Theoretical Computer Science 418 (2012) 106–115

Contents lists available at SciVerse ScienceDirect

Theoretical Computer Science

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

Threshold changeable secret sharing schemes revisited☆

Zhifang Zhang [a], Yeow Meng Chee [b,*], San Ling [b], Mulan Liu [a], Huaxiong Wang [b]

[a] Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, China

[b] Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore

ARTICLE INFO

Article history:
Received 3 March 2009
Received in revised form 24 October 2010
Accepted 28 September 2011
Communicated by A. Fiat

Keywords:
Secret sharing schemes
Threshold changeable secret sharing schemes
Perfect security
Computational security

ABSTRACT

This paper studies the methods for changing thresholds in the absence of secure channels after the setup of threshold secret sharing schemes. First, we construct a perfect (t, n) threshold scheme that is threshold changeable to $t' > t$, which is optimal with respect to the share size. This improves the scheme of Wang and Wong by relaxing the requirement from $q \geq n + v$ to $q > n$ with the secret-domain $\mathbb{F}_q^v$. But these threshold changeable schemes along with most previously known schemes turn out to be insecure under the collusion attack of players holding initial shares. By adding a broadcast enforcement term we enhance the model with collusion security and N options of threshold change. Then we construct a computationally secure scheme under the enhanced model, which involves much shorter shares and broadcast messages than the perfect schemes. Finally, we discuss how to realize the enrollment and disenrollment of players, and particularly, how to deal with L-fold changes of access polices.

1. Introduction

A (t, n) threshold secret sharing scheme enables the sharing of a secret among n players such that any t of the players can later recover the secret from their shares, while any less than t players cannot. The first (t, n) threshold secret sharing schemes were designed by Blakley [3] and Shamir [17] in 1979. Blakley gave a geometric construction and Shamir constructed a scheme based on polynomial interpolation. Secret sharing schemes were first proposed as a tool for key management. Now it is a fundamental building block in many cryptographic protocols such as threshold signature schemes, threshold encryption schemes, and secure multiparty computation.

During the setup phase of a (t, n) threshold secret sharing scheme, a dealer (represented as Dealer hereafter) distributes a share to each of the n players through secure channels. The security requirement is that any fewer than t players cannot recover the secret from their shares. Therefore, a (t, n) threshold secret sharing scheme can protect the secret against an adversary who can corrupt at most $t - 1$ players. In practice, after the setup of a secret sharing scheme and before the recovery of the secret, the security policy and adversary structure may change. For instance, some players might have left the group and the adversary might have corrupted more than $t - 1$ players. Thus, it is desirable to design a threshold secret sharing scheme which allows the parameters t and n to change before the recovery of the secret, and which remains secure under these changes. Many methods have been developed for solving this problem. Examples include share redistribution (where secure channels between players are needed) [6,8,16], local updates to shares [15,18], and message broadcast [1,4].

☆ Part of this work was done while the first author was visiting Nanyang Technological University, under the support of the Singapore Ministry of Education Research Grant T206B2204.

* Corresponding author. Tel.: +65 6513 7188.
E-mail addresses: zfz@amss.ac.cn (Z. Zhang), ymchee@ntu.edu.sg (Y.M. Chee), lingsan@ntu.edu.sg (S. Ling), mlliu@amss.ac.cn (M. Liu), hxwang@ntu.edu.sg (H. Wang).

0304-3975/$ – see front matter © 2012 Published by Elsevier B.V.
doi:10.1016/j.tcs.2011.09.027

In this paper, we study how to update the threshold t as well as the number of players n in the absence of secure channels after the setup of threshold secret sharing schemes. More specifically, the contributions of this paper are as follows.

- We design a perfect (t, n) threshold secret sharing scheme that is threshold changeable to $t' > t$. Martin et al. [15] proved a lower bound for the share size in such schemes and constructed an *optimal* scheme that achieves the bound based on geometric methods. Maeda et al. [12] constructed an *almost optimal* threshold changeable secret sharing scheme based on Shamir's scheme. Our scheme, which is also based on Shamir's scheme, is optimal. The idea behind our scheme originates from Wang and Wong [19], where they focused on the communication complexity in secret reconstruction. In the process, we also improve the scheme of Wang and Wong by relaxing the requirement from $q \geq n + v$ to $q > n$, where $\mathbb{F}_q^v$ is the secret-domain.
- There exists a security drawback in our threshold changeable scheme, as well as in many previously known schemes [6,8,16,15,18]: after the threshold has been changed to t', less than t' players may get partial information about the secret from their updated shares. Even worse, any t players can still recover the secret if they keep their initial shares. In order to overcome this problem, we adopt the model of threshold changeable schemes which is broadcast enforced. That is, a threshold is validated only after Dealer broadcasts the associated message. The broadcast enforced model has already been adopted in the dynamic secret sharing scheme [4] and the threshold scheme with disenrollment [11]. Under this model, we construct a computationally secure (in the sense of [10]) threshold changeable scheme that is secure even if the adversary gets the entire history of the corrupted players' shares. If the threshold of the scheme is changeable to any threshold in $\{t_1, \ldots, t_N\}$, with $1 < t_1 < \cdots < t_N \leq n$, then the size of each share is $\frac{N}{t_N - 1} H(S)$ and the size of the broadcast message required to activate the (changed) threshold t_j is $\frac{N-j+1}{t_N-1} H(S)$, where $H(S)$ denotes the size of the secret. Since N is usually a small number in practice, and $t_i > i$ for $1 \leq i \leq N$, the sizes of shares and broadcast messages are much smaller than those for the perfect scheme.
- We also provide methods for realizing the disenrollment of players and L-fold changes of the access policies under the condition that no secure channels exist any more after the initial phase.

Organization of this paper is as follows. Section 2 introduces related notions and results. Section 3 gives a construction for an optimal perfect threshold changeable scheme from Shamir's scheme. Section 4 describes the model of threshold changeable schemes that we adopt thereafter. Section 5 gives a construction of a computationally secure scheme under the model of Section 4. Section 6 discusses the methods of realizing the disenrollment of players and L-fold changes of the access policies.

2. Preliminaries

Let $\mathbb{Z}_{\geq 0}$ denote the set of nonnegative integers. For integers $i \leq j$, the set $\{i, i+1, \ldots, j\}$ is denoted by $[i, j]$. We further abbreviate $[1, j]$ to $[j]$. A function $\mu : \mathbb{Z}_{\geq 0} \to \mathbb{R}$ is *negligible* if for every positive polynomial $p(\cdot)$, there exists a positive integer N such that $\mu(n) < 1/p(n)$ for all $n > N$.

