Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa

Fair secret reconstruction in (*t*, *n*) secret sharing

Lein Harn [a], *Changlu Lin* [b,*], *Yong Li* [c,d]

[a] Department of Computer Science Electrical Engineering, University of Missouri-Kansas City, MO 64110, USA
[b] College of Mathematics and Computer Science, Fujian Normal University, Fujian 350007, China
[c] School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China
[d] Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China

ARTICLE INFO

Article history:
Available online 22 July 2015

Keywords:
Secret sharing
Rational secret sharing
Lagrange component
Secret reconstruction
Fair secret reconstruction
Asynchronous network

ABSTRACT

In Shamir's (t, n) threshold secret sharing scheme, one secret s is divided into n shares by a dealer and all shares are shared among n shareholders, such that knowing t or more than t shares can reconstruct this secret; but knowing fewer than t shares cannot reveal any information about the secret s. The secret reconstruction phase in Shamir's (t, n) threshold secret sharing is very simple and unconditionally secure. In 2014, Harn has shown that Shamir's secret reconstruction phase cannot prevent an outside attacker from knowing the secret if more than t participants work together in the secret reconstruction phase. Harn's paper also has proposed a reconstruction scheme which can prevent the outside adversary from knowing the secret. However, in Shamir's secret reconstruction, when shares are released asynchronously, a dishonest shareholder (an inside adversary) can always release a fake share last so the dishonest shareholder can exclusively retrieve the secret; but other honest shareholders retrieve a fake secret. In this paper, we design a secret reconstruction scheme against both inside and outside adversaries. This scheme can also be called an *asynchronously rational secret sharing scheme*. Unlike other rational secret sharing schemes, our scheme does not need any interactive dealer, complicate cryptographic primitives, or any assumption on the number of honest shareholders.

1. Introduction

Secret sharing (SS) scheme which was introduced by Blakley (1979) and Shamir (1979) independently in 1979 is a basic tool for protecting cryptographic keys. A threshold SS involves a dealer who has a secret, a set of n participants called shareholders, and a collection of subsets of shareholders who could work together to recover the secret called the access structure. In Shamir's (t, n) SS, the dealer divides the secret s into n *shares* and distributes shares to n shareholders such that: (1) any t or more than t shares can reconstruct the secret, and (2) fewer than t shares cannot obtain any information about the secret s.

Although secret reconstruction phase in Shamir's scheme is very simple, the assumption that participants in this phase are all legitimate shareholders is not always true. In fact, adversaries who do not own valid shares can impersonate shareholders to obtain the secret in Shamir's reconstruction. One simple way to overcome this security problem is to authenticate every participating user to be a legitimate shareholder before reconstructing the secret. Since normal user authentication schemes are one-to-one type of interactions between a prover and a verifier, this approach may slow down the secret

[*] *Corresponding author*. College of Mathematics and Computer Science, Fujian Normal University, Fujian 350007, China. Tel.: +86-152-8010-2192; fax: +86-591-2286-8115

E-mail address: cllin@fjnu.edu.cn (C. Lin).

http://dx.doi.org/10.1016/j.jisa.2015.07.001

reconstruction significantly especially when there is a large number of users participating in the process. In fact, in the secret sharing scheme, only the dealer needs to know who are the shareholders during registration. In the secret reconstruction, shareholders do not need to know each other. Whether or not the participants can reconstruct the secret should depend only on their shares. If all shares are valid, then the secret can be reconstructed. Otherwise, the secret cannot be reconstructed.

The notion of verifiable secret sharing (VSS) which is used to verify the validity of shareholders' shares without revealing their shares and the secret was proposed in 1985 by Chor et al. (1985). There are many papers on VSS in the literature (see Feldman, 1978; Harn and Lin, 2010; Katz et al., 2008; Pedersen, 1992 for more details). Although VSS scheme can be used to check the validity of shares, VSS scheme cannot prevent the adversary from obtaining the secret since shares are revealed to participants in the secret reconstruction. In VSSs, share of each shareholder is protected from others.

In an asynchronous secret reconstruction, when all other shareholders honestly release their shares, a dishonest shareholder can always exclusively recover the secret by presenting a fake share last. Thus, the other honest shareholders get nothing but a fake secret. Although VSS schemes have been developed to detect fake shares (Brickell and Stinson, 1990; Harn and Lin, 2009; Rabin and Ben-Or, 1989), they do not prevent the cheater from exclusively recovering the secret.

