Published in IET Information Security
Received on 16th August 2012
Revised on 10th April 2013
Accepted on 1st July 2013
doi: 10.1049/iet-ifs.2012.0381

ISSN 1751-8709

Generalised cheater detection and identification

Lein Harn

Department of Computer Science Electrical Engineering, University of Missouri, Kansas City, USA
E-mail: harnl@umkc.edu

Abstract: Cheater detection and identification are important issues in the process of secret reconstruction. To detect and identify cheaters most of the algorithms need the dealer to generate and distribute additional information to shareholders. Recently, algorithms have been proposed to detect and identify cheaters. If more than t (i.e. the threshold) shares, for example j (i.e. $t<j$) shares in the secret reconstruction, then redundancy of shares can be used to detect and identify cheaters. The detectability and identifiability of cheaters are proportional to the number of redundant shares. However, the number of redundant shares, $j-t$ is fixed if original shares are used in the secret reconstruction. So, a threshold changeable verifiable secret sharing (TCVSS) has been developed, which allows shareholders working together to change the threshold t into a new threshold t' (i.e. $t'<j$) and generate new shares; whereas at the same time, maintain the original secret. The verifiability of the proposed TCVSS enables shareholders to verify that their new shares have been properly generated. The number of redundant shares can be changed to $j-t'$ if new shares are used in the secret reconstruction. Discussion on how to determine the new threshold t' in order to detect and identify cheaters successfully has also been included.

1 Introduction

In a (t, n) secret-sharing scheme, a dealer divides the secret into shares in such a way that any t (i.e. the threshold) or more than t shares can reconstruct the secret; whereas any fewer than t shares cannot obtain any information about the secret. Shamir's (t, n) secret-sharing scheme [1] is based on the linear polynomial, and secret reconstruction uses Lagrange interpolating polynomial.

When shareholders present their shares in the secret reconstruction, dishonest shareholders (i.e. cheaters) can always exclusively derive the secret by presenting fake shares, and thus the other honest shareholders get nothing but a fake secret. It is easy to see that Shamir's (t, n) secret-sharing scheme does not prevent dishonest shareholders in the secret reconstruction. Cheater detection and identification are important functions in order to provide fair reconstruction of a secret.

There are many research papers in the literature to propose algorithms for cheater detection and identification. Most of these algorithms [2–6] assume that there are exactly t shareholders participating in the secret reconstruction. The dealer needs to provide additional information to enable shareholders to detect and identify cheaters. Some algorithms [7, 8] use error-correcting codes to detect and identify fake shares.

In a recent paper, Harn and Lin [9] proposed a new approach to detect and identify cheaters. The algorithm uses shares to detect and identify cheaters. When there are more than t (i.e. the threshold) shares, for example j (i.e. $t<j$) shares in the secret reconstruction, the redundant shares can be used to detect and identify cheaters. In this approach, shares in a secret-sharing scheme serve for two purposes; that are (a) reconstructing the secret and (b) detecting and identifying cheaters. The detectability and identifiability of cheaters are proportional to the number of redundant shares in the secret reconstruction. However, the number of redundant shares, $j-t$, is fixed in the secret reconstruction. In other words, the detectability and identifiability of cheaters are fixed in the proposed algorithm.

In this paper, we develop a threshold changeable verifiable secret sharing (TCVSS) that allows the shareholders working together to change the threshold t to a new threshold t' (i.e. $t'<t$) and generate new shares used for the secret reconstruction; whereas at the same time, maintain the original secret. The verifiability of the proposed TCVSS enables shareholders to create enough number of redundant shares for the purpose of cheater detection and identification. We also include discussion on how to determine the new threshold t' in order to successfully detect and identify cheaters.

1.1 Related works on threshold changeable secret sharing (TCSS) and verifiable secret sharing (VSS)

In 1999, Martin *et al.* [10] first extended threshold secret-sharing scheme to threshold changeable research and referred it as threshold changeable secret sharing (TCSS). A TCSS scheme allows the threshold of a (t, n) secret sharing to change into a new threshold t' and generates new shares; whereas at the same time, maintains the original secret. TCSS scheme can be used by shareholders to refresh their shares to new shares that are different from previous shares. TCSS is an effective way against adversary attack.

Most TCSS schemes only consider the situation when the threshold is changed from its original value to a larger

value if some shares have been compromised by adversaries. However, there are situations when the threshold needs to be changed to a smaller value. For example, if the total number of shares available for the secret reconstruction is decreased, the threshold needs to be adjusted to a smaller value than the original threshold in order to be able to recover the secret. In this paper, we propose a TCSS scheme such that the threshold can be changed to any value in a simple way.

In a straightforward approach, the dealer can refresh shares by broadcasting some public information to all shareholders if the dealer is active all the time [10, 11]. In general, there are two different approaches to design a TCSS scheme without the assistance of an active dealer. The first approach requires the dealer to prepare the threshold changeability while generating shares for shareholders during set up [12, 13]. For example, instead of providing only one share per shareholder using standard Shamir's secret-sharing scheme, the dealer needs to prepare multiple shares per shareholder or publish some public values during set up. Later, shareholders can change threshold and refresh shares based on these additional information without the need of any secure communication among shareholders. The tradeoffs of this approach is that it does not need any secure channel to refresh shares, but shareholders need more storage space to store their shares or some public information. In addition, since the changeability of threshold needs to be predicated in advance, this approach is only feasible for some applications when the activity in future secret sharing is predicable. The second approach requires shareholders to work together to refresh shares of a new threshold secret sharing [14, 15]. However, this approach needs secure channels to distribute new shares to shareholders. Shareholders need a verifiable secret-sharing scheme [16] to verify their new shares of a TCSS scheme under this approach.

