Nonperfect Secret Sharing Schemes and Matroids

Kaoru KUROSAWA, Koji OKADA, Keiichi SAKANO,
Wakaha OGATA, Shigeo TSUJII

Department of Electrical and Electronic Engineering,
Faculty of Engineering, Tokyo Institute of Technology
2-12-1 O-okayama, Meguro-ku, Tokyo 152, Japan
E-mail: `kkurosaw@ss.titech.ac.jp`

Abstract. This paper shows that nonperfect secret sharing schemes (NSS) have matroid structures and presents a direct link between the secret sharing matroids and entropy for both perfect and nonperfect schemes. We define natural classes of NSS and derive a lower bound of $|V_i|$ for those classes. "Ideal" nonperfect schemes are defined based on this lower bound. We prove that every such ideal secret sharing scheme has a matroid structure. The rank function of the matroid is given by the entropy divided by some constant. It satisfies a simple equation which represents the access level of each subset of participants.

1 Introduction

Secret sharing schemes are defined by using entropy such as follows. The inputs to a secret sharing scheme are a secret S and a random number R. The outputs of the scheme are V_1 through V_n, which are called shares. Each V_i is given to a party P_i. We assume that S and R are uniformly distributed. Then, V_i becomes a random variable with a certain distribution. We denote the entropy as $H(V_i)$. In a "perfect" secret sharing scheme, any subset of parties is an access set or a non-access set. If A is an access set, A can recover S. The conditional entropy is that $H(S|A) = 0$. If B is a non-access set, B has absolutely no information on S. That is, $H(S|B) = H(S)$, which equals the bit length of S (denoted by $|S|$) because S is assumed to be uniformly distributed. No subset is allowed in between.

Many researchers have investigated perfect secret sharing schemes extensively so far [1]~[16]. Let's review the history of perfect secret sharing schemes. An access structure Γ is defined as the family of all access sets.

1. First, (k, n) threshold schemes were proposed by Shamir and Blakley [1][2].
2. Later, more general access structures were considered. It was shown that Γ is an access structure of a perfect secret sharing scheme if and only if Γ is monotone [3].

The meaning of monotone is as follows. If A can recover S, then any set A' which contains A can also recover S. Formally, Γ is monotone if A belongs to Γ and A' contains A, then A' also belongs to Γ.

T. Helleseth (Ed.): Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 126-141, 1994.

Further, it was proved that $|V_i| \geq |S|$ for any V_i [6][7]. This lower bound was obtained by using entropy. Recently, more tight lower bounds of V_i were shown for some access structures [6][8][9][11][12].

We call a scheme ideal if $|V_i| = |S|$. Brickell and Davenport showed that every ideal perfect scheme has a matroid structure by using a combinatorial argument [5]. Matroids play a central role in many combinatorial problems [17]. Many subjects can be more clearly understood by using the matroids. No relation is known between the entropy and the secret sharing matroids.

The size of V_i should be as small as possible. As we saw, in any perfect scheme, $|V_i| \geq |S|$. Therefore, if $|V_i| < |S|$, the scheme must be "nonperfect".

A nonperfect scheme consists of not only access sets and non-access sets but also semi-access sets. If C is a semi-access set, C has some information on S but can not recover S. $H(S|C)$ takes a value between 0 and $|S|$. (d, k, n) ramp schemes shown by Blakley and Meadows which are an extension of (k, n) threshold schemes, are such an example [16]. However, only a little effort has been paid for nonperfect schemes.

Let Γ_1 denote the family of access sets, Γ_2 denote the family of semi-access sets and Γ_3 denote that of non-access sets.

In [18], we showed the following results.

Result 1. $(\Gamma_1, \Gamma_2, \Gamma_3)$ has a nonperfect secret sharing scheme if and only if Γ_1 is monotone and $\Gamma_1 \cup \Gamma_2$ is monotone.

Result 2. $\max|V_i| \geq |S|/\sharp(A \backslash C)$, for any access set A in Γ_1 and any non-access set C in Γ_3, where $\sharp(A \setminus C)$ denotes the cardinality of A set minus C.

Result 2 shows a possibility that V_i can be smaller by the factor of $\sharp(A \backslash C)$ than $|S|$.

In this paper, we will show that nonperfect schemes also have matroid structures. We will also present a direct connection between the secret sharing matroids and the entropy for both perfect and nonperfect schemes.

We define natural classes of NSS and derive a lower bound of $|V_i|$ for those classes. "Ideal" nonperfect schemes are defined based on this lower bound. We prove that every such ideal nonperfect secret sharing scheme has a matroid structure. The rank function of the matroid is given by the entropy divided by some constant. It satisfies a simple equation which represents the access level of each subset of the participants in the NSS.

