Analysis and Design of Multiple Threshold Changeable Secret Sharing Schemes

Tiancheng Lou[1] and Christophe Tartary[1,2]

[1] Institute for Theoretical Computer Science
Tsinghua University
Beijing, 100084
People's Republic of China
[2] Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
Singapore
loutiancheng860214@gmail.com,
ctartary@ntu.edu.sg

Abstract. In a (r, n)-threshold secret sharing scheme, no group of $(r-1)$ colluding members can recover the secret value s. However, the number of colluders is likely to increase over time. In order to deal with this issue, one may also require to have the ability to increase the threshold value from r to $r'(> r)$, such an increment is likely to happen several times.

In this paper, we study the problem of threshold changeability in a dealer-free environment. First, we compute a theoretical bound on the information and security rate for such a secret sharing. Second, we show how to achieve multiple threshold change for a Chinese Remainder Theorem like scheme. We prove that the parameters of this new scheme asymptotically reach the previous bound.

Keywords: Secret Sharing Scheme, Threshold Changeability, Information Rate, Security Rate, Chinese Remainder Theorem, Dealer Free Update.

1 Introduction

A (r, n)-threshold secret-sharing (TSS) scheme is a cryptographic primitive, allowing a dealer to divide a secret s into n pieces of information called shares (or shadows), distribute them among a group of n participants in such a way that the secret is reconstructible from any r shares while any set of $r-1$ shadows cannot uniquely determine s. Classical constructions for threshold secret-sharing schemes include the polynomial-based Shamir scheme [12], geometry-based Blakley scheme [3] and the integer-based Chinese Remainder Theorem (CRT) scheme [1].

A common application for TSS schemes is to achieve robustness of distributed security systems. A distributed system is called robust if its security is maintained against an attacker who manages to break into a certain number of components of the system. In many settings, the attacker capabilities are likely to change over time. This threat requires the security level (i.e. the threshold value) to vary as well.

M.K. Franklin, L.C.K. Hui, and D.S. Wong (Eds.): CANS 2008, LNCS 5339, pp. 196–213, 2008.

There is a trivial solution to the problem of increasing the threshold parameter of a (r, n)-TSS scheme. The participants simply discard their old shares while the dealer distribute shadows of a (r', n)-TSS scheme to all participants. However, this solution is not very attractive since it requires the dealer to be involved after the setup stage as well as the availability of a secure channel between the dealer and each one of the n group members. Such secure channels may not exist or may be difficult to establish after the initial setup phase.

There already exist TSS schemes allowing the threshold parameters to be changed after the initial setup. Using secret redistribution [6, 11] involves communication amongst the participants in order to redistribute the secret using a new threshold parameter. Although this technique can be applied to standard secret-sharing schemes, its disadvantage is the need of secure channels for communication between participants. Constructions from [5, 2, 9] do not need such secure channels, but they all require the initial secret-sharing scheme to be a non-standard one, i.e. it must specially be designed for threshold increase. Ramp schemes [4, 8] use optimal size of shares but they are not perfect. Other techniques [13, 14] can be applied to existing schemes even if they were set up without consideration to future threshold increases. Unfortunately, those approaches have worse security than the construction presented in [5, 2, 9]. The secret schemes designed in [10, 16] achieve perfect security before and after threshold modification. However, the share size has to be at least twice of the size of secret. Moreover, if we change to threshold c times, the size of the initial shares needs to be at least $(c + 1)$ times as large as the secret's.

In this paper, we first construct an upper-bound on the security rate (ratio between the entropy of a largest unauthorized group and the entropy of the secret) and information rate (ratio between the share size and the secret size) of a changeable-threshold scheme. Second, we propose a new CRT-based secret sharing scheme allowing multiple threshold updates. Our construction allows to choose the security rate of the scheme while having an information rate meeting the previous bound. We will show that our scheme can achieves perfect security, ideal initial scheme and optimal ramp-scheme (the ramp-scheme uses optimal size of shares) easily.

In Sect. 2, we briefly recall some definitions about TSS schemes. In Sect. 3, we discuss the definition of the changeable-threshold secret-sharing scheme as well as the upper-bound on the security rate and information rate for threshold change. In Sect. 4, we present our construction allowing to increase the threshold parameter $c(\geq 1)$ times. After proving its correctness and efficiency, we present two examples: one for standard initial scheme and one for optimal ramp-scheme. The last section concludes the paper.

2 Preliminaries

In this section, we review some basic definitions related to secret sharing.

Definition 1 (TSS Scheme [13]). *Denote $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$ a group of n participants. Let $\mathcal{S}$ be the set of secrets and let the share of P_i come from a set $\mathcal{S}_i$. Denote $\mathcal{R}$ a set of random strings. A* (r, n)-Threshold Secret-Sharing (TSS) scheme *is a pair of algorithms called the* dealer *and the* combiner *working as follows:*

– *For a given secret from $\mathcal{S}$ and some random string from $\mathcal{R}$, the dealer algorithm applies the mapping:*

$$\mathcal{D}_{r,n} : \mathcal{S} \times \mathcal{R} \rightarrow \mathcal{S}_1 \times \mathcal{S}_2 \times \cdots \times \mathcal{S}_n$$

to assign shares to participants from $\mathcal{P}$.
– *The shares of a subset $\mathcal{A} \subseteq \mathcal{P}$ of participants can be input into the combiner algorithm. Denote $S_{\mathcal{A}}$ the set of shares of participants from $\mathcal{A}$. The mapping:*

$$\mathcal{C}_{r,n} : S_{\mathcal{A}} \rightarrow \mathcal{S}$$

uniquely determines the secret when $|\mathcal{A}| \geq r$. Otherwise, it fails to uniquely determine the secret value.

The previous definition is rather general and it does not specify what can occur when the secret is not reconstructed. As a consequence, one of the basic problems in the field of secret sharing schemes is to derive bounds on the amount of information revealed by at most $r-1$ shares.

Definition 2 (Security Rate [15]). *For a (r,n)-*TSS *scheme with secret s, the* security rate *ϕ is the real number defined as:*

$$\phi = \min\left\{ \frac{H(\mathcal{S}|S_{i_1}, \ldots, S_{i_m})}{H(\mathcal{S})} : \{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\} \text{ and } m < r \right\}$$

where S_i is the i-th share (for $i \in \{1, \ldots, n\}$).

Definition 3 (Perfect TSS Scheme [15]). *Consider a (r,n)-*TSS *scheme with the following properties:*

1. *if $|\mathcal{A}| \geq r$ then $H(\mathcal{S}|\mathcal{S}_{\mathcal{A}}) = 0$*
2. *if $|\mathcal{A}| < r$ then $H(\mathcal{S}|\mathcal{S}_{\mathcal{A}}) = H(\mathcal{S})$*

where s denote the secret and H is the entropy function. Then, this secret sharing is called perfect*.*

Note that, for a perfect scheme, we have: $\phi = 1$. A perfect (r,n)-TSS scheme allows the dealer to distribute a secret s amongst a group of n participants in such a way that any r-subgroup of members can reconstruct it while no subsets of less than r participants can gain any information about s.