In current literature, TCSS schemes can also be classified into three types: (i) schemes based on the polynomial [1], (ii) schemes based on the geometry [17] and (iii) schemes based on the Chinese Remainder Theorem (CRT) [12]. Since standard Shamir's secret-sharing scheme is very simple and is unconditionally secure, efforts have been devoted to propose TCSS schemes [18, 19] to support standard Shamir's secret-sharing scheme. In 2004, Steinfeld *et al.* [18] have proposed a lattice-based TCSS scheme for supporting standard Shamir's secret generation algorithm. Their scheme does not require secure channel to distribute new shares. The basic idea of their scheme to increase the threshold is to introduce an appropriate amount of random noise to their original shares to compute new shares which contain partial information about original shares. The lattice-based reduction techniques are used to construct an 'error-correction' algorithm to recover the secret. The TCSS scheme proposed by Steinfeld *et al.* [18] cannot use standard Shamir's secret reconstruction algorithm to recover the secret. One important contribution of our paper is that our proposed TCSS scheme can support not only standard Shamir's secret generation algorithm, but also standard Shamir's secret reconstruction algorithm. Our TCSS scheme is very simple and is unconditionally secure.

After shares being refreshed, all shareholders need to work together to verify that the refreshing process is performed by legitimate shareholders and all new shares are valid. In 1985, Chor *et al.* [16] presented the notion of verifiable secret sharing (VSS). In VSS, shareholders are able to verify that their shares are consistent without revealing their shares or the secret. There are vast research papers on the VSS in the literature. On the basis of security assumptions, we can classify VSS into two different types: (i) schemes that are computationally secure and (ii) schemes that are unconditionally secure. For example, Feldman [20] and Pedersen [21] developed non-interactive VSSs based on cryptographic commitment schemes. The security of Feldman's VSS is based on the hardness of solving discrete logarithm, while the privacy of Pedersen's VSS is unconditionally secure and the correctness of the shares depends on a computational assumption. Benaloh [22] proposed an interactive VSS scheme and it is unconditionally secure. Stinson and Wei [23] proposed an unconditionally secure VSS and later, Patra *et al.* [24] proposed a generalised VSS scheme.

1.2 Our contribution

In this paper, shareholders can use our proposed TCVSS to generate new shares and use new shares to reconstruct the secret. These new shares can create enough number of redundant shares to detect and identify cheaters. We summarise the contribution of this paper here.

- We propose to adopt a TCSS scheme to create enough number of redundant shares to detect and identify cheaters.
- We propose an unconditionally secure TCSS to allow shareholders to decrease the threshold t to any new threshold t', that is, $t' < t$.
- The verifiability of the TCVSS enables shareholders to verify that (a) the threshold of new shares is valid and (b) the new shares can recover the original secret.
- We show how to determine the new threshold in order to detect and identify cheaters successfully.

The rest of this paper is organised as follows. In the next section, we briefly review Shamir's (t, n) secret-sharing scheme [1] and Harn and Lin's algorithms [9]. We introduce the model of our TCVSS in Section 3 and scheme in Section 4. We discuss on how to determine the new threshold in Section 5. We conclude in Section 6.

2 Preliminaries

2.1 Review of Shamir's (t, n) secret-sharing scheme [1]

In Shamir's (t, n) secret-sharing scheme based on the polynomial, there are n shareholders and a mutually trusted dealer. The scheme consists of two algorithms as shown in Fig. 1. We note that the above algorithms satisfy the basic requirements of the secret-sharing scheme, that are: (i) with the knowledge of any t or more than t shares, shareholders can reconstruct the secret s, and (ii) with the knowledge of any $t-1$ or fewer than $t-1$ shares, shareholders cannot obtain the secret s. Shamir's secret-sharing scheme is unconditionally secure since the scheme satisfies these two requirements without making any computational assumption. For more information on this scheme, refer to the original paper [1].

2.2 Review of Harn and Lin's algorithm [9]

Benaloh [22] presented a notion of 't-consistency' to determine whether a set of n (i.e. $n > t$) shares are generated from a polynomial having degree $t-1$ at most. Recently,

doi: 10.1049/iet-ifs.2012.0381

Shares generation

Dealer D picks a random polynomial $f(x)$ of degree t-1 : $f(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1} \bmod p$, such that the secret is $s = f(0) = a_0$, and all coefficients, a_i, $i = 1,\ldots,t$-1, are in the finite field $GF(p)$ with $p>s$. D computes n shares, $y_i = f(x_i)$, $i = 1,2,\ldots,n$, where x_i is the public information associated with shareholder U_i. Then, dealer distributes each share y_i to corresponding shareholder U_i secretly.

Secret reconstruction

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

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

Harn and Lin [25] proposed a new definition of 'strong t-consistency' which is the extension of Benaloh's definition.

