PAPER *Special Issue on Cryptography and Information Security*

Analysis on secret sharing schemes with non-graphical access structures

Koji OKADA[†], *Nonmember*, **Wakaha OGATA**[††], *Member*, **Keiichi SAKANO**[†††], *Nonmember* *and* **Kaoru KUROSAWA**[†], *Member*

SUMMARY Lower bounds on the size of shares $|\mathcal{V}_i|$ which are more tight than $|\mathcal{V}_i| \geq |\mathcal{S}|$, where $|\mathcal{S}|$ is the size of the secret, are known only for some graphical access structures. This paper shows lower bounds on $|\mathcal{V}_i|$ greater than $|\mathcal{S}|$ for some non-graphical access structures Γ. We first prove that if $\{P_1, P_i\} \in \Gamma^-$ for any $P_i \in \hat{P} = \{P_2, \ldots, P_n\}$ and $\hat{\Gamma} = 2^{\hat{P}} \cap \Gamma$ is the access structure of a $(k, n-1)$-threshold scheme on $\hat{P}$, then

$$\max_i \log |\mathcal{V}_i| \geq \frac{n+k-3}{n-1} \log |\mathcal{S}|$$

for $P_i \in \{P_1, P_2, \ldots, P_n\}$. Next, we show that $\max_i \log |\mathcal{V}_i| \geq 1.5 \log |\mathcal{S}|$ holds for a wider class of access structures.

key words: secret sharing, share size, non-graphical

1. Introduction

Secret sharing schemes [1], [2] have been studied extensively because of their wide applications in fields such as key management and secure computation. In such schemes, a dealer D distributes a secret s to n participants $P_1, \ldots, P_n$ in such a way that only qualified subsets of participants can recover the secret s. A secret sharing scheme is called perfect if non-qualified subsets of participants have no information on s. In a (k, n)-threshold secret sharing scheme, any k or more participants can recover s, but any $k-1$ or less participants have no information on s.

Let S denote the random variable induced by s and $\mathcal{S}$ be the domain of S. A piece v_i given to user i is called a share. Let V_i denote the random variable induced by v_i and $\mathcal{V}_i$ be the domain of V_i.

An important issue in secret sharing schemes is $|\mathcal{V}_i|$ because the security of a system will decrease if $|\mathcal{V}_i|$ increases, where $|X|$ denotes the cardinality of a finite set X. Karnin, Green, and Hellman showed that

$$\log_2 |\mathcal{V}_i| \geq H(S) \tag{1}$$

for (k, n)-threshold secret sharing schemes [7], where $H(S)$ denotes the entropy of S. On the other hand, it is well-known that

$$\log_2 |\mathcal{S}| \geq H(S).$$

The equality holds if and only if S is uniformly distributed. Therefore if S is uniformly distributed, Eq. (1) becomes

$$|\mathcal{V}_i| \geq |\mathcal{S}|. \tag{2}$$

It is a tight lower bound on $|\mathcal{V}_i|$ because Shamir's (k, n)-threshold secret sharing scheme [1] satisfies the equality. Capocelli, De Santis, Gargano, and Vaccaro showed that Eq. (1) can be extended to any perfect secret sharing scheme [6]. Kurosawa and Okada showed that Eq. (2) holds for any perfect secret sharing scheme with any distribution on S [15].

A family of all access sets is called an access structure, denoted by Γ. Let Γ^- denote the family of minimal access sets. For

$$\Gamma^- = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}\},$$

Capocelli, De Santis, Gargano and Vaccaro [6] showed that

$$\log_2 |\mathcal{V}_2| + \log_2 |\mathcal{V}_3| \geq 3H(S).$$

If S is uniformly distributed, we have

$$\log_2 |\mathcal{V}_2| + \log_2 |\mathcal{V}_3| \geq 3 \log_2 |\mathcal{S}|.$$

And the following is obtained:

$$\max_i \log |\mathcal{V}_i| \geq 1.5 \log |S|.$$

This is the smallest access structure such that $\max_i |\mathcal{V}_i|$ is strictly larger than $|\mathcal{S}|$.