$H(X)$ denotes the entropy of X (see [19] or Appendix). $\sharp X$ denotes the cardinality of a finite set X. $|X| \triangleq \log_2 \sharp X$. $A \setminus B \triangleq \{x | x \in A \text{ but } x \notin B\}$. 2^P denotes the family of all subsets of P. $\mathcal{Z}$ denotes the set of nonnegative integers. Γ^- denotes the family of minimal sets of a family Γ.

2 Perfect and Nonperfect Secret Sharing Scheme

1. $P = \{P_1, \cdots, P_n\}$ denotes a set of participants.
2. s denotes a secret uniformly distributed over a finite set S ($H(S) = |S|$).
3. v_i is the share of P_i distributed over a finite set V_i. $V \triangleq \{V_1, \cdots, V_n\}$.

Usually, access structures are defined as a subset of 2^P. For convenience, we define them as a subset of 2^V. We use P_i and V_i interchangeably such as follows. $\tilde{\Gamma}_i$ denotes a subset of 2^P. Γ_i denotes a subset of 2^V. $(V_{i1}, \cdots, V_{ik}) \in \Gamma_i$ iff $(P_{i1}, \cdots, P_{ik}) \in \tilde{\Gamma}_i$. (The index set in $\tilde{\Gamma}_i$ and that in Γ_i are the same.)

Definition 1. (Π, S, V) is a secret sharing scheme (SS) if Π is a mapping: $S \times R \rightarrow V_1 \times V_2 \times \cdots \times V_n$, where R is a set of random inputs.

Definition 2. Let $\Gamma \subseteq 2^V$. We say that an SS is a perfect SS (PSS) on Γ if

(1) $H(S|A) = 0 \quad \text{for } \forall A \in \Gamma.$
(2) $H(S|C) = H(S) \quad \text{for } \forall C \notin \Gamma.$

Remark.

1. A is called an access subset. (1) means that A can recover S.
2. C is called a non-access subset. (2) means that C obtains absolutely no information on S.

Definition 3. A family Γ is said to be monotone if $A \in \Gamma, A \subseteq A' \Rightarrow A' \in \Gamma$.

Proposition 4. *[3][4] There exists a PSS on Γ if and only if Γ is monotone.*

Proposition 5. *[6] $|V_i| \geq |S|$ for any i in PSSs if $V_i \in \exists A \in \Gamma^-$.*

Definition 6. Suppose that $\Gamma_1 \subseteq 2^V, \Gamma_2 \subseteq 2^V, \Gamma_1 \cap \Gamma_2 = \phi$. We say that an SS is a nonperfect SS (NSS) on (Γ_1, Γ_2) if

(1) $H(S|A) = 0 \quad \text{for } \forall A \in \Gamma_1.$
(2) $0 < H(S|B) < H(S) \quad \text{for } \forall B \in \Gamma_2.$
(3) $H(S|C) = H(S) \quad$ otherwise.

The authors showed the following results in [18].

Proposition 7. *[18] Suppose that $\sharp S$ is not a prime. There exists an NSS on (Γ_1, Γ_2) if and only if Γ_1 is monotone and $\Gamma_1 \cup \Gamma_2$ is monotone.*

Proposition 8. *[18]*

$$\max_i |V_i| \geq |S| / \sharp(A \setminus C), \forall A \in \Gamma_1, \forall C \in \Gamma_3 \;,$$

where $\Gamma_3 \triangleq 2^V \setminus (\Gamma_1 \cup \Gamma_2)$.

Proposition 8 shows a possibility that $|V_i|$ can be smaller by the factor $1/\sharp(A \setminus C)$ than $|S|$.

3 Matroid

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 [17].

(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 $\sharp X = \sharp Y + 1$, then there exists $x \in X \backslash Y$ such that $Y \cup \{x\} \in \mathcal{I}$.

We show an example. Let W be a finite vector space and let $\mathcal{I}$ be the collection of linearly independent subsets of vectors of W. Then, such a pair of W and $\mathcal{I}$ is a matroid.

The elements of W are called the points of the matroid and the sets $\mathcal{I}$ are called independent sets. A base of M is a maximal independent subset of W. The rank function of a matroid is a function $\rho : 2^W \to \mathcal{Z}$ defined by $\rho(A) = \max(\sharp X : X \subseteq A, X \in \mathcal{I})$. The rank of matroid, denoted by $\rho(M)$, is the rank of the set W.

There exists an equivalent axiom of a matroid based on the rank function.