2.2.1 Definition: strong t-consistency [25]: A set of n shares (i.e. $n > t$) is said to be strong t-consistent if (a) any subset of t or more than t shares can reconstruct the same secret, and (b) any subset of fewer than t shares cannot reconstruct the same secret.

We briefly review the algorithm [9] to detect and identify cheaters using the properties of strong t-consistency and majority voting mechanism, respectively. The algorithm assumes that there are more than t shareholders participated in the secret reconstruction.

It is obvious that if shares in Shamir's (t, n) secret-sharing scheme are generated by a polynomial having degree $t-1$ exactly, then shares are strong t-consistent. Checking strong t-consistency of n shares can be executed very efficiently by using the Lagrange interpolating formula. In fact, to check whether n shares are strong t-consistent or not, it only needs to check whether the interpolation of n shares yields a polynomial having degree $t-1$ exactly. If this condition is satisfied, we can conclude that all shares are strong t-consistent. However, if there are some invalid shares, the degree of the interpolating polynomial of these n shares is more than $t-1$ with very high probability. In other words, most likely, these n shares are not strong t-consistent.

- *Method for detecting cheaters:* If there are more than t shares in Shamir's (t, n) secret-sharing scheme and all shares are valid, all shares must be strong t-consistent. Cheater detection is determined by checking the property of strong t-consistency of n shares.
- *Method for identifying cheaters:* If there are n (i.e. $n > t$) shares in the secret reconstruction and there are some invalid shares, then the reconstructed secrets must be inconsistent. This is because any t shares can reconstruct a secret and there are $\binom{n}{t}$ different combinations. If there are some invalid shares among any t shares, it is very likely to reconstruct a fake secret that is different from the real secret using t valid shares. After cheaters being detected, if the real secret is the majority among $\binom{n}{t}$ reconstructed secrets using any t shares, we can use the majority voting mechanism to identify fake shares. The cheater identification method needs to find out the majority among $\binom{n}{t}$ reconstructed secrets first. Then, the set, A, consisting of t valid shares is identified. Cheaters (i.e. who have presented fake shares) can be identified one at a time by replacing an element in A with the testing share.

The primary advantage of Harn and Lin's algorithm is its simplicity. Cheaters can be detected and identified without needing any additional modification. In [9], it also investigates in detail the bounds of detectability and identifiability of cheaters in terms of the threshold, the number of cheaters and the number of redundant shares in the secret reconstruction. For detail information, interested readers can refer to the original paper.

Remark: As pointed out in [9], the computational complexity of algorithm to detect cheaters is $O(1)$ and the complexity to identify cheaters is $O(j!)$, where j is the number of shares in the secret reconstruction. The algorithm of cheater identification only works when the number of shares in the secret reconstruction is not a big integer. There is one major problem of Harn and Lin's algorithm if original shares are used in the secret reconstruction. Since the number of redundant shares, $j-t$, is fixed, the detectability and identifiability of cheaters are pre-fixed in the proposed algorithm. In the following two sections, we propose a model and a TCVSS scheme to allow shareholders to generate new shares. Using new shares in the secret reconstruction can create enough number of redundant shares to detect and identify cheaters.

3 Model of TCVSS scheme

3.1 Entities

In most VSSs, the dealer is the prover and all shareholders are the verifiers. The verifiers want to verify that their shares are strong t-consistent but without revealing their shares and the secret. In our proposed TCVSS, since all shareholders work together to refresh their original shares to new shares having smaller threshold as compared with the original threshold, each shareholder acts like a prover and a verifier. Thus, in our TCVSS, there are multiple dealers. We do not consider the case when a dealer (the prover) colludes with shareholders (the verifiers). This is because if a dealer colludes with any shareholder, the dealer can just reveal the secret to the shareholder directly and VSS cannot protect the secrecy of the secret. In addition, if any verifier acts dishonestly by releasing a fake value, our proposed TCVSS can detect the existence of the fake share. The cheating shareholder has no advantage over other honest

shareholders. Thus, in our proposed TCVSS, we assume that all shareholders (verifiers) act honestly to verify the strong t-consistent of their shares. The existence of any inconsistent shares may be caused by any shareholder (the prover) who generates invalid sub-shares or by transmission errors in distributing shares.

Cheaters in the secret reconstruction have been differentiated into three types [9] and the capabilities of cheater detection and identification are proportional to the number of redundant shares available in the secret reconstruction. We would like to point out that since the number of redundant shares, $j-t$ is fixed, where j is the number of shares available in the secret reconstruction, the detectability and identifiability of cheaters are pre-fixed in the original Harn–Lin scheme [9]. There are possibilities that the original shares cannot be used to detect/identify cheaters since there is not enough number of redundant shares in the secret reconstruction. In order to increase the number of redundant shares to detect/identify cheaters, TCVSS is used to generate new shares. After the refreshing of shares in TCVSS, the threshold of new shares is decreased as compared with the threshold of original shares. Thus, the number of redundant shares is increased to detect/identify cheaters. Only after all new shares being verified to be strong t-consistent, new shares are used to reconstruct the secret.

