

# Relative Generalized Rank Weight of Linear Codes and Its Applications to Network Coding

Jun Kurihara, *Member, IEEE*, Ryutaroh Matsumoto, *Member, IEEE*,  
and Tomohiko Uyematsu, *Senior Member, IEEE*

**Abstract**—By extending the notion of *minimum rank distance*, this paper introduces two new relative code parameters of a linear code  $C_1$  of length  $n$  over a field extension  $\mathbb{F}_{q^m}$  and its subcode  $C_2 \subseteq C_1$ . One is called the *relative dimension/intersection profile* (RDIP), and the other is called the *relative generalized rank weight* (RGRW). We clarify their basic properties and the relation between the RGRW and the minimum rank distance. As applications of the RDIP and the RGRW, the security performance and the error correction capability of secure network coding, guaranteed independently of the underlying network code, are analyzed and clarified. We propose a construction of secure network coding scheme, and analyze its security performance and error correction capability as an example of applications of the RDIP and the RGRW. Silva and Kschischang showed the existence of a secure network coding in which no part of the secret message is revealed to the adversary even if any  $\dim C_1 - 1$  links are wiretapped, which is guaranteed over any underlying network code. However, the explicit construction of such a scheme remained an open problem. Our new construction is just one instance of secure network coding that solves this open problem.

**Index Terms**—Network error correction, rank distance, relative dimension/intersection profile, relative generalized Hamming weight, relative generalized rank weight, secure network coding.

## I. INTRODUCTION

*Secure network coding* was first introduced by Cai and Yeung [6], and further investigated by Feldman et al. [12]. In the scenario of secure network coding, a source node transmits

$n$  packets from  $n$  outgoing links to sink nodes through a network that implements network coding [1], [19], [23], and each sink node receives  $N$  packets from  $N$  incoming links. In the network, there is an adversary who eavesdrops  $\mu$  links. The problem of secure network coding is how to encode a secret message into  $n$  transmitted packets at the source node, in such a way that the adversary obtains as little information as possible about the message in terms of information theoretic security.

As shown in [4], [11], secure network coding can be seen as a generalization of *secret sharing schemes* [2], [33] or the *wiretap channel II* [32] to network coding. The problem of secret sharing schemes is how to encode a secret message into  $n$  information symbols called *shares* in such a way that the message can be recovered only from certain subsets of shares. In order to solve both problems of secure network coding and secret sharing schemes, the *nested coset coding scheme* [44] is commonly used to encode a secret message to shares/transmitted packets, e.g., it has been used in [10], [11], [29], [32], [33], [37]. The nested coset coding scheme is defined by a linear code  $C_1 \subseteq \mathbb{F}_{q^m}^n$  and its subcode  $C_2 \subseteq C_1$  with  $\dim C_2 = \dim C_1 - l$  ( $l \geq 1$ ) over  $\mathbb{F}_{q^m}$ , where  $\mathbb{F}_{q^m}$  denotes an  $m$ -degree ( $m > 0$ ) field extension of a field  $\mathbb{F}_q$  of order  $q$ . From a secret message of  $l$  elements in  $\mathbb{F}_{q^m}$ , it generates each transmitted packet/each share defined as an element of  $\mathbb{F}_{q^m}$ .

Duursma and Park [10] defined the *coset distance* as a relative code parameter of  $C_1$  and  $C_2$ . The coset distance is the minimum value of the Hamming weight of codewords in  $C_1 \setminus C_2$ . They investigated the mathematical properties of the coset distance, and proved that in the case of secret sharing schemes using the nested coset coding scheme, the security guarantee of the scheme is exactly expressed in terms of the coset distance when the message consists of one information symbol, i.e.,  $l = 1$ . Motivated by their result using the coset distance, we [20] generalized their analysis to a secret message consisting of multiple ( $l \geq 1$ ) information symbols. In [20], it was clarified that the minimum uncertainty of the message given  $\mu (< n)$  shares is exactly expressed in terms of a relative code parameter of  $C_1$  and  $C_2$ , called the *relative dimension/length profile* (RDLP) [25]. The paper [20] also introduced a definition of the security in secret sharing schemes for the information leakage of every possible subset of elements composing the message by generalizing the security definition of *strongly secure ramp threshold secret sharing schemes* [43]. It was revealed in [20] that this security is also exactly expressed in terms of a relative code parameter of dual codes of  $C_1$  and  $C_2$ , called the *relative generalized*

Manuscript received January 24, 2013; revised December 27, 2013; revised again December 2, 2014; accepted April 18, 2015. This research was partially supported by the Japan Society for the Promotion of Science Grant Nos. 23246071 and 26289116, and the Villum Foundation through their VELUX Visiting Professor Programme. The material in this paper was presented in part at the 2012 IEEE International Symposium on Information Theory, Cambridge, MA, USA, Jul. 2012 [21], and in part at the 50th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA, Oct. 2012 [22].

J. Kurihara is with KDDI R&D Laboratories, Inc., 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502 Japan (e-mail: kurihara@ieee.org).

T. Uyematsu and R. Matsumoto are with Department of Communications and Integrated Systems, Tokyo Institute of Technology 2-12-1 Ookayama, Meguro-ku, Tokyo, 152-8550 Japan (e-mail: uyematsu@ieee.org; ryutaroh@rmatsumoto.org).

R. Matsumoto is also with Department of Mathematical Sciences, Aalborg University, Fredrik Bajers Vej 7G, 9220 Aalborg Ø, Denmark.

This paper is registered to the ORCID of Ryutaroh Matsumoto: <http://orcid.org/0000-0002-5085-8879>.

© 2015 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Digital Object Identifier <http://dx.doi.org/10.1109/TIT.2015.2429713>.

*Hamming weight* (RGHW) [25], where the coset distance coincides with the first RGHW. We note that in [25], the mathematical properties of the RDLP and the RGHW are extensively investigated in a systematic manner.

#### A. Our Aims and Motivations

The main aim of this paper is to extend the work in [20] to the security analysis of secure network coding based on the nested coset coding schemes, and to demonstrate its security performance guaranteed over *any* underlying network coded network. Namely, the security performance is guaranteed even over the *random network coding* [18]. On the other hand, the adversary in the scenario of network coding might be able to not only eavesdrop but also inject erroneous packets anywhere in the network, and the network may suffer from a rank deficiency of the transfer matrix at a sink node. Hence the second aim of this paper is to reveal the error correction capability of secure network coding based on the nested coset coding schemes with  $C_1$  and  $C_2$  which is guaranteed over *any* underlying network coded network as well as the security performance.

Simultaneously, we also aim to investigate the security performance and error correction capability in a general manner with no restriction on parameters. In particular, we aim to study them for a smaller extension degree  $m$  of  $\mathbb{F}_{q^m}$ , i.e., the packet length. To see the reason why smaller  $m$  deserve investigation in its own right, consider the case where the secure network coding is implemented as an application layer overlay network [47] on the Internet. Recall that the Internet protocol allows an intermediate router to split single packet into multiple fragments and route those fragments over different paths [40]. When the packet length  $m$  is larger than the path MTU [40, Section 2.9] (the maximum size that can avoid fragmentation on every link to a sink), symbols in a packet can be routed on different paths. Shioji et al. [34] demonstrated that existing security proofs cannot ensure the promised security when symbols in a packet are routed on different paths, because such a case is equivalent to the situation that an adversary changes the set of eavesdropped links according to the position of a symbol in a packet. Then, the maximum possible  $m$  is the path MTU, and hence the packet length  $m$  may have to be small, e.g.,  $m < n$ .

Furthermore, consider the software implementation of the encoder and decoder of the nested coset coding scheme. Recall that the encoding and decoding operations are executed not over the base field  $\mathbb{F}_q$  but over the field extension  $\mathbb{F}_{q^m}$  in the secure network coding scenario. In general, the operations over the smaller field work faster on software, and hence the size of  $\mathbb{F}_{q^m}$  should be as small as possible for the fast encoding and decoding operations. On the other hand, the intermediate network nodes execute  $\mathbb{F}_q$ -linear operations on packets as the underlying network coding operations. Considering the case where the random network coding [18] is employed as the underlying network coding, the size of  $\mathbb{F}_q$  should be appropriately large to guarantee the feasibility of the underlying network coded network with high probability near 1. Moreover, we may be unable to change the size of  $\mathbb{F}_q$  if the network coded

network is already in-use, and the packet length  $m$  may be naturally only the parameter that can be changed by the source node. Especially in such cases, the  $m$  may have to be small like  $m < n$  in order to attain the system requirements for high-speed data processing at software encoder and decoder.

From these observations, although the majority of existing researches of secure network coding, e.g., [31], [37] have assumed  $m \geq n$ , it is necessary to consider the secure network coding and its security performance and error correction capability for an arbitrary  $m$  in a general manner.

#### B. Our Contributions

To these ends, this paper first investigates mathematical properties of new relative code parameters of a linear code  $C_1 \subseteq \mathbb{F}_{q^m}^n$  and its subcode  $C_2 \subsetneq C_1$  in a similar manner to [25] on the RDLP and the RGHW. In Section II of this paper, we introduce two new relative code parameters called the *relative dimension/intersection profile* (RDIP) and the *relative generalized rank weight* (RGRW), and give some basic properties of the RDIP and the RGRW. Similar to the aim of this paper, Ngai et al. [29] introduced a code parameter called the *network generalized Hamming weight* (Network-GHW), and later Zhang et al. [46] extended Network-GHW to the *relative generalized network Hamming weight* (R-Network-GHW). The value of the (R-)Network-GHW depends on the underlying network topology and the network code, and hence the security performance expressed in terms of the (R-)Network-GHW is not guaranteed independently of the underlying network code. We will clarify the relation between the R-Network-GHW and the proposed parameters in Section II-B. We note that the *generalized rank weight* [31] was introduced by Oggier and Shouli concurrently and independently of the conference version [22] of this paper, and that the generalized rank weight is a special case of the RGRW. In Section II, we also point out that the RGRW can be viewed as a generalization of the *minimum rank distance* [15] of a linear code.

In order to measure the security performance of secure network coding, we first define a criterion called the *universal equivocation*  $\Theta_{\mu, P_{S,X}}$ , in Section III, which is the minimum uncertainty of the message under observation with  $\mu$  links for the joint distribution  $P_{S,X}$  of the secret message  $S$  and the transmitted packets  $X$ . Although  $P_{S,X}$  have been assumed to be uniform for the definition of  $\Theta_{\mu, P_{S,X}}$  in the conference version of this paper [22], we make no assumption regarding  $P_{S,X}$  in this paper. In [6], [11], [29], [46], the minimum uncertainty of the message was analyzed, but their analyses depend on the underlying network code. In contrast,  $\Theta_{\mu, P_{S,X}}$  is guaranteed independently of the underlying network code. Hence, it is called universal in the sense of [37]. Next, we introduce the second criterion. Consider the case where  $\Theta_{\mu, P_{S,X}}$  is less than the Shannon entropy [8, Ch. 2, p. 13] of the secret message. Then, some part of the secret message could be uniquely determined by the adversary. It is clearly desirable that no part of the secret message is deterministically revealed and that every part is kept hidden, even if some information of the secret message leaks to the adversary. From this observation,

we define the *universal  $\omega$ -strong security* to be the condition where the mutual information between any  $r$   $\mathbb{F}_{q^m}$ -symbols of the secret message and observed packets from arbitrary  $\omega-r+1$  tapped links ( $1 \leq r \leq l$ ) is always zero. Note that  $\omega$  is defined independently of the underlying network code and universal. The universal strong security defined in [21], [36] is a special case for  $\omega = n - 1$ .

The rest of Section III of this paper gives the main contribution of the paper: *we demonstrate that the universal security performance of secure network coding based on the nested coset coding scheme with  $C_1$  and  $C_2$  is exactly expressed in terms of our new code parameters, the RDIP and the RGRW.* This section first presents the upper and lower bound of the mutual information leaked from a set of tapped links with an arbitrary distribution  $P_{S,X}$ . By using this analysis, we demonstrate that the upper and lower bounds of  $\Theta_{\mu, P_{S,X}}$  are expressed in terms of the RDIP of  $C_1$  and  $C_2$  for arbitrary  $P_{S,X}$ , and the maximum possible value of  $\omega$ , defined as the *universal maximum strength*  $\Omega$ , is expressed in terms of the RGRW of dual codes of  $C_1$  and  $C_2$ . Moreover, in terms of  $\Omega$ , we express the upper bound of the maximum mutual information between a part of the secret message and observed packets for arbitrary  $P_{S,X}$ , which is independent of the underlying network code. In a later section, we give an example of this analysis for specific parameters of  $C_1$  and  $C_2$ .

For the error correction problem of secure network coding, in Section IV, we define the universal error correction capability against at most  $t$  injected error packets and at most  $\rho$  rank deficiency of the transfer matrix of a sink node. This is called universal because it is guaranteed independently of the underlying network code, as well as  $\Theta_{\mu, P_{S,X}}$  and  $\Omega$ . Then, Section IV gives the other main contribution of the paper: *We clarified that in secure network coding based on the nested coset coding scheme with  $C_1$  and  $C_2$ , the universal error correction capability against  $t$  errors and  $\rho$  rank deficiency is exactly expressed in terms of the first RGRW of  $C_1$  and  $C_2$ .* Although the conference version [22] of this paper considered only the case where the transfer matrix is completely known to each sink node, the analysis in this paper includes not only the case of known transfer matrices but also the case where the transfer matrix is unknown to every sink node.

As an example of applications of the above analyses by the RDIP and the RGRW, Section V of this paper also proposes a universal strongly secure network coding constructed from the nested coset coding schemes with  $C_1$  and  $C_2$  for fixed parameters, and provides its analysis. An explicit construction of the nested coset coding scheme that always achieves  $\Omega = \dim C_1 - 1$  had remained an open problem [36]. Inspired by Nishiara et al.'s strongly secure threshold ramp secret sharing scheme [30] using a Reed-Solomon code and its systematic generator matrix, Section V of this paper proposes an explicit construction with  $\Omega = \dim C_1 - 1$  using an maximum rank distance (MRD) code [15] and its systematic generator matrix, and solves the open problem. The earlier version of the proposed scheme was presented in the conference paper [21]. We note that in [21], the error correction in the scheme was not considered at all. With the addition of error correction, the scheme proposed in this paper is an extension of the earlier

version. Also note that the proposed scheme completely solves the open problem posed at the end of Section V-B of the survey paper of Cai and Chan on secure network coding [4].

