# Nonperfect Secret Sharing Schemes and Matroids 

Kaoru KUROSAWA, Koji OKADA, Keiichi SAKANO, Wakaha OGATA, Shigeo TSUJII<br>Department of Electrical and Electronic Engineering, Faculty of Engineering, Tokyo Institute of Technology<br>2-12-1 O-okayama, Meguro-ku, Tokyo 152, Japan<br>E-mail: kkurosaw@s.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 $\left|V_{i}\right|$ 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 $H\left(V_{i}\right)$. 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 $H(S \mid A)=0$. If $B$ is a non-access set, $B$ has absolutely no information on $S$. That is, $H(S \mid B)=H(S)$, 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 $\Gamma$ 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 $\Gamma$ is an access structure of a perfect secret sharing scheme if and only if $\Gamma$ is monotone [3].
The meaning of monotone is as follows. If $A$ can recover $S$, then any set $A^{\prime}$ which contains $A$ can also recover $S$. Formally, $\Gamma$ is monotone if $A$ belongs to $\Gamma$ and $A^{\prime}$ contains $A$, then $A^{\prime}$ also belongs to $\Gamma$.

Further, it was proved that $\left|V_{i}\right| \geq|S|$ 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 $\left|V_{i}\right|=|S|$. 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, $\left|V_{i}\right| \geq|S|$. Therefore, if $\left|V_{i}\right|<|S|$, 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 $S . H(S \mid C)$ 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 $\Gamma_{1}$ denote the family of access sets, $\Gamma_{2}$ denote the family of semi-access sets and $\Gamma_{3}$ 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 $\Gamma_{1}$ is monotone and $\Gamma_{1} \cup \Gamma_{2}$ is monotone.
Result 2. $\max \left|V_{i}\right| \geq|S| / \sharp(A \backslash C)$, for any access set $A$ in $\Gamma_{1}$ and any non-access set $C$ in $\Gamma_{3}$, where $\sharp(A \backslash C)$ 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 $\left|V_{i}\right|$ 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). $\forall X$ denotes the cardinality of a finite set $X .|X| \triangleq \log _{2} \sharp X . A \backslash B \triangleq\{x \mid x \in A$ but $x \notin B\} .2^{P}$ denotes the family of all subsets of $P . \mathcal{Z}$ denotes the set of nonnegative integers. $\Gamma^{-}$denotes the family of minimal sets of a family $\Gamma$.

## 2 Perfect and Nonperfect Secret Sharing Scheme

1. $P=\left\{P_{1}, \cdots, P_{n}\right\}$ 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 $V_{i} . V \triangleq\left\{V_{1}, \cdots, V_{n}\right\}$.

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 $2^{P} . \Gamma_{i}$ denotes a subset of $2^{V} .\left(V_{i 1}, \cdots, V_{i k}\right) \in \Gamma_{i}$ iff $\left(P_{i 1}, \cdots, P_{i k}\right) \in \tilde{\Gamma}_{i}$. (The index set in $\tilde{\Gamma}_{i}$ and that in $\Gamma_{i}$ are the same.)

Definition 1. ( $\Pi, S, V$ ) is a secret sharing scheme (SS) if $\Pi$ 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 $\Gamma$ if
(1) $H(S \mid A)=0 \quad$ for $\forall A \in \Gamma$.
(2) $H(S \mid C)=H(S) \quad$ 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 $\Gamma$ is said to be monotone if $A \in \Gamma, A \subseteq A^{\prime} \Rightarrow A^{\prime} \in \Gamma$.

Proposition 4. [9]/4] There exists a PSS on $\Gamma$ if and only if $\Gamma$ is monotone.
Proposition 5. $[6]\left|V_{i}\right| \geq|S|$ 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 ( $\Gamma_{1}, \Gamma_{2}$ ) if
(1) $H(S \mid A)=0 \quad$ for $\forall A \in \Gamma_{1}$.
(2) $0<H(S \mid B)<H(S) \quad$ for $\forall B \in \Gamma_{2}$.
(3) $H(S \mid C)=H(S)$ 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 ( $\Gamma_{1}, \Gamma_{2}$ ) if and only if $\Gamma_{1}$ is monotone and $\Gamma_{1} \cup \Gamma_{2}$ is monotone.

