Efficient and unconditionally secure verifiable threshold changeable scheme

Ayako Maeda[0], Atsuko Miyaji and Mitsuru Tada

School of Information Science,
Japan Advanced Institute of Science and Technology (JAIST),
Asahidai 1-1, Tatsunokuchi, Nomi, Ishikawa 923-1292, JAPAN.

Abstract. In this paper, we describe how to construct an efficient and unconditionally secure verifiable threshold changeable scheme, in which any participants can verify whether the share given by the dealer is correct or not, in which the combiner can verify whether the pooled shares are correct or not, and in which the threshold can be updated plural times to the values determined in advance. An optimal threshold changeable scheme was defined and given by Martin et. al., and an unconditionally secure verifiable threshold scheme was given by Pedersen. Martin's scheme is based on Blakley's threshold scheme whereas Pedersen's is based on Shamir's. Hence these two schemes cannot directly be combined. Then we first construct an *almost* optimal threshold changeable scheme based on Shamir's, and after that using Pedersen's scheme, construct a unconditionally secure verifiable threshold scheme in which the threshold can be updated plural times, say N times. Furthermore, our method can decrease the amount of information the dealer has to be publish, comparing with simply applying Pedersen's scheme N times.

1 Introduction

In a secret sharing scheme, a *secret* is broken into several pieces so that certain subsets of those pieces can reconstruct the secret. In a protocol, *a dealer* has a secret, and breaks it into several pieces called *shares*. An entity given a share is called *a participant*, *a shareholder* or *a member* simply. In this paper, we adopt the term *participant*. The entity to gather shares and recover the secret, is called *the combiner*. Basically, a secret sharing is regarded as a strategy for some important data protection. On the other hand, it is useful also for multiparty computation, for example, electronic auction, electronic voting, and so on.

As the most popular secret sharing schemes, we can see Shamir's polynomial-based scheme [Sha79] and Blakley's geometry-based scheme [Bla79]. In that scheme, a secret is broken into n pieces so that the secret can reconstruct with any t ($\leq n$) pieces, and not so that any $(t-1)$ pieces can determine the secret. Such a t is called *the threshold* of the scheme. Also we call such secret sharing schemes with the property given above (t, n)*-threshold schemes*.

[0] Current affiliation of the first author: Alpha systems corporation.

There are some threshold schemes in which the threshold can be changed without reconstructing the system [TTO99,MPSW99]. In this paper, we generically call such schemes *threshold changeable schemes*. In [TTO99] and in the first part of [MPSW99], after the initial setting, no secure channels is required, and the schemes before and after the threshold is changed are set to be *perfect*. However the required share size, precise to say the entropy of each share, has to be equal to or greater than the twice of that of the secret. Hence if we construct a scheme in which the threshold can be changed N times, the required share size is equal to or greater than $(N+1)$ times of that of the secret. On the other hand, in the latter part of [MPSW99], an optimal (t, n)-threshold scheme that is threshold changeable to t' $(> t)$ is defined, and a concrete construction is actually given. (As described later, we write as a $(t \to t', n)$-threshold changeable scheme instead of writing as a (t, n)-threshold scheme that is threshold changeable to t'.) In that kind of a threshold changeable scheme, the scheme after the threshold change sacrifices the perfect security, but is an optimal $(t-1, t', n)$-ramp scheme. Furthermore the scheme requires only the share size coinciding with the secret size. Even in changing the threshold N times, this scheme requires the same size share as the secret size.

In Section 3, we define a $(t \to \mathbf{t}, n)$-*threshold changeable scheme*, in which the threshold can be changed $N(\geq 1)$ times, where $\mathbf{t} = (t_1, t_2, \ldots, t_N)$ with $t < t_k$ for $1 \leq k \leq N$. Note that in case $N = 1$, that scheme has already been defined by [MPSW99]. Each t_k is the threshold after the threshold is changed k times. The optimal $(t \to t', n)$-threshold changeable scheme given by [MPSW99] can easily be extended to be a $(t \to \mathbf{t}, n)$-threshold changeable scheme.

In this paper, we discuss to make a $(t \to \mathbf{t}, n)$-threshold changeable scheme verifiable. By the technique by [Ped92], we can make a scheme non-interactive and unconditionally secure. The optimal $(t \to t', n)$-threshold changeable scheme given by [MPSW99] is unfortunately based on [Bla79]. Since Pedersen's scheme [Ped92] is based on Shamir's one [Sha79], it cannot directly be applied to that optimal $(t \to \mathbf{t}, n)$-threshold changeable scheme. Then we first construct, based on [Sha79], an *almost optimal* $(t \to \mathbf{t}, n)$-threshold changeable scheme. After that we contrive to make such a scheme verifiable so that the whole scheme required the dealer to publish much less information including the commitment than we simply construct a $(t \to \mathbf{t}, n)$-threshold changeable scheme by combining a $(t \to t_1, n)$-threshold changeable, a $(t \to t_2)$-threshold changeable scheme, ..., and a $(t \to t_N, n)$-threshold changeable scheme, and apply, to the whole scheme, the technique by [Ped92] $(N+1)$ times for the (t, n)-threshold scheme and for each (t_k, n)-threshold scheme $(1 \leq k \leq N)$.

2 Preliminaries

First of all, we review some definitions on secret sharing schemes after giving our notations. Let s be a secret belonging to a set S. The secret s is broken into

n shares $s_1, \ldots, s_n$. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be the set of participants. We assume that each share s_i is securely distributed to the i-th participant P_i. Let P_i denote also the set of possible shares for the participant P_i. Similarly, we denote, by $\mathcal{A}$, the set of the shares the participants in $\mathcal{A} \subset \mathcal{P}$ hold. We say that a set $\mathcal{A} \subset \mathcal{P}$ of shares can recover the secret s if $H(S|\mathcal{A}) = 0$, where $H(*)$ denotes Shannon's entropy function. Such an $\mathcal{A}$ is called *an access set*. The set consists of all access sets is called *the access structure (of a secret sharing scheme)*.

