IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 April 2024, accepted 10 May 2024, date of publication 15 May 2024, date of current version 22 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3401471

THEORY

A New Security Measure in Secret Sharing Schemes and Secure Network Coding

ITARU KURIHARA[1], JUN KURIHARA[1,2], (Member, IEEE), AND TOSHIAKI TANAKA[1], (Member, IEEE)

[1]Department of Data and Computational Science, Graduate School of Information Science, University of Hyogo, Kobe 650-0047, Japan
[2]Zettant Inc., Tokyo 103-0025, Japan

Corresponding author: Itaru Kurihara (skyjump517@gmail.com)

This work was supported in part by the National Institute of Information and Communications Technology, Japan, under Grant NICT22401; in part by Japan Society for the Promotion of Science, Japan, KAKENHI, under Grant JP22K11994 and Grant JP21H03442; and in part by the KDDI Foundation Research Grant.

ABSTRACT Linear secret sharing schemes protect secret information from leakage and destruction by encoding secret information into multiple shares, where the secret information can be reconstructed by collecting a certain subsets of shares. Perfect Security, α-strong Security, and Individual Security (IS) have been given as security measures of linear secret sharing schemes. Consider the threshold for each security measure, which is defined as the maximum allowable size of the set of leaked shares. Kurihara et al. have revealed that thresholds for Perfect Security and α-strong Security are characterized in terms of a relative code parameter *Relative Generalized Hamming Weight (RGHW)*. However, the threshold for IS is not yet characterized. In this paper, we focus on individual elements of secret information and give the threshold for IS (*Individual Security Threshold IST*) as a new security measure, where each element of secret information cannot be uniquely determined from subsets of shares with size less than or equal to the IST. We show that the IST can be characterized in terms of RGHW as well as Perfect Security and α-strong Security. We also give a precoding method for secret information that can guarantee IST above a certain value in any existing linear secret sharing schemes. Moreover, we extend the notion of the IST to universal secure network coding (USNC) and present the *Universal IST*. We also show that the Universal IST can be represented by the code parameter *Relative Generalized Rank Weight (RGRW)* similarly to the IST of the linear secret sharing schemes.

INDEX TERMS Individual security, individual security threshold, linear secret sharing schemes, nested coset coding, perfect security, relative generalized Hamming weight, relative generalized rank weight, universal secure network coding, α-strong security.

I. INTRODUCTION

The secret sharing scheme [1], [2] is a technique to protect information from leakage and destruction. This technique encodes secret information S into n (≥ 1) pieces of information called *shares* $X_1, \ldots, X_n$. Here, S can be reconstructed only from certain subsets of shares, called *qualified sets*. Otherwise, S cannot be uniquely determined. If the mapping from the secret information to the set of shares satisfies linearity, the secret sharing scheme is called the *linear secret sharing scheme* [3]. The (k, n)-*threshold scheme* introduced by Shamir [1] is a typical linear secret sharing scheme. This scheme guarantees that no information about S can be obtained from less than k ($\leq n$) shares. When $\mathbb{F}$ denotes a finite field, Shamir's (k, n)-threshold scheme uses a polynomial of order $k-1$ to encode the secret information $S \in \mathbb{F}$ into shares $X_1, \ldots, X_n \in \mathbb{F}$. By extending the notion of the (k, n)-threshold scheme, Yamamoto [4] and Blakley and Meadows [5] independently proposed the (k, l, n)-*threshold ramp scheme* as one of linear secret sharing schemes, which uses secret information $S \triangleq [S_1, \ldots, S_l] \in \mathbb{F}^l$ ($l \geq 1$) and encodes S into $X_1, \ldots, X_n$.

The associate editor coordinating the review of this manuscript and approving it for publication was Luca Barletta.

However, unlike the (k, n)-threshold scheme, this scheme partially leaks information about S from a subset of shares of size $k-l+r$ $(1 \leq r < l)$. Yamamoto also defined the *strong* (k, l, n)-threshold ramp scheme in which no information of any subsets $\mathcal{L} \subseteq \{S_i : i = 1, \ldots, l\}$, $|\mathcal{L}| = 1, \ldots, l-1$ cannot be obtained from any $k - |\mathcal{L}|$ shares [4].

The relationship between linear codes and the construction of linear secret sharing schemes has been investigated. McEliece and Sarwate [6] demonstrated that shares in Shamir's threshold scheme [1] can be viewed as symbols of a codeword in the Reed-Solomon code [7]. Piepryzk and Zhang [8] revealed that threshold schemes can be constructed from maximum distance separable (MDS) codes [7]. Massey [9] extended McEliece et al.'s construction to the one based on general linear code $\mathcal{C}$, and revealed that there exists a relationship between a qualified set and a codeword of its dual code $\mathcal{C}^{\perp}$. Duursma and Park [10] and Chen et al. [11] further generalized Massey's construction, and defines linear secret sharing schemes using a linear code $\mathcal{C}_1 \subseteq \mathbb{F}^n$ and its subcode $\mathcal{C}_2 \subsetneq \mathcal{C}_1$. Their construction can represent any existing construction of linear secret sharing in which every share is a single element in $\mathbb{F}$. Later, Subramanian and McLaughlin [12] pointed out the relationship between linear secret sharing schemes and *Nested Coset Coding* [13] with $\mathcal{C}_1$ and $\mathcal{C}_2$. In fact, the generalized scheme by Duursma and Chen et al. can be represented by the Nested Coset Coding [3]. From another perspective, there have been studied the design of secret sharing schemes constructed using linear codes for distributed storage systems (DSSs) [14], [15], [16]. Although these schemes require additional properties specific to DSSs, such as the repairing process of shares, the constructions themselves align with existing linear secret sharing schemes.[1]

On the other hand, in the general linear secret sharing scheme not limited to the threshold scheme and the threshold ramp scheme, security properties called *Perfect Security* and *α-strong Security* [3] have been considered. Let $\mathcal{J} \subseteq \{1, \ldots, n\}$ and let $X_{\mathcal{J}} \triangleq (X_t : t \in \mathcal{J})$ be a tuple of leaked shares. Then, Perfect Security is defined by the amount of information about the entire $S \in \mathbb{F}^l$ that can be obtained from $X_{\mathcal{J}}$. In other words, it is defined as the security property for a given set $\mathcal{J}$ that no information about the entire S can be obtained. Also, let $\mathcal{B} \subseteq \{1, \ldots, l\}$ and let $S_{\mathcal{B}} \triangleq (S_{t'} : t' \in \mathcal{B})$ be a tuple of elements of S. Then, α-strong Security is evaluated by the amount of information about any subsets $S_{\mathcal{B}}$ of S that can be obtained from the set $X_{\mathcal{J}}$ of leaked shares. That is, it is the security property for a given parameter α that no information about $S_{\mathcal{B}}$ can be obtained from $X_{\mathcal{J}}$ of size $|\mathcal{J}| \leq \alpha - |\mathcal{B}|$ for all non-empty $\mathcal{B} \subseteq \{1, \ldots, l\}$. The α-strong Security generalizes the strong security in the (k, l, n)-threshold ramp scheme.