Another efficiency parameter of secret sharing schemes is the amount of information that the participants must keep secret.

Definition 4 (Information Rate [15]). *For a (r,n)-*TSS *scheme with secret s, we call* information rate *of the scheme ρ, the value ρ defined as:*

$$\rho = \min\left\{ \frac{H(\mathcal{S})}{H(S_i)} : 1 \leq i \leq n \right\}$$

where S_i is the i-th share (for $i \in \{1, \ldots, n\}$).

Note that, for any perfect secret sharing scheme, we have: $\rho \leq 1$ [15]. The following definition characterize the property that the information rate is in optimal situation.

Definition 5 (Ideal TSS Scheme [15]). *A perfect* (r, n)-TSS *scheme is called* ideal *if and only if* $\rho = 1$.

In other words, a perfect threshold scheme is ideal when the size of the shares is the same as the secret's. We can easily see that Shamir's scheme is ideal.

An example of non-perfect threshold scheme is given by ramp schemes [4]. Such constructions offer a trade-off between security and share size. We first review the definitions of ramp-schemes as well as optimal ramp-schemes [7].

Definition 6 (Ramp Scheme [4]). *A* $(\mathcal{T}, n)$*-threshold secret sharing scheme with secret* s *is said to be a* $(\mathcal{C}, \mathcal{T}, n)$*-ramp scheme if it satisfies the following properties:*

1. *If* $|\mathcal{A}| \geq \mathcal{T}$*, then* $H(\mathcal{S}|\mathcal{A}) = 0$.
2. *If* $\mathcal{C} < |\mathcal{A}| < \mathcal{T}$*, then* $0 < H(\mathcal{S}|\mathcal{A}) < H(\mathcal{S})$.
3. *If* $|\mathcal{A}| \leq \mathcal{C}$*, then* $H(\mathcal{S}|\mathcal{A}) = H(\mathcal{S})$.

In a ramp scheme, each share size can be smaller than the secret size. However, the smaller the share size gets, the more information about the secret is revealed. We have the following theorem presented in [7].

Theorem 1 ([7]). *For any* $(\mathcal{C}, \mathcal{T}, n)$*-ramp scheme, we have:*

$$H(\mathcal{S}|S_{\mathcal{A}}) \geq \frac{\mathcal{T} - \mathcal{R}}{\mathcal{T} - \mathcal{C}} H(\mathcal{S}) \quad \text{and} \quad \forall i \in \{1, \ldots, n\}\ H(S_i) \geq \frac{H(\mathcal{S})}{\mathcal{T} - \mathcal{C}}$$

Definition 7 (Optimal Ramp Scheme [7]). *A* $(\mathcal{C}, \mathcal{T}, n)$*-ramp scheme is said to be optimal, if it has the property that* $H(\mathcal{S}|S_{\mathcal{A}}) = \frac{\mathcal{T} - \mathcal{R}}{\mathcal{T} - \mathcal{C}} H(\mathcal{S})$ *hold for any* $\mathcal{A} \subseteq \{1, 2, \ldots, n\}$ *such that* $|\mathcal{A}| = \mathcal{R}$ *and* $\mathcal{C} \leq \mathcal{R} \leq \mathcal{T}$ *and shares are of minimal size* $H(S_i) = \frac{H(\mathcal{S})}{\mathcal{T} - \mathcal{C}}$.

3 Threshold Changeability for Secret-Sharing Scheme

3.1 Definition and Efficiency Measures

As said in Sect. 1, it sometimes occurs that the security level be changed before the secret is to be reconstructed. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a group of n participants and denote S the set of secrets.

Definition 8 (Threshold Changeability). *A* $(r_0 \rightarrow \boldsymbol{r}, n)$-threshold changeable *scheme is a threshold scheme where the threshold can be increased* $c\,(\geq 1)$ *times,* $\boldsymbol{r} = (r_1, \ldots, r_c)$ *with* $r_{i-1} < r_i$ *for* $i \in \{1, \ldots, c\}$.

The initial (r_0, n)*-threshold scheme is denoted* Π_0 *and the* i^{th} *derived* (r_i, n)*-threshold scheme is denoted* Π_i*. For any* $i \in \{0, \ldots, c\}$ *and any* $j \in \{1, \ldots, n\}$*, we let* $\mathcal{S}_{i,j}$ *denote the set of* j*-th shares of* Π_i*. There exists one dealer algorithm,* c *combiner (sub-share combiner) algorithms and* $c\,n$ *sub-share generation algorithms with the following properties:*

- *For a given secret from $\mathcal{S}$ and some random string from $\mathcal{R}$, the dealer algorithm applies the mapping:*

$$\mathcal{D}_{r_0,n} : \mathcal{S} \times \mathcal{R} \rightarrow \mathcal{S}_{0,1} \times \cdots \times \mathcal{S}_{0,n}$$

  to assign shares to participants from $\mathcal{P}$.
- *For any share from $\mathcal{S}_{i,j}$, there exists a sub-share generation algorithm:*

$$\mathcal{E}_{r_0 \rightarrow \boldsymbol{r},i,j} : \mathcal{S}_{i,j} \rightarrow \mathcal{S}_{i+1,j}$$

  to modify shares for increasing the threshold parameter from r_i to r_{i+1} for any $i \in \{0, \ldots, c-1\}$.
- *For any $i \in \{0, \ldots, c\}$, the shares of a subset $\mathcal{A} \subseteq \mathcal{P}$ of participants can be input into the combiner algorithm. Let $\mathcal{S}_{i,\mathcal{A}}$ denote the set of shares of $\mathcal{A}$ in Π_i, if $|\mathcal{A}| \geq r_i$ then the mapping:*

$$\mathcal{C}_{r_0 \rightarrow \boldsymbol{r},i} : \mathcal{S}_{i,\mathcal{A}} \rightarrow \mathcal{S}$$

  reconstructs the secret. And for any $r_i - 1$ participants, it always failed to recover the secret.

In the definitions given above, the sub-share generation algorithms can be probabilistic (dealer free). The third point of Definition 8 involves that, for any r_i-group G, there exists $j_0 \in G$ such that $H(s_{i,j_0}|s_{i+1,j_0}) > 0$. Indeed, in the opposite situation, there would be a r_i-group $\tilde{G}$ such that: $\forall P_j \in \tilde{G} \quad H(s_{i,j}|s_{i+1,j}) = 0$. This would imply that each of the r_i members of $\tilde{G}$ could reconstruct his share related to threshold r_i from his share related to the new value $r_{i+1}(> r_i)$. Thus, we would not have a (r_{i+1}, n)-threshold scheme after threshold update which contradicts the definition of threshold changeability.

Remark. We would like to call the reader's attention to the fact that old shares are assumed to be deleted after performing any threshold update. That is, after updating the threshold value from r_i to r_{r+1}, each of the n participants keeps the share related to the new value r_{i+1} and discards the shadow related to r_i (for $i \in \{0, \ldots, c-1\}$).

