Journal of Universal Computer Science, vol. 4, no. 8 (1998), 690-704
submitted: 29/7/97, accepted: 11/8/98, appeared: 28/8/98 © Springer Pub. Co.

Some Basic Properties of General Nonperfect Secret Sharing Schemes

Wakaha OGATA
(Himeji Institute of Technology, Japan
wakaha@comp.eng.himeji-tech.ac.jp)

Kaoru KUROSAWA
(Tokyo Institute of Technology, Japan
kurosawa@ss.titech.ac.jp)

Abstract: Nonperfect secret sharing schemes (NSSs) have an advantage such that the size of shares can be shorter than that of perfect secret sharing schemes. This paper shows some basic properties of general NSS. First, we present a necessary and sufficient condition on the existence of an NSS. Next, we show two bounds of the size of shares, a combinatorial type bound and an entropy type bound. Further, we define a compact NSS as an NSS which meets the equalities of both our bounds. Then we show that a compact NSS has some special access hierarchy and it is closely related to a matroid. Verifiable nonperfect secret sharing schemes are also presented.

Key Words: secret sharing scheme, nonperfect

Category: E.3 Data encryption

1 Introduction

Secret sharing schemes permit a secret to be shared by participants in such a way that only qualified subsets of participants (access subset) can recover the secret. Secret sharing schemes are useful in the management of cryptographic keys, in multiparty protocols, and etc.

"Perfect" secret sharing schemes (PSS) have been studied extensively so far. In a perfect secret sharing scheme, any subset of participants is an access subset or a non-access subset that has absolutely no information on the secret. No subsets are allowed in between.

Blakley [Blakley 79] and Shamir [Shamir 79] introduced (k, n)-threshold secret sharing schemes independently. In such a scheme, the access subsets are all the subsets whose cardinality is more than $k-1$. A family of all the access subsets is called an access structure. A family Δ is said to be monotone if

$$A \in \Delta, A \subseteq A' \Rightarrow A' \in \Delta \ .$$

Then it was shown [Itoh et al. 87] that a perfect secret sharing scheme exists if and only if the access structure is monotone. Subsequently, Benaloh and Leichter [Benaloh, Leichter 90] gave a simpler and more efficient way to realize monotone access structures.

The most important issue of secret sharing schemes is the size of shares owned by the participants. The size of shares should be as small as possible to save resources, say, memory. In secure multi-party computations, small size of shares can reduce the communication complexity, too (see [Franklin, Yung 92]). However, for any PSS, it is known that

$$|V_i| \geq |S|, \tag{1}$$

where $|S|$ denotes the size of the secret and $|V_i|$ denotes the size of the share of participant P_i [Karnin et al. 82][Capocelli at el. 93][Kurosawa, Okada 96]. More tight lower bounds of $|V_i|$ such that

$$|V_i| > |S|$$

which depend on the access structure have also been presented [Capocelli at el. 93][Blundo at el. 92b][Brickell, Stinson 92][Blundo at el. 92a][Stinson 92]. This result means that every participants must hold very large information keeping secret. It will cost them much. If share size can be reduced then each participant save costs or obtains higher security with same cost. So, it is desired $|V_i|$ is as small as possible.

We emphasize here that $|V_i| \geq |S|$ in any PSS. Therefore, schemes which can achieve

$$|V_i| < |S|$$

must be "nonperfect", where semi-access subsets should be allowed. A semi-access subset is a set of participants who can have some information on the secret but cannot recover the secret completely. An example of nonperfect secret sharing schemes is (d, k, n)-ramp schemes [Blakley, Meadows 84] which are an extension of (k, n)-threshold schemes such as follows. In a (d, k, n)-ramp scheme,

$$B \text{ is } \begin{cases} \text{an access subset if} & |B| \geq k, \\ \text{an non-access subset if} & |B| \leq k - d. \end{cases}$$

If $k - d < |B| < k$, then B has some information about the secret, but cannot recover it.

As a practical example, let us consider the following situation. For a bank, the list of clients is an important secret. Usually, it is stored in the main computer of the headquarters of the bank. At the same time, it should be stored in the computers of the branches of the bank in case the main computer is damaged by some disaster like Kobe earthquake of 1995. However, it is dangerous to make each branch have the complete list because the security of the branches is not so high as that of the headquarters. Now assume that

1. there are 10 branches,
2. attackers can break the security of at most 5 branches,
3. any 8 branches should be able to reconstruct the list at a crucial moment.

For that purpose, we can use a $(8, 10)$-threshold scheme or a $(3, 8, 10)$-ramp scheme. Let

- S denote the list of clients and
- V_i denote the share of the i-th branch.