2.1 Threshold scheme

A secret sharing scheme which has n participants, and whose access structure is of the form $\{\mathcal{A} \subset \mathcal{P} \mid \#\mathcal{A} \geq t\}$ for some $t(\leq n)$, is called *a (t, n)-threshold (secret sharing) scheme*. In a (t, n)-threshold scheme, we, in general, have the following properties: $H(S|\mathcal{A}) = 0$ if $\#\mathcal{A} \geq t$ and $H(S|\mathcal{A}) > 0$ otherwise.

Definition 1. A (t, n)-threshold scheme is said to be *perfect*, if $H(S|\mathcal{A}) = H(S)$ holds for any set $\mathcal{A} \subset \mathcal{P}$ such that $\#\mathcal{A} < t$. A perfect threshold scheme is said to be *ideal*, if $H(P_i) = H(S)$ holds for any i $(1 \leq i \leq n)$.

We can easily see that Shamir's scheme [Sha79] is perfect and ideal. The following theorem states that there exists the lower bound for the share size in a perfect threshold scheme.

Theorem 1 (in [Sti95]). In a perfect (t, n)-threshold scheme, for any i $(1 \leq i \leq n)$, $H(P_i) \geq H(S)$ holds.

2.2 Ramp scheme

As we can see in Theorem 1, in a perfect threshold scheme, there exists the lower bound for the share size. That means if $H(P_i) < H(S)$ holds for some i, then the threshold scheme cannot be perfect. As a compromise between security and efficiency, *a ramp scheme* is introduced in [MPSW99].

Definition 2. A (t, n)-threshold scheme is said to be *a (c, t, n)-ramp scheme* if it satisfies the following properties:

$$\begin{cases} H(S|\mathcal{A}) = 0, & \text{if } \#\mathcal{A} \geq t\ ; \\ 0 < H(S|\mathcal{A}) < H(S), & \text{if } c < \#\mathcal{A} < t\ ; \\ H(S|\mathcal{A}) = H(S), & \text{if } \#\mathcal{A} \leq c. \end{cases}$$

In a ramp scheme, each share size can be smaller than the secret size. However the smaller the share size gets, the more the information on the secret is disclosed.

Definition 3. A (c, t, n)-ramp scheme is said to be *optimal*, if it has the property that $H(S|\mathcal{A}) = \dfrac{t-r}{t-c} H(S)$ holds for any $\mathcal{A} \subset \mathcal{P}$ such that $\#\mathcal{A} = r$ and $c \leq r \leq t$.

It is shown by [JM96], that a (c, t, n)-ramp scheme with the property that $H(P_i) = \dfrac{H(S)}{t-c}$ holds for each i $(1 \leq i \leq n)$ is optimal.

2.3 Threshold changeable scheme

In a secret sharing scheme, it often occurs that the access structure should to be changed before the secret is reconstructed. Furthermore the dealer may often be suspended after distributing shares. This is why we need a threshold scheme in which the threshold can be changed without any dealer assistance, and hereafter call such a scheme *a threshold changeable scheme*.

Here in a threshold changeable scheme, the first (t, n)-threshold scheme is denoted by Π, and the derived (t', n)-threshold scheme is denoted by Π'. The whole scheme is denoted by $\langle \Pi, \Pi' \rangle$.

As seen in Definition 4 given above, for a subset $\mathcal{A} \subset \mathcal{P}$, we denote the set of the images of respective elements by h_* by $\mathcal{H}(\mathcal{A})$. That is, for $\mathcal{A} = \{P_{i_1}, \ldots, P_{i_\ell}\} \subset \mathcal{P}$, we define $\mathcal{H}(\mathcal{A})$ as follows:

$$\mathcal{H}(\mathcal{A}) := h_{i_1}(P_{i_1}) \times h_{i_2}(P_{i_2}) \times \cdots \times h_{i_\ell}(P_{i_\ell}).$$

Definition 4 (in [MPSW99]). We say that a perfect (t, n)-threshold scheme is called *threshold changeable to* t', if there exist known functions h_i for $1 \leq i \leq n$, such that $H(S|\mathcal{H}(\mathcal{A})) = 0$ for any $\mathcal{A} \geq t'$, and $H(S|\mathcal{H}(\mathcal{A})) > 0$ for any $\#\mathcal{A} < t'$ where $\mathcal{A} \subset \mathcal{P}$. (In this paper, we simply write as a *perfect* $(t \to t', n)$*-threshold changeable scheme* instead of a perfect (t, n)-threshold scheme that is threshold changeable to t'.)

In the definitions given above, each known function h_i has to satisfy the property that for any P_i $(1 \leq i \leq n)$, $H(P_i|h_i(P_i)) > 0$ holds not so that s_i can uniquely figured out from s'_i. In this paper, we call each s_i *a full share* (or *share* simply), and each $h_i(s_i)$ *a subshare*.

Though [TTO99] presents an efficient way to derive Π' from Π both of which are perfect, in that scheme, the functions $\{h_i\}$ do not satisfy the property given above. Hence when the threshold is changed, the corresponding secret also has to be simultaneously changed. Since we need to change not the secret but the threshold, we focus the methods given by [MPSW99]. The method given by the first part of [MPSW99] presents a threshold changeable scheme in which both Π and Π' are perfect. But that method requires each share of a threshold changeable scheme to be quite large. Concrete to say, letting α and β denote the secret size and the share size, respectively, we have $\beta \geq 2\alpha$ holds in such a threshold changeable scheme. Hence as described in the following section, if we extend a threshold changeable scheme so that the threshold can be changed plural times, say $N(\geq 2)$ times, then the required share size β is equal to or greater than $(N+1)$ times of the secret size, i.e. $\beta \geq (N+1)\alpha$. For efficiency of

the whole scheme, we aim at a perfect threshold changeable scheme in which Π is ideal as the latter part of [MPSW99] even if the perfect security is lost.