[1]Existing schemes such as [16] in which a share is expressed as multiple, say t, symbols in $\mathbb{F}$ are still $\mathbb{F}$-linear secret sharing, and interpreted by Nested Coset Coding with $\mathcal{C}_1 \subseteq \mathbb{F}^{tn}$ and $\mathcal{C}_2 \subsetneq \mathcal{C}_1$.

Consider the threshold for each security: for Perfect Security, it is defined as the maximum allowable size of sets of leaked shares that the linear secret sharing scheme can satisfy Perfect Security, regardless of the combination of shares; for α-strong Security, it is defined as the maximum allowable α that the linear secret sharing scheme can satisfy α-strong Security. Namely, the maximum allowable $|\mathcal{J}|$ that no information about S obtained from $X_{\mathcal{J}}$ is the threshold for Perfect Security, and the maximum allowable α that no information about $S_{\mathcal{B}}$ obtained from $X_{\mathcal{J}}$ is the threshold for α-strong Security. Consider linear secret sharing schemes in which every share is an element of $\mathbb{F}$, and recall that such schemes can be represented by Nested Coset Coding with a linear code $\mathcal{C}_1 \subseteq \mathbb{F}^n$ and its subcode $\mathcal{C}_2 \subsetneq \mathcal{C}_1$. For such schemes, Kurihara et al. [3] showed that the threshold for Perfect Security and α-strong Security can be characterized by the code parameter *Relative Generalized Hamming Weight (RGHW)* [17] of $\mathcal{C}_1$ and $\mathcal{C}_2$. Kurihara et al. also extended this result to *Universal Secure Network Coding (USNC)* [18], [19], and proved that the security of USNC can be characterized in terms of the code parameter *Relative Generalized Rank Weight (RGRW)* [18], as well as linear secret sharing schemes.

Differently from Perfect Security and α-Strong Security, Cohen et al. [20] introduced *Individual Security (IS)*, which defines security focusing on individual element S_i of $S \in \mathbb{F}^l$. In linear secret sharing schemes, when each S_i cannot be uniquely determined from $X_{\mathcal{J}}$, this linear secret sharing scheme is called the one satisfying IS for $X_{\mathcal{J}}$. Thus, the IS is security given based on the concept that it is sufficient if every single element S_i of S can be kept secret. Furthermore, Cohen et al. presented a specific encoding method to satisfy the IS for any $\mathcal{J}$ of size $l-1$ [21]. We see that the IS is less secure than Perfect Security and α-strong Security since the target of security is only individual elements of secret information. However, when the linear secret sharing scheme satisfies IS, it is guaranteed that any part of S cannot be uniquely determined. Currently, in the linear secret sharing scheme, the threshold for IS has not yet been considered and is not thus characterized in terms of a code parameter, unlike thresholds for α-strong Security and Perfect Security.

The contributions of this paper are summarized as follows.

1) We focus on individual elements of secret information as a target of security and present the *Individual Security Threshold (IST)* as a new security measure for linear secret sharing schemes. This is defined as the maximum allowable size of the set of shares for which an individual element of secret information can not be uniquely determined. In other words, IST provides a sufficient condition for satisfying IS. Moreover, we prove the relationship between IST and thresholds for other security properties.
2) We clarify that IST can be characterized in terms of the code parameter RGHW, similar to thresholds for Perfect Security and α-strong Security.

3) We also propose a precoding method for secret information that can guarantee IST above a certain value for all linear secret sharing schemes.
4) Additionally, we extend the notion of IST to the security of USNC. This security measure is called Universal IST and is given as the maximum allowable number of eavesdropped links on a network that can not leak individual elements of secret information, regardless of the network structure. We reveal that this security can be expressed in terms of RGRW.

The structure of this paper is as follows. In Section II, we introduce several notations and definitions, and explain the Nested Coset Coding. In Section III, we present the definition of the IST as a new security measure for linear secret sharing schemes. Furthermore, we show that the IST can be represented in terms of the code parameter RGHW. In Section IV, we propose a precoding method for secret information that can always guarantee an IST above a certain value for all linear secret sharing schemes. In Section V, we extend the notion of IST to USNC and present the Universal IST. We then reveal that it can be represented in terms of the code parameter RGRW. Finally, Section VI concludes this paper.

II. PRELIMINARY

A. NOTATIONS

Let $H(X)$ be the Shannon entropy of the random variable X, $H(Y|X)$ be the conditional entropy of Y given X, and $I(X;Y)$ be the mutual information between X and Y [22].

Let $\mathbb{F}$ be a finite field. Let $\mathbb{F}^n$ be an n-dimensional vector space over $\mathbb{F}$. Let a linear code $\mathcal{C} \subseteq \mathbb{F}^n$ consisting of vectors of length n over $\mathbb{F}$ be a linear subspace of $\mathbb{F}^n$. Let $\mathcal{N} \triangleq \{1,\ldots,n\}$. For a vector $X = [X_1,\ldots,X_n] \in \mathbb{F}^n$ and a subset $\mathcal{J} \subseteq \mathcal{N}$, let $X_{\mathcal{J}} \triangleq (X_t : t \in \mathcal{J})$ be a tuple of elements of X. Then, the subspace of a linear code $\mathcal{C}$ is called a subcode of $\mathcal{C}$ [7]. The dual code $\mathcal{C}^{\perp}$ of $\mathcal{C}$ is defined as follows.

$$\mathcal{C}^{\perp} \triangleq \{x \in \mathbb{F}^n : x \cdot v = 0, \quad \forall v \in \mathcal{C}\},$$

where $x \cdot v$ is the standard inner product of the vectors x and v.

B. NESTED COSET CODING AND LINEAR SECRET SHARING SCHEMES

Throughout this paper, we focus on linear secret sharing schemes in which every share is expressed as an element of $\mathbb{F}$. Any of such schemes can be represented by an encoding method called *Nested Coset Coding* [13] with a linear code $\mathcal{C}_1 \subseteq \mathbb{F}^n$ and its subcode $\mathcal{C}_2 \subsetneq \mathcal{C}_1$ [3].

Definition 1 (Nested Coset Coding [13]): Let $\mathcal{C}_1 \subseteq \mathbb{F}^n$ be a linear code and let $\mathcal{C}_2 \subsetneq \mathcal{C}_1$ be its subcode. Let $l \triangleq dim(\mathcal{C}_1/\mathcal{C}_2)$ denote the dimension of the quotient space $\mathcal{C}_1/\mathcal{C}_2$. Let $\psi : \mathbb{F}^l \to \mathcal{C}_1/\mathcal{C}_2$ be an arbitrary linear bijection. This linear bijection ψ takes $S \in \mathbb{F}^l$ as input and randomly selects an n-dimensional vector $X \in \mathcal{C}_1$ from the coset $\psi(S) \in \mathcal{C}_1/\mathcal{C}_2$ for output. In this paper, for Nested Coset Coding, the distributions of S and X are assumed to be uniform over $\mathbb{F}^l$ and $\psi(S)$, respectively.