The efficiency of a TSS scheme can be measured by its security rate and information rate. We generalize those definitions to the case of a threshold changeable scheme.

Definition 9 (Security and Information Rates). *Let $\langle \Pi_0, \ldots, \Pi_c \rangle$ be a $(r_0 \rightarrow \boldsymbol{r}, n)$-threshold changeable scheme where $\boldsymbol{r} = (r_1, \ldots, r_c)$ with $r_{i-1} < r_i$ for $i \in \{1, \ldots, c\}$. Let ϕ_i denote the security rate of Π_i. The* security rate *ϕ of the changeable scheme $\langle \Pi_0, \ldots, \Pi_c \rangle$ is defined as $\min_{i \in \{0,\ldots,c\}} \{\phi_i\}$. Let ρ_i denote the information rate of Π_i. The* information rate *ρ of the changeable scheme $\langle \Pi_0, \ldots, \Pi_c \rangle$ is defined as $\min_{i \in \{0,\ldots,c\}} \{\rho_i\}$.*

We will present the definition of deterministic $(r_0 \rightarrow \mathbf{r}, n)$-threshold changeable scheme, where $\mathbf{r} = (r_1, r_2 \cdots r_c)$.

Definition 10 (Deterministic Threshold Changeable Scheme). *Let $\langle \Pi_0, \ldots, \Pi_c \rangle$ be a $(r_0 \rightarrow \boldsymbol{r}, n)$-threshold changeable scheme. The scheme $\langle \Pi_0, \ldots, \Pi_c \rangle$ is called* deterministic*, if all the c sub-share generation algorithms are deterministic. In other words, there exist deterministic functions $h_{i,j}$, such that $s_{i+1,j} = h_{i,j}(s_{i,j})$, where $s_{i,j}$ is j-th shadow of Π_i for $i \in \{0, \ldots, c-1\}$ and $j \in \{1, \ldots, n\}$.*

Many existing secret-sharing schemes (like Shamir's construction [12] and the CRT-based secret sharing [1]) are ideal. We have the following result.

Lemma 1. *Let $\langle \Pi_0, \ldots, \Pi_c \rangle$ be a deterministic $(r_0 \rightarrow \boldsymbol{r}, n)$-threshold changeable scheme. If the initial (r_0, n)-*TSS *scheme Π_0 is ideal then the final (r_c, n)-*TSS *scheme Π_c cannot be ideal.*

Proof. We demonstrate this result by contradiction. Assume the (r_c, n)-TSS scheme Π_c is ideal. We fix $i \in \{1, \ldots, n\}$. We have:

$$I(S_{0,i}; S_{c,i}) = H(S_{0,i}) - H(S_{0,i}|S_{c,i}) = H(S_{c,i}) - H(S_{c,i}|S_{0,i})$$

So, we get:

$$H(S_{0,i}|S_{c,i}) = H(S_{0,i}) - H(S_{c,i}) + H(S_{c,i}|S_{0,i}) = H(S_{c,i}|S_{0,i})$$

Since the algorithm to update the threshold is deterministic, we have: $H(S_{0,i}|S_{c,i}) = H(S_{c,i}|S_{0,i}) = 0$. This means that one can recover $S_{0,i}$ from $S_{c,i}$ for any $i \in \{1, \ldots, n\}$. Thus, the resulting scheme Π_c is also a (r_0, n)-threshold secret-sharing scheme, which is impossible. □

3.2 Upper Bounds on the Security Rate and the Information Rate

Definition 11. *Suppose $\mathcal{T}$ is a (r, n)-*TSS *scheme with secret s. It is called a (ϕ, ρ) (Semi-Random Dealer and Complete Randomness Recovery Combiner)* SRDCRRC*-scheme if it has the following properties:*

1. *$\mathcal{T}$ has security rate ϕ. This means that we have $H(\mathcal{S}|S_{i_1}, \ldots, S_{i_m}) \geq \phi H(\mathcal{S})$ for any $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\}$ and $m < r$.*
2. *$\mathcal{T}$ has information rate ρ. This means that we have $H(S_i) \leq \frac{H(\mathcal{S})}{\rho}$ for any $i \in \{1, \ldots, n\}$.*
3. *When the dealer of $\mathcal{T}$ wants to share s, he secretly chooses one random string a and uses the pair $\alpha = (s, a)$ to construct the n shares. The method to output n shares using α is deterministic.*
4. *The combiner of $\mathcal{T}$ can recover the secret s if and only if it can uniquely determine α. In other words, by any r shares, the combiner can reconstruct not only the secret s but also all random bits a.*

Lemma 2. *Suppose $\mathcal{T}$ is a (r, n)-threshold secret-sharing scheme as well as a (ϕ, ρ)* SRDCRRC*-scheme. Let S_i denote i-th share of $\mathcal{T}$. We have: $H(\alpha) = H(S_1, \ldots, S_r)$.*

Proof. Since the dealer algorithm is deterministic, we have: $H(S_1, \ldots, S_r|\alpha) = 0$. On the other hand, using $S_1, \ldots, S_r$, the combiner can recover the vector α. So, we have: $H(\alpha|S_1, \ldots, S_r) = 0$. As a consequence, we get: $H(\alpha) = H(S_1, \ldots, S_r)$. □

Remark. The previous result is valid for any r shares. We focused on $S_1, \ldots, S_r$ as this will be used to demonstrate the following lemma.

Lemma 3. *Suppose $\mathcal{T}$ is a (r, n)-threshold secret-sharing scheme with secret s as well as a (ϕ, ρ)* SRDCRRC*-scheme. Then: $H(\alpha) \geq r\phi H(\mathcal{S})$.*

Proof. Let S_i denote the i-th share of $\mathcal{T}$. According to Lemma 2, we have:

$$\begin{aligned} H(\alpha) &= H(S_1, \ldots, S_r) = H(S_1) + H(S_2, \ldots, S_n|S_1) \\ &= H(S_1) + H(S_2|S_1) + H(S_3, \ldots, S_n|S_1, S_2) \\ &= \sum_{k=1}^{r} H(S_k|S_1, \ldots, S_{k-1}) \end{aligned}$$

We get: $H(\alpha) \geq \sum_{k=1}^{r} H(S_k|\{S_1, \ldots, S_r\} \setminus \{S_k\})$.

