PAPER

Secret Sharing Schemes Based on Linear Codes Can Be Precisely Characterized by the Relative Generalized Hamming Weight

Jun KURIHARA[†,††a)], ***Member***, **Tomohiko UYEMATSU**[†b)], ***Senior Member***, ***and*** **Ryutaroh MATSUMOTO**[†,†††c)], ***Member***

SUMMARY This paper precisely characterizes secret sharing schemes based on arbitrary linear codes by using the relative dimension/length profile (RDLP) and the relative generalized Hamming weight (RGHW). We first describe the equivocation Δ_m of the secret vector $\vec{s} = [s_1, \ldots, s_l]$ given m shares in terms of the RDLP of linear codes. We also characterize two thresholds t_1 and t_2 in the secret sharing schemes by the RGHW of linear codes. One shows that any set of at most t_1 shares leaks no information about $\vec{s}$, and the other shows that any set of at least t_2 shares uniquely determines $\vec{s}$. It is clarified that both characterizations for t_1 and t_2 are better than Chen et al.'s ones derived by the regular minimum Hamming weight. Moreover, this paper characterizes the strong security in secret sharing schemes based on linear codes, by generalizing the definition of strongly-secure threshold ramp schemes. We define a secret sharing scheme achieving the α-strong security as the one such that the mutual information between any r elements of $(s_1, \ldots, s_l)$ and any $\alpha - r + 1$ shares is always zero. Then, it is clarified that secret sharing schemes based on linear codes can always achieve the α-strong security where the value α is precisely characterized by the RGHW.

key words: *secret sharing scheme, linear code, relative generalized Hamming weight, relative dimension/length profile*

1. Introduction

Secret sharing scheme [2], [15] is a process of encoding a secret s into a set of n pieces of information segments (called *shares*) in such a way that only certain subsets of them can determine s. The collection of subsets that can determine s is called the *access structure* of the secret sharing scheme. An element in the access structure is called *qualified set*, otherwise, *nonqualified set*. Secret sharing schemes typically have the following complementary *thresholds* $t_1, t_2 (\leq n)$: (1) any set of at most t_1 shares leaks no information of the secret, and (2) any set of at least t_2 shares is qualified set. When the secret sharing scheme satisfies $t_1 + 1 = t_2$, the scheme is called a secret sharing scheme with the (t_2, n)-threshold access structure or (t_2, n)-*threshold scheme*. Shamir's scheme [15] is based on interpolation of a $(t_2 - 1)$-degree polynomial, and it is known as a typical (t_2, n)-threshold scheme.

McEliece et al. [12] first investigated the relation between linear codes and secret sharing schemes. They pointed out that shares in Shamir's threshold scheme [15] can be viewed as symbols of a codeword in Reed-Solomon code [10]. Piepryzk et al. [14] clarified that threshold schemes can be constructed from maximum distance separable (MDS) codes [10]. Massey [11] extended McEliece et al.'s construction to those based on general linear codes $\mathscr{C}$, and demonstrated that there exists a relationship between a qualified set and a codeword in the dual code $\mathscr{C}^{\perp}$ of $\mathscr{C}$. Duursma et al. [6] gave another construction of secret sharing schemes which use a linear code $\mathscr{C}$ and its subcode $\mathscr{C}' \subset \mathscr{C}$ with $\mathsf{dim}\,(\mathscr{C}/\mathscr{C}') = 1$ to encode s into shares. Moreover, they characterized the thresholds t_1, t_2 in their scheme by the minimum distance of the collection of cosets $\mathscr{C}/\mathscr{C}'$, called *coset distance*.

On the other hand, since regular (t_2, n)-threshold schemes generate shares from a secret scalar s, i.e., an element of a field $\mathbb{F}$, Blakley [1] and Yamamoto [18] generalized (t_2, n)-threshold schemes for an l-dimensional vector $\vec{s} = [s_1, \ldots, s_l] \in \mathbb{F}^l$ $(1 \leq l \leq t_2 - 1)$. Their schemes are called (t_2, l, n)-*threshold ramp schemes*, and realize l times smaller bit-size of each share than regular (t_2, n)-threshold schemes. In (t_2, l, n)-threshold schemes, there exists a trade-off between the size of each share and the amount of information leaked from nonqualified sets according to l. Namely, the thresholds t_1, t_2 satisfy $t_1 + l = t_2$, and i/l $(i = 1, \ldots, l-1)$ of Shannon entropy about $\vec{s}$ leaks from any set of $t_1 + i$ shares. Yamamoto [18] classified threshold ramp schemes into two classes. One is *weakly-secure* schemes, and the other is *strongly-secure* schemes. In the case of weakly-secure schemes, some elements of $\vec{s}$ might leak out deterministically from a set whose cardinality is smaller than t_2. In contrast, strongly-secure schemes guarantee that no information about a tuple $(s_i : i \in \mathscr{I})$ for any $\mathscr{I} \subseteq \{1, \ldots, l\}$ can be obtained from any $t_2 - |\mathscr{I}|$ shares. Hence, strongly-secure schemes are more secure than weakly-secure schemes. Threshold ramp schemes can be constructed by using MDS codes as well as regular threshold schemes. Nishiara et al. [13] proposed a strongly-secure threshold ramp schemes based on a polynomial interpolation. Their scheme employs a systematic MDS code transformed from a Reed-Solomon code.

Chen et al. [4] extended threshold ramp schemes, and

Manuscript received December 28, 2011.
Manuscript revised July 23, 2012.

[†]The authors are with the Department of Communications and Integrated Systems, Tokyo Institute of Technology, Tokyo, 152-8550 Japan.
[††]The author is with KDDI R&D Laboratories, Inc., Fujiminoshi, 356-8502 Japan.
[†††]The author is with the Department of Mathematical Sciences, Aalborg University, Denmark.
a) E-mail: kurihara@kddilabs.jp
b) E-mail: uyematsu@ieee.org
c) E-mail: ryutaroh@rmatsumoto.org

DOI: 10.1587/transfun.E95.A.2067

Table 1 Comparison of characterizations for thresholds t_1, t_2.

	Characterization method	Tightness of the characterization
[4, Sect. 4.1]	by minimum Hamming weight	not tight (Proposition 15, Example 16)
[4, Sect. 4.2]	by minimum Hamming weight	not tight (Proposition 12, Example 14)
[6]	by coset distance	tight (only for a scalar secret)
Theorem 9	by RGHW	always tight

Table 2 Comparison of characterizations for the α-strong security.

	Characterization method	Tightness of the characterization
[8]	by minimum Hamming weight	not tight (Proposition 20, Example 16)
Theorem 19	by RGHW	always tight

proposed two secret sharing schemes based on arbitrary linear codes. Namely, one given in [4, Sect. 4.1] is a simple extension of Massey's construction for an l-dimensional secret vector $\vec{s}$. The other called *more fruitful approach* in [4, Sect. 4.2] can be also viewed as a generalization of Duursma et al.'s construction [6] for $\vec{s}$. Later, Subramanian et al. [16] proposed a nested coding scheme over the erasure-erasure wiretap channel, which can be viewed as the same secret sharing scheme as Chen et al.'s more fruitful approach. By the minimum Hamming weight of linear codes, Chen et al. characterized thresholds t_1 and t_2 in each of their two constructions, respectively. However, these characterizations are loose, i.e., they do not always describe the maximum possible value of t_1 and the minimum possible value of t_2 in their schemes. Also, the information leaked from more than t_1 shares was not precisely analyzed. That is, no precise characterization of secret sharing schemes based on arbitrary linear codes has been presented yet.

The first aim of this paper is to characterize secret sharing schemes based on general linear codes precisely. We give a formal definition of secret sharing schemes based on linear codes by a linear code $\mathscr{D}_1$, its subcode $\mathscr{D}_2$, and their punctured codes $\mathscr{C}_1$ and $\mathscr{C}_2$. Our definition includes Massey's construction [11], Duursma et al.'s one [6] and both of Chen et al.'s two constructions [4]. We precisely characterize the minimum uncertainty (called *equivocation* [17]) of the secret vector given $m(\leq n)$ shares by the relative dimension/length profile (RDLP) [9] of $\mathscr{C}_1, \mathscr{C}_2$ or $\mathscr{D}_1, \mathscr{D}_2$. We also derive a new characterization of thresholds t_1 and t_2 by the relative generalized Hamming weight (RGHW) [9]. Table 1 summarizes the comparison of our characterization by the RGHW and existing ones by different methods for thresholds t_1, t_2. Duursma et al.'s characterization by the coset distance can be viewed as a special case of ours where the secret is restricted to be an elements of $\mathbb{F}$. Moreover, it is clarified that our characterization by the RGHW always describe the maximum possible t_1 and the minimum possible t_2, unlike Chen et al.'s ones.