For a univariate polynomial $f(x) = \sum_{i \geq 0} a_i x^i$, the *coefficient operator* $[x^k]$ is defined so that $[x^k]f(x) = a_k$.

Let $P = \{P_1, \ldots, P_n\}$ be a set of n *players* and $t \in [n]$. Let S be a finite set of secrets, called the *secret-domain*, and let R be a set of *random strings*. Let $H(\cdot)$ denote the *entropy function*. A *secret sharing scheme over* P is a mapping $\Pi : S \times R \to S_1 \times \cdots \times S_n$, where S_i is called the *share-domain* of P_i. Dealer shares a *secret* $s \in S$ among the players according to Π by first sampling a random string $r \in R$, computing the shares $\Pi(s, r) = \langle s_1, \ldots, s_n \rangle$, and then privately communicating each *share* s_i to P_i. For any subset $A \subseteq P$, S_A denotes the set of shares held by all players in A.

For simplicity, the symbol used to denote a set is also used to denote the random variable which ranges over it. For instance, S denotes the random variable ranging over the secret-domain S according to some specified distribution, and $\Pi(s, R)|_A$ denotes a random variable ranging over S_A induced by the random variable R and the secret s. Whether a symbol denotes a set or a random variable should be clear from the context.

A (t, n) *threshold secret sharing scheme* (or *threshold scheme*, in short) over P is a secret sharing scheme $\Pi : S \times R \to S_1 \times \cdots \times S_n$ satisfying the following two conditions:

(1) for all $A \subseteq P$ and $|A| \geq t$, $H(S|S_A) = 0$;
(2) for all $B \subseteq P$ and $|B| < t$, $0 < H(S|S_B) \leq H(S)$.

Condition (1) above states the recoverability of the secret by any t players, and condition (2) states that any fewer than t players cannot uniquely determine the secret, although they may get partial information of the secret. Furthermore, if it holds that $H(S|S_B) = H(S)$ for all $B \subseteq P$ and $|B| < t$, then the (t, n) threshold scheme is called *perfect*. In a perfect (t, n) threshold scheme, any fewer than t players get absolutely no information about the secret even though they may have unlimited computational power.

2.1. Threshold changeable schemes

Definition 2.1 (*Martin et al. [15]*)**.** A perfect (t, n) threshold scheme $\Pi : S \times R \to S_1 \times \cdots \times S_n$ is called *threshold changeable* to $t' > t$ if there exist publicly known functions $h_i : S_i \to T_i$, $i \in [n]$, such that for all $A \subseteq P$, it holds that

$$\begin{cases} H(S|T_A) = 0, & \text{if } |A| \geq t' \\ H(S|T_A) \leq H(S), & \text{if } |A| < t', \end{cases}$$

where $T_A = \{\ h_i(S_i) \mid P_i \in A\}$. We call this a perfect $(t \to t', n)$ *threshold changeable scheme*, and call h_i the *share updating function*.

Since a perfect $(t \to t', n)$ threshold changeable scheme is initially a perfect (t, n) threshold scheme, we have $H(S|S_A) = H(S)$ for $|A| < t$. It trivially follows that $H(S|T_A) = H(S)$ for $|A| < t$.

The efficiency of a perfect $(t \to t', n)$ threshold changeable scheme is typically measured by the size of each player's shares, given by the entropy $H(S_i)$ as well as the size of each updated share, $H(T_i)$. The following theorem gives lower bounds for these share sizes.

Theorem 2.1 (*Martin et al. [15]*). *Let $\Pi : S \times R \to S_1 \times \cdots \times S_n$ be a perfect $(t \to t', n)$ threshold changeable scheme over P with the set of share updating functions $\{h_i : S_i \to T_i \mid i \in [n]\}$. Then*

(1) $H(S_i) \geq H(S)$ *for* $i \in [n]$;
(2) $\sum_{P_i \in A} H(T_i) \geq \frac{t'}{t'-t+1} H(S)$ *for* $A \subseteq P$ *and* $|A| = t'$;
(3) $\max_{i \in [n]}\{H(T_i)\} \geq \frac{1}{t'-t+1} H(S)$.

A perfect $(t \to t', n)$ threshold changeable scheme is called *optimal* if the bounds in Theorem 2.1 are met with equality. Martin et al. [15] gave a geometric construction for an optimal perfect $(t \to t', n)$ threshold changeable scheme. As to our knowledge, no other constructions for optimal perfect $(t \to t', n)$ threshold changeable schemes are known. An almost optimal scheme was proposed by Maeda et al. [12].

3. An optimal perfect threshold changeable scheme

In this section, we construct an optimal perfect $(t \to t', n)$ threshold changeable scheme, which may be viewed as a variant of the geometric construction by Martin et al. [15] and the polynomial construction by Wang and Wong [19]. We also point out some security problems existing in the threshold changeable scheme.

3.1. Our construction: Scheme P-TCSS

Without loss of generality, suppose that the secret domain is $S = \mathbb{F}_q^{t'-t+1}$, where $q > n$ is a prime power. We also assume that $x_1, \ldots, x_n \in \mathbb{F}_q$ are n distinct nonzero elements that are publicly known.

Our construction Scheme P-TCSS is as follows.

To share a secret $s \in \mathbb{F}_q^{t'-t+1}$, Dealer randomly selects polynomials $f_1, \ldots, f_{t'-t+1} \in \mathbb{F}_q[x]$, where

$$\begin{aligned} f_1(x) &= a_{1,0} + a_{1,1}x + \cdots + a_{1,t-1}x^{t-1}, \\ f_2(x) &= a_{2,0} + a_{2,1}x + \cdots + a_{2,t-1}x^{t-1} + a_{2,t}x^t, \\ &\vdots \\ f_{t'-t+1}(x) &= a_{t'-t+1,0} + a_{t'-t+1,1}x + \cdots + a_{t'-t+1,t'-t}x^{t'-t} + \cdots + a_{t'-t+1,t'-1}x^{t'-1}, \end{aligned}$$

such that the following conditions are satisfied:

(1*) for $i \in [t'-t+1]$, $a_{i,i-1} = a_{i+1,i-1} = a_{i+2,i-1} = \cdots = a_{t'-t+1,i-1}$, that is, for $i \in [t'-t+1]$, $f_i(x) = f_{i-1}(x) + x^{i-1}g_{i-1}(x)$, where $g_{i-1}(x) \in \mathbb{F}_q[x]$ is of degree less than t;
(2*) the secret $s = (a_{t'-t+1,0}, a_{t'-t+1,1}, \ldots, a_{t'-t+1,t'-t})$.