The analysis of universal security performance of the proposed scheme is provided as an example of applications of the RDIP and the RGRW by means of the approach in Section III, which is a different from the analysis in the conference version [21]. We also provide an analysis of the universal error correction capability of our scheme as an application of the RGRW by the approach of Section IV. Note that by the analyses in Section III and Section IV, the universal equivocation and error correction capability of the scheme of Silva and Kschischang [37] can be also easily explained in terms of the RDIP and the RGRW for MRD codes  $C_1$  and  $C_2$ . We shall briefly explain the difference between our sample scheme and [37] in the next subsection.

### C. Difference Between Our Scheme and [37]

In [37], Silva and Kschischang [37] proposed a secure network coding scheme based on the nested coset coding scheme with MRD codes  $C_1$  and  $C_2$  [15]. Although our scheme is based on the nested coset coding scheme using an MRD code as well as their schemes, there exist several differences between these two schemes. Table I summarizes the comparison between the scheme in [37] and the proposed scheme for the universal security performance and the universal error correction capability.

Both in the proposed scheme and in the scheme of Silva and Kschischang [37], it is guaranteed that the universal equivocation  $\Theta_{\mu, P_{S,X}}$  for  $\mu \leq \dim C_2$  equals the Shannon entropy  $H(S)$  [8, Ch. 2, p. 13] of the secret message  $S$  when the distribution of the transmitted packets  $X$  is conditionally uniform given  $S$ . This implies that no information about the message leaks out even if any  $\dim C_2$  links are observed by an adversary. Both schemes also guarantee that the secret message is correctly decodable against any  $t$  error packets injected somewhere in the network and  $\rho$  rank deficiency of the transfer matrix of the sink node whenever  $n - \dim C_1 + 1 > 2t + \rho$  holds.

Our only assumption is that the network must transport packets of size  $m \geq l + n$  symbols. Although this necessary condition on the packet length is greater than the that of the scheme of Silva and Kschischang given as  $m \geq n$ , our scheme has an advantage on the universal maximum strength over their scheme. Unlike Silva et al.'s scheme [37], our scheme always guarantees the universal maximum strength  $\Omega = \dim C_1 - 1 = n - 1$  for  $C_1 = \mathbb{F}_{q^m}^n$ . This implies that in our scheme no information about any  $r$   $\mathbb{F}_{q^m}$ -symbols of the secret message is obtained by the adversary with  $\mu = \dim C_1 - r$  tapped links ( $1 \leq r \leq l$ ). In [36], Silva and Kschischang proved that there exist cases where their scheme [37] has  $\Omega = \dim C_1 - 1 = n - 1$ , and showed that the sufficient condition on the existence of such a case is given as  $m \geq (l + n)^2/8 + \log_q 16l$  for the packet length. However,  $\Omega = \dim C_1 - 1 = n - 1$  is not always guaranteed in their scheme even if the sufficient condition is satisfied, and an explicit construction of the scheme that always has  $\Omega = \dim C_1 - 1 = n - 1$  had been an open problem, as stated in the previous subsection.

TABLE I

COMPARISON BETWEEN THE SCHEME IN [37] AND OUR SCHEME IN SECTION V WITH THE FOLLOWING CRITERIA: THE MAXIMUM POSSIBLE NUMBER OF TAPPED LINKS  $\mu$  WITH NO INFORMATION LEAKAGE OF THE SECRET MESSAGE; THE GUARANTEE OF THE UNIVERSAL MAXIMUM STRENGTH  $\Omega = \dim C_1 - 1$ ; THE CONDITION TO CORRECTLY DECODE THE SECRET MESSAGE AGAINST  $t$  INJECTED ERROR PACKETS AND  $\rho$  RANK DEFICIENCY OF THE TRANSFER MATRIX AT THE SINK NODE.

| Universal Security Performance |  |   | Universal Error Correction Capability   |  |
|--------------------------------|--|---|---|--|
|                                | Maximum Possible $\mu$ with No Information Leakage | Guarantee of $\Omega = \dim C_1 - 1$      | Condition to Correctly Decode the Message against $t$ Errors and $\rho$ Rank Deficiency | Necessary Condition on the Size of $m$ |
| [37]                           | $\dim C_2$   | Not Always ( $\Omega \leq \dim C_1 - 1$ ) | $n - \dim C_1 \geq 2t + \rho$   | $m \geq n$                             |
| Section V                      | $\dim C_2$   | Always                                    | $n - \dim C_1 \geq 2t + \rho$   | $m \geq l + n$                         |

#### D. Organization

Here again, we briefly show the structure of this paper. The remainder of this paper is organized as follows. Section II defines the RDIP and RGRW of linear codes, and introduces their basic properties. We also show their relations to the existing code parameters in this section. Section III defines the universal security performance over the wiretap network model, and reveals that the universal security performance of secure network coding is exactly expressed in terms of the RDIP and the RGRW. In Section IV, we also reveal that the universal error correction capability of secure network coding is exactly expressed in terms of the RGRW. As an example, an explicit construction of strongly secure network coding is proposed in Section V, and its security performance and error correction capability are analyzed by the RDIP and the RGRW. Finally, Section VI presents our conclusions.

## II. NEW PARAMETERS OF LINEAR CODES AND THEIR PROPERTIES

### A. Notations and Preliminaries

Let  $\mathbb{F}_q$  be a finite field containing  $q$  elements and  $\mathbb{F}_{q^m}$  be an  $m$ -degree field extension of  $\mathbb{F}_q$  ( $m \geq 1$ ). Let  $\mathbb{F}_q^n$  denote an  $n$ -dimensional row vector space over  $\mathbb{F}_q$ . Similarly,  $\mathbb{F}_{q^m}^n$  denotes an  $n$ -dimensional row vector space over  $\mathbb{F}_{q^m}$ . Unless otherwise stated, we consider subspaces, ranks, dimensions, etc., over the field extension  $\mathbb{F}_{q^m}$  instead of the base field  $\mathbb{F}_q$ .

An  $[n, k]$  linear code  $C$  over  $\mathbb{F}_{q^m}^n$  is a  $k$ -dimensional subspace of  $\mathbb{F}_{q^m}^n$ . Let  $C^\perp$  denote the *dual code* of a code  $C$  [26, Ch. 1, p. 26]. A subspace of a code is called a *subcode*. For  $C \subseteq \mathbb{F}_{q^m}^n$ , we denote by  $C|_{\mathbb{F}_q}$  a *subfield subcode*  $C \cap \mathbb{F}_q^n$  [26, Ch. 7, p. 207]. Observe that  $\dim C$  means the dimension of  $C$  as a vector space over  $\mathbb{F}_{q^m}$  whereas  $\dim C|_{\mathbb{F}_q}$  is the dimension of  $C|_{\mathbb{F}_q}$  over  $\mathbb{F}_q$ .

For a vector  $v = [v_1, \dots, v_n] \in \mathbb{F}_{q^m}^n$  and a subspace  $V \subseteq \mathbb{F}_{q^m}^n$ , we denote  $v^q = [v_1^q, \dots, v_n^q]$  and  $V^q = \{v^q : v \in V\}$ . For a subspace  $V \subseteq \mathbb{F}_{q^m}^n$ , we define by  $V^* \triangleq \sum_{i=0}^{m-1} V^{q^i}$  the sum of subspaces  $V, V^q, \dots, V^{q^{m-1}}$ . Define a family of subspaces  $V \subseteq \mathbb{F}_{q^m}^n$  satisfying  $V = V^q$  by

$$\Gamma(\mathbb{F}_{q^m}^n) \triangleq \{\mathbb{F}_{q^m}\text{-linear subspace } V \subseteq \mathbb{F}_{q^m}^n : V = V^q\}.$$

Also define

$$\Gamma_i(\mathbb{F}_{q^m}^n) \triangleq \{V \in \Gamma(\mathbb{F}_{q^m}^n) : \dim V = i\}.$$

For  $\Gamma(\mathbb{F}_{q^m}^n)$ , we have the following lemmas given in [39].

**Lemma 1** ([39, Lemma 1]). Let  $V \subseteq \mathbb{F}_{q^m}^n$  be a subspace. Then, the followings are equivalent; 1)  $V \in \Gamma(\mathbb{F}_{q^m}^n)$ , 2) There is a basis of  $V$  consisting of vectors in  $\mathbb{F}_q^n$ . In particular,  $V \in \Gamma(\mathbb{F}_{q^m}^n)$  if and only if  $\dim V|_{\mathbb{F}_q} = \dim V$ .

**Lemma 2** ([39]). For a subspace  $V \subseteq \mathbb{F}_{q^m}^n$ ,  $V^*$  is the smallest subspace in  $\Gamma(\mathbb{F}_{q^m}^n)$ , containing  $V$ .

**Lemma 3** ([39]). For a subspace  $V \subseteq \mathbb{F}_{q^m}^n$ ,  $\dim V^* \leq m \cdot \dim V$ .

### B. Definitions of New Parameters

We first define the *relative dimension/intersection profile* (RDIP) of linear codes as follows.

**Definition 4** (Relative Dimension/Intersection Profile). Let  $C_1 \subseteq \mathbb{F}_{q^m}^n$  be a linear code and  $C_2 \subsetneq C_1$  be its subcode. Then, the  $i$ -th relative dimension/intersection profile ( $i$ -th RDIP) of  $C_1$  and  $C_2$  is the greatest difference between dimensions of intersections, defined as

$$K_{R,i}(C_1, C_2) \triangleq \max_{V \in \Gamma_i(\mathbb{F}_{q^m}^n)} \{\dim(C_1 \cap V) - \dim(C_2 \cap V)\}, \quad (1)$$

for  $0 \leq i \leq n$ .

Next, we define the *relative generalized rank weight* (RGRW) of linear codes as follows.

**Definition 5** (Relative Generalized Rank Weight). Let  $C_1 \subseteq \mathbb{F}_{q^m}^n$  be a linear code and  $C_2 \subsetneq C_1$  be its subcode. Then, the  $i$ -th relative generalized rank weight ( $i$ -th RGRW) of  $C_1$  and  $C_2$  is defined by

$$\begin{aligned} M_{R,i}(C_1, C_2) \\ \triangleq \min \left\{ \dim V : V \in \Gamma(\mathbb{F}_{q^m}^n), \dim(C_1 \cap V) - \dim(C_2 \cap V) \geq i \right\}, \end{aligned} \quad (2)$$

for  $0 \leq i \leq \dim(C_1/C_2)$ .

In [31], Oggier and Sbouï proposed the *generalized rank weight* under the restriction of the degree  $m \geq n$ . The generalized rank weight can be viewed as a special case of the RGRW with  $C_2 = \{0\}$  when  $m \geq n$ . In the first version of this paper, we pointed out this fact, but we did not give its proof. Later, Ducoat proved this in [9].

Here we briefly explain the relation between these new parameters and the existing *relative* parameters defined by a code and its subcode. For an index set  $I \subseteq \{1, \dots, n\}$ , define a subspace  $\mathcal{E}_I \triangleq \{x = [x_1, \dots, x_n] \in \mathbb{F}_{q^m}^n : x_i = 0 \text{ for } i \notin I\} \subseteq \mathbb{F}_{q^m}^n$ . We have  $\dim \mathcal{E}_I = |I|$ . Let  $\Lambda(\mathbb{F}_{q^m}^n)$  and  $\Lambda_i(\mathbb{F}_{q^m}^n)$  for  $0 \leq i \leq n$  be collections of  $\mathbb{F}_{q^m}$ -linear subspaces of  $\mathbb{F}_{q^m}^n$ , defined by

$$\Lambda(\mathbb{F}_{q^m}^n) \triangleq \{\mathcal{E}_I \subseteq \mathbb{F}_{q^m}^n : I \subseteq \{1, \dots, n\}\},$$

$$\Lambda_i(\mathbb{F}_{q^m}^n) \triangleq \{\mathcal{E}_I \in \Lambda(\mathbb{F}_{q^m}^n) : \dim \mathcal{E}_I = i\}.$$

The  $i$ -th *relative dimension/length profile* (RDLP) defined by Luo et al. [25] is obtained by replacing  $\Gamma_i(\mathbb{F}_{q^m}^n)$  in (1)

with  $\Lambda_i(\mathbb{F}_{q^m}^n)$ . Also, the *relative generalized Hamming weight* (RGHW) [25] is given by replacing  $\Gamma(\mathbb{F}_{q^m}^n)$  in (2) with  $\Lambda(\mathbb{F}_{q^m}^n)$ . Additionally, the *generalized Hamming weight* (GHW) [42] is obtained by replacing  $\Gamma(\mathbb{F}_{q^m}^n)$  in (2) with  $\Lambda(\mathbb{F}_{q^m}^n)$  and setting  $C_2 = \{0\}$ .

**Remark 6.** For an arbitrary index set  $I \subseteq \{1, \dots, n\}$ , a basis of  $\mathcal{E}_I$  is  $\{e^{(i)} = [e_1^{(i)}, \dots, e_n^{(i)}] : i \in I\}$  from the definition of  $\mathcal{E}_I$ , where  $e_j^{(i)} = 1$  if  $i = j$ , and  $e_j^{(i)} = 0$  if  $i \neq j$ . This implies that a basis of  $\mathcal{E}_I$  consists of vectors in  $\mathbb{F}_q^n$ , and hence we have  $\mathcal{E}_I \in \Gamma(\mathbb{F}_{q^m}^n)$  from Lemma 1. We thus have  $\Lambda(\mathbb{F}_{q^m}^n) \subseteq \Gamma(\mathbb{F}_{q^m}^n)$  and  $\Lambda_i(\mathbb{F}_{q^m}^n) \subseteq \Gamma_i(\mathbb{F}_{q^m}^n)$ . This implies that the RDIP of linear codes is always greater than or equal to the RDLP of the codes, and that the RGRW of linear codes is always smaller than or equal to the RGHW of the codes.

