Strongly Secure Ramp Secret Sharing Schemes for General Access Structures ⋆

Mitsugu Iwamoto [1] , Hirosuke Yamamoto [2]

Abstract

Ramp secret sharing (SS) schemes can be classified into strong ramp SS schemes and weak ramp SS schemes. The strong ramp SS schemes do not leak out any part of a secret explicitly even in the case that some information about the secret leaks out from some set of shares, and hence, they are more desirable than the weak ramp SS schemes. In this paper, it is shown that for any feasible general access structure, a strong ramp SS scheme can be constructed from a partially decryptable ramp SS scheme, which can be considered as a kind of SS scheme with plural secrets. As a byproduct, it is pointed out that threshold ramp SS schemes based on Shamir's polynomial interpolation method are *not* always strong.

Key words: Cryptography, Information security, Secret sharing schemes, Strong/weak ramp secret sharing schemes, General access structures.

1 Introduction

A secret sharing (SS) scheme (1; 2) is a method to encode a secret $\boldsymbol{S}$ into n shares each of which has no information of $\boldsymbol{S}$, but $\boldsymbol{S}$ can be decrypted by collecting several shares. For example, a (k, n)-threshold SS scheme means that any k out of n shares can decrypt secret $\boldsymbol{S}$ although any $k-1$ or less shares do not leak out any information of $\boldsymbol{S}$. The (k, n)-threshold access structure

⋆ This work was supported in part by the MEXT Grant-in-Aid for Scientific Research on Priority Areas of "Informatics" (Nos.14019028, 15017227) and the MEXT Grant-in-Aid for Young Scientists (B) (No.17760298).

Email addresses: `mitsugu@hn.is.uec.ac.jp` (Mitsugu Iwamoto), `Hirosuke@ieee.org` (Hirosuke Yamamoto).

[1] Graduate School of Information Systems, University of Electro-Communications, 1-5-1 Chofugaoka, Chofu-shi, Tokyo, 182-8585, Japan.

[2] Graduate School of Frontier Science, University of Tokyo. 5-1-5 Kashiwanoha, Kashiwa-shi, Chiba 277-8561, Japan.

can be generalized to so-called *general access structures* which consist of the families of *qualified sets* and *forbidden sets*. A qualified set is the subset of shares that can decrypt the secret, but any information does not leak out from any forbidden set. Generally, the efficiency of SS schemes is evaluated by the entropy of each share, and it must hold that $H(V_i) \geq H(\boldsymbol{S})$ where $H(\boldsymbol{S})$ and $H(V_i)$ are the entropies of secret $\boldsymbol{S}$ and shares V_i, $i = 1, 2, \ldots, n$, respectively (3; 4).

In order to improve the efficiency of SS schemes, *ramp* SS schemes are proposed, which have a trade-off between security and coding efficiency (5; 6; 7; 8; 9). In ramp SS schemes, we can consider *intermediate* sets, which are neither qualified nor forbidden sets, and hence, leak out partly the information of secret $\boldsymbol{S}$. For instance, in the (k, L, n)-threshold ramp SS scheme (5; 6), we can decrypt $\boldsymbol{S}$ from arbitrary k or more shares, but no information of $\boldsymbol{S}$ can be obtained from any $k - L$ or less shares. Furthermore, an arbitrary set of $k - \ell$ shares is an intermediate set which leaks out about $\boldsymbol{S}$ with equivocation $(\ell/L)H(\boldsymbol{S})$ for $\ell = 1, 2, \ldots, L$. In the case of $L = 1$, the (k, L, n)-threshold ramp SS scheme reduces to the ordinal (k, n)-threshold SS scheme. Hence, to distinguish ordinal SS schemes with ramp SS schemes, we call ordinal SS schemes *perfect* SS schemes. For any (k, L, n)-threshold access structure, we can realize that $H(V_i) = H(\boldsymbol{S})/L$ (6), and hence, ramp SS schemes are more efficient than perfect SS schemes (5; 6). Furthermore, ramp schemes with general access structures are studied in (7; 9; 8).

Since intermediate sets in ramp SS schemes are allowed to leak out a part of a secret, it is important to analyze how the secret partially leaks out. For example, if a secret is a personal data that consists of name, address, job, income, bank account, etc., any part of the secret should not leak out explicitly. However, in the case that the security is measured by the conditional entropy, we cannot know whether or not some part of the secret can be decrypted from an intermediate set. Hence, Yamamoto introduced the notion of *strong* and *weak* ramp SS schemes (6). A ramp SS scheme is called a strong ramp SS scheme if it does not leak out any part of a secret explicitly from any intermediate set of shares. A ramp SS scheme is weak if it is not strong. But, it is not given how to construct strong ramp SS schemes for arbitrarily given general access structures although it is known for (k, L, n)-threshold ramp SS schemes in (6).

