Some new results on nonperfect secret sharing schemes

Wakaha OGATA[1] Kaoru KUROSAWA[2]

[1] Department of Computer Engineering,
Faculty of Engineering, Himeji Institute of Technology
2167 Shosya, Himeji-shi, Hyogo 671-22, JAPAN
Tel. +81–792-67-4919
E-mail: wakaha@comp.eng.himeji-tech.ac.jp

[2] Department of Electrical and Electronic Engineering,
Faculty of Engineering, Tokyo Institute of Technology
2–12–1 O-okayama, Meguro-ku, Tokyo 152, JAPAN
Tel. +81–3–5734–2577, Fax. +81–3–5734–2905
E-mail: kurosawa@ss.titech.ac.jp

Abstract. In secret sharing schemes, $|V_i|$ should be as small as possible, where V_i denotes the set of share of player P_i. It is known that the scheme must be nonperfect if $|V_i| < |S|$, where S denotes the set of s. A secret sharing scheme is called nonperfect if there exists a subset of players who have some information on the sectret s but cannot recover s. For nonperfect secret sharing schemes, the authers showed a lower bound on $|V_i|$. The neccessary and sufficient condition that the access structure must satisfy was also shown by the authers, but only for $|S|$ which is a composite number.

In this paper, we show a necessary and sufficient condition on the existence of NSSs for any $|S|$. That is, a nonperfect secret sharing scheme exists if and only if Γ_1 is monotone and $\Gamma_1 \cup \Gamma_2$ is monotone, where Γ_1 is the family of access sets and Γ_2 is the family of semi-access sets.

Further, we show that there exists a tradeoff between $|V_i|$ and the amount of the leaked information on s.

keywords: secret sharing schemes, nonperfect, entropy, share size

1 Introduction

Secret sharing schemes are useful in the management of cryptographic keys, in multiparty protocols and etc. In a secret sharing scheme, a dealer transforms a secret S into n shares $V_1, \ldots, V_n$ so that only qualified subsets of $\{V_1, \ldots, V_n\}$ can recover the secret. Then, V_i is given to a participant P_i, for $i = 1, 2, \ldots, n$. The qualified subsets of the participants who can recover the secrets are called access sets.

Secret sharing schemes are classified into two types, perfect secret sharing schemes (PSS) and nonperfect secret sharing schemes (NSS). In a PSS, any subset of the participants is either an access set or a non-access set which has absolutely no information on the secret. An example of a PSS is a (k, n) threshold scheme [3, 14] where every k or more participants are an access set and every less than k participants are a non-access set. In an NSS, in addition to access sets and non-access sets, there exists a semi-access set which has some information on the secret but cannot recover the secret. An example of an NSS is a (d, k, n) ramp scheme [4] in which every k or more participants are an access set, every $k - d$ or less participants are a non-access set, and more than $k - d$ and less than k participants are a semi-access set. The motivation of such an NSS is to reduce the bit length of V_i which a participant P_i must hold secretly.

PSSs have been studied extensively so far, especially focusing on their general structures and the lower bound on the size of V_i. They are summarized as follows.

(1) The family of an access set is called an access structure. The first basic question is what access structure can have a PSS. [12] showed that a PSS exists if and only if the access structure is monotone. A family Γ is said to be monotone if

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

Subsequently, [1] gave a simpler and more efficient way to realize monotone access structures.

(2) The next question is the lower bound of the size of V_i. Let $|X|$ denotes the bit length of X. For simplicity, assume that S is uniformly distributed. Then, [10] showed that $|V_i| \geq |S|$ for any PSS by extending the technique of [13]. More tight lower bounds of $|V_i|$ which depend on the access structure have also been shown [10, 6, 9, 5, 15].

(3) The third question is what happens if $|V_i| = |S|$. A PSS is called ideal if $|V_i| = |S|$ for all i. [8] characterized ideal PSSs in terms of a matroid.

It is important that $|V_i|$ is as small as possible because, otherwise, the security of the system degrades. However, as mentioned in (2), $|V_i| \geq |S|$ in a PSS. Therefore, if we desire that $|V_i| < |S|$, the secret sharing scheme must be an NSS.