Γ^- can be represented as a graph if the cardinality of each minimal access set is less than or equal to two. In such a graph, a minimal access set A corresponds to an edge if $|A| = 2$. It corresponds to a point if $|A| = 1$. We say that Γ is a graphical access structure if Γ^- is represented as a graph in this way. $\Gamma^- = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}\}$ is a graphical access structure. Blundo, De Santis, Gargano, and Vaccaro [10] showed another lower bound on $|V_i|$ for another graphical access structure on $P = \{P_1, \ldots, P_{2k+2}\}$ $(k \geq 1)$ such as follows: if $\Gamma^- = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}, \ldots, \{P_2, P_{k+2}\}, \{P_3, P_{k+3}\}, \{P_4, P_{k+4}\}, \ldots, \{P_{k+2}, P_{2k+2}\}\}$, then $\max_i \log |\mathcal{V}_i| = (2k+1)/(k+1) \log |\mathcal{S}|$ for $P_i \in P$.

Manuscript received
Manuscript revised

[†]The authors are with the Faculty of Engineering, Tokyo Institute of Technology, Tokyo, JAPAN
[††]The author are with the Faculty of Engineering, Himeji Institute of Technology, Hyougo, JAPAN
[†††]The author are with Matsushita Electric Industrial Co., LTD, Osaka, JAPAN

On the other hand, we say that Γ is non-graphical access structure if there exists a minimal access set with the cardinality greater than two. For non-graphical access structures, no lower bound on $|\mathcal{V}_i|$ is known which is strictly greater than $|\mathcal{S}|$.

This paper shows lower bounds on $|\mathcal{V}_i|$ which are strictly greater than $|\mathcal{S}|$ for some non-graphical access structures. We first prove the following theorem. If

1. $\{P_1, P_i\} \in \Gamma^-$ for $2 \leqq i \leqq n$,
2. $\{P_2, P_3, \cdots, P_n\}$ has a structure of a $(k, n-1)$-threshold scheme and

then,

$$\max_i \log|\mathcal{V}_i| \geq \frac{n+k-3}{n-1} \log|\mathcal{S}|$$

for $P_i \in \{P_1, P_2, \ldots, P_n\}$. If $k > (n+3)/2$, then this bound is strictly greater than $1.5 \log|\mathcal{S}|$. Next, we show that $\max_i \log|\mathcal{V}_i| \geq 1.5 \log|\mathcal{S}|$ holds for a wider class of non-graphical access structures.

2. Preliminaries

$H(Z)$ denotes the entropy of Z. $|X|$ denotes the cardinality of a finite set X. $A \setminus B = \{x | x \in A \ but \ x \notin B\}$. 2^P is the family of all subsets of P.

2.1 Secret sharing schemes

- $P = \{P_1, \cdots, P_n\}$ denotes a set of participants.
- s denotes a secret distributed over a finite set $\mathcal{S}$ and S denotes the random variable induced by s.
- v_i is the share of P_i distributed over a finite set $\mathcal{V}_i$ and V_i denotes the random variable induced by v_i.
- For $A = \{P_{i_1}, \ldots, P_{i_k}\} \subseteqq \mathcal{P}$, let $\mathcal{V}_A = \mathcal{V}_{i_1} \times \cdots \times \mathcal{V}_{i_k}$, and V_A be the random variable induced by $(v_{i_1}, \ldots, v_{i_k})$.

For simplicity, A often denotes the random variable V_A of shares on a set of participants A.

Definition 2.1: (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 2.2: We say that an SS is a perfect SS (PSS) for an access structure $\Gamma \subseteqq 2^P$ if (1) $H(S|A) = 0$ for $\forall A \in \Gamma$, (2) $H(S|C) = H(S)$ for $\forall C \notin \Gamma$.

Definition 2.3: A family Γ is said to be monotone if $A \in \Gamma, A \subseteqq A' \Rightarrow A' \in \Gamma$.