We can easily see that a perfect $(t \to t', n)$-threshold changeable scheme $\langle \Pi, \Pi' \rangle$, in which Π is a (t, n)-threshold scheme and Π' is a (t', n)-threshold scheme, has the property that $H(S|\mathcal{H}(\mathcal{A})) = 0$ if $\#\mathcal{A} \geq t'$ and $H(S|\mathcal{H}(\mathcal{A})) = H(S)$ if $\#\mathcal{A} < t$, since $\#\mathcal{A} < t$ implies $H(S) \geq H(S|\mathcal{H}(\mathcal{A})) \geq H(S|\mathcal{A}) = H(S)$.

2.4 Efficiency measure

Let $\langle \Pi, \Pi' \rangle$ be a perfect $(t \to t', n)$-threshold changeable scheme. Then the efficiency of such a scheme can be measured by the followings:

(1) The maximum and average size of the share which needs to be stored by participants, and which is denoted by $H(P_i)$ for $1 \leq i \leq n$;
(2) The amount of information which needs to be derivered for reconstruction of the secret at the pooling time, and denoted by $\sum_{i \in \mathcal{A}} H(h_i(P_i))$ for $\mathcal{A} \subset \mathcal{P}$ where $\#\mathcal{A} = t'$;
(3) The size of shares after update of the threshold denoted by $H(h_i(P_i))$ for $1 \leq i \leq n$.

Theorem 2 (in [MPSW99]). Let $\langle \Pi, \Pi' \rangle$ be a perfect $(t \to t', n)$-threshold changeable scheme using functions $\{h_i\}_{1 \leq i \leq n}$. Then the followings hold:

(1) $H(P_i) \geq H(S)$ holds for each i $(1 \leq i \leq n)$;
(2) $\sum_{i \in \mathcal{A}} H(h_i(P_i)) \geq \dfrac{t'}{t' - t + 1} H(S)$ holds for every $\mathcal{A} \subset \mathcal{P}$ with $\#\mathcal{A} = t'$;
(3) $\mathsf{max}_{1 \leq i \leq n}\{H(h_i(P_i))\} \geq \dfrac{1}{t' - t + 1} H(S)$ holds.

Note that $\mathsf{max}_{1 \leq i' \leq n}\{H(h_{i'}(P_{i'}))\} = H(h_i(P_i))$ for each i $(1 \leq i \leq n)$, if $\{h_i\}$ is common among the participants, and if all P_i's come from the same domain with the same probability.

Definition 5 (in [MPSW99]). We say that a perfect $(t \to t', n)$-threshold changeable scheme that is threshold changeable to t' is *optimal*, if each bound in Theorem 2 is met with equality.

Corollary 1. If a perfect $(t \to t', n)$-threshold changeable scheme $\langle \Pi, \Pi' \rangle$, is optimal, then Π is ideal and then Π' is an optimal $(t - 1, t', n)$-ramp scheme.

In addition to the definition given above, we define the slightly loose property of a threshold changeable scheme.

Definition 6. Let $\langle \Pi, \Pi' \rangle$ be a perfect $(t \to t', n)$-threshold changeable scheme using functions $\{h_i\}_{1 \leq i \leq n}$. Then the whole scheme is defined to be *almost optimal* if the following holds:

(1) $H(P_i) = H(S)$ holds for each i $(1 \le i \le n)$;

(2) $0 \le \sum_{i \in \mathcal{A}} H(h_i(P_i)) - \dfrac{t'}{t'-t+1} H(S) \le c_1$ holds for every $\mathcal{A} \subset \mathcal{P}$ with $\#\mathcal{A} = t'$ and some $c_1 \ge 0$ independent of $H(S)$ or n;

(3) $0 \le \mathsf{max}_{1 \le i \le n}\{H(h_i(P_i))\} - \dfrac{1}{t'-t+1} H(S) \le c_2$ holds for some $c_2 \ge 0$ which does not depend upon $H(S)$, t, t' or n.

From the definition, we can immediately see that an optimal threshold changeable scheme is an almost optimal one in a special case $c_1 = c_2 = 0$.

2.5 Verifiable secret sharing scheme

A verifiable secret sharing scheme enables each participant to check whether her share given by the dealer is indeed correct, or not, and also the combiner to check whether each pooled share is indeed correct, or not. A verifiable secret sharing scheme is applied as tools for secure multi-party computation and for key management. In this paper, we extend our proposed threshold changeable scheme to be verifiable using the method given by [Ped92], since it provides unconditional security and non-interactivity among the dealer and the participants.

3 Threshold scheme with N-time threshold changeability

In this section, we first extend a perfect $(t \to t', n)$-threshold changeable scheme $\langle \Pi, \Pi' \rangle$ to a perfect $(t \to \mathbf{t}, n)$-threshold changeable scheme $\langle \Pi, \Pi_1, \ldots, \Pi_N \rangle$, where $\mathbf{t} = (t_1, \ldots, t_N)$ with $t < t_k$ for each k $(1 \le k \le N)$ and with $t_k \ne t_{k'}$ for $k \ne k'$. In such a scheme, without the dealer assistance, the threshold can be changed one after another, that is, from t to t_1, from t_1 to t_2, and so on[1] , under the assumption that the secret has not been recovered before the threshold is changed, and that no share has been pooled. We name each derived (t_k, n)-threshold scheme Π_k. The dealer publishes a set of functions $\{h_i^{(k)}\}_{1 \le k \le N}$ so that the participants can compute their subshare for $\{\Pi_k\}_{1 \le k \le N}$ by themselves. For a participant P_i given a share s_i, her subshare for Π_k is computed as $h_i^{(k)}(s_i)$. For a set $\mathcal{A} \subset \mathcal{P}$, the set of their subshares for Π_k is denoted by $\mathcal{H}^{(k)}(\mathcal{A})$, that is, we define $\mathcal{H}^{(k)}(\mathcal{A})$ as follows:

$$\mathcal{H}^{(k)}(\mathcal{A}) := h_{i_1}^{(k)}(P_{i_1}) \times h_{i_2}^{(k)}(P_{i_2}) \times \cdots \times h_{i_\ell}^{(k)}(P_{i_\ell}),$$

where $\mathcal{A} = \{P_{i_1}, P_{i_2}, \ldots, P_{i_\ell}\}$. Note that the thresholds $(t_1, \ldots, t_N)$ have to be determined in advance, since we assume that the dealer is suspended after the initial setting of the scheme. Formally, a $(t \to \mathbf{t}, n)$-threshold changeable scheme is defined as follows.