1.1. *Related works on fair reconstruction of the secret*

The first fair secret reconstruction scheme is proposed by Tompa and Woll (1988). They proposed to hide the secret s in a sequence, $\{d_1, d_2, \ldots, d_{j-1}, d_j, d_{j+1}, \ldots, d_k\}$, where $d_j = s$, for some j chosen randomly, and $d_i = PDI$, for all $i \neq j$, where PDI is a public dummy integer. Secret reconstruction process involves multiple rounds to recover elements of the sequence one at a time following the order of the sequence. At each round, all shareholders release their shares and perform the reconstruction to recover each element of the sequence. In their scheme, if all shareholders release their shares asynchronously, it is possible that a cheater who releases his share last can obtain the secret exclusively while honest shareholders cannot. On the other hand, if all shareholders release their shares simultaneously, the cheater has a probability $1/k$ of discovering the secret while the honest participants cannot. In other words, the secret reconstruction scheme proposed by Tompa and Woll (1988) works only for synchronous communication channels.

In 1995, Lin and Harn (1995) proposed a fair secret reconstruction scheme. In their scheme, the secret can be reconstructed as a whole in an asynchronous network. Furthermore, the secret s is hidden in a sequence, $\{d_1, \ldots, d_{j-1}, d_j, d_{j+1}, \ldots, d_k\}$, where $d_j = s$, and $d_{j+1} = PI$, for some j and PI chosen randomly, where PI is a public information, and d_i, for $i \neq j$ and $i \neq j+1$, are random dummy secrets. They used the scheme proposed by Rabin and Ben-Or (1989) to verify the validity of each share. Secret reconstruction process involves multiple rounds to recover elements of the sequence one at a time following the order of the sequence. If all shares are valid, the process continues to recover another secret at the next round; otherwise, the reconstruction process stops. When the public information PI is recovered, the previously recovered secret is the secret. Their scheme allows shares to be released asynchronously. However, if the cheater can correctly guess the position of the secret, the cheater can obtain the secret exclusively. The probability of the cheater obtaining the secret exclusively is $1/k$. In 1997, Laih and Lee (1997) proposed a V-fairness (t, n) secret reconstruction scheme and all shareholders have the same probability of obtaining the secret without the need of releasing their shares simultaneously. In their scheme, the dealer divides the secret into multiple subsecrets with different threshold values and generates shares for each sub-secret. There are some recent papers (Lee, 2011; Yang et al., 2011) to improve Laih et al.'s scheme. One main problem of the V-fairness (t, n) secret reconstruction scheme is that the number of cheaters in this model is limited to be less than $t/2$. However, the (t, n) secret reconstruction scheme can prevent up to $t - 1$ dishonest shareholders from recovering the secret. These dishonest shareholders can be the same cheaters in the V-fairness (t, n) secret reconstruction scheme. Thus, the number of cheaters in the V-fairness (t, n) secret reconstruction is inconsistent with the threshold of the (t, n) secret reconstruction scheme.

Recently, Tian et al. (2011) proposed a fair secret reconstruction following Gordon et al.'s approach (Gordon et al., 2008) on complete fairness in secure two-party computation. In the proposed scheme, the secret is hidden in a sequence of secrets and the property of consistency of shares is used to detect cheaters in the secret reconstruction phase. If the cheater can guess correctly the position of the secret, the probability of the cheater obtaining the secret exclusively is $1/k$. Cheating immune secret sharing schemes that the cheaters gain no advantage over honest participants are proposed in Pieprzyk and Zhang (2001, 2004). In this model, the dealer and the combiner are assumed to be honest. Participants can cheat during the secret reconstruction by submitting their fake shares to the combiner. In cheating immune secret sharing scheme, cheaters have no advantage over honest shareholders. D'Arcoa et al. (2006) pointed out that a perfect secret sharing scheme cannot be cheating-immune. All existing cheating immune secret sharing schemes are prohibitively expensive to be suitable for practical use. In 2013, Tian et al. (2013) proposed a fair threshold SS. In their scheme, the cheater detection is based on the scheme proposed by Harn and Lin (2009) which utilizes the redundancy of shares if there are more than t shares available in the secret reconstruction phase and the fairness is based on a similar approach proposed by Tompa and Woll (1988) which utilized a sequence of elements and the secret is hidden in the sequence. However, Harn (2014a) pointed out that the fair threshold SS proposed by Tian et al. only works properly in a synchronous network, but not in an asynchronous network.