Proposition 2.4: [3][4] There exists a PSS for Γ if and only if Γ is monotone.

In this paper, we assume that Γ is monotone.

Proposition 2.5: [6] $|\mathcal{V}_i| \geq |\mathcal{S}|$ for any i.

Definition 2.6: We say that a PSS is ideal if $|\mathcal{V}_i| = |\mathcal{S}|$ for any i.

Proposition 2.7: [6] $P = \{P_1, \ldots P_4\}$. If Γ^- is one of the following four cases:

- $\Gamma^- = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}\}$,
- $\Gamma^- = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}\{P_2, P_4\}\}$,
- $\Gamma^- = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_1, P_3, P_4\}\}$,
- $\Gamma^- = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_1, P_3, P_4\}\{P_2, P_4\}\}$,

then $\log|\mathcal{V}_2| + \log|\mathcal{V}_3| \geq 3 \log|\mathcal{S}|$.
Also, there exists a PSS for the above Γ^- which holds that $\log|\mathcal{V}_2| = \log|\mathcal{V}_3| = 1.5 \log|\mathcal{S}|$, for the first and the second structures.

Proposition 2.8: [10] $P = \{P_1, \ldots, P_{2k+2}\}$ $(k \geq 1)$. If $\Gamma^- = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}, \ldots, \{P_2, P_{k+2}\}, \{P_3, P_{k+3}\}, \{P_4, P_{k+4}\}, \ldots, \{P_{k+2}, P_{2k+2}\}\}$, then $\max_i \log|\mathcal{V}_i| = (2k+1)/(k+1) \log|\mathcal{S}|$ for $P_i \in P$.

2.2 Entropy

In this section, we review information theoretic concepts. For a complete treatment of the subject, the reader is advised to refer to [16].

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

$$H(X) \stackrel{\triangle}{=} -\sum_{x \in X} p(x) \ \log_2 p(x). \tag{3}$$

The entropy $H(X)$ is a measure of the average information content of the elements in X or, equivalently, a measure of the average uncertainty one has about which element of the set X has been chosen when the choices of the elements from X are made according to the probability distribution $\{p(x)\}_{x \in X}$. There is the following useful property of $H(X)$ which holds that

$$0 \leqq H(X) \leqq \log_2 |X|, \tag{4}$$

where $H(X) = 0$ if and only if there exists $x \in X$ such that $p(x) = 1$; $H(X) = \log_2 |X|$ if and only if $p(x) = 1/|X|$, 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* $H(X|Y)$, also called the equivocation of X given Y, is defined as

$$H(X|Y) \stackrel{\triangle}{=} -\sum_{y \in Y} \sum_{x \in X} p(x,y) \log_2 p(x|y). \tag{5}$$

The conditional entropy can be written as

$$H(X|Y) = \sum_{y \in Y} p(y) H(X|Y = y),$$

where $H(X|Y=y) = -\sum_{x\in X} p(x|y)\log_2 p(x|y)$ can be interpreted as the average uncertainty one has about which element of X has been chosen when the choice are made according to the probability distribution $\{p(x|y)\}_{x\in X}$, that is, when it is known that the value chosen from the set Y is y. From the definition of conditional entropy, it is easy to see that

$$H(X|Y) \geqq 0. \tag{6}$$

The entropy of the joint space XY satisfies

$$H(XY) = H(X)+H(Y|X) = H(Y)+H(X|Y). \tag{7}$$

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

$$I(X;Y) \stackrel{\triangle}{=} H(X) - H(X|Y). \tag{8}$$

This equation shows that we can interpret $I(X;Y)$ as the average amount of uncertainty in X resolved by the observation of the outcome in Y, $H(X|Y)$ being the average remaining uncertainty in X after the observation. The mutual information has the following properties:

$$I(X;Y) = I(Y;X), \tag{9}$$
$$I(X;Y) \geqq 0. \tag{10}$$

From the above inequality, one gets

$$H(X) \geqq H(X|Y). \tag{11}$$

The *conditional mutual information* is defined by

$$I(X;Y|Z) \stackrel{\triangle}{=} H(X|Z) - H(X|YZ). \tag{12}$$

Notice that $H(X|ZY) = \sum_{y\in Y} p(y)H(X|Z,Y=y)$, where

$$H(X|Z,Y=y) = -\sum_{x,z} p(xz|y)\log_2 p(x|yz).$$

3. Analysis of non-graphical structure

Proposition 2.7 means that $\max_i \log|\mathcal{V}_i| \geqq 1.5\log|\mathcal{S}|$ for the access structures given in the proposition. We show a lower bound of $\log|\mathcal{V}_i|$ which is greater than $1.5\log|\mathcal{S}|$ for some non-graphical access structures.

Lemma 3.1: If $X \notin \Gamma, X\cup Y \in \Gamma$, then $H(Y|X) = H(S) + H(Y|XS)$.

Proof

$$\begin{aligned} &H(Y|X)\\ &= I(Y;S|X) + H(Y|XS) \quad \text{(from (12))}\\ &= H(S|X) - H(S|XY) + H(Y|XS) \quad \text{(from (12))}\\ &= H(S) + H(Y|XS). \end{aligned}$$

Note that $H(S|X) = H(S)$ because $X \notin \Gamma$. Also, $H(S|XY) = 0$ because $X\cup Y \in \Gamma$.

□

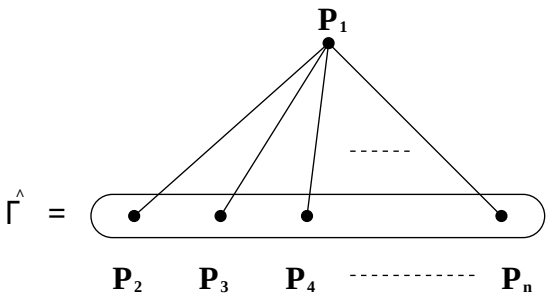

Fig. 1 Access structure in Theorem 3.2

Theorem 3.2: If the following conditions hold:

1. $\{P_1, P_i\} \in \Gamma^-$ for $2 \leqq i \leqq n$,
2. $\{P_2, P_3, \cdots, P_n\}$ has a structure of a $(k, n-1)$-threshold scheme and

then

$$\max_i \log|\mathcal{V}_i| \geq \frac{n+k-3}{n-1} H(S) \quad \text{for } 1 \leqq i \leqq n.$$

(Even if there is another minimal access set, this theorem holds.)

Proof Consider the conditional entropy $H(V_3\ldots V_n|V_2)$. We have

$$\begin{aligned} &H(V_3\ldots V_n|V_2)\\ &= H(V_3|V_2) + H(V_4|V_2V_3) +\\ &\qquad \cdots\cdots + H(V_n|V_2V_3\ldots V_{n-1}) \quad \text{(from (7))}\\ &\geq H(V_3|V_2) + H(V_4|V_2V_3) +\\ &\qquad \cdots + H(V_{k+1}|V_2V_3\ldots V_k) \quad \text{(from (6))}\\ &\geq H(V_3|V_2V_4\ldots V_{k+1}) + H(V_4|V_2V_3V_5\ldots V_{k+1}) +\\ &\qquad \cdots + H(V_{k+1}|V_2V_3\ldots V_k) \quad \text{(from (11))}\\ &\geq (k-1)H(S) \qquad \text{(from Lemma 3.1).} \end{aligned}$$

On the other hand, we also have

$$\begin{aligned} &H(V_3\ldots V_n|V_2)\\ &= H(V_3\ldots V_n|V_2S) + H(S) \quad \text{(from Lemma 3.1)}\\ &\leq H(V_1V_3\ldots V_n|V_2S) + H(S) \quad \text{(from (6),(7))}\\ &\leq H(V_1|V_2S) + H(V_3|V_1V_2S) +\\ &\qquad \cdots + H(V_n|V_1V_2\ldots V_{n-1}S) + H(S)\\ &\qquad\qquad \text{(from (7))}\\ &\leq H(V_1|V_2S) + H(V_3|V_1S) +\\ &\qquad \cdots + H(V_n|V_1S) + H(S) \quad \text{(from (11))}\\ &= H(V_1|V_2) - H(S) + H(V_3|V_1) - H(S) +\\ &\qquad \cdots + H(V_n|V_1) - H(S) + H(S)\\ &\qquad\qquad \text{(from Lemma 3.1)}\\ &\leq H(V_1) + H(V_3) + \cdots + H(V_n) - (n-2)H(S)\\ &\qquad\qquad \text{(from (11)).} \end{aligned}$$