3.2 Informal model of our proposed TCVSS

We assume that there are j shareholders, U_i, for $i=1, 2, \ldots, j$, participated in the TCVSS. These shareholders want to make sure that (a) new shares, s_i, for $i=1, 2, \ldots, j$, are strong t-consistent, and (b) new shares can reconstruct the original secret s. In our proposed TCVSS, each shareholder computes, $c_i=F(s_i)$, as his/her released value, where F is a public function. There is an algorithm, VSS, which allows shareholders to verify that all released values are valid, that is

$$\mathrm{VSS}\{\forall c_i = F(s_i) | i = 1, 2, \ldots, j\} = \begin{cases} 0 \rightarrow \text{exists invalid shares;} \\ 1 \rightarrow \text{(a) all are valid shares and (b) these shares can be used to reconstruct the original secret } s \end{cases}$$

Our proposed VSS is different from most other VSSs which verify one share at a time; but our VSS verifies all shares at once. There are only two possible outcomes of our proposed VSS, that are, either all shares are strong t-consistent or there are inconsistent shares. Thus, our proposed VSS is sufficient if all shares are t-consistent; however, if there are inconsistent shares, TCVSS needs to be restarted to generate new shares.

3.3 Properties

We propose TCVSS with the following properties:

Correctness: The outcome of this proposed TCVSS is positive if all new shares are strong t-consistent and can recover the same secret of the original shares; otherwise, there are inconsistent shares.

Efficiency: Our proposed VSS is different from most other VSSs which verify one share at a time; but our VSS verifies all shares at once. In other words, the computational complexity of most VSSs is $O(n)$ where n is the total number of shares involved; but the computational complexity of our proposed VSS is $O(1)$. Thus, the proposed TCVSS is more efficient than other VSSs.

Secrecy: The TCVSS must be able to protect the secrecy of shares and the secret in verification.

4 TCVSS scheme

In this section, we introduce a TCVSS scheme which allows shareholders to change the threshold to a new threshold so that enough number of redundant shares can be created and used to detect and identify cheaters. The proposed TCVSS scheme has three phases: the initial phase, the refreshing phase and the verification phase.

4.1 Initial phase: generating original shares from a trusted dealer

There are n shareholders and a mutually trusted dealer. The scheme is shown in Fig. 2.

4.2 Refreshing phase: generating new shares by shareholders

In Shamir's (t, n) secret-sharing scheme, shareholders are denoted to be in the set $U=\{U_i|i=1, 2, \ldots, n\}$. We assume that j (i.e. $j>t$) shareholders, denoted as $U'=\{U_i'|i=1, 2, ..., j\}$ with their shares $\{(x_1', f(x_1')), (x_2', f(x_2')), \ldots, (x_j', f(x_j'))\}$, want to recover

Original shares generation

Dealer D picks a random polynomial $f(x)$ having 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, $i=1,...,t$-1, are in the finite field $GF(p)$, where p is a prime with $p>s$. D computes n shares, $y_i=f(x_i)$, $i=1,2,...,n$, where x_i is the public information associated with shareholder U_i. Then, dealer distributes each share y_i to corresponding shareholder U_i secretly.

Secret reconstruction

It takes any t or more than t shares, for example, j shares, $\{(x_1', f(x_1')),(x_2', f(x_2')),...,(x_j', f(x_j'))\}$,, as inputs (i.e., $t \le j \le n$), and outputs the secret s using the Lagrange interpolating formula as $s=f(0)=\sum_{i=1}^{j} f(x_i') \prod_{r=1, r\neq i}^{j} \frac{-x_r'}{x_i'-x_r'} \bmod p$.

Fig. 2 *Generating original shares from a trusted dealer*

doi: 10.1049/iet-ifs.2012.0381

New shares generation

Step 1 For each shareholder $U_i^{'}$ in $U^{'}$ uses his share $y_i^{'} = f(x_i^{'})$ obtained from the dealer initially to compute the Lagrange component as $y_i^{''} = f(x_i^{'}) \prod_{r=1, r\neq i}^{j} \frac{-x_r^{'}}{x_i^{'} - x_r^{'}} \bmod p$.

Srep 2 Each shareholder $U_i^{'}$ selects a random polynomial $f_i(x)$ having degree t'-1 and satisfying $f_i(0) = y_i^{''}$. Then, each shareholder $U_i^{'}$ computes ***sub-shares***, $f_i(x_r^{'})$, $i = 1,2,...,j$, for all shareholders in $U^{'}$, and sends each sub-share $f_i(x_r^{'})$ to shareholder $U_r^{'}$ secretly.

Step 3 For each shareholder $U_i^{'}$ in $U^{'}$, after receiving all sub-shares, $f_r(x_i^{'})$, $r = 1,2,...,j$, shareholder $U_i^{'}$ computes $z_i = \sum_{r=1}^{j} f_r(x_i^{'})$. z_i is called the ***new share*** of shareholder $U_i^{'}$. Later, in Theorem 1, we will prove that the threshold of these new shares is t'

Secret reconstruction

It takes any t' or more than t' shares can recover the secret s following the Lagrange interpolating formula.

Fig. 3 *Refreshing shares*

the secret. To successfully detect and identify cheaters in the secret reconstruction, these shareholders work together to change the threshold from t to a new threshold t', where $1 \leq t' \leq t$. In the next section, we will explain how to determine the new threshold value in order to detect and identify cheaters successfully. In our proposed scheme, all j shareholders are needed in the refreshing phase. Our proposed TCVSS scheme works the way as shown in Fig. 3.