For nonperfect secret sharing schemes, the authers [16] showed a lower bound on $|V_i|$ such that

$$\max \log_2 |V_i| \geq H(S) / \min |A \setminus C|,$$

where A is an access set and C is a non-access set. $|A \setminus C|$ denotes the cardinality of $A \setminus C$. The neccessary and sufficient condition that the access structure must satisfy was also shown by the authers [16], but only for $|S|$ which is a composite number.

In this paper, we show a necessary and sufficient condition on the existence of NSSs for any $|S|$. Further, we show that there exists a tradeoff between $|V_i|$ and the amount of the leaked information on s.

The rest of this paper is organized as follows. Subsection 2.1 shows notation. Subsection 2.2 states the definitions of perfect and nonperfect secret sharing schemes. In subsection 3.1, we show a necessary and sufficient condition on the existence of NSSs for any $|S|$. Subsection 3.2 presents a lower bound of the $\max |V_i|$. In subsection 3.3, we show that there exists a tradeoff between $|V_i|$ and the amount of the leaked information on s. Section 4 gives some lemmas on entropy which will be used to prove the above results (Lemma 4.1, Lemma 4.2).

(Our another paper on NSS was presented at Eurocrypt'93 [17].)

2 Preliminaries

2.1 Notation

$H(X)$ denotes the entropy of X (for example, see [11]). $|X|$ denotes the cardinality of a finite set X. $A \setminus B = \{x | x \in A \textit{ but } x \notin B\}$. 2^V denotes the family of all subsets of V.

2.2 Definitions

- $P = \{P_1, \cdots, P_n\}$ denotes a set of participants.
- s is a secret distributed over a finite set S.
- v_i is the share of P_i distributed over a finite set V_i.
- $V \stackrel{\triangle}{=} \{V_1, \cdots, V_n\}$.

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.

For convenience, we use S to denote the random variable induced by s, also. Similarly, V_i is used to denote the random variable induced by v_i.

Definition 2.2 *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 is called an access set. C is called an non-access set. Γ is called the access structure of the PSS.

Definition 2.3 *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. $H(S|A) = 0$ *for* $\forall A \in \Gamma_1$ *(A can recover S),*
2. $0 < H(S|B) < H(S)$ *for* $\forall B \in \Gamma_2$
   (B has some information on S, but cannot recover S),
3. $H(S|C) = H(S)$ *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.

3 Basic Properties of Nonperfect Secret Sharing Schemes

3.1 Monotone Property

Definition 3.1 *A family Γ is said to be monotone if $A \in \Gamma, A \subseteq A' \Rightarrow A' \in \Gamma$.*

It is known that Γ is an access structure of a PSS if and only if Γ is monotone [12][1]. For NSSs, we show the following theorem.

Theorem 3.1 *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* Γ_1 *is monotone and* $\Gamma_1 \cup \Gamma_2$ *is monotone.*

proof: Only if part is clear. We will prove if part. Suppose that Γ_1 and $\Gamma_1 \cup \Gamma_2$ are monotone.

(Case 1) Suppose that $|S| > 2$. Express $s \in S$ as $s = 2s_1 + s_2$ where $s_2 = 0$ or 1 and $0 \leq s_1 \leq \lfloor |S|/2 \rfloor$. Let $S_1 \stackrel{\triangle}{=} \{0, \ldots, \lfloor |S|/2 \rfloor\}$, and $S_2 \stackrel{\triangle}{=} \{0, 1\}$. Since Γ_1 is monotone, there exists a PSS $(\Pi_1, S_1, V', \Gamma_1)$ for s_1, where v_i' is the share of P_i, V_i' is the random variable induced by v_i' and $V' = \{V_1', \cdots, V_n'\}$. 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_i'' is the share of P_i, V_i'' is the random variable induced by v_i'' and $V'' = \{V_1'', \cdots, V_n''\}$. To share $s = 2s_1 + s_2$, apply Π_1 for s_1 and apply Π_2 for s_2, independently. Clearly, there is at least a value of s of the form $s = 2s_1 + 1$ with positive probability. Also, there is at least a value of s of the form $s = 2s_1$ with positive probability. Therefore, $\forall B \in \Gamma_2$ has some information on s. Then, it is easy to see that *1.* $\sim$ *3.* of Definition 2.3 are satisfied.