By Nested Coset Coding, the secret sharing scheme is represented as follows. In linear secret sharing schemes, S in Definition 1 is regarded as a secret information, and is mapped to an element of the quotient space $\mathcal{C}_1/\mathcal{C}_2$, i.e., the coset $\psi(S)$ by the isomorphism ψ. Note that the number of elements of $\mathcal{C}_1/\mathcal{C}_2$ is $|\mathbb{F}|^{dim\mathcal{C}_1 - dim\mathcal{C}_2} = |\mathbb{F}|^l$. For a given S, a vector $X = [X_1,\ldots,X_n]$ is randomly selected from $\psi(S)$, and then each element $X_j, j \in \mathcal{N}$ is regarded as a share of a linear secret sharing schemes using $\mathcal{C}_1$, $\mathcal{C}_2$, and ψ.

Remark 1: Definition 1 includes the Ozarow-Wyner coset coding scheme for Wire-tap channel II [23] as a special case with $\mathcal{C}_1 = \mathbb{F}^n$. We thus see that linear secret sharing schemes can be viewed as a generalization of the coset coding scheme for Wire-tap channel II in terms of $\mathcal{C}_1$.

C. SECURITY IN SECRET SHARING SCHEMES

In linear secret sharing schemes, security properties called Perfect Security, α-strong Security [3], and Individual Security(IS) [20] have been considered. In the following, we shall explain their definitions.

Firstly, Perfect Security focuses on the security of the entire secret information for a subset of leaked shares evaluated by the mutual information.

Definition 2 (Perfect Security [3]): Let $S \in \mathbb{F}^l$ be a secret information. Let $X \in \mathbb{F}^n$ be a vector consisting of n shares. For $\mathcal{J} \subseteq \mathcal{N}$, $|\mathcal{J}| = \mu$, let $X_{\mathcal{J}}$ be a tuple of leaked shares. The secret sharing scheme satisfies the Perfect Security for μ if the following condition is satisfied.

$$I(S; X_{\mathcal{J}}) = 0, \ \forall \mathcal{J} \subseteq \mathcal{N}, \ |\mathcal{J}| = \mu.$$

When Perfect Security is satisfied with $\mu = k - l$, the scheme coincides with the (k,l,n)-*threshold ramp scheme* [4].

The maximum possible μ for Perfect Security is called the *Perfect Security Threshold* Θ, as defined as follows.

Definition 3 (Perfect Security Threshold):

$$\Theta \triangleq \max\{\mu : I(S; X_{\mathcal{J}}) = 0, \ \forall \mathcal{J} \subseteq \mathcal{N}, \ |\mathcal{J}| = \mu\}.$$

On the other hand, α-*strong Security* is the security that for $1 \le i \le l$, no information on i elements of the secret information can be obtained from any $\alpha - i + 1$ or less shares. In other words, α-strong Security focuses on the security of subsets of the secret information.

Definition 4 (α-strong Security [3, Definitions 17 and 18]): For a secret information $S \triangleq [S_1,\ldots,S_l] \in \mathbb{F}^l$, the linear secret sharing scheme satisfying the following equation is said to satisfy α-strong Security.

$$I(S_{\mathcal{B}}; X_{\mathcal{J}}) = 0,$$
$$\forall \mathcal{J} \subseteq \mathcal{N} \text{ and } \forall \mathcal{B} \subseteq \{1,\ldots,l\} \text{ with} |\mathcal{J}| + |\mathcal{B}| = \alpha + 1.$$

When a (k,l,n)-threshold ramp scheme satisfies α-strong Security for $\alpha = k - 1$, then it is called the *strong* (k,l,n)-*threshold ramp scheme* [4].

The maximum possible α for α-strong Security is called the α-*strong Security Threshold*.

Definition 5 (α-strong Security Threshold):

$$\Omega \triangleq \max\{\alpha : I(S_{\mathcal{B}}; X_{\mathcal{J}})=0, \forall \mathcal{J} \subseteq \mathcal{N} \text{ and } \forall \mathcal{B} \subseteq \{1,\ldots,l\} \text{ with } |\mathcal{J}|+|\mathcal{B}| = \alpha+1\}.$$

Unlike Definitions 2 and 4, *Individual Security* is defined as the security of each element consisting of S, for a subset of shares.

Definition 6 (Individual Security (IS) [20, Definition 1]): Let $S \triangleq [S_1,\ldots,S_l] \in \mathbb{F}^l$ be a secret information. For $\mathcal{J} \subseteq \mathcal{N}$, $|\mathcal{J}| = \mu$, let $X_{\mathcal{J}}$ be a tuple of elements of shares. We say that the scheme satisfies Individual Security for μ if it satisfies the following condition.

$$I(S_i; X_{\mathcal{J}}) = 0, \ \forall i \in \{1,\ldots,l\}, \forall \mathcal{J} \subseteq \mathcal{N}, |\mathcal{J}| = \mu.$$

Remark 2: When α-strong security is achieved, for $\mu = \alpha$, IS is also attained. Nevertheless, it should be noted that even when IS is satisfied for μ, this does not invariably imply that α-strong security is attained for $\alpha = \mu$.

From Definition 6, the IS defines security for individual components of secret information S. Furthermore, Cohen gave a coding method that satisfies the property of IS in the field of network coding. The property of the coding method satisfying IS in a special case will be introduced in Section IV.

Remark 3: The coding method satisfying IS given by Cohen [21] encodes S by Neted Coset Coding with $\mathcal{C}_2 = \{0\}$ and a specific isomorphic map ψ.

It has been shown by Kurihara et al. [3] that Perfect Security Threshold and α-strong Security Threshold can be represented by the code parameter Relative Generalized Hamming Weight (RGHW) [17]. However, the threshold to satisfy the IS is not clear.

Remark 4: Wei [24] characterized the Perfect Security in Wire-tap channel II in terms of another code parameter called *Generalized Hamming Weight* (GHW). Note that RGHW [17] can be seen as a generalization of GHW (See also Remark 6). Also, recall that linear secret sharing schemes are a generalization of Ozarow-Wyner coset coding for Wire-tap channel II, as mentioned in Remark 1. From this context, Kurihara et al.'s work [3] can be seen as a generalization of Wei's result to general secret sharing schemes using RGHW.

III. INDIVIDUAL SECURITY THRESHOLD AND ITS REPRESENTATION BY THE CODE PARAMETER

In this section, we present the *Individual Security Threshold (IST)* as a new measure of security in linear secret sharing schemes. Also, we shall explain how the IST differs from other security thresholds. Furthermore, we shall show that IST can be represented by RGHW similarly to the Perfect Security Threshold and α-strong Security Threshold as [3].

A. INDIVIDUAL SECURITY THRESHOLD

We start by introducing the Individual Security Threshold, which is defined as the maximum possible μ for Individual Security in Definition 6, as shown in the following definition.