Theorem 1: The threshold of these new shares z_i is t' and the secret s can be recovered successfully if any t' or more than t' new shares are used in the secret reconstruction.

Proof: In the following discussion, we assume that all shareholders participated in this phase are legitimate shareholders and act honestly. Since, in Step 3, each new share z_i is the additive sum of sub-shares of polynomials, $f_i(x)$, $i = 1, \ldots, j$, selected by shareholders in U', according to the property of secret sharing homomorphism, these new shares z_i are shares of polynomial, $F(x) = \sum_{i=1}^{j} f_i(x)$ It is obvious that the degree of polynomial $F(x)$ is $t' - 1$. Thus, the threshold of these new shares z_i is t'. In addition, in Step 2, each polynomial $f_i(x)$ selected by shareholder U'_i satisfies

$$f_i(0) = y_i'' = f(x_i') \prod_{r=1, r\neq i}^{j} \frac{-x_r'}{x_i' - x_r'} \bmod p$$

Thus, the interpolating polynomial based on these new shares is $F(x)$ satisfying

$$F(0) = \sum_{i=1}^{j} f_i(0) = \sum_{i=1}^{j} f(x_i') \prod_{r=1, r\neq i}^{j} \frac{-x_r'}{x_i' - x_r'} \bmod p$$

□

Theorem 2: The security of the proposed TCVSS is the same as the Shamir's secret-sharing scheme, which is unconditionally secure.

Proof: In Step 1, each shareholder U'_i in U' acts as the dealer in Shamir's secret-sharing scheme to compute a secret (i.e. a Lagrange component) and in Step 2 to generate sub-shares, $f_i(x_r^{'})$, $i = 1, \ldots, t-1$, for all shareholders. The threshold of the secret is the new threshold value t'. In other words, it needs at least t' sub-shares to recover each Lagrange component. In fact, our TCVSS is a (j, t', j) secret-sharing scheme as proposed in [25] that involves j shareholders to act as dealers to refresh their shares. The security of each sub-share is the same as Shamir's secret sharing scheme which is unconditionally secure. □

Remark: Herzberg *et al.* [26] proposed a share refreshing algorithm. In their algorithm, each shareholder selects a random polynomial $f_i(x_r^{'})$ having degree $t' - 1$ and satisfying $f_i(0) = 0$. Then, shareholder $U_i^{'}$ computes and sends each sub-shares, $f_i(x_r^{'})$, to shareholder U_r', $r = 1, \ldots, j$. Each shareholder $U_i^{'}$ computes new shares as $z_i = f(x_i^{'}) + \sum_{r=1}^{j} f_r(x_r^{'})$. Since $f_r(0) = 0$, $i = 1, \ldots, t-1$, it has $f(0) + \sum_{r=1}^{j} f_r(0) = s$. Thus, the interpolating polynomial based on new shares can recover the original secret. However, since new shares are generated by the polynomial, $z_i = f(x) + \sum_{r=1}^{j} f_r(x)$ having degree $\max\{t' - 1, t - 1\}$, Herzberg *et al.*'s scheme cannot be used to refresh shares with a smaller threshold than the original threshold (i.e. $t' < t$).

4.3 Verification phase

In a conventional VSS, shareholders are able to verify that their shares are consistent (i.e. shares are generated by a polynomial having degree at most $t - 1$) without revealing their shares or the secret. In our proposed TCVSS, shareholders need to verify that (a) the threshold of new shares is t', and (b) any t' or more than t' new shares can recover the original secret. Our proposed TCVSS is based on the model proposed by Benaloh [22] in which all shareholders work together to verify their new shares. Only after new shares having been successfully verified, shareholders can upload their new shares to replace original shares. The verification is shown in Fig. 4.

New shares verification

In order to verify npew shares, $z_i, i = 1,2,..., j$, generated in Scheme 2, shareholders need to repeat Scheme 2 to generate verification shares, $w_i, i = 1,2,..., j$. In other words, each shareholder $U_i^{'}$ selects a random polynomial $g_i(x)$ having degree t'-1 and computes sub-shares, $g_i(x_r^{'})$, $i = 1,2,..., j$, for all shareholders in U' , and sends each sub-share $g_i(x_r^{'})$ to shareholder $U_r^{'}$ secretly. After receiving all sub-shares, $g_r(x_i^{'})$, $r = 1,2,..., j$, each shareholder $U_i^{'}$ computes verification share, w_i, as $w_i = \sum_{r=1}^{j} g_r(x_i^{'})$.

Step 1 All shareholders agree on a random integer, $d \in Z_p$. Each shareholder $U_i^{'}$ uses his new share z_i and verification share w_i to compute $u_i = z_i + dw_i \bmod p$. u_i is made publicly known.

Step 2 From the released values, $u_i, i = 1,2,..., j$, each shareholder can construct an interpolating polynomial $U(x)$. If the degree of polynomial $U(x)$ is exactly t'-1, the degree of the new shares is exactly t'-1 (i.e., We will prove that the new threshold is t' in ***Theorem 3***) and continue to the next step; otherwise, it needs to restart a new share refreshing process.