For $i \in [n]$, player P_i gets the share $s_i = (f_1(x_i), f_2(x_i), \ldots, f_{t'-t+1}(x_i)) \in \mathbb{F}_q^{t'-t+1}$ and the share updating function is defined by

$$\begin{array}{rccc} h_i : & \mathbb{F}_q^{t'-t+1} & \longrightarrow & \mathbb{F}_q \\ & (s_{i,1}, s_{i,2}, \ldots, s_{i,t'-t+1}) & \longmapsto & s_{i,t'-t+1}. \end{array}$$

Proposition 3.1. *Scheme P-TCSS is an optimal perfect $(t \to t', n)$ threshold changeable scheme.*

Proof. It is evident that the scheme meets the bounds in Theorem 2.1 with equality. We are left to verify the perfectness and security required.

Recoverability: We show that for all $A \subseteq P$ and $|A| = t$, $H(S|S_A) = 0$. Indeed, for any set of t players $A = \{P_{i_1}, \ldots, P_{i_t}\}$, we have $S_A = \{(f_1(x_{i_j}), f_2(x_{i_j}), \ldots, f_{t'-t+1}(x_{i_j})) \mid j \in [t]\}$. The players in A can determine f_1 by polynomial interpolation from the shares $f_1(x_{i_1}), \ldots, f_1(x_{i_t})$, since f_1 has degree less than t. Now let $i \in [2, t'-t+1]$ and suppose that $f_1, \ldots, f_{i-1}$ have been determined. Since $g_{i-1}(x) = (f_i(x) - f_{i-1}(x))/x^{i-1}$ is a polynomial of degree less than t, we can determine g_{i-1} from $f_{i-1}(x_{i_1}), \ldots, f_{i-1}(x_{i_t})$ and $f_i(x_{i_1}), \ldots, f_i(x_{i_t})$ (which are known to A) by polynomial

interpolation. From g_{i-1}, we can in turn determine f_i (since f_{i-1} has already been determined). By induction, we can determine $f_{t'-t+1}$, and hence recover the secret as the coefficients of $f_{t'-t+1}$.

Perfectness: We show that for all $A \subseteq P$ and $|A| < t$, $H(S|S_A) = H(S)$. Equivalently, we require that for all $s, s' \in S$ and $view_A \in S_A$, $\Pr[\Pi(s,R)|_A = view_A] = \Pr[\Pi(s',R)|_A = view_A]$. Without loss of generality, suppose $A = \{P_1, \ldots, P_{t-1}\}$ and the secret is $s = (a_{t'-t+1,0}, a_{t'-t+1,1}, \ldots, a_{t'-t+1,t'-t}) \in \mathbb{F}_q^{t'-t+1}$, which we distribute through the polynomials $f_1, \ldots, f_{t'-t+1}$. We show that for any other $s' = (b_0, b_1, \ldots, b_{t'-t}) \in \mathbb{F}_q^{t'-t+1}$, there exist unique polynomials $f'_1, \ldots, f'_{t'-t+1}$ of degrees less than $t, t+1, \ldots, t'$ in order, satisfying the conditions (1*)–(2*)[1] and $f'_i(x_j) = f_i(x_j)$ for $i \in [t'-t+1]$ and $j \in [t-1]$. Indeed, let

$$\begin{aligned}
f'_1(x) &= f_1(x) + (x-x_1)(x-x_2)\cdots(x-x_{t-1})\cdot r_1(x),\\
f'_2(x) &= f_2(x) + (x-x_1)(x-x_2)\cdots(x-x_{t-1})\cdot r_2(x),\\
&\vdots\\
f'_{t'-t+1}(x) &= f_{t'-t+1}(x) + (x-x_1)(x-x_2)\cdots(x-x_{t-1})\cdot r_{t'-t+1}(x),
\end{aligned}$$

where r_i is of degree at most $i-1$ for $i \in [t'-t+1]$, and where $f'_1, \ldots, f'_{t'-t+1}$ take the forms

$$\begin{aligned}
f'_1(x) &= b_0 + x(\cdots),\\
f'_2(x) &= b_0 + b_1 x + x^2(\cdots),\\
&\vdots\\
f'_{t'-t+1}(x) &= b_0 + b_1 x + \cdots + b_{t'-t}x^{t'-t} + x^{t'-t+1}(\cdots).
\end{aligned}$$

Then, for $i \in [t'-t+1]$, r_i can be determined by Algorithm 1 below.

Algorithm 1: Determining r_i

Input: $f_i, x_1, \ldots, x_{t-1}, b_0, b_1, \ldots, b_{i-1}$
Output: $r_i(x)$
$r_i(x) = 0$;
for $j = 0$ *to* $i-1$ **do**
  $f'_i(x) = f_i(x) + (x-x_1)\cdots(x-x_{t-1})r_i(x)$;
  $c = [x^j]f'_i(x)$;
  $r_i(x) = r_i(x) + \dfrac{(-1)^{t-1}(b_j - c)}{\prod_{l=1}^{t-1} x_l}x^j$;
end

It can be verified that distributing the secret s' through the polynomials $f'_1, \ldots, f'_{t'-t+1}$ constructed above results in the players $P_1, \ldots, P_{t-1}$ receiving the same shares as they do in distributing s through $f_1, \ldots, f_{t'-t+1}$. Moreover, there is a one-to-one correspondence between polynomials $f_1, \ldots, f_{t'-t+1}$ and polynomials $f'_1, \ldots, f'_{t'-t+1}$. This implies that $\Pr[\Pi(s,R)|_A = view_A] = \Pr[\Pi(s',R)|_A = view_A]$. Hence $H(S|S_A) = H(S)$.