Definition 7 (Individual Security Threshold (IST)): Let $S \triangleq [S_1,\ldots,S_l] \in \mathbb{F}^l$ be a secret informaiton. Let μ be a number of shares. Then, the IST Υ is defined as follows.

$$\Upsilon \triangleq \max\{\mu : I(S_i; X_{\mathcal{J}}) = 0, \ \forall i \in \{1,\ldots,l\}, \forall \mathcal{J} \subseteq \mathcal{N}, |\mathcal{J}| = \mu\}.$$

The IST Υ focuses on the security of individual elements rather than subsets of a secret information, and provides a maximum number of leaked shares in which no element of the secret information can be uniquely determined. Thus, IST provides a sufficient condition for satisfying the IS in linear secret sharing schemes.

Next, we explicitly show the relationship between the Perfect Security Threshold, α-strong Security Threshold, and Individual Security Threshold. The α-strong Security Threshold Ω given in Definition 5 can be rewritten as follows.

$$\Omega = \min_{p\in\{1,\ldots,l\}} \Omega^p,$$

where,

$$\Omega^p \triangleq \max\{\alpha : I(S_{\mathcal{B}}; X_{\mathcal{J}}) = 0, \ \forall \mathcal{J} \subseteq \mathcal{N}, \ |\mathcal{B}| = p, \ |\mathcal{J}| = \alpha - p + 1\}.$$

Consider the number of leaked shares, $\alpha - p + 1$. For Ω^p, no information on $S_{\mathcal{B}}$ for any $\mathcal{B}$ ($|\mathcal{B}| = p$) leaks from at most $\Omega^p - p + 1$ shares. This means that when $p = 1$, Ω^1 matches the IST Υ. On the other hand, when $p = l$, $\Omega^l - l + 1$ matches the Perfect Security Threshold Θ. Therefore, the relationship among the Perfect Security Threshold Θ, α-strong Security Threshold Ω, and IST Υ is

$$\Omega \le \Omega^l = \Theta + l - 1, \text{ and } \Omega \le \Omega^1 = \Upsilon.$$

Table 1 shows the characteristics of Perfect Security Threshold, α-strong Security Threshold, and IST. Unlike other security thresholds, IST limits the target of security to each element that consists of secret information. Therefore, IST provides a threshold that satisfies weaker security than other security thresholds. However, IST more clearly gives the maximum number of shares that can at least conceal every individual element S_i.

Remark 5: Here, it is worth noting that the IST in Definition 7 introduces a definition similar to the *access complexity* [14, Section II-B, Definition 4] that has been introduced in the context of linear secret sharing for distributed storage systems (DSSs). The access complexity r is defined as

$$r \triangleq \min\{\mu : I(S_i; X_{\mathcal{J}}) = H(S_i), \ \forall i \in \{1,\ldots,l\}, \exists \mathcal{J} \subseteq \mathcal{N}, |\mathcal{J}| = \mu\}.$$

Namely, r is the minimum possible number of shares that can uniquely determine any single (or more) element of S. On the other hand, the IST Υ is the maximum possible number of shares that can uniquely determine no individual element of S. We thus see that although the access complexity represents the cost measure of repairing the secret information in DSSs, the IST expresses the security measure.

TABLE 1. The comparison of characteristics of each security measure, where the symbols +, ++, and +++ mean their strength, and $S \triangleq [S_1, \ldots, S_l]$.

Security measure	Perfect Security Threshold Θ	α-strong Security Threshold Ω	IST Υ
The target of security	Entirety of S	Any subsets of S	Individual elements S_i, $\forall i \in \{1, \ldots, l\}$
Strength	++	+++	+
Relationship of thresholds	$\Omega \leq \Omega^l = \Theta + l - 1$, and $\Omega \leq \Omega^1 = \Upsilon$		

B. IST IN LINEAR SECRET SHARING SCHEMES

It is evidently challenging to calculate the IST as defined in Definition 7 due to the necessity of exhaustively examining all combinations of shares. Representing IST through a preexisting code parameter allows a clearer deduction of IST from a coding-theoretic perspective. Hence, in this subsection, we show that IST can be represented by the code parameter *Relative Generalized Hamming Weight (RGHW)* [17], in linear secret sharing schemes.

First, for a linear code $\mathcal{C} \subseteq \mathbb{F}^n$, we define its *shortened code* [7] $\mathcal{C}_\mathcal{J}$ as below.

$$\mathcal{C}_\mathcal{J} \triangleq \{[c_1, \ldots, c_n] \in \mathcal{C} : c_t = 0 \text{ for } t \notin \mathcal{J}\}.$$

Next, we introduce the code parameter RGHW in linear codes. We also introduce a theorem showing that RGHW characterizes the Perfect Security Threshold in the linear secret sharing scheme [3].

Definition 8 (RGHW [17]): Let $\mathcal{C}_1 \subseteq \mathbb{F}^n$ be a linear code and $\mathcal{C}_2 \subsetneq \mathcal{C}_1$ be its subcode. Then, the i-th Relative Generalized Hamming Weight (i-th RGHW) of $\mathcal{C}_1$ and $\mathcal{C}_2$ is defined by

$$\begin{aligned} M_i(\mathcal{C}_1, \mathcal{C}_2) &\triangleq \min\{|\mathcal{J}| : dim(\mathcal{C}_1)_\mathcal{J} - dim(\mathcal{C}_2)_\mathcal{J} \geq i\} \\ &= \min\{|\mathcal{J}| : dim(\mathcal{C}_1)_\mathcal{J} - dim(\mathcal{C}_2)_\mathcal{J} = i\}, \end{aligned}$$

for $0 \leq i \leq dim(\mathcal{C}_1/\mathcal{C}_2)$.

Remark 6: When $\mathcal{C}_2 = \{0\}$, the i-th RGHW $M_i(\mathcal{C}_1, \mathcal{C}_2) = M_i(\mathcal{C}_1, \{0\})$ coincides with the i-th GHW [24] of $\mathcal{C}_1$. Also note that the first GHW of $\mathcal{C}_1$, i.e., $M_1(\mathcal{C}_1, \{0\})$, is exactly the minimum Hamming weight [7] of $\mathcal{C}_1$.

Proposition 1: [3, Theorem 9] Consider a linear secret sharing scheme represented by Nested Coset Coding with a linear code $\mathcal{C}_1 \subseteq \mathbb{F}^n$ and its subcode $\mathcal{C}_2 \subsetneq \mathcal{C}_1$. Then, for $\mathcal{J} \subseteq \mathcal{N}$, the relationship between the Perfect Security Threshold Θ and the first RGHW is given as follows.

$$\Theta = M_1(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp) - 1.$$

From Definition 3, the following corollary of Proposition 1 is immediate.

Corollary 1: There exists a subset $\mathcal{J} \subseteq \mathcal{N}$ satisfying $I(S; X_\mathcal{J}) > 0$ when $|\mathcal{J}| = \Theta + 1$.

Here, from a code-theoretic perspective, we express the IST in Definition 7 by code parameter RGHW. The following theorem is given for the IST of the linear secret sharing scheme represented by Nested Coset Coding.