In the first case, the size of the share of each branch must be as large as the size of the list itself. That is,

$$\log_2 |V_i| = \log_2 |S|.$$

On the other hand, in the second case, we can have

$$\log_2 |V| = \log_2 |S|/3.$$

Thus, V_i can be smaller than that of the threshold scheme.

This paper characterizes general nonperfect secret sharing schemes. A nonperfect secret sharing scheme can be defined as $(\Gamma_1, \Gamma_2, \Gamma_3)$, where Γ_1 is a family of access subsets, Γ_2 is a family of semi-access subsets and Γ_3 is a family of non-access subsets.

(1) First, we show a necessary and sufficient condition on the existence of NSSs.

(2) Next, we show two lower bounds on $|V_i|$, a combinatorial type bound such that

$$\max_i \log_2 |V_i| \geq H(S) / \min_{A \in \Gamma_1, B \in \Gamma_3} |A \setminus C|,$$

and an entropy type bound such that

$$\log_2 |V_i| \geq \min_{B \notin \Gamma_1} H(S|B).$$

The combinatorial type bound is a generalization of [Blundo at el. 93, Theorem 3.3] which holds only for linear ramp schemes. The entropy type bound shows that there exists a tradeoff between $|V_i|$ and amount of information leakage to semi-access set.

(3) Further, we define a compact NSS as an NSS which meets the equalities of both our bounds. Then we show that a compact NSS has some special access hierarchy and it is closely related to a matroid.

(4) Verifiable nonperfect secret sharing schemes are also presented.

The rest of this paper is organized as follows. Section 2 states definitions and related works. In section 3, we show a necessary and sufficient condition on the existence of NSSs. Section 4 presents two lower bounds of the $|V_i|$. In section 5, we define a compact NSS and characterize it. Section 6 shows verifiable nonperfect secret sharing schemes. Section 7 gives some lemmas on entropy which will be used to prove the above results (Lemma 22, Lemma 23).

2 Preliminaries

$|A|$ denotes the cardinality of a set A. $A \setminus B = \{x | x \in A \text{ but } x \notin B\}$. 2^A denotes the family of all subsets of A.

2.1 Entropy

For random variables X and Y, the entropy and its variants are defined as follows. (For example, see [Gallager 68].)

$$
\begin{aligned}
H(X) &\stackrel{\triangle}{=} \sum_a -\Pr(X=a)\log\Pr(X=a),\\
H(X \mid Y=b) &\stackrel{\triangle}{=} \sum_a -\Pr(X=a)\log\Pr(X=a \mid Y=b),\\
H(X \mid Y) &\stackrel{\triangle}{=} \sum_b \Pr(Y=b)H(X \mid Y=b),\\
I(X;Y) &\stackrel{\triangle}{=} H(X) - H(X \mid Y).
\end{aligned}
$$

Then they have the following properties.

$$
\begin{aligned}
H(X|Y) &= H(XY) - H(Y),\\
I(X;Y) &= H(X) - H(X \mid Y)\\
&= H(Y) - H(Y \mid X)\\
&= H(X) + H(Y) - H(XY),\\
I(X;Y \mid Z) &= H(X \mid Z) - H(X \mid YZ).
\end{aligned}
$$

2.2 Definition of secret sharing schemes

$P = \{P_1, \ldots, P_n\}$ denotes a set of participants. s is a secret distributed over a finite set. S is a random variable induced by s. v_i is a share of P_i distributed over a finite set. V_i is a random variable induced by v_i.

Given a distribution over the secrets represented by the random variable S and a distribution over finite set of random bit-strings with random variable R, suppose that there is a mapping Π which maps a secret s and a random string r to a vector of n shares $(v_1, ..., v_n)$. That is,

$$\Pi : (s, r) \to (v_1, \ldots, v_n).$$

The distributions over the set of secrets and the set of random strings induce a distribution over these vectors of shares. Let V be the random variable over the vectors and V_i be the random variable for the i-th component induced by the construction. That is,

$$V = (V_1, \ldots, V_n).$$

Definition 1. We say that (Π, S, V) is a secret sharing scheme (SS).

The selection of shares $(v_1, ..., v_n)$ guarantees that the secret can be reconstructed given a qualified subset of shares.

Definition 2. Let $\Gamma \subseteq 2^V$. We say that (Π, S, V, Γ) is a perfect secret sharing scheme (PSS) if (Π, S, V) is a secret sharing scheme and

1. $H(S|A) = 0$ for $\forall A \in \Gamma$
   (A can recover S),
2. $H(S|C) = H(S)$ for $\forall C \notin \Gamma$
   (C has no information on S).