Proposition 9. *A function ρ is the rank function of a matroid on W if and only if for $X \subseteq W, y, z \in W$,*

(R0) *$\rho(X)$ takes a value of a non-negative integer.*
(R1) $\rho(\phi) = 0$.
(R2) $\rho(X) \leq \rho(X \cup y) \leq \rho(X) + 1$.
(R3) *If $\rho(X \cup y) = \rho(X \cup z) = \rho(X)$, then $\rho(X \cup y \cup z) = \rho(X)$.*

4 Overview

4.1 Background

The background of our problem is summarized as follows. In a perfect scheme, it is known that $|V_i| \geq |S|$ [6][7]. This was proved by using entropy. If they are equal for all i, the scheme is called ideal. On the other hand, an ideal perfect scheme has a matroid structure [5]. No relation between the matroid and the entropy is known.

Now, we ask

(1) Do the matroids have any relation with the entropy ?
(2) Suppose that Π_1 and Π_2 are two ideal perfect schemes for the same access structure Γ. Then each Π_i has a matroid structure. What is common between the two matroids?
(3) Does an ideal nonperfect scheme also have a matroid structure (if "ideal" is properly defined for nonperfect schemes) ?

This paper gives answers to these questions.

4.2 Perfect SS

Our observation is as follows.

In a PSS, from Definition 2,

$$H(S|A) = H(SA) - H(A) = \begin{cases} 0 & \text{if } A \in \Gamma \\ H(S) & \text{if } A \notin \Gamma \ . \end{cases} \tag{1}$$

Define $\hat{\rho}(A)$ as

$$\hat{\rho}(A) \triangleq \frac{H(A)}{H(S)} \ . \tag{2}$$

Then, from eq.(1), we obtain that

$$\hat{\rho}(SA) - \hat{\rho}(A) = \begin{cases} 0 & \text{if } A \in \Gamma \\ 1 & \text{if } A \notin \Gamma \ . \end{cases} \tag{3}$$

We will prove that, in an ideal PSS, $\hat{\rho}(A)$ so defined is the rank function of a matroid.

Note that eq.(2) gives a direct connection between the secret sharing matroid and the entropy. This is an answer to our problem 1.

Also note that eq.(3) depends only on Γ, not on each scheme. Thus, this is an answer to our problem 2.

It will be proved that our $\hat{\rho}$ satisfies the conditions (R0)~(R3) of Proposition 9. The proof will be given in Section 6 in a more general form.

4.3 Nonperfect SS

In a nonperfect scheme, $H(S|A)$ can take a value between 0 and $|S|$. As an example, let's assume that

$$H(S|A) = H(SA) - H(A) = 0,\ H(S)/3,\ 2H(S)/3 \text{ or } H(S) \ .$$

Let

$$\hat{\rho}(A) \triangleq \frac{H(A)}{H(S)/3} \ .$$

Then, we have

$$\hat{\rho}(SA) - \hat{\rho}(A) = 0, 1, 2, \text{ or } 3 \ .$$

We will prove that in an ideal nonperfect scheme, $\hat{\rho}(A)$ so defined is the rank function of a matroid.

This is an answer for our problem 3 if "ideal nonperfect" is defined. However, we have not yet defined "ideal nonperfect". In Section 5, we will give a definition of "ideal nonperfect".

5 "Ideal" Nonperfect Secret Sharing Schemes

5.1 Access Hierarchy

In this subsection, we will define a natural class of nonperfect schemes.

Definition 10. Let d be a positive integer. We say that an SS (Π, S, V) has a level d access hierarchy $(\Sigma_0, \Sigma_1, \cdots, \Sigma_d)$ if

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

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

Theorem 11. *Suppose that* $\sharp S = q^d$ *for some positive integer* q*. There exists an SS which has a level* d *access hierarchy* $(\Sigma_0, \Sigma_1, \cdots, \Sigma_d)$ *if and only if* $\Delta_k \triangleq \bigcup_{i=0}^{k} \Sigma_i$ *is monotone for* $0 \leq \forall k \leq d-1$.

Proof. "Only if" part is clear. We prove "if" part. The secret s can be expressed as $(s_0, \cdots, s_{d-1})$ such that $s_i \in \{0, \cdots, q-1\}$. From Proposition 4, there exists a PSS T_k on each Δ_k. Apply T_k to s_k for $0 \leq \forall k \leq d-1$, independently. Then, it is easy to see that the above scheme has a level d access hierarchy. □

5.2 Lower Bound of $|V_i|$

This subsection will derive a lower bound of $|V_i|$ (Note that Proposition 8 gives a lower bound of the "max"$|V_i|$).