In this paper, we discuss strong ramp SS schemes with general access structures. In section 2, we define ramp SS schemes called *partially decryptable* (PD) ramp SS schemes, in which every intermediate set can decrypt explicitly some parts of a secret. Then, we point out that (k, L, n)-threshold ramp SS schemes based on Shamir's polynomial interpolation method are not always strong. In section 3, we propose how to convert PD ramp SS schemes into strong ramp SS schemes by using a linear transformation, and we clarify that any access structure can be realized as a strong ramp SS scheme if it can be realized as a weak ramp SS scheme.

2 Background and Preliminaries

Let $\boldsymbol{V} = \{V_1, V_2, \ldots, V_n\}$ be the set of all shares, and let $2^{\boldsymbol{V}}$ be the family of all the subsets of $\boldsymbol{V}$. Denote a secret by an L-tuple $\boldsymbol{S} = \{S_1, S_2, \ldots, S_L\}$, and each element of $\boldsymbol{S}$ is assumed to be a mutually independent random variable according to the uniform distribution which takes values in a finite field $\mathbb{F}$. We assume that $|\mathbb{F}|$ is sufficiently large[3]. Then, denote by $H(\boldsymbol{S})$ and $H(\boldsymbol{A})$ the entropies of the secret $\boldsymbol{S}$ and a set of shares $\boldsymbol{A} \subseteq \boldsymbol{V}$, respectively.

For families $\mathcal{A}_\ell \subseteq 2^{\boldsymbol{V}}$, $\ell = 0, 1, \ldots, L$, which satisfy $\mathcal{A}_\ell \cap \mathcal{A}_{\ell'} = \emptyset$ for $\ell \neq \ell'$ and $\bigcup_{\ell=0}^{L} \mathcal{A}_\ell = 2^{\boldsymbol{V}}$, we define ramp SS schemes as follows:

Definition 1 *Let $\boldsymbol{S}$ and $\Gamma_L = \{\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_L\}$ be a given secret and a given access structure, respectively. Then, $\{\boldsymbol{S}, \boldsymbol{V}, \Gamma_L\}$ is called a* ramp secret sharing *scheme if every subset $\boldsymbol{A} \in \mathcal{A}_\ell$ satisfies the following for $\ell = 0, 1, \ldots, L$.*

$$H(\boldsymbol{S}|\boldsymbol{A}) = \frac{L-\ell}{L} H(\boldsymbol{S}). \tag{1}$$

□

Equation (1) implies that secret $\boldsymbol{S}$ leaks out from any set $\boldsymbol{A} \in \mathcal{A}_\ell$ with the amount of $(\ell/L)H(\boldsymbol{S})$. Especially, $\boldsymbol{S}$ can be completely decrypted from any $\boldsymbol{A} \in \mathcal{A}_L$, but any $\boldsymbol{A} \in \mathcal{A}_0$ leaks out no information of $\boldsymbol{S}$. Hence, in the case of $L = 1$, ramp SS schemes reduce to perfect SS schemes.

For example, the access structure of a (k, L, n)-threshold ramp SS scheme (5; 6) can be defined as $\mathcal{A}_0 = \{\boldsymbol{A} : 0 \leq |\boldsymbol{A}| \leq k - L\}$, $\mathcal{A}_\ell = \{\boldsymbol{A} : |\boldsymbol{A}| = k - L + \ell\}$ for $1 \leq \ell \leq L - 1$, and $\mathcal{A}_L = \{\boldsymbol{A} : k \leq |\boldsymbol{A}| \leq n\}$. It is shown in (7) that ramp SS schemes with general access structures can be constructed if and only if the following monotonicity condition is satisfied.

Theorem 2 ((7)) *A ramp SS scheme with access structure $\Gamma_L = \{\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_L\}$ can be constructed if and only if each $\tilde{\mathcal{A}}_\ell \overset{\text{def}}{=} \bigcup_{k=\ell}^{L} \mathcal{A}_k$, $\ell = 1, 2, \ldots, L$ satisfies*

[3] Throughout this paper, a set of shares and a family of share sets are represented by upper case bold-face and calligraphic font letters, respectively. For simplicity of notation, we use $\boldsymbol{AB}$ to represent $\boldsymbol{A} \cup \boldsymbol{B}$ for sets $\boldsymbol{A}$ and $\boldsymbol{B}$, and $\{V\}$ is represented as V. For example, $\boldsymbol{A}V = \boldsymbol{A} \cup \{V\}$. Furthermore, let $\boldsymbol{A} - \boldsymbol{B}$ be a difference set of $\boldsymbol{A}$ and $\boldsymbol{B}$, and the cardinality of a set $\boldsymbol{A}$ is denoted by $|\boldsymbol{A}|$.

the monotonicity *in the following sense:*

$$\boldsymbol{A} \in \tilde{\mathcal{A}}_\ell \;\Rightarrow\; \boldsymbol{A}' \in \tilde{\mathcal{A}}_\ell \textit{ for all } \boldsymbol{A}' \supseteq \boldsymbol{A}. \tag{2}$$

□

In the case of $L = 1$, (2) in Theorem 2 coincides with the necessary and sufficient condition to realize a perfect SS scheme with an access structure $\Gamma_1 = \{\mathcal{A}_0, \mathcal{A}_1\}$, which is proved in (10).