Let $\mathcal{A}$ be a r-subset and choose any participant i from $\mathcal{A}$, define $\mathcal{B} = \mathcal{A} \setminus \{i\}$ and the size of $\mathcal{B}$ is $r - 1$. Let $S_{\mathcal{B}}$ denote the shares of all participants in $\mathcal{B}$. Since $\mathcal{T}$ has a security rate ϕ, we have $H(\mathcal{S}|S_{\mathcal{B}}) \geq \phi H(\mathcal{S})$. Using $S_{\mathcal{B}}$, we get a set of possible secrets $\mathcal{S}'(\subseteq \mathcal{S})$ such that $s \in \mathcal{S}'$ and $H(\mathcal{S}') = \phi H(\mathcal{S})$ where $\mathcal{S}$ is the set of all secrets. Hence, for each $s' \in \mathcal{S}'$, there is a distribution rule[15] $dist(s')$ such that the shares of $\mathcal{B}$ are the same. Since $\mathcal{A}$ is authorized, we must have: $S_i^{dist(s_1)} \neq S_i^{dist(s_2)}$ when $s_1 \neq s_2$ and $s_1, s_2 \in \mathcal{S}'$. Thus: $H(S_i|S_{\mathcal{B}}) \geq H(\mathcal{S}') \geq \phi H(\mathcal{S})$.

Thus: $\forall k \in \{1, \ldots, r\}\ H(S_k|\{S_1, \ldots, S_r\}\setminus\{S_k\}) \geq \phi H(\mathcal{S})$. This achieves our proof. □

Theorem 2. *Suppose that there exists a deterministic algorithm for changing a (r, n)-*TSS *scheme $\mathcal{T}_1$ to (r', n)-*TSS *scheme $\mathcal{T}_2$. Assume that $\mathcal{T}_1$ is a (ϕ_1, ρ_1)* SRDCRRC*-scheme and $\mathcal{T}_2$ is a (ϕ_2, ρ_2)* SRDCRRC*-scheme. We have:*

$$\min(\rho_1, \rho_2) \times \min(\phi_1, \phi_2) \leq \frac{r}{r'}$$

Proof. The dealer algorithm of $\mathcal{T}_2$ is the dealer algorithm of $\mathcal{T}_1$ followed by the deterministic algorithm $\mathcal{A}$ to change the threshold. According to Lemma 3, we have: $H(\alpha) \geq r'\phi_2 H(\mathcal{S})$.

Let $S_{1,i}$ denote the i-th share of $\mathcal{T}_1$. According to Lemma 2, we have:

$$H(S_{1,1}, \ldots, S_{1,r}) = H(\alpha) \geq r'\phi_2 H(\mathcal{S})$$

So:

$$\max_{1\leq i\leq n} H(S_{1,i}) \geq \max_{1\leq i\leq r} H(S_{1,i}) \geq \frac{1}{r}\sum_{i=1}^{r} H(S_{1,i}) \geq \frac{1}{r}H(S_{1,1}, \ldots, S_{1,r}) \geq \frac{r'\phi_2}{r}H(\mathcal{S})$$

Thus, we get:

$$\rho_1 \leq \frac{H(\mathcal{S})}{\max\limits_{1\leq i\leq n} H(S_{1,i})} \leq \frac{H(\mathcal{S})}{\frac{r'\phi_2}{r}H(\mathcal{S})} \leq \frac{r}{r'\phi_2}$$

Therefore, we have:

$$\min(\rho_1, \rho_2) \times \min(\phi_1, \phi_2) \leq \rho_1\phi_2 \leq \frac{r}{r'}$$

□

Remark. Note that if both $\mathcal{T}_1$ and $\mathcal{T}_2$ are perfect secret-sharing schemes, then the information rate of $\langle \mathcal{T}_1, \mathcal{T}_2 \rangle$ is at most $\frac{r}{r'}$. Similarly, if both $\mathcal{T}_1$ and $\mathcal{T}_2$ have shares as large as the secret, then the security rate of $\langle \mathcal{T}_1, \mathcal{T}_2 \rangle$ is at most $\frac{r}{r'}$.

4 Threshold Changeability for CRT Secret-Sharing Schemes

4.1 CRT Secret Sharing Scheme

We now describe the CRT secret sharing scheme presented in [1]. Denote $\mathfrak{S}_i$ the set of all i-subsets of $\{1, \ldots, n\}$. A set of pairwise coprime integers $\{p, m_1, \ldots, m_n\}$ is chosen subject to the following:

$$\exists M : \left(\forall S \in \mathfrak{S}_r \prod_{i\in S} m_i \geq M\right) \text{ and } \left(\forall S \in \mathfrak{S}_{r-1} \prod_{i\in S} m_i \leq \frac{M}{p}\right)$$

The reader may notice that the original definition by [1] is slightly different. However, it can be shown that both definitions are equivalent.

Dealer. Suppose the secret value is s, we can assume that $0 \leq s < p$. Selecting a random integer A in $[0, \frac{M}{p} - 1]$ and set $y = s + A\,p$. The set of shadows is $(y_1, \ldots, y_n)$, where $y_i = y \bmod m_i$ for $i \in \{1, \ldots, n\}$.

Combiner. To recover secret s, it clearly suffices to find y. If $y_{i_1}, \ldots, y_{i_r}$ are known, then y is known modulo $\mathcal{N}_1 = \prod\limits_{j=1}^{r} m_{i_j}$ (CRT). As $\mathcal{N}_1 \geq M$, this uniquely determines y and thus s. On the other hand, if only $r - 1$ shadows were known, essentially no information about the key can be recovered. If $y_{i_1}, \ldots, y_{i_{r-1}}$ are known, then we have the value of y modulo $\mathcal{N}_2 = \prod\limits_{j=1}^{r-1} m_{i_j}$. Since $\frac{M}{\mathcal{N}_2} \geq p$ and $\gcd(\mathcal{N}_2, p) = 1$, the collection of numbers n_i with $n_i \equiv y \pmod{\mathcal{N}_2}$ and $n_i \leq M$ cover all congruence classes modulo p, with each class containing at most one more or one less n_i than any other class.

The CRT sharing scheme described above is perfect. However, the construction that we will present in the next section will not as its security rate will not be equal to 1.

4.2 A New CRT-Based Secret Sharing Scheme

In this section, we present our construction which is a modification of the CRT secret sharing scheme. Let n be the number of participants, we choose a set of integers $\{p, q, m_1, \ldots, m_n, w_1, \ldots, w_n\}$ as follows:

1. $\gcd(m_i^{w_i}, m_j^{w_j}) = \gcd(m_i, m_j) = 1$ for $i \neq j$,
2. $\gcd(p, m_i^{w_i}) = \gcd(p, m_i) = 1$ for all i and $q|p$,
3. $\exists M : \left(\forall S \in \mathfrak{S}_r \prod_{i \in S} m_i^{w_i} \geq M\right)$ and $\left(\forall S \in \mathfrak{S}_{r-1} \prod_{i \in S} m_i^{w_i} \leq \frac{M}{q}\right)$.

Share Construction. Suppose the secret value is s, we can assume that $0 \leq s < p$. Selecting a random integer A in $[0, \frac{M}{p} - 1]$, and set $y = s + A\,p$. The set of shadows are $(y_1, \ldots, y_n)$, where $y_i = y \bmod m_i^{w_i}$.