$A \in \Gamma$ is called an access set. $C \notin \Gamma$ is called a non-access set. Γ is called the access structure of the PSS.

Definition 3. Let $(\Gamma_1, \Gamma_2, \Gamma_3)$ be a partition of 2^V. That is, $\Gamma_1 \cup \Gamma_2 \cup \Gamma_3 = 2^V, \Gamma_1 \cap \Gamma_2 = \Gamma_2 \cap \Gamma_3 = \Gamma_3 \cap \Gamma_1 = \phi$. We say that $(\Pi, S, V, (\Gamma_1, \Gamma_2, \Gamma_3))$ is a nonperfect secret sharing scheme (NSS) if (Π, S, V) is a secret sharing scheme, $\Gamma_1 \neq \phi$ and

1. $H(S|A) = 0 \quad$ for $\forall A \in \Gamma_1$
   (A can recover S),
2. $0 < H(S|B) < H(S) \quad$ for $\forall B \in \Gamma_2$
   (B has some information on S, but cannot recover S),
3. $H(S|C) = H(S) \quad$ for $\forall C \in \Gamma_3$
   (C has no information on S).

We say that $(\Gamma_1, \Gamma_2, \Gamma_3)$ is the access structure of the NSS.

2.3 Related works

A (k, n)-threshold secret sharing scheme is a PSS such that

$$\Gamma = \{A \subseteq V \mid |A| \geq k\}.$$

Karnin et al. proved that [Karnin et al. 82]

$$\log_2 |V_i| \geq H(S) \tag{2}$$

for any (k, n)-threshold secret sharing schemes. Capocelli et al. showed that the above bound holds for any PSS [Capocelli at el. 93]. Kurosawa et al. proved that [Kurosawa, Okada 96]

$$|V_i| \geq |S| \tag{3}$$

for any PSS. This is a more tight bound than eq.(2) because $\log_2 |S| \geq H(S)$.

For PSSs with certain Γs, more tight lower bounds on $|V_i|$ than eq.(3) is known [Capocelli at el. 93] [Blundo at el. 92b] [Brickell, Stinson 92] [Blundo at el. 92a] [Stinson 92].

McEliece and Sarwate [McEliece, Sarwate 81] showed that Shamir's (k, n)-threshold secret sharing scheme [Shamir 79] is closely related to Reed Solomon codes.

A (d, k, n)-ramp scheme is an NSS such that

$$\begin{aligned}
\Gamma_1 &= \{A \subseteq V \mid |A| \geq k\}, \\
\Gamma_2 &= \{B \subseteq V \mid k - d < |B| < k\}, \\
\Gamma_3 &= \{C \subseteq V \mid |C| \geq k - d\}.
\end{aligned}$$

Blakley and Meadows [Blakley, Meadows 84] showed a (d, k, n)-ramp scheme such as follows. Let $|S| = p^d$ for some prime p, and express each secret $s = (s_0, \ldots, s_{d-1})$ where s_i is an element of $GF(p)$. To share a secret $s = (s_0, \ldots, s_{d-1})$, the dealer chooses a random polynomial over $GF(p)$ such that

$$f(x) = s_0 + s_1 x + \cdots + s_{d-1} x^{d-1} + a_d x^d + \cdots + a_{k-1} x^{k-1}.$$

He computes a share

$$v_i = f(i)$$

and gives v_i to P_i for $1 \le i \le n$. Then it is easy to see that k or more participants can recover s and $k - d$ or less participants have no information on s.

Blundo at el. showed lower bounds on $|V_i|$ for ramp schemes such as follows [Blundo at el. 93].

Proposition 4. *[Blundo at el. 93, Theorem 3.2]*
In any (d, k, n)-ramp scheme, the sum of the sizes of the shares given to any group of d participants is at least $\log |S|$.

Definition 5. A (d, k, n)-linear ramp scheme is a (d, k, n)-ramp scheme which meets the following additional property: Any set of more than $k - d$ and less that k participants might have "some" information on the secret s. Formally, for all $A \subseteq V$ with $k - d < |A| < k$, it holds that

$$H(S|A) = H(S)(k - |A|)/d.$$

Proposition 6. *[Blundo at el. 93, Theorem 3.3]*
In any (d, k, n)-linear ramp scheme,

$$H(V_i) \ge H(S)/d.$$

Shamir's (k, n)-threshold secret sharing scheme is used in multi-party protocols to cope with faulty players. Franklin and Yung used a (d, k, n)-ramp scheme to parallelize a multi-party protocol d times [Franklin, Yung 92]. Their method can reduce the communication complexity although only $k - d + 1$ faulty players can be allowed.