We also show the relation between the RGRW and the *relative network generalized Hamming weight* (R-Network-GHW) [46]. Let  $\mathcal{F}$  be a set of some one-dimensional subspaces of  $\mathbb{F}_q^n$ . Each subspace in  $\mathcal{F}$  was defined as a space spanned by a global coding vector [14, Ch. 2, p. 18] of each link in the network coded network. (For the definition of global coding vectors, see Section III-A or [14]). Let  $2^\mathcal{F}$  be the power set of  $\mathcal{F}$ . For  $2^\mathcal{F}$ , define a set of direct sums of subspaces by

$$\Upsilon_\mathcal{F} \triangleq \left\{ W \subseteq \mathbb{F}_q^n : W = \sum_{V \in \mathcal{J}} V, \mathcal{J} \in 2^\mathcal{F} \right\}.$$

We restrict the degree  $m$  of field extension  $\mathbb{F}_{q^m}$  to  $m = 1$ , i.e.,  $C_1$  and  $C_2$  are  $\mathbb{F}_q$ -linear subspaces of  $\mathbb{F}_q^n$ . Then, the R-Network-GHW of  $C_1$  and  $C_2$  for the network is obtained by replacing  $\Gamma(\mathbb{F}_{q^m}^n)$  in (2) with  $\Upsilon_\mathcal{F}$ . In addition, the *network generalized Hamming weight* (Network-GHW) [29] is obtained by replacing  $\Gamma(\mathbb{F}_{q^m}^n)$  in (2) with  $\Upsilon_\mathcal{F}$  and set  $C_2 = \{0\}$ , as the relation between the RGHW and the GHW.

**Remark 7.** Note that in the definitions of R-Network-GHW and Network-GHW, the field over which the global coding vectors are defined must coincide with the field over which linear codes  $C_1$  and  $C_2$  are defined. Hence, we restricted the degree  $m$  to 1 of the field extension  $\mathbb{F}_{q^m}$  over which  $C_1$  and  $C_2$  are defined. In the case of  $m = 1$ , we have  $\Upsilon_\mathcal{F} \subseteq \Gamma(\mathbb{F}_{q^m}^n)$ . Thus, the RGRW of  $C_1$  and  $C_2$  for  $m = 1$  is always smaller than or equal to the R-Network-GHW.

### C. Basic Properties of the RDIP and the RGRW

This subsection introduces some basic properties of the RDIP and the RGRW. They will be used for expressions of the universal security performance (Section III) and the universal error correction capability (Section IV) of secure network coding.

**Theorem 8** (Monotonicity of the RDIP). Let  $C_1 \subseteq \mathbb{F}_{q^m}^n$  be a linear code and  $C_2 \subseteq C_1$  be its subcode. Then, the  $i$ -th RDIP  $K_{R,i}(C_1, C_2)$  is nondecreasing with  $i$  from  $K_{R,0}(C_1, C_2) = 0$  to  $K_{R,n}(C_1, C_2) = \dim(C_1/C_2)$ , and  $0 \leq K_{R,i+1}(C_1, C_2) - K_{R,i}(C_1, C_2) \leq 1$  holds.

*Proof:*  $K_{R,0}(C_1, C_2) = 0$  and  $K_{R,n}(C_1, C_2) = \dim(C_1/C_2)$  are obvious from Definition 4. By Lemma 1, for any subspace

$V_1 \in \Gamma_{i+1}(\mathbb{F}_{q^m}^n)$ , some  $V_2$ 's satisfying  $V_2 \in \Gamma_i(\mathbb{F}_{q^m}^n)$  and  $V_2 \subsetneq V_1$  always exist. This yields  $K_{R,i}(C_1, C_2) \leq K_{R,i+1}(C_1, C_2)$ .

Next we show that the increment at each step is at most 1. Consider arbitrary subspaces  $V, V' \in \Gamma(\mathbb{F}_{q^m}^n)$  such that  $\dim V' = \dim V + 1$  and  $V \subsetneq V'$ . Let  $f = \dim(C_1 \cap V) - \dim(C_2 \cap V)$  and  $g = \dim(C_1 \cap V') - \dim(C_2 \cap V')$ . Since

$$\dim(C_1 \cap V) + 1 \geq \dim(C_1 \cap V') \geq \dim(C_1 \cap V),$$

holds and  $C_2 \subsetneq C_1$ , we have  $f + 1 \geq g \geq f$  and hence  $K_{R,i}(C_1, C_2) + 1 \geq K_{R,i+1}(C_1, C_2) \geq K_{R,i}(C_1, C_2)$ . ■

We note that if we replace  $\Gamma_i(\mathbb{F}_{q^m}^n)$  with  $\Lambda_i(\mathbb{F}_{q^m}^n)$  in Theorem 8, it coincides with [25, Proposition 1] for the monotonicity of the RDLP.

**Lemma 9.** Let  $C_1 \subseteq \mathbb{F}_{q^m}^n$  be a linear code and  $C_2 \subsetneq C_1$  be its subcode. Then, the  $i$ -th RGRW  $M_{R,i}(C_1, C_2)$  is strictly increasing with  $i$ . Moreover,  $M_{R,0}(C_1, C_2) = 0$  and

$$\begin{aligned} M_{R,i}(C_1, C_2) &= \min \{ j : K_{R,j}(C_1, C_2) = i \} \\ &= \min \{ \dim V : V \in \Gamma(\mathbb{F}_{q^m}^n), \dim(C_1 \cap V) - \dim(C_2 \cap V) = i \}, \end{aligned}$$

for  $0 \leq i \leq \dim(C_1/C_2)$ .

*Proof:* First we have

$$\begin{aligned} &\min \{ j : K_{R,j}(C_1, C_2) \geq i \} \\ &= \min \{ j : \exists V \in \Gamma_j(\mathbb{F}_{q^m}^n), \\ &\quad \text{such that } \dim(C_1 \cap V) - \dim(C_2 \cap V) \geq i \} \\ &= \min \{ \dim V : V \in \Gamma(\mathbb{F}_{q^m}^n), \dim(C_1 \cap V) - \dim(C_2 \cap V) \geq i \} \\ &= M_{R,i}(C_1, C_2). \end{aligned}$$

We also have

$$\{ j : K_{R,j}(C_1, C_2) = i \} \cap \{ j : K_{R,j}(C_1, C_2) \geq i + 1 \} = \emptyset,$$

by the basic set theory. Recall that from Theorem 8,  $K_{R,j}(C_1, C_2)$  is nondecreasing function of  $j$  and  $\{ j : K_{R,j}(C_1, C_2) = i \} \neq \emptyset$  for all  $i \in \{0, \dots, \dim(C_1/C_2)\}$ . We thus have

$$\begin{aligned} M_{R,i}(C_1, C_2) &= \min \{ j : K_{R,j}(C_1, C_2) \geq i \} \\ &= \min \{ j : K_{R,j}(C_1, C_2) = i \}. \end{aligned}$$

Therefore the RGRW is strictly increasing with  $i$  and thus

$$\begin{aligned} M_{R,i}(C_1, C_2) &= \min \{ \dim V : V \in \Gamma(\mathbb{F}_{q^m}^n), \dim(C_1 \cap V) - \dim(C_2 \cap V) = i \}, \end{aligned}$$

is established. ■

In [31, Lemma 1], it was shown that in the case of  $C_2 = \{0\}$ , the second RGRW  $M_{R,2}(C_1, \{0\})$  is greater than the first RGRW  $M_{R,1}(C_1, \{0\})$ .

We note that if we replace  $\Gamma(\mathbb{F}_{q^m}^n)$  and  $K_{R,j}(C_1, C_2)$  in Lemma 9 with  $\Lambda(\mathbb{F}_{q^m}^n)$  and the  $j$ -th RDLP, the lemma coincides with [25, Theorem 3] for the properties of RGHW. Also, if we replace  $\Gamma(\mathbb{F}_{q^m}^n)$  in Lemma 9 with  $\Upsilon_\mathcal{F}$ , the property of strictly

increasing the RGRW shown in the lemma also becomes the property of the R-Network-GHW [46, Theorem 3.2].

Now we present the following upper bound of the RGRW.

**Proposition 10.** Let  $C_1 \subseteq \mathbb{F}_{q^m}^n$  be a linear code and  $C_2 \subsetneq C_1$  be its subcode. Then, the RGRW of  $C_1$  and  $C_2$  is upper bounded by

$$M_{R,i}(C_1, C_2) \leq \min\{n - \dim C_1, (m-1) \dim C_1/C_2\} + i, \quad (3)$$

for  $1 \leq i \leq \dim(C_1/C_2)$ .

*Proof:* We can assume that  $C_2$  is a systematic code without loss of generality. That is, we can choose a basis of  $C_2$  in such a way that the set of subvectors consisting of the first  $\dim C_2$  coordinates of the chosen basis coincides with the canonical basis of  $\mathbb{F}_{q^m}^{\dim C_2}$ . Let  $\mathcal{S} \subsetneq \mathbb{F}_{q^m}^n$  be a linear code such that  $C_1$  is the direct sum of  $C_2$  and  $\mathcal{S}$ . Then, after suitable permutation of coordinates, a basis of  $\mathcal{S}$  can be chosen such that its first  $\dim C_2$  coordinates are zero. Hence, a code  $\mathcal{S}$  can be regarded as a code of length  $n - \dim C_2$ , and we have  $M_{R, \dim \mathcal{S}}(\mathcal{S}, \{0\}) \leq n - \dim C_2$  from the definition of the RGRW. On the other hand, since  $M_{R, \dim \mathcal{S}}(\mathcal{S}, \{0\}) = \dim \mathcal{S}^*$  from the definition of the RGRW and Lemma 2, and  $\dim \mathcal{S}^* \leq m \cdot \dim \mathcal{S}$  from Lemma 3, we have  $M_{R, \dim \mathcal{S}}(\mathcal{S}, \{0\}) \leq m \cdot \dim \mathcal{S} = m \cdot \dim C_1/C_2$ . We thus have

$$M_{R, \dim \mathcal{S}}(\mathcal{S}, \{0\}) \leq \min\{n - \dim C_2, m \cdot \dim C_1/C_2\}.$$

We shall use the mathematical induction on  $t$ . We see that

$$M_{R,t}(\mathcal{S}, \{0\}) \leq \min\{n - \dim C_1, (m-1) \dim C_1/C_2\} + t, \quad (4)$$

is true for  $t = \dim \mathcal{S} = \dim C_1 - \dim C_2$ . Assume that for some  $t \geq 1$ , (4) is true. Then, since the  $M_i(\mathcal{S}, \{0\})$  is strictly increasing with  $i$  from Lemma 9, we have

$$\begin{aligned} M_{R,t-1}(\mathcal{S}, \{0\}) &\leq M_{R,t}(\mathcal{S}, \{0\}) - 1 \\ &\leq \min\{n - \dim C_1, (m-1) \dim C_1/C_2\} + t - 1, \end{aligned}$$

holds. Thus, it is proved by mathematical induction that (4) holds for  $1 \leq t \leq \dim(C_1/C_2)$ .

Lastly, we prove (3) by the above discussion about the RGRW of  $\mathcal{S}$  and  $\{0\}$ . For an arbitrarily fixed subspace  $V \subseteq \mathbb{F}_{q^m}^n$ , we have  $\dim(C_1 \cap V) \geq \dim(\mathcal{S} \cap V) + \dim(C_2 \cap V)$ , because  $C_1$  is a direct sum of  $\mathcal{S}$  and  $C_2$ . Hence,  $\dim(C_1 \cap V) - \dim(C_2 \cap V) \geq \dim(\mathcal{S} \cap V)$  holds, and we have  $M_{R,i}(C_1, C_2) \leq M_{R,i}(\mathcal{S}, \{0\})$  for  $1 \leq i \leq \dim(C_1/C_2)$  from the definition of the RGRW. Therefore, from the foregoing proof, we have

$$\begin{aligned} M_{R,i}(C_1, C_2) &\leq M_{R,i}(\mathcal{S}, \{0\}) \\ &\leq \min\{n - \dim C_1, (m-1) \dim C_1/C_2\} + i, \end{aligned} \quad (5)$$

for  $1 \leq i \leq \dim(C_1/C_2)$ , and the proposition is proved.  $\blacksquare$

If  $n - \dim C_2 \leq m \cdot \dim C_1/C_2$  holds and  $\Gamma(\mathbb{F}_{q^m}^n)$  is replaced with  $\Lambda(\mathbb{F}_{q^m}^n)$ , this lemma coincides with the generalized Singleton bound for the RGHW [25, Theorem 4]. Also, if  $n - \dim C_2 \leq m \cdot \dim C_1/C_2$  holds and  $\Gamma(\mathbb{F}_{q^m}^n)$  is replaced with  $\Upsilon_{\mathcal{F}}$ , i.e., the RGRW is replaced to the R-Network-GHW, it becomes [46, Theorem 3.4].

#### D. Relation between the Rank Distance and the RGRW

Next, we show the relation between the rank distance [15] and the RGRW. We will use the relation to express the universal security performance (Section III) and the universal error correction capability (Section IV) of secure network coding.