Secret Recovery. To recover secret s, it clearly suffices to find y. If $y_{i_1}, \ldots, y_{i_r}$ are known, then y is known modulo $N_1 = \prod_{j=1}^{r} m_{i_j}^{w_{i_j}}$ (CRT). As $N_1 \geq M$, this uniquely determines y and thus s.

On the other hand, if only $r - 1$ shadows were known, we can not uniquely determine the secret s. If $y_{i_1}, \ldots, y_{i_{r-1}}$ are known, then we have the value of y modulo $N_2 = \prod_{j=1}^{r-1} m_{i_j}^{w_{i_j}}$. Since $\frac{M}{N_2} \geq q$ and $\gcd(N_2, p) = 1$, the collection of numbers n_i with $n_i \equiv y \pmod{N_2}$ and $n_i \leq M$ cover all congruence classes modulo q, with each class containing at most one more or one less n_i than any other class. So, the security rate of the scheme:

$$\phi = \frac{H(x|y_{i_1}, y_{i_2}, \ldots, y_{i_{r-1}})}{H(x)} = \frac{\log q}{\log p} = \log_p q$$

The information rate of the scheme is:

$$\rho = \frac{\log p}{\log\left(\max\{m_i^{w_i} : 1 \leq i \leq n\}\right)} = \frac{\log p}{\max\{w_i \log m_i : 1 \leq i \leq n\}}$$

Remark. If the parameters p and q are equal, we can set $m'_i = m_i^{w_i}$ such that $\{p, m'_1, \ldots, m'_n\}$ became a standard CRT secret sharing scheme defined in Sect. 4.1.

4.3 Construction of a Multiple Threshold Changeable Secret Sharing Scheme

For the threshold increase problem, the basic idea of our method is the following one: to **increase** the threshold parameter from r to $r' > r$, the participants **decrease** values from w_i to $w'_i < w_i$.

For any $\phi \in (0, 1]$, we can get a $(r_0 \rightarrow \mathbf{r}, n)$-threshold changeable scheme, such that the security rate is at least ϕ and the information rate ρ is at least $\frac{r_0}{r_c\,\phi}$. So, the bound constructed in Theorem 2 is met with equality.

Suppose the secret value is s, we can assume that $0 \leq s < B$. Let $w_{i,j}$ denote the value of w_i after the j-th transitions (the i-th share of scheme Π_j), for $1 \leq i \leq n$ and $0 \leq j \leq c$. Let ϕ be any element of $(0, 1]$. We construct our scheme as follows:

1. GC(s)(Public Parameter Generation)
   (a) Pick any integer $u \geq \left\lceil \frac{r_c^2}{r_0} \right\rceil$, set $k = r_0 \cdot u$ and $d = k \cdot r_c$.
   (b) Pick any integer $\ell \geq r_c + \frac{\phi \cdot \log_2 B}{k} + 2\log_2 n$, choose $n+1$ distinct primes $m_0 < m_1 < \cdots < m_n$ from the interval $[2^\ell, 2^{\ell+1}]$. Estimates of the density of primes show that one could easily find primes m_i.
   (c) Pick a prime $\hat{m}$ from the interval $[2^{\ell - r_c}, 2^{\ell+1-r_c}]$.
   (d) Set $M = m_0^d$, $q = \hat{m}^k$ and $p = \hat{m}^{\frac{k}{\phi}}$ (we have: $p \geq 2^{(\ell - r_c)\frac{k}{\phi}} \geq 2^{\log_2 B} \geq B$).
   (e) Pick uniformly at random a number A in $[0, \frac{M}{p} - 1]$.
2. D(s,A)(Dealer Setup)
   To share secret s, set $y = s + A\,p$. Set $w_{i,0} = \left\lceil \frac{d}{r_0} \right\rceil$, and the i-th initial share is $s_{i,0} = y \bmod m_i^{w_{i,0}}$.
3. E($s_{i,j}$)(Sub-share Generation)
   To generate sub-shares, let $s_{i,j}$ denote the i-th share of Π_j (the scheme after j changes). Set $w_{i,j+1} = \left\lceil \frac{d}{r_{j+1}} \right\rceil$ and the sub-share is: $s_{i,j+1} = s_{i,j} \bmod m_i^{w_{i,j+1}}$.
4. C($s_{i,S,j}$)(Combiner)
   To recover s, it clearly suffices to find y. Suppose $S = \{v_1, \ldots, v_{r_j}\}$, if $s_{v_1,j}, \ldots, s_{v_{r_j},j}$ are known, by the Chinese remainder theorem, y is known modulo $N = \prod_{k=1}^{r_j} m_{v_k}^{w_{v_k,j}}$. We will prove that $N \geq p$ in the next section.

In this settings, only $p, q, m_1, \ldots, m_n, r_0, r_c$ need to be publicly known when setting up the original scheme. When the participants want to increase the threshold value r_i, they simply need to agree on the new value r_{i+1}. Each of them can compute his new share without any other interaction.

4.4 Scheme Analysis

In this section, we want to proof that our scheme satisfies the following three conditions at any step $j \in \{0, \ldots, c\}$.

C1 : $\forall (i, i') \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ $\gcd(m_i^{w_{i,j}}, m_{i'}^{w_{i',j}}) = 1$ for $i \neq i'$,
C2 : $\forall i \in \{1, \ldots, n\}$ $\gcd(p, m_i^{w_{i,j}}) = 1$ and $q | p$,
C3 : $\left(\forall S \in \mathfrak{S}_{r_j} : \prod_{i \in S} m_i^{w_{i,j}} \geq M \right)$ and $\left(\forall S \in \mathfrak{S}_{r_j - 1} : \prod_{i \in S} m_i^{w_{i,j}} \leq \frac{M}{q} \right)$.

For any $j \in \{0, \ldots, c\}$, conditions C1 and C2 are trivially satisfied due to the choice of $p, q, m_1, \ldots, m_n$ by the dealer. The proofs of the following two lemmas can be found in Appendix A and Appendix B respectively.

Lemma 4. *For any $j \in \{0, \ldots, c\}$, Condition* C3 *is satisfied if the following two inequalities are satisfied:*

$$\forall S \in \mathfrak{S}_{r_j} \sum_{i \in S} w_{i,j} \geq d \tag{1}$$

$$\forall S \in \mathfrak{S}_{r_j - 1} \sum_{i \in S} w_{i,j} \leq d - k \tag{2}$$

Lemma 5. *For any $j \in \{0, \ldots, c\}$,* (1) *and* (2) *hold.*

Combining Lemma 4 and Lemma 5, we can prove that the scheme satisfies the three conditions C1, C2, C3 for any $j \in \{0, \ldots, c\}$.

Our construction is a $(r_0 \rightarrow \mathbf{r}, n)$-threshold changeable scheme. The following theorem shows that it has security rate ϕ and the information rate of the scheme ρ asymptotically equals to $\frac{r_0}{r_c\,\phi}$ for any $0 < \phi \leq 1$.