Proposition 8. [18]

$$
\max _{i}\left|V_{i}\right| \geq|S| / \sharp(A \backslash C), \forall A \in \Gamma_{1}, \forall C \in \Gamma_{3},
$$

where $\Gamma_{3} \triangleq 2^{V} \backslash\left(\Gamma_{1} \cup \Gamma_{2}\right)$.
Proposition 8 shows a possibility that $\left|V_{i}\right|$ can be smaller by the factor $1 / \sharp(A \backslash C)$ 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) $\sim(I 3)$ are satisfied [17].
(II) $\phi \in \mathcal{I}$.
(12) If $X \in \mathcal{I}$ and $Y \subseteq X$, then $Y \in \mathcal{I}$.
(13) 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 $I$ are called independent sets. A base of $M$ is a maximal independent subset of $W$. The rank function of a matroid is a function $\rho: 2^{\boldsymbol{W}} \rightarrow \mathcal{Z}$ 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 $\rho$ 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 $\left|V_{i}\right| \geq|S|[6][7]$. 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 $\Pi_{1}$ and $\Pi_{2}$ are two ideal perfect schemes for the same access structure $\Gamma$. Then each $\Pi_{i}$ 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,

$$
H(S \mid A)=H(S A)-H(A)=\left\{\begin{array}{cl}
0 & \text { if } A \in \Gamma  \tag{1}\\
H(S) & \text { if } A \notin \Gamma .
\end{array}\right.
$$

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

$$
\begin{equation*}
\hat{\rho}(A) \triangleq \frac{H(A)}{H(S)} \tag{2}
\end{equation*}
$$

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

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

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

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

Let

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

Then, we have

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

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 $S S(\Pi, S, V)$ has a level $d$ access hierarchy ( $\Sigma_{0}, \Sigma_{1}, \cdots, \Sigma_{d}$ ) if

$$
\begin{gathered}
\bigcup_{i=0}^{d} \Sigma_{i}=2^{V}, \quad \Sigma_{i} \cap \Sigma_{j}=\phi \quad(i \neq j) \text { and } \\
H(S \mid A)=(k / d) H(S) \quad \text { for } \forall A \in \Sigma_{k} .
\end{gathered}
$$

Theorem 11. Suppose that $\sharp S=q^{d}$ for some positive integer $q$. There exists an $S S$ which has a level $d$ access hierarchy $\left(\Sigma_{0}, \Sigma_{1}, \cdots, \Sigma_{d}\right)$ 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 $\Delta_{k}$. 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 $\left|V_{i}\right|$

This subsection will derive a lower bound of $\left|V_{i}\right|$ (Note that Proposition 8 gives a lower bound of the "max" $\left|V_{i}\right|$ ).

Theorem 12. If an SS has a level $d$ access hierarchy $\left(\Sigma_{0}, \Sigma_{1}, \cdots, \Sigma_{d}\right)$ and if $V_{i} \in A \in \Sigma_{k}^{-}$for some $A$ and some $k(\leq d-1)$, then

$$
\left|V_{i}\right| \geq H\left(V_{i}\right) \geq H(S) / d
$$

Proof.

$$
\begin{aligned}
H\left(V_{i}\right) & \geq H\left(V_{i} \mid A \backslash\left\{V_{i}\right\}\right) \\
& \geq I\left(S ; V_{i} \mid A \backslash\left\{V_{i}\right\}\right) \\
& =H\left(S \mid A \backslash\left\{V_{i}\right\}\right)-H(S \mid A) \\
& \geq(k+1) / d \times H(S)-k / d \times H(S) \\
& =H(S) / d .
\end{aligned}
$$

### 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

$$
\left|V_{i}\right|=H\left(V_{i}\right)=H(S) / d, \quad \forall V_{i} \in V .
$$

Theorem 14. If an SS has a level d access hierarchy ( $\Sigma_{0}, \Sigma_{1}, \cdots, \Sigma_{d}$ ) and if the $S S$ is ideal, then for $\forall A \in \Sigma_{i}, \forall C \in \Sigma_{j}$,

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

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

$$
\begin{aligned}
I(S ; B \mid C) & =H(S \mid C)-H(S \mid C B) \\
& =H(B \mid C)-H(B \mid S C) \\
& \leq H(B \mid C) \leq H(B) \leq \sum_{V_{i} \in B} H\left(V_{i}\right)
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
\sharp(A \backslash C) H(S) / d & =\sum_{V_{i} \in B} H\left(V_{i}\right) \\
& \geq H(S \mid C)-H(S \mid A) \\
& =(j-i) H(S) / d .
\end{aligned}
$$