[1] We may regard this kind of scheme as one in which the threshold can be changed to an arbitrary values among $\{t_1, t_2, \ldots, t_N\}$ each of which is, in advance, determined.

Definition 7. Let $\mathbf{t}$ be $(t_1, \ldots, t_N)$ with $t_k > t$ for each k $(1 \leq k \leq N)$. *A* $(t \to \mathbf{t}, n)$*-threshold changeable scheme* is a (t, n)-threshold scheme, in which for $1 \leq i \leq n$ and $1 \leq k \leq N$, there exist known functions $h_i^{(k)}$ such that $H(S|\mathcal{H}^{(k)}(\mathcal{A})) = 0$ for any $\mathcal{A} \geq t_k$, and $H(S|\mathcal{H}^{(k)}(\mathcal{A})) > 0$ for any $\#\mathcal{A} < t_k$ where $\mathcal{A} \subset \mathcal{P}$.

The properties of "*optimal*" and "*almost optimal*", can be defined also for a perfect $(t \to \mathbf{t}, n)$-threshold changeable scheme.

Definition 8. A perfect $(t \to \mathbf{t}, n)$-threshold changeable scheme $\langle \Pi, \Pi_1, \ldots, \Pi_N \rangle$ is said to be *optimal* (or *almost optimal*), if each threshold changeable scheme $\langle \Pi, \Pi_k \rangle$ $(1 \leq k \leq N)$ is optimal (or almost optimal, respectively), and if for distinct k and k', Π_k and $\Pi_{k'}$ are independent of each other, that is, if it holds that $I(h_i^{(k)}(P_i); h_i^{(k')}(P_i)) = 0$ for any k and k' with $k \neq k'$.

The equation $I(h_i^{(k)}(P_i); h_i^{(k')}(P_i)) = 0$ means that the subshare for Π_k gives no information on the subshare for $\Pi_{k'}$. In the following, we construct a perfect $(t \to \mathbf{t}, n)$-threshold changeable scheme $\langle \Pi, \Pi_1, \ldots, \Pi_N \rangle$ based on [Sha79], in which Π is ideal. From now on, we omit the subscript of $h_i^{(k)}$ and write as $h^{(k)}$, since in this paper, $\{h_i^{(k)}\}$ is common among the participants for each k $(1 \leq k \leq N)$. By defining $\{h^{(k)}\}$ as in Section 3.2, the following $(t \to \mathbf{t}, n)$-threshold changeable scheme can be shown to be almost optimal.

3.1 Construction of a perfect threshold changeable scheme with N-time threshold changeability

Let n be the number of participants. For simplicity, we assume that the thresholds t and $\mathbf{t} = (t_1, \ldots, t_N)$ with $t < t_k \leq n$ for $1 \leq k \leq N$, satisfy $(2 \leq) t < t_1 < t_2 < \cdots < t_N \leq n$. Let q be a prime of the length L such that L is a multiple of $\mathtt{lcm}(t_1 - t + 1, \ldots, t_N - t + 1)$. Note that the prime q satisfies $q = 2^L - \varepsilon$ with $\varepsilon < 2^{L-1}$. Then for the secret $s \in \mathbb{Z}_q$, the dealer constructs a perfect $(t \to \mathbf{t}, n)$-threshold scheme as follows:

(i) First the dealer constructs Shamir's (t, n)-threshold scheme for the secret $s \in \mathbb{Z}_q$. That means, the dealer chooses a degree at most $(t-1)$ polynomial $f(x) = a_{0,1}x + a_{0,2}x^2 + \cdots + a_{0,t-1}x^{t-1} \in \mathbb{Z}_q[x]$ with $f(0) = s$. Each (full) share s_i for P_i is defined to be $f(i) \pmod q$.

(ii) The dealer provides N public function $\{h^{(k)}\}_{1 \leq k \leq N}$ such that for all i and k, $H(h^{(k)}(P_i)|P_i) = 0$ and $H(P_i|h^{(k)}(P_i)) > 0$, $(1 \leq i \leq n,\ 1 \leq k \leq N)$. (A concrete example of the set $\{h^{(k)}\}$ is given the following subsection.) For each participant P_i, her subshare $s_i^{(k)}$ for the (t_k, n)-threshold scheme Π_k, is defined by $h^{(k)}(s_i)$.

(iii) To construct Π_1 from Π, the dealer figures out the polynomial $f_1(x)$ for a (t_1, n)-threshold scheme Π_1 using $f(x)$. $f_1(x)$ is of the form:

$$f_1(x) = f(x) + a_{1,t}x^t + a_{1,t+1}x^{t+1} + \cdots + a_{1,t+n-1}x^{t+n-1},$$

where each coefficient $a_{1,j}$ $(t \leq j \leq t+n-1)$ is found by the n equations $f_1(i) = h^{(1)}(s_i)$ $(1 \leq i \leq n)$. Here we define as follows:

$$\begin{aligned} f_1^{\mathrm{s}} &:= f(x) + a_t x^t + \cdots + a_{t_1-1} x^{t_1-1}; \\ f_1^{\mathrm{p}} &:= f_1(x) - f_1^{\mathrm{s}}(x). \end{aligned}$$

Then if the polynomial $f_1^{\mathrm{p}}(x)$ is open, the (secret) polynomial $f_1(x)$ can be disclosed by any t_1 subshares from $\{h^{(1)}(i)\}_{1 \leq i \leq n}$.