Threshold Changeability: We show that for all $A \subseteq P$ and $|A| = t'$, $H(S|T_A) = 0$. Any t' players, say $P_1, \ldots, P_{t'}$, can determine the polynomial $f_{t'-t+1}$ from their updated shares $f_{t'-t+1}(x_1), \ldots, f_{t'-t+1}(x_{t'})$, since $f_{t'-t+1}$ is of degree less than t'. Therefore they can recover the secret. □

3.2. Comparisons and security problems

Wang and Wong [19] studied the communication complexity of secret reconstruction in secret sharing schemes, showing that there exists trade-offs between the communication complexity and the number of players involved in the secret reconstruction. That is, by increasing the number of players to contribute their partial shares, the total communication costs can be reduced, they also proposed a scheme that achieves the optimal communication complexity. It is not hard to see that their scheme can be easily modified into a threshold changeable scheme. However, our construction Scheme P-TCSS differs from Wang and Wong's scheme in the positions where the secret is hidden and the ways the polynomials $f_1, f_2, \ldots, f_{t'-t+1}$ relate to each other. Specifically, they chose $t'-t+1$ distinct elements $e_1, \ldots, e_{t'-t+1} \in \mathbb{F}_q$ such that $f_i(e_j) = f_{i+1}(e_j)$ for $i \in [t'-t]$ and $j \in [i]$, and let $(f_{t'-t+1}(e_1), f_{t'-t+1}(e_2), \ldots, f_{t'-t+1}(e_{t'-t+1}))$ be the secret. Since $n + (t'-t+1)$ distinct

[1] Since polynomials $f'_1(x), \ldots, f'_{t'-t+1}(x)$ are used to distribute $s' = (b_0, b_1, \ldots, b_{t'-t})$, conditions (1*)–(2*) should be adjusted accordingly: for example, (2*) should read $f_{t'-t+1}(x) = b_0 + b_1 x + \cdots + b_{t'-t}x^{t'-t} + \cdots + a'_{t'-t+1,t'-1}x^{t'-1}$.

elements (namely, $x_1, \ldots, x_n, e_1, \ldots, e_{t'-t+1}$) in $\mathbb{F}_q$ are needed, the condition $q \geq n + (t' - t + 1)$ is required to hold. Our scheme relaxes the requirement to $q > n$, a more natural condition as in Shamir's threshold scheme. It is not clear whether our polynomial construction and the geometric construction of Martin et al. [15] are interconvertible in an obvious way for the general setting. This is an interesting problem that merits further study.

We also point out that all the $(t \to t', n)$ threshold changeable schemes proposed so far suffer some security problems. First, for all $A \subseteq P$ and $t \leq |A| < t'$, Definition 2.1 states $H(S|T_A) \leq H(S)$, which means that any less than t' players may get some partial information about the secret from their updated shares. Thus, even if players honestly update their shares and delete initial ones, it is still not a perfect (t', n) threshold scheme. Second, some semi-honest players may retain their initial shares, and the adversary may not only tap the channel between the players and the *combiner*[2], but also corrupt some players directly to obtain the entire history of their shares. Hence by using the initial shares, the scheme constructed above, as well as many previously known threshold changeable schemes [6,8,15,16,18], cannot prevent t players from recovering the secret, even though the threshold has been changed to $t' > t$. We attempt to provide some solutions to these problems for the rest of the paper.

4. The model of threshold changeable secret sharing

In [14], Martin gave a detailed classification of the models of secret sharing schemes that deal with dynamic access policies. He classified the models according to the communication channels, advance information about changes, robustness and some other issues. Based on the security problems of threshold changeable secret sharing schemes we pointed out in the last section, we are interested in the model in the two phases of *Share Distribution* and *Secret Recovery*.

Share Distribution: Dealer is present and secure channels exist between Dealer and each player.
To share a secret $s \in S$ among the players, Dealer selects a random string $r \in R$, computes the distribution function $\Pi(s, r) = (s_1, \ldots, s_n)$, and then privately sends each share s_i to P_i.

Secret Recovery: Dealer is present and only broadcast channels are available.
A group of players request to recover the secret. Then it is followed by the two steps below:

- Dealer Broadcast: After confirming the recovery request, Dealer checks the updated security requirement and broadcasts a message (t_j, b_j), where t_j is the updated threshold and b_j is the message that validates the threshold t_j.
- Secret Reconstruction: Any t_j players get together and broadcast their updated shares according to the threshold t_j. Then the t_j updated shares along with Dealer's broadcast message b_j can uniquely determine the secret s.

We further clarify some related issues as follows:

Advance information about changes. For simplicity, we assume the advance knowledge of possible threshold changes. In particular, there are N allowable thresholds denoted by $t_1, \ldots, t_N$. Without loss of generality, assume that $1 < t_1 < \cdots < t_N \leq n$, where the trivial threshold $t = 1$ is not considered. All these N thresholds are invalid before Dealer makes the broadcast at the secret recovery phase, and only the threshold chosen by Dealer is valid after the broadcast. Although our model assumes such specific information about changes in advance, we have no limitations on N. When $N = n - 1$, then every nontrivial threshold is allowable and the model is quite flexible.

Collusion Security Against Passive Adversaries. Our model deals with the adversary who may passively corrupt a group of players under some threshold. As pointed out in Section 3.2, many threshold changeable schemes [6,8,15,16,18] suffer from the collusion attack of players holding initial shares. To fix this problem, we introduce the broadcast enforcement term. That is, before Dealer broadcasts at the recovery phase, any collusion of players cannot reconstruct the secret; after Dealer broadcasts the message (t_j, b_j), any collusion of less than t_j players still cannot recover the secret, even they see the message b_j and retain their initial shares. This is a strict security requirement dealing with dynamic access policies in secret sharing schemes, and was already studied in the dynamic secret sharing scheme [4] and the threshold scheme with disenrollment [11]. To resist active adversaries in the threshold changeable schemes, one may apply some techniques in "verifiable secret sharing" (VSS) [7], which is however beyond the scope of this paper.

One-Fold Changes. Only one-fold change of threshold is considered in our model. Because once the recovery is activated by Dealer broadcasting the message (t_j, b_j), the secret can be recovered by any group of t_j players with the broadcast message b_j. If, once again, the threshold is to change to $t_k > t_j$, the secret has to be updated. This update of secret is inevitable when dealing with changes of access policies under strict security requirements. For example, the threshold scheme with L-fold disenrollment of players [2,14] needs to update the secret at each disenrollment of a player.

For simplicity, we call a secret sharing scheme under this model a $([t_1, \ldots, t_N], n)$ *threshold changeable scheme*. Specifically, the model in this section only allows one-fold threshold change among N options, while the $(t \to t', n)$ threshold changeable scheme defined in Definition 2.1 allows a threshold change from t to t' (both thresholds t and t' are valid, but security under the second threshold t' is discounted as described in Section 3.2). Certainly, it is desirable

[2] Some secret sharing models assume that the secret is constructed by having players send their shares through secure channels to a *combiner*, who then computes the secret (and possibly returning the result to the players).

to consider schemes which allow L-fold changes. We leave this issue to Section 6 and display two simple $([t_1, \ldots, t_N], n)$ threshold changeable schemes in this section. The first scheme is derived form the advance share technique [15], and the second is from [13,4]. These two schemes are helpful in understanding our construction in the next section and serve as benchmarks for comparisons.