Theorem 12. *If an SS has a level* d *access hierarchy* $(\Sigma_0, \Sigma_1, \cdots, \Sigma_d)$ *and if* $V_i \in A \in \Sigma_k^-$ *for some* A *and some* k $(\leq d-1)$*, then*

$$|V_i| \geq H(V_i) \geq H(S)/d \ .$$

Proof.

$$\begin{aligned} H(V_i) &\geq H(V_i|A \setminus \{V_i\}) \\ &\geq I(S; V_i|A \setminus \{V_i\}) \\ &= H(S|A \setminus \{V_i\}) - H(S|A) \\ &\geq (k+1)/d \times H(S) - k/d \times H(S) \\ &= H(S)/d \ . \end{aligned}$$

□

5.3 Definition of "Ideal"

Based on Theorem 12, we will define "ideal" as follows.

Definition 13. We say that an SS of a level d access hierarchy is ideal if

$$|V_i| = H(V_i) = H(S)/d, \quad \forall V_i \in V \ .$$

Theorem 14. *If an SS has a level d access hierarchy* $(\Sigma_0, \Sigma_1, \cdots, \Sigma_d)$ *and if the SS is ideal, then for* $\forall A \in \Sigma_i, \forall C \in \Sigma_j$,

$$\sharp(A \setminus C) \geq j - i \quad (j > i) \ .$$

Proof.

(1) First we assume that $B = (A \setminus C)$. Then,

$$\begin{aligned} I(S; B|C) &= H(S|C) - H(S|CB) \\ &= H(B|C) - H(B|SC) \\ &\leq H(B|C) \leq H(B) \leq \sum_{V_i \in B} H(V_i) \ . \end{aligned}$$

Therefore,

$$\begin{aligned} \sharp(A \setminus C) H(S)/d &= \sum_{V_i \in B} H(V_i) \\ &\geq H(S|C) - H(S|A) \\ &= (j - i) H(S)/d \ . \end{aligned}$$

Hence,

$$\sharp(A \setminus C) \geq j - i \ .$$

(2) Next we assume that $C \not\subset A$. Let $A' \triangleq C \cup A, A' \in \Sigma_k$. It is clear that $k \leq i$. Then, from (1) of this proof,

$$\sharp(A \setminus C) \ = \ \sharp(A' \setminus C) \ \geq \ j - k \geq j - i \ .$$

□

5.4 Mixed Access Hierarchy

Now, we will define a slight variation of Definition 10.

Definition 15. 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 $W \triangleq \{S_1, \cdots, S_d, V_1, \cdots, V_n\}$. We say that an SS (Π, S, V) has a level d mixed access hierarchy $(\hat{\Sigma}_0, \hat{\Sigma}_1, \cdots, \hat{\Sigma}_d)$ if

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

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

Remark.

1. Many examples of NSS in [16] have mixed access hierarchies.
2. A PSS has a level 1 mixed access hierarchy.

The following theorem clearly holds.

Theorem 16. *If an SS has a level d mixed access hierarchy $(\hat{\Sigma}_0, \hat{\Sigma}_1, \cdots, \hat{\Sigma}_d)$, it has a level d access hierarchy $(\Sigma_0, \Sigma_1, \cdots, \Sigma_d)$ such that $\Sigma_k = \hat{\Sigma}_k \cap 2^V$.*

Therefore, Theorem 12 also holds for an SS of a level d mixed access hierarchy.

Definition 17. We say that an SS of a level d mixed access hierarchy is ideal if

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

Theorem 18. *If an SS has a level d mixed access hierarchy $(\hat{\Sigma}_0, \hat{\Sigma}_1, \cdots, \hat{\Sigma}_d)$ and if the SS is ideal, then for $\forall A \in \hat{\Sigma}_i, \forall C \in \hat{\Sigma}_j$,*

$$\sharp(A \setminus C) \geq j - i \quad (j > i) \ .$$

The proof is similar to Theorem 14.

6 Ideal NSS and Matroid

In this section, we will show that each ideal nonperfect SS (in the sense of Definition 17) has a matroid structure. The rank function of the matroid is given by the entropy divided by some constant. It satisfies a simple equation which represents the access level of the subset. This property also holds for ideal perfect SSs.

6.1 Ideal NSS and Matroid

Theorem 19. *Suppose that*

1. *An SS has a level d mixed access hierarchy $(\hat{\Sigma}_0, \hat{\Sigma}_1, \cdots, \hat{\Sigma}_d)$ 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 $W \triangleq \{S_1, \cdots, S_d, V_1, \cdots, V_n\}$ 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* $X \in \Sigma_k$, *where* $\Sigma_k = \hat{\Sigma}_k \cap 2^V$.

To prove the Theorem, we define

$$\hat{\rho}(X) \triangleq \begin{cases} 0 & \text{if } X = \phi \\ H(X) \times (d/|S|) & \text{otherwise} \ . \end{cases}$$

We will prove that $\hat{\rho}$ is the desired rank function. We have to show that $\hat{\rho}$ satisfies (R0)~(R3) of Proposition 9 and (N1), (N2) of Theorem 19. The proof of (R0) will be given in the next subsection.