Srep 3 Each shareholder $U_i^{'}$ uses his new share z_i and the original share $f(x_i^{'})$ to compute $v_i = f(x_i^{'}) - z_i \bmod p$. v_i is made publicly known.

Step 4 From the released values, $v_i, i = 1,2,..., j$, each shareholder can construct an interpolating polynomial $V(x)$. If $V(0) = 0$, new shares can be used in Harn-Lin's scheme [9] to reconstruct the original secret and to detect/identify cheaters (i.e., We will prove this result in ***Theorem 4***); otherwise, it needs to restart a new share refreshing process.

Fig. 4 *Verifying shares*

Theorem 3: The threshold of these new shares z_i is t' if the verification is successful in Step 2.

Proof: In the following discussion, we assume that all shareholders participated in this refreshing phase are legitimate shareholders and act honestly. Since each new share z_i is the additive sum of sub-shares of polynomials, $f_i(x)$, $i = 1, 2, \ldots, j$, selected by shareholders in U', according to the property of secret sharing homomorphism, these new shares z_i are shares of polynomial $F(x) = \sum_{i=1}^{j} f_i(x) \bmod p$. Similarly, verification shares w_i are shares of polynomial $G(x) = \sum_{i=1}^{j} g_i(x) \bmod p$. The interpolating polynomial of j released values, u_i, $i = 1, 2, \ldots, j$, is $U(x) = F(x) + dG(x)$. It is obvious that the degree of polynomial $U(x)$ is $t' - 1$ exactly if and only if either (a) the degree of both polynomials, $F(x)$ and $G(x)$, is larger than $t' - 1$, or (b) the degree of both polynomials, $F(x)$ and $G(x)$, is at most $t' - 1$. Since d is a random integer selected by all shareholders together, the probability that the degree of both polynomials, $F(x)$ and $G(x)$, is larger than $t' - 1$ is extremely small. In other words, if the degree of polynomial $U(x)$ is $t' - 1$ exactly, each shareholder can be convinced that the degree of polynomials, $F(x) = \sum_{i=1}^{j} f_i(x) \bmod p$ is at most $t' - 1$. Furthermore, since each shareholder has contributed a random polynomial, $f_i(x)$, having degree $t' - 1$ exactly in the additive sum of polynomial, $F(x)$, the degree of $F(x)$ should be $t' - 1$ exactly. Thus, the threshold of these new shares z_i is t'. □

Theorem 4: The new shares z_i can be used to reconstruct the original secret if $V(0) = 0$ in Step 4.

Proof: In the following discussion, we assume that all shareholders participated in this refreshing phase are legitimate shareholders and act honestly. The interpolating polynomial of j released values, v_i, $i = 1, 2, \ldots, j$, is $V(x) = f(x) - F(x)$. Since

$$F(x) = \sum_{i=1}^{j} f_i(x) \bmod p \quad \text{and}$$

$$f_i(0) = y_i'' = f(x_i') \prod_{r=1, r \neq i}^{j} \frac{-x_r'}{x_i' - x_r'} \bmod p$$

we have

$$\begin{aligned} V(0) &= f(0) - F(0) = f(0) - \sum_{i=1}^{j} f_i(0) \\ &= f(0) - \sum_{i=1}^{j} f(x_i') \prod_{r=1, r \neq i}^{j} \frac{-x_r'}{x_i' - x_r'} \bmod p = f(0) - f(0) \\ &= 0 \end{aligned}$$

Theorems 3 and 4 have shown that our proposed VSS satisfies the property of correctness as stated in Section 3.3. Since our proposed VSS verifies all shares at once, the proposed TCVSS is very efficient. In the following theorem, we show that our proposed VSS satisfies the property of secrecy as stated in Section 3.3.

Theorem 5: The new shares and the secret have not been revealed in the proposed VSS and the security is unconditionally secure.

Proof: In the proposed VSS, the only values available to the adversary are $u_i = z_i + dw_i \bmod p$ and $v_i = f(x'_i) - z_i \bmod p$,

doi: 10.1049/iet-ifs.2012.0381

$i = 1, 2, \ldots, j$. It is impossible to determine the new share z_i from public values, u_i and v_i, since both verification share w_i and original share $f(x'_i)$ have never been released to the public. In addition, the interpolating polynomial $U(x) = F(x) + dG(x)$ based on public values, u_i, $i = 1, 2, \ldots, j$, does not reveal the secrecy of polynomials, $F(x)$ and $G(x)$. Similarly, the interpolating polynomial $V(x) = F(x) - f(x)$ based on public values, v_i, $i = 1, 2, \ldots, j$, does not reveal the secrecy on polynomials, $F(x)$ and $f(x)$. The secrecy of VSS is unconditionally protected. □

Remark: Our proposed TCVSS works properly if the new threshold t' satisfies $j \geq t' \geq 1$. However, if $t' > t$, there is no need to refresh shares since the number of redundant shares is already enough to detect and identify cheaters.

Remark: There are $j - t$ redundant shares if original shares are used in the secret reconstruction. However, there are $j - t'$ redundant shares if new shares are used in the secret reconstruction. In the next section, we will discuss how to choose the new threshold t' properly in order to successfully detect and identify cheaters.