Brickell and Davenport [Brickell, Davenport 91] characterized ideal PSS in terms of a matroid. Kurosawa et al. generalized this result to NSSs as follows [Kurosawa et al. 93].

Definition 7. [Kurosawa et al. 93] Suppose that $S = S_1 \circ S_2 \circ \cdots \circ S_d$ and $|S_i| = |S|/d$ for all i ($\circ$ means concatenation). Let $W \stackrel{\triangle}{=} \{S_1, \ldots, S_d, V_1, \ldots, V_n\}$. We say that an SS (Π, S, V) has a *level d mixed access hierarchy* $(\hat{\Sigma}_0, \hat{\Sigma}_1, \ldots, \hat{\Sigma}_d)$ if

$$\bigcup_{i=0}^{d} \hat{\Sigma}_i = 2^W, \quad \hat{\Sigma}_i \cap \hat{\Sigma}_j = \phi \ (i \ne j) \quad \text{and}$$

$$H(S|A) = (k/d)H(S) \quad \mathit{for} \ \forall A \in \hat{\Sigma}_k \ .$$

Definition 8. [Kurosawa et al. 93] We say that an SS of a level d mixed access hierarchy is *ideal* if

$$|a| = H(a) = H(S)/d, \quad \forall a \in W \ .$$

A matroid $M = (W, \mathcal{I})$ is a finite set W and a collection $\mathcal{I}$ of subsets of W such that $(I1) \sim (I3)$ are satisfied

(I1) $\phi \in \mathcal{I}$.
(I2) If $X \in \mathcal{I}$ and $Y \subseteq X$, then $Y \in \mathcal{I}$.

(I3) If X and Y are members of $\mathcal{I}$ with $|X| = |Y|+1$, then there exists $x \in X \setminus Y$ such that $Y \cup \{x\} \in \mathcal{I}$.

Proposition 9. *[Kurosawa et al. 93] Suppose that*

1. *An SS has a level d mixed access hierarchy $(\hat{\Sigma}_0, \hat{\Sigma}_1, \ldots, \hat{\Sigma}_d)$ and the SS is ideal.*
2. *For $\forall a \in V$ such that $\{a\} \in \hat{\Sigma}_d$, there exists $B \in \hat{\Sigma}^{-}_{d-1}$ such that $a \in B$.*

Then, there exists a matroid on $W \triangleq \{S_1, \ldots, S_d, V_1, \ldots, V_n\}$ with a rank function ρ such that

(N1) $\rho(S_1 \cdots S_d) = d$.
(N2) $\rho(S_1 \cdots S_d X) - \rho(X) = k$ *if* $X \in \hat{\Sigma}_k \cap 2^V$.

(After an early version of this paper [Ogata et al. 92], Okada and Kurosawa showed a more tight lower bound on $|V_i|$ than Theorem 14 of this paper for NSSs with certain $(\Gamma_1, \Gamma_2, \Gamma_3)$ [Okada, Kurosawa 94].)

3 Monotone Property

Definition 10. A family Γ is said to be monotone if

$$A \in \Gamma, A \subseteq A' \Rightarrow A' \in \Gamma.$$

It is known that there exists a perfect secret sharing scheme (PSS), (Π, S, V, Γ) if and only if Γ is monotone [Itoh et al. 87][Benaloh, Leichter 90]. For NSSs, we show the following theorem.

Theorem 11. *Suppose that $|S| \geq 2$. Let $(\Gamma_1, \Gamma_2, \Gamma_3)$ be a partition of 2^V. Then, there exists an NSS whose access structure is $(\Gamma_1, \Gamma_2, \Gamma_3)$ if and only if both Γ_1 and $\Gamma_1 \cup \Gamma_2$ are monotone.*

Proof. First, we will prove that if there exists an NSS $(\Pi, S, V, (\Gamma_1, \Gamma_2, \Gamma_3))$ then Γ_1 and $\Gamma_1 \cup \Gamma_2$ are monotone. For all $A \in \Gamma_1$,

$$H(S|A) = 0$$

from definition of NSS. Therefore, for all $A' \supset A$,

$$\begin{aligned} H(S|A') &\leq H(S|A) = 0, \\ H(S|A') &= 0, \\ A' &\in \Gamma_1. \end{aligned}$$

This mean that Γ_1 is monotone. Similarly, $\Gamma_1 \cup \Gamma_2$ is monotone.