Theorem 1: Let $\mathcal{C}_1 \subseteq \mathbb{F}^n$ be a linear code and $\mathcal{C}_2 \subsetneq \mathcal{C}_1$ be its subcode. Consider Nested Coset Coding by $\mathcal{C}_1$, $\mathcal{C}_2$, and ψ shown in Definition 1. Then, for $i \in \{1, \ldots, l\}$, we define the subcode $\mathcal{D}_i$ of $\mathcal{C}_1$ as follows.

$$\mathcal{D}_i \triangleq \bigcup_{\substack{S_i = 0 \\ S_j \in \mathbb{F}: j \neq i}} \psi([S_1, \ldots, S_l]).$$

Then, the IST Υ of the secret sharing scheme by Nested Coset Coding with $\mathcal{C}_1$, $\mathcal{C}_2$, and ψ is given by

$$\Upsilon = \min\{M_1(\mathcal{D}_i^\perp, \mathcal{C}_1^\perp) : 1 \leq i \leq l\} - 1.$$

Proof: For $i \in \{1, \ldots, l\}$, $\mathcal{D}_i$ is the subcode of $\mathcal{C}_1$, and $dim\mathcal{D}_i = dim\mathcal{C}_1 - 1$ holds. Next, we define the following coset.

$$\sigma(S_i = s_i) \triangleq \bigcup_{\substack{S_i = s_i \\ S_j \in \mathbb{F}: j \neq i}} \psi([S_1, \ldots, S_l]) \in \mathcal{C}_1/\mathcal{D}_i. \tag{1}$$

From (1), when we fix only $S_i = s_i$, X is a vector uniformly distributed over $\sigma(s_i)$. Thus, X can be regarded as a vector generated by the Nested Coset Coding with $\mathcal{C}_1$, $\mathcal{D}_i$, and σ. Hence, from Proposition 1, for any tuple $X_\mathcal{J}$ of shares satisfying $|\mathcal{J}| \leq M_1(\mathcal{D}_i^\perp, \mathcal{C}_1^\perp) - 1, I(S_i; X_\mathcal{J}) = 0$ holds. Also, from Corollary 1, a subset $\mathcal{J} \subseteq \mathcal{N}$ satisfying $I(S_i; X_\mathcal{J}) > 0$ exists when $|\mathcal{J}| = M_1(\mathcal{D}_i^\perp, \mathcal{C}_1^\perp)$. Therefore, we have the theorem. □

IV. LINEAR SECRET SHARING SCHEMES WITH THE COHEN'S SCHEME

In the previous section, IST was characterized by RGHW. Since a linear secret sharing scheme guarantees stronger security the larger the IST, it is desirable to be able to make the IST increased with no change of existing linear secret sharing schemes. To this end, this section presents a precoding method for secret information in all linear secret sharing schemes, ensuring a certain value of IST.

From now on, we redenote by $\mathbb{F}_q$ a finite field containing q elements, over which a secret sharing scheme works, instead of $\mathbb{F}$. Also, let $\mathbb{F}_{q^m}$ be an m-degree extension field of $\mathbb{F}_q$ ($m \geq 1$), and we redefine a secret information $S \triangleq [S_1, \ldots, S_l] \in \mathbb{F}_{q^m}^l$ as a vector over $\mathbb{F}_{q^m}$.

Here, we introduce a special linear bijection given by Cohen et al. [21, Section VI] and explain its properties. Let $\phi : \mathbb{F}_{q^m}^l \to \mathbb{F}_{q^m}^l$ be the linear bijection. Then, their scheme

encodes S to $\phi(S)$ to guarantee the IS in a specific setting. Particulary, the following is satisfied, when $\mu = l - 1$, and $m \geq l$.

$$I(S_i; \phi(S)D) = 0, \qquad \forall D \in \mathbb{F}_q^{l\times(l-1)}. \tag{2}$$

The proposed method uses the bijection ϕ for the precoding of secret information in any linear secret sharing schemes over $\mathbb{F}_q$. Recall that because of the isomorphism of $\mathbb{F}_{q^m} \simeq \mathbb{F}_q^{m\times 1}$, each element $S_i \in \mathbb{F}_{q^m}$ of the secret information S can be regarded as an element of $\mathbb{F}_q^{m\times 1}$. The proposed method first encodes S into $\phi(S) = S' \in \mathbb{F}_{q^m}^l$ by ϕ. This precoded secret information $S' \triangleq [S'_1, \ldots, S'_l] \in \mathbb{F}_{q^m}^l$ can be represented by a matrix over $\mathbb{F}_q$ as shown below.

$$S' = \begin{bmatrix} S'^1 \\ \vdots \\ S'^e \\ \vdots \\ S'^m \end{bmatrix} \in \mathbb{F}_q^{m\times l}, 1 \leq e \leq m. \tag{3}$$

Secondly, each row $S'^e \triangleq [S'^e_1, \ldots, S'^e_l] \in \mathbb{F}_q^l$ of S', regarded as an l-dimensional vector over $\mathbb{F}_q$, is encoded into an n-dimensional vector $X^e \in \psi(S'^e)$ by the given $\mathbb{F}_q$-linear secret sharing schemes, i.e. Nested Coset Coding with a linear code $\mathcal{C}_1$, its subcode $\mathcal{C}_2$, and ψ. Finally, a matrix

$$X = \begin{bmatrix} X^1 \\ \vdots \\ X^e \\ \vdots \\ X^m \end{bmatrix} \in \mathbb{F}_q^{m\times n}$$

of shares is obtained. This means that the $\mathbb{F}_q$-linear secret sharing scheme is executed in parallel for each of m secret information. Then, we finally obtain the matrix $X \in \mathbb{F}_q^{m\times n}$, and its each column is regarded as share.

The following theorem is given for this proposed method.

Theorem 2: Let Υ be the IST of an $\mathbb{F}_q$-linear secret sharing scheme. The IST of the proposed method based on the linear secret sharing schemes is then given by

$$\Upsilon' = \max\{\Upsilon, l - 1\}.$$

Proof: Let R be a uniform random variable over $\mathbb{F}_q^{m\times(k-l)}$. Let S' be the precoded secret information given by (3). We define a matrix $T \in \mathbb{F}_q^{m\times k}$ as follows.

$$T \triangleq [S', R] \in \mathbb{F}_q^{m\times k}, \ R \in \mathbb{F}_q^{m\times(k-l)}.$$

Let us assume that the linear secret sharing scheme is represented by Nested Coset Coding of Definition 1, with the linear code $\mathcal{C}_1$ ($\subseteq \mathbb{F}_q^n$), its subcode $\mathcal{C}_2$, and ψ. $\mathcal{C}_1$ can be defined as $\mathcal{C}_1 \triangleq \{uG : u \in \mathbb{F}_q^k\}$, where $G \in \mathbb{F}_q^{k\times n}$ is a generator matrix of $\mathcal{C}_1$. The matrix of shares generated by G for each row of S' can be represented as follows.

$$X = TG \in \mathbb{F}_q^{m\times n}.$$

Let G' be a matrix obtained by arbitrarily selecting $l - 1$ columns from G, which is defined as follows.

$$G' \triangleq \begin{bmatrix} D \\ C \end{bmatrix} \in \mathbb{F}_q^{k\times(l-1)}, \qquad D \in \mathbb{F}_q^{l\times(l-1)}, \ C \in \mathbb{F}_q^{(k-l)\times(l-1)}.$$