(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

$$\begin{aligned} \Pr(s_2 = 0 | s = 0) &= \frac{2}{3} \\ \Pr(s_2 = 1 | s = 0) &= \frac{1}{3} \\ \Pr(s_2 = 1 | s = 1) &= \frac{2}{3} \\ \Pr(s_2 = 0 | s = 1) &= \frac{1}{3} \end{aligned}$$

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

3.2 Lower Bound of the Size of the Shares

In a PSS, it is known that $\log_2 |V_i| \geq H(S)$ if V_i belongs to some minimal access set [10][13]. If S is uniformly distributed, it is well known that $H(S) = \log_2 |S|$. Therefore, $|V_i| \geq |S|$ for uniformly distributed S. (V_i which doesn't belong to any minimal access set is redundant and meaningless.)

An NSS has a possibility such that $\log_2 |V_i| < H(S)$. In this subsection, we derive a lower bound of the $\max |V_i|$ for an NSS $(\Pi, S, V, (\Gamma_1, \Gamma_2, \Gamma_3))$.

Lemma 3.1 *If* $A \in \Gamma_1, C \in \Gamma_3, C \subset A$, *then* $\sum_{V_i \in A \setminus C} H(V_i) \geq H(S)$.

proof: ¿From lemma 4.2 (see Section 4), $H(S|A) \geq H(S|C) - \sum_{V_i \in A \setminus C} H(V_i)$. Note that Lemma 4.2 requires that $C \subset A$. ¿From Definition 2.3 (1) and (3), $\sum_{V_i \in A \setminus C} H(V_i) \geq H(S|C) - H(S|A) = H(S)$. □

Theorem 3.2 *In an NSS,*

$$\max_i \log_2 |V_i| \geq H(S) / \min |A \setminus C| \tag{1}$$

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 2.3.)
proof: First we assume $C \subset A$. Then, from lemma 3.1,

$$\sum_{V_i \in A \setminus C} H(V_i) \geq H(S) \ . \tag{2}$$

On the other hand,

$$\sum_{V_i \in A \setminus C} H(V_i) \leq |A \setminus C| \max_i \log_2 |V_i| \ . \tag{3}$$

because $H(V_i) \leq \log_2 |V_i|$. ¿From eq.(2) and eq.(3), we obtain

$$H(S) \leq |A \setminus C| \max_i \log_2 |V_i| \ . \tag{4}$$

Next, we assume $C \not\subset A$. Let $A' \stackrel{\triangle}{=} C \cup A$. Since Γ_1 is monotone (from Theorem 3.1), $A' \in \Gamma_1$. Then, from eq.(4), we have

$$H(S) \leq |A' \setminus C| \max_i \log_2 |V_i| \ . \tag{5}$$

It is clear that

$$|A \setminus C| \ = \ |A' \setminus C| \ . \tag{6}$$

¿From eq.(5) and eq.(6), we obtain

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

Therefore, we have eq.(1). □

Corollary 3.1 *If S is uniformly distributed, then*

$$\max_i \log_2 |V_i| \geq \log_2 |S| / \min |A \setminus C| \tag{8}$$

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.(8). □

(Remarks)

(1) Let $d \stackrel{\triangle}{=} \min |A \setminus C|$ for $\forall A \in \Gamma_1$ and $\forall C \in \Gamma_3$. Then, d is a distance between Γ_1 and Γ_3 in a sense. Corollary 3.1 shows a possibility that $\log_2 |V_i|$ can be smaller than $\log_2 |S|$ by the factor of d.

(2) The above result was first shown in our preliminary version [16]. The special case of our result for ramp schemes has independently appeared in [7].

3.3 A Tradeoff in NSS

It is important that $|V_i|$ is as small as possible. On the other hand, form a view point of information leakage, $H(S|B)$ should be large for $B \in \Gamma_2$. In this subsection, we show that the two quantities, $\max_i |V_i|$ and $H(S|B)$, bound each other.

For $B \in \Gamma_2$, let $\hat{B}$ be a maximal semi-access set which includes B. Then, clearly

$$H(S|\hat{B}) \leq H(S|B) \ .$$

Therefore, we consider maximal semi-access sets in what follows.