5 Determining t' in our design

After new shares being successfully verified in Phase 3, these new shares can be used to reconstruct the secret and at the same time, to detect/identify cheaters following the scheme proposed in [9]. Harn and Lin [9] have classified three types of attacks according to the behaviour of cheaters; that are, (a) *Type 1 attack* – attackers present fake shares without any collaboration; (b) *Type 2 attack* – shares are released synchronously and colluded attackers modify their shares to fool honest shareholders; and (c) *Type 3 attack* – shares are released asynchronously and colluded attackers modify their shares to fool honest shareholders. The bounds of detection and identification of cheaters are functions of the threshold, the number of cheaters and the number of shares in the secret reconstruction. Interested readers can refer to Theorems 1–3 in the original paper [9] for detail proofs. A recent paper, Ghodosi [27] has proposed a wise cheating attack on the cheater detection method based on the property of strong t-consistency. New bounds of detection of cheaters can be found in a straightforward approach. Here, we list the new bounds of detection and identification of cheaters incorporating the attack proposed by Ghodosi as the following Corollaries of Theorems 1, 2 and 3 in the original paper [9].

Corollary 1: Under Type 1 attack, Harn–Lin's scheme can successfully detect cheaters if $j \geq t + 1$, and identify cheaters if $j - c > t$, where j is the number of shares, t is the threshold and c is the number of cheaters in the secret reconstruction. □

Corollary 2: Under Type 2 attack, Harn–Lin's scheme can successfully detect cheaters if $j - c \geq t$, and identify cheaters if $\{(c < t) \cap (j - c \geq t + 1)\} \cup \{(c \geq t) \cap (j - c > c + t - 1)\}$. □

Corollary 3: Under Type 3 attack, Harn–Lin's scheme can successfully detect cheaters if $j - c \geq t$, and identify cheaters if $\{j \geq t + 1\} \cup \{j - c > c + t - 1\}$. □

In this paper, we consider the situation when there are j (i.e. $n \geq j \geq t$) shares presented in the secret reconstruction. To create enough number of redundant shares to detect and identify cheaters successfully, the proposed TCVSS algorithm enables shareholders to work together to change the threshold from its original value t to a new value t' such that there are $j - t'$ redundant shares in the secret reconstruction. New shares of the (t', j) secret-sharing scheme are generated and are used in the secret reconstruction.

Table 1 Bounds of detectability and identifiability

	Detectability	Identifiability
Type 1 attack	$t' \leq j - 1$	$t' \leq j - c - 1$
Type 2 attack	$t' \leq j - c$	$\{c - 1 \leq t' \leq j - c - 1\} \cup \{t' \leq \min(c, j - 2c)\}$
Type 3 attack	$t' \leq j - c$	$t' \leq \min(j - c, j - 2c)$

Table 2 Maximum values of t' for $t = 7$, $j = 9$, $n = 15$, and $c = 2$

	max(t') for detectability	max(t') for identifiability
Type 1 attack	8	6
Type 2 attack	7	6
Type 3 attack	7	5

Let us re-evaluate the bounds in terms of the new threshold t'. We can rewrite conditions associated with Corollaries 1, 2 and 3, in terms of the new threshold value: (i) Under Type 1 attack, the proposed algorithm can successfully detect cheaters if $t' \leq j - 1$, and identify cheaters if $t' \leq j - c - 1$, (ii) Under Type 2 attack, the proposed algorithm can successfully detect cheaters if $t' \leq j - c$, and identify cheaters if $\{c - 1 \leq t' \leq j - c - 1\} \cup \{t' \leq \min(c, j - 2c)\}$, (iii) Under Type 3 attack, the proposed algorithm can successfully detect cheaters if $t' \leq j - c$, and identify cheaters if $t' \leq \min(j - c, j - 2c)$. We summarise this result in Table 1.

We use the following example to explain how to choose the new threshold t' to meet the requirements of cheater detection and identification. Assume that in Shamir's (7, 15) secret-sharing scheme, the secret reconstruction needs to detect and identify at most two cheaters. From Table 1, we can compute the maximal values of the new threshold t'. We list the threshold values in Table 2.

6 Conclusions

Harn and Lin proposed a very simple scheme to detect and identify cheaters recently. The detectability and identifiability of the proposed scheme is proportional to the number of redundant shares in the secret reconstruction. However, if there are j shares in the secret reconstruction, the number of redundant shares is $j - t$ which is a pre-fixed number. We propose a TCVSS scheme to allow shareholders to generate new shares from their original shares. Using these new shares to reconstruct the secret, it creates enough number of redundant shares to detect and identify cheaters successfully. The proposed TCVSS scheme is simple and is unconditionally secure. With this TCVSS scheme, Harn–Lin's scheme becomes very flexible and is able to detect and identify various numbers of cheaters in the secret reconstruction.