For a vector  $x = [x_1, \dots, x_n] \in \mathbb{F}_{q^m}^n$ , we denote by  $\mathfrak{S}(x) \subseteq \mathbb{F}_{q^m}^n$  an  $\mathbb{F}_q$ -linear subspace of  $\mathbb{F}_{q^m}^n$  spanned by  $x_1, \dots, x_n$ . The rank distance [15] between two vectors  $x, y \in \mathbb{F}_{q^m}^n$  is given by  $d_R(x, y) \triangleq \dim_{\mathbb{F}_q} \mathfrak{S}(y - x)$ , where  $\dim_{\mathbb{F}_q}$  denotes the dimension over the base field  $\mathbb{F}_q$ . In other words, it is the maximum number of coordinates in  $(y - x)$  that are linearly independent over  $\mathbb{F}_q$ . The minimum rank distance [15] of a code  $C$  is given as

$$\begin{aligned} d_R(C) &\triangleq \min\{d_R(x, y) : x, y \in C, x \neq y\} \\ &= \min\{d_R(x, 0) : x \in C, x \neq 0\}. \end{aligned}$$

**Lemma 11.** Let  $b \in \mathbb{F}_{q^m}^n$  be an  $n$ -dimensional nonzero vector over  $\mathbb{F}_{q^m}$ , and let  $\langle b \rangle \subseteq \mathbb{F}_{q^m}^n$  be an  $\mathbb{F}_{q^m}$ -linear one-dimensional subspace of  $\mathbb{F}_{q^m}^n$  spanned by  $b$ . Then, we have  $\dim \langle b \rangle^* = d_R(b, 0)$ .

*Proof:* Let  $\{\gamma_1, \dots, \gamma_m\}$  be an  $\mathbb{F}_q$ -basis of  $\mathbb{F}_{q^m}$ . Let  $d = d_R(b, 0) = \dim_{\mathbb{F}_q} \mathfrak{S}(b)$ . From the definition of the rank distance, there exists a nonsingular matrix  $P \in \mathbb{F}_q^{n \times n}$  satisfying

$$b = \underbrace{[\gamma_1, \dots, \gamma_d, 0, \dots, 0]}_{\triangleq a \in \mathbb{F}_{q^m}^n} P.$$

For  $\alpha_1, \alpha_2 \in \mathbb{F}_q$ ,  $\beta_1, \beta_2 \in \mathbb{F}_{q^m}$ , we have  $\alpha_1 \beta_1^{q^i} + \alpha_2 \beta_2^{q^i} = (\alpha_1 \beta_1 + \alpha_2 \beta_2)^{q^i}$  ( $0 \leq i \leq m-1$ ). Thus, since  $P$  is a matrix over  $\mathbb{F}_q$ , we have  $b^{q^i} = (aP)^{q^i} = a^{q^i} P$ . Let  $\langle b, b^q, \dots, b^{q^{m-1}} \rangle \subseteq \mathbb{F}_{q^m}^n$  be an  $\mathbb{F}_{q^m}$ -linear subspace of  $\mathbb{F}_{q^m}^n$  spanned by  $m$  vectors  $b, b^q, \dots, b^{q^{m-1}}$ , then we have  $\langle b \rangle^* = \langle b, b^q, \dots, b^{q^{m-1}} \rangle$ . Hence, since  $P$  is nonsingular, we have

$$\begin{aligned} \dim \langle b \rangle^* &= \dim \langle b, b^q, \dots, b^{q^{m-1}} \rangle \\ &= \dim \langle aP, a^q P, \dots, a^{q^{m-1}} P \rangle \\ &= \dim \langle a, a^q, \dots, a^{q^{m-1}} \rangle \\ &= \text{rank} \underbrace{\begin{bmatrix} a \\ a^q \\ \vdots \\ a^{q^{m-1}} \end{bmatrix}}_{\triangleq T \in \mathbb{F}_q^{m \times n}}. \end{aligned}$$

Since the right  $n-d$  columns of  $T$  are zero columns, we have  $\text{rank } T \leq d$ . On the other hand, the upper-left  $d \times d$  submatrix  $T'$  of  $T$  is the generator matrix of Gabidulin code of length  $d$  and dimension  $d$  [15], and hence we must have  $\text{rank } T' = d$ . Thus, we have  $\text{rank } T \geq d$ . Therefore, we have  $\dim \langle b \rangle^* = \text{rank } T = d$ .  $\blacksquare$

**Lemma 12.** For a code  $C_1 \subseteq \mathbb{F}_{q^m}^n$  and its subcode  $C_2 \subsetneq C_1$ , the first RGRW can be represented as  $M_{R,1}(C_1, C_2) = \min\{d_R(x, 0) : x \in C_1 \setminus C_2\}$ .

*Proof:* From Lemma 2,  $M_{R,1}(C_1, C_2)$  can be represented as

$$\begin{aligned} M_{R,1}(C_1, C_2) &= \min \left\{ \dim W : W \in \Gamma(\mathbb{F}_{q^m}^n), \dim(C_1 \cap W) - \dim(C_2 \cap W) \geq 1 \right\} \\ &= \min \left\{ \dim W : W \in \Gamma(\mathbb{F}_{q^m}^n), \exists v \in (C_1 \cap W) \setminus C_2 \right\} \\ &= \min \{ \dim \langle v \rangle^* : v \in C_1 \setminus C_2 \}. \end{aligned}$$

Therefore, since  $\dim \langle v \rangle^* = d_R(v, 0)$  for a vector  $v \in \mathbb{F}_{q^m}^n$  from Lemma 11, we have  $M_{R,1}(C_1, C_2) = \min \{ d_R(v, 0) : v \in C_1 \setminus C_2 \}$ . ■

Lemma 12 immediately yields that  $M_{R,1}(\cdot, \{0\})$  coincides with  $d_R(\cdot)$ .

**Corollary 13.** For a linear code  $C$ ,  $d_R(C) = M_{R,1}(C, \{0\})$  holds. ■

Here we introduce the Singleton-type bound of rank distance [15], [24].

**Proposition 14** (Singleton-Type Bound of Rank Distance [15], [24]). Let  $C \subseteq \mathbb{F}_{q^m}^n$  be a linear code. Then, the minimum rank distance of  $C$  is upper bounded by

$$d_R(C) \leq \min \left\{ 1, \frac{m}{n} \right\} (n - \dim C) + 1. \quad (6)$$

Note that the right-hand side of (6) is  $n - \dim C + 1$  if  $m \geq n$  and  $\frac{m}{n}(n - \dim C) + 1$  if  $m < n$ . A code satisfying the equality of (6) is called a *maximum rank distance* (MRD) code [15]. The Gabidulin code [15] is known as an MRD code.

In the following, we shall present some extra properties of the RGRW  $M_{R,i}(\cdot, \cdot)$  and the minimum rank distance  $d_R(\cdot)$  by using the relation between  $M_{R,i}(\cdot, \cdot)$  and  $d_R(\cdot)$  shown above and the properties of the RGRW described in the previous subsection. In the case where  $m \geq n$ , Corollary 15 gives a generalization of the Singleton-type bound of rank distance [15], [24] of  $C \subseteq \mathbb{F}_{q^m}^n$ , and Corollary 16 shows that the RGRW of  $C_1 \subseteq \mathbb{F}_{q^m}^n$  and  $C_2 \subseteq C_1$  depends only on  $C_1$  when  $C_1$  is MRD. Proposition 17 presents an upper bound of the first RGRW by combining the Singleton-type bound of rank distance [15], [24] of  $C \subseteq \mathbb{F}_{q^m}^n$  for  $m < n$  and the upper bound of the RGRW given in Proposition 10. In the case where  $m < n$ , Corollary 18 gives a tighter upper bound of the minimum rank distance of  $C \subseteq \mathbb{F}_{q^m}^n$  for  $m < n$  and  $\dim C = 1$  than that shown in Proposition 14.

First, Lemma 9 and Proposition 10 yield the following corollary from Corollary 13 and Proposition 14. This corollary shows a generalization of the Singleton-type bound of rank distance [15], [24] of  $C \subseteq \mathbb{F}_{q^m}^n$  in the case where  $m \geq n$ .

**Corollary 15.** For a linear code  $C \subseteq \mathbb{F}_{q^m}^n$  with  $m \geq n$ ,  $M_{R,i}(C, \{0\}) \leq (n - \dim C) + i$  for  $1 \leq i \leq \dim C$ . The equality holds for all  $i$  if and only if  $C$  is an MRD code.

*Proof:* From Proposition 10,  $M_{R,i}(C, \{0\}) \leq (n - \dim C) + i$  is immediate. The RGRW  $M_{R,i}(C, \{0\})$  is strictly increasing with  $i$  from Lemma 9, and  $M_{R,\dim C}(C, \{0\}) \leq n$  holds. Therefore, from Corollary 13 and Proposition 14,  $M_{R,i}(C, \{0\}) = n - \dim C + i$  for  $1 \leq i \leq \dim C$  must hold if and only if  $C$  is MRD with  $m \geq n$ . ■

Next, we give the following corollary of Proposition 10 for the RGRW of  $C_1 \subseteq \mathbb{F}_{q^m}^n$  and  $C_2 \subseteq C_1$ . This corollary reveals that when  $C_1$  is an MRD code with  $m \geq n$ , the  $i$ -th RGRW  $M_{R,i}(C_1, C_2)$  always coincides with the maximum possible value of  $M_{R,i}(C_1, \{0\})$ , shown in Corollary 15, regardless of its subcode  $C_2$ .

**Corollary 16.** Let  $m \geq n$ . Let  $C_1 \subseteq \mathbb{F}_{q^m}^n$  be an MRD code and  $C_2 \subseteq C_1$  be its arbitrary subcode. Then, the RGRW of  $C_1$  and  $C_2$  is  $M_{R,i}(C_1, C_2) = n - \dim C_1 + i$  for  $1 \leq i \leq \dim(C_1/C_2)$ .

*Proof:* By the definition of the RGRW in Definition 5, we first have  $M_{R,i}(C_1, C_2) \geq M_{R,i}(C_1, \{0\})$ . Hence, since  $C_1$  is MRD with  $m \geq n$ , we have  $M_{R,i}(C_1, C_2) \geq M_{R,i}(C_1, \{0\}) = n - \dim C_1 + i$  from Corollary 15. On the other hand, we have  $M_{R,i}(C_1, C_2) \leq n - \dim C_1 + i$  from Proposition 10. Therefore, we have  $M_{R,i}(C_1, C_2) = n - \dim C_1 + i$ . ■

By combining Proposition 14 and Proposition 10, we also have the following proposition only for the first RGRW. This proposition presents an upper bound of the first RGRW, obtained by the Singleton-type bound of the rank distance of  $C \subseteq \mathbb{F}_{q^m}^n$  for  $m < n$  in Proposition 14.

**Proposition 17.** The first RGRW of a linear code  $C_1 \subseteq \mathbb{F}_{q^m}^n$  and its subcode  $C_2 \subseteq C_1$  is upper bounded by

$$\begin{aligned} M_{R,1}(C_1, C_2) &\leq \min \left\{ n - \dim C_1, (m - 1) \dim C_1 / C_2, \frac{m(n - \dim C_1)}{n - \dim C_2} \right\} + 1. \end{aligned}$$

*Proof:* As in the proof of Proposition 10, let  $\mathcal{S} \subseteq \mathbb{F}_{q^m}^n$  be a linear code such that  $C_1 = C_2 + \mathcal{S}$ . Also, we suppose that the first  $\dim C_2$  coordinates of  $\mathcal{S}$  are zero without loss of generality. Since  $\mathcal{S}$  can be viewed as a code of length  $n - \dim C_2$ , we have the following inequality from Proposition 14.

$$\begin{aligned} d_R(\mathcal{S}) &= M_{R,1}(\mathcal{S}, \{0\}) \\ &\leq \frac{m}{n - \dim C_2} \{ (n - \dim C_2) - \dim \mathcal{S} \} + 1 \\ &= \frac{m(n - \dim C_1)}{n - \dim C_2} + 1. \end{aligned}$$

Thus, from (5),

$$M_{R,1}(C_1, C_2) \leq M_{R,1}(\mathcal{S}, \{0\}) \leq \frac{m(n - \dim C_1)}{n - \dim C_2} + 1.$$

Therefore, from Proposition 10, the proposition is proved. ■

The following corollary is immediately obtained from Proposition 17.

**Corollary 18.** Assume  $m \geq 2$ . For a linear code  $C \subseteq \mathbb{F}_{q^m}^n$ , we have the following inequalities.

$$\begin{aligned} d_R(C) &= M_{R,1}(C, \{0\}) \\ &\leq \begin{cases} n - \dim C + 1 & (n \leq m) \\ (m - 1) \dim C + 1 & (n > m, \dim C = 1) \\ \frac{m}{n} (n - \dim C) + 1 & (n > m, \dim C \geq 2). \end{cases} \end{aligned}$$

■

This corollary presents a tighter upper bound of  $d_R(C)$  for  $C \subseteq \mathbb{F}_{q^m}^n$  than that shown in Proposition 14, when  $m < n$  and  $\dim C = 1$ .

Lastly, by using the relation between the RGRW and the rank distance [15] presented above, we introduce an extra property of the RDIP  $K_{R,i}(C_1, C_2)$  when  $C_1$  is MRD. We define  $[x]^+ = \max\{0, x\}$ .

**Proposition 19.** Let  $C_1 \subseteq \mathbb{F}_{q^m}^n$  be a linear code and  $C_2 \subsetneq C_1$  be a its subcode. Assume  $m \geq n$  and  $C_1$  be an MRD code. Then, the RDIP of  $C_1$  and  $C_2$  is given by  $K_{R,\mu}(C_1, C_2) = [\mu - n + \dim C_1]^+$  for  $0 \leq \mu \leq n - \dim C_2$ .