In 2004, Halpern and Teague (2004) considered a scenario in which shareholders in the secret reconstruction are neither completely honest nor arbitrarily malicious, but instead shareholders are assumed to be *rational*. A rational shareholder acts honestly when he cannot gain any advantage over other shareholders (i.e., they will all obtain the secret), but acts dishonestly when he can gain advantage over others (i.e., he is the only one to obtain the secret). There are several research papers on the *rational secret sharing* (RSS) (Fuchsbauer et al., 2010; Ong et al., 2009; Tartary et al., 2011; Tian et al., 2015). In fact, the objective of the RSS scheme is to ensure rational shareholders that the secret can be reconstructed successfully. This is the same as that of the fair secret reconstruction scheme which was originally proposed by Tompa and Woll (1988). In most RSS schemes, information exchanged among shareholders is restricted to be in a synchronous channel. There are only a handful papers on RSS schemes using asynchronous channel. These include Maleka et al.'s result (Maleka et al., 2008) which requires an interactive dealer, Fuchsbauer et al.'s work (Fuchsbauer et al., 2010) which requires cryptographic primitives, Ong et al.'s work (Ong et al., 2009) and Moses et al.'s result (Moses and Rangan, 2011) which require to assume that certain number of shareholders must be honest.

One common assumption made for most SS schemes including RSS schemes is that all participants are legitimate shareholders. Therefore, additional process such as VSS is needed prior to the secret reconstruction. We will propose a novel approach in this paper. In our proposed scheme, the secret can only be reconstructed successfully if all participants are legitimate shareholders. Our secret reconstruction scheme is based only on shares and it can prevent illegitimate adversary from obtaining the secret because the adversary does not have any valid share generated by the dealer. Unlike other asynchronous RSS schemes, our proposed scheme is an asynchronously RSS scheme which does not need any interactive dealer, complicate cryptographic primitives, or any assumption on the number of honest shareholders.

1.2. *Our contribution*

In Shamir's (t, n) threshold secret sharing scheme, the dealer uses a linear polynomial of degree $t - 1$ to generate shares for shareholders. Shamir's secret reconstruction scheme considers the situation when all participating users in the secret reconstruction are legitimate shareholders. In this paper, we consider secret reconstruction in a practical situation where inside and outside adversaries may co-exist. The outcome of our proposed solution can be either a random value (not a real secret) if there are any adversaries, or the secret if all participants are legitimate shareholders and act honestly.

We summarize main contributions of this paper here.

- Adversaries in the secret reconstruction are divided into two types: the outside adversary and the inside adversary.
- We propose an asynchronous secret reconstruction scheme (i.e., it can also be called an asynchronously RSS scheme) against both inside and outside adversaries.

1.3. *Outline of this paper*

In the next section, we describe the model of the secret reconstruction including entities, communication networks, assumptions and the objectives of the proposed scheme. Then, in Section 3, we review security of Shamir's threshold secret reconstruction scheme and an asynchronous secret reconstruction against any outside adversary which was published recently (Harn, 2014b). An asynchronous secret reconstruction scheme against both inside and outside adversaries is proposed in Section 4. Section 5 concludes the paper.

2. Models

2.1. *Entities*

Entities in the secret reconstruction phase are classified into the following types.

- **Shareholders:** Each shareholder has obtained a valid share from the dealer initially in the secret reconstruction phase.
- **Participants:** Participants are users who participated in the secret reconstruction phase. Each participant is either an honest shareholder who owns and presents a valid share in the secret reconstruction or an adversary who tries to cheat in the secret reconstruction. In particular, we just focus on two types of adversaries.
  - **Outside adversary:** The outside adversary is an attacker who does not own any valid share when the attacker participated in the secret reconstruction phase.
  - **Inside adversary:** The inside adversary is a shareholder who owns a valid share, but releases a fake share in the secret reconstruction phase. At the same time, the inside adversary can release his fake share last in an asynchronous network and reconstruct the secret exclusively by himself, but other honest shareholders retrieve a fake secret. The inside adversary is a shareholder who is neither completely honest nor arbitrarily malicious, but instead the shareholder is assumed to be *rational*.

Remarks. In the next section, we will show that Shamir's threshold secret reconstruction scheme cannot prevent one outside attacker from knowing the secret when there are more than t participants. VSS can be used to detect outside adversary, but it cannot prevent any outside adversary from gaining access to the secret. This is because the outside adversary is able to recover the secret from any t valid shares when more than t participants work together in the secret reconstruction. The objective of a recently proposed secret reconstruction scheme (Harn, 2014b) is to ensure that the secret cannot be reconstructed successfully when any outside adversary is participated in the secret reconstruction.