Scheme 1 ([15]): To share a secret $s \in \mathbb{F}_q$ with $q > n$, Dealer independently and uniformly selects $r_1, \ldots, r_N \in \mathbb{F}_q$, and for each $i \in [N]$, implements Shamir's (t_i, n) threshold scheme with secret $s + r_i$. More precisely, Dealer independently selects N random polynomials $f_1, \ldots, f_N \in \mathbb{F}_q[x]$ such that the degree of f_i is less than t_i and $f_i(0) = s + r_i$. Let $x_1, \ldots, x_n$ be n distinct nonzero elements of $\mathbb{F}_q$. Player P_i receives the share $(f_1(x_i), f_2(x_i), \ldots, f_N(x_i))$. In the Dealer broadcast phase, r_j is broadcasted to validate the threshold $t_j, j \in [N]$.

Scheme 2 ([13,4]): To share a secret $s \in \mathbb{F}_q$ with $q > 2n$, Dealer randomly selects a polynomial $f \in \mathbb{F}_q[x]$ of degree less than $n + 1$ such that $f(0) = s$. Let $x_1, \ldots, x_n, y_1, \ldots, y_n$ be $2n$ distinct nonzero elements of $\mathbb{F}_q$. Player P_i receives the share $f(x_i)$. In the Dealer broadcast phase, the message $(f(y_{t_j}), f(y_{t_j+1}), \ldots, f(y_n))$ is broadcasted to validate the threshold $t_j, j \in [N]$.

5. Computationally secure threshold changeable schemes

In our model of $([t_1, \ldots, t_N], n)$ threshold changeable scheme, Scheme 1 and Scheme 2 given in the previous section have perfect security. But the sizes of both the share and the broadcast message are many times the size of the secret. In [10] Krawczyk constructed a secret sharing scheme with computational security. He designed the scheme by encrypting the secret with a secure encryption function and then sharing the decryption key through a perfect threshold scheme. For the scheme in [10] each player holds a share of size $\frac{H(S)}{t} + |K|$, where $H(S)$ is the length of the secret and $|K|$ denotes the length of the key. Since $|K|$ usually does not grow with the secret size $H(S)$ but relates to the security parameter only, it can result in a much smaller share compared to a perfect scheme.

In this section, we combine Krawczyk's method and the threshold changeable scheme designed in Section 3.1 to construct a computationally secure $([t_1, \ldots, t_N], n)$ threshold changeable scheme.

5.1. Definitions

First we introduce some definitions related to computational security.

Definition 5.1 (*Computational Indistinguishability [9]*)**.** Let $X = \{X_n\}_{n \in \mathbb{Z}_{\geq 0}}$ and $Y = \{Y_n\}_{n \in \mathbb{Z}_{\geq 0}}$ be two probability ensembles such that each X_n and Y_n is a distribution that ranges over strings of length n. We say that X and Y are *computationally indistinguishable* if for every probabilistic polynomial-time algorithm Dist,

$$|\Pr[\mathsf{Dist}(X_n) = 1] - \Pr[\mathsf{Dist}(Y_n) = 1]| < \mu(k),$$

for some negligible function $\mu(k)$, where the probabilities are taken over the relevant distribution (X_n or Y_n) and over internal coin tosses of algorithm Dist.

Definition 5.2 (*Computational Secret Sharing [10]*)**.** A (t, n) threshold scheme $\Pi : S \times R \to S_1 \times \cdots \times S_n$ is called *computationally secure* if

(1) For all $A \subseteq P$ and $|A| \geq t$, there exists a probabilistic polynomial-time reconstruction algorithm Recon_A such that for all $s \in S$,

$$\Pr[\mathsf{Recon}_A(\Pi(s, R)|_A, 1^k) = s] > 1 - \mu(k),$$

for some negligible function μ.

(2) For all $A \subseteq P$ with $|A| < t$ and for all $s, s' \in S$, the probability ensembles $\{\Pi(s, R)|_A\}_{|r|:r \in R}$ and $\{\Pi(s', R)|_A\}_{|r|:r \in R}$ are computationally indistinguishable.

Definition 5.3 (*Encryption Scheme [9]*)**.** An *encryption scheme* is a triple $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ of three probabilistic polynomial-time algorithms satisfying the conditions:

(1) On input 1^k, algorithm Gen (called the *key generator*) outputs a pair of bit strings, corresponding to the encryption/decryption keys.

(2) For every pair (e, d) in the range of $\mathsf{Gen}(1^k)$, and for every $\alpha \in \{0, 1\}^*$, the algorithms Enc and Dec satisfy

$$\Pr[\mathsf{Dec}(d, \mathsf{Enc}(e, \alpha)) = \alpha] = 1,$$

where the probability is taken over the internal coin tosses of algorithms Enc and Dec.

For simplicity, when the encryption key and the decryption key are always the same (i.e. $e = d$), the scheme $\mathcal{E}$ is called a *symmetric* (or *private key*) encryption scheme.

Definition 5.4 (*Semantic Security [9]*)**.** Let $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a symmetric encryption scheme. Then $\mathcal{E}$ is *semantically secure* if for all plaintexts $m, m' \in \{0,1\}^{poly(k)}$, the probability ensembles of ciphertexts, $\{\mathsf{Enc}(\mathsf{Gen}(1^k), m)\}_{k\in\mathbb{Z}_{\geq 0}}$ and $\{\mathsf{Enc}(\mathsf{Gen}(1^k), m')\}_{k\in\mathbb{Z}_{\geq 0}}$, are computationally indistinguishable.

Now we define the computational $([t_1, \ldots, t_N], n)$ threshold changeable secret sharing scheme as follows.

Definition 5.5 (*Computational Threshold Changeable Scheme*)**.** A computationally secure $([t_1, \ldots, t_N], n)$ threshold changeable scheme over P consists of a secret sharing scheme $\Pi : S \times R \to S_1 \times \cdots \times S_n$, a broadcast message generator $\{\mathfrak{B}_i : S \times R \to B_i \mid i \in [N]\}$ and a set of reconstructions functions $\{\mathsf{Recon}_A^{(i)} : (S_1 \times \cdots \times S_n)|_A \times B_i \to S \mid i \in [N], A \subseteq P, |A| \geq t_i\}$, such that the following three conditions are satisfied:

(1) For all $s, s' \in S$, the probability ensembles, $\{\Pi(s,R)\}_{|r|:r\in R}$ and $\{\Pi(s',R)\}_{|r|:r\in R}$, are computationally indistinguishable.
(2) For each $i \in [N]$ and for all $A \subseteq P$ with $|A| \geq t_i$, $\mathsf{Recon}_A^{(i)}$ is polynomial-time computable, and that for all $s \in S$,

$$\Pr[\mathsf{Recon}_A^{(i)}(\Pi(s,R)|_A, \mathfrak{B}_i(s,R), 1^k) = s] > 1 - \mu(k),$$

for some negligible function μ.
(3) For each $i \in [N]$ and for all $A \subseteq P$ with $|A| < t_i$, the probability ensembles, $\{(\Pi(s,R)|_A, \mathfrak{B}_i(s,R))\}_{|r|:r\in R}$ and $\{(\Pi(s',R)|_A, \mathfrak{B}_i(s',R))\}_{|r|:r\in R}$, where $s, s' \in S$, are computationally indistinguishable.