Therefore we get

$$H(V_1) + H(V_3) + \cdots + H(V_n) \geq (n+k-3)H(S).$$

Similarly

$$H(V_1) + H(V_2) + \cdots + H(V_{n-1}) \geq (n+k-3)H(S).$$

Hence there exists $P_i \in P$ such that

$$\log|\mathcal{V}_i| \geq H(V_i) \geq \frac{n+k-3}{n-1}H(S).$$

□

Remark If $k > (n+3)/2$, then $\max_i \log|\mathcal{V}_i|$ is strictly greater than $1.5\log|\mathcal{S}|$. The minimal structure satisfying this condition is a $(5,5)$-threshold scheme on $\hat{P}$. This bound is $\max_i \log|\mathcal{V}_i| \geq (8/5)\log|\mathcal{S}| > 1.5\log|\mathcal{S}|$ for $P_i \in P$.

4. Generalization of Proposition 2.7

This section shows $\max_i \log|\mathcal{V}_i| \geq 1.5\log|\mathcal{S}|$ for a wider class of non-graphical access structures than that of Proposition 2.7.

4.1 Wider class of non-graphical access structures

Theorem 4.1: $\log|\mathcal{V}_2| + \log|\mathcal{V}_3| \geq 3H(S)$ if $\{P_1,P_2\} \in \Gamma^-, \{P_2,P_3\} \in \Gamma^-, \{P_1,P_3\} \notin \Gamma^-$ and there exists Δ such that $P_3 \in \Delta \in \Gamma^- \setminus \{P_2,P_3\}, P_1 \cup \Delta \setminus P_3 \notin \Gamma$.

Before we prove the theorem, we show some lemmas on entropy.

Lemma 4.2: $I(X;YZ) \geq H(Y|Z) - H(Y|XZ)$

Proof

$$\begin{aligned} & I(X;YZ) \\ &= H(YZ) - H(YZ|X) \quad \text{(from (8))} \\ &= H(Z) + H(Y|Z) - H(Z|X) - H(Y|XZ) \\ & \qquad \text{(from (7))} \\ &\geq H(Y|Z) - H(Y|XZ) \quad \text{(from (11)).} \end{aligned}$$

□

Lemma 4.3: If $X \cup Y \in \Gamma$, then $H(Z|XS) \geq H(Z|XY)$

Proof

$$\begin{aligned} & H(ZS|XY) \\ &= H(Z|XY) + H(S|XYZ) \;=\; H(Z|XY) \\ &= H(S|XY) + H(Z|XYS) \;=\; H(Z|XYS) \\ & \qquad \text{(from (7)).} \end{aligned}$$

Note that $H(S|XY) = 0$ because $X \cup Y \in \Gamma$. On the other hand,

$$I(Z;Y|XS) \;=\; H(Z|XS) - H(Z|XYS) \;\geq\; 0 \qquad \text{(from (12)).}$$

Hence

$$H(Z|XS) \geq H(Z|XYS) = H(Z|XY).$$

□

Proof of Theorem 4.1.