The second aim of this paper is to characterize the strong security in secret sharing schemes based on general linear codes, by generalizing the definition of strongly-secure threshold ramp schemes. We first define an *anti-access set* $\mathscr{J}$ as a special set of shares, which is a generalized definition of nonqualified sets in strongly-secure ramp threshold schemes [18]. An anti-access set $\mathscr{J}$ guarantees that for any $\mathscr{I} \subseteq \{1, \ldots, l\}$, no information about a tuple $(s_i : i \in \mathscr{I})$ can be obtained from $|\mathscr{J}| + 1 - |\mathscr{I}|$ shares of $\mathscr{J}$. We also define a secret sharing scheme achieving the α-*strong security* as the one such that all subsets of shares with cardinality at most α are anti-access sets. We then clarify that the schemes of Massey [11] and Chen et al. [4, Sect. 4.1] can always achieve the α-strong security where the value α is precisely characterized by the RGHW. Table 2 presents the comparison of our characterization by the RGHW and existing one for the α-strong security. Similar to the thresholds t_1, t_2 we stated above, it is proved that the characterization of α by the RGHW is better than the existing characterization by the minimum Hamming weight [8].

One merit of secret sharing schemes based on arbitrary linear code is the efficiency in terms of the size of a field $\mathbb{F}$, since there is a rich variety of long linear codes over $\mathbb{F}$ rather than MDS codes over $\mathbb{F}$. This is because the MDS nature of the code restricts the maximum possible number of shares in threshold schemes. In fact, the so-called Main Conjecture on MDS codes [10, p.327] implies that the length of an MDS code over $\mathbb{F}$ is at most $|\mathbb{F}|$ plus a constant (1 or 2). Especially, the possible length of Reed-Solomon code over $\mathbb{F}$ is at most $|\mathbb{F}| - 1$. Hence, in order to generate more than $|\mathbb{F}|$ shares from a secret element $s \in \mathbb{F}$ by an MDS code, the MDS code must be constructed over a field whose size is larger than $|\mathbb{F}|$. It is quite inefficient, especially in the case where a secret sharing scheme is used in cryptographic secure computation [4]. In contrast, secret sharing schemes based on long linear codes can construct such applications efficiently. Then, our characterization precisely determines the property of secret sharing schemes from the parameter of the linear code.

The remainder of this paper is organized as follows. Sect. 2 introduces basic notations and gives a formal definition of secret sharing schemes based on linear codes. Sect. 3 precisely characterizes the amount of the secret information leaked from $m(\leq n)$ pieces of shares, and clarifies that our characterization is better than existing researches. Sect. 4 gives the definition of the strong security in secret sharing schemes. Further, this section reveals the region of the number of shares, in which the strong security can be achieved. Finally, Sect. 5 concludes this paper.

2. Preliminary

2.1 Basic Notations

Let $H(X)$ be Shannon's entropy of a random variable X, $H(X|Y)$ be the conditional entropy of X given Y, and $I(X;Y)$ be the mutual information between X and Y [5]. Let $\mathbb{F}$ stand for a finite field. Let $|\mathscr{X}|$ denote the cardinality of a set $\mathscr{X}$. For sets $\mathscr{X}$ and $\mathscr{Y}$, we denote by $\mathscr{X}\setminus\mathscr{Y} = \{x \in \mathscr{X} : x \notin \mathscr{Y}\}$ the difference of sets $\mathscr{X}$ and $\mathscr{Y}$. The *Hamming weight* of a vector $\vec{x} = [x_1, \ldots, x_n] \in \mathbb{F}^n$ is defined by

$$\mathsf{wt}(\vec{x}) = |\{i : x_i \neq 0\}|.$$

The *Hamming distance* between two vectors $\vec{x} = [x_1, \ldots, x_n] \in \mathbb{F}^n$, $\vec{y} = [y_1, \ldots, y_n] \in \mathbb{F}^n$ is defined by

$$d(\vec{x}, \vec{y}) = |\{i : x_i \neq y_i\}|.$$

For a linear subspace $\mathscr{C} \subseteq \mathbb{F}^n$, the *minimum Hamming distance* or *minimum Hamming weight* of $\mathscr{C}$ is given by

$$\begin{aligned} d(\mathscr{C}) &= \min\{d(\vec{x}, \vec{y}) : \vec{x}, \vec{y} \in \mathscr{C}, \vec{x} \neq \vec{y}\} \\ &= \min\left\{\mathsf{wt}(\vec{x}) : \vec{x} \in \mathscr{C}\setminus\{\vec{0}\}\right\}. \end{aligned}$$

An $[n,k,d]$ linear code $\mathscr{C}$ over $\mathbb{F}$ is a k-dimensional subspace of $\mathbb{F}^n$, where $d = d(\mathscr{C})$. A subspace of a code is called a *subcode*. For any linear code $\mathscr{C}$, we define its *dual code* by

$$\mathscr{C}^{\perp} = \{\vec{x} \in \mathbb{F}^n : \vec{x} \cdot \vec{y} = 0, \forall \vec{y} \in \mathscr{C}\},$$

where $\vec{x} \cdot \vec{y}$ represents the standard inner product of vectors $\vec{x}$ and $\vec{y}$.

2.2 Secret Sharing Scheme Based on Linear Codes

In this subsection, we formally define a secret sharing scheme based on linear codes.

Let $\mathscr{A} = \{1, \ldots, N\}$ be a set of indices. For a subset $\mathscr{J} \subseteq \mathscr{A}$ and a vector $\vec{c} = [c_1, \ldots, c_N] \in \mathbb{F}^N$, let $P_{\mathscr{J}}(\vec{c})$ be a vector of length N, and the t-th component of $P_{\mathscr{J}}(\vec{c})$ is c_t if $t \in \mathscr{J}$ and given by 0 if $t \notin \mathscr{J}$. For example for $\mathscr{J} = \{1,3,5\}$ and $\vec{c} = [1,1,0,1,1]$ ($N = 5$), we have $P_{\mathscr{J}}(\vec{c}) = [1,0,0,0,1]$. The *projection* or *punctured code* $P_{\mathscr{J}}(\mathscr{C})$ of a code $\mathscr{C} \in \mathbb{F}^N$ is the map given by

$$P_{\mathscr{J}}(\mathscr{C}) = \left\{P_{\mathscr{J}}(\vec{c}) : \vec{c} \in \mathscr{C}\right\}.$$

Now we define the following secret sharing scheme that generates n shares.

Definition 1 (Secret sharing schemes)**.** Let $\mathscr{D}_1 \subseteq \mathbb{F}^N$ be a linear code over $\mathbb{F}$, and $\mathscr{D}_2 \subset \mathscr{D}_1$ be a subcode of $\mathscr{D}_1$. For an index set $\mathscr{X} \subseteq \mathscr{A} = \{1, \ldots, N\}$ with $|\mathscr{X}| = n$ elements, we define the punctured codes $\mathscr{C}_1 = P_{\mathscr{X}}(\mathscr{D}_1)$ and $\mathscr{C}_2 = P_{\mathscr{X}}(\mathscr{D}_2)$. Assume that $|\mathscr{X}|$ is chosen in such a way that $\mathscr{C}_1 \neq \mathscr{C}_2$. Choose an arbitrary linear code $\mathscr{S}$ satisfying

$$\mathscr{C}_1 = \mathscr{S} + \mathscr{C}_2 \text{ and } \mathscr{S} \cap \mathscr{C}_2 = \{\vec{0}\},$$

i.e., direct sum. We then write the dimension of the coset $\mathscr{C}_1/\mathscr{C}_2$ by

$$l = \mathsf{dim}\,(\mathscr{C}_1/\mathscr{C}_2) = \mathsf{dim}\,\mathscr{S}.$$

Let $\vec{s} \in \mathbb{F}^l$ be the secret which is assumed to be uniformly distributed over $\mathbb{F}^l$. To generate n shares, we first choose a codeword $\vec{c}_2 \in \mathscr{C}_2$ uniformly at random and independently from $\vec{s}$. Fix an arbitrary isomorphism $\psi : \mathbb{F}^l \to \mathscr{S}$. Then, generate a share vector $\vec{c}_1 = [c_1, \ldots, c_N] = \psi(\vec{s}) + \vec{c}_2 \in \mathscr{C}_1$, and send or store each element c_i for $i \in \mathscr{X}$ as a share.