5.2. Our construction: Scheme C-TCSS

Let $S = \mathbb{F}_q^{t_N - 1}$ be the secret-domain, where $q > n$. We make the following assumptions in our construction of a computationally secure $([t_1, \ldots, t_N], n)$ threshold changeable scheme:

(a) $\max_{i\in[N]}\{t_i - t_{i-1}\} < t_1$.
(b) There exists a semantically secure symmetric encryption scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with key space $\mathcal{K}$. Without loss of generality, we assume that $\mathcal{K} = \mathbb{F}_q$.

Assumption (a) can be easily achieved by adding new allowable thresholds to shorten the difference between two allowable thresholds, while assumption (b) is substantial to our scheme.

Our construction Scheme C-TCSS is as follows.

Share Distribution: To share a secret $s = (s_1, \ldots, s_{t_N-1}) \in \mathbb{F}_q^{t_N-1}$, Dealer performs the following steps:

(D1) Secretly select a key $K \in \mathcal{K}$ for the symmetric encryption scheme $\mathcal{E}$.
(D2) Compute $(c_0, c_1, \ldots, c_{t_N-1}) = (K, \mathsf{Enc}(K, s_1), \ldots, \mathsf{Enc}(K, s_{t_N-1}))$.
(D3) Construct the polynomials

$$\begin{aligned} f_N(x) &= c_0 + c_1 x + \cdots + c_{t_N-1} x^{t_N-1}, \\ f_{N-1}(x) &= f_N(x) - x^{t_N - t_1} g_{N-1}(x), \\ &\vdots \\ f_1(x) &= f_2(x) - x^{t_2 - t_1} g_1(x), \end{aligned}$$

where g_i is a random polynomial of degree less than t_1 and $f_i(x) = f_{i+1}(x) - x^{t_{i+1}-t_1} g_i(x)$ is of degree at most $t_i - 1$, $i \in [N-1]$. The random polynomial g_i is generated by Algorithm 2 below.

Algorithm 2: Determining g_i

Input: t_i, t_{i+1}, f_{i+1}
Output: $g_i(x)$
$g_i(x) = 0$;
$d = \deg(f_{i+1}(x) - x^{t_{i+1}-t_1} g_i(x))$;
while $d \geq t_i$ **do**
  $c = [x^d] f_{i+1}(x)$;
  $g_i(x) = g_i(x) + c x^{d-(t_{i+1}-t_1)}$;
  $d = \deg(f_{i+1}(x) - x^{t_{i+1}-t_1} g_i(x))$;
end
$r(x) =$ random polynomial of degree at most $t_1 - (t_{i+1} - t_i) - 1$;
$g_i(x) = g_i(x) + r(x)$;

(D4) Independently and randomly select keys $K_1, \ldots, K_N \in \mathcal{K}$.
(D5) Let $x_1, \ldots, x_n$ be n distinct nonzero elements of $\mathbb{F}_q$ which are made public. For $i \in [n]$, P_i receives the share $(\mathsf{Enc}(K_1, f_1(x_i)), \mathsf{Enc}(K_2, f_2(x_i)), \ldots, \mathsf{Enc}(K_N, f_N(x_i)))$.

Dealer Broadcast: To activate an allowable threshold t_j ($j \in [N]$), Dealer broadcasts to the players the message $(K_j, K_{j+1}, \ldots, K_N)$.

The process of share distribution and Dealer broadcast is illustrated in the diagram below.

P_1	P_2	$\cdots$	P_n	Broadcast message
$\mathsf{Enc}(K_1, f_1(x_1))$	$\mathsf{Enc}(K_1, f_1(x_2))$	$\cdots$	$\mathsf{Enc}(K_1, f_1(x_n))$	K_1
$\mathsf{Enc}(K_2, f_2(x_1))$	$\mathsf{Enc}(K_2, f_2(x_2))$	$\cdots$	$\mathsf{Enc}(K_2, f_2(x_n))$	K_2
$\vdots$	$\vdots$		$\vdots$	$\vdots$
$\mathsf{Enc}(K_N, f_N(x_1))$	$\mathsf{Enc}(K_N, f_N(x_2))$	$\cdots$	$\mathsf{Enc}(K_N, f_N(x_n))$	K_N

Secret Reconstruction: After receiving the broadcast message $(K_j, K_{j+1}, \ldots, K_N)$, any set of t_j players, say $A = \{P_1, \ldots, P_{t_j}\}$, can recover the secret by performing the following steps:

(R1) For each $i \in [t_j]$, P_i uses K_ℓ (which can be found in the broadcast message) to decrypt the ℓ-th coordinate of his share to obtain $f_\ell(x_i)$, for each $\ell \in [j, N]$. P_i then makes $(f_j(x_i), f_{j+1}(x_i), \ldots, f_N(x_i))$ known to all other players in A.

(R2) The players in A can determine f_j by polynomial interpolation on $f_j(x_1), \ldots, f_j(x_{t_j})$, since f_j is of degree at most $t_j - 1$. Now let $i \in [j+1, N]$ and suppose that $f_j, \ldots, f_{i-1}$ have been determined. Since $g_{i-1}(x) = (f_i(x) - f_{i-1}(x))/x^{t_i - t_1}$ is of degree less than t_1 (and hence less than t_j), we can determine g_{i-1} by polynomial interpolation on $f_{i-1}(x_1), \ldots, f_{i-1}(x_{t_j})$ and $f_i(x_1), \ldots, f_i(x_{t_j})$. From g_{i-1}, we can in turn determine f_i (since f_{i-1} has already been determined). By induction, f_N can be determined.

(R3) Let $c_i = [x^i]f_N(x)$, $i \in [0, t_N - 1]$. The secret $(s_1, \ldots, s_{t_N - 1})$ can be recovered by decrypting each c_i, $i \in [t_N - 1]$, under the key c_0: $s_i = \mathsf{Dec}(c_0, c_i)$.