(iv) For k $(1 \leq k \leq N-1)$, to construct Π_{k+1} from Π_k, the dealer figures out the polynomial $f_{k+1}(x)$ for Π_{k+1} using $f_k^{\mathrm{s}}(x)$. $f_{k+1}(x)$ is of the form:

$$f_{k+1}(x) = f_k^{\mathrm{s}}(x) + a_{k+1,t_k} x^{t_k} + \cdots + a_{k+1,t_k+n-1} x^{t_k+n-1},$$

where the n coefficients $a_{k+1,j}$ $(t_k \leq j \leq t_k+n-1)$ are found by the n equations $f_{k+1}(i) = h^{(k+1)}(s_i)$ $(1 \leq i \leq n)$. Here we similarly define as follows:

$$\begin{aligned} f_{k+1}^{\mathrm{s}}(x) &:= f_k^{\mathrm{s}}(x) + a_{k+1,t_k} x^{t_k} + \cdots + a_{k+1,t_{k+1}-1} x^{t_{k+1}-1}; \\ f_{k+1}^{\mathrm{p}}(x) &:= f_{k+1}(x) - f_{k+1}^{\mathrm{s}}(x). \end{aligned}$$

(v) The dealer securely distributes each s_i to P_i, and publishes N polynomials $f_1^{\mathrm{p}}(x), \ldots, f_N^{\mathrm{p}}(x)$ and the N functions $h^{(1)}, \ldots, h^{(N)}$ which derive the subshares from shares.

If no threshold changing has happened, the combiner recovers the secret s by gathering any t (full) shares s_{i_j} $(1 \leq j \leq t)$ as well as in Shamir's scheme. On the other hand, in case that the combiner attempts to recover the secret in the scheme Π_k $(1 \leq k \leq N)$, she gathers any t_k subshares $s_{i_\ell}^{(k)}$ $(1 \leq \ell \leq t_k)$. Then the secret s can be figured out by the following formula which resembles so-called Lagrange polynomial interpolation:

$$s = \sum_{j=1}^{t_k} \left(s_{i_j}^{(k)} - f_k^{\mathrm{p}}(i_j) \right) \prod_{\substack{1 \leq \ell \leq t_k \\ \ell \neq j}} \frac{\ell}{\ell - j}.$$

Note that in the scheme given above, Π_1 is constructed using Π, and each Π_k $(2 \leq k \leq N)$ is constructed using Π_{k-1}. On the other hand, we can also construct $\langle \Pi, \Pi_1, \ldots, \Pi_N \rangle$ by the way that every Π_k $(1 \leq k \leq N)$ is constructed using Π, not using the previous Π_{k-1}. Such a scheme is, however, less efficient in the viewpoint of the amount of information the dealer has to publish, than the scheme we have just constructed in this subsection. We show the detail in Section 5.

3.2 Example of the functions $\{h^{(k)}\}$

As far as we construct the scheme given in the previous subsection, we cannot make any $\langle \Pi, \Pi_k \rangle$ $(1 \leq k \leq N)$ exactly optimal. If we constructed the scheme on

a field $\mathbb{Z}_{q'}^{\alpha}$ with a prime q' and α being a multiple of $\mathtt{lcm}(t_1-t+1,\ldots,t_N-t+1)$, then we could make each $\langle \Pi, \Pi_k \rangle$ exactly optimal. But in that case, we cannot efficiently apply the technique by [Ped92] to that threshold changeable scheme. In a $(t \to \mathbf{t}, n)$-threshold changeable scheme, if Π is ideal, then the possible frequency N of threshold changing is restricted as the following proposition states:

Proposition 1. In a $(t \to \mathbf{t}, n)$-threshold changeable scheme $\langle \Pi, \Pi_1, \ldots, \Pi_N \rangle$, if Π is ideal, and if the whole scheme is (almost) optimal, then the possible frequency N of the possible thresholds satisfy $\sum_{k=1}^{N} 1/(t_k - t + 1) \leq 1$.

Proof. Since Π is ideal, we have the following:

$$\begin{aligned} H(S) &= H(P_i) \geq H(P_i^{(1)}) + \cdots + H(P_i^{(N)}) \\ &\geq \left(\frac{1}{t_1 - t + 1} + \cdots + \frac{1}{t_N - t + 1} \right) H(S), \end{aligned}$$

for each i $(1 \leq i \leq n)$, which is what we claim. ∎

For example in case $t_1 = t+1$, $t_2 = t+2$ and $t_3 = t+5$, since $\sum_{k=1}^{3} 1/(t_k - t+1) = 1$, the correlation yields among $\{P_i^{(k)}\}$ if the threshold is changed more than four times. Hereafter we implicitly assume that for the set of the thresholds $\{t, t_1, \ldots, t_N\}$ and the number N of the threshold changing satisfy the statement of the previous proposition.

Now we define the functions $h^{(k)}$ $(1 \leq k \leq N)$ as follows. Note that q is of the length L and that L is a multiple of $\mathtt{lcm}(t_1 - t + 1, \ldots, t_N - t + 1)$.

- For an element $x \in \mathbb{Z}_q$, $h^{(1)}(x)$ is the substring of x from the first (rightmost) bit to the $(L/(t_1 - t + 1))$-th bit. That is, for $x \in \mathbb{Z}_q$, we define $h^{(1)}(x) := x \pmod{2^{L/(t_1 - t+1)}}$.
- Define T_k to be $\sum_{\ell=1}^{k} 1/(t_\ell - t + 1)$. For an element $x \in \mathbb{Z}_q$ and k $(2 \leq k \leq N)$, $h^{(k)}(x)$ is the substring of x from the $(1 + LT_{k-1})$-th bit to (LT_k)-th bit. That is, for $x \in \mathbb{Z}_q$ and k $(2 \leq k \leq N)$, we define $h^{(k)}(x) := \left\lceil \frac{x}{2^{LT_{k-1}}} \right\rceil \pmod{2^{L/(t_k - t+1)}}$.