From Theorem 2, the *minimal* access structure $\mathcal{A}_\ell^-$, $\ell = 1, 2, \ldots, L$ can be defined as follows:

$$\mathcal{A}_\ell^- = \{\boldsymbol{A} \in \mathcal{A}_\ell : \boldsymbol{A} - \{V\} \notin \mathcal{A}_\ell \text{ for any } V \in \boldsymbol{A}\}. \tag{3}$$

Proof of Theorem 2 ((7)): We will prove only the sufficiency of (2) because the necessity is obvious. Let $\boldsymbol{S} = \{S_1, S_2, \ldots, S_L\}$ be a secret. From (10), in the case that (2) holds, we can construct a perfect SS scheme for the secret S_ℓ with the access structure $\tilde{\Gamma}_\ell \overset{\text{def}}{=} \{2^{\boldsymbol{V}} - \tilde{\mathcal{A}}_\ell, \tilde{\mathcal{A}}_\ell\}$ for every $\ell = 1, 2, \ldots, L$. Then, let $\tilde{\boldsymbol{V}}_\ell \overset{\text{def}}{=} \{V_{\ell,1}, V_{\ell,2}, \ldots, V_{\ell,n}\}$ be the whole shares of such a perfect SS scheme with access structure $\tilde{\Gamma}_\ell$ for the secret S_ℓ.

Now, we define $\boldsymbol{V}_i \overset{\text{def}}{=} \{V_{1,i}, V_{2,i}, \ldots, V_{L,i}\}$ by collecting the i-th share of $\tilde{\boldsymbol{V}}_\ell$, $\ell = 1, 2, \ldots, L$. Then, it is easy to check that the share set $\boldsymbol{V} = \{\boldsymbol{V}_1, \boldsymbol{V}_2, \ldots, \boldsymbol{V}_n\}$ realizes the ramp SS scheme with access structure Γ_L for the secret $\boldsymbol{S}$. In this case, we can decrypt $\{S_1, S_2, \ldots, S_\ell\}$ from a share set $\boldsymbol{A} \in \tilde{\mathcal{A}}_\ell$, although $\boldsymbol{A}$ does not leak out any information of $\{S_\ell, S_{\ell+1}, \ldots, S_L\}$, and hence, (1) is satisfied. □

The method shown in the above proof, say KOSOT method, can construct a ramp SS scheme for any ramp access structure satisfying (2). But, we note that the ramp SS scheme constructed by KOSOT method is not efficient generally. In ramp SS schemes, the *coding rate* of the i-th share can be defined as $\rho_i \overset{\text{def}}{=} H(V_i)/H(\boldsymbol{S})$, which should be as small as possible to realize efficient ramp SS schemes. It is known that $\rho_i \geq 1/L$ must hold for each $i = 1, 2, \ldots, n$ in any ramp SS scheme with L-level access structure Γ_L (6; 7) and the equality $\rho_i = 1/L$ can always be attained for any (k, L, n)-threshold ramp access structure (6; 5). But, KOSOT method can attain only $\rho_i \geq H(\boldsymbol{V}_i)/H(\boldsymbol{S}) = 1$. For instance, the following example shows that there exists a ramp SS scheme with a general access structure, which is more efficient than the ramp SS scheme constructed by KOSOT method.

Example 3 *Consider the following access structure Γ_3^{ex} for the set of shares*

$\boldsymbol{V} = \{V_1, V_2, V_3, V_4\}$.

$$\begin{aligned} \mathcal{A}_3^- &= \{\{V_1, V_2, V_3, V_4\}\}, & (4)\\ \mathcal{A}_2^- &= \{\{V_1, V_2, V_4\}, \{V_1, V_3, V_4\}, \{V_2, V_3, V_4\}\}, & (5)\\ \mathcal{A}_1^- &= \{\{V_1, V_2\}, \{V_1, V_3\}, \{V_2, V_4\}, \{V_3, V_4\}\}, & (6) \end{aligned}$$