Next, we will prove if part. Suppose that Γ_1 and $\Gamma_1 \cup \Gamma_2$ are monotone.
(Case 1) Suppose that $|S| > 2$. Without loss of generality, we assume S is distributed over $\{0, \ldots, |S| - 1\}$. Express $s \in S$ as

$$s = 2s_1 + s_2,$$

where $s_2 = 0$ or 1 and $0 \le s_1 \le \lfloor (|S| - 1)/2 \rfloor$. Let S_1, S_2 be random variables induced by s_1, s_2 respectively. S_1 is distributed over $\{0, \ldots, \lfloor (|S| - 1)/2 \rfloor\}$ and S_2 is distributed over $\{0, 1\}$.

Since Γ_1 is monotone, there exists a PSS $(\Pi_1, S_1, V', \Gamma_1)$ for s_1, where $V' = \{V_1', \ldots, V_n'\}$ and V_i' is the random variable induced by P_i's share, v_i'. Similarly, there exists a PSS $(\Pi_2, S_2, V'', \Gamma_1 \cup \Gamma_2)$ for s_2 because $\Gamma_1 \cup \Gamma_2$ is monotone, where $V'' = \{V_1'', \ldots, V_n''\}$ and V_i'' is the random variable induced by P_i's share, v_i''. Now we consider a SS (Π, S, V) in which P_i's share is $v_i = (v_i', v_i'')$, V_i is the random variable induced by V_i and $V = (V_1, \ldots, V_n)$.

1. $\forall A \in \Gamma_1$, $H(S_1|A) = H(S_2|A) = 0$.
   So,
   $$H(S|A) = 0.$$
2. $\forall B \in \Gamma_2$, $H(S_1|B) = H(S_1), H(S_2|B) = 0$.
   So, B gets partial information for S, that is,
   $$0 < H(S|B) < H(S).$$
3. $\forall C \in \Gamma_1$, $H(S_1|C) = H(S_1), H(S_2|C) = H(S_2)$.
   So,
   $$H(S|C) = H(S).$$

Consequently, (Π, S, V) is a nonperfect secret sharing scheme whose access structure is $(\Gamma_1, \Gamma_2, \Gamma_3)$.
(Case 2) Suppose that $|S| = 2$. Consider a distribution rule such as follows.

s	0	0	0	1	1	1
s_1	0	0	0	1	1	1
s_2	0	0	1	1	1	0

That is, $S_1 = S$ and

$$\Pr(S_2 = 0|S = 0) = \frac{2}{3},$$
$$\Pr(S_2 = 1|S = 0) = \frac{1}{3},$$
$$\Pr(S_2 = 1|S = 1) = \frac{2}{3},$$
$$\Pr(S_2 = 0|S = 1) = \frac{1}{3}.$$

The rest of the proof is the same as (Case 1). □

4 Lower Bounds on the Size of the Shares

In a PSS, it is known that

$$\log_2 |V_i| \geq H(S) \tag{4}$$

if V_i belongs to some minimal access set [Karnin et al. 82][Capocelli at el. 93] [Kurosawa, Okada 96]. If S is uniformly distributed, it is well known that

$$H(S) = \log_2 |S|.$$

Therefore, $|V_i| \geq |S|$ for uniformly distributed S. (Recently, it was proved that $|V_i| \geq |S|$ even for nonuniformly distributed S [Kurosawa, Okada 96].)

An NSS has a possibility of shorter length of shares such as

$$\log_2 |V_i| < H(S).$$

In this section, we derive two types of lower bounds on $\log_2 |V_i|$ of NSSs, a combinatorial type bound and an entropy type bound.

Definition 12. We say that the NSS is *connected* if for all i,

$$\exists A \in \Gamma_1^- : \quad V_i \in A$$

where Γ_1^- is a family of minimum sets of Γ_1.

If there exists V_i which is not included in all minimum access sets, we can consider that P_i does not participate the scheme.

4.1 Combinatorial type bound

Lemma 13. *In any NSS, if $A \in \Gamma_1, C \in \Gamma_3$ and $C \subset A$, then*

$$\sum_{V_i \in A \setminus C} H(V_i) \geq H(S) \ .$$

Proof. From Lemma 23 (see Section 7),

$$H(S|A) \geq H(S|C) - \sum_{V_i \in A \setminus C} H(V_i).$$

Note that Lemma 23 requires that $C \subset A$. From Definition 3 (1) and (3),

$$\sum_{V_i \in A \setminus C} H(V_i) \geq H(S|C) - H(S|A) = H(S).$$

□

Theorem 14. *In any NSS,*

$$\max_i \log_2 |V_i| \geq H(S)/\min |A \setminus C|, \tag{5}$$

where the minimum is taken over $\forall A \in \Gamma_1$ and $\forall C \in \Gamma_3$.