Here we note that $\mathscr{C}_2 \subset \mathscr{C}_1$ always holds in this definition. Also note that $\mathscr{S}$ can be always chosen, for instance by completing a basis of $\mathscr{C}_2$ to one of $\mathscr{C}_1$.

Let us consider the following case. Assume that $N - n < d(\mathscr{D}_1)$ and $N - n = \mathsf{dim}\,\mathscr{D}_1 - \mathsf{dim}\,\mathscr{D}_2$. We then write $l = \mathsf{dim}\,\mathscr{D}_1 - \mathsf{dim}\,\mathscr{D}_2 = N - n$, and let $\mathscr{X} = \{l+1, \ldots, l+n\}$. Choose ψ in such a way that $([\vec{s}, \vec{0}] + \psi(\vec{s}) + \vec{c}_2) \in \mathbb{F}^N$ is a codeword of $\mathscr{D}_1$. Then, our definition is equivalent to the one proposed by Massey [11] and Chen et al. [4, Sect. 4.1].

Moreover, the scheme given by Duursma et al. [6] and the scheme referred to as *a more fruitful approach* in [4, Sect. 4.2] by Chen et al. are also included in our definition as the case for $\mathscr{X} = \mathscr{A}$, i.e., $\mathscr{C}_1 = \mathscr{D}_1$ and $\mathscr{C}_2 = \mathscr{D}_2$.

3. Characterization of Secret Sharing Schemes

This section precisely characterizes the amount of the secret information leaked from $m(\leq n)$ pieces of shares in the secret sharing scheme given by Definition 1.

3.1 Equivocation of the Secret

Let S be a random variable whose realization is a secret vector $\vec{s}$. Let $C_{\mathscr{I}} = (C_i : i \in \mathscr{I})$ be a tuple of random variables for an index set $\mathscr{I} \subseteq \mathscr{X}$, where the realization of C_i is a share c_i. Then, the minimum uncertainty of S given m shares is defined by

$$\Delta_m = \min_{\mathscr{I} \subseteq \mathscr{X}, |\mathscr{I}| = m} H(S|C_{\mathscr{I}}), \tag{1}$$

which is called *equivocation* [17]. We will clarify that, in the secret sharing scheme defined by Definition 1, the equivocation of S is precisely characterized by the relative dimension/length profile (RDLP) [9].

For a subset $\mathscr{I}$ of $\mathscr{A} = \{1, \ldots, N\}$, the *shortened code* $\mathscr{C}_{\mathscr{I}}$ of a code $\mathscr{C} \subseteq \mathbb{F}^N$ is defined as the set of all codewords whose components are all zero outside of $\mathscr{I}$, that is,

$$\mathscr{C}_{\mathscr{I}} = \{\vec{c} = [c_1, \ldots, c_N] \in \mathscr{C} : c_i = 0 \text{ for } i \notin \mathscr{I}\}.$$

For example, for $\mathscr{J} = \{2,3\}$ ($N = 3$) and

$$\mathscr{C} = \{[0,0,0], [1,1,0], [1,0,1], [0,1,1]\},$$

we have $\mathscr{C}_{\mathscr{J}} = \{[0,0,0], [0,1,1]\}$.

The RDLP of $\mathscr{C}_1$ and $\mathscr{C}_2$ is defined by the maximum difference of dimension between shortened codes $(\mathscr{C}_1)_{\mathscr{I}}$ and $(\mathscr{C}_2)_{\mathscr{I}}$ as follows.

Definition 2 (Relative dimension/length profile [9])**.** Let $\mathscr{C}_1 \in \mathbb{F}^N$ be a linear code and $\mathscr{C}_2$ be a subcode of $\mathscr{C}_1$. The i-th relative dimension/length profile (RDLP) of $\mathscr{C}_1$ and $\mathscr{C}_2$ is defined by

$$K_i(\mathscr{C}_1,\mathscr{C}_2) = \max_{\mathscr{I}\subseteq\mathscr{A},|\mathscr{I}|=i}\{\mathsf{dim}\,(\mathscr{C}_1)_{\mathscr{I}} - \mathsf{dim}\,(\mathscr{C}_2)_{\mathscr{I}}\},$$

for $0 \le i \le N$.

Remark 3. When $\mathscr{C}_2 = \{\vec{0}\}$ in this definition, the i-th RDLP $K_i(\mathscr{C}_1,\mathscr{C}_2) = K_i(\mathscr{C}_1,\{\vec{0}\})$ is equivalent to the i-th regular dimension/length profile [7] of $\mathscr{C}_1$.

Note that, for a code $\mathscr{C} \subseteq \mathbb{F}^N$ and an index set $\mathscr{J} \subseteq \mathscr{A}$, dual codes of a punctured code $P_{\mathscr{J}}(\mathscr{C})$ and a shortened code $\mathscr{C}_{\mathscr{J}}$ are defined as

$$(P_{\mathscr{J}}(\mathscr{C}))^{\perp} = \{\vec{x} \in P_{\mathscr{J}}(\mathbb{F}^N) : \vec{x}\cdot\vec{y} = 0, \forall \vec{y} \in P_{\mathscr{J}}(\mathscr{C})\},$$
$$(\mathscr{C}_{\mathscr{J}})^{\perp} = \{\vec{x} \in P_{\mathscr{J}}(\mathbb{F}^N) : \vec{x}\cdot\vec{y} = 0, \forall \vec{y} \in \mathscr{C}_{\mathscr{J}}\},$$

respectively, i.e., dual codes over $P_{\mathscr{J}}(\mathbb{F}^N)$.

Theorem 4 determines the equivocation Δ_m defined in Eq.(1) by the RDLP of $\mathscr{C}_2^{\perp}$ and $\mathscr{C}_1^{\perp}$, and also $(\mathscr{D}_2^{\perp})_{\mathscr{X}}$ and $(\mathscr{D}_1^{\perp})_{\mathscr{X}}$.

Thereom 4. In the secret sharing scheme defined by Definition 1, the equivocation given $m(\le n)$ shares is characterized by the RDLP as follows.

$$\begin{aligned}\Delta_m &= l - K_m\left(\mathscr{C}_2^{\perp},\mathscr{C}_1^{\perp}\right)\\ &= l - K_m\left((\mathscr{D}_2^{\perp})_{\mathscr{X}},(\mathscr{D}_1^{\perp})_{\mathscr{X}}\right).\end{aligned}$$

Proof. Let $\mathscr{I} \subseteq \mathscr{X}$ be an arbitrary index set with cardinality $|\mathscr{I}| = m$. It is shown by [4, Theorem 10] that we have the conditional entropy of S given $C_{\mathscr{I}}$ as follows.

$$H(S|C_{\mathscr{I}}) = l - \mathsf{dim}\,P_{\mathscr{I}}(\mathscr{C}_1) + \mathsf{dim}\,P_{\mathscr{I}}(\mathscr{C}_2). \tag{2}$$

For a code $\mathscr{C} \subseteq \mathbb{F}^N$ and an index set $\mathscr{J} \subseteq \mathscr{A}$, we have $P_{\mathscr{J}}(\mathscr{C}^{\perp}) = (\mathscr{C}_{\mathscr{J}})^{\perp}$ and hence $P_{\mathscr{J}}(\mathscr{C}) = P_{\mathscr{J}}((\mathscr{C}^{\perp})^{\perp}) = ((\mathscr{C}^{\perp})_{\mathscr{J}})^{\perp}$ from Forney's second duality lemma [7, Lemma 2]. Thus, Eq.(2) can be rewritten as

$$\begin{aligned}H(S|C_{\mathscr{I}}) &= l - \mathsf{dim}\,((\mathscr{C}_1^{\perp})_{\mathscr{I}})^{\perp} + \mathsf{dim}\,((\mathscr{C}_2^{\perp})_{\mathscr{I}})^{\perp}\\ &= l - m + \mathsf{dim}\,(\mathscr{C}_1^{\perp})_{\mathscr{I}} + m - \mathsf{dim}\,(\mathscr{C}_2^{\perp})_{\mathscr{I}}\\ &= l - \mathsf{dim}\,(\mathscr{C}_2^{\perp})_{\mathscr{I}} + \mathsf{dim}\,(\mathscr{C}_1^{\perp})_{\mathscr{I}}.\end{aligned}$$

Recall $\mathscr{C}_1^{\perp}$ and $\mathscr{C}_2^{\perp}$ are defined as subspaces of $P_{\mathscr{X}}(\mathbb{F}^N)$ for an index set $\mathscr{X} \subseteq \mathscr{A}$. Hence the equivocation Δ_m is given by

$$\begin{aligned}\Delta_m &= l - \max_{\mathscr{I}\subseteq\mathscr{X},|\mathscr{I}|=m}\{\mathsf{dim}\,(\mathscr{C}_2^{\perp})_{\mathscr{I}} - \mathsf{dim}\,(\mathscr{C}_1^{\perp})_{\mathscr{I}}\}\\ &= l - K_m(\mathscr{C}_2^{\perp},\mathscr{C}_1^{\perp}),\end{aligned}$$

from Definition 2.