5.3. Security and efficiency

We now establish the security and efficiency of Scheme C-TCSS.

Theorem 5.1. *If $\mathcal{E}$ is a semantically secure symmetric encryption scheme, then Scheme C-TCSS is a computationally secure $([t_1, \ldots, t_N], n)$ threshold changeable scheme.*

Proof. It is easy to verify that the broadcast message enables any t_j or more players to recover the secret in polynomial time by performing steps (R1)–(R3). Hence, condition (2) in Definition 5.5 is satisfied. It remains to show that conditions (1) and (3) in Definition 5.5 are also satisfied.

First, without seeing the broadcast message, all players have absolutely no information on the keys $K_1, \ldots, K_N$, except for some public knowledge known before the scheme. So the semantic security of $\mathcal{E}$ implies the computational security of the secret. More precisely, for distinct $s = (s_1, \ldots, s_{t_N - 1})$, $s' = (s'_1, \ldots, s'_{t_N - 1}) \in S$, let $(c_0, \ldots, c_{t_N - 1})$ and $(c'_0, \ldots, c'_{t_N - 1})$ be the vectors computed in step (D2) of the share distribution phase for s and s', respectively. We have the following:

- If s and s' are encrypted under the same key K, that is, $c_i = \mathsf{Enc}(K, s_i)$ and $c'_i = \mathsf{Enc}(K, s'_i)$, $i \in [t_N - 1]$, then by the rationality of $\mathcal{E}$, different plaintexts cannot give rise to the same ciphertext. Thus, $c_i \neq c'_i$, for some $i \in [t_N - 1]$.
- If s and s' are encrypted under different keys K and K', then $c_0 \neq c'_0$ by construction.

In either case, $f_N \neq f'_N$, where $f_N(x) = \sum_{i=0}^{t_N - 1} c_i x^i$ and $f'_N(x) = \sum_{i=0}^{t_N - 1} c'_i x^i$. Since f_N and f'_N are of degree at most $n - 1$, $f_N(x_j) \neq f'_N(x_j)$ for some $j \in [n]$. Therefore, ability to distinguish between $\{\Pi(s, R)\}_{|r|:r \in R}$ and $\{\Pi(s', R)\}_{|r|:r \in R}$ implies ability to distinguish between $\{\mathsf{Enc}(K_N, f_N(x_j))\}_{K_N \in \mathcal{K}}$ and $\{\mathsf{Enc}(K_N, f'_N(x_j))\}_{K_N \in \mathcal{K}}$. However, the semantic security of $\mathcal{E}$ implies that $\{\mathsf{Enc}(K_N, f_N(x_j))\}_{K_N \in \mathcal{K}}$ and $\{\mathsf{Enc}(K_N, f'_N(x_j))\}_{K_N \in \mathcal{K}}$ are computationally indistinguishable. It follows that $\{\Pi(s, R)\}_{|r|:r \in R}$ and $\{\Pi(s', R)\}_{|r|:r \in R}$ are also computationally indistinguishable. Condition (2) of Definition 5.5 is therefore satisfied.

After seeing the broadcast message $(K_j, K_{j+1}, \ldots, K_N)$, any $t_j - 1$ players, say $P_1, \ldots, P_{t_j - 1}$, has knowledge of

$$\left(\bigcup_{i \in [j-1]} \bigcup_{k \in [t_j - 1]} \{\mathsf{Enc}(K_i, f_i(x_k))\} \right) \bigcup \left(\bigcup_{i \in [j, N]} \bigcup_{k \in [t_j - 1]} \{f_i(x_k)\} \right). \tag{1}$$

We show that no information of the key K is leaked. Indeed, for $K' \in \mathbb{F}_q$, let

$$f'_j(x) = f_j(x) + \frac{(-1)^{t_j - 1}(K' - K)}{\prod_{i=1}^{t_j - 1} x_i} \prod_{i=1}^{t_j - 1} (x - x_i),$$

and

$$f'_i(x) = f'_{i-1}(x) + x^{t_i - t_1} g_{i-1}(x),$$

for $i \in [j+1, N]$. Under these polynomials, $f'_j, \ldots, f'_{t_N - 1}$, and the broadcast message $K_j, K_{j+1}, \ldots, K_N$, P_i obtains $f'_i(x_k) = f_i(x_k)$ for $i \in [j, t_N]$ and $k \in [t_j - 1]$. Since the keys $K_1, \ldots, K_{j-1}$ are unknown, $\bigcup_{i \in [j-1]} \bigcup_{k \in [t_j - 1]} \{\mathsf{Enc}(K_i, f_i(x_k))\}$ induces nothing new about the key K. Thus, even with the information provided by (1), the secret key K is computationally indistinguishable from any $K' \in \mathbb{F}_q$. Therefore the secret is computationally secure against any $t_j - 1$ players. □

The efficiency of a secret sharing scheme can be measured by the size of the shares and the broadcast messages. The following table displays a comparison between Scheme C-TCSS and the two schemes in Section 4.

	Share size	Broadcast message size	Security
Scheme 1	$N \cdot H(S)$	$H(S)$	Perfect
Scheme 2	$H(S)$	$(n - t_j + 1)H(S)$	Perfect
Scheme C-TCSS	$\frac{N}{t_N - 1}H(S)$	$\frac{N-j+1}{t_N-1}H(S)$	Computational

In practice, N is usually a small integer (such as $N = 3$) corresponding to the "low, middle, high" level of security in computers, while t_N could be linearly related to n. Even if t_N is a small constant, we always have $t_i > i$ for $i \in [N]$. Therefore, by relaxing the security requirement from information-theoretic to computational, the efficiency is significantly improved.

6. Disenrollment and L-fold changes

In previous sections we discuss changes of the threshold in a (t, n) threshold secret sharing scheme. In practice the number n may also change, corresponding to the enrollment or disenrollment of players. Dealing with the enrollment of players is straightforward by using secure channels between Dealer and the newcomers or secure channels between original players and the newcomers. As to the disenrollment of the players, since it is closely related to the problem of threshold change, in the below we give a simple implementation of disenrollment based on our model of $([t_1, \ldots, t_N], n)$ threshold changeable scheme. Thus it simultaneously allows threshold changes and multiple disenrollment of players.