Hence,

$$
\sharp(A \backslash C) \geq j-i
$$

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

$$
\sharp(A \backslash C)=\sharp\left(A^{\prime} \backslash C\right) \geq j-k \geq j-i
$$

### 5.4 Mixed Access Hierarchy

Now, we will define a slight variation of Definition 10.
Deflnition 15. Suppose that $S=S_{1} \circ S_{2} \circ \cdots \circ S_{d}$ and $\left|S_{i}\right|=|S| / d$ for all $i$ (o means concatenation). Let $W \triangleq\left\{S_{1}, \cdots, S_{d}, V_{1}, \cdots, V_{n}\right\}$. We say that an SS ( $\Pi, S, V$ ) has a level $d$ mixed access hierarchy $\left(\hat{\Sigma}_{0}, \hat{\Sigma}_{1}, \cdots, \hat{\Sigma}_{d}\right)$ if

$$
\begin{gathered}
\bigcup_{i=0}^{d} \hat{\Sigma}_{i}=2^{W}, \quad \hat{\Sigma}_{i} \cap \hat{\Sigma}_{j}=\phi(i \neq j) \quad \text { and } \\
H(S \mid A)=(k / d) H(S) \quad \text { for } \forall A \in \dot{\Sigma}_{k} .
\end{gathered}
$$

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 leveld access hierarchy $\left(\Sigma_{0}, \Sigma_{1}, \cdots, \Sigma_{d}\right)$ such that $\Sigma_{k}=\dot{\Sigma}_{k} \cap 2^{V}$.

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 $\left(\hat{\Sigma}_{0}, \hat{\Sigma}_{1}, \cdots, \hat{\Sigma}_{d}\right)$ and if the $S S$ is ideal, then for $\forall A \in \hat{\Sigma}_{i}, \forall C \in \hat{\Sigma}_{j}$,

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

The proof is similar to Theorem 14.

## 6 Ideal NSS and Matroid

In this section, we will show that each ideal nonperfect $S S$ (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 $\left(\hat{\Sigma}_{0}, \hat{\Sigma}_{1}, \cdots, \hat{\Sigma}_{d}\right)$ and the $S S$ 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 $W \triangleq\left\{S_{1}, \cdots, S_{d}, V_{1}, \cdots, V_{n}\right\}$ with a rank function $\rho$ such that
(N1) $\rho\left(S_{1} \cdots S_{d}\right)=d$.
(N2) $\rho\left(S_{1} \cdots S_{d} X\right)-\rho(X)=k$ 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) $\sim(R 3)$ 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) $H(X) \leq H(X \cup y) \leq H(X)+H(y)=H(X)+|S| / d$. Hence,

$$
d H(X) /|S| \leq d H(X \cup y) /|S| \leq d H(X) /|S|+1
$$

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

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

Then,

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

Similarly,

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

Since $0 \leq H(z \mid y X) \leq H(z \mid X)=0$,

$$
H(z \mid y X)=0 .
$$

(N2) If $X \in \Sigma_{k}$,

$$
\begin{aligned}
(k / d)|S| & =H(S \mid X) \\
& =H(S X)-H(X) \\
& =H\left(S_{1} \cdots S_{d} X\right)-H(X)
\end{aligned}
$$

As a special case of Theorem 19, we have the following corollary.
Corollary 21. For a perfect ideal SS, there exists a matroid on $\left\{S, V_{1}, \cdots, V_{n}\right\}$ with a rank function $\rho$ such that

1. $\rho(S)=1$.
2. $\rho(S X)-\rho(X)=\left\{\begin{array}{l}0 \text { if } X \text { is an access subset } \\ 1 \text { if } X \text { is a non-access subset. }\end{array}\right.$
6.2 $\quad H(X)=(|S| / d) \times$ Integer

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

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

On the other hand,

$$
I(y ; S \mid X)=H(y \mid X)-H(y \mid X S)
$$

Then,

$$
0 \leq H(y \mid X S)=H(y \mid X)-H(S) / d \leq H(y)-H(S) / d=0 .
$$

Therefore,

$$
H(y \mid X S)=0
$$

Hence,

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

Lemma 23. $\forall A \in \hat{\Sigma}_{i}, \forall C \in \hat{\Sigma}_{i+2}, \forall(A \backslash C) \geq 2$.
Proof. It is clear from Theorem 18.
Lemma 24. For $0 \leq \forall i \leq d-1$, if $a \in B \subseteq A \in \hat{\Sigma}_{i},(A \backslash\{a\}) \in \hat{\Sigma}_{i}$ and $B \in \hat{\Sigma}_{i}^{-}$, then $H(a \mid(A \backslash\{a\}))=0$.