2.2. *Communication channels*

Throughout this paper, we assume that all information are communicated asynchronously. In this type of communication, adversaries can always take advantage by releasing their shares last.

2.3. *Assumptions*

The following assumptions are used in the design of our proposed secret reconstruction scheme.

- We assume that j participants, where $t \le j \le n$, work together to recover the secret in the secret reconstruction phase.

- Each participant uses his share(s) to compute one value and send this value to all other participants. There is no need of the dealer in the secret reconstruction.
- The recovered secret is computed based on j exchanged values among participants.
- Each participant is responsible to reconstruct the secret by him/herself without the need of a combiner.
- Participants do not need to know who are legitimate shareholders. The outcome of a secret reconstruction depends only on their shares.

2.4. *Objectives of our proposed secret reconstruction scheme*

There are two secret reconstruction schemes in this paper. The first scheme, ***Scheme 1***, proposed recently (Harn, 2014b) is able to prevent attacks from any outside adversary and the second scheme, ***Scheme 2***, which incorporates Scheme 1, is able to prevent attacks from both inside and outside adversaries.

In the secret reconstruction, an outside adversary acts as a regular shareholder. In Section 4, we review a newly proposed secret reconstruction, called as Scheme 1, based on a simple modification of Shamir's scheme against outside adversary. The objective of Scheme 1 is given in the following definition.

Definition 1. (The objective of Scheme 1). *Scheme 1 is to ensure that under the assumption that all shareholders act honestly (i.e., there is no inside adversary), either (a) all participants recover the secret if all participants are shareholder or (b) no one can recover the secret if there are outside adversaries.*

In an asynchronous secret reconstruction, an inside adversary may release a fake share last after knowing the shares of other honest shareholders. In doing so, the inside adversary can exclusively reconstruct the secret, but other honest shareholders retrieve a fake secret. Secret reconstruction scheme which resists both inside and outside attacks cannot be found in the literature. In Section 5, we introduce a new secret reconstruction, called as Scheme 2, using a space-fairness trade-off technique and the technique in Scheme 1 to prevent attacks from both inside and outside adversaries. The objective of Scheme 2 is given in the following definition.

Definition 2. (The objective of Scheme 2). *Scheme 2 is to ensure that either (a) all participants recover the secret if all participants are shareholders and they act honestly or (b) no one can recover the secret if there are either outside adversaries or any shareholder acts dishonestly.*

3. Review of asynchronous secret reconstruction against outside adversary

In Shamir's (t, n) threshold secret sharing scheme, there are n shareholders $\mathcal{U} = \{U_1, \ldots, U_n\}$ and a dealer D and this scheme consists of two phases.

Scheme: Shamir's (t, n) threshold secret sharing scheme

Share generation phase

Dealer D randomly picks a linear polynomial $f(x)$ with degree $t-1$: $f(x) = a_0 + a_1x + \ldots + a_{t-1}x^{t-1}$, such that the secret is $s = a_0$, where all coefficients $a_i, i = 1, \ldots, t-1$, are in the finite field $\mathbb{F}_p = GF(p)$, and $s \in \mathbb{F}_p = GF(p)$. D does compute n shares $\{s_1, s_2, \ldots, s_n\}$ as:

$$s_i = f(i), i = 1 \ldots, n.$$

Then, the dealer sends each share s_i to the corresponding shareholder U_i via a secure channel.

Secret reconstruction phase

Assume that t shareholders, such as $R = \{U_1, U_2, \ldots, U_t\}$, want to reconstruct the secret s. Shareholders in the set R reveal their shares and reconstruct the secret via using the Lagrange interpolating formula as follows.

$$s = f(0) = \sum_{j=1}^{t} f(j) \left(\prod_{r=1, r \neq j}^{t} \frac{-r}{j-r} \right) (\text{mod}\, p).$$

Shamir's (t, n) scheme satisfies security requirements of the threshold secret sharing scheme, that are, (a) with knowledge of any t or more than t shares can reconstruct the secret s, and (b) with knowledge of fewer than t shares cannot get *any* information about the secret s. Shamir's scheme is *unconditionally secure* since the scheme satisfies these two requirements without making any computational assumption (see Shamir, 1979 for more details).