Lemma 20. *$\hat{\rho}$ satisfies (R0)~(R3), (N1) and (N2).*

Proof. (R1) and (N1) are clear.

(R2) $H(X) \le H(X \cup y) \le H(X) + H(y) = H(X) + |S|/d$. Hence,

$$dH(X)/|S| \le dH(X \cup y)/|S| \le dH(X)/|S| + 1 \ .$$

(R3) $H(X \cup y \cup z) = H(X) + H(y|X) + H(z|yX)$.
Suppose that

$$H(X \cup y) = H(X \cup z) = H(X) \ .$$

Then,

$$H(y|X) = H(X \cup y) - H(X) = 0 \ .$$

Similarly,

$$H(z|X) = 0 \ .$$

Since $0 \le H(z|yX) \le H(z|X) = 0$,

$$H(z|yX) = 0 \ .$$

(N2) If $X \in \Sigma_k$,

$$\begin{aligned}(k/d)|S| &= H(S|X) \\ &= H(SX) - H(X) \\ &= H(S_1 \cdots S_d X) - H(X) \ .\end{aligned}$$

□

As a special case of Theorem 19, we have the following corollary.

Corollary 21. *For a perfect ideal SS, there exists a matroid on $\{S, V_1, \cdots, V_n\}$ with a rank function ρ such that*

1. $\rho(S) = 1$.
2. $\rho(SX) - \rho(X) = \begin{cases} 0 \textit{ if } X \textit{ is an access subset} \\ 1 \textit{ if } X \textit{ is a non-access subset.} \end{cases}$

6.2 $H(X) = (|S|/d) \times$ Integer

Lemma 22. *If $X \in \hat{\Sigma}_{i+1}$ and $(X \cup y) \in \hat{\Sigma}_i$, then $H(y|X) = |S|/d, H(y|XS) = 0$.*

Proof.

$$\begin{aligned}I(y;S|X) &= H(S|X) - H(S|Xy) \\ &= ((i+1)/d)H(S) - (i/d)H(S) \\ &= H(S)/d \ .\end{aligned}$$

On the other hand,

$$I(y;S|X) = H(y|X) - H(y|XS) \ .$$

Then,

$$0 \le H(y|XS) = H(y|X) - H(S)/d \le H(y) - H(S)/d = 0 \ .$$

Therefore,

$$H(y|XS) = 0 \ .$$

Hence,

$$H(y|X) = H(S)/d = |S|/d \ .$$

□

Lemma 23. $\forall A \in \hat{\Sigma}_i,\ \forall C \in \hat{\Sigma}_{i+2},\ \sharp(A \setminus C) \ge 2.$

Proof. It is clear from Theorem 18. □

Lemma 24. *For* $0 \le \forall i \le d-1$, *if* $a \in B \subsetneq A \in \hat{\Sigma}_i$, $(A \setminus \{a\}) \in \hat{\Sigma}_i$ *and* $B \in \hat{\Sigma}_i^-$, *then* $H(a|(A \setminus \{a\})) = 0$.

Proof. Choose $C \subsetneq (A \setminus \{a\})$ such that $C \in \hat{\Sigma}_i^-$. Let $D \overset{\triangle}{=} (B \setminus \{a\})$.
Since $C \subsetneq C \cup D \subsetneq C \cup B \subsetneq A$ and $C \in \hat{\Sigma}_i^-, A \in \hat{\Sigma}_i$, then $C \cup D \in \hat{\Sigma}_i, C \cup B \in \hat{\Sigma}_i$.
Therefore,

$$H(S|CD) = H(S|CB) \ .$$

On the other hand,

$$H(aS|CD) = H(a|CD) + H(S|CB) = H(S|CD) + H(a|SCD) \ .$$

Then,

$$0 \le H(a|(A \setminus \{a\})) \le H(a|CD) = H(a|SCD) \le H(a|SD) = 0$$

(from Lemma 22).