Lastly, we will prove the second equality. Forney's second duality lemma [7, Lemma 2] yields $\mathscr{C}_i = P_{\mathscr{X}}(\mathscr{D}_i) = P_{\mathscr{X}}((\mathscr{D}_i^{\perp})^{\perp}) = ((\mathscr{D}_i^{\perp})_{\mathscr{X}})^{\perp}$, and hence $\mathscr{C}_i^{\perp} = (\mathscr{D}_i^{\perp})_{\mathscr{X}}$ for $i = 1,2$. We thus have

$$\Delta_m = l - K_m((\mathscr{D}_2^{\perp})_{\mathscr{X}},(\mathscr{D}_1^{\perp})_{\mathscr{X}}).$$

□

3.2 Bounds of Thresholds

Secret sharing schemes typically have the following complementary *thresholds* t_1,t_2: (1) any set $\mathscr{I} \subseteq \mathscr{X}$ of at most t_1 shares offers the mutual information $I(S;C_{\mathscr{I}}) = 0$, and (2) any set $\mathscr{J} \subseteq \mathscr{X}$ of at least t_2 shares offers the mutual information $I(S;C_{\mathscr{J}}) = H(S)$. This section clarifies the maximum value of t_1 and minimum value of t_2 in the secret sharing scheme of Definition 1 by the relative generalized Hamming weight (RGHW) defined by Luo et al. [9].

Definition 5 (Relative generalized Hamming weight [9])**.** Let $\mathscr{A} = \{1,\ldots,N\}$. Let $\mathscr{C}_1 \in \mathbb{F}^N$ be a linear code and $\mathscr{C}_2$ be a subcode of $\mathscr{C}_1$. The i-th relative generalized Hamming weight (RGHW) of $\mathscr{C}_1$ and $\mathscr{C}_2$ is defined by

$$M_i(\mathscr{C}_1,\mathscr{C}_2) = \min_{\mathscr{I}\subseteq\mathscr{A}}\{|\mathscr{I}| : \mathsf{dim}\,(\mathscr{C}_1)_{\mathscr{I}} - \mathsf{dim}\,(\mathscr{C}_2)_{\mathscr{I}} \ge i\},$$

for $0 \le i \le \mathsf{dim}\,(\mathscr{C}_1/\mathscr{C}_2)$.

The following proposition given by Luo et al. [9] clarifies the relationship between the RGHW and the RDLP.

Proposition 6 ([9, Proposition 2])**.** Let $\mathscr{A} = \{1,\ldots,N\}$. For a linear code $\mathscr{C}_1 \in \mathbb{F}^N$ and its subcode $\mathscr{C}_2 \subset \mathscr{C}_1$, the i-th RGHW $M_i(\mathscr{C}_1,\mathscr{C}_2)$ is strictly increasing with i. Moreover, $M_0(\mathscr{C}_1,\mathscr{C}_2) = 0$ and

$$\begin{aligned}M_i(\mathscr{C}_1,\mathscr{C}_2) &= \min_{\mathscr{I}\subseteq\mathscr{A}}\{|\mathscr{I}| : \mathsf{dim}\,(\mathscr{C}_1)_{\mathscr{I}} - \mathsf{dim}\,(\mathscr{C}_2)_{\mathscr{I}} = i\},\\ &= \min\{m : K_m(\mathscr{C}_1,\mathscr{C}_2) = i\},\end{aligned}$$

for $0 \le i \le \mathsf{dim}\,(\mathscr{C}_1/\mathscr{C}_2)$, where $K_m(\cdot,\cdot)$ is the RDLP defined by Definition 2.

Remark 7. When $\mathscr{C}_2 = \{\vec{0}\}$, the i-th RGHW $M_i(\mathscr{C}_1,\mathscr{C}_2) = M_i(\mathscr{C}_1,\{\vec{0}\})$ is equivalent to the i-th regular generalized Hamming weight [17] of $\mathscr{C}_1$.

Remark 8. The first RGHW $M_1(\mathscr{C}_1,\mathscr{C}_2)$ of $\mathscr{C}_1$ and $\mathscr{C}_2$ is equivalent to the coset distance of $\mathscr{C}_1/\mathscr{C}_2$, given by Duursma et al. [6].

We then give the following theorem.

Thereom 9. Consider the secret sharing scheme defined by Definition 1. Then, for a set $\mathscr{I} \subseteq \mathscr{X}$, the mutual information between S and $C_{\mathscr{I}}$ satisfies $I(S;C_{\mathscr{I}}) = 0$ if

$$|\mathscr{I}| \le M_1(\mathscr{C}_2^{\perp},\mathscr{C}_1^{\perp}) - 1, \tag{3}$$

and $I(S;C_{\mathscr{I}}) = H(S)$ if

$$|\mathscr{I}| \geq n - M_1(\mathscr{C}_1, \mathscr{C}_2) + 1. \tag{4}$$

Proof. For an arbitrary index set $\mathscr{I} \subseteq \mathscr{X}$ with cardinality $|\mathscr{I}| = m$, the maximum mutual information between S and $C_{\mathscr{I}}$ is expressed by the equivocation from Theorem 4 as follows.

$$\begin{aligned}\max_{\mathscr{I}\subseteq\mathscr{X},|\mathscr{I}|=m} I(S;C_{\mathscr{I}}) &= H(S) - \min_{\mathscr{I}\subseteq\mathscr{X},|\mathscr{I}|=m} H(S|C_{\mathscr{I}}) \\ &= K_m(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}).\end{aligned}$$

Hence, from Proposition 6, the smallest index set satisfying $I(S;C_{\mathscr{I}}) = 1$ is of size

$$\min\{m : K_m(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}) = 1\} = M_1(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}).$$

This implies that $I(S;C_{\mathscr{I}}) = 0$ whenever Eq.(3) holds.

Next consider the minimum mutual information between S and $C_{\mathscr{I}}$ for $|\mathscr{I}| = m$. The relation between the shortened code and punctured code of a code $\mathscr{C} \subseteq \mathbb{F}^N$ for an index set $\mathscr{J} \subseteq \mathscr{A}$ is given by $\dim \mathscr{C} = \dim \mathscr{C}_{\mathscr{J}} + \dim P_{\mathscr{J}}(\mathscr{C})$ from Forney's first duality lemma [7, Lemma 1], where $\bar{\mathscr{J}} = \mathscr{A} \setminus \mathscr{J}$. Hence, Eq.(2) can be rewritten as

$$H(S|C_{\mathscr{I}}) = \dim (\mathscr{C}_1)_{\bar{\mathscr{I}}} - \dim (\mathscr{C}_2)_{\bar{\mathscr{I}}}, \tag{5}$$

where $\bar{\mathscr{I}} = \mathscr{X} \setminus \mathscr{I}$. Thus, the minimum mutual information is given by

$$\begin{aligned}&\min_{\mathscr{I}\subseteq\mathscr{X},|\mathscr{I}|=m} I(S;C_{\mathscr{I}}) \\ &\quad= H(S) - \max_{\mathscr{I}\subseteq\mathscr{X},|\mathscr{I}|=m} H(S|C_{\mathscr{I}}) \\ &\quad= l - \max_{\mathscr{I}\subseteq\mathscr{X},|\mathscr{I}|=m} \{\dim (\mathscr{C}_1)_{\bar{\mathscr{I}}} - \dim (\mathscr{C}_2)_{\bar{\mathscr{I}}}\} \\ &\quad= l - \max_{\bar{\mathscr{I}}\subseteq\mathscr{X},|\bar{\mathscr{I}}|=n-m} \{\dim (\mathscr{C}_1)_{\bar{\mathscr{I}}} - \dim (\mathscr{C}_2)_{\bar{\mathscr{I}}}\} \\ &\quad= l - K_{n-m}(\mathscr{C}_1, \mathscr{C}_2).\end{aligned}$$

From Proposition 6, we thus have the largest index set $\mathscr{I}$ satisfying $I(S;C_{\mathscr{I}}) = l - 1$ is of size

$$\begin{aligned}&\max\{m : K_{n-m}(\mathscr{C}_1, \mathscr{C}_2) = 1\} \\ &\quad= \max\{n - m : K_m(\mathscr{C}_1, \mathscr{C}_2) = 1\} \\ &\quad= n - \min\{m : K_m(\mathscr{C}_1, \mathscr{C}_2) = 1\} \\ &\quad= n - M_1(\mathscr{C}_1, \mathscr{C}_2).\end{aligned}$$

This implies that $I(S;C_{\mathscr{I}}) = 0$ whenever Eq.(4) holds. □

Remark 10. Eq.(5) is the same equation as [16, Eq. (4)] derived by Subramanian et al.