Theorem 3 (Security and Information Rate). *For any $0 < \phi \leq 1$, the $(r_0 \rightarrow \boldsymbol{r}, n)$-threshold changeable scheme has security rate ϕ. In addition, it asymptotically meets with equality the upper bounds in Theorem 2.*

Proof. For any $0 < \phi \leq 1$, the security rate of the scheme is:

$$\log_p q = \frac{\log q}{\log p} = \frac{\log \hat{m}^k}{\log \hat{m}^{\frac{k}{\phi}}} = \frac{k \log \hat{m}}{\frac{k}{\phi} \log \hat{m}} = \phi$$

The information rate ρ of the scheme is:

$$\rho \geq \min_{1 \leq i \leq n} \left\{ \frac{H(\mathcal{S})}{H(S_i)} \right\} \geq \frac{\log \left(\hat{m}^{\frac{k}{\phi}} \right)}{\max\limits_{1 \leq i \leq n,\ 0 \leq j \leq c} \left\{ \log \left(m_i^{w_{i,j}} \right) \right\}} \geq \frac{(\ell - r_c)\,\frac{k}{\phi}}{\max\limits_{1 \leq i \leq n, 0 \leq j \leq c} \{(\ell+1) w_{i,j}\}}$$

Therefore, we have:

$$\rho \geq \frac{(\ell - r_c)\,\frac{k}{\phi}}{(\ell+1)\left\lceil \frac{d}{r_0} \right\rceil} \geq \frac{\ell - r_c}{\ell+1} \times \frac{r_0\,k}{r_c\,k + r_0 - 1} \times \frac{1}{\phi} \geq \frac{r_0}{r_c\,\phi} \times \frac{\ell - r_c}{\ell+1} \times \frac{k}{k + \frac{(r_0 - 1)}{r_c}}$$

For any $j \in \{0, \cdots, c\}$, it is easy to see that Π_j is a SRDCRRC-scheme (as defined in Sect.3.2). So, we have:

$$\rho \leq \frac{r_0}{r_c \phi}$$

If ℓ and k are asymptotically large, then we have:

$$\rho = \frac{r_0}{r_c \phi}$$

Note that "ℓ large" means that u is large. So, the upper bound in Theorem 2 is met with equality. □

4.5 Comparison

In this section, we want to compare our construction with previous methods from [10, 16, 13, 14, 7]. It should be remembered that ϕ is to be chosen during the set-up phase. We will see that for different values of ϕ, $\langle \Pi_0, \ldots, \Pi_c \rangle$ can be perfectly secure ($\phi = 1$), an asymptotically optimal ramp-scheme ($\phi = \frac{1}{\mathcal{T} - \mathcal{C}}$) or it can use a standard initial scheme as Π_0.

The secret sharing schemes designed in [10, 16] achieve perfect security before and after threshold modification. However, the share size has to be at least twice of the size of secret. Moreover, if we change to threshold c times, the information rate is at most $\frac{1}{c+1}$. We have the following result for our construction which is a direct consequence of Theorem 3.

Proposition 1 (Perfect Secure Changeable Scheme). *Let $\langle \Pi_0, \ldots, \Pi_c \rangle$ be a $(r_0 \rightarrow \boldsymbol{r}, n)$-threshold changeable scheme (where $\boldsymbol{r} = (r_1, \ldots, r_c)$) as constructed in Sect. 4.3. If we set $\phi = 1$, then $\langle \Pi_0, \ldots, \Pi_c \rangle$ has security rate 1 and information rate ρ such that:*

$$\frac{r_0}{r_c} \times \frac{\ell - r_c}{\ell + 1} \times \frac{k}{k + \frac{(r_0 - 1)}{r_c}} \leq \rho \leq \frac{r_0}{r_c}$$

This proposition involves that each (r_j, n)-TSS scheme Π_j achieves perfect secrecy (for any $j \in \{1, \ldots, c\}$). This means that the secret s is reconstructible from any r_j shares while no information about s leaks out from any set of $r_i - 1$ shadows.

Techniques in [13, 14] can be applied to existing schemes even if they were set up without consideration of future threshold increases. This is called the *standard initial scheme* approach. Unfortunately, those constructions have worse security. In addition, the secret recovery is only probabilistic. Our construction always guarantees s to be recovered.

We will show how to construct a threshold changeable secret sharing scheme $\langle \Pi_0, \ldots, \Pi_c \rangle$, where Π_0 is a standard CRT scheme (as defined in Sect. 4.1), for any given (r, n) and $\mathbf{r} = (r_0, \ldots, r_c)$ with $r_0 = r$. Our idea is to use the construction from Sect. 4.3 which is valid for any $(n, r_0, \ldots, r_c)$. We simply need to choose the construction parameter ϕ of $\langle \Pi_0, \ldots, \Pi_c \rangle$ so that Π_0 is standard scheme. We use the next two lemmas, the proofs of which are in Appendix C and Appendix D respectively.

Lemma 6. *For a $(r_0 \rightarrow \boldsymbol{r}, n)$-threshold changeable scheme $\langle \Pi_0, \ldots, \Pi_c \rangle$ where $\boldsymbol{r} = (r_1, \ldots, r_c)$, if we set $\phi = \frac{r_0}{r_c}$, then the initial scheme Π_0 has perfect security.*

Lemma 7. *For a $(r_0 \rightarrow \boldsymbol{r}, n)$-threshold changeable scheme $\langle \Pi_0, \ldots, \Pi_c \rangle$ where $\boldsymbol{r} = (r_1, \ldots, r_c)$, if we set $\phi = \frac{r_0}{r_c}$, then the initial scheme Π_0 is a standard* CRT *scheme.*

When a secret sharing is set-up, the dealer ignores what security level will be required in the future. Thus, the value r_c is a priori unknown. We would like to emphasized that this issue can be overcome easily. Indeed, when setting-up the scheme the dealer simply consider the pair $(r_0, r_{c'})$ where $r_{c'} = n$. He can construct $\langle \Pi_0, \Pi_{c'} \rangle$. When the different threshold updates occur, the participants can recursively construct $\langle \Pi_0, \Pi_1, \Pi_{c'} \rangle$, $\langle \Pi_0, \Pi_1, \Pi_2, \Pi_{c'} \rangle, \ldots, \langle \Pi_0, \Pi_1, \Pi_2, \ldots, \Pi_{c'} \rangle$ without interacting with the dealer. Note that this technique allows to design an (intermediate) SSS for any threshold value from $\{r_0 + 1, \ldots, n\}$.

We can use our method to construct an asymptotically optimal $(\mathcal{C}, \mathcal{T}, n)$-ramp scheme Π. The idea of our construction is the following one. Set $\phi = \frac{1}{\mathcal{T} - \mathcal{C}}$, and use our method from Sect. 4.3 to construct an $((\mathcal{C} - 1) \rightarrow \mathcal{T}, n)$-threshold changeable scheme

$\hat{\pi} = \langle \Pi_0, \Pi_1 \rangle$ where $\Pi = \Pi_1$. We have the following result, the proof of which is in Appendix E.