□

Lemma 25. *For* $\forall X \in \hat{\Sigma}_d$, $H(X) = (|S|/d) \times$ *integer.*

Proof. Let X be a minimal set such that

$$X \in \hat{\Sigma}_d \quad \textit{and} \quad H(X) \ne (|S|/d) \times \textit{integer} \ .$$

Claim 26. $\forall y \in X, \quad H(X \setminus \{y\}) = (\sharp X - 1)|S|/d.$

Proof. Let $X \setminus \{y\} = \{a_1, \cdots, a_l\}$. From the minimality of X,

$$q_i \overset{\triangle}{=} H(a_1 \cdots a_i) = (|S|/d) \times \textit{integer} \ .$$

Therefore,

$$t_i \overset{\triangle}{=} H(a_i|a_1 \cdots a_{i-1}) = q_i - q_{i-1} = (|S|/d) \times \textit{integer} \ .$$

On the other hand,

$$0 \leq t_i \leq H(a_i) = |S|/d \ .$$

Hence,

$$t_i = 0 \ or \ |S|/d \ .$$

If $t_i = 0$,

$$H(a_i|X \setminus \{a_i\}) = 0$$

because

$$0 \leq H(a_i|X \setminus \{a_i\}) \leq H(a_i|a_1 \cdots a_{i-1}) = 0 \ .$$

Then,

$$H(X) = H(X \setminus \{a_i\}) + H(a_i|X \setminus \{a_i\}) = H(X \setminus \{a_i\}) \ .$$

This contradicts the minimality of X. Therefore,

$$t_i = |S|/d \quad \text{for } 1 \leq i \leq l \ .$$

Hence,

$$H(X \setminus \{y\}) = H(a_1) + t_2 + \cdots + t_l = (\sharp X - 1)|S|/d \ .$$

□

Claim 27. *There exists* $Y = \{y_1, \cdots, y_k\} \in \hat{\Sigma}_d$ *such that* $(X \cup Y) \in \hat{\Sigma}_{d-1}$ *and* $(X \cup Y) \setminus \{\forall y_i\} \in \hat{\Sigma}_d$.

Proof. From the assumption of Theorem 19,

$$\forall a \in X, \ \exists B \in \hat{\Sigma}^{-}_{d-1}, \ s.t. \ a \in B \ .$$

Clearly, $B \setminus X \in \hat{\Sigma}_d$. Let $Y \subseteq (B \setminus X)$ be a minimal set such that $(X \cup Y) \in \hat{\Sigma}_{d-1}$.

□

Claim 28. $\forall Z \subseteq X, \quad H(Z \cup Y) = H(Z) + \sharp Y|S|/d.$

Proof. Let

$$u_i \triangleq H(y_i|Z \cup \{y_1, \cdots, y_{i-1}\}) \ .$$

Then,

$$u_i \leq H(y_i) = |S|/d \ .$$

On the other hand,

$$u_i \geq H(y_i|(X \cup Y) \setminus \{y_i\}) = |S|/d \ .$$

The equality comes from Lemma 22. Therefore,

$$u_i = |S|/d \ .$$

Hence

$$H(Z \cup Y) = H(Z) + u_1 + \cdots + u_k = H(Z) + \sharp Y|S|/d \ .$$

□

Claim 29. *$H(X \cup Y) \neq |S|/d \times$ integer.*

Proof. From Claim 3,

$$H(X \cup Y) = H(X) + \sharp Y|S|/d \ .$$

□

Claim 30. $\forall a \in X, \quad (X \cup Y) \setminus \{a\} \in \hat{\Sigma}_{d-1}$.

Proof. Suppose that

$$\exists a \in X, \quad (X \cup Y) \setminus \{a\} \in \hat{\Sigma}_d \ .$$

Then, from Lemma 22,

$$H(a|(X \cup Y) \setminus \{a\}) = |S|/d \ .$$

Therefore,

$$\begin{aligned} H(X \cup Y) &= H((X \cup Y) \setminus \{a\}) + H(a|(X \cup Y) \setminus \{a\}) \\ &= H(X \setminus \{a\}) + \sharp Y|S|/d + |S|/d \\ &= ((\sharp X - 1) + \sharp Y + 1)|S|/d = (\sharp X + \sharp Y)|S|/d \ . \end{aligned}$$

The second line comes from Claim 3. The third line comes from Claim 1. This is against Claim 4. □

(Proof of Lemma 25). Choose $B \in \hat{\Sigma}^{-}_{d-1}$ such that $B \subseteq (X \cup Y)$. Let $a \in (B \cap X)$. From Claim 5 and Lemma 24,

$$H(a|(X \cup Y) \setminus \{a\}) = 0 \ .$$

Then, from Claim 3 and Claim 1,

$$\begin{aligned} H(X \cup Y) &= H((X \cup Y) \setminus \{a\}) + H(a|(X \cup Y) \setminus \{a\}) \\ &= H(X \setminus \{a\}) + \sharp Y|S|/d \\ &= (\sharp X - 1 + \sharp Y)|S|/d \ . \end{aligned}$$

This is against Claim 4. □

Theorem 31. *For $0 \leq \forall k \leq d$,*

$$\forall A \in \hat{\Sigma}_k, \quad H(A) = |S|/d \times \textit{integer} \ . \tag{4}$$

