
6. Harn L. Efficient sharing (broadcasting) of multiple secrets. *IEE Computers and Digital Techniques* 1995; **142**(3): 237–240.
7. Harn L. Comment multistage secret sharing based on one-way function. *Electronic letters* 1995; **31**(4):262.
8. He J0, Dawson E. Multistage secret sharing based on one-way function. *Electronic letters* 1994; **30**(19): 1591–1592.
9. He J, Dawson E. Multi-secret sharing scheme based on one-way function. *Electronic letters* 1995; **31**(2): 93–94.
10. Harn L, Lin C. Strong (n, t, n) verifiable secret sharing scheme. *Information Sciences* 2010; **180**(16): 3059–3064.
11. Katz J, Koo C, Kumaresan R. Improved the round complexity of VSS in point-to-point networks. *ICALP 2008, Part II*, LNCS 5126, Springer-Verlag: 2008; 499–510
12. Lin HY, Yeh YS. Dynamic multi-secret sharing scheme. *International Journal Contemporary Mathematics Sciences* 2008; **3**(1): 37–42.
13. Lin TY, Wu TC. (t, n) threshold verifiable multisecret sharing scheme based on factorisation intractability and discrete logarithm modulo a composite problems. *IEE Proceedings-Computers & Digital Techniques* 1999; **146**(5): 264–268.
14. Pedersen TP. Non-interactive and information-theoretic secure verifiable secret sharing. *Advances in Cryptology - Crypto '91*, LNCS 576, Springer-Verlag: 1992; 129–140.
15. Shao J, Cao Z. A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme. *Applied Mathematics and Computation* 2005; **168**(1): 135–140.
16. Shamir A. How to share a secret. *Communications of the ACM* 1979; **22**(11): 612–613.
17. Tang C, Yao Z.-A. A new (t, n) -threshold secret sharing scheme. *Proceedings of 2008 International Conference on Advanced Computer Theory and Engineering - ICACTE'08*, 2008; 920–924.
18. Tompa M, Woll H. How to share a secret with cheaters. *Journal of Cryptology* 1989; **1**(3): 133–138.
19. Yang CC, Chang TY, Hwang MS. A (t, n) multi secret sharing scheme. *Applied Mathematics and Computation* 2004; **151**: 483–490.
20. Zhang X, Zhang L, Zhang Q, Tang C. A secret sharing shuffling scheme based on polynomial. *Proceedings of 2008 IEEE International Conference on Information and Automation* 2008; 1746–1750.