The thresholds given by the right-hand side of Eq.(3) and Eq.(4) in Theorem 9 are always tight. This is because the proof of Theorem 9 also reveals that there exist index sets $\mathscr{I} \subseteq \mathscr{X}$ with $|\mathscr{I}| = M_1(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp})$ satisfying $I(S;C_{\mathscr{I}}) = 1$ and $\mathscr{J} \subseteq \mathscr{X}$ with $|\mathscr{J}| = n - M_1(\mathscr{C}_1, \mathscr{C}_2)$ satisfying $I(S;C_{\mathscr{J}}) = l - 1$.

Although we have assumed, in Definition 1, that $\vec{s}$ is uniformly distributed over $\mathbb{F}^l$, the following corollary immediately follows from [3, Lemma 2, Theorem 3].

Corollary 11. In Definition 1, assume that $\vec{s} \in \mathbb{F}^l$ is chosen according to an arbitrary distribution over $\mathbb{F}^l$ and independently from $\vec{c}_2$. Even in this case, Theorem 9 still holds.

Note that the size of smallest index set $\mathscr{I}$ satisfying $I(S;C_{\mathscr{I}}) = l$ is $M_l(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp})$, since $\dim \mathscr{C}_2^{\perp} - \dim \mathscr{C}_1^{\perp} = \dim \mathscr{C}_1 - \dim \mathscr{C}_2 = l$ from Definition 1. Then, $M_l(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}) \leq n$ always holds from Definition 5. Thus the secret vector $\vec{s}$ can always be reconstructed from some subsets of shares in the secret sharing scheme.

3.2.1 Comparison with Existing Results

Here we clarify that our bounds given in Theorem 9 are tighter than the ones of existing results.

First, consider the case of $\mathscr{X} = \mathscr{A}$, i.e., $\mathscr{D}_1 = \mathscr{C}_1$ and $\mathscr{D}_2 = \mathscr{C}_2$, in the secret sharing scheme defined in Definition 1. Then, the scheme is equivalent to that of Duursma et al. [6] and the one referred to as a more fruitful approach in [4, Sect. 4.2]. For this case, Chen et al. proved in [4, Corollary 4] that any index set $\mathscr{I} \subseteq \mathscr{X}$ offers $I(S;C_{\mathscr{I}}) = 0$ if

$$|\mathscr{I}| \leq d(\mathscr{C}_2^{\perp}) - 1,$$

and $I(S;C_{\mathscr{I}}) = H(S)$ if

$$|\mathscr{I}| \geq n - d(\mathscr{C}_1) + 1.$$

Although Chen et al. [4] mentioned that these bounds are not tight, they did not show any evidence.

Proposition 12. Assume that $\mathscr{X} = \mathscr{A}$ in the secret sharing scheme defined by Definition 1. Then, thresholds given by the right-hand side of Eq.(3) and Eq.(4) in Theorem 9 satisfy $M_1(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}) - 1 \geq d(\mathscr{C}_2^{\perp}) - 1$ and $n - M_1(\mathscr{C}_1, \mathscr{C}_2) + 1 \leq n - d(\mathscr{C}_1) + 1$, respectively.

Proof. From the definition of the RGHW (Definition 5), we always have $M_1(\mathscr{C}_1, \mathscr{C}_2) \geq M_1(\mathscr{C}_1, \{\vec{0}\})$. Recall that the first generalized Hamming weight [17] of $\mathscr{C}_1$ is represented by $M_1(\mathscr{C}_1, \{\vec{0}\})$ from Remark 7. Since the first generalized Hamming weight is the minimum Hamming weight [17], we have $d(\mathscr{C}_1) = M_1(\mathscr{C}_1, \{\vec{0}\})$. Thus, $M_1(\mathscr{C}_1, \mathscr{C}_2) \geq d(\mathscr{C}_1)$ always holds. Similarly, we have $M_1(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}) \geq M_1(\mathscr{C}_2^{\perp}, \{\vec{0}\}) = d(\mathscr{C}_2^{\perp})$. These establish $|\mathscr{I}| > n - d(\mathscr{C}_1) \geq n - M_1(\mathscr{C}_1, \mathscr{C}_2)$ for the threshold of $I(S;C_{\mathscr{I}}) = H(S)$, and $|\mathscr{I}| < d(\mathscr{C}_2^{\perp}) \leq M_1(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp})$ for that of $I(S;C_{\mathscr{I}}) = 0$, respectively. □

Remark 13. The scheme of Duursma et al. is equivalent to the case of $l = \dim \mathscr{C}_1 - \dim \mathscr{C}_2 = 1$. The bounds derived by the coset distance in [6, Corollary 1.7] is equivalent to our bounds of Theorem 9 for $l = 1$.

The next example shows that [4, Corollary 4] is not tight.

Example 14 ([9, p.1227])**.** Let $\mathscr{C}_1$ be a binary linear code with generator matrix G_1 and $\mathscr{C}_2 \subset \mathscr{C}_1$ be a subcode with a generator matrix G_2, where

$$G_1 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad G_2 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Then, $d(\mathscr{C}_1) = 2$ and $K_2(\mathscr{C}_1, \mathscr{C}_2) = 0$. Since the RDLP is monotonically increasing, $M_1(\mathscr{C}_1, \mathscr{C}_2) > 2$ holds. We thus have $M_1(\mathscr{C}_1, \mathscr{C}_2) > d(\mathscr{C}_1)$.

Next, consider the following case of Definition 1. Assume that $N - n < d(\mathscr{D}_1)$ and $N - n = \mathsf{dim}\ \mathscr{D}_1 - \mathsf{dim}\ \mathscr{D}_2$. We then write $l = \mathsf{dim}\ \mathscr{D}_1 - \mathsf{dim}\ \mathscr{D}_2 = N - n$, and let $\mathscr{X} = \{l+1, \ldots, l+n\}$. Choose ψ in such a way that $([\vec{s}, \vec{0}] + \psi(\vec{s}) + \vec{c}_2) \in \mathbb{F}^N$ is a codeword of $\mathscr{D}_1$. Then, this case is equivalent to the one proposed by Massey [11] and Chen et al. [4, Sect. 4.1]. We note that $\mathsf{dim}\ \mathscr{D}_1 = \mathsf{dim}\ \mathscr{C}_1$ and $\mathsf{dim}\ \mathscr{D}_2 = \mathsf{dim}\ \mathscr{C}_2$ since $N - n < d(\mathscr{D}_1)$, and that such ψ always exists. For this case, Chen et al. characterized in [4, Sect. 4.1] that any index set $\mathscr{I} \subseteq \mathscr{X}$ offers $I(S; C_{\mathscr{I}}) = 0$ if

$$|\mathscr{I}| \leq d(\mathscr{D}_1^\perp) - l - 1,$$

and $I(S; C_{\mathscr{I}}) = H(S)$ if

$$|\mathscr{I}| \geq n + l - d(\mathscr{D}_1) + 1.$$

The following proposition proves that these bounds are not tight.

Proposition 15. Assume that $N - n < d(\mathscr{D}_1)$ and $l = N - n = \mathsf{dim}\ \mathscr{D}_1 - \mathsf{dim}\ \mathscr{D}_2$ in the secret sharing scheme defined by Definition 1. Let $\mathscr{X} = \{l+1, \ldots, l+n\}$, and let ψ be chosen such that $([\vec{s}, \vec{0}] + \psi(\vec{s}) + \vec{c}_2) \in \mathscr{D}_1$. Then, thresholds given by the right-hand side of Eq.(3) and Eq.(4) in Theorem 9 satisfy $M_1(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp) - 1 \geq d(\mathscr{D}_1^\perp) - l - 1$ and $n - M_1(\mathscr{C}_1, \mathscr{C}_2) + 1 \leq n + l - d(\mathscr{D}_1) + 1$, respectively.

Proof. First, we prove $M_1(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp) - 1 \geq d(\mathscr{D}_1^\perp) - l - 1$. Let $G \in \mathbb{F}^{\mathsf{dim}\ \mathscr{D}_1 \times N}$ be a generator matrix of $\mathscr{D}_1$. Then, the first l columns of G and arbitrary $d(\mathscr{D}_1^\perp) - l - 1$ columns chosen from the last n columns of G always span $\mathbb{F}^{d(\mathscr{D}_1)-1}$. This guarantees that $I(S; C_{\mathscr{I}}) = 0$ if $|\mathscr{I}| \leq d(\mathscr{D}_1^\perp) - l - 1$ [4, Sect. 4.1].