*Proof:* From Corollary 16, we have  $M_{R,i}(C_1, C_2) = n - \dim C_1 + i$  for  $0 \leq i \leq \dim(C_1/C_2)$ . Thus, from Proposition 9 for  $i = 1$ , we have

$$\min\{\mu : K_{R,\mu}(C_1, C_2) = 1\} = n - \dim C_1 + 1,$$

and hence  $K_{R,\mu}(C_1, C_2) = 0$  for  $0 \leq \mu \leq n - \dim C_1$  from Theorem 8. On the other hand, from Proposition 9 for  $i = \dim(C_1/C_2)$ , we have

$$\begin{aligned} \min\{\mu : K_{R,\mu}(C_1, C_2) = \dim(C_1/C_2)\} \\ &= n - \dim C_1 + \underbrace{\dim(C_1/C_2)}_{=\dim C_1 - \dim C_2} \\ &= n - \dim C_2, \end{aligned}$$

and hence  $K_{R,n-\dim C_2}(C_1, C_2) = \dim(C_1/C_2)$ . Thus, since

$$\begin{aligned} K_{R,n-\dim C_2}(C_1, C_2) - K_{R,n-\dim C_1}(C_1, C_2) &= \dim(C_1/C_2) \\ &= \dim C_1 - \dim C_2, \end{aligned}$$

holds,  $K_{R,\mu}(C_1, C_2) = \mu - n + \dim C_1$  for  $n - \dim C_1 \leq \mu \leq n - \dim C_2$  must hold from Theorem 8. Therefore, the proposition is established. ■

### III. UNIVERSAL SECURITY PERFORMANCE OF SECURE NETWORK CODING

This section derives the security performance of secure network coding based on the *nested coset coding scheme* [44], which is guaranteed independently of the underlying network code construction.

This section first presents the network model with errors, and introduces the wiretap network model and the nested coset coding scheme in secure network coding. Next, we define the universal equivocation, the universal  $\omega$ -strong security and the universal maximum strength as the universal security performance of secure network coding on the wiretap network model. We then give the main contribution of this paper: we exactly express the universal security performance of secure network coding based on the nested coset coding scheme in terms of the RDIP and the RGRW.

#### A. Network Model with Errors

We first introduce the basic network model in which no errors occur in the network. As in [6], [11], [29], [37], [46], we consider a multicast communication network represented by a directed acyclic multigraph with unit capacity links, a

single source node, and multiple sink nodes. We assume that *linear network coding* [19], [23] is employed over the network. Elements of a column vector space  $\mathbb{F}_q^{m \times 1}$  are called *packets*. Assume that each link in the network can carry a single  $\mathbb{F}_q$ -symbol per one time slot, and that each link transports a single packet over  $m$  time slots without delays, erasures, or errors.

The source node produces  $n$  packets  $X_1, \dots, X_n \in \mathbb{F}_q^{m \times 1}$  and transmits  $X_1, \dots, X_n$  on  $n$  outgoing links over  $m$  consecutive time slots. Define the  $m \times n$  matrix  $X = [X_1, \dots, X_n]$ . The data flow on any link can be represented as an  $\mathbb{F}_q$ -linear combination of packets  $X_1, \dots, X_n \in \mathbb{F}_q^{m \times 1}$ . Namely, the information transmitted on a link  $e$  can be denoted as  $b_e X^T \in \mathbb{F}_q^{1 \times m}$ , where  $b_e \in \mathbb{F}_q^n$  is called a *global coding vector* [14, Ch. 2, p. 18] of  $e$ . Suppose that a sink node has  $N$  incoming links. Then, the information received at a sink node can be represented as an  $N \times m$  matrix  $AX^T \in \mathbb{F}_q^{N \times m}$ , where  $A \in \mathbb{F}_q^{N \times n}$  is the transfer matrix of the network constructed by gathering the global coding vectors of  $N$  incoming links. The network code is called *feasible* if each transfer matrix to each sink node has rank  $n$  over  $\mathbb{F}_q$ , otherwise it is called rank deficient. The *rank deficiency* of the network coded network [35], [37], [38] is defined by

$$\rho \triangleq n - \min\{\text{rank } A : A \text{ at each sink node}\},$$

i.e., the maximum column-rank deficiency of the transfer matrix  $A$  among all sink nodes. As in [35], [37], [38],  $\rho$  is also referred to as  $\rho$  *erasures*.

The above setup of the network coded network is referred to as an  $(n \times m)_q$  *linear network* [37]. We may also call it a  $\rho$ -*erasure*  $(n \times m)_q$  *linear network* when we need to indicate the rank deficiency  $\rho$  of the network.

Now we extend the basic model of the  $(n \times m)_q$  linear network defined above to incorporate packet errors, as [35], [37]. We define the network model with errors as follows.

**Definition 20** ( $t$ -Error  $(n \times m)_q$  Linear Network). Suppose that the network is an  $(n \times m)_q$  linear network. Also suppose that at most  $t$  error packets, represented by  $Z \in \mathbb{F}_q^{m \times t}$ , are injected from  $t$  links chosen arbitrarily in the network. That is, the information transported over a link  $e$  with the global coding vector  $b_e$  is represented by  $b_e X^T + f_e Z^T \in \mathbb{F}_q^{1 \times m}$ , where  $f_e \in \mathbb{F}_q^{1 \times t}$  corresponds to the overall linear transformation applied to the injected error packets  $Z$  on the route to the link  $e$ . Then, the network is called a  $t$ -*error*  $(n \times m)_q$  *linear network*.

This  $t$ -error  $(n \times m)_q$  linear network may also be called a  $t$ -*error*- $\rho$ -*erasure*  $(n \times m)_q$  *linear network* for the rank deficiency  $\rho$ . Note that in the  $t$ -error  $(n \times m)_q$  linear network, the information received at a sink node is expressed as

$$Y^T = AX^T + DZ^T \in \mathbb{F}_q^{N \times m}, \quad (7)$$

where  $D \in \mathbb{F}_q^{N \times t}$  is constructed by gathering  $f_e$ 's of incoming links  $e$ 's to the sink node, and hence  $D$  corresponds to the overall linear transformation applied to  $Z$  on the route to the sink node.

The system of linear network coding is called *coherent* if the transfer matrix  $A$  is known to each sink node, otherwise it is called *noncoherent*.



### B. Wiretap Network Model and Nested Coset Coding Scheme

Following [37], [46], assume that in the  $t$ -error  $(n \times m)_q$  linear network defined in Definition 20, there is an adversary who observes packets transmitted on any  $\mu$  links. We also assume that the adversary knows the coding scheme applied at the source node and all the global coding vectors in the network.

Let  $\mathcal{W}$  be the set of  $\mu$  links observed by the adversary, and let  $B_{\mathcal{W}} \in \mathbb{F}_q^{\mu \times n}$  be the transfer matrix whose rows are the global coding vectors  $b_e$ 's associated with the links  $e$ 's in  $\mathcal{W}$ . The information obtained by the adversary can be expressed by

$$W^T = B_{\mathcal{W}}X^T + F_{\mathcal{W}}Z^T \in \mathbb{F}_q^{\mu \times m}, \quad (8)$$

where  $F_{\mathcal{W}} \in \mathbb{F}_q^{\mu \times t}$  is constructed by gathering  $f_e$ 's of links  $e$ 's in  $\mathcal{W}$ , and  $F_{\mathcal{W}}Z^T \in \mathbb{F}_q^{\mu \times m}$  corresponds to the errors. In the following, we consider the reliable transmission of a secret message through this wiretap network model.

The procedure of the secure message transmission over the wiretap network model is called *secure network coding* [6], [11], [29], [37], [46]. In the scenario of secure network coding, first regard an  $m$ -dimensional column vector space  $\mathbb{F}_q^{m \times 1}$  as  $\mathbb{F}_q^m$ , and fix  $l$  for  $1 \leq l \leq n$ . Let  $S = [S_1, \dots, S_l] \in \mathbb{F}_q^{l \times m}$  be the secret message of  $l$  packets. Under the adversary's observation of  $\mu$  links, the source node wants to transmit  $S$  as small information leakage to the adversary as possible. To protect  $S$  from the adversary, the source node encodes  $S$  to the transmitted vector  $X = [X_1, \dots, X_n] \in \mathbb{F}_q^n$  of  $n$  packets according to some kind of coding scheme. Then, the source node finally transmits  $X$  as an  $m \times n$  matrix over  $\mathbb{F}_q$  to sink nodes through the network. In this paper, we assume that the source node knows nothing about the errors that occur in the network, as in the model of [37], [46].

In the secure network coding described in [11], [29], [37], [46],  $S$  is encoded by the *nested coset coding scheme* [7], [10], [41], [44] at the source node. In secure network coding based on the nested coset coding scheme,  $S$  is encoded to  $X$  at the source node as follows.

**Definition 21** (Nested Coset Coding Scheme). Let  $C_1 \subseteq \mathbb{F}_q^n$  be a linear code over  $\mathbb{F}_q$  ( $m \geq 1$ ), and  $C_2 \subsetneq C_1$  be its subcode with dimension  $\dim C_2 = \dim C_1 - l$  over  $\mathbb{F}_q$ . Let  $\psi : \mathbb{F}_q^l \rightarrow C_1/C_2$  be an arbitrary linear bijection. For a secret message  $S \in \mathbb{F}_q^l$ , we randomly choose  $X$  from a coset  $\psi(S) \in C_1/C_2$ . We make no assumption on the joint distribution  $P_{S,X}$  unless otherwise stated.

In [7], [10], [20], the nested coset coding scheme is called a *secret sharing scheme based on linear codes*. Definition 21 includes the Ozarow-Wyner coset coding scheme [32] as a special case with  $C_1 = \mathbb{F}_q^n$ .

Corresponding to  $X$  transmitted from the source node, the sink node receives a vector of  $N$  packets  $Y \in \mathbb{F}_q^N$ . The decoding of  $S$  from  $Y$  will be discussed in Section IV.

### C. Definition of the Universal Security Performance

In order to measure the security performance of secure network coding in the above model, this subsection presents

two criteria. The security performance measured by our criteria is guaranteed independently of the underlying network code, hence we call them *universal*.

Let  $H(X)$  be the Shannon entropy for 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  $Y$  [8, Ch. 2, pp. 12–19]. The entropy and the mutual information are always computed using  $\log_{q^m}$ .

1) *Universal Equivocation*: First, we define *universal equivocation* as follows.

**Definition 22** (Universal Equivocation). Assume that the secret message  $S$  is chosen according to an arbitrary distribution  $P_S$  over  $\mathbb{F}_q^l$ , and suppose that  $S$  is encoded to the transmitted packets  $X \in \mathbb{F}_q^n$  by a certain coding scheme. We make no assumption on the joint distribution  $P_{S,X}$ . Then, the *universal equivocation*  $\Theta_{\mu, P_{S,X}}$  of the coding scheme is the minimum uncertainty of  $S$  given  $BX^T$  for all  $B \in \mathbb{F}_q^{\mu \times n}$ , defined as

$$\begin{aligned} \Theta_{\mu, P_{S,X}} &\triangleq \min_{B \in \mathbb{F}_q^{\mu \times n}} H(S|BX^T) \\ &= H(S) - \max_{B \in \mathbb{F}_q^{\mu \times n}} I(S; BX^T). \end{aligned}$$

We will also call  $\max_{B \in \mathbb{F}_q^{\mu \times n}} I(S; BX^T)$  in the above equation the *maximum amount of information leakage* to the adversary.

Note that the conditional entropy of  $S$  given  $BX^T$  is considered in Definition 22. But, we need to consider the adversary in the  $t$ -error  $(n \times m)_q$  linear network as the model presented in Section III-B, i.e., we need to consider the conditional entropy of  $S$  given  $W$  that contains the errors, as given in (8). In order to justify this difference between Definition 22 and the wiretap network model, we derive the following proposition.

**Proposition 23.** Fix a matrix  $B \in \mathbb{F}_q^{\mu \times n}$  arbitrarily. Let  $S \in \mathbb{F}_q^l$  be chosen according to an arbitrary distribution, and let  $X \in \mathbb{F}_q^n$  be chosen according to an arbitrary distribution such that  $S$  is uniquely determined from  $X$  by some surjection. Suppose that  $E \in \mathbb{F}_q^{\mu}$  is chosen according to an arbitrary distribution. Then, for  $W^T = BX^T + E^T$ ,  $H(S|W) \geq H(S|BX^T)$  always holds.

*Proof:* Observe that  $S \leftrightarrow BX^T \leftrightarrow W$  forms a Markov chain. By the data processing inequality [8, Ch. 2, pp. 32–33], we have  $I(S; BX^T) \geq I(S; W)$ , which implies  $H(S|W) \geq H(S|BX)$ . ■

The statement equivalent to Proposition 23 was given in [46, Theorem 4.1]. This proposition shows that for  $\mu$  tapped links, the uncertainty of at least  $\Theta_{\mu, P_{S,X}}$  defined by Definition 22 is always guaranteed even if errors occur in the network. In other words, from Proposition 23, we can see that Definition 22 considers the most advantageous case for the adversary in the wiretap network model given in Section III-B, as with the model considered in [37], [46].

As the security measure for secure network coding, the maximum uncertainty of  $S$  given  $B_{\mathcal{W}}X^T$  for all possible  $\mathcal{W}$ 's of tapped links was considered in [6], [11], [29], [46], where  $m = 1$ . However, the security measure in [6], [11], [29], [46] is dependent on the underlying network coded network,

i.e., it is not *universal*. On the other hand, as defined in Definition 22,  $\Theta_{\mu, P_{S,X}}$  does not depend on the set of possible  $\mathcal{W}$ 's of tapped links in the network. Thus,  $\Theta_{\mu, P_{S,X}}$  is guaranteed on any underlying network code, and hence it is *universal*.

Silva and Kschischang proposed a scheme based on the nested coset coding scheme with MRD codes  $C_1, C_2$  [37] with which no information of  $S$  is obtained from any  $\dim C_1 - l = \dim C_2$  links for any distribution of  $S$  when the conditional distribution of  $X$  given  $S$  is uniform over  $\psi(S)$ , provided  $m \geq n$ . That is, their scheme guarantees the universal equivocation  $\Theta_{\dim C_1 - l, P_{S,X}} = H(S)$  for any distribution of  $S$ .