Theorem 4. *The secret sharing scheme Π constructed by the previous method is asymptotically an optimal $(\mathcal{C}, \mathcal{T}, n)$-ramp scheme.*

5 Conclusion

In this paper, we first studied the properties of threshold changeable schemes. We deduced some bounds on the information and security rates for these constructions. Second, we introduce a new CRT-based secret sharing, allowing multiple threshold changes after the original set-up phase without requiring any interactions with the dealer. One benefit of our construction is that the secret is always guaranteed to be recovered after any threshold update contrary to [13, 14] where recovery is only probabilistic. We also demonstrated that a suitable choice of the security rate ϕ led to a perfectly secure construction. As in [13, 14], a point of interest to further investigate is to deal with malicious participants who deviate from the threshold update protocol.

Acknowledgments

The authors would like to thank Professor Xiaoming Sun for valuable discussions on secret sharing. The authors are also grateful to the anonymous reviewers for their comments to improve the quality of this paper. The two authors' work was supported by the National Natural Science Foundation of China grant 60553001 and the National Basic Research Program of China grants 2007CB807900 and 2007CB807901. Christophe Tartary's research was also financed by the Ministry of Education of Singapore under grant T206B2204.

References

[1] Asmuth, C., Bloom, J.: A modular approach to key safeguarding. IEEE Transactions on Information Theory IT-29(2), 208–210 (1983)
[2] Barwick, S.G., Jackson, W.-A., Martin, K.M.: Updating the parameters of a threshold scheme by minimal broadcast. IEEE Transactions on Information Theory 51(2), 620–633 (2005)
[3] Blakley, G.R.: Safeguarding cryptographic keys. In: AFIPS 1979 National Computer Conference, New York, USA, June 1979, pp. 313–317. AFIPS Press (1979)
[4] Blakley, G.R., Meadows, C.: Security of ramp schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 242–268. Springer, Heidelberg (1985)
[5] Blundo, C., Cresti, A., De Santis, A., Vaccaro, U.: Fully dynamic secret sharing schemes. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 110–125. Springer, Heidelberg (1994)
[6] Desmedt, Y., Jajodia, S.: Redistributing secret shares to new access structures and its applications. Technical Report ISSE TR-97-01, George Mason university (1997)
[7] Jackson, W.-A., Martin, K.M.: A combinatorial interpretation of ramp schemes. Australasian Journal of Combinatorics 14, 51–60 (1996)

[8] Maeda, A., Miyaji, A., Tada, M.: Efficient and unconditionally secure verifiable threshold changeable scheme. In: Varadharajan, V., Mu, Y. (eds.) ACISP 2001. LNCS, vol. 2119, pp. 402–416. Springer, Heidelberg (2001)
[9] Martin, K.: Untrustworthy participants in secret sharing schemes. In: Cryptography and Coding III, vol. 45, pp. 255–264. Oxford University Press, Oxford (1993)
[10] Martin, K.M., Pieprzyk, J., Safavi-Naini, R., Wang, H.: Changing thresholds in the absence of secure channels. Australian Computer Journal 31, 34–43 (1999)
[11] Martin, K.M., Safavi-Naini, R., Wang, H.: Bounds and techniques for efficient redistribution of secret shares to new access structures. The Computer Journal 42(8), 638–649 (1999)
[12] Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)
[13] Steinfeld, R., Pieprzyk, J., Wang, H.: Lattice-based threshold-changeability for standard CRT secret-sharing schemes. Finite Field and their Applications 12, 653–680 (2006)
[14] Steinfeld, R., Wang, H., Pieprzyk, J.: Lattice-based threshold-changeability for standard Shamir secret-sharing schemes. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 170–186. Springer, Heidelberg (2004)
[15] Stinson, D.R.: Cryptography: Theory and Practice. 3rd edn. Chapman & Hall/CRC, Boca Raton (2006)
[16] Tamura, Y., Tada, M., Okamoto, E.: Update of access structure in Shamir's (k, n) threshold scheme. In: The 1999 Symposium on Cryptography and Information Security, Kobe, Japan, January 1999, vol. I, pp. 469–474 (1999)

A Proof of Lemma 4

Let S be any element of $\mathfrak{S}_{r_j}$. We have: $\forall i \in \{1, \ldots, n\}\, m_i > m_0$. Thus, if we have $\sum_{i \in S} w_{i,j} \geq d$ then we obtain: $\prod_{i \in S} m_i^{w_{i,j}} \geq m_0^d \geq M$.

Let S be any element of $\mathfrak{S}_{r-1}$. Assume that $\sum_{i \in S} w_{i,j} \leq d - k$. We get:

$$\prod_{i \in S} m_i^{w_{i,j}} \leq \prod_{i \in S} (2^{\ell+1})^{w_{i,j}} \leq 2^{(\ell+1)\sum_{i \in S} w_{i,j}} \leq 2^{(\ell+1)(d-k)} \leq \frac{2^{\ell d}}{\left(2^{\ell+1-\frac{d}{k}}\right)^k} \leq \frac{2^{\ell d}}{(2^{\ell+1-r_c})^k}$$

So, we have:

$$\prod_{i \in S} m_i^{w_{i,j}} \leq \frac{M}{q}$$

.

B Proof of Lemma 5

We first demonstrate that (1) holds. Let j be any element of $\{0, \ldots, c\}$ and let S be any element of $\mathfrak{S}_{r_j}$. We have:

$$\sum_{i \in S} w_{i,j} \geq r_j \left\lceil \frac{d}{r_j} \right\rceil \geq d$$

Now, we want to demonstrate (2). We consider $j = c$. Let S be any element of $\mathfrak{S}_{r_c}$. We have:

$$\sum_{i \in S} w_{i,j} = (r_c - 1) \left\lceil \frac{d}{r_c} \right\rceil = (r_c - 1)\, k = d - k$$

Assume that $j \in \{0, \ldots, c-1\}$. We have:

$$k \geq r_0 \left\lceil \frac{r_c^2}{r_0} \right\rceil \geq r_0 \left\lceil \frac{1}{r_0} \times \frac{(r_{c-1} - 1)^2}{r_c - r_{c-1}} \right\rceil \geq \frac{(r_{c-1} - 1)^2}{r_c - r_{c-1}} \geq \frac{(r_j - 1)^2}{r_c - r_j}$$

In addition, we have the following bound:

$$\left\lceil \frac{d}{r_j} \right\rceil \leq \left\lfloor \frac{d + r_j - 1}{r_j} \right\rfloor \leq \frac{d + r_j - 1}{r_j}$$

Let S be any element of $\mathcal{S}_{r_j}$, we have:

$$\begin{aligned}
\sum_{i \in S} w_{i,j} &\leq (r_j - 1) \left\lceil \frac{d}{r_j} \right\rceil \\
&\leq (r_j - 1)\, \frac{d + r_j - 1}{r_j} \\
&\leq \frac{(r_j - 1)(k\, r_c + r_j - 1)}{r_j} \\
&\leq k\, r_c - \frac{k\, r_c - r_j^2 + 2 r_j - 1}{r_j} \\
&\leq d - \frac{k\, r_c - (r_j - 1)^2}{r_j} \\
&\leq d - k \left(\frac{r_c}{r_j} - \frac{(r_j - 1)^2}{k\, r_j} \right)
\end{aligned}$$