(Note that $\Gamma_1 \neq \phi$ from Definition 3.)

Proof. First we assume $C \subset A$. Then, from lemma 13,

$$\sum_{V_i \in A \setminus C} H(V_i) \geq H(S) \ . \tag{6}$$

On the other hand,

$$\sum_{V_i \in A \setminus C} H(V_i) \leq |A \setminus C| \max_i \log_2 |V_i| \tag{7}$$

because $H(V_i) \leq \log_2 |V_i|$. From eq.(6) and eq.(7), we obtain

$$H(S) \leq |A \setminus C| \max_i \log_2 |V_i| \ . \tag{8}$$

Next, we assume $C \not\subset A$. Let $A' \stackrel{\triangle}{=} C \cup A$. Since Γ_1 is monotone (from Theorem 11), $A' \in \Gamma_1$. Then, from eq.(8), we have

$$H(S) \leq |A' \setminus C| \max_i \log_2 |V_i| \ . \tag{9}$$

It is clear that

$$|A \setminus C| \ = \ |A' \setminus C| \ . \tag{10}$$

From eq.(9) and eq.(10), we obtain

$$H(S) \leq |A \setminus C| \max_i \log_2 |V_i| \ .$$

Therefore, we have eq.(5). □

Corollary 15. *If S is uniformly distributed, then*

$$\max_i \log_2 |V_i| \geq \log_2 |S| / \min |A \setminus C|, \tag{11}$$

where the minimum is taken over $\forall A \in \Gamma_1$ and $\forall C \in \Gamma_3$.

Proof. If S is uniformly distributed, then

$$H(S) = \log_2 |S|.$$

Therefore, we have eq.(11). □

Remark. Lemma 13 is a generalization of Proposition 4. Theorem 14 is a generalization of Proposition 6.

4.2 Entropy type bound

Lemma 16. *For all $B \notin \Gamma_1$ and for all D such that $B \cup D \in \Gamma_1$,*

$$H(S|B) \leq \sum_{V_i \in D} \log_2 |V_i|.$$

Proof. Let $D = \{V_{i_1}, \ldots, V_{i_k}\}$.

$$0 \;=\; H(S|B \cup D) \geq H(S|B) - \sum_{j=1}^{k} H(V_{i_j}) \quad \text{(lemma 23)}$$

$$H(S|B) \leq \sum_{j=1}^{k} H(V_{i_j})$$

$$\leq \sum_{j=1}^{k} \log_2 |V_{i_j}| \;=\; \sum_{V_i \in D} \log_2 |V_i$$

□

Theorem 17. *In any connected NSS, for all i,*

$$\log_2 |V_i| \geq \min H(S|B). \tag{12}$$

The minimum is taken over all $B \notin \Gamma_1$.

Proof. In a connected NSS, for all V_i there exists $A \in \Gamma_1^-$ such that $V_i \in A$. Let

$$B \triangleq A \setminus \{V_i\}.$$

Then $B \notin \Gamma_1$ and $B \cup \{V_i\} \in \Gamma_1$. So, from lemma 16,

$$\log_2 |V_i| \geq H(S|B) \geq \min_{B \notin \Gamma_1} H(S|B).$$

□

Theorem 17 is a generalization of Eq. (4) because in a PSS, $H(S|B) = H(S)$ if $B \notin \Gamma_1$.

5 Compact NSS and Matroid

In this section, we define a compact NSS as an NSS which meets all the equalities of our bounds, Theorem 14, Theorem 17 and lemma 16. Then we show that a compact NSS has some special access hierarchy and it is closely related to a matroid.

Definition 18. Let

$$d = \min_{A \in \Gamma_1, C \in \Gamma_3} |A \setminus C|.$$

We say that a connected NSS is *compact* if

– for all i,

$$\log_2 |V_i| = \min_{B \notin \Gamma_1} H(S|B) \ = \ H(S)/d$$

– and any $B \notin \Gamma_1$ satisfies

$$H(S|B) = \min_{B \cup D \in \Gamma_1} \sum_{V_i \in D} \log_2 |V_i|. \qquad (13)$$

Theorem 19. *In a compact NSSs, for all set $B \subseteq V$, there exists an integer k such that*

$$H(S|B) = (k/d)H(S),$$

where $d = \min_{A \in \Gamma_1, C \in \Gamma_3} |A \setminus C|$.