For simplicity, suppose at most t players may quit the scheme after the share distribution phase and $\{t_1, \ldots, t_N\}$ is the set of allowable thresholds. It is reasonable to assume that the allowable threshold t_N is still meaningful when t players quit. Hence, $t_N \leq n - t$. For $i \in [N]$ and $j \in [0, t]$, let $t_{ij} = t_i + j$. By regarding $\{t_{ij} \mid i \in [N], j \in [0, t]\}$ as the new set of allowable thresholds, we construct a threshold changeable scheme like Scheme C-TCSS. For secret recovery after the threshold has been chosen as t_i ($i \in [N]$), and j ($j \in [0, t]$) players quit the scheme, Dealer publishes the shares of the j players who have quited and broadcasts the message related to the threshold t_{ij}. It is easy to verify that the scheme constructed in this way is a $([t_1, \ldots, t_N], n)$ threshold changeable scheme that can tolerate the disenrollment of up to t players.

As pointed out in Section 4, the above scheme just involves one-fold change of the threshold and disenrollment of players, while previous threshold schemes [2,5,11] mostly considered L-fold disenrollment of players. To deal with L-fold changes of the threshold and disenrollment of players, we suggest to use the advance key technique with computational security. Precisely, at the initial phase Dealer distributes to each player a secret key. Then Scheme C-TCSS enhanced with disenrollment is implemented. Once another change is required, Dealer computes the new shares according to the updated secret and access policies, and encrypts P_i's share with the secret key k_i that has been secretly distributed to P_i at the initial phase. Then at the recovery phase Dealer broadcasts the encrypted shares needed to validate the changed access policies, along with the corresponding broadcast message.

Therefore, our scheme, apart from the additional capability for simultaneously dealing with L-fold changes of threshold and disenrollment of players, has the collusion security as the broadcast enforced threshold scheme in [11], and the appealing efficiency as the computational scheme in [5] which is more efficient than the perfect schemes [2].

Acknowledgements

The authors are indebted to the anonymous referee for the valuable comments on the original version of this paper.

The first author's research was supported in part by the National Natural Science Foundation of China (Grant Nos. 60821002/F02, 11001254), 973 Project (No. 2011CB302401) and the Foundation of President of AMSS, CAS. The second, third and fifth author's research was supported in part by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03. The second author's research was also supported in part by the Nanyang Technological University under Research Grant M58110040. The fifth author's research was also supported in part by the Australian Research Council under ARC Discovery Project DP0665035.

References

[1] S.G. Barwick, W.-A. Jackson, K.M. Martin, Updating the parameters of a threshold scheme by minimal broadcast, IEEE Trans. Inform. Theory 51 (2) (2005) 620–633.
[2] B. Blakley, G.R. Blakley, A.H. Chan, J.L. Massey, Threshold schemes with disenrollment, in: Advances in Cryptology – CRYPTO '92 (Santa Barbara, CA, 1992), in: Lecture Notes in Computer Science, vol. 740, Springer, Berlin, 1993, pp. 540–548.
[3] G.R. Blakley, Safeguarding cryptographic keys, in: Proceedings of the National Computer Conference, American Federation of Information Processing Societies, 1979, pp. 313–317.
[4] C. Blundo, A. Cresti, A. De Santis, U. Vaccaro, Fully dynamic secret sharing schemes, Theor. Comput. Sci. 165 (2) (1996) 407–440.
[5] C. Charnes, J. Pieprzyk, R. Safavi-Naini, Conditionally secure secret sharing schemes with disenrollment capability, in: CCS'94: Proceedings of the 2nd ACM Conference on Computer and Communications Security, ACM, New York, NY, USA, 1994, pp. 89–95.
[6] L. Chen, D. Gollmann, C.J. Mitchell, Key escrow in mutually mistrusting domains, in: Proceedings of the International Workshop on Security Protocols, in: Lecture Notes in Computer Science, vol. 1189, Springer-Verlag, London, UK, 1997, pp. 139–153.

[7] B. Chor, S. Goldwasser, S. Micali, B. Awerbuch, Verifiable secret sharing and achieving simultaneity in the presence of faults, in: FOCS'85: Proceedings of the 26th Annual Symposium on Foundations of Computer Science, IEEE Computer Society, Washington, DC, USA, 1985, pp. 383–395.
[8] Y. Desmedt, S. Jajodia, Redistributing secret shares to new access structures and its applications, Tech. Rep. ISSE-TR-97-01, George Mason University, Fairfax, Virginia, 1997.
[9] O. Goldreich, Foundations of Cryptography II: Basic Applications, Cambridge University Press, 2004.
[10] H. Krawczyk, Secret sharing made short, in: Advances in Cryptology – CRYPTO'93: Proceedings of the 13th Annual International Cryptology Conference, in: Lecture Notes in Computer Science, vol. 773, Springer, 1993, pp. 136–146.
[11] M. Li, R. Poovendran, Broadcast-enforced disnrollment in threshold schemes, SAC 2003, Lecture Notes in Comput. Sci., vol. 3006, pp. 101–116.
[12] A. Maeda, A. Miyaji, M. Tada, Efficient and unconditionally secure verifiable threshold changeable scheme, in: ACISP 2001: Proceedings of the 6th Australasian Conference on Information Security and Privacy, in: Lecture Notes in Computer Science, vol. 2119, Springer, 2001, pp. 403–416.
[13] K.M. Martin, Untrustworthy participants in secret sharing schemes, in: M.J. Ganley (Ed.), Cryptography and Coding III, Oxford University Press, 1993, pp. 255–264.
[14] K.M. Martin, Dynamic access policies for unconditionally secure secret sharing schemes, in: Proceedings of IEEE Information Theory Workshop, ITW 05, Awaji Island, Japan, 2005, pp. 61–66.
[15] K.M. Martin, J. Pieprzyk, R. Safavi-Naini, H. Wang, Changing thresholds in the absence of secure channels, in: ACISP'99: Proceedings of the 4th Australasian Conference on Information Security and Privacy, in: Lecture Notes in Computer Science, vol. 1587, Springer, 1999, pp. 177–191.
[16] K.M. Martin, R. Safavi-Naini, H. Wang, Bounds and techniques for efficient redistribution of secret shares to new access structures, Comput. J. 42 (8) (1999) 638–649.
[17] A. Shamir, How to share a secret, Commun. ACM 22 (11) (1979) 612–613.
[18] R. Steinfeld, J. Pieprzyk, H. Wang, Lattice-based threshold changeability for standard Shamir secret-sharing schemes, IEEE Trans. Inform. Theory 53 (7) (2007) 2542–2559.
[19] H. Wang, D.S. Wong, On secret reconstruction in secret sharing schemes, IEEE Trans. Inform. Theory 54 (1) (2008) 473–480.