If $r_j = 1$ then, we have:

$$\sum_{i \in S} w_{i,j} \leq d - k\, \frac{r_c}{r_j} \leq d - k$$

Otherwise, we have:

$$\sum_{i \in S} w_{i,j} \leq d - k \left(\frac{r_c}{r_j} - \frac{(r_j - 1)^2}{\frac{(r_j - 1)^2}{r_c - r_j}\, r_j} \right) \leq d - k$$

C Proof of Lemma 6

Let S be any element of $\mathfrak{S}_{r_0 - 1}$. Firstly, we want to prove that $\prod_{i \in S} m_i^{w_{i,0}} \leq \frac{M}{p}$. Since $r_0 | k$, we have $r_0 | d$. Therefore:

$$w_{i,0} = \left\lceil \frac{d}{r_0} \right\rceil = \frac{d}{r_0}$$

We get:

$$\sum_{i\in S} w_{i,0} = (r_0 - 1)\frac{d}{r_0} = d - \frac{d}{r_0} = d - k\,\frac{r_c}{r_0}$$

We obtain:

$$\prod_{i\in S} m_i^{w_{i,0}} \leq \prod_{i\in S} (2^{\ell+1})^{w_{i,0}} \leq 2^{(\ell+1)\sum_{i\in S} w_{i,0}} \leq 2^{(\ell+1)(d-k\,\frac{r_c}{r_0})} \leq \frac{2^{\ell d}}{\left(2^{\ell+1-\frac{d}{\left(k\,\frac{r_c}{r_0}\right)}}\right)^{k\,\frac{r_c}{r_0}}}$$

Finally, we have:

$$\prod_{i\in S} m_i^{w_{i,0}} \leq \frac{2^{\ell d}}{\left(2^{\ell+1-\frac{d}{k}}\right)^{\frac{k}{\phi}}} \leq \frac{M}{p}$$

If only $r_0 - 1$ shares $y_{i_1}, \ldots, y_{i_{r_0-1}}$ were known, then have have the value of y modulo $N_3 = \prod_{\lambda=1}^{r_0-1} m_{i_\lambda}^{w_{i_\lambda}}$. Since $N_3 \leq \frac{M}{p}$ and $\gcd(N_3, p) = 1$, the collection of numbers n_i with $n_i \equiv y \bmod N_3$ and $n_i \leq M$ cover all congruence classes mod p, with each class containing at most one more or one less n_i than any other class. Thus, no useful information(even probabilistic) is available without r shares. Therefore, the initial scheme Π_0 is perfect.

D Proof of Lemma 7

Set $m'_i = m_i^{w_{i,0}}$. Since $\{p, m_1, \ldots, m_n\}$ are pairwise coprime, we always have pairwise coprime integers $\{p, m'_1, \ldots, m'_n\}$. Now, we want to prove that the integers $\{p, m'_1, \ldots, m'_n\}$ satisfy the following conditions:

$$\left(\forall S \in \mathfrak{S}_r \prod_{i\in S} m'_i \geq M\right) \text{ and } \left(\forall S \in \mathfrak{S}_{r-1} \prod_{i\in S} m'_i \leq \frac{M}{p}\right)$$

According to Lemma 4 and Lemma 5, we have:

$$\forall S \in \mathfrak{S}_r \quad \prod_{i\in S} m_i \geq M$$

Using the result in the proof of Lemma 6, we get:

$$\forall S \in \mathfrak{S}_{r-1} \quad \prod_{i\in S} m_i \leq \frac{M}{p}$$

Therefore, Π_0 is a standard CRT scheme.

E Proof of Theorem 4

Let S_i denote the i-th share of Π. For $|\mathcal{A}| = \mathcal{R}, \mathcal{C} \leq \mathcal{R} \leq \mathcal{T}$, we have

$$H(\mathcal{S}|S_{\mathcal{A}}) = \min \left\{ 1, \frac{\log \left(\frac{M}{\prod_{i \in A} m_i^k} \right)}{\log \hat{m}^{\frac{k}{\phi}}} \right\} H(\mathcal{S})$$

$$= \min \left\{ 1, \frac{d \log m_0 - \sum_{i \in A} (k \log m_i)}{\frac{k}{\phi} \log \hat{m}} \right\} H(\mathcal{S})$$

So, we have:

$$H(\mathcal{S}|S_{\mathcal{A}}) \geq \min \left\{ 1, \frac{\ell\, d - \mathcal{R}\, k\, (\ell + 1)}{k\, (\ell - \mathcal{T} + 1)\, (\mathcal{T} - \mathcal{C})} \right\} H(\mathcal{S})$$

$$\geq \min \left\{ 1, \frac{\ell\, \mathcal{T} - \mathcal{R}\, (\ell + 1)}{(\ell - \mathcal{T} + 1)\, (\mathcal{T} - \mathcal{C})} \right\} H(\mathcal{S})$$

and:

$$H(\mathcal{S}|S_{\mathcal{A}}) \leq \min \left\{ 1, \frac{(\ell + 1)\, d - \mathcal{R}\, k\, \ell}{k\, (\ell - \mathcal{T})\, (\mathcal{T} - \mathcal{C})} \right\} H(\mathcal{S})$$

$$\leq \min \left\{ 1, \frac{(\ell + 1)\, \mathcal{T} - \mathcal{R}\, \ell}{(\ell - \mathcal{T})\, (\mathcal{T} - \mathcal{C})} \right\} H(\mathcal{S})$$

If ℓ is asymptotically large, then we have:

$$\frac{H(\mathcal{S}|S_{\mathcal{A}})}{H(\mathcal{S})} = \frac{\mathcal{T} - \mathcal{R}}{\mathcal{T} - \mathcal{C}}$$

Therefore, the information rate:

$$\rho = \frac{H(S_i)}{H(\mathcal{S})} = \frac{\log m_i^k}{\log \hat{m}^{\frac{k}{\phi}}} = \frac{k \log m_i}{\frac{k}{\phi} \log \hat{m}}$$

So, we have:

$$\frac{H(S_i)}{H(\mathcal{S})} \geq \frac{\ell}{(\mathcal{T} - \mathcal{C})\, (\ell - \mathcal{T} + 1)}$$

and:

$$\frac{H(S_i)}{H(\mathcal{S})} \leq \frac{\ell + 1}{(\mathcal{T} - \mathcal{C})(\ell - \mathcal{T})}$$

Finally, we deduce that, when ℓ is asymptotically large, we have:

$$\frac{H(S_i)}{H(\mathcal{S})} = \frac{1}{\mathcal{T} - \mathcal{C}}$$

Therefore, the scheme Π is an optimal ramp scheme.