$$\begin{aligned} & H(V_2V_3) \\ &= H(V_2) + H(V_3|V_2) \quad \text{(from (7))} \\ &= H(V_2) + H(S) + H(V_3|V_2S) \\ & \qquad \text{(from Lemma 3.1).} \end{aligned} \tag{13}$$

$$\begin{aligned} & H(V_2) \\ &= H(V_2|V_3V_1) + I(V_2;V_3V_1) \quad \text{(from (8))} \\ &= H(S) + H(V_2|V_3V_1S) + I(V_2;V_3V_1) \\ & \qquad \text{(from Lemma 3.1)} \\ &\geq H(S) + I(V_2;V_3V_1) \quad \text{(from (6)).} \end{aligned} \tag{14}$$

$$\begin{aligned} & I(V_2;V_3V_1) \\ &\geq H(V_3|V_1) - H(V_3|V_2V_1) \quad \text{(from Lemma 4.2)} \\ &\geq H(V_3|V_1 \cup (\Delta \setminus V_3)) - H(V_3|V_2V_1) \\ & \qquad \text{(from (11))} \\ &= H(S) + H(V_3|V_1 \cup (\Delta \setminus V_3) \cup S) \\ & \quad - H(V_3|V_2V_1) \qquad \text{(from Lemma 3.1)} \\ &\geq H(S) - H(V_3|V_2V_1) \quad \text{(from (6)).} \end{aligned} \tag{15}$$

From (13)–(15),

$$\begin{aligned} H(V_2V_3) &\geq 3H(S) + H(V_3|V_2S) - H(V_3|V_2V_1) \\ &\geq 3H(S) \qquad \text{(from Lemma 4.3).} \end{aligned}$$

Hence

$$\begin{aligned} \log|\mathcal{V}_2| + \log|\mathcal{V}_3| &\geq H(V_2) + H(V_3) \quad \text{(from (4))} \\ &\geq H(V_2V_3) \quad \text{(from (7),(11))} \\ &\geq 3H(S). \end{aligned}$$

□

4.2 Optimal cases

Theorem 4.4: Let $\hat{P} = \{P_2, P_3, \cdots, P_n\}$, and $\hat{\Gamma} = 2^{\hat{P}} \cap \Gamma$. Suppose that

1. $\{P_1,P_i\} \in \Gamma^-$ for any $P_i \in \hat{P}$ and $\{P_i,P_j\} \notin \Gamma$ for any $P_i, P_j, \in \hat{P}$,
2. for $\forall P_i \in \hat{P}$, there exists $\Delta \in \hat{\Gamma}$ such that $P_i \in \Delta$,

then

$$\log|\mathcal{V}_1| + \log|\mathcal{V}_i| \geq 3H(S) \text{ for any } P_i \in \hat{P}.$$

Further, if there exists an ideal PSS for $\hat{\Gamma}$, then there exists a PSS for Γ such that

$$\log|\mathcal{V}_1| + \log|\mathcal{V}_i| = 3\log|\mathcal{S}| \text{ for any } P_i \in \hat{P}.$$

Proof The former part is clear from Theorem 4.1. We prove the latter part. Let c_i denote the share given to P_i by the ideal PSS for $\hat{\Gamma}$. Choose randomly a and b such that $a+b = s \bmod q$. Let $v_1 = a$ and $v_i = c_i \circ b$ for $P_i \in \hat{P}$. It is clear that the above scheme is a PSS for Γ and $\log|\mathcal{V}_1| + \log|\mathcal{V}_i| = 3H(S)$ for any $P_i \in \hat{P}$. □

(Example 1) $\hat{\Gamma} = \{\hat{P}\}$.
(Example 2) $\hat{\Gamma}$ = the access structure of a $(k, n-1)$-threshold scheme on $\hat{P}$ ($k \geqq 4$).
(Example 3) $\hat{\Gamma}$ = the access structure of a $(3,4)$-threshold scheme on $\hat{P}$.