Then, by letting the secret be $\boldsymbol{S} = \{S_1, S_2, S_3\}$*, a ramp SS scheme for the access structure* Γ_3^{ex} *in (4)–(6) can be realized as*

$$\begin{aligned} V_1 &= \{R_1 + S_1\}, & (7)\\ V_2 &= \{R_2 + S_2, R_1\}, & (8)\\ V_3 &= \{R_3 + S_3, R_1\}, & (9)\\ V_4 &= \{R_2, R_3\}, & (10) \end{aligned}$$

where R_1*,* R_2*, and* R_3 *are mutually independent random numbers which take values in the same finite field* $\mathbb{F}$*. In this example, it holds that* $\rho_1 = 1/3$ *and* $\rho_2 = \rho_3 = \rho_4 = 2/3$*, i.e., we can attain* $\rho_i < 1$ *for all* i*.*

It is obvious that the secret S_1 *can be decrypted from* $\{V_1, V_2\}$*, but any information of* S_2 *and* S_3 *cannot be obtained from the set. Hence, since* S_1*,* S_2 *and* S_3 *are mutually independent, it holds that* $H(\boldsymbol{S}|V_1V_2) = H(S_2S_3) = (2/3)H(\boldsymbol{S})$*. Similarly, we can easily check that* $H(\boldsymbol{S}|V_1V_3) = H(\boldsymbol{S}|V_2V_4) = H(\boldsymbol{S}|V_3V_4) = (2/3)H(\boldsymbol{S})$ *and* $H(\boldsymbol{S}|V_1V_2V_4) = H(\boldsymbol{S}|V_1V_3V_4) = H(\boldsymbol{S}|V_2V_3V_4) = (1/3)H(\boldsymbol{S})$*.* □

In the same way as Example 3, if the partial information of the secret can be explicitly decrypted from every intermediate set of shares, it is easy to calculate the amount of leaked information.

Hence, we give the definition of the partially decryptable ramp SS schemes, which characterizes the ramp SS schemes constructed by KOSOT method or shown in Example 3.

Definition 4 *Let* $\boldsymbol{S} = \{S_1, S_2, \ldots, S_L\}$ *be a secret for an access structure* $\Gamma_L = \{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_L\}$*. Then,* $\{\boldsymbol{S}, \boldsymbol{V}, \Gamma_L\}$ *is called a* partially decryptable *(PD) ramp SS scheme if there exists a part of the secret* $\boldsymbol{S_A} \subseteq \boldsymbol{S}$ *satisfying that*

$$\begin{aligned} |\boldsymbol{S_A}| &= \ell & (11)\\ H(\boldsymbol{S_A}|\boldsymbol{A}) &= 0, & (12)\\ H\left(\overline{\boldsymbol{S_A}}|\boldsymbol{A}\right) &= H\left(\overline{\boldsymbol{S_A}}\right), & (13) \end{aligned}$$

for all $\boldsymbol{A} \in \mathcal{A}_\ell$ *where* $\overline{\boldsymbol{S_A}} \overset{\mathrm{def}}{=} \boldsymbol{S} - \boldsymbol{S_A}$*.* □

From (12) and (13) in Definition 4, it holds that $H(\boldsymbol{S}|\boldsymbol{A}) = H(\boldsymbol{S_A}|\overline{\boldsymbol{S_A}}\boldsymbol{A}) + H(\overline{\boldsymbol{S_A}}|\boldsymbol{A}) = H(\overline{\boldsymbol{S_A}})$, and hence, a PD ramp SS scheme satisfies Definition 1.

Remark 5 *A PD ramp SS scheme can be considered as a special case of SS schemes with L plural secrets $\boldsymbol{S} = \{S_1, S_2, \ldots, S_L\}$ (11; 12; 13). In the case of the SS schemes with plural secrets, a certain subset $\boldsymbol{S_A}$ of $\boldsymbol{S}$ must be decrypted if $\boldsymbol{A} \subseteq \boldsymbol{V}$ is a qualified set for $\boldsymbol{S_A}$. On the contrary, in the case of PD ramp SS schemes, a share set $\boldsymbol{A} \in \mathcal{A}_\ell$ decrypts some $\boldsymbol{S_A}$ which satisfies (11), i.e., $\boldsymbol{S_A}$ is not uniquely specified by the access structure Γ_L.* □

We note that the amount of the leaked information about $\boldsymbol{S}$ from a share set $\boldsymbol{A} \in \mathcal{A}_\ell$ is $(\ell/L)H(\boldsymbol{S})$ in PD ramp SS schemes. Hence, if the security is measured only by the conditional entropy as shown in (1), there is no difference between Definition 1 and Definition 4. That is, both definitions guarantee the same security in the case that $\boldsymbol{S}$ is meaningless if some part of $\boldsymbol{S}$ is missing. However, if each part of $\boldsymbol{S}$ has explicit meaning, PD ramp SS schemes are not secure, and hence, not desirable.