During secret reconstruction, participating users can be either legitimate shareholders or outside adversaries. Shamir's scheme only considers the situation when all participating users are legitimate shareholders. When more than t users work together and are participated in the secret reconstruction phase and shares are released asynchronously, an outside adversary can always release his share last. After knowing t valid shares of legitimate shareholders, since the secret polynomial, having degree $t-1$, the outside adversary can reconstruct the secret. Furthermore, the attacker can successfully forge a valid share on the polynomial without being detected. Thus, Shamir's (t, n) threshold secret sharing is no longer secure if more than t users are participating in the secret reconstruction phase.

Recently, an asynchronous secret reconstruction (Harn, 2014b), Scheme 1, against outside adversary has been proposed. The main difference between Scheme 1 and Shamir's (t, n) threshold secret sharing scheme is that in Scheme 1, (a) instead of selecting a single polynomial as in Shamir's (t, n) threshold secret sharing scheme, the dealer selects multiple polynomials with degree $t-1$, and (b) instead of hiding the secret in the constant term of the polynomial in Shamir's (t, n) threshold secret sharing scheme, the secret is a linear combination of multiple points of the polynomials. The basic idea of Scheme 1 is that the dealer follows Shamir's (t, n) threshold secret sharing scheme to pick k random polynomials, $f_i(x)$, $i = 1, 2, \ldots, k$, where $kt > n - 1$ (this condition enables the total of coefficients in k random polynomials are no less than n participants), and each polynomial has degree $t-1$ and the dealer generates shares, $f_i(x_r)$, $i = 1, 2, \ldots, k$, for each shareholder U_r, $r = 1, 2, \ldots, n$. For any secret, s, the dealer picks integers, w_i, z_i, in $GF(p)$ where $z_i \notin \{x_1, \ldots, x_n\}$, where x_r is the public information of shareholder U_r, and $z_i \neq z_u$ for any i and u, such that $s = \sum_{i=1}^{k} w_i f_i(z_i)(\bmod p)$. The dealer publicly reveals all integers, w_i, z_i, $i = 1, 2, \ldots, k$. The additive sum of shares, $\sum_{i=1}^{k} w_i f_i(z_i)$, is a share of the additive polynomial $\sum_{i=1}^{k} w_i f_i(x)$ since Shamir's scheme is homomorphic. When there are j shareholders where $t \le j \le n$, for example, $\{U_1, U_2, \ldots, U_j\}$, in the secret reconstruction phase, each shareholder U_r uses his shares, $f_i(x_r)$, where $i = 1, 2, \ldots, k$, to evaluate and release one *Lagrange component*, $c_r = \sum_{i=1}^{k} w_i f_i(x_r) \prod_{l=1, l \neq r}^{j} \frac{z_i - x_l}{x_r - x_l} (\bmod p)$, to all other shareholders. Finally, each shareholder can recover the secret as $s = \sum_{r=1}^{j} c_r$ after they knew c_r, $r = 1, 2, \ldots, j$.

Scheme 1: Asynchronous secret reconstruction against outside adversary (Harn, 2014b)

Share generation phase
Dealer D randomly picks k polynomials, $f_i(x)$, for $i = 1, 2, \ldots, k$, where $kt > n-1$, and each polynomial has degree $t-1$: $f_i(x) = a_{i,0} + a_{i,1}x + \ldots + a_{i,t-1}x^{t-1}$, such that the secret $s = \sum_{i=1}^{k} w_i f_i(z_i)(\bmod p)$ and all coefficients $a_{i,0}, a_{i,1}, \ldots, a_{i,t-1}$ and w_i, z_i, are in the finite field $\mathbb{F}_p = GF(p)$ with $p > s$ (that is $s \in \mathbb{F}_p = GF(p)$) and $z_i \notin \{x_1, \ldots, x_n\}$, x_r is the public information of shareholder U_r, and $z_i \neq z_u$ for any i and u. For every shareholder U_r with public information x_r, D computes k shares, $f_i(x_r)$, $i = 1, 2, \ldots, k$. Then, dealer distributes shares, $f_i(x_r)$, $i = 1, 2, \ldots, k$, to corresponding shareholder U_r secretly. Dealer makes w_i, z_i, $i = 1, 2, \ldots, k$, publicly known.