Proof. We will prove by induction on k. When $k = d$, (4) holds from Lemma 25. Suppose that (4) holds for $k \geq i + 1$. Let A be a minimal set such that

$$A \in \hat{\Sigma}_i, \quad H(A) \neq (|S|/d) \times \textit{integer}.$$

(1) Assume that

$$\exists a \in A,\ \ A \setminus \{a\} \notin \hat{\Sigma}_i \ .$$

From Lemma 23,

$$A \setminus \{a\} \in \hat{\Sigma}_{i+1} \ .$$

Then, from Lemma 22,

$$H(a|A \setminus \{a\}) = |S|/d \ .$$

Hence

$$H(A) = H(A \setminus \{a\}) + H(a|A \setminus \{a\}) = H(A \setminus \{a\}) + |S|/d \ .$$

From the hypothesis of the induction,

$$H(A \setminus \{a\}) = |S|/d \times integer \ .$$

This is a contradiction.

(2) Assume that

$$\forall a \in A,\ \ A \setminus \{a\} \in \hat{\Sigma}_i \ .$$

Choose $B \in \hat{\Sigma}_i^-$ such that $B \subseteq A$. Let $b \in B$. From Lemma 24,

$$H(b|A \setminus \{b\}) = 0 \ .$$

Then,

$$H(A) = H(A \setminus \{b\}) + H(b|A \setminus \{b\}) = H(A \setminus \{b\}) \ .$$

This contradicts the minimality of A.

Therefore,

$$\forall A \in \hat{\Sigma}_i,\ \ H(A) = |S|/d \times integer \ .$$

□

6.3 Other Theorems

Theorem 32. *Under the assumption of Theorem 19, let Y be any maximal independent set contained in X. Then, $X \in \hat{\Sigma}_i$ if and only if $Y \in \hat{\Sigma}_i$.*

Proof. Let $X = Y \cup Z$. Because Y be a maximal independent set,

$$H(X) = H(Y) \ .$$

On the other hand,

$$H(X) = H(Y) + H(Z|Y) \ .$$

Therefore,

$$H(Z|Y) = 0 \ .$$

Here,

$$0 \leq H(Z|YS) \leq H(Z|Y) = 0 \ .$$

Hence,

$$H(Z|YS) = 0 \ .$$

Then,

$$I(S;Z|Y) = H(Z|Y) - H(Z|YS) = 0 = H(S|Y) - H(S|YZ) \ .$$

Now, we have

$$H(S|Y) = H(S|YZ) = H(S|X) \ .$$

□

Theorem 33. *If there exists a representable matroid over a finite field $GF(q)$ on W which satisfies (N1) and (N2), there exists an SS which has a level d mixed access hierarchy $(\hat{\Sigma}_0, \hat{\Sigma}_1, \cdots, \hat{\Sigma}_d)$ and is ideal.*

Proof. There exist a vector space D over $GF(q)$ and a mapping $\phi : W \rightarrow D$, which preserves rank. Let $\phi(S_i) = \alpha_i$ and $\phi(V_i) = \beta_i$. α_i and β_i are column vectors. For a secret $s = (s_1, \cdots, s_d)$ $(s_i \in GF(q))$, choose a vector γ such that

$$s_i = \alpha_i' \cdot \gamma \quad (1 \leq i \leq d)$$

at random, where $\cdot$ means inner product. We can do this because the rank of $\{\alpha_1, \cdots, \alpha_d\}$ equals d. Then, compute each share v_i as

$$v_i = \beta_i' \cdot \gamma \quad (1 \leq i \leq n) \ .$$

It is easy to see that the above scheme satisfies the desired condition. □

Remark. Let $E \triangleq \{x_1, x_2, \cdots, x_n\}$, where x_i is a random variable. It is known that (E, H) is a polymatroid [20]. The rank function of a polymatroid takes a value in nonnegative real numbers. It doesn't have to be integer valued, while the rank function of a matroid must be integer valued. Generally, $H(X)$ is not integer valued. Our contribution is to show that $H(S)$ is integer valued in ideal secret sharing schemes (for both perfect and nonperfect.)

7 Summary

This paper has shown that nonperfect secret sharing schemes (NSS) have matroid structures and has presented a direct link between the secret sharing matroids and entropy for both perfect and nonperfect schemes. We have defined natural classes of NSS and have derived a lower bound of $|V_i|$ for those classes. "Ideal" nonperfect schemes are defined based on this lower bound. We have proved that every such ideal secret sharing scheme has a matroid structure. The rank function of the matroid has been given by the entropy divided by some constant. It satisfies a simple equation which represents the access level of each subset of participants.

Acknowledgement

We would like to thank Prof. S.Ueno of Tokyo Institute of Technology for useful discussion.