Proof. From the definition of compact,

$$H(S|B) = \min_{B \cup D \in \Gamma_1} \sum_{V_i \in D} \log_2 |V_i| = H(S) \min_{B \cup D \in \Gamma_1} |D|/d \qquad (14)$$

for any $B \notin \Gamma_1$. □

Definition 20. [Kurosawa et al. 93] Let d be a positive integer. We say that an SS (Π, S, V) has a *level d access hierarchy* $(\Sigma_0, \Sigma_1, \ldots, \Sigma_d)$ if

$$\bigcup_{i=0}^{d} \Sigma_i = 2^V, \quad \Sigma_i \cap \Sigma_j = \phi \quad (i \neq j) \text{ and}$$

$$H(S|A) = (k/d)H(S) \quad for\ \forall A \in \Sigma_k \ .$$

A level d access hierarchy is a partition of V while a *mixed* access hierarchy of Def.7 is a partition of $W = \{S_1, \ldots, S_d, V_1, \ldots, V_n\}$.

Corollary 21. *A compact NSS has a level d access hierarchy.*

From Proposition 9, there exists a matroid if an NSS has a level d *mixed* access hierarchy and each $|V_i|$ is the minimum in the NSS. This suggests that a compact NSS is closely related to a matroid. In particular, suppose that a level d access hierarchy implies a level d *mixed* access hierarchy. (A (d, k, n)-ramp scheme has a level d *mixed* access hierarchy as well as a level d access hierarchy.) Then there exists a matroid if there exists a compact NSS.

6 Verifiable Nonperfect Secret Sharing Scheme

A verifiable secrets sharing scheme is a secrets sharing scheme such that each participant can verify the validity of his share. In other words, a dealer cannot distribute incorrect shares. Feldman showed a verifiable (k, n)-threshold secret sharing scheme in which participants are polynomially time bounded [Feldman 87]. Pedersen showed a verifiable (k, n)-threshold secret sharing scheme in which the dealer is polynomially time bounded [Pedersen 91]. Benaloh showed an interactive verifiable (k, n)-threshold secret sharing scheme which is zero knowledge [Benaloh 86].

These schemes can be easily generalized to (d, k, n)-ramp schemes. For example, we can obtain a Feldman type verifiable (d, k, n)-ramp scheme such as follows. As we noted in Sec.2.3, each secret is expressed $s = (s_0, \ldots, s_{d-1})$ and $v_i = f(i)$ for a random polynomial

$$f(x) = s_0 + \cdots + s_{d-1}x^{d-1} + a_d x^d + \cdots + a_{k-1}x^{k-1}.$$

Let g be a p-th root of unity of $GF(q)$, where $p \mid q - 1$. To verify the shares, the dealer publicizes

$$\begin{aligned} t_i &= g^{s_i} \quad \text{for } 0 \le i \le d-1, \\ u_i &= g^{a_i} \quad \text{for } d \le i \le k-1. \end{aligned}$$

Each participant P_i is convinced that v_i is a correct share if

$$g^{v_i} = t_0(t_1)^i \cdots (t_{d-1})^{i^{d-1}}(u_d)^{i^d} \cdots (u_{k-1})^{i^{k-1}}.$$

7 Some Lemmas on Entropy

In this section, we derive some useful lemmas on entropy which are used in this paper.

Lemma 22. $H(S|XW) \ge H(S|X) - H(W)$.

Proof.

$$\begin{aligned} I(S, W|X) &= H(S|X) - H(S|XW) \\ &= H(W|X) - H(W|SX) \\ &\le H(W|X) \ \le \ H(W) \end{aligned}$$

□

Lemma 23. *If* $Y = X \cup V_{i_1} \cup \cdots \cup V_{i_k}$, *then*

$$H(S|Y) \ge H(S|X) - \sum_{j=1}^{k} H(V_{i_j}).$$

Proof. From Lemma 22,

$$\begin{aligned} H(S|Y) &= H(S|XV_{i_1} \cdots V_{i_k}) \\ &\ge H(S|X) - H(V_{i_1} \cdots V_{i_k}). \end{aligned}$$

So,

$$H(S|X) - H(V_{i_1} V_{i_k}) \ge H(S|X) - \sum_{j=1}^{k} H(V_{i_j}).$$

□

Acknowledgement

The authors would like to acknowledge Koji OKADA for useful discussion.