To overcome such defects, Yamamoto defined strong ramp SS schemes as follows (6)[4]:

Definition 6 ((6)) *Let $\boldsymbol{S} = \{S_1, S_2, \ldots, S_L\}$ and Γ_L be a secret and an access structure, respectively. Then, $\{\boldsymbol{S}, \boldsymbol{V}, \Gamma_L\}$ is called a* strong *ramp SS scheme if all $\boldsymbol{A} \in \mathcal{A}_\ell$ satisfy (1) and*

$$H(S_{j_1} S_{j_2} \cdots S_{j_{L-\ell}} | \boldsymbol{A}) = H(S_{j_1} S_{j_2} \cdots S_{j_{L-\ell}}), \tag{14}$$

for all $\{S_{j_1}, S_{j_2}, \ldots, S_{j_{L-\ell}}\} \subseteq \boldsymbol{S}$, $\ell = 0, 1, \ldots, L-1$. □

Definition 6 implies that the strong ramp SS schemes do not leak out any part of the secret explicitly from intermediate or forbidden sets. Now, from this point of view, we review the (k, L, n)-threshold SS scheme based on Shamir's interpolation method.

Remark 7 *The (k, L, n)-threshold ramp SS scheme constructed by Shamir's interpolation method (1) is not always a strong ramp SS scheme. For instance, consider a $(4, 2, 15)$-threshold ramp SS scheme by using the following polynomial of degree 3 over the finite field $\mathbb{Z}_{17}$.*

$$f(x) = S_1 + S_2 x + R_1 x^2 + R_2 x^3, \tag{15}$$

where $\boldsymbol{S} = \{S_1, S_2\}$ is a secret, and R_1 and R_2 are independent random numbers. The i-th share is given by $V_i = f(i)$. Then, from a simple calculation of V_3, V_6 and V_{15}, we have

$$5S_2 = 7V_3 + 9V_6 + V_{15}. \tag{16}$$

[4] In (6), strong ramp SS schemes are defined only for (k, L, n)-threshold ramp access structures.

This means that partial information S_2 can be decrypted completely from shares V_3, V_6 and V_{15}.

We also note that we have $H(S_\ell|V_1V_2V_3) = H(S_\ell)$ for $\ell = 1, 2$, and hence, the ramp SS scheme in this example is neither PD nor strong[5] *.* □

Remark 7 shows that it is difficult to construct strong ramp SS schemes in general. In (6), it is proposed how to construct strong (k, L, n)-threshold ramp SS schemes, but it is not known how to construct strong ramp SS schemes for general access structures.

Fortunately, PD ramp SS schemes with general access structure Γ_L can easily be constructed, for instance by KOSOT method, if Γ_L satisfies the monotonicity defined by (2) in Theorem 2. Furthermore, it is easy to calculate how much information leaks out from each intermediate set in PD ramp SS schemes. Therefore, we propose a method to construct strong ramp SS schemes with general access structures based on PD ramp SS schemes.

3 Strong Ramp Secret Sharing Schemes with General Access Structures

In this section, we propose how to construct a strong ramp SS scheme with general access structure Γ_L from a given PD ramp SS scheme with the same access structure Γ_L.

Assume that a PD ramp SS scheme with access structure $\Gamma_L = \{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_L\}$ is given for a secret $\boldsymbol{S} = \{S_1, S_2, \ldots, S_L\}$. Then, denote by $\phi_{\Gamma_L}(\boldsymbol{S}, \boldsymbol{R})$ the encoder of the PD ramp SS scheme with the access structure Γ_L for the secret $\boldsymbol{S}$, where $\boldsymbol{R}$ represents a set of random numbers used in the encoder. Then, we choose publicly an $L \times L$ non-singular matrix T and define a new encoder $\varphi_{\Gamma_L}(\boldsymbol{S}', \boldsymbol{R}) \stackrel{\text{def}}{=} \phi_{\Gamma_L}(\boldsymbol{S}'T, \boldsymbol{R})$ where $\boldsymbol{S}' = \{S'_1, S'_2, \ldots, S'_L\}$ and $\boldsymbol{S} = \boldsymbol{S}'T$ [6] .

The next theorem gives the necessary and sufficient condition of T that realizes a strong ramp SS scheme with the access structure Γ_L for secret $\boldsymbol{S}' = \{S'_1, S'_2, \ldots, S'_L\}$.

Theorem 8 *Suppose that the encoder $\phi_\Gamma(\boldsymbol{S}, \boldsymbol{R})$ of a PD ramp SS scheme with an access structure Γ_L for a secret $\boldsymbol{S}$ is given. Let $\boldsymbol{S_A}$ be the partial*

[5] In (14), a construction method is discussed for neither PD nor strong ramp SS schemes.