References

1. G.R.Blakley : Safeguarding cryptographic keys. Proc. of the AFIPS 1979 National Computer Conference, vol.48, pp.313-317 (1979)
2. A.Shamir : How to share a secret. Communications of the ACM, 22, (11), pp.612-613 (1979)
3. M.Itoh, A.Saito, T.Nishizeki : Secret sharing scheme realizing general access structure. Proc. of IEEE Globecom '87, Tokyo, pp.99-102 (1987)
4. J.C.Benaloh, J.Leichter : Generalized secret sharing and monotone functions. Crypto'88, pp.27-36 (1990)
5. E.F.Brickell, D.M.Davenport : On the classification of ideal secret sharing schemes. Journal of Cryptology, vol.4, No.2, pp.123-134 (1991)
6. R.M.Capocelli, A.De Santis, L.Gargano, U.Vaccaro : On the size of shares for secret sharing schemes. Crypto'91, pp.101-113 (1991)
7. E.D.Karnin, J.W.Green, M.E.Hellman : On secret sharing systems. IEEE Trans. IT-29, No.1, pp.35-41 (1982)
8. E.F.Brickell, D.R.Stinson : Some improved bounds on the information rate of perfect secret sharing schemes. Crypto'90, pp.242-252 (1990)
9. C.Blund, A.De Santis, D.R.Stinson, U.Vaccaro : Graph decomposition and secret sharing schemes. Eurocrypt'92, pp.1-20 (1992)
10. Y.Frankel, Y.Desmedt : Classification of ideal homomorphic threshold schemes over finite Abelian groups. Eurocrypt'92, pp.21-29 (1992)
11. C.Blund, A.De Santis, L.Gargano, U.Vaccaro : On the information rate of secret sharing schemes. Crypto'92 (1992)
12. D.R.Stinson : New general bounds on the information rate of secret sharing schemes. Crypto'92 (1992)
13. A.Beimel, B.Chor : Universally ideal secret sharing schemes. Crypt'92 (1992)
14. W.A.Jackson, K.M.Martin : Cumulative arrays and geometric secret sharing schemes. Auscrypt'92 (1992)
15. M.Bertilsson, I.Ingemarsson : A construction of practical secret sharing schemes using linear block codes. Auscrypt'92 (1992)
16. G.R.Blakley, C.Meadows : Security of ramp schemes. Crypto'84, pp.242-268 (1984)
17. D.J.A.Welsh : Matroid theory. Academic Press (1976)
18. W.Ogata, K.Kurosawa, S.Tsujii : Nonperfect secret sharing schemes. Auscrypt'92 (1992)
19. R.G.Gallager : Information Theory and Reliable Communications. John Wiley & Sons, New York, NY, (1968)
20. S.Fujishige : Polymatroidal dependence structure of a set of random variables. Information and Control 39, pp.55-72, (1978)

Appendix

Given a probability distribution $\{p(x)\}_{x \in X}$, the *entropy* of X is defined as

$$H(X) \triangleq - \sum_{x \in X} p(x) \ \log_2 p(x) \ .$$

It holds that

$$0 \leq H(X) \leq \log_2 \sharp X = |X| \ ,$$

where $H(X) = 0$ if and only if there exists $x \in X$ such that $p(x) = 1$; $H(X) = |X|$ if and only if $p(x) = 1/\sharp X$, for $\forall x \in X$.

Given two sets X and Y and a joint probability distribution $\{p(x, y)\}_{x \in X, y \in Y}$ on their Cartesian product, the *conditional entropy* $H(X|Y)$ is defined as

$$H(X|Y) \triangleq - \sum_{y \in Y} \sum_{x \in X} p(x, y) \log_2 p(x|y) \ .$$

From the definition of conditional entropy, it is easy to see that

$$H(X|Y) \geq 0 \ .$$

The entropy of the joint space XY satisfies

$$H(XY) = H(X) + H(Y|X) = H(Y) + H(X|Y) \ .$$

The *mutual information* between X and Y is defined by

$$I(X;Y) \triangleq H(X) - H(X|Y) \ .$$

The mutual information has the following properties:

$$I(X;Y) = I(Y;X) \ ,$$
$$I(X;Y) \geq 0 \ .$$

From the above inequality, one gets

$$H(X) \geq H(X|Y) \ .$$

The *conditional mutual information* is defined by

$$I(X;Y|Z) \triangleq H(X|Z) - H(X|YZ) \ .$$

$I(X;Y|Z)$ satisfies the following properties.

$$I(X;Y|Z) \geq 0 \ ,$$
$$I(X;Y|Z) = I(Y;X|Z) \ ,$$
$$I(X;YZ) = I(X;Z) + I(X;Y|Z) \ .$$