Remark The method of the proof of Theorem 4.4 yields that $\log|\mathcal{V}_1| = H(S)$ and $\log|\mathcal{V}_i| = 2H(S)$ for $P_i \in \hat{P}$. But in Example 3, there exists a PSS such that $\log|\mathcal{V}_1| = 2H(S)$ and $\log|\mathcal{V}_i| = H(S)$ for $P_i \in \hat{P}$. The PSS is as follows. Choose a random polynomial $f(x)$ over $GF(q)$ such that

$$f(x) = s + a_1 x + a_2 x^2.$$

Let $v_1 = f(1) \circ f(2)$ and $v_2 = f(3), v_3 = f(4), v_4 = f(5), v_5 = f(6)$. If $|\mathcal{S}| = q^2$, then we can construct a PSS which satisfies $\log|\mathcal{V}_1| = \log|\mathcal{V}_i| = 1.5H(S)$ for any $P_i \in \hat{P}$, using two methods.

References

[1] A. Shamir, "How to share a secret", *Communications of the ACM,* **22**, *(11), pp. 612–613, 1979.*
[2] G. R. Blakley, "Safeguarding cryptographic keys", *Proc. of the AFIPS 1979 National Computer Conference, vol.* **48**, *pp. 313–317, 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 and J. Leichter, "Generalized secret sharing and monotone functions", *Proc. of Crypto'88, Lecture Notes in Computer Science,* **403**, *Springer Verlag, pp. 27–36, 1990.*
[5] E. F. Brickell and 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", *Journal of Cryptology, vol.* **6**, *No. 3, pp. 157–167, 1993.*
[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", *Journal of Cryptology, vol.* **5**, *No. 3, pp. 153–166, 1992.*
[9] C. Blund, A. De Santis, D. R. Stinson, U. Vaccaro, "Graph decomposition and secret sharing schemes", *Journal of Cryptology, vol.* **8**, *No. 1, pp. 39–64, 1995.*
[10] C. Blundo, A. De Santis, L. Gargano, U. Vaccaro, "On the information rate of secret sharing schemes", *Proc. of Crypto'92, Lecture Notes in Computer Science,* **740**, *Springer Verlag, pp. 149–169, 1993.*
[11] D. R. Stinson, "New general bounds on the information rate of secret sharing schemes", *Proc. of Crypto'92, Lecture Notes in Computer Science,* **740**, *Springer Verlag, pp. 170–184, 1993.*
[12] G. R. Blakeley, C. Meadows, "Security of ramp schemes", *Proc. of Crypto'84, Lecture Notes in Computer Science,* **196**, *Springer Verlag, pp. 242–268, 1984.*
[13] D. J. A. Welsh, "Matroid Theory", *Academic Press, 1976.*
[14] W. Ogata, K. Kurosawa, S. Tsujii, "Nonperfect secret sharing schemes", *Proc. of Auscrypt'92, Lecture Notes in Computer Science,* **718**, *Springer Verlag, pp. 56–66, 1992.*
[15] K. Kurosawa and K. Okada, "Combinatorial interpretation of secret sharing schemes", *Proc. of Asiacrypt'94, Lecture Notes in Computer Science,* 917, *Springer Verlag, pp. 55–64, 1994.*
[16] R.G.Gallager, "Information theory and reliable communications", *John Wiley & Sons, New York, NY, 1968.*

Koji Okada received received B.E. and M.E. degrees in electrical and electronic engineering from Tokyo Institute of Technology in 1994 and 1996, respectively. He is currently working toward the Ph.D. degree in electrical and electronic engineering at Tokyo Institute of Technology, and involved researches on information security.

Wakaha Ogata received B.S. degree in 1989 and Dr.Eng. degree in electrical and electronic engineering in 1994 from Tokyo Institute of Technology. She is currently a research associate in the Department of Computer Engineering at Himeji Institute of Technology, and involved researches on information security.

Keiichi Sakano received the B.E. degree in computer science in 1993 and M.E. degree in electrical and electronic engineering in 1995 from Tokyo Institute of Technology. He then joined the Multimedia Development Center, Matsushita Electrical Industrial Co., LTD. His interests include software development on computer-based A/V editing.

Kaoru Kurosawa received the B.E. and Dr. Eng. degrees in electrical engineering in 1976 and 1981, respectively, from Tokyo Institute of Technology. He is currently an Associate Professor in the Department of Electrical and Electronic Engineering at Tokyo Institute of Technology. His research interests are information security and digital signal processing.