Recall that arbitrary $d(\mathscr{D}_1^\perp) - 1$ columns of G are always linearly independent, and some $d(\mathscr{D}_1^\perp)$ columns are linearly dependent [10]. However, in Chen et al.'s proof, only $d(\mathscr{D}_1^\perp) - l - 1$ columns of $d(\mathscr{D}_1^\perp) - 1$ columns are arbitrary chosen. This implies that, depending on $\mathscr{D}_1$, there exist cases such that the first l columns of G and arbitrary $d(\mathscr{D}_1^\perp) - l$ columns chosen from the last n columns are always linearly independent. Then, $I(S; C_{\mathscr{I}}) = 0$ if $|\mathscr{I}| \leq d(\mathscr{D}_1^\perp) - l$. Hence we have $d(\mathscr{D}_1^\perp) - l - 1 \leq M_1(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp) - 1$ since the threshold given by the right-hand side of Eq.(3) is always tight.

Next we prove $n - M_1(\mathscr{C}_1, \mathscr{C}_2) + 1 \leq n + l - d(\mathscr{D}_1) + 1$. Since $\mathscr{C}_1 = P_{\mathscr{X}}(\mathscr{D}_1)$ is generated by puncturing the first l symbols of each codeword in $\mathscr{D}_1$, we have $d(\mathscr{C}_1) \geq d(\mathscr{D}_1) - l$. On the other hand, $M_1(\mathscr{C}_1, \mathscr{C}_2) \geq d(\mathscr{C}_1)$ holds since $d(\mathscr{C}_1)$ can be represented by $d(\mathscr{C}_1) = M_1(\mathscr{C}_1, \{\vec{0}\})$. We thus obtain

$$M_1(\mathscr{C}_1, \mathscr{C}_2) \geq d(\mathscr{C}_1) \geq d(\mathscr{D}_1) - l.$$

This establishes $n + l - d(\mathscr{D}_1) + 1 \geq n - M_1(\mathscr{C}_1, \mathscr{C}_2) + 1$. □

Example 14 gives a case satisfying the inequality $n + l - d(\mathscr{D}_1) + 1 \geq n - d(\mathscr{C}_1) + 1 > n - M_1(\mathscr{C}_1, \mathscr{C}_2) + 1$, and the following example shows a case satisfying the inequality $d(\mathscr{D}_1^\perp) - l - 1 < M_1(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp) - 1$ in Proposition 15.

Example 16. Let $\mathscr{D}_1$ be a binary linear code with a generator matrix G and a parity check matrix H defined by

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix},$$

respectively. We have $d(\mathscr{D}_1) = 2$ and $d(\mathscr{D}_1^\perp) = 2$. Let $l = 1 < d(\mathscr{D}_1)$ and $\mathscr{X} = \{2, 3, 4, 5, 6\}$. Then, $d(\mathscr{D}_1^\perp) - l - 1 = 0$. However, the first column of G and arbitrary $1 = d(\mathscr{D}_1^\perp) - l$ column chosen from the last 5 columns of G are always linearly independent. On the other hand, now consider a punctured code $\mathscr{C}_1 = P_{\mathscr{X}}(\mathscr{D}_1)$ with a generator matrix G_1 and its subcode $\mathscr{C}_2$ with a generator matrix G_2, where

$$G_1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad G_2 = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Let $\mathscr{C}_2^\perp$ and $\mathscr{C}_1^\perp$ be their dual codes with generator matrices G_2' and G_1' given by

$$G_2' = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad G_1' = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix},$$

respectively. Then, we obtain $K_2(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp) = 1$ and hence $M_1(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp) = 2$. Therefore, $M_1(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp) > d(\mathscr{D}_1^\perp) - l$ holds.

4. Strong Security of Secret Sharing Schemes

This section gives a refined definition of the strong security in secret sharing schemes. Further, we reveal that the scheme of Massey [11] and Chen et al. [4] can always achieve the strong security in the certain range of the number of shares, characterized by the RGHW.

4.1 Definition of the Strong Security

First, we introduce a special subset $\mathscr{J}$ of $\mathscr{X}$ called an *anti-access set*. This is the generalized definition of non-qualified sets in strongly-secure threshold ramp schemes, which is given by Yamamoto [18]. Let a secret vector be represented by $\vec{s} = [s_1, \ldots, s_l]$, and S_i $(1 \leq i \leq l)$ be

a random variable whose realization is s_i. We denote by $S_{\mathscr{I}} = (S_i : i \in \mathscr{I})$ a tuple of random variables for an index set $\mathscr{I} \subseteq \{1,\ldots,l\}$. Assume that each share c_i $(i \in \mathscr{X})$ is obtained from $\vec{s}$ as we presented in Sect. 2.1, and $S_1,\ldots,S_l$ are uniformly distributed over $\mathbb{F}$ and mutually independent. We then define an anti-access set as follows.

Definition 17 (Anti-access sets)**.** Let $\mathscr{J} \subseteq \mathscr{X}$ be an index set. For any subsets $\mathscr{F} \subseteq \mathscr{J}$ and $\mathscr{E} \subseteq \{1,\ldots,l\}$ with $|\mathscr{E}| + |\mathscr{F}| = |\mathscr{J}| + 1$, if we have

$$I(S_{\mathscr{E}}; C_{\mathscr{F}}) = 0, \tag{6}$$

$\mathscr{J}$ is called an *anti-access set*.

Now we define the *α-strong security* of secret sharing schemes.

Definition 18 (α-strong security)**.** A secret sharing scheme is called the one achieving *α-strong security* if all $\mathscr{J} \subseteq \mathscr{X}$ with $|\mathscr{J}| = \alpha$ are anti-access sets.

Consider the case where the thresholds given by the right-hand side of Eq.(3) and Eq.(4) in Theorem 9 satisfy

$$M_1(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}) - 1 = \mathsf{dim}\, \mathscr{C}_2,$$
$$\text{and} \quad n - M_1(\mathscr{C}_1, \mathscr{C}_2) + 1 = \mathsf{dim}\, \mathscr{C}_1,$$

respectively. This can be attained when both $\mathscr{C}_1$ and $\mathscr{C}_2$ are maximum distance separable (MDS) codes [10], e.g., Reed-Solomon codes. Then, from Theorem 9, the secret sharing scheme defined by Definition 1 is equivalent to a $(\mathsf{dim}\, \mathscr{C}_1, \mathsf{dim}\, (\mathscr{C}_2/\mathscr{C}_1), n)$-threshold ramp scheme [1], [18]. Moreover, if the scheme achieves the $(\mathsf{dim}\, \mathscr{C}_1 - 1)$-strong security, i.e., all nonqualified sets are anti-access sets, it is called a strongly-secure threshold ramp scheme [13], [18].

4.2 Characterization of the α-Strong Security

This subsection clarifies that the scheme proposed by Massey [11] and Chen et al. [4] can achieve the α-strong security where the value α is precisely characterized by the RGHW.

Consider the following case of Definition 1. Assume that $N - n < d(\mathscr{D}_1)$ and $N - n = \mathsf{dim}\, \mathscr{D}_1 - \mathsf{dim}\, \mathscr{D}_2$. We then write $l = \mathsf{dim}\, \mathscr{D}_1 - \mathsf{dim}\, \mathscr{D}_2 = N - n$, and let $\mathscr{X} = \{l+1,\ldots,l+n\}$. Choose ψ in such a way that $([\vec{s}, \vec{0}] + \psi(\vec{s}) + \vec{c}_2) \in \mathbb{F}^N$ is a codeword of $\mathscr{D}_1$. Then, this case is equivalent to the one proposed by Massey [11] and Chen et al. [4, Sect. 4.1]. We note that $\mathsf{dim}\, \mathscr{D}_1 = \mathsf{dim}\, \mathscr{C}_1$ and $\mathsf{dim}\, \mathscr{D}_2 = \mathsf{dim}\, \mathscr{C}_2$ since $N - n < d(\mathscr{D}_1)$, and that such ψ always exists.

Without any loss of generality, we suppose that $\mathscr{D}_1$ is a systematic code. In other words, a generator matrix G_1 of $\mathscr{D}_1$ is defined by the systematic form,

$$G_1 = \begin{bmatrix} I & P \end{bmatrix} \in \mathbb{F}^{\mathsf{dim}\, \mathscr{D}_1 \times N},$$

where I is an identity matrix. Also, a generator matrix G_2 of $\mathscr{D}_2$ consists of last $\mathsf{dim}\, \mathscr{D}_2$ rows of G_1. Under these suppositions, we have the following theorem.