In the following, we show that the proposed $(t \to \mathbf{t}, n)$-threshold changeable scheme using functions $\{h^{(k)}\}$ given above, is almost optimal.

Proposition 2. The $(t \to \mathbf{t}, n)$-threshold changeable scheme $\langle \Pi, \Pi_1, \ldots, \Pi_N \rangle$ in Section 3.1, is almost optimal, if it uses the functions $\{h^{(k)}\}$ given above.

Proof. We will prove that our scheme satisfies the conditions in Definition 8, that is, the conditions (1), (2) and (3) in Definition 6 and the condition that for k and k' with $k \neq k'$, Π_k and $\Pi_{k'}$ are independent of each other.

The first condition (1) follows immediately from the fact that Π is just Shamir's scheme.

Next we show the third condition. Since we suppose that q is a prime such that $q = 2^L - \varepsilon$ with $\varepsilon < 2^{L-1}$, then we have the following:

$$H(S) = \log(2^L - \varepsilon) \geq \log(2^L - 2^{L-1}) = L - 1.$$

Furthermore from $H(h^{(k)}(P_i)) \leq L/(t_k - t + 1)$ for each k $(1 \leq k \leq N)$, we can get the following:

$$0 \leq H(h^{(k)}(P_i)) - \frac{H(S)}{t_k - t + 1} \leq \frac{L}{t_k - t + 1} - \frac{L-1}{t_k - t + 1} = \frac{1}{t_k - t + 1} \leq \frac{1}{2}.$$

Hence the third condition is satisfied. The second one is immediately obtained from the third one.

Finally, the last condition that $I(h^{(k)}(P_i); h^{(k')}) = 0$ for each k, k' with $k \neq k'$, comes from the fact that for any $x \in \mathbb{Z}_q$, the strings $h^{(k)}(x)$ and $h^{(k')}(x)$ are indeed disjoint. ∎

4 Efficient VSS for $(t \rightarrow \mathbf{t}, n)$-threshold changeable scheme

In this section, we make the $(t \rightarrow \mathbf{t}, n)$-threshold scheme $\langle \Pi, \Pi_1, \ldots, \Pi_N \rangle$ verifiable. Denote, by Π^v, the verifiable (t, n)-threshold scheme derived by making Π verifiable. Also for each k $(1 \leq k \leq N)$, denote, by Π_k^v, the verifiable (t_k, n)-threshold scheme derived by making Π_k verifiable. To provide the unconditional security and non-interactivity among the entities for verification, we adopt Pedersen's technique [Ped92]. Of course, by constructing Π and Π_k's independently and by applying that technique to Π and each Π_k, we can accomplish our purpose, but here we contrive to make the amount of information the dealer has to publish, by applying [Ped92] to the very $(t \rightarrow \mathbf{t}, n)$-threshold changeable scheme given in the previous section.

How to set up the parameters q, t, t_k $(1 \leq k \leq N)$, N and $\{h^{(k)}\}$ $(1 \leq k \leq N)$ is exactly the same as the previous section. In addition to those parameters, we let p be a prime such that q divides $p-1$ and such that $q^2 < p$ holds[2] , and let α and β be order-q elements in $\mathbb{Z}_p^*$. Those two bases α and β should be randomly picked up by the dealer, or should be chosen by some trusted third party, not so that $\log_\alpha \beta$ may be known to any entities joining the scheme. Note that for s and u belonging to $\mathbb{Z}_q$, the dealer can find another pair $(s', u') \in \mathbb{Z}_q \times \mathbb{Z}_q$ such that $\alpha^s \beta^u = \alpha^{s'} \beta^{u'} \pmod{p}$ if and only if she knows the discrete logarithm $\log_\alpha \beta$ under the modulo p.

In the following, we describe how to construct an almost optimal $(t \rightarrow \mathbf{t}, n)$-threshold changeable scheme with verifiability.

[2] Usually we let p and q be a 1024-bit prime and a 160-bit prime, respectively. Hence this assumption $q^2 < p$ restricts quite little for p and q.

(i) First the dealer constructs a perfect and verifiable (t, n)-threshold scheme Π just like [Ped92]. That means for a secret $s \in \mathbb{Z}_q$, the dealer randomly picks up a degree at most $(t-1)$ polynomial $f(x) \in \mathbb{Z}_q[x]$ such that $f(0) = s$, and also picks up a random $u \in \mathbb{Z}_q$ and a degree at most $(t-1)$ polynomial $g(x) \in \mathbb{Z}_q[x]$ such that $g(0) = u$. The full share for P_i is defined by $f(i)$. Also u_i is defined by $g(i)$ and called *a twin share* for P_i. Here let $f(x) = s + a_{0,1}x + \ldots + a_{0,t-1}x^{t-1}$ and $g(x) = u + b_{0,1}x + \ldots + b_{0,t-1}x^{t-1}$. The commitments $E_0, E_1, \ldots, E_{t-1}$ for $(s, u), (a_{0,1}, b_{0,1}), \ldots, (a_{0,t-1}, b_{0,t-1})$ are defined by $E_0 := E(s, u)$ and $E_j := E(a_{0,j}, b_{0,j})$ $(1 \leq j \leq t-1)$, where for $x, y \in \mathbb{Z}_q$, $E(x, y) := \alpha^x \beta^y \pmod p$.

(ii) For each i and k $(1 \leq i \leq n,\ 1 \leq k \leq N)$, the dealer computes $s_i^{(k)}$ and $u_i^{(k)}$ defined by $h^{(k)}(s_i)$ and $h^{(k)}(u_i)$, respectively. Each $s_i^{(k)}$ and each $u_i^{(k)}$ are called a subshare and *a twin subshare*, respectively.