[6] Hereafter, for simplicity of notation, we identify the sets $\boldsymbol{S} = \{S_1, S_2, \ldots, S_L\}$ and $\boldsymbol{S}' = \{S'_1, S'_2, \ldots, S'_L\}$ with L-dimensional row vectors $[S_1 \;\; S_2 \cdots S_L]$ and $[S'_1 \;\; S'_2 \cdots S'_L]$, respectively.

information of the secret $\boldsymbol{S}$ that can be decrypted explicitly from a share set $\boldsymbol{A}$ in the PD ramp SS scheme, and denote by $\boldsymbol{I}(\boldsymbol{A})$ the set of indices of $\boldsymbol{S_A}$. Then, we construct a new encoder $\varphi_{\Gamma_L}(\boldsymbol{S}', \boldsymbol{R}) \overset{\text{def}}{=} \phi_{\Gamma_L}(\boldsymbol{S}'T, \boldsymbol{R})$ for a new secret $\boldsymbol{S}' = \{S'_1, S'_2, \ldots, S'_L\}$ by using a publicly opened $L \times L$ non-singular matrix T.

Then, the necessary and sufficient condition of T to realize a strong ramp SS scheme $\{\boldsymbol{S}', \boldsymbol{V}, \Gamma_L\}$ is given by

$$\text{rank}\ \left[T^{-1}\right]^{\langle\{1,2,\ldots,L\}-\boldsymbol{I}(\boldsymbol{A})\rangle}_{\langle j_1,j_2,\ldots,j_{L-\ell}\rangle} = L - \ell, \tag{17}$$

for all $\boldsymbol{A} \in \mathcal{A}_\ell$, $\ell = 0, 1, \ldots, L$, where $[T^{-1}]^{\langle i_1,i_2,\ldots,i_u\rangle}_{\langle j_1,j_2,\ldots,j_u\rangle}$ is the minor that consists of the i_1-th, i_2-th, $\ldots, i_u$-th rows, and the j_1-th, j_2-th, $\ldots, j_u$-th columns of T^{-1}.
□

Remark 9 *Theorem 8 implies that any strong ramp SS schemes can be derived from the corresponding PD ramp SS schemes* without *loss of coding rates.*
□

Proof of Theorem 8: Since the matrix T is non-singular, $\boldsymbol{S}$ has one to one correspondence with $\boldsymbol{S}'$. Hence, $\boldsymbol{S}'$ is also a set of L mutually independent random variables according to the same uniform distribution. Therefore, it holds that $H(\boldsymbol{S}) = H(\boldsymbol{S}') = L \log|\mathbb{F}|$ where $\mathbb{F}$ is a finite field in which S_ℓ, $\ell = 1, 2, \ldots, L$ take values.

Then, for any $\boldsymbol{A} \in \mathcal{A}_\ell$, $\ell = 1, 2, \ldots, L$, where $\Gamma_L = \{\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_L\}$ is the access structure of the PD ramp SS scheme, we have

$$H(\boldsymbol{S}'|\boldsymbol{A}) = H(\boldsymbol{S}|\boldsymbol{A}) = \frac{L-\ell}{L} H(\boldsymbol{S}) = (L-\ell)\log|\mathbb{F}| = \frac{L-\ell}{L} H(\boldsymbol{S}'). \tag{18}$$

Therefore, (1) holds for secret $\boldsymbol{S}'$. Next, we have for any $\{S'_{j_1}, S'_{j_2}, \ldots, S'_{j_{L-\ell}}\} \subseteq \boldsymbol{S}'$ that

$$\begin{aligned} H(S'_{j_1}S'_{j_2}\cdots S'_{j_{L-\ell}}|\boldsymbol{A}) &= H\left(\boldsymbol{S}\left[T^{-1}\right]^{\langle 1,2,\ldots,L\rangle}_{\langle j_1,j_2,\ldots,j_{L-\ell}\rangle}\middle|\,\boldsymbol{A}\right) \\ &\overset{\text{(a)}}{=} H\left(\overline{\boldsymbol{S_A}}\left[T^{-1}\right]^{\langle\{1,\ldots,L\}-\boldsymbol{I}(\boldsymbol{A})\rangle}_{\langle j_1,j_2,\ldots,j_{L-\ell}\rangle}\middle|\,\boldsymbol{A}\right) \\ &\overset{\text{(b)}}{=} H\left(\overline{\boldsymbol{S_A}}\middle|\,\boldsymbol{A}\right) \\ &\overset{\text{(c)}}{=} H\left(\overline{\boldsymbol{S_A}}\right) = (L-\ell)\log|\mathbb{F}| = H(S'_{j_1}S'_{j_2}\cdots S'_{j_{L-\ell}}). \end{aligned} \tag{19}$$

where equalities (a), (b), and (c) hold because of (12), (17) and (13), respectively. Hence, (14) is satisfied, which implies that (17) is sufficient.