Thereom 19. Assume $N - n < d(\mathscr{D}_1)$ and $l = N - n = \mathsf{dim}\, \mathscr{D}_1 - \mathsf{dim}\, \mathscr{D}_2$ in the secret sharing scheme defined by Definition 1. Let $\mathscr{X} = \{l+1,\ldots,l+n\} \subset \mathscr{A}$, and let ψ be chosen such that $([\vec{s}, \vec{0}] + \psi(\vec{s}) + \vec{c}_2) \in \mathscr{D}_1$. Let $\mathscr{Y}_i = \{1,\ldots,l+n\}\backslash\{i\}$ be another index set for $1 \le i \le l$, and define a punctured code $\mathscr{G}_{1,i} = P_{\mathscr{Y}_i}(\mathscr{D}_1)$ and a shortened code $\mathscr{G}_{2,i} = (\mathscr{D}_1)_{\mathscr{Y}_i}$. Then, the secret sharing scheme defined by Definition 1 can achieve the α-strong security for

$$\alpha = \min\left\{ M_1(\mathscr{G}_{2,i}^{\perp}, \mathscr{G}_{1,i}^{\perp}) : 1 \le i \le l \right\} - 1.$$

Proof. Since we supposed that a generator matrix G_1 of $\mathscr{D}_1$ is systematic, the secret sharing scheme generates shares $c_{l+1},\ldots,c_{l+n}$ by

$$[s_1,\ldots,s_l,c_{l+1},\ldots,c_{l+n}] = [s_1,\ldots,s_l,r_{l+1},\ldots,r_{\mathsf{dim}\, \mathscr{D}_1}]G_1, \tag{7}$$

where $r_{l+1},\ldots,r_{\mathsf{dim}\, \mathscr{D}_1}$ are chosen from $\mathbb{F}$ at random. This guarantees that, for each $i \in \{1,\ldots,l\}$, $\mathscr{G}_{2,i}$ is a subcode of $\mathscr{G}_{1,i}$ with dimension $\mathsf{dim}\, \mathscr{G}_{2,i} = \mathsf{dim}\, \mathscr{G}_{1,i} - 1 = \mathsf{dim}\, \mathscr{D}_1 - 1$. We have supposed that $s_1,\ldots,s_l$ are mutually independent and uniformly distributed over $\mathbb{F}$. Hence, for each $i \in \{1,\ldots,l\}$, the secret sharing scheme given by Eq.(7) can be viewed as another secret sharing scheme that generates shares $s_1,\ldots,s_{i-1},s_{i+1},\ldots,s_l,c_{l+1},\ldots,c_{l+n}$ from one secret element s_i. Namely, a secret sharing scheme with $\mathscr{D}_1$, subcode $\mathscr{G}_{2,i} \subset \mathscr{D}_1$, and their punctured codes $P_{\mathscr{Y}_i}(\mathscr{D}_1) = \mathscr{G}_{1,i}, P_{\mathscr{Y}_i}(\mathscr{G}_{2,i}) = \mathscr{G}_{2,i}$ for an index set $\mathscr{Y}_i$. Therefore, Theorem 9 yields that for any index sets $\mathscr{R}_1 \subseteq \{1,\ldots,l\}\backslash\{i\}$ and $\mathscr{R}_2 \subseteq \{l+1,\ldots,l+n\}$ with $|\mathscr{R}_1| + |\mathscr{R}_2| \le M_1(\mathscr{G}_{2,i}^{\perp}, \mathscr{G}_{1,i}^{\perp}) - 1$, we have

$$I(S_i; S_{\mathscr{R}_1}, C_{\mathscr{R}_2}) = 0. \tag{8}$$

Next consider the mutual information between a subset of secret elements and a subset of shares. Let $\mathscr{E} = \{k_1,\ldots,k_{|\mathscr{E}|}\} \subseteq \{1,\ldots,l\}$ and $\mathscr{F} \subseteq \{l+1,\ldots,l+n\}$ be arbitrary index sets. We then have

$$\begin{aligned} I(S_{\mathscr{E}}; C_{\mathscr{F}}) &= H(S_{k_1},\ldots,S_{k_{|\mathscr{E}|}}) - H(S_{k_1},\ldots,S_{k_{|\mathscr{E}|}}|C_{\mathscr{F}}) \\ &= \sum_{j=1}^{|\mathscr{E}|} H(S_{k_j}) - \sum_{j=1}^{|\mathscr{E}|} H(S_{k_j}|C_{\mathscr{F}}, S_{k_1},\ldots,S_{k_{j-1}}) \\ &= \sum_{j=1}^{|\mathscr{E}|} I(S_{k_j}; C_{\mathscr{F}}, S_{k_1},\ldots,S_{k_{j-1}}), \end{aligned}$$

from the chain rule of conditional entropy [5]. Since the mutual information is nonnegative, we have $I(S_{\mathscr{E}}; C_{\mathscr{F}}) = 0$ if and only if $I(S_{k_j}; C_{\mathscr{F}}, S_{k_1},\ldots,S_{k_{j-1}}) = 0$ for all $k_j \in \mathscr{E}$. If $|\mathscr{E}| + |\mathscr{F}| \le M_1(\mathscr{G}_{2,k_j}^{\perp}, \mathscr{G}_{1,k_j}^{\perp})$, by substituting $i = k_j$, $\mathscr{R}_1 = \{k_1,\ldots,k_{j-1}\}$ and $\mathscr{R}_2 = \mathscr{F}$ in Eq.(8), we always have $I(S_{k_j}; C_{\mathscr{F}}, S_{k_1},\ldots,S_{k_{j-1}}) = 0$ for only k_j. Thus, for any index sets $\mathscr{E}$ and $\mathscr{F}$ satisfying

$$|\mathscr{E}|+|\mathscr{F}| \le \min\left\{M_1(\mathscr{G}_{2,i}^{\perp},\mathscr{G}_{1,i}^{\perp}) : 1 \le i \le l\right\},$$

we always have $I(S_{k_j};C_{\mathscr{F}},S_{k_1},\ldots,S_{k_{j-1}}) = 0$ for all k_j simultaneously, and hence $I(S_{\mathscr{E}};C_{\mathscr{F}}) = 0$ holds. Therefore, every subset of $\{l+1,\ldots,l+n\}$ with cardinality at most

$$\alpha = \min\left\{M_1(\mathscr{G}_{2,i}^{\perp},\mathscr{G}_{1,i}^{\perp}) : 1 \le i \le l\right\} - 1,$$

is an anti-access set. □

The value α in Theorem 19 for the α-strong security is as tight as the bounds in Theorem 9. This is because as follows. Let $j \in \{1,\ldots,l\}$ be an element satisfying $M_1(\mathscr{G}_{2,j}^{\perp},\mathscr{G}_{1,j}^{\perp}) = \min\left\{M_1(\mathscr{G}_{2,i}^{\perp},\mathscr{G}_{1,i}^{\perp}) : 1 \le i \le l\right\}$. Then, since the the threshold given by the right-hand side of Eq.(3) in Theorem 9 is tight, there always exists at least one combination of subsets $\mathscr{T}_1 \subseteq \{1,\ldots,l\}\backslash\{j\}$ and $\mathscr{T}_2 \subseteq \{l+1,\ldots,l+n\}$ with $|\mathscr{T}_1|+|\mathscr{T}_2| = M_1(\mathscr{G}_{2,j}^{\perp},\mathscr{G}_{1,j}^{\perp})$ that satisfy $I(S_j;S_{\mathscr{T}_1},C_{\mathscr{T}_2}) > 0$. Hence, there exist subsets of $\{l+1,\ldots,l+n\}$ with cardinality $M_1(\mathscr{G}_{2,j}^{\perp},\mathscr{G}_{1,j}^{\perp})$ that do not satisfy Definition 17.

The thresholds given by Theorem 9 are independent of the distribution of $\vec{s}$ as shown in Corollary 11. In contrast, $\vec{s}$ must be uniformly distributed over $\mathbb{F}^l$ to establish Theorem 19. This is because elements of $\vec{s}$ need to be treated as random numbers that are mutually independent and uniformly distributed over $\mathbb{F}$, as shown in the proof of Theorem 19.

It is proved in [8] that the secret sharing scheme with the same setting as Theorem 19 achieves the $(d(\mathscr{D}_1^{\perp}))-2)$-strong security. Unlike Theorem 19, this characterization by the minimum Hamming weight is not tight.