(iii) To construct Π_1^v from Π^v, the dealer figures out the polynomials $f_1(x)$ and $g_1(x)$ of the form:

$$\begin{aligned} f_1(x) &= f(x) + a_{1,t}x^t + \cdots + a_{1,t+n-1}x^{t+n-1}; \\ g_1(x) &= g(x) + b_{1,t}x^t + \cdots + b_{1,t+n-1}x^{t+n-1}, \end{aligned}$$

where the n coefficients $a_{1,j}$ and the n coefficients $b_{1,j}$ $(t \leq j \leq t+n-1)$ are determined by the n equations $f_1(i) = s_i^{(1)}$ and by the n equations $g_1(i) = u_i^{(1)}$, respectively. Here we define as follows:

$$\begin{aligned} f_1^{\mathrm{s}}(x) &:= f(x) + a_{1,t}x^t + \cdots + a_{1,t_1-1}x^{t_1-1}; \\ f_1^{\mathrm{p}}(x) &:= f_1(x) - f_1^{\mathrm{s}}(x). \end{aligned}$$

Similarly we define $g_1^{\mathrm{s}}(x) := g(x) + b_{1,t}x^t + \cdots + b_{1,t_1-1}x^{t_1-1}$ and $g_1^{\mathrm{p}}(x) := g_1(x) - g_1^{\mathrm{s}}(x)$. For each j $(t \leq j \leq t_1 - 1)$, the commitment E_j for $(a_{1,j}, b_{1,j})$ is defined by $E(a_{1,j}, b_{1,j})$.

(iv) For k $(1 \leq k \leq N-1)$, to construct Π_{k+1}^v from Π_k^v, the dealer figures out the polynomials $f_{k+1}(x)$ and $g_{k+1}(x)$ using $f_k^{\mathrm{s}}(x)$ and $g_k^{\mathrm{s}}(x)$, respectively. $f_{k+1}(x)$ and $g_{k+1}(x)$ are of the form:

$$\begin{aligned} f_{k+1}(x) &= f_k^{\mathrm{s}}(x) + a_{k+1,t_k}x^{t_k} + \cdots + a_{k+1,t_k+n-1}x^{t_k+n-1}; \\ g_{k+1}(x) &= g_k^{\mathrm{s}}(x) + b_{k+1,t_k}x^{t_k} + \cdots + b_{k+1,t_k+n-1}x^{t_k+n-1}, \end{aligned}$$

where the n coefficients $a_{k+1,j}$ and the n coefficients $b_{k+1,j}$ $(t_k \leq j \leq t_k + n - 1)$ are determined by the n equations $f_{k+1}(i) = s_i^{(k+1)}$ and by the n equations $g_{k+1}(i) = u_i^{(k+1)}$, respectively. Here we define as follows:

$$\begin{aligned} f_{k+1}^{\mathrm{s}}(x) &:= f_k^{\mathrm{s}}(x) + a_{k+1,t_k}x^{t_k} + \cdots + a_{k+1,t_{k+1}-1}x^{t_{k+1}-1}; \\ f_{k+1}^{\mathrm{p}}(x) &:= f_{k+1}(x) - f_{k+1}^{\mathrm{s}}(x). \end{aligned}$$

Similarly we define $g^{\mathrm{s}}_{k+1}(x) := g^{\mathrm{s}}_k(x) + b_{1,t_k}x^t + \cdots + b_{k+1,t_{k+1}-1}x^{t_{k+1}-1}$ and $g^{\mathrm{p}}_{k+1}(x) := g_{k+1}(x) - g^{\mathrm{s}}_{k+1}(x)$. For each j $(t_k \le j \le t_{k+1}-1)$, the commitments E_j for $(a_{k+1,j}, b_{k+1,j})$ are defined by $E(a_{k+1,j}, b_{k+1,j})$.

(v) The dealer securely distributes each (s_i, u_i) to P_i, and publishes the $2n$ polynomials $\{f^{\mathrm{p}}_k(x)\}_{1\le k\le N}$ and $\{g^{\mathrm{p}}_k(x)\}_{1\le k\le N}$, $\{h^{(k)}\}_{1\le k\le N}$ and the commitments $\{E_j\}_{0\le j\le N}$.

Each participant P_i given (s_i, u_i) can verify whether her share and twin share are correct, or not, by the following verification:

$$E(s_i, u_i) = \prod_{j=0}^{t-1} E_j^{i^j} \pmod p,$$

and also can, for each k $(1 \le k \le N)$, verify whether each pair $(s_i^{(k)}, u_i^{(k)})$ of her subshares and twin subshares is correct, or not, by the following verification:

$$E(s_i^{(k)} - f^{\mathrm{p}}_k(i), u_i^{(k)} - g^{\mathrm{p}}_k(i)) = \prod_{j=0}^{t_k-1} E_j^{i^j} \pmod p.$$

In recovering the secret, the combiner can similarly verify whether the full shares or the subshares she has gathered, are correct, or not, by the verification given above.

5 Efficiency of the proposed scheme

In this section, we estimate the efficiency of the proposed verifiable threshold changeable scheme with N-time threshold changeability. For simple description, we name the various types of the schemes as follows:

`Scheme-I`: A verifiable $(t \to \mathbf{t}, n)$-threshold changeable scheme $\langle \Pi^v, \Pi_1^v, \ldots, \Pi_N^v \rangle$ in which Π and all Π_k $(1 \le k \le N)$ are independently constructed by using Shamir's method, and in which Pedersen's technique is independently applied to Π and each Π_k.

`Scheme-II`: A verifiable $(t \to \mathbf{t}, n)$-threshold changeable scheme $\langle \Pi^v, \Pi_1^v, \ldots, \Pi_N^v \rangle$ in which each $(t \to t_k, n)$-threshold changeable scheme $\langle \Pi, \Pi_k \rangle$ $(1 \le k \le N)$ is independently constructed, and in which Pedersen's technique is independently applied to each $\langle \Pi, \Pi_k \rangle$.

`Scheme-III`: The proposed verifiable $(t \to \mathbf{t}, n)$-threshold changeable scheme $\langle \Pi^v, \Pi_1^v, \ldots, \Pi_N^v \rangle$ we have constructed in Section 4.