Theorem 3.3 *Consider V_i and $B \in \Gamma_2$ such that $B \cup \{V_i\} \in \Gamma_1$. Then,*

$$\log_2 |V_i| \geq H(S|B) \ .$$

proof:

$$\begin{aligned} H(S|B) &= H(S|BV_i) + I(S;V_i|B) \\ &= I(S;V_i|B) \\ &= H(V_i|B) - H(V_i|SB) \\ &\leq H(V_i|B) \ \leq \ H(V_i) \ \leq \ \log_2 |V_i| \ . \end{aligned}$$

□

Corollary 3.2 *For any maximal semi-access set B,*

$$\max_i \log_2 |V_i| \geq H(S|B) \ .$$

proof: For any maximal semi-access set B, there exists V_i such that $B \cup \{V_i\}$ because $\{V_1, \cdots, V_n\} \in \Gamma_1$. Then, from Theorem 3.3, we obtain this corollary. □

4 Some Lemmas on Entropy

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

Lemma 4.1 $H(S|XW) \geq H(S|X) - H(W)$.

proof:

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

□

Lemma 4.2 *If $Y = X \cup V_{i_1} \cup V_{i_2} \cdots \cup V_{i_k}$, then $H(S|Y) \geq H(S|X) - \sum_{j=1}^{k} H(V_{i_j})$.*

proof:

$$\begin{aligned} H(S|Y) &= H(S|XV_{i_1} \cdots V_{i_k}) \\ &\geq H(S|X) - H(V_{i_1} \cdots V_{i_k}) \quad \text{(from Lemma 4.1)} \\ &\geq H(S|X) - \sum_{j=1}^{k} H(V_{i_j}) \ . \end{aligned}$$

□

5 Summary

We have characterized nonperfect secret sharing schemes. First, we have shown that $(\Gamma_1, \Gamma_2, \Gamma_3)$ is realizable if and only if Γ_1 is monotone and $\Gamma_1 \cup \Gamma_2$ is monotone. Then, we have derived a lower bound of the $\max |V_i|$ in terms of a distance between Γ_1 and Γ_3.

References

[1] J.C.Benaloh, J.Leichter, *Generalized secret sharing and monotone functions*, Proceedings of Crypto'88, Lecture Notes on Comput. Sci., **403** (1990) 27–36

[2] C.Berge, *Graphs and Hypergraphs*, North Holland (1973)

[3] G.R.Blakley, *Safeguarding cryptographic keys*, Proceedings of the AFIPS 1979 National Computer Conference 48 (1979) 313–317

[4] G.R.Blakeley, C.Meadows, *Security of ramp schemes*, Proceedings of Crypto'84, Lecture Notes on Comput. Sci., **196** (1984) 242–268

[5] C.Blundo, A.De Santis, L.Gargano, U.Vaccaro, *On the information rate of secret sharing schemes*, Proceedings of Crypto'92, Lecture Notes on Comput. Sci., **740** (1992) 148–167

[6] C.Blundo, A.De Santis, D.R.Stinson, U.Vaccaro, *Graph decomposition and secret sharing schemes*, Proceedings of Eurorypt'92, Lecture Notes on Comput. Sci., **658** (1992) 1–20

[7] C.Blundo, A.De Santis, U.Vaccaro,

Efficient sharing of many secrets, Proceedings of STACS'93, Lecture Notes on Comput. Sci., **665** (1993) 692–703

[8] E.F.Brickell, D.M.Davenport, *On the classification of ideal secret sharing schemes*, Journal of Cryptology, vol.**4**, No.2 (1991) 123–134

[9] 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 (1992) 153–166

[10] 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 (1993) 157–167

[11] R.G.Gallager, *Information Theory and Reliable Communications*, John Wiley & Sons, New York, NY (1968)

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

[13] E.D.Karnin, J.W.Green, M.E.Hellman, *On secret sharing systems*, IEEE Trans. on Inform. Theory, IT-29 (1982) 35–41

[14] A.Shamir, *How to share a secret*, Communications of the ACM, Vol.**22**, No.11 (1979) 612–613

[15] D.R.Stinson, *New general bounds on the information rate of secret sharing schemes*, Proceedings of Crypto'92, Lecture Notes on Comput. Sci., **740** (1992) 168–182

[16] W.Ogata, K.Kurosawa, S.Tsujii, *Nonperfect secret sharing schemes*, Proceedings of Auscrypt'92, Lecture Notes on Comput. Sci., **718** (1992) 56–66

[17] K.Kurosawa, K.Okada, K.Sakano, W.Ogata, S.Tsujii, *Nonperfect secret sharing schemes and matroids*, Proceedings of Eurocrypt'93, Lecture Notes on Comput. Sci., **765** (1993) 126–141