Then, $TG' = S'D + RC$, which represents the matrix consisting of collected $l - 1$ shares. Here, by (2), it holds that $I(S_i; S'D) = 0$. Considering the non-negativity of the mutual information, Theorem 2 holds if the following condition is satisfied.

$$I(S_i; S'D + RC) \leq I(S_i; S'D), \ \forall i \in \{1, \ldots, l\}. \tag{4}$$

Hence, we shall verify (4). Here, we assume that the random variables O, P, and Q form a Markov chain in the sequence $O \to P \to Q$. In this case, the following holds [22].

$$I(O; P) \geq I(O; Q).$$

In our method, note that a Markov chain is established in the sequence $S_i \to S'D \to S'D + RC$ for random variables S_i, $S'D$, and $S'D + RC$. Thus, in accordance with the aforementioned property of the Markov chain, (4) holds. Therefore, no element of the secret information S can be uniquely determined from at least $l - 1$ shares. Consequently, Theorem 2 holds. □

Introducing Cohen et al.'s coding scheme as a preprocessing step in the linear secret sharing scheme will ensure a certain value of IST without compromising the formal structure of the linear secret sharing scheme.

V. IST IN NETWORK CODING

In Section III, the IST was given as a measure of security of linear secret sharing schemes, and we revealed that IST can be represented by RGHW. In this section, we extend the notion of IST to *Universal Secure Network Coding (USNC)* [18], [19], and present *Universal IST* as a new measure of security in USNC. We also show that Universal IST can be represented by a coding parameter *Relative Generalized Rank Weight (RGRW)* [18] as Section III.

A. UNIVERSAL SECURE NETWORK CODING (USNC)

First, we give assumptions on network coding. Let $\mathbb{F} = \mathbb{F}_{q^m}$, where $\mathbb{F}_q$ is a finite field containing q elements and $\mathbb{F}_{q^m}$ ($m \geq 1$) be an m-degree extension of $\mathbb{F}_q$. We consider a multicast communication network represented by a directed multigraph with unit capacity links, a single source node, and multiple sink nodes. We assume that $\mathbb{F}_q$-linear network coding [25] is employed over the network.

Suppose that the source node encodes a secret information $S \in \mathbb{F}_{q^m}^l$ to $X \in \mathbb{F}_{q^m}^n$ by Nested Coset Coding in Definition 1 over $\mathbb{F}_{q^m}$. $X \in \mathbb{F}_{q^m}^n$ can be considered as an $m \times n$ matrix $X = [X_1, \ldots, X_g, \ldots, X_n] \in \mathbb{F}_q^{m\times n}$ consisting of elements in $\mathbb{F}_q$, where each column $X_g \in \mathbb{F}_q^{m\times 1}$ ($g \in \{1, \ldots, n\}$) is a single packet and the source node transmits packets $X_1, \ldots, X_n$ on n outgoing links. The information transmitted over each link can be represented as an $\mathbb{F}_q$-linear combination

of packets $X_1, \ldots, X_n \in \mathbb{F}_q^{m\times 1}$. Namely, the information transmitted on link e is $Xb_e \in \mathbb{F}_q^{m\times 1}$, where $b_e \in \mathbb{F}_q^{n\times 1}$ is the coding vector [25] for link e. Each sink node has N ($\geq n$) incoming links and receives information transmitted over each link from the source node [18], [26], [27], [28], [29], [30].

In this model, suppose that μ out of n links on the network are eavesdropped. Then, the information leaked from μ links is $XB \in \mathbb{F}_q^{m\times\mu}$, where $B \in \mathbb{F}_q^{n\times\mu}$ denotes the matrix consisting of coding vectors for eavesdropped links. In the realm of secure network coding, the source node encodes the secret information $S \in \mathbb{F}_{q^m}^{l}$ into X and sends it so that information about S cannot be obtained from XB [18], [26], [27], [28], [29], [30]. In particular, the scheme that leaks no information about S for any $B \in \mathbb{F}_q^{n\times\mu}$ is called *Universal Secure Network Coding (USNC)* [18], [19].

In the USNC, a sufficient condition that no information about S can be obtained has been given as a measure of security [18]. In this paper, we refer to this sufficient condition as the *Universal Perfect Security Threshold*, which gives the maximum number of eavesdropped links that leaks no information on the entire part of S. This security measure is defined as follows.

Definition 9 (Universal Perfect Security Threshold [18]): The USNC satisfies the *Universal Perfect Security* if the following condition is satisfied.

$$I(S; XB) = 0, \ \forall B \in \mathbb{F}_q^{n\times\mu}.$$

The maximum possible μ for Universal Perfect Security is called the *Universal Perfect Security Threshold* Θ_{USNC}, defined as follows.

$$\Theta_{USNC} \triangleq \max\{\mu : I(S; XB) = 0, \ \forall B \in \mathbb{F}_q^{n\times\mu}\}.$$

Kurihara et al. [18] extended the α-strong Security [Definition 4] of the linear secret sharing scheme to the USNC, and gave Universal ω-strong Security. This security focused on any subset of secret information S in the USNC. They also gave Universal Maximum Strength [18] as a measure of security for any subset of secret information S in USNC. Universal ω-strong Security and Universal Maximum Strength are defined as follows.

Definition 10 (Universal ω-strong Security and Universal Maximum Strength [18, Definition 6]): Let $\mathcal{B} \subseteq \{1, \ldots, l\}$ and $S_{\mathcal{B}} \triangleq (S_i : i \in \mathcal{B})$. Then, the USNC satisfies the Universal ω-strong Security if the following condition is satisfied.

$$I(S_{\mathcal{B}}; XB) = 0, \qquad \forall \mathcal{B}, \ \forall B \in \mathbb{F}_q^{n\times(\omega-|\mathcal{B}|+1)}.$$

The maximum possible ω for Universal ω-strong Security is called the Universal Maximum Strength Ω_{USNC}.

$$\Omega_{USNC} \triangleq \max\{\omega : I(S_{\mathcal{B}}; XB)=0, \ \forall \mathcal{B}, \ \forall B \in \mathbb{F}_q^{n\times(\omega-|\mathcal{B}|+1)}\}.$$

In this paper, we introduce a new security measure called *Universal IST* in USNC, which measure will be defined in the following subsection.

B. THE UNIVERSAL INDIVIDUAL SECURITY THRESHOLD

In this subsection, we define the new security measure called *Universal Individual Security Threshold (Universal IST)* in USNC. We also explain the relationship among Universal Perfect Security Threshold, Universal Maximum Strength, and Universal IST.

The Universal IST gives a maximum number of eavesdropped links satisfying that each element S_i ($1 \leq i \leq l$) of secret information S can not be uniquely determined, regardless of the wiretap matrix B, and is defined as follows.