Proposition 20. Assume that $N-n < d(\mathscr{D}_1)$ and $l = N-n = \mathsf{dim}\ \mathscr{D}_1 - \mathsf{dim}\ \mathscr{D}_2$ in the secret sharing scheme defined by Definition 1. Let $\mathscr{X} = \{l+1,\ldots,l+n\}$, and let ψ be chosen such that $([\vec{s},\vec{0}]+\psi(\vec{s})+\vec{c}_2) \in \mathscr{D}_1$. Let $\mathscr{Y}_i = \{1,\ldots,N\}\backslash\{i\}$ be another index set for $1 \le i \le l$, and define a punctured code $\mathscr{G}_{1,i} = P_{\mathscr{Y}_i}(\mathscr{D}_1)$ and a shortened code $\mathscr{G}_{2,i} = (\mathscr{D}_1)_{\mathscr{Y}_i}$. Then, we have

$$\min\left\{M_1(\mathscr{G}_{2,i}^{\perp},\mathscr{G}_{1,i}^{\perp}) : 1 \le i \le l\right\} - 1 \ge d(\mathscr{D}_1^{\perp}) - 2.$$

This can be proved in a similar way to the proof of Proposition 15. Hence the proof is omitted. We note that Example 16 also gives a case of $\min\left\{M_1(\mathscr{G}_{2,i}^{\perp},\mathscr{G}_{1,i}^{\perp}) : 1 \le i \le l\right\} - 1 > d(\mathscr{D}_1^{\perp}) - 2$ for $l = 1$.

5. Conclusion

This paper has given a precise characterization of secret sharing schemes based on arbitrary linear codes. We have characterized thresholds t_1 and t_2 by the relative generalized Hamming weight (RGHW). One shows that any set of at most t_1 shares leaks no information about the secret, and the other shows that any set of at least t_2 shares uniquely determines the secret. Moreover, this paper has precisely characterized the strong security in secret sharing schemes by the RGHW, as a generalization of strongly-secure threshold ramp schemes. These characterizations enable to determine the property of secret sharing schemes from the parameters of linear codes, when we design systems using secret sharing schemes.

Acknowledgment

The authors would like to thank Dr. Tomohiro Ogawa, associate professor at University of Electro-Communications, for his fruitful comments on the relationship between distribution of the secret and thresholds in secret sharing schemes. The authors would also like to thank two anonymous reviewers for their helpful comments. This research was partially supported by the MEXT Grant-in-Aid for Scientific Research (A) No. 23246071, and the Villum Foundation through their VELUX Visiting Professor Programme 2011–2012. A part of this research was done during the third author's stay at Department of Mathematical Sciences, Aalborg University. He greatly appreciates the hospitality by Prof. O. Geil.

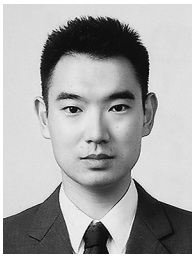
References

[1] G.R. Blakley and C. Meadows, "Security of ramp schemes," Proc. CRYPTO 1984, ser. Lect. Notes Comput. Sci., vol.196, pp.242–268, Springer-Verlag, 1984.
[2] G.R. Blakley, "Safeguarding cryptographic keys," Proc. AFIPS 1979 National Computer Conf., vol.48, pp.313–317, 1979.
[3] C. Blundo, A.D. Santis, and U. Vaccaro, "On secret sharing schemes," Inf. Process. Lett., vol.65, no.1, pp.25–32, 1998.
[4] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan, "Secure computation from random error correcting codes," Proc. EUROCRYPT 2007, ser. Lect. Notes Comput. Sci., no.4515, pp.291–310, Springer-Verlag, 2007.
[5] T.M. Cover and J.A. Thomas, Elements of Information Theory, 2nd ed., Wiley-Interscience, 2006.
[6] I.M. Duursma and S. Park, "Coset bounds for algebraic geometric codes," Finite Fields and Their Applications, vol.16, no.1, pp.36–55, 2010.
[7] G.D. Forney, Jr., "Dimension/length profiles and trellis complexity of linear block codes," IEEE Trans. Inf. Theory, vol.40, no.6, pp.1741–1752, 1994.
[8] J. Kurihara and T. Uyematsu, "Strongly-secure secret sharing based on linear codes can be characterized by generalized Hamming weight," Proc. 49th Annual Allerton Conference on Communication, Control, and Computing, pp.951–957, Sept. 2011.
[9] Y. Luo, C. Mitrpant, A.J. Han Vinck, and K. Chen, "Some new characters on the wire-tap channel of type II," IEEE Trans. Inf. Theory, vol.51, no.3, pp.1222–1229, 2005.
[10] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, student revised ed., North-Holland Mathematical Library, 1977.
[11] J.L. Massey, "Some applications of coding theory in cryptography," in Codes and Ciphers: Cryptography and Coding IV, pp.33–47, 1995.
[12] R.J. McEliece and D.V. Sarwate, "On sharing secrets and Reed-Solomon codes," Commun. ACM, vol.24, no.9, pp.583–584, 1981.
[13] M. Nishiara and K. Takizawa, "Strongly secure secret sharing

scheme with ramp threshold based on Shamir's polynomial interpolation scheme," IEICE Trans. Fundamentals (Japanese Edition), vol.J92-A, no.12, pp.1009–1013, Dec. 2009.
[14] J. Pieprzyk and X.-M. Zhang, "Ideal threshold schemes from MDS codes," Proc. 5th Int. Conf. Information Security and Cryptology (ICISC), ser. Lect. Notes Comput. Sci., vol.2587, pp.253–263, Springer-Verlag, 2002.
[15] A. Shamir, "How to share a secret," Commun. ACM, vol.22, no.11, pp.612–613, 1979.
[16] A. Subramanian and S.W. McLaughlin, "MDS codes on the erasure-erasure wiretap channel," arXiv:0902.3286v1, 2009, available at http://arxiv.org/abs/0902.3286
[17] V.K. Wei, "Generalized Hamming weights for linear codes," IEEE Trans. Inf. Theory, vol.37, no.5, pp.1412–1418, 1991.
[18] H. Yamamoto, "On secret sharing systems using (k,L,n) threshold scheme," IEICE Trans. Fundamentals (Japanese Edition), vol.J68-A, no.9, pp.945–952, Sept. 1985, [English translation: H. Yamamoto, "Secret sharing system using (k,L,n) threshold scheme," Electron. Commun. Jpn. Part I, vol.69, no.9, pp.46–54, (Scripta Technica, Inc.), Sept. 1986.].

Jun Kurihara received the B.E. degree in computer science and the M.E. degree in communication engineering from Tokyo Institute of Technology, Japan, in 2004 and 2006 respectively. He joined KDDI and has been engaged in the research on information theory, secret sharing and coding theory. He is currently a Ph.D. student in the Department of Communications and Integrated Systems at Tokyo Institute of Technology, and a researcher in KDDI R&D Laboratories, Inc.

Tomohiko Uyematsu received the B.E., M.E. and Dr.Eng. degrees from Tokyo Institute of Technology in 1982, 1984 and 1988, respectively. From 1984 to 1992, he was with the Department of Electrical and Electronic Engineering of Tokyo Institute of Technology, first as research associate, next as lecturer, and lastly as associate professor. From 1992 to 1997, he was with School of Information Science of Japan Advanced Institute of Science and Technology as associate professor. Since 1997, he returned to Tokyo Institute of Technology as associate professor, and currently he is with the Department of Communications and Integrated Systems as professor. In 1992 and 1996, he was a visiting researcher at the Centre National de la Recherche Scientifique, France and Delft University of Technology, Netherlands, respectively. He received the Achievement Award in 2008, and the Best Paper Award in 1993, 1996, 2002 and 2007 both from IEICE. His current research interests are in the areas of information theory, especially Shannon theory and multi-terminal information theory. Dr. Uyematsu is a senior member of IEEE.



Ryutaroh Matsumoto was born in Nagoya, Japan, on November 29, 1973. He received the B.E. degree in computer science, the M.E. degree in information processing, and the Ph.D. degree in electrical and electronic engineering, all from Tokyo Institute of Technology, Japan, in 1996, 1998, 2001, respectively. He was an Assistant Professor from 2001 to 2004, and has been an Associate Professor since 2004 in the Department of Communications and Integrated Systems of Tokyo Institute of Technology. His research interest includes error-correcting codes, quantum information theory, and communication theory. Dr. Matsumoto received the Young Engineer Award from IEICE and the Ericsson Young Scientist Award from Ericsson Japan in 2001. He received the Best Paper Awards from IEICE in 2001, 2008 and 2011.