Proof. Choose $C \subseteq(A \backslash\{a\})$ such that $C \in \hat{\Sigma}_{i}^{-}$. Let $D \triangleq(B \backslash\{a\})$.
Since $C \subseteq C \cup D \subseteq C \cup B \subseteq A$ 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,

$$
H(S \mid C D)=H(S \mid C B)
$$

On the other hand,

$$
H(a S \mid C D)=H(a \mid C D)+H(S \mid C B)=H(S \mid C D)+H(a \mid S C D)
$$

Then,

$$
0 \leq H(a \mid(A \backslash\{a\})) \leq H(a \mid C D)=H(a \mid S C D) \leq \Lambda(a \mid S D)=0
$$

(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

$$
X \in \hat{\Sigma}_{d} \quad \text { and } \quad H(X) \neq(|S| / d) \times \text { integer }
$$

Claim 26. $\forall y \in X, \quad H(X \backslash\{y\})=(\sharp X-1)|S| / d$.
Proof. Let $X \backslash\{y\}=\left\{a_{1}, \cdots, a_{l}\right\}$. From the minimality of $X$,

$$
q_{i} \triangleq H\left(a_{1} \cdots a_{i}\right)=(|S| / d) \times \text { integer } .
$$

Therefore,

$$
t_{i} \triangleq H\left(a_{i} \mid a_{1} \cdots a_{i-1}\right)=q_{i}-q_{i-1}=(|S| / d) \times \text { integer }
$$

On the other hand,

$$
0 \leq t_{i} \leq H\left(a_{i}\right)=|S| / d .
$$

Hence.

$$
t_{i}=0 \text { or }|S| / d
$$

If $t_{i}=0$,

$$
H\left(a_{i} \mid X \backslash\left\{a_{i}\right\}\right)=0
$$

because

$$
0 \leq H\left(a_{i} \mid X \backslash\left\{a_{i}\right\}\right) \leq H\left(a_{i} \mid a_{1} \cdots a_{i-1}\right)=0 .
$$

Then.

$$
H(X)=H\left(X \backslash\left\{a_{i}\right\}\right)+H\left(a_{i} \mid X \backslash\left\{a_{i}\right\}\right)=H\left(X \backslash\left\{a_{i}\right\}\right)
$$

This contradicts the minimality of $X$. Therefore,

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

Hence,

$$
H(X \backslash\{y\})=H\left(a_{1}\right)+t_{2}+\cdots+t_{l}=(\sharp X-1)|S| / d .
$$

Claim 27. There exists $Y=\left\{y_{1}, \cdots, y_{k}\right\} \in \hat{\Sigma}_{d}$ such that $(X \cup Y) \in \hat{\Sigma}_{d-1}$ and $(X \cup Y) \backslash\left\{\forall y_{i}\right\} \in \hat{\Sigma}_{d}$.

Proof. From the assumption of Theorem 19,

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

Clearly, $B \backslash X \in \hat{\Sigma}_{d}$. Let $Y \subseteq(B \backslash X)$ 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

$$
u_{i} \triangleq H\left(y_{i} \mid Z \cup\left\{y_{1}, \cdots, y_{i-1}\right\}\right)
$$

Then,

$$
u_{i} \leq H\left(y_{i}\right)=|S| / d
$$

On the other hand,

$$
u_{i} \geq H\left(y_{i} \mid(X \cup Y) \backslash\left\{y_{i}\right\}\right)=|S| / d
$$

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. $\forall a \in X, \quad(X \cup Y) \backslash\{a\} \in \hat{\Sigma}_{d-1}$.
Proof. Suppose that

$$
\exists a \in X, \quad(X \cup Y) \backslash\{a\} \in \hat{\Sigma}_{d}
$$

Then, from Lemma 22,

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

Therefore,

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

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,

$$
H(a \mid(X \cup Y) \backslash\{a\})=0
$$

Then, from Claim 3 and Claim 1,

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

This is against Claim 4.
Theorem 31. For $0 \leq \forall k \leq d$,

$$
\begin{equation*}
\forall A \in \hat{\Sigma}_{k}, \quad H(A)=|S| / d \times \text { integer } \tag{4}
\end{equation*}
$$