Definition 11 (Universal Individual Security Threshold (Universal IST)): Suppose that μ links are observed in the model of Section V-A. Then, the Universal IST is defined as the maximum number of wiretapped links from which each element S_i of S cannot be uniquely determined as follows.

$$\Upsilon_{USNC} \triangleq \max\{\mu : I(S_i; XB) = 0, \\ \forall i \in \{1, \ldots, l\}, \forall B \in \mathbb{F}_q^{n\times\mu}\}.$$

The Universal IST focuses on individual elements S_i of secret information S as the target of security, and the scope of the security target to be protected is smaller than that of Universal Perfect Security Threshold and Universal Maximum Strength. Therefore, the Universal IST provides a sufficient condition providing weaker security than these security measures. Next, we explicitly show the relationship among these security measures. First, the Universal Maximum Strength Ω_{USNC} can be rewritten as follows.

$$\Omega_{USNC} = \min_{p\in\{1,\ldots,l\}} \Omega^p_{USNC},$$

where,

$$\Omega^p_{USNC} \triangleq \max\{\omega : I(S_{\mathcal{B}}; XB) = 0, \\ |\mathcal{B}| = p, \ \forall B \in \mathbb{F}_q^{n\times(\omega-p+1)}\}.$$

Consider the number of eavesdropped links, $\omega - p + 1$. For Ω^p_{USNC}, no information on $S_{\mathcal{B}}$ for any $\mathcal{B}$ ($|\mathcal{B}| = p$) leaks from at most $\Omega^p_{USNC} - p + 1$ eavesdropped links. This means that when $p = 1$, Ω^1_{USNC} matches the Universal IST Υ_{USNC}. On the other hand, when $p = l$, $\Omega^l_{USNC} - l + 1$ matches the Universal Perfect Security Threshold Θ_{USNC}. Therefore, the relationship among the Universal Perfect Security Threshold Θ_{USNC}, Universal Maximum Strength Ω_{USNC}, and Universal IST Υ_{USNC} is

$$\Omega_{USNC} \leq \Omega^l_{USNC} = \Theta_{USNC} + l - 1, \text{ and}$$
$$\Omega_{USNC} \leq \Omega^1_{USNC} = \Upsilon_{USNC}.$$

On the other hand, it was clarified that the Universal Perfect Security Threshold and Universal Maximum Strength can be characterized from a code-theoretic perspective by the code parameter RGRW [18]. In the following subsection, we clarify that Universal IST can be characterized by RGRW as well as these measures.

C. REPRESENTATION OF THE UNIVERSAL IST BY RELATIVE GENERALIZED RANK WEIGHT

In this subsection, we show that the Universal IST of Definition 11 can be characterized by the code parameter *Relative Generalized Rank Weight (RGRW)*.

Firstly, we define RGRW and denote how it characterizes the existing security of USNC. From now on, for a subspace $V \subseteq \mathbb{F}_{q^m}^n$, let $dim V$ denote the dimension over $\mathbb{F}_{q^m}$ of V. We also define the following set $\mathcal{G}$.

$$\mathcal{G} \triangleq \{\mathbb{F}_{q^m} - \text{linear subspace } V \subseteq \mathbb{F}_{q^m}^n \text{ basis of } V \in \mathbb{F}_q^n\}.$$

Then, RGRW is defined as follows.

Definition 12 (RGRW [18, Definition 2, Lemma 4]): Let $\mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$ be a linear code and $\mathcal{C}_2 \subsetneq \mathcal{C}_1$ be its subcode. Then, the i-th Relative Generalized Rank Weight (i-th RGRW) of $\mathcal{C}_1$ and $\mathcal{C}_2$ is defined by

$$\begin{aligned} &M_{R,i}(\mathcal{C}_1, \mathcal{C}_2) \\ &\triangleq \min\{dim V : V \in \mathcal{G}, dim(\mathcal{C}_1 \cap V) - dim(\mathcal{C}_2 \cap V) \geq i\} \\ &= \min\{dim V : V \in \mathcal{G}, dim(\mathcal{C}_1 \cap V) - dim(\mathcal{C}_2 \cap V) = i\}, \end{aligned}$$

for $1 \leq i \leq dim(\mathcal{C}_1/\mathcal{C}_2)$.

The following proposition expresses how the Universal Perfect Security Threshold can be characterized by RGRW.

Proposition 2: [18, Corollary 5] Let $\mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$ be a linear code and $\mathcal{C}_2 \subsetneq \mathcal{C}_1$ be its subcode. In the model given in Section V-A, the source node encodes S into X by Nested Coset Coding with a linear code $\mathcal{C}_1$ and its subcode $\mathcal{C}_2$. If the number of eavesdropped links is μ, then the following holds.

$$\Theta_{USNC} = M_{R,1}(\mathcal{C}_2^{\perp}, \mathcal{C}_1^{\perp}) - 1.$$

From Definition 9, the following corollary of Proposition 2 is immediate.

Corollary 2: $B \in \mathbb{F}_q^{n\times\mu}$ such that $I(S; XB) > 0$ exists with $\mu = \Theta_{USNC} + 1$.

Using the aforementioned RGRW and the characterized USNC security properties, the following theorem is given for Universal IST.

Theorem 3: Let $\mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$ be a linear code and $\mathcal{C}_2 \subsetneq \mathcal{C}_1$ be its subcode. Consider Nested Coset Coding using $\mathcal{C}_1$, $\mathcal{C}_2$, and ψ over $\mathbb{F}_{q^m}$ in Definition 1. For $i \in \{1, \ldots, l\}$, we define the subcode $\mathcal{E}_i$ of $\mathcal{C}_1$ as follows.

$$\mathcal{E}_i \triangleq \bigcup_{\substack{S_i=0 \\ S_j \in \mathbb{F}_{q^m} : j \neq i}} \psi([S_1, \ldots, S_l]).$$

Then, the IST in the USNC that can be achieved by Nested Coset Coding with $\mathcal{C}_1, \mathcal{C}_2$ and ψ is

$$\Upsilon_{USNC} = \min\{M_{R,1}(\mathcal{E}_i^{\perp}, \mathcal{C}_1^{\perp}) : 1 \leq i \leq l\} - 1.$$

Proof: For $i \in \{1, \ldots, l\}$, $\mathcal{E}_i$ is the subcode of $\mathcal{C}_1$, and $dim\mathcal{E}_i = dim\mathcal{C}_1 - 1$ holds. Next, we define the following coset.

$$\tau(S_i = s_i) \triangleq \bigcup_{\substack{S_i=s_i \\ S_j \in \mathbb{F}_{q^m} : j \neq i}} \psi([S_1, \ldots, S_l]) \in \mathcal{C}_1/\mathcal{E}_i. \quad (5)$$

From (5), when we fix only $S_i = s_i$, X is a vector uniformly distributed over $\tau(s_i)$. Hence, X can be regarded as a vector generated by the Nested Coset Coding with $\mathcal{C}_1$, $\mathcal{E}_i$, and τ. Thus, from Proposition 2, when $\mu \leq M_{R,1}(\mathcal{E}_i^{\perp}, \mathcal{C}_1^{\perp}) - 1$, it follows that $I(S_i; XB) = 0$ for arbitrary $B \in \mathbb{F}_q^{n\times\mu}$. Also, from Corollary 2, a matrix $B \in \mathbb{F}_q^{n\times\mu}$ satisfying $I(S_i; XB) > 0$ exists when $\mu = M_{R,1}(\mathcal{E}_i^{\perp}, \mathcal{C}_1^{\perp})$. Therefore, we have the Theorem 3. □

VI. CONCLUSION

In this paper, we gave the IST as a new measure of security for linear secret sharing schemes. The IST indicates the maximum number of shares for which no individual element of secret information can be uniquely determined in linear secret sharing schemes, i.e., it provides a sufficient condition for satisfying IS. In linear secret sharing schemes, we also showed that the IST can be characterized by the code parameter RGHW. Moreover, we gave a precoding method for secret information that can guarantee the IST above a certain value in any linear secret sharing schemes. We further extended the notion of IST proposed in linear secret sharing schemes to USNC, and presented Universal IST. We also clarified that the Universal IST can be characterized by the code parameter RGRW.