Secret reconstruction phase

1. Each participant U_r uses his shares, $f_i(x_r)$, $i = 1, 2, \ldots, k$, to compute $c_r = \sum_{i=1}^{k} w_i f_i(x_r) \prod_{l=1, l \neq r}^{j} \frac{z_i - x_l}{x_r - x_l} (\bmod p)$ and sends c_r to all other participants.
2. Each participant computes as follows after he/she knew all c_r, for $r = 1, 2, \ldots, j$.

$$s' = \sum_{r=1}^{j} c_r (\bmod p).$$

The secret can be recovered successfully if participants are all honest shareholders and act honestly to reveal their Lagrange components in Scheme 1. In fact, the secret shares, $f_i(x_r)$, $i = 1, 2, \ldots, k$, are protected unconditionally in the released *Lagrange component*, c_r. Since any released Lagrange component c_r is a linear combination of private shares, $f_i(x_r)$, $i = 1, 2, \ldots, k$, it is impossible to obtain any private share from any released Lagrange component c_r. The outside adversaries do not have enough number of Lagrange components to recover the secret. On the other hand, each released Lagrange component is a linear function of kt coefficients of polynomials, $f_i(x) = a_{i,0} + a_{i,1}x + \ldots + a_{i,t-1}x^{t-1}$, $i = 1, 2, \ldots, k$, and each polynomial has degree $t-1$. If the outside adversary is the last one to release his Lagrange component, the outside adversary cannot compute the secret polynomials, $f_i(x)$, $i = 1, 2, \ldots, k$, from previously released Lagrange components. Detailed discussion can be found in Harn (2014b).

Remark 1. Scheme 1 cannot prevent an inside adversary to gain advantage over honest shareholders. This is because the inside adversary can be the last one to release a fake Lagrange component in an asynchronous network. In the next section, we use both the space-fairness trade-off technique and the technique in Scheme 1 to propose an asynchronous reconstruction scheme to prevent both inside and outside adversaries from taking advantage over honest shareholders.

4. Asynchronous secret reconstruction against both inside and outside adversaries

The basic idea of our proposed scheme to prevent *an inside adversary to gain advantage over honest shareholders* is that the dealer hides the secret v_q in a sequence of k secrets, $\{v_1, v_2, \ldots, v_{q-1}, v_q, v_{q+1}, \ldots, v_k\}$, where v_{q+1} is the "*flag*" used to indicate the position of the secret. Dealer follows Scheme 1 to select k secrets and generate private shares for all shareholders. Dealer also publishes the one-way values, $H(v_r)$, $r = 1, 2, \ldots, k$, to enable shareholders to detect fake shares in the secret reconstruction process. In the process, participants work together to reconstruct secrets one at a time. If there is any fake share in the process, the fake share can be detected and the secret reconstruction process is stopped. Therefore, no one recover the secret. On the other hand, the secret reconstruction process proceeds until reconstructing the flag v_{q+1} if there is no fake share in the process. When the flag is reconstructed, all shareholders have already obtained the secret since the secret is the one that has been previously reconstructed.

Scheme 2: Asynchronous secret reconstruction against both inside and outside adversaries

Share generation phase
The dealer needs to select k secrets $\{v_1, \ldots, v_k\}$ satisfying $v_1 > v_2 > \ldots > v_{q-1} > v_q < v_{q+1}$, where v_q is the secret and each v_r is a random integer in $GF(p)$ $r = 1, 2, \ldots, k, r \neq q$. For each secret, v_r, D follows share generation algorithm of Scheme 1 to compute shares and distribute every share to corresponding shareholder U_i privately where $i = 1, 2, \ldots, n$. At the end, every shareholder has received k shares from the dealer. Dealer computes $H(v_r)$, $r = 1, 2, \ldots, k$, where H is a *collision-resistant* one-way function (Goldreich, 2001), and makes $H(v_r)$, $r = 1, 2, \ldots, k$, publicly known. Note that the public-known one-way value $H(v_r)$ is used to detect cheaters in the secret reconstruction process.

Secret reconstruction phase
Participants work together to reconstruct the secrets $\{v_1, \ldots, v_k\}$ in the following order, $v_1 \rightarrow v_2 \rightarrow \ldots \rightarrow v_{q-1} \rightarrow v_q \rightarrow v_{q+1} \rightarrow \ldots \rightarrow v_k$, one at a time.

1. For each secret v_r, $r = 1, 2, \ldots, k$, participants follow the secret reconstruction algorithm of Scheme 1 to reconstruct the secret.
2. After each secret v_r being recovered, participants check whether the one-way value of the recovered secret is equivalent to the published value $H(v_r)$.
   - If the checking is successful, participants compare the recovered secret with the previously recovered secret.
     - If the recovered secret is greater than the previously recovered secret, the secret is the previously recovered secret and the secret reconstruction process is stopped.
     - Otherwise, continue to recover the next secret in the sequence.
   - If the checking fails, the secret reconstruction process is stopped.