2) *Universal  $\omega$ -Strong Security and Universal Maximum Strength*: Definition 22 defines the universal equivocation  $\Theta_{\mu, P_{S,X}}$  as the security measure for all the components of a secret message  $S = [S_1, \dots, S_l]$ . Consider the case where  $\Theta_{\mu, P_{S,X}} < H(S)$ , i.e., some information of the secret message leaks to the adversary. Then, some components of  $S_1, \dots, S_l$  could be uniquely determined by the adversary. It is clearly desirable that no component of  $S_1, \dots, S_l$  is deterministically revealed and that every symbol  $S_i$  is kept hidden, even if some information of  $S$  leaks to the adversary. Hence, we can say that the number of tapped links such that every symbol  $S_i$  is kept hidden represents the resiliency or strength of the coding scheme against eavesdropping. Now we focus on such security and give the following definition as the resiliency of the coding scheme against eavesdropping.

**Definition 24** (Universal  $\omega$ -Strong Security and Universal Maximum Strength). Let  $S_Z = (S_i : i \in Z)$  be a tuple whose indices belong to a subset  $Z \subseteq \{1, \dots, l\}$ . We say that the coding scheme attains *universal  $\omega$ -strong security* if we have

$$I(S_Z; BX^T) = 0, \quad \forall Z, \forall B \in \mathbb{F}_q^{(\omega - |Z| + 1) \times n}, \quad (9)$$

for uniformly distributed  $S$  and conditionally uniformly distributed  $X$  given  $S$ . The maximum possible value of  $\omega$  in the scheme is called *universal maximum strength*  $\Omega$  of the coding scheme, defined by

$$\Omega \triangleq \max \left\{ \omega : I(S_Z; BX^T) = 0, \right. \\ \left. \forall Z \subseteq \{1, \dots, l\}, \forall B \in \mathbb{F}_q^{(\omega - |Z| + 1) \times n} \right\}. \quad (10)$$

The universal strong security defined in [36] is a special case of Definition 24 for  $\Omega = n - 1$  and  $C_1 = \mathbb{F}_{q^m}^n$ . Unlike the definition of  $\Theta_{\mu, P_{S,X}}$  in Definition 22, we have considered the case where the secret message  $S$  is uniformly distributed and the transmitted packets  $X$  are conditionally uniformly distributed given  $S$ . This is because the value of  $I(S_Z; BX^T)$  is dependent on the conditional distribution of  $X$  given  $S_Z$ , while  $\Theta_{\mu, P_{S,X}}$  does not have such dependence. Without assuming a joint probability distribution on  $S$  and  $X$ , we cannot have a meaningful sufficient condition for  $I(S_Z; BX^T) = 0$  in (10).

In Definition 24, the mutual information between a part of  $S$  and  $BX^T$  is considered, and the errors  $Z$  contained in the eavesdropped information are not considered. This is based on the same reason that errors are not considered in Definition 22. That is, from Proposition 23, the universal  $\Omega$ -strong security is always guaranteed even if errors occur in the network.

As in [17], [27], [36], a scheme with universal  $\omega$ -strong security does not leak any  $|Z|$  components of  $S$  even if at most

$\omega - |Z| + 1$  links are observed by the adversary, provided that  $P_{S,X}$  satisfies the assumption in Definition 24. Moreover, this guarantee holds over any underlying network code as  $\Theta_{\mu, P_{S,X}}$ . Hence,  $\omega$  and  $\Omega$  are also *universal*. In Corollary 30, we will present an upper bound of  $I(S_Z; BX^T)$  with arbitrary  $P_{S,X}$  in terms of  $\Omega$ .

#### D. Expression of the Universal Security Performance in Terms of the RDIP and RGRW

In this subsection, we express  $\Theta_{\mu, P_{S,X}}$  and  $\Omega$  given in Section III-C in terms of the RDIP and RGRW.

We first give a lemma for the mutual information between the message and information observed by the adversary. From now on, for a matrix  $M \in \mathbb{F}_{q^m}^{\mu \times n}$ , we represent a row space of  $M$  over  $\mathbb{F}_{q^m}$  by  $\text{row}(M) \triangleq \{uM : u \in \mathbb{F}_{q^m}^\mu\} \subseteq \mathbb{F}_{q^m}^n$ . For a set  $\mathcal{A}$ , denote by  $U_{\mathcal{A}}$  the random variable uniform on  $\mathcal{A}$ . For a random variable  $V$  and a set  $\mathcal{A}(V)$  depending on  $V$ , denote by  $U_{\mathcal{A}(V)}$  the random variable conditionally uniform on  $\mathcal{A}(V)$  given  $V$ . For three random variables  $A, B, C$ , denote by  $D(A||B)$  the relative entropy [8, Ch. 2, p. 18] between probability distributions  $P_A$  and  $P_B$ . Also we denote by  $D(A||B|C)$  the conditional relative entropy [8, Ch. 2, p. 22] between two conditional probability distributions  $P_{A|C}$  and  $P_{B|C}$  given  $C$ .

**Lemma 25.** Let  $C_1 \subseteq \mathbb{F}_{q^m}^n$  be a linear code and  $C_2 \subsetneq C_1$  be its subcode with  $\dim C_2 = \dim C_1 - l$ . Assume that a random variable  $S \in \mathbb{F}_{q^m}^l$  is chosen according to an arbitrary distribution over  $\mathbb{F}_{q^m}^l$ . For a bijective function  $\psi : \mathbb{F}_{q^m}^l \rightarrow C_1/C_2$  and given  $S$ , let  $X \in \mathbb{F}_{q^m}^n$  be a random variable arbitrarily distributed over a coset  $\psi(S) \in C_1/C_2$ . Fix a matrix  $B \in \mathbb{F}_{q^m}^{\mu \times n}$  over  $\mathbb{F}_{q^m}$  arbitrarily, and let  $W^T = BX^T \in \mathbb{F}_{q^m}^{\mu \times 1}$ . Then, we have the following three statements.

- 1) For any distributions of  $S$  and  $X$ , we have

$$I(S; W) \leq \dim(C_2^\perp \cap \text{row}(B)) - \dim(C_1^\perp \cap \text{row}(B)) \\ + D(X||U_{\psi(S)}|S), \quad (11)$$

and

$$I(S; W) \geq \dim(C_2^\perp \cap \text{row}(B)) - \dim(C_1^\perp \cap \text{row}(B)) \\ - D(S||U_{\mathbb{F}_{q^m}^l}). \quad (12)$$

- 2) If both  $S$  and  $X$  are uniformly distributed over  $\mathbb{F}_{q^m}^l$  and  $C_1$  respectively, the equalities in (11) and (12) hold, i.e.,  $I(S; W) = \dim(C_2^\perp \cap \text{row}(B)) - \dim(C_1^\perp \cap \text{row}(B))$ .
- 3) If  $I(S; W) = 0$  holds for a distribution of  $S$  that assigns a positive probability to every element in  $\mathbb{F}_{q^m}^l$ , then we have  $\dim(C_2^\perp \cap \text{row}(B)) - \dim(C_1^\perp \cap \text{row}(B)) = 0$ .

*Proof:* See Appendix A. ■

Note that the matrix  $B$  in Lemma 25 is defined over the field extension  $\mathbb{F}_{q^m}$ , while the transfer matrix  $B$  to the wiretapper is restricted to the subfield  $\mathbb{F}_q$  in the wiretap network model defined in Section III-B.

Cai and Yeung [3], [5], [6] considered the security condition of secure network coding such that the adversary obtains no information about the secret message when  $S$  and  $X$  are chosen according to distributions that assign positive probabilities

to all the secret messages and the transmitted packets [4, Lemma 3.1]. Their security condition corresponds to the statement 3) in Lemma 25 and the fact that  $I(S; W) = 0$  when  $\dim(C_2^\perp \cap \text{row}(B)) = \dim(C_1^\perp \cap \text{row}(B))$  holds and  $X$  is conditionally uniform over  $\psi(S)$  given  $S$  from (11). Note that in the statement 3) in Lemma 25, we made no assumption on the distribution of  $X$ , unlike [4, Lemma 3.1]. For an arbitrary joint distribution of  $S$  and  $X$ , Zhang and Yeung [45] generalized the security condition of [3], [5], [6] that corresponds to the statement 3) in Lemma 25. We should note that in the statement 3) in Lemma 25, we assumed the distribution of  $S$  that assigns a positive probability to every message, in order to express the condition in terms of the dimensions of subspaces. The proof of Lemma 25 (See Appendix A) can be adapted to the case of arbitrarily distributed  $S$ , and we can easily show that if  $I(S; W) = 0$  for  $P_S$ , we have  $I(S'; W') = 0$  for any  $P_{S'}$  satisfying  $\{s : P_{S'}(s) > 0\} \subseteq \{s : P_S(s) > 0\}$ . Further, unlike [3], [5], [6], [45], Lemma 25 additionally derived the upper and lower bounds of the mutual information leaked to the adversary by using the relative entropy for arbitrarily distributed  $S$  and  $X$ . In the following, we shall derive the security performance expressed in terms of the RDIP and the RGRW by using Lemma 25, which is guaranteed independently of the underlying network coded network.

Here we recall that if an  $\mathbb{F}_{q^m}$ -linear space  $V \subseteq \mathbb{F}_{q^m}^n$  admits a basis in  $\mathbb{F}_q^n$ , then  $V \in \Gamma(\mathbb{F}_{q^m}^n)$  by Lemma 1. Since the transfer matrix  $B$  is defined over the base field  $\mathbb{F}_q$  in Section III-B, this implies

$$\text{row}(B) \in \Gamma(\mathbb{F}_{q^m}^n). \quad (13)$$

We give the following theorem for the maximum amount of information leakage to the adversary, defined in Definition 22.

**Theorem 26.** Consider the nested coset coding scheme with  $C_1, C_2$  and  $\psi$  in Definition 21. Then, the maximum amount of information leakage to the adversary, defined in Definition 22, is in the range of

$$\begin{aligned} & K_{R,\mu}(C_2^\perp, C_1^\perp) - D(S \| U_{\mathbb{F}_q^l}) \\ & \leq \max_{B \in \mathbb{F}_q^{\mu \times n}} I(S; BX^T) \\ & \leq K_{R,\mu}(C_2^\perp, C_1^\perp) + D(X \| U_{\psi(S)} | S). \end{aligned} \quad (14)$$

If both the secret message  $S$  and the transmitted packets  $X$  are uniformly distributed over  $\mathbb{F}_{q^m}^l$  and  $C_1$  respectively, the maximum amount of information leakage exactly equals  $\max_{B \in \mathbb{F}_q^{\mu \times n}} I(S; BX^T) = K_{R,\mu}(C_2^\perp, C_1^\perp)$ . If the maximum amount of information leakage is exactly zero for a distribution of  $S$  that assigns a positive probability to every element in  $\mathbb{F}_{q^m}^l$ , we have  $K_{R,\mu}(C_2^\perp, C_1^\perp) = 0$ , which corresponds to [4, Lemma 3.1].

*Proof:* By Lemma 1 and (13), we have

$$\{\text{row}(B) : B \in \mathbb{F}_q^{\mu \times n}\} = \bigcup_{i \leq \mu} \Gamma_i(\mathbb{F}_{q^m}^n). \quad (15)$$

From Lemma 25, we have

$$\begin{aligned} \max_{B \in \mathbb{F}_q^{\mu \times n}} I(S; BX^T) & \leq \max_{B \in \mathbb{F}_q^{\mu \times n}} \{\dim(C_2^\perp \cap \text{row}(B)) - \dim(C_1^\perp \cap \text{row}(B))\} \\ & \quad + D(X \| U_{\psi(S)} | S), \end{aligned} \quad (16)$$

and

$$\begin{aligned} \max_{B \in \mathbb{F}_q^{\mu \times n}} I(S; BX^T) & \geq \max_{B \in \mathbb{F}_q^{\mu \times n}} \{\dim(C_2^\perp \cap \text{row}(B)) - \dim(C_1^\perp \cap \text{row}(B))\} \\ & \quad - D(S \| U_{\mathbb{F}_q^l}). \end{aligned} \quad (17)$$

For the first terms on the right-hand side of (16) and (17), we have

$$\begin{aligned} & \max_{B \in \mathbb{F}_q^{\mu \times n}} \{\dim(C_2^\perp \cap \text{row}(B)) - \dim(C_1^\perp \cap \text{row}(B))\} \\ & = \max_{V \in \bigcup_{i \leq \mu} \Gamma_i(\mathbb{F}_{q^m}^n)} \{\dim(C_2^\perp \cap V) - \dim(C_1^\perp \cap V)\} \quad (\text{by (15)}) \\ & = \max \{K_{R,i}(C_2^\perp, C_1^\perp) : i \leq \mu\} \quad (\text{by Definition 4}) \\ & = K_{R,\mu}(C_2^\perp, C_1^\perp). \quad (\text{by Theorem 8}) \end{aligned} \quad (18)$$

Therefore, we have (14).

If  $S$  and  $X$  are uniform over  $\mathbb{F}_{q^m}^l$  and  $C_1$  respectively, we have  $I(S; BX^T) = \dim(C_2^\perp \cap \text{row}(B)) - \dim(C_1^\perp \cap \text{row}(B))$  from Lemma 25. Therefore, for the uniformly distributed  $S$  and  $X$ , we have  $\max_{B \in \mathbb{F}_q^{\mu \times n}} I(S; BX^T) = K_{R,\mu}(C_2^\perp, C_1^\perp)$  by (18).

Finally, we prove the last statement. Assume that  $\max_{B \in \mathbb{F}_q^{\mu \times n}} I(S; BX^T) = 0$  holds for a distribution of  $S$  that assigns a positive probability to every element in  $\mathbb{F}_{q^m}^l$ . Then, we have  $\dim(C_2^\perp \cap \text{row}(B)) - \dim(C_1^\perp \cap \text{row}(B)) = 0$  simultaneously for all  $B \in \mathbb{F}_q^{\mu \times n}$  from Lemma 25. Therefore, we have  $K_{R,\mu}(C_2^\perp, C_1^\perp) = 0$ . ■

This theorem includes the condition such that the maximum amount of information leakage is exactly zero. This corresponds to the security condition of secure network coding given in [3]–[6], for all possible sets of tapped links, as Lemma 25 for one set of possible tapped links. We note that while our condition is independent of the underlying network code, i.e., universal, their security condition is dependent on the underlying network code. Further, as Lemma 25, we should note that the distribution of  $X$  is arbitrary in the last statement in Theorem 26.