Finally, we note that the necessity of (17) is obvious since equality (b) in (19) does not hold if (17) is not satisfied. □

From the proof of Theorem 8, it is sufficient to choose the matrix T satisfying, instead of the condition (17), that every minor of T^{-1} has the full rank. We note that the *Hilbert matrix* T_H has such a property. Each element of an $L \times L$ Hilbert matrix $T_H = [t_{ij}]_{\substack{1 \le i \le L \\ 1 \le j \le L}}$ is given by

$$t_{ij} = \frac{1}{x_i + y_j}, \tag{20}$$

where x_i and y_j must satisfy for all $i, j \in \{1, 2, \ldots, L\}$ that

$$x_i + y_j \neq 0. \tag{21}$$

Note that every minor of the Hilbert matrix is also a Hilbert matrix, and the determinant of the matrix T_H can be calculated as follows:

$$\det T_H = \frac{\displaystyle\prod_{1 \le i < j \le L} (x_i - x_j) \prod_{1 \le i < j \le L} (y_i - y_j)}{\displaystyle\prod_{i=1}^{L} \prod_{j=1}^{L} (x_i + y_j)}. \tag{22}$$

Hence, it is clear that every minor of T_H is non-singular if and only if

$$x_i \neq x_j \quad \text{and} \quad y_i \neq y_j \tag{23}$$

are satisfied for $i \neq j$ in addition to (21). Since $|\mathbb{F}|$ is usually assumed to be sufficiently large in ordinal ramp SS schemes, it is easy to choose $\{x_i\}_{i=1}^{L}$ and $\{y_i\}_{i=1}^{L}$ satisfying (21) and (23).

We also note from the proof of Theorem 2 that a PD ramp SS scheme can always be constructed by KOSOT method if the monotonicity condition is satisfied. Therefore, from Theorem 8, the following theorem holds.

Theorem 10 *A strong ramp SS scheme with access structure Γ_L can be constructed if and only if each $\tilde{\mathcal{A}}_\ell$, $\ell = 1, 2, \ldots, L$, satisfies the monotonicity defined by (2) in Theorem 2.* □

Example 11 *Let us consider the access structure Γ_3^{ex} shown in Example 3. Note that the inverse of a* 3×3 *Hilbert matrix is given by*

$$T_H^{\mathrm{ex}} = \begin{bmatrix} 1/1 & 1/2 & 1/3 \\ 1/2 & 1/3 & 1/4 \\ 1/3 & 1/4 & 1/5 \end{bmatrix}^{-1} = \begin{bmatrix} 9 & -36 & 30 \\ -36 & 192 & -180 \\ 30 & -180 & 180 \end{bmatrix}. \tag{24}$$

Hence, by applying the above matrix T_H^{ex} to access structure Γ_3^{ex}, the PD ramp SS scheme given by (7)–(10) can be transformed into a strong ramp SS scheme *such that* $V_1 = \{R_1 + (9S'_1 - 36S'_2 + 30S'_3)\}$*,* $V_2 = \{R_2 + (-36S'_1 + 192S'_2 - 180S'_3), R_1\}$*,* $V_3 = \{R_3 + (30S'_1 - 180S'_2 + 180S'_3), R_1\}$*, and* $V_4 = \{R_2, R_3\}$*. That is,* $\boldsymbol{V} = \{V_1, V_2, V_3, V_4\}$ *realizes a strong ramp SS scheme with access structure* Γ_3^{ex} *for secret* $\boldsymbol{S}' = \{S'_1, S'_2, S'_3\}$*.* □

Remark 12 *Note that matrices satisfying (17) may exist besides the inverse of Hilbert matrices. As an example, in the case of* $L = 2$ *and* $|\mathbb{F}| \geq 3$*, we can use the following matrix* T^{ex}*, the inverse of which is not a Hilbert matrix.*

$$T^{\mathrm{ex}} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{25}$$

Now, let us consider the case of PD ramp SS scheme $\{\boldsymbol{S}, \boldsymbol{V}, \Gamma_2^{\mathrm{ex}}\}$ *where* $\boldsymbol{S} = \{S_1, S_2\}$*,* $\boldsymbol{V} = \{V_1, V_2, V_3\}$ *and* Γ_2^{ex}*:* $\mathcal{A}_2^- = \{\{V_1, V_2, V_3\}\}$*, and* $\mathcal{A}_1^- = \{\{V_1, V_3\}, \{V_2, V_3\}\}$*. The PD ramp SS scheme* $\{\boldsymbol{S}, \boldsymbol{V}, \Gamma_2^{\mathrm{ex}}\}$ *can be realized as* $V_1 = \{R_1 + S_1\}$*,* $V_2 = \{R_2 + S_2\}$*, and* $V_3 = \{R_1, R_2\}$*, where* R_1*,* R_2 *are mutually independent random numbers. In this case, by using the matrix* T^{ex} *in (25), the PD ramp SS scheme can be transformed into a strong ramp SS scheme such that* $V_1 = \{R_1 + (S'_1 + S'_2)\}$*,* $V_2 = \{R_2 + (S'_1 - S'_2)\}$*,* $V_3 = \{R_1, R_2\}$*. We can easily check that* $\boldsymbol{V} = \{V_1, V_2, V_3\}$ *realizes a strong ramp SS scheme with access structure* Γ_2^{ex} *for secret* $\boldsymbol{S}' = \{S'_1, S'_2\}$*.*