ACKNOWLEDGMENT

The authors would like to thank the editors and the anonymous reviewers for their helpful comments.

REFERENCES

[1] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Int. Workshop Manag. Requirements Knowl. (MARK)*, Jun. 1979, pp. 313–318.
[3] J. Kurihara, T. Uyematsu, and R. Matsumoto, "Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight," *IEICE Trans. Fundamentals Electron., Commun. Comput. Sci.*, vol. 95, no. 11, pp. 2067–2075, 2012.
[4] H. Yamamoto, "Secret sharing system using (k, L, n) threshold scheme," *Electron. Commun. Jpn.*, vol. 69, no. 9, pp. 46–54, 1986.
[5] G. R. Blakley and C. Meadows, "Security of ramp schemes," in *Advances in Cryptology—CRYPTO*. Heidelberg, Germany: Springer, 1985, pp. 242–268.
[6] R. J. McEliece and D. V. Sarwate, "On sharing secrets and Reed–Solomon codes," *Commun. ACM*, vol. 24, no. 9, pp. 583–584, 1981.
[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland Mathematical Library, 1977.
[8] J. Pieprzyk and X.-M. Zhang, "Ideal threshold schemes from MDS codes," in *Proc. 5th Int. Conf. Inf. Secur. Cryptol.* (Lecture Notes in Computer Science), vol. 2587. Heidelberg, Germany: Springer, 2002, pp. 253–263.
[9] J. L. Massey, "Minimal codewords and secret sharing," in *Proc. 6th Joint Swedish–Russian Int. Workshop Inf. Theory*, 1993, pp. 276–279.
[10] I. M. Duursma and S. Park, "Coset bounds for algebraic geometric codes," *Finite Fields Their Appl.*, vol. 16, no. 1, pp. 36–55, 2010.
[11] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan, "Secure computation from random error correcting codes," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 4515. Heidelberg, Germany: Springer, 2007, pp. 291–310.
[12] A. Subramanian and S. W. McLaughlin, "MDS codes on the erasure-erasure wiretap channel," 2009, *arXiv:0902.3286*.
[13] R. Zamir, S. Shamai (Shitz), and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1250–1276, Jun. 2002.

[14] L. Holzbaur, S. Kruglik, A. Frolov, and A. Wachter-Zeh, "Secure codes with accessibility for distributed storage," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 5326–5337, 2021.
[15] L. Holzbaur, S. Kruglik, A. Frolov, and A. Wachter-Zeh, "Secrecy and accessibility in distributed storage," in *Proc. IEEE Global Commun. Conf.*, Dec. 2020, pp. 1–6.
[16] W. Huang and J. Bruck, "Secure RAID schemes for distributed storage," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2016, pp. 1401–1405.
[17] Y. Luo, C. Mitrpant, A. H. 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, Mar. 2005.
[18] J. Kurihara, R. Matsumoto, and T. Uyematsu, "Relative generalized rank weight of linear codes and its applications to network coding," *IEEE Trans. Inf. Theory*, vol. 61, no. 7, pp. 3912–3936, Jul. 2015.
[19] D. Silva and F. R. Kschischang, "Security for wiretap networks via rank-metric codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 176–180.
[20] A. Cohen, R. G. L. D'Oliveira, K. R. Duffy, and M. Médard, "Partial encryption after encoding for security and reliability in data systems," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2022, pp. 1779–1784.
[21] A. Cohen, A. Cohen, M. Médard, and O. Gurewitz, "Secure multi-source multicast," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 708–723, Jan. 2019.
[22] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: Wiley, Jan. 2006.
[23] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *ATT Bell Laboratories Tech. J.*, vol. 63, no. 10, pp. 2135–2157, 1984.
[24] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 5, pp. 1412–1418, Sep. 1991.
[25] S.-Y. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.
[26] N. Cai and R. W. Yeung, "Secure network coding on a wiretap network," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424–435, Jan. 2011.
[27] S. El Rouayheb, E. Soljanin, and A. Sprintson, "Secure network coding for wiretap networks of type II," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1361–1371, Mar. 2012.
[28] C.-K. Ngai, R. W. Yeung, and Z. Zhang, "Network generalized Hamming weight," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1136–1143, Feb. 2011.
[29] D. Silva and F. R. Kschischang, "Universal secure network coding via rank-metric codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1124–1135, Feb. 2011.
[30] Z. Zhang and B. Zhuang, "An application of the relative network generalized Hamming weight to erroneous wiretap networks," in *Proc. IEEE Inf. Theory Workshop*, Oct. 2009, pp. 70–74.

ITARU KURIHARA received the B.S. degree from the Department of Material Science, University of Hyogo, Japan, in 2022, where he is currently pursuing the master's degree with the Department of Data and Computational Science, Graduate School of Information Science. His research interests include secret sharing schemes and network coding.

JUN KURIHARA (Member, IEEE) received the B.E., M.E., and Ph.D. degrees in engineering from Tokyo Institute of Technology, in 2004, 2006, and 2012, respectively. From 2006 to 2017, he was with KDDI Corporation and KDDI R&D Laboratories Inc., as a Strategic Planner and a Research Engineer. He is currently an Associate Professor with the Graduate School of Information Science, University of Hyogo, and also a Principal Researcher with Zettant Inc. He was a Visiting Researcher with the Palo Alto Research Center (PARC), CA, USA, from 2013 to 2014, and Carnegie Mellon University, PA, USA, in 2022. His research interests include coding theory, networking architecture, and privacy in networking. He received the Best Paper Award from IEICE, in 2014.

TOSHIAKI TANAKA (Member, IEEE) received the B.E. and M.E. degrees in communication engineering from Osaka University, in 1984 and 1986, respectively, and the Ph.D. degree from Kyushu University, in 2007. He was with KDDI Corporation, from 1986 to 2021, was the Vice President of KDDI Research Inc., and has been a fellow of KDDI Corporation, since 2017. He is currently a Professor with the Graduate School of Information Science, University of Hyogo. His research interests include 5G security, network security, data trust, and privacy. He received the MEXT Commendation for Science and Technology, in 2014, the IEICE Achievement Award, in 2015, and the TTC Information and Communication Technology Award, in 2019.