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

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

(1) Assume that

$$
\exists a \in A, A \backslash\{a\} \notin \hat{\Sigma}_{i} .
$$

From Lemma 23,

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

Then, from Lemma 22,

$$
H(a \mid A \backslash\{a\})=|S| / d
$$

Hence

$$
H(A)=H(A \backslash\{a\})+H(a \mid A \backslash\{a\})=H(A \backslash\{a\})+|S| / d
$$

From the hypothesis of the induction,

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

This is a contradiction.
(2) Assume that

$$
\forall a \in A, A \backslash\{a\} \in \hat{\Sigma}_{\mathrm{i}} .
$$

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

$$
H(b \mid A \backslash\{b\})=0
$$

Then,

$$
H(A)=H(A \backslash\{b\})+H(b \mid A \backslash\{b\})=H(A \backslash\{b\})
$$

This contradicts the minimality of $A$.
Therefore,

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

### 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,

$$
H(X)=H(Y)+H(Z \mid Y)
$$

Therefore,

$$
H(Z \mid Y)=0
$$

Here,

$$
0 \leq H(Z \mid Y S) \leq H(Z \mid Y)=0
$$

Hence,

$$
H(Z \mid Y S)=0 .
$$

Then,

$$
I(S ; Z \mid Y)=H(Z \mid Y)-H(Z \mid Y S)=0=H(S \mid Y)-H(S \mid Y Z)
$$

Now, we have

$$
H(S \mid Y)=H(S \mid Y Z)=H(S \mid X)
$$

Theorem 33. If there exists a representable matroid over a finite field $G F(q)$ on $W$ which satisfies (N1) and (N2), there exists an SS which has a level d mixed access hierarchy $\left(\hat{\Sigma}_{0}, \hat{\Sigma}_{1}, \cdots, \hat{\Sigma}_{d}\right)$ and is ideal.

Proof. There exist a vector space $D$ over $G F(q)$ and a mapping $\phi: W \rightarrow D$, which preserves rank. Let $\phi\left(S_{i}\right)=\alpha_{i}$ and $\phi\left(V_{i}\right)=\beta_{i} . \alpha_{i}$ and $\beta_{i}$ are column vectors. For a secret $s=\left(s_{1}, \cdots, s_{d}\right)\left(s_{i} \in G F(q)\right)$, choose a vector $\gamma$ such that

$$
s_{i}=\alpha_{i}^{\prime} \cdot \gamma \quad(1 \leq i \leq d)
$$

at random, where means inner product. We can do this because the rank of $\left\{\alpha_{1}, \cdots, \alpha_{d}\right\}$ equals $d$. Then, compute each share $v_{i}$ as

$$
v_{i}=\beta_{i}^{\prime} \cdot \gamma \quad(1 \leq i \leq n) .
$$

It is easy to see that the above scheme satisfies the desired condition.
Remark. Let $E \triangleq\left\{x_{1}, x_{2}, \cdots, x_{n}\right\}$, 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 $\left|V_{i}\right|$ 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.612613 (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 schernes. 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 $H(X \mid Y)$ is defined as

$$
H(X \mid Y) \triangleq-\sum_{y \in Y} \sum_{x \in X} p(x, y) \log _{2} p(x \mid y)
$$

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

$$
H(X \mid Y) \geq 0
$$

The entropy of the joint space $X Y$ satisfies

$$
H(X Y)=H(X)+H(Y \mid X)=H(Y)+H(X \mid Y)
$$

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

$$
I(X ; Y) \triangleq H(X)-H(X \mid Y)
$$

The mutual information has the following properties:

$$
\begin{aligned}
& I(X ; Y)=I(Y ; X) \\
& I(X ; Y) \geq 0
\end{aligned}
$$

From the above inequality, one gets

$$
H(X) \geq H(X \mid Y)
$$

'The conditional mutual information is defined by

$$
I(X: Y \mid Z) \triangleq H(X \mid Z)-H(X \mid Y Z)
$$

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

$$
\begin{aligned}
I(X ; Y \mid Z) & \geq 0 \\
I(X ; Y \mid Z) & =I(Y ; X \mid Z) \\
I(X ; Y Z) & =I(X ; Z)+I(X ; Y \mid Z)
\end{aligned}
$$