We note here that, in the case of the access structure Γ_2^{ex}*, the minimum size of* $\mathbb{F}$ *is* 2 *in order to realize the PD ramp SS schemes for secret* $\boldsymbol{S}$*, although* $|\mathbb{F}| \geq 3$ *is required to realize a strong ramp SS schemes for* $\boldsymbol{S}'$ *if we use the transformation* T^{ex} *in (25). In this way, the minimum size of* $\mathbb{F}$ *to realize strong ramp SS schemes generally becomes larger than that required to realize PD ramp SS schemes.* □

Remark 13 *Note that the matrix* T *described in Theorem 8 is the transformation from a PD ramp SS scheme to a corresponding strong ramp SS scheme. Hence, weak but not PD ramp SS schemes as shown in Remark 7 cannot always be transformed into strong ramp SS schemes by the matrix* T *satisfying (17). For example, consider the* $(3, 2, 3)$*-threshold ramp SS scheme given by* $V_1 = S_1 + R, V_2 = S_1 + S_2 + R$*, and* $V_3 = R$*, where* R *is a random number (6). Then, these shares realize a weak but not PD ramp SS scheme. If we transform this ramp SS scheme by using* $\boldsymbol{S} = \boldsymbol{S}'T^{\mathrm{ex}}$ *where* T^{ex} *is given by (25), we have* $V_1 = S'_1 + S'_2 + R, V_2 = 2S'_1 + R$*, and* $V_3 = R$*. It is easy to check that* V_1, V_2 *and* V_3 *do not realize a strong ramp SS scheme for* $\boldsymbol{S}'$*.* □

References

[1] A. Shamir, How to share a secret, Comm. ACM 22 (11) (1979) 612–613.

[2] G. R. Blakley, Safeguarding cryptographic keys, AFIPS 1979 Nat. Computer Conf. 48 (1979) 313–317.

[3] E. D. Karnin, J. W. Greene, M. E. Hellman, On secret sharing systems, IEEE Trans. Inform. Theory 29 (1) (1983) 35–41.

[4] R. M. Capocelli, A. D. Santis, L. Gargano, U. Vaccaro, On the size of shares for secret sharing schemes, J. of Cryptology 6 (1993) 157–167.

[5] G. R. Blakley, C. Meadows, Security of ramp schemes, Advances in Cryptology-CRYPTO'84, LNCS 196, Springer-Verlag (1985) 242–269.

[6] H. Yamamoto, On secret sharing systems using (k, L, n) threshold scheme, IECE. Trans. J68–A (9) (1985) 945–952, (in Japanese). English translation: Electronics and Communications in Japan, Part I, vol. 69, no. 9, pp. 46–54, Scripta Technica, Inc., 1986.

[7] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, T. Tsujii, Nonperfect secret sharing schemes and matroids, Advances in Cryptology-EUROCRYPT'93, LNCS 765, Springer-Verlag (1993) 126–141.

[8] W. Ogata, K. Kurosawa, Some basic properties of general nonperfect secret sharing schemes, J. of Universal Computer Science 4 (8) (1998) 690–704.

[9] K. Okada, K. Kurosawa, Lower bound on the size of shares of nonperfect secret sharing schemes, Advances in Crypology-ASIACRYPT'94, LNCS 917, Springer-Verlag (1994) 34–41.

[10] M. Itoh, A. Saito, T. Nishizeki, Secret sharing scheme realizing general access structure, IEEE Globecom (1987) 99–102.

[11] C. Blundo, A. D. Santis, U. Vaccaro, Efficient sharing of many secrets, Proc. of STACS'93 LNCS 665, Springer-Verlag (1993) 692–703.

[12] C. Blundo, A. D. Santis, G. D. Crescenzo, A. G. Gaggia, U. Vaccaro, Multi-secret sharing schemes, Advances in Cryptology-CRYPTO'94, LNCS 839, Springer-Verlag (1994) 150–163.

[13] G. D. Crescenzo, Sharing one secret vs. sharing many secrets, Theoretical Computer Science (295) (2003) 123–140.

[14] K. Hirota, R. Kitahara, M. Endo, M. Yamamuro, Reconstruction control of practical information in ramp scheme, Technical Repotrt of IEICE (ISEC2003-74) (2003) 57–64, (in Japanese).