Theorem 26 immediately yields the following proposition for the universal equivocation.

**Proposition 27.** Consider the nested coset coding scheme with  $C_1, C_2$  and  $\psi$  in Definition 21. Then, the universal equivocation  $\Theta_{\mu, P_{S,X}}$ , defined in Definition 22, is in the range of

$$\begin{aligned} & H(S) - D(X \| U_{\psi(S)} | S) - K_{R,\mu}(C_2^\perp, C_1^\perp) \\ & \leq \Theta_{\mu, P_{S,X}} \\ & \leq l - K_{R,\mu}(C_2^\perp, C_1^\perp). \end{aligned}$$

When both the secret message  $S$  and the transmitted packets  $X$  are uniformly distributed over  $\mathbb{F}_{q^m}^l$  and  $C_1$  respectively, we have  $\Theta_{\mu, P_{S,X}} = l - K_{R,\mu}(C_2^\perp, C_1^\perp)$ . ■

Also from Theorem 26, we obtain the following corollary.

**Corollary 28.** Consider the transmission of  $X \in \mathbb{F}_{q^m}^n$  over the wiretap network, which is generated from the secret message  $S$  by the nested coset coding scheme with  $C_1, C_2$  and  $\psi$ , defined in Definition 21. Then, we have the following four statements for an arbitrarily fixed  $j \in \{1, \dots, l\}$ .

- 1) If the adversary observes  $\mu < M_{R,j}(C_2^\perp, C_1^\perp)$  links, the maximum amount of information leakage in Definition 22 is at most  $j - 1 + D(X||U_{\psi(S)}|S)$  between  $S$  and observed packets;
- 2) If the adversary observes  $\mu \geq M_{R,j}(C_2^\perp, C_1^\perp)$  links, the maximum amount of information leakage is at least  $j - D(S||U_{\mathbb{F}_{q^m}^l})$  between  $S$  and observed packets.
- 3) If the adversary observes  $\mu = M_{R,j}(C_2^\perp, C_1^\perp)$  links, there exist  $P_{S,X}$  and  $B$  by which the adversary obtains the mutual information  $j$  between  $S$  and the observed packets  $BX^T$ ; and
- 4) If the maximum amount of information leakage is exactly zero for a distribution of  $S$  that assigns a positive probability to every element in  $\mathbb{F}_{q^m}^l$ , the number of tapped links is  $\mu < M_{R,1}(C_2^\perp, C_1^\perp)$ , which again corresponds to [4, Lemma 3.1].

*Proof:* Since we have

$$\min\{\mu : K_{R,\mu}(C_2^\perp, C_1^\perp) = j\} = M_{R,j}(C_2^\perp, C_1^\perp),$$

from Lemma 9, we obtain  $K_{R,\mu}(C_2^\perp, C_1^\perp) = j$  and  $K_{R,\mu-1}(C_2^\perp, C_1^\perp) = j - 1$  for  $\mu = M_{R,j}(C_2^\perp, C_1^\perp)$ . This implies that from Theorem 26, the maximum amount of information leakage is at most  $j - 1 + D(X||U_{\psi(S)}|S)$  from less than  $M_{R,j}(C_2^\perp, C_1^\perp)$  links. Also, the maximum amount of information leakage is at least  $j - D(S||U_{\mathbb{F}_{q^m}^l})$  from  $M_{R,j}(C_2^\perp, C_1^\perp)$  or more links. Also note that when  $S$  and  $X$  are uniformly distributed, the maximum information leakage for  $\mu$  is exactly equal to  $K_{R,\mu}(C_2^\perp, C_1^\perp)$  by Theorem 26, and recall again that  $\min\{\mu : K_{R,\mu}(C_2^\perp, C_1^\perp) = j\} = M_{R,j}(C_2^\perp, C_1^\perp)$ . Thus, statements 1)–3) are proved.

When  $\max_{B \in \mathbb{F}_q^{\mu \times n}} I(S; BX^T) = 0$  holds for a distribution of  $S$  that assigns a positive probability to every element in  $\mathbb{F}_{q^m}^l$ , we have  $K_{R,\mu}(C_2^\perp, C_1^\perp) = 0$  from Theorem 26, and  $M_{R,1}(C_2^\perp, C_1^\perp) = \min\{\mu : K_{R,\mu}(C_2^\perp, C_1^\perp) = 1\}$  holds from Lemma 9. Therefore, statement 4) is proved. ■

Statement 1) in Corollary 28 shows that if the transmitted packets  $X$  are chosen uniformly at random from a coset  $\psi(S)$  given  $S$ , the adversary obtains no information of the message  $S$  from any  $M_{R,1}(C_2^\perp, C_1^\perp) - 1$  links, independently of the distribution of  $S$ . In contrast, if  $X$  is not uniform and  $D(X||U_{\psi(S)}|S) > 0$ , the information of  $S$  leaks out from less than  $M_{R,1}(C_2^\perp, C_1^\perp)$  links.

In [31, Proposition 2], Oggier and Sbouy introduced a special case of Corollary 28 for  $j = 1$ ,  $C_1 = \mathbb{F}_{q^m}^n$  and uniformly distributed  $X \in C_1$ , in terms of the minimum rank distance. Namely, they showed that the adversary obtains no information of  $S$  from any  $d_R(C_2^\perp) - 1 = M_{R,1}(C_2^\perp, \{0\}) - 1$  links.

Ngai et al. [29] and Zhang et al. [46] analyzed the lower bound of the uncertainty of the secret message by the (R-)Network-GHW in the case where the transmitted packets  $X$  are uniformly distributed over  $\psi(S)$ . Proposition 27 and Corollary 28 correspond to their results using (R-)Network-GHW. We should note that unlike [29], [46], we considered the case where both  $S$  and  $X$  are arbitrarily distributed, and derived both upper and lower bounds. Further, while our analyses using the RDIP and the RGRW are universal, the analyses

using (R-)Network-GHW in [29], [46] are dependent on the underlying network code.

Lastly, we express  $\Omega$  in Definition 24 in terms of the RGRW. In order to derive  $\Omega$ , we first introduce the following proposition that reveals the mutual information between a part of the message  $S$  and observed packets of the adversary in the case where  $S$  and the transmitted packets  $X$  are arbitrarily distributed.

**Proposition 29.** Consider the nested coset coding scheme and fix  $C_1, C_2$  and  $\psi$  in Definition 21. For a subset  $\mathcal{Z} \subseteq \{1, \dots, l\}$ , let  $S_{\mathcal{Z}} \triangleq (S_i : i \in \mathcal{Z})$ , and  $C_{3,\mathcal{Z}}$  be a subcode of  $C_1$  defined by

$$C_{3,\mathcal{Z}} \triangleq \bigcup_{\substack{S_{j=0:i \in \mathcal{Z}}, \\ S_{j \in \mathbb{F}_{q^m}^l : j \notin \mathcal{Z}}} \psi([S_1, \dots, S_l]). \quad (19)$$

Also, define a bijective function  $\psi_{\mathcal{Z}} : \mathbb{F}_{q^m}^{|\mathcal{Z}|} \rightarrow C_1/C_{3,\mathcal{Z}}$  by

$$\psi_{\mathcal{Z}}(S_{\mathcal{Z}}) \triangleq \bigcup_{S_{j \in \mathbb{F}_{q^m}^l : j \notin \mathcal{Z}}} \psi([S_1, \dots, S_l]). \quad (20)$$

Then, the maximum amount of the mutual information between  $S_{\mathcal{Z}}$  and  $BX^T$  is in the range of

$$\begin{aligned} & K_{R,\mu}(C_{3,\mathcal{Z}}^\perp, C_1^\perp) - D(S_{\mathcal{Z}}||U_{\mathbb{F}_{q^m}^{|\mathcal{Z}|}}) \\ & \leq \max_{B \in \mathbb{F}_q^{\mu \times n}} I(S_{\mathcal{Z}}; BX^T) \\ & \leq K_{R,\mu}(C_{3,\mathcal{Z}}^\perp, C_1^\perp) + D(X||U_{\psi_{\mathcal{Z}}(S_{\mathcal{Z}})}|S_{\mathcal{Z}}). \end{aligned} \quad (21)$$

If both  $S$  and  $X$  are uniformly distributed over  $\mathbb{F}_{q^m}^l$  and  $C_1$  respectively, it exactly equals  $\max_{B \in \mathbb{F}_q^{\mu \times n}} I(S_{\mathcal{Z}}; BX^T) = K_{R,\mu}(C_{3,\mathcal{Z}}^\perp, C_1^\perp)$ .

*Proof:* For a subset  $\mathcal{Z} \subseteq \{1, \dots, l\}$ ,  $C_{3,\mathcal{Z}}$  is an  $\mathbb{F}_{q^m}$ -linear subspace satisfying  $C_2 \subseteq C_{3,\mathcal{Z}} \subseteq C_1$  and  $\dim C_{3,\mathcal{Z}} = \dim C_1 - |\mathcal{Z}|$ . Observe that  $S_{\mathcal{Z}}$  is chosen from  $\mathbb{F}_{q^m}^{|\mathcal{Z}|}$  according to the distribution  $P_{S_{\mathcal{Z}}}$ , and that  $X$  can be regarded as a random variable chosen from a coset  $\psi_{\mathcal{Z}}(S_{\mathcal{Z}}) \in C_1/C_{3,\mathcal{Z}}$  according to the conditional distribution  $P_{X|S_{\mathcal{Z}}}$  given  $S_{\mathcal{Z}}$ . Also recall that  $\psi_{\mathcal{Z}}$  is bijective. Hence, the information leakage of  $S_{\mathcal{Z}}$  in the nested coset coding with  $C_1$  and  $C_2$  according to  $P_{S,X}$  is equal to the one in the nested coset coding scheme with  $C_1$  and  $C_{3,\mathcal{Z}}$  according to  $P_{S_{\mathcal{Z}},X}$ , where  $P_{S_{\mathcal{Z}},X}$  is the joint distribution of  $S_{\mathcal{Z}}$  and  $X$ . Thus, by Theorem 26, (21) holds. Assume that  $S$  and  $X$  are uniformly distributed over  $\mathbb{F}_{q^m}^l$  and  $C_1$ , respectively. Then,  $S_{\mathcal{Z}}$  is uniform over  $\mathbb{F}_{q^m}^{|\mathcal{Z}|}$ , and from the definition of  $\psi_{\mathcal{Z}}$  in (20),  $X$  is also uniform over  $\psi_{\mathcal{Z}}(S_{\mathcal{Z}})$  given  $S_{\mathcal{Z}}$ . Therefore, we have  $\max_{B \in \mathbb{F}_q^{\mu \times n}} I(S_{\mathcal{Z}}; BX^T) = K_{R,\mu}(C_{3,\mathcal{Z}}^\perp, C_1^\perp)$ . ■

From Proposition 29 and the definition of the universal maximum strength  $\Omega$  in Definition 24, we give the following upper bound of  $\max_{B \in \mathbb{F}_q^{\mu \times n}} I(S_{\mathcal{Z}}; BX^T)$  for arbitrarily distributed  $S$  and  $X$ , which is expressed in terms of  $\Omega$ .

**Corollary 30.** Consider the nested coset coding scheme defined in Definition 21 with the universal maximum strength  $\Omega$ . Then, for fixed  $\mu$  and  $\mathcal{Z} \subseteq \{1, \dots, l\}$ , we have

$$\max_{B \in \mathbb{F}_q^{\mu \times n}} I(S_{\mathcal{Z}}; BX^T) \leq [\mu - \Omega + |\mathcal{Z}| - 1]^+ + D(X||U_{\psi_{\mathcal{Z}}(S_{\mathcal{Z}})}|S_{\mathcal{Z}}),$$

where  $\psi_{\mathcal{Z}}(S_{\mathcal{Z}})$  is defined by (20).

*Proof:* When  $S$  and  $X$  are uniformly distributed, we have  $\max_{B \in \mathbb{F}_q^{\mu \times n}} I(S_{\mathcal{Z}}; BX^T) = K_{R,\mu}(C_{3,\mathcal{Z}}^\perp, C_1^\perp)$  from Proposition 29. Recall that the RDIP  $K_{R,\mu}(C_{3,\mathcal{Z}}^\perp, C_1^\perp)$  is monotonically increasing with  $\mu$  from Theorem 8, and that  $\max_{B \in \mathbb{F}_q^{\mu \times n}} I(S_{\mathcal{Z}}; BX^T) = 0$  if  $\mu \leq \Omega - |\mathcal{Z}| + 1$  from Definition 24. We thus have

$$K_{R,\mu}(C_{3,\mathcal{Z}}^\perp, C_1^\perp) \leq [\mu - \Omega + |\mathcal{Z}| - 1]^+.$$

Therefore, from Proposition 29, we have

$$\begin{aligned} \max_{B \in \mathbb{F}_q^{\mu \times n}} I(S_{\mathcal{Z}}; BX^T) &\leq K_{R,\mu}(C_{3,\mathcal{Z}}^\perp, C_1^\perp) + D(X \| U_{\psi_{\mathcal{Z}}(S_{\mathcal{Z}})} | S_{\mathcal{Z}}) \\ &\leq [\mu - \Omega + |\mathcal{Z}| - 1]^+ + D(X \| U_{\psi_{\mathcal{Z}}(S_{\mathcal{Z}})} | S_{\mathcal{Z}}), \end{aligned}$$

for arbitrarily distributed  $S$  and  $X$ . ■

This corollary shows that if the universal maximum strength  $\Omega$  is known, the maximum amount of information leakage of  $S_{\mathcal{Z}}$  to the adversary can be estimated by calculating  $D(X \| U_{\psi_{\mathcal{Z}}(S_{\mathcal{Z}})} | S_{\mathcal{Z}})$  depending on distributions of  $S$  and  $X$ . This also implies that when  $D(X \| U_{\psi_{\mathcal{Z}}(S_{\mathcal{Z}})} | S_{\mathcal{Z}}) > 0$  for some  $\mathcal{Z}$ , a part of the secret message might be revealed to the wiretapper from  $\mu < \Omega - |\mathcal{Z}|$  tapped links. Here, we note that  $D(X \| U_{\psi_{\mathcal{Z}}(S_{\mathcal{Z}})} | S_{\mathcal{Z}})$  is always zero for any  $\psi$  and any  $\mathcal{Z}$  when  $S$  and  $X$  are uniformly distributed over  $\mathbb{F}_q^l$  and  $C_1$ , respectively. From these observations, we can say that since  $S$  and  $X$  are assumed to be uniform in Definition 24, the universal maximum strength  $\Omega$  represents the resiliency of the scheme against eavesdropping in the ideal environment in which every part of the secret message is hidden.