In the following, we show the efficiency for the dealer. Precisely, we, in Figure 1, show the amount of information she has to securely distributed and the amount of information she has to publish, in `Scheme-I`, in `Scheme-II` and in `Scheme-III`, respectively. As seen in Figure 1, to be sure that `Scheme-I` is su-

Scheme	By-SC ($\times H(S)$)	COP ($\times \log q$)	Commitment ($\times \log p$)	Security
I	$2(N+1)$	0	$t+\sum_{k=1}^{N}(t_k-1)$	Π : perfect (t,n)-TS Π_k : perfect (t_k,n)-TS
II	2	$2\sum_{k=1}^{N}(n-t_k+1)$	$t+\sum_{k=1}^{N}(t_k-1)$	Π : perfect (t,n)-TS Π_k : $(t-1,t_k,n)$-RS
III	2	$2(nN+t-t_N)$	$\mathsf{max}_{1\le k\le N}t_k$	Π : perfect (t,n)-TS Π_k : $(t-1,t_k,n)$-RS

By-SC : The amount of information per one participant, which the dealer has to distribute by some secure channel.

COP : The amount of information of the coefficients of the open polynomials $\{f_k^{\mathrm{p}}(x)\}$ and $\{g_k^{\mathrm{p}}(x)\}$, which the dealer has to publish to control the thresholds.

Commitment : The amount of information of the commitments, which the dealer has to open for verification of the full shares and the subshare.

Security : The security of the schemes $\Pi, \Pi_1, \ldots, \Pi_N$ as threshold schemes. The terms "TS" and "RS" stand for "threshold scheme" and "ramp scheme", respectively.

Fig. 1. Comparison of the efficiency of Scheme-I,II,III

perior to the others in view of the security of each Π_k, but that scheme requires much more amount of information to be securely distributed. Since in Scheme-II and Scheme-III, such amount does not depend upon the number of the frequency of the threshold changing, we discuss Scheme-II and Scheme-III.

Denote, by A_{II} and A_{III}, the total amount of information the dealer has to publish in Scheme-II and in Scheme-III, respectively.

Proposition 3. Suppose that $t \ge 2$, $t_k > 2$ $(1 \le k \le N)$ and p, q are prime such that $q|(p-1)$ and such that $q^2 < p$. Then $A_{\mathrm{III}} < A_{\mathrm{II}}$ holds. That means Scheme-III is more efficient than Scheme-III in view of the amount of information the dealer has to publish.

Proof. First note that we may let $\mathsf{max}_{1\le k\le N}t_k = t_N$ without loss of generality. From the definition, we have

$$\begin{aligned} A_{\mathrm{II}} &= \left(t+\sum_{k=1}^{N}(t_k-1)\right)\log p + 2\left(\sum_{k=1}^{N}(n-t_k+1)\right)\log q; \\ A_{\mathrm{III}} &= t_N \log p + 2(nN+t-t_N)\log q. \end{aligned}$$

Then we can get the following:

$$A_{\mathrm{II}} - A_{\mathrm{III}} = \left(t+\sum_{k=1}^{N-1}t_k - N\right)\left(\log p - \log q^2\right),$$

which is necessarily positive, since $p > q^2$ and $t + \sum_{k=1}^{N-1} t_k - N > 2N - N = N > 0$. ∎

6 Conclusion

Remember that a $(t \to \mathbf{t}, n)$-threshold changeable scheme simply constructed by an optimal (t, n)-threshold scheme that is threshold changeable to t' given by [MPSW99], cannot be efficiently made verifiable by the technique [Ped92]. Then in this paper, we have constructed a $(t \to \mathbf{t}, n)$-threshold changeable scheme $\langle \Pi, \Pi_1, \ldots, \Pi_N \rangle$ based on Shamir's threshold scheme. This is an almost optimal $(t \to \mathbf{t}, n)$-threshold changeable scheme, and can be easily made a verifiable $(t \to \mathbf{t}, n)$-threshold changeable scheme with unconditional security and non-interactivity among the entity for verification. As seen in the primitive one (`Scheme-I`) in Figure 1, the perfect security of each Π_k $(1 \leq k \leq N)$ requires much more size full shares to be securely distributed. On the other hand, though in the proposed scheme (that is, `Scheme-III`), each scheme Π_k $(1 \leq k \leq N)$ sacrifices the perfect security, the entropy of the full share does not depend upon the number of the frequency of the threshold changing. Furthermore we decrease the amount of information the dealer has to publish by constructing Π_k using Π_{k-1} $(1 \leq k \leq N)$, where $\Pi_0 := \Pi$. This difference is indicated by the inequality $A_{\mathrm{II}} - A_{\mathrm{III}} > 0$ appearing Proposition 3 in Section 5.

References

[Bla79] G. R. Blakley: "*Safeguarding cryptographic keys*", Proceedings of AFIPS 1979, National Computer Conference, vol.48, pp.313-317, 1979.

[JM96] W. A. Jackson and K. M. Martin: "*A combinatorial interpretation of ramp schemes*", Australasian Journal of Combinatorics 14, pp.51-60, 1996.

[MPSW99] K. M. Martin, J. Pieprzyk, R. Safavi-Naini and H. Wang: "*Changing thresholds in the absence of secure channels*", Proceedings of ACISP'99, Lecture Notes in Computer Science 1587, pp.177-191, 1999.

[Ped92] T. P. Pedersen: "*Non-interactive and information theoretic secure verifiable secret sharing*", Advances in cryptology - Crypto'92, Lecture Notes in Computer Science 576, pp.129-140, 1992.

[Sha79] A. Shamir: "*How to share a secret*", Communications of ACM, pp.612-613, 1979.

[Sti95] D. R. Stinson: Cryptography - Theory and Practice, The CRC press series on discrete mathematics and its applications, CRC Press, 1995.

[TTO99] Y. Tamura, M. Tada and E. Okamoto: "*Update of access structure in Shamir's* (k, n) *threshold scheme*", Proceedings of The 1999 Symposium on Cryptography and Information Security (SCIS'99), vol.I, pp.469-474, 1999.