7 References

1 Shamir, A.: 'How to share a secret', *Commun. ACM*, 1979, **22**, (11), pp. 612–613
2 Tompa, M., Wollm, H.: 'How to share a secret with cheaters', *J. Cryptol.*, 1989, **1**, (3), pp. 133–138
3 Rabin, T., Ben-Or, M.M.: 'Verifiable secret sharing and multiparty protocols with honest majority'. Proc. 21st Annual ACM Symp. Theory of Computing, 1989, pp. 73–85
4 Carpentieri, M., De Santis, A., Vaccaro, U.: 'Size of shares and probability of cheating in threshold schemes'. Advances in Cryptology – EUROCRYPT '93, (*LNCS*, **765**), 1994, pp. 118–125
5 Kurosawa, K., Obana, S., Ogata, W.: '*t*-cheater identifiable (*k*, *n*) secret sharing schemes'. Advances in Cryptology – CRYPTO '95, (*LNCS*, **963**), 1995, pp. 410–423
6 He, J., Dawson, E.: 'Shared secret reconstruction', *Des. Codes Cryptogr.*, 1998, **14**, (3), pp. 221–237
7 McEliece, R.J., Sarwate, D.V.: 'On sharing secrets and Reed-Solomon codes', *Commun. ACM*, 1981, **24**, (9), pp. 583–584
8 Blundo, C., De Santis, A., Gargano, L., Vaccaro, U.: 'Secret sharing schemes with veto capabilities'. Proc. First French-Israeli Workshop on Algebraic Coding, (*LNCS*, **781**), 1993, pp. 82–89
9 Harn, L., Lin, C.: 'Detection and identification of cheaters in (*t*, *n*) secret sharing scheme', *Des. Codes Cryptogr.*, 2009, **52**, (1), pp. 15–24
10 Martin, K., Pieprzyk, J., Safavi-Naini, R., Wang, H.: 'Changing thresholds in the absence of secure channels', *J. Australian Comput.*, 1999, **31**, pp. 34–43
11 Blundo, C., Cresti, A., Santis, A.D., Vaccaro, U.: 'Fully dynamic secret sharing schemes'. Proc. Crypto '93, (*LNCS*, **773**), 1993, pp. 110–125
12 Lou, T., Tartary, C.: 'Analysis and design of multiple threshold changeable secret sharing schemes'. Proc. CANS '08, (*LNCS*, **5339**), 2008, pp. 196–213
13 Maeda, A., Miyaji, A., Tada, M.: 'Efficient and unconditionally secure verifiable threshold changeable scheme'. Proc. ACISP '01, (*LNCS*, **2119**), 2001, pp. 403–416
14 Shi, R., Zhong, H.: 'A secret sharing scheme with the changeable threshold value'. Proc. 2009 Int. Symp. Information Engineering and Electronic Commerce, 2009, pp. 238–246
15 Zhang, X., He, M.: 'Collusion attack resistance and practice-oriented threshold changeable sharing schemes'. Proc. 24th IEEE Int. Conf. Advanced Information Networking and Applications, 2010, pp. 745–752
16 Chor, B., Goldwasser, S., Micali, S., Awerbuch, B.: 'Verifiable secret sharing and achieving simultaneously in the presence of faults'. Proc. 26th IEEE Symp. Foundations of Computer Science, 1985, pp. 383–395
17 Martin, K.M., Pieprzyk, J., Safavi-Naini, R., Wang, H.: 'Changing thresholds in the absence of secure channels'. Proc. ACISP'99, (*LNCS*, **1587**), 1999, pp. 177–19
18 Steinfeld, R., Wang, H., Pieprzyk, J.: 'Lattice-based threshold changeability for standard Shamir secret-sharing schemes'. Advances in Cryptology – ASIACRYPT'04, (*LNCS*, **3329**), 2004, pp. 170–186
19 Tartary, C., Wang, H.: 'Dynamic threshold and cheater resistance for Shamir secret sharing scheme'. Proc. Inscrypt'06, (*LNCS*, **4318**), 2006, pp. 103–117
20 Feldman, P.: 'A practical scheme for non-interactive verifiable secret sharing'. Proc. 28th IEEE Symp. Foundations of Computer Science, 1987, pp. 427–437
21 Pedersen, T.P.: 'Non-interactive and information-theoretic secure verifiable secret sharing'. Advances in Cryptology – CRYPTO'91, (*LNCS*, **576**), 1992, pp. 129–140
22 Benaloh, J.C.: 'Secret sharing homomorphisms: keeping shares of a secret secret'. Advances in Cryptology – CRYPTO'86, (*LNCS*, **263**), 1987, pp. 251–260
23 Stinson, D.R., Wei, R.: 'Unconditionally secure proactive secret sharing scheme with combinatorial structures'. Proc. SAC'99, (*LNCS*, **1758**), 2000, pp. 200–214
24 Patra, A., Choudhary, A., Rangan, C.P.: 'Efficient statistical asynchronous verifiable secret sharing with optimal resilience'. Proc. ICITS'09, (*LNCS*, **5973**), 2010, pp. 74–92
25 Harn, L., Lin, C.: 'Strong (*n*, *t*, *n*) verifiable secret sharing scheme', *Inf. Sci.*, 2010, **180**, (16), pp. 3059–3064
26 Herzberg, A., Jarecki, S., Krawczyk, H., Yung, M.: 'Proactive secret sharing or: how to cope with perpetual leakage'. Advances in Cryptology – CRYPTO'95, (*LNCS*, **963**), 1995, pp. 339–352
27 Ghodosi, H.: 'Comments on Harn–Lin's cheating detection scheme'. Designs, Codes and Cryptography, DOI: 10.1007/s10623-010-9416-6, Online version, July, 2010

doi: 10.1049/iet-ifs.2012.0381