Lemma 1. *In Scheme 2, the probability that anyone can correctly guess the position of the secret in the sequence is 1/k where k is the number of secrets in the sequence.*

Proof. In Scheme 2, the secret v_q is hidden in the sequence, $\{v_1, \ldots, v_k\}$ by the dealer during system set up. Thus, the probability that anyone can correctly guess the position of the secret in the sequence is $1/k$. □

Theorem 1. *Scheme 2 is able to prevent attacks from both inside adversaries and outside adversaries with very high successful probability if k is a large integer.*

Proof. Since Scheme 1 is used by the dealer to generate shares of secrets, it can prevent any outside adversary to recover any secret in the sequence. In other words, Scheme 2 can detect any outside adversary successfully. On the other hand, in Scheme 2, when there is no cheater and all participants are legitimate shareholders in the reconstruction process, the secret reconstruction process proceeds until reconstructing v_{q+1}. Once v_{q+1} is recovered, all participants have already obtained the secret which is the previously recovered secret. On the other hand, when there is an inside adversary in the reconstruction process and the inside adversary releases his fake share last in Scheme 2, the cheating can be detected since $H(v_r') \neq H(v_r)$ and the reconstruction process is stopped. We can classify the occurrences of cheats into three different categories: (a) if the secret reconstruction process is stopped before it reaches the round to reconstruct the secret v_q, then no one can obtain the secret. (b) If the secret reconstruction process is stopped at the round to reconstruct v_q and the inside adversary presents a fake share, then the inside adversary obtains the secret exclusively, but not by other honest shareholders. And (c) if the secret reconstruction process is stopped at the round to reconstruct v_{q+1}, then all participants obtain the secret since the secret has already been reconstructed at the previous round. Among these three categories, only (b) fails to prevent the inside adversary from taking advantage over other honest participants. In this case, the inside adversary needs to guess correctly about the position of the secret in the sequence. According to Lemma 1, the probability of this guess can be reduced by increasing the length of sequence. In summary, Scheme 2 is able to prevent attack from any inside adversary since the probability $1/k$ can be almost ignored if k is large enough. For the other two cases, no one gets the secret for case (a) and everyone gets the secret for case (c). There exists a minor advantage for the inside adversary in these two cases. The adversary knows exactly whether the failure of checking in Scheme 2 is caused by either case (a) or case (c), but honest shareholders cannot differentiate these two cases. However, the result of these two cases, either no one gets the secret or every one gets the secret, satisfies the objective of fairness as we have defined in Section 2. □

5. Conclusion

In this paper, adversaries in the secret reconstruction are classified into two types: the outside adversary and the inside adversary. The former is a participant who does not own any valid share, but impersonates to be a shareholder and tries to reconstruct the secret, and the latter is a shareholder, but releases a fake share. We propose an asynchronous secret reconstruction scheme to protect the secret against both inside and outside adversaries.

Acknowledgements

This research is supported in part by the National Natural Science Foundation of China under Grant Nos. 61103247, U1405255 and 61472032, Natural Science Foundation of Fujian Province under Grant No. 2015J01239, Fujian Provincial Key Laboratory of Network Security and Cryptology Research Fund (Fujian Normal University) (No. 15007) and Key Laboratory of Information Security of ZhongBan Research Fund (Beijing Electronic Science & Technology Institute) (No. 2014KF-CHY).

REFERENCES

Blakley GR. Safeguarding cryptographic keys. In: Proceedings of AFIPS ‘79 nat. computer conf, vol. 48. AFIPS Press; 1979. p. 313–17.

Brickell EF, Stinson DR. The detection of cheaters in threshold schemes. In: Advances in cryptology — crypto ‘88, LNCS 403. Springer-Verlag; 1990. p. 564–77.

Chor B, Goldwasser S, Micali S, Awerbuch B. Secret sharing and achieving simultaneously in the presence of faults. In: Proceedings of 26th IEEE symp. on foundations of computer science. IEEE; 1985. p. 383–95.

D'Arcoa P, Kishimotob W, Stinson DR. Properties and constraints of cheating-immune secret sharing schemes. Discrete Appl Math 2006;154(2):219–33.

Feldman P. A practical scheme for non-interactive verifiable secret sharing. In: Proceedings of 28th IEEE symp. on foundations of computer science. IEEE; 1978. p. 427–37.

Fuchsbauer G, Katz J, Naccache D. Efficient rational secret sharing in standard communication networks. In: Proceedings of the 7th theory of cryptography conference — TCC ‘10, LNCS 5978. Springer-Verlag; 2010. p. 419–36.