References

[Benaloh 86] Benaloh, J.C.: "Secret sharing homomorphisms: Keeping a secret secret"; Proc. of Crypto'86, Lecture Notes on Comput. Sci., 263, Springer Verlag (1986) 251-260

[Benaloh, Leichter 90] Benaloh, J.C., Leichter, J.,: "Generalized secret sharing and monotone functions"; Proc. of Crypto'88, Lecture Notes on Comput. Sci., 403, Springer Verlag (1990) 27–36

[Berge 73] Berge, C.: "Graphs and Hypergraphs"; North Holland (1973)

[Blakley 79] Blakley, G.R.: "Safeguarding cryptographic keys"; Proc. of the AFIPS 1979 National Computer Conference 48 (1979) 313–317

[Blakley, Meadows 84] Blakley, G.R., Meadows, C.: "Security of ramp schemes"; Proc. of Crypto'84, Lecture Notes on Comput. Sci., 196, Springer Verlag (1984) 242–268

[Blundo at el. 92a] Blundo, C., De Santis, A., Gargano, L., Vaccaro, U.: "On the information rate of secret sharing schemes"; Proc. of Crypto'92, Lecture Notes on Comput. Sci., 740, Springer Verlag (1992) 148–167

[Blundo at el. 92b] Blundo, C., De Santis, A., Stinson, D.R., Vaccaro, U.: "Graph decomposition and secret sharing schemes"; Proc. of Eurocrypt'92, Lecture Notes on Comput. Sci., 658, Springer Verlag (1992) 1–20

[Blundo at el. 93] Blundo, C., De Santis, A., Vaccaro, U.: "Efficient sharing of many secrets"; Proc. of STACS'93, Lecture Notes on Comput. Sci., 665, Springer Verlag (1993) 692–703

[Brickell, Davenport 91] Brickell, E.F., Davenport, D.M.: "On the classification of ideal secret sharing schemes"; Journal of Cryptology, 4, 2 (1991) 123–134

[Brickell, Stinson 92] Brickell, E.F., Stinson, D.R.: "Some improved bounds on the information rate of perfect secret sharing schemes"; Journal of Cryptology, 5, 3 (1992) 153–166

[Capocelli at el. 93] Capocelli, R.M., De Santis, A., Gargano, L., Vaccaro, U.: "On the size of shares for secret sharing schemes"; Journal of Cryptology, 6, 3 (1993) 157–167

[Feldman 87] Feldman, P.: "Practical Scheme for Non-Interactive Verifiable Secret Sharing"; Proc. of 28th IEEE symposium on Foundations of Computer Science, (1987) 427-437

[Franklin, Yung 92] Franklin, M. and Yung, M.: "Communication Complexity of Secure Computation"; ACM STOC 1992, 699–710

[Gallager 68] Gallager, R.G.: "Information Theory and Reliable Communications"; John Wiley & Sons / New York, NY (1968)

[Itoh et al. 87] Itoh, M., Saito, A., Nishizeki, T.: *Secret sharing scheme realizing general access structure*, Proc. IEEE Global Telecommunication Conference, Globecom'87, Tokyo (1987) 99–102

[Karnin et al. 82] Karnin, E.D., Green, J.W., Hellman, M.E.: "On secret sharing systems"; IEEE Trans. on Inform. Theory, IT-29 (1982) 35–41

[Kurosawa et al. 93] Kurosawa, K., Okada, K., Sakano, K. Ogata, W., Tsujii, S.: "Nonperfect secret sharing schemes and matroids"; Proc. of Eurocrypt'93, Lecture Notes on Comput. Sci. 765, Springer Verlag (1993) 126-141

[Kurosawa, Okada 96] Kurosawa, K. and Okada, K.: "Combinatorial Lower Bounds for Secret Sharing Schemes"; Information Processing Letters, 60, 6 (1996) 301–304

[McEliece, Sarwate 81] McEliece, R.J. and Sarwate, D.V.: "On Sharing Secrets and Reed-Solomon Codes"; Communications of the ACM, 24, 9 (1981) 583–584

[Ogata et al. 92] Ogata, W., Kurosawa, K., Tsujii, S.: "Nonperfect secret sharing schemes"; Proc. Auscrypt'92, Lecture Notes on Comput. Sci., 718, Springer Verlag (1992) 56–66

[Okada, Kurosawa 94] Okada, K., Kurosawa, K.: "Lower bound on the size of shares of nonperfect secret sharing schemes"; Proc. of Asiacrypt'94, Lecture Notes on Comput. Sci. 917, Springer Verlag (1994) 33-41

[Pedersen 91] Pedersen, T.P.: "Noninteractive and information theoretic secure verifiable secret sharing"; Proc. of Crypto'91, Lecture Notes on Comput. Sci. 576, Springer Verlag (1991) 129-140

[Shamir 79] Shamir, A.: "How to share a secret"; Communications of the ACM, 22, 11 (1979) 612–613

[Stinson 92] Stinson, D.R.: "New general bounds on the information rate of secret sharing schemes"; Proc. Crypto'92, Lecture Notes on Comput. Sci., 740, Springer Verlag (1992) 168–182