Goldreich O. Foundations of cryptography, vol. 1. Basic tools. Cambridge University Press; 2001.

Gordon SD, Hazay C, Katz J, Lindell Y. Complete fairness in secure two-party computation. In: Proceeding of 40th ACM symp. on the theory of computing — STOC '08. ACM Press; 2008. p. 413–22.

Halpern J, Teague V. Rational secret sharing and multiparty computation: extended abstract. In: Proceedings of the thirty-sixth annual ACM symposium on theory of computing — STOC '04. ACM Press; 2004. p. 623–32.

Harn L. Comments on “Fair (*t*, *n*) threshold secret sharing scheme”. IET Inf Secur 2014a;8(6):303–4.

Harn L. Secure secret reconstruction and multi-secret sharing schemes with unconditional security. Security Comm. Netwoks 2014b;7(3):567–73.

Harn L, Lin CL. Detection and identification of cheaters in (*t*, *n*) secret sharing scheme. Des Codes Crypt 2009;52(1):15–24.

Harn L, Lin CL. Strong (*n*, *t*, *n*) verifiable secret sharing scheme. Inf Sci (Ny) 2010;180(16):3059–64.

Katz J, Koo C, Kumaresan R. Improved the round complexity of VSS in point-to-point networks. In: ICALP 2008. Part II, LNCS 5126. Springer-Verlag; 2008. p. 499–510.

Laih CS, Lee YC. V-fairness (t, n) secret sharing scheme. In: Proceedings of IEE conference on computers and digital techniques. IEEE; 1997. p. 245–8.

Lee YC. A simple (*v*, *t*, *n*)-fairness secret sharing scheme with one shadow for each participant. In: Proceedings of WISM 2011. Part I, LNCS 6987. Springer-Verlag; 2011. p. 384–9.

Lin HY, Harn L. Fair reconstruction of a secret. Inf Proc Lett 1995;55(1):45–7.

Maleka S, Shareef A, Rangan CP. Rational secret sharing with repeated games. In: Proceedings of the 4th international information security practice and experience conference — ISPEC '08, LNCS 4991. Springer-Verlag; 2008. p. 334–46.

Moses WK Jr, Rangan CP. Rational secret sharing over an asynchronous broadcast channel with information theoretic security. Int J Netw Secur Appl 2011;3(6):1–18.

Ong SJ, Parkes DC, Rosen A, Vadhan SP. Fairness with an honest minority and a rational majority. In: Proceedings of the 6th theory of cryptography conference — TCC '09, LNCS 5444. Springer-Verlag; 2009. p. 419–36.

Pedersen TP. Non-interactive and information-theoretic secure verifiable secret sharing. In: Advances in cryptology — crypto '91, LNCS 576. Springer-Verlag; 1992. p. 129–40.

Pieprzyk J, Zhang XM. Cheating prevention in secret sharing over $GF(p^t)$. In: Proceedings of indocrypt 2001. LNCS 2247. Springer-Verlag; 2001. p. 79–90.

Pieprzyk J, Zhang XM. On cheating immune secret sharing. Discrete Math Theor Comput Sci 2004;6(2):253–64.

Rabin T, Ben-Or M. Verifiable secret sharing and multiparty schemes with honest majority. In: Proceedings of the 21th ACM symp. on the theory of computing. ACM Press; 1989. p. 73–85.

Shamir A. How to share a secret. Commun ACM 1979;22(11):612–13.

Tartary C, Wang HX, Zhang Y. An efficient and information theoretically secure rational secret sharing scheme based on symmetric bivariate polynomials. Int J Found Comput Sci 2011;22(6):1395–416.

Tian Y, Ma J, Peng C, Zhu J. Secret sharing scheme with fairness. In: Proceedings of 2011 international joint conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11. IEEE; 2011. p. 494–500.

Tian Y, Ma J, Peng C, Jiang Q. Fair (*t*, *n*) threshold secret sharing scheme. IET Inf Secur 2013;7(2):106–12.

Tian Y, Peng C, Lin D, Ma J, Jiang Q, Ji W. Bayesian mechanism for rational secret sharing scheme. Sci China Inf Sci 2015;58(5):1–13.

Tompa M, Woll H. How to share a secret with cheaters. J Cryptol 1988;1(3):133–8.

Yang JH, Chang CC, Wang CH. An efficient V-fairness (t, n) threshold secret sharing scheme. In: Proceedings of the fifth international conference on genetic and evolutionary computing. IEEE; 2011. p. 180–3.