By Proposition 29, we have the following theorem which exactly expresses  $\Omega$  in terms of the RGRW.

**Theorem 31.** Fix  $C_1, C_2$  and  $\psi$  in Definition 21, and consider the corresponding nested coset coding scheme with uniformly distributed  $S$  and  $X$ . For a subset  $\mathcal{Z} \subseteq \{1, \dots, l\}$ , let  $S_{\mathcal{Z}} \triangleq (S_i : i \in \mathcal{Z})$  and  $C_{3,\mathcal{Z}}$  be a subcode of  $C_1$ , defined by (19). Then, the universal maximum strength  $\Omega$  of the scheme, defined in Definition 24, is given by

$$\Omega = \min \{M_{R,1}(C_{3,\mathcal{Z}}^\perp, C_1^\perp) + |\mathcal{Z}| : \mathcal{Z} \subseteq \{1, \dots, l\}\} - 2.$$

*Proof:* The universal maximum strength  $\Omega$ , i.e., the maximum value of  $\omega$ , is given as

$$\begin{aligned} \Omega &= \max \left\{ \omega : I(S_{\mathcal{Z}}; BX^T) = 0, \forall \mathcal{Z} \subseteq \{1, \dots, l\}, \forall B \in \mathbb{F}_q^{(\omega - |\mathcal{Z}| + 1) \times n} \right\} \\ &= \min \left\{ \mu : \mathcal{Z} \subseteq \{1, \dots, l\}, \exists B \in \mathbb{F}_q^{(\mu - |\mathcal{Z}| + 1) \times n}, I(S_{\mathcal{Z}}; BX^T) = 1 \right\} - 1 \\ &\quad \text{(by Definition 24)} \\ &= \min \left\{ \mu + |\mathcal{Z}| - 1 : \mathcal{Z} \subseteq \{1, \dots, l\}, \exists B \in \mathbb{F}_q^{\mu \times n}, I(S_{\mathcal{Z}}; BX^T) = 1 \right\} - 1 \\ &= \min_{\mathcal{Z} \subseteq \{1, \dots, l\}} \left\{ \min \left\{ \mu : \exists B \in \mathbb{F}_q^{\mu \times n}, I(S_{\mathcal{Z}}; BX^T) = 1 \right\} + |\mathcal{Z}| - 1 \right\} - 1 \\ &= \min_{\mathcal{Z} \subseteq \{1, \dots, l\}} \left\{ \min \left\{ \mu : \max_{B \in \mathbb{F}_q^{\mu \times n}} I(S_{\mathcal{Z}}; BX^T) = 1 \right\} + |\mathcal{Z}| - 1 \right\} - 1 \\ &= \min_{\mathcal{Z} \subseteq \{1, \dots, l\}} \left\{ \min \left\{ \mu : K_{R,\mu}(C_{3,\mathcal{Z}}^\perp, C_1^\perp) = 1 \right\} + |\mathcal{Z}| - 1 \right\} - 1 \\ &\quad \text{(by Proposition 29)} \\ &= \min_{\mathcal{Z} \subseteq \{1, \dots, l\}} \left\{ M_{R,1}(C_{3,\mathcal{Z}}^\perp, C_1^\perp) + |\mathcal{Z}| \right\} - 2. \quad \text{(by Lemma 9)} \end{aligned}$$

In order to derive the exact value of  $\Omega$ , we must calculate the RGRW's of  $C_1$  and  $C_{3,\mathcal{Z}}$ 's for all possible  $\mathcal{Z}$ 's as shown in Theorem 31. Thus, the calculation of  $\Omega$  involves the search for the minimum value of the RGRW over the exponentially large set for  $l$ . Here, we give the upper and lower bounds of  $\Omega$ . The bounds can be obtained by calculating only  $l$  values of RGRW's, hence they are useful for estimating the value of  $\Omega$  in nested coset coding schemes. An upper bound of  $\Omega$  is simply obtained by Theorem 31 as follows.

**Proposition 32.** Fix  $C_1, C_2$  and  $\psi$  in Definition 21, and consider the corresponding nested coset coding scheme with uniformly distributed  $S$  and  $X$ . For  $i \subseteq \{1, \dots, l\}$ , let  $C_{3,\{i\}}$  be a subcode of  $C_1$ , defined in (19) for  $\mathcal{Z} = \{i\}$ . Then, the universal maximum strength  $\Omega$  of the scheme is upper bounded by

$$\Omega \leq \min \{M_{R,1}(C_{3,\{i\}}^\perp, C_1^\perp) : 1 \leq i \leq l\} - 1.$$

■

We also give a lower bound of  $\Omega$ . For a subset  $\mathcal{J} \subseteq \{1, \dots, N\}$  and a vector  $c = [c_1, \dots, c_N] \in \mathbb{F}_{q^m}^N$ , let  $P_{\mathcal{J}}(c)$  be a vector of length  $|\mathcal{J}|$  over  $\mathbb{F}_{q^m}$ , obtained by removing the  $t$ -th components  $c_t$  for  $t \notin \mathcal{J}$ . For example for  $\mathcal{J} = \{1, 3\}$  and  $c = [1, 1, 0, 1]$  ( $N = 4$ ), we have  $P_{\mathcal{J}}(c) = [1, 0]$ . The *punctured code*  $P_{\mathcal{J}}(C)$  of a code  $C \subseteq \mathbb{F}_{q^m}^N$  is given by  $P_{\mathcal{J}}(C) \triangleq \{P_{\mathcal{J}}(c) : c \in C\}$ . The *shortened code*  $C_{\mathcal{J}}$  of a code  $C \subseteq \mathbb{F}_{q^m}^N$  is defined by  $C_{\mathcal{J}} \triangleq \{P_{\mathcal{J}}(c) : c = [c_1, \dots, c_N] \in C, c_i = 0 \text{ for } i \notin \mathcal{J}\}$ . For example for  $C = \{[0, 0, 0], [1, 1, 0], [1, 0, 1], [0, 1, 1]\}$  ( $N = 3$ ) and  $\mathcal{J} = \{2, 3\}$ , we have  $C_{\mathcal{J}} = \{[0, 0], [1, 1]\}$ .

**Proposition 33.** Fix  $C_1, C_2$  and  $\psi$  in Definition 21, and consider the corresponding nested coset coding scheme with uniformly distributed  $S$  and  $X$ . Define a lengthened code of  $C_1$  by

$$C'_1 \triangleq \{[S, X] : S \in \mathbb{F}_{q^m}^l \text{ and } X \in \psi(S)\} \subseteq \mathbb{F}_{q^m}^{l+n}.$$

Let  $\overline{\{i\}} \triangleq \{1, \dots, l+n\} \setminus \{i\}$ . For each index  $1 \leq i \leq l$ , we define a punctured code  $\mathcal{D}_{1,i}$  of  $C'_1$  as  $\mathcal{D}_{1,i} \triangleq P_{\overline{\{i\}}}(C'_1) \subseteq \mathbb{F}_{q^m}^{l+n-1}$ , and a shortened code  $\mathcal{D}_{2,i}$  of  $C'_1$  as  $\mathcal{D}_{2,i} \triangleq (C'_1)_{\overline{\{i\}}} \subseteq \mathbb{F}_{q^m}^{l+n-1}$ . Then, the universal maximum strength  $\Omega$  of the scheme is lower bounded by

$$\Omega \geq \min \{M_{R,1}(\mathcal{D}_{2,i}^\perp, \mathcal{D}_{1,i}^\perp) : 1 \leq i \leq l\} - 1. \quad (22)$$

*Proof:* See Appendix B. ■

**Remark 34.** In [20], the security analysis of secret sharing schemes based on linear codes was given in terms of the relative dimension/length profile and the relative generalized Hamming weight [25]. By replacing the RDIP and the RGRW in all the theorems given in this section with the RDLP and the RGHW and restricting shares to be uniformly distributed over  $C_1$ , we can obtain the theorems presented in [20]. In particular, Theorem 26 and Proposition 27 become [20, Theorem 4], and Corollary 28 becomes [20, Theorem 9, Corollary 11]. Also, Theorem 31 and Theorem 33 become [20, Theorem 12], where

we note that in the case of secret sharing schemes, the exact value of  $\Omega$  in Theorem 31 coincides with its lower bound given in Theorem 33.

**Remark 35.** In [29], [46], the security analysis of secure network coding in the case of packet length  $m = 1$  was given in terms of the (relative) network generalized Hamming weight (R-)Network-GHW. By replacing the RGRW with the (R-)Network-GHW and restricting transmitted packets to be uniformly distributed over  $C_1$ , Corollary 28 becomes [29, Theorem 7], [46, Lemma 4.3]. Note that since the (R-)Network-GHW is determined according to the global coding vectors of all links as we explained in Section II-B, their security analysis by the (R-)Network-GHW is dependent on the underlying network code construction, unlike our analysis by the RDIP and RGRW.

#### IV. UNIVERSAL ERROR CORRECTION CAPABILITY OF SECURE NETWORK CODING

This section reveals the error correction capability of the nested coset coding scheme which is guaranteed independently of the underlying network code construction. Here, recall that as described in the end of Section III-A, the system of network coding is called *coherent* if the transfer matrix is known to each sink node and otherwise it is called *noncoherent*. In this section, we shall consider the error correction not only over the coherent system of network coding but also over the noncoherent system. Here we note that the decoding of the secret message is executed independently by each sink node in the network. Hence, from now on, only one sink node may be assumed without loss of generality and for the sake of simplicity.

We first give a definition of error correction capability in secure network coding. Now we consider a coding scheme that is a generalization of the nested coset coding scheme, described as follows.

**Definition 36.** Let  $\mathcal{S}$  be a set of possible secret messages. Let  $\mathcal{P}_S$  be a collection of sets of  $n$ -dimensional vectors over  $\mathbb{F}_{q^m}$  such that  $|\mathcal{P}_S| = |\mathcal{S}|$  and each element in  $\mathcal{P}_S$  is a non-empty set. Assume that there exists a certain bijective function between  $\mathcal{S}$  and  $\mathcal{P}_S$ . The coding scheme first maps a secret message  $S \in \mathcal{S}$  to a unique set  $X_S \in \mathcal{P}_S$  ( $X_S \subseteq \mathbb{F}_{q^m}^n, |X_S| > 0$ ) of  $n$ -dimensional vectors by the bijective function. Then, an element  $X \in X_S$  is chosen from  $X_S$  and served as  $n$  packets transmitted through the network.

Here we note that in the nested coset coding scheme with  $C_1$  and  $C_2$ ,  $\mathcal{S} = \mathbb{F}_{q^m}^l$ ,  $X_S = \psi(S) \in C_1/C_2$  and  $\mathcal{P}_S = \{X_S : S \in \mathcal{S}\} = C_1/C_2$ , as defined in Definition 21. The reason we consider Definition 36 is that we need to analyze the error correction capability in generalized fashion in the case of the noncoherent network coding system, due to the modification to the nested coset coding scheme as described later in Section IV-B. For this generalized coding scheme, we define the following error correction capability in the model of network coding described in Section III-A.

**Definition 37** (Universally  $t$ -Error- $\rho$ -Erasure-Correcting). Consider the  $t$ -error- $\rho$ -erasure  $(n \times m)_q$  linear network in

Definition 20. Consider a coding scheme defined in Definition 36. Then, the coding scheme is called *universally  $t$ -error- $\rho$ -erasure-correcting*, if every  $S \in \mathcal{S}$  can be uniquely determined from  $Y^T = AX^T + DZ^T \in \mathbb{F}_{q^m}^N$  for  $\forall A \in \mathbb{F}_q^{N \times n} : \text{rank } A \geq n - \rho, \forall X \in X_S, \forall D \in \mathbb{F}_q^{N \times t}, \forall Z \in \mathbb{F}_{q^m}^t$ .

As defined in Definition 37, the capability of universally  $t$ -error- $\rho$ -erasure-correcting is guaranteed on any underlying network code, and hence it is called *universal*. Silva et al.'s secure network coding scheme [37, Section VI] uses MRD codes  $C_1$  and  $C_2$ , and it is universally  $t$ -error- $\rho$ -erasure-correcting when the minimum rank distance [15] of  $C_1$  is greater than  $2t + \rho$ .

In the following subsections, we explain the coding scheme executed at the source node in the both cases of a coherent system and a noncoherent system, and present the main theorems about universal error-correction capability for both cases. The derivations of these main theorems are given in Appendix C, and they are a natural generalization of the work in [35] from the ordinary encoding scheme of a linear code and the rank distance to the nested coset coding scheme and the RGRW.

##### A. Case of Coherent System

First we explain the fundamental case of a coherent network coding system, i.e., the transfer matrix  $A$  is known to the sink node. In this case, the source node simply encodes a secret message  $S \in \mathcal{S} = \mathbb{F}_{q^m}^l$  to the transmitted  $n$  packets  $X \in X_S = \psi(S)$  by the nested coset coding scheme with  $C_1, C_2$ , as explained in Section III-B. And then,  $\mathcal{P}_S = C_1/C_2$ . Finally,  $X \in \mathbb{F}_{q^m}^n$  is regarded as an  $m \times n$  matrix over  $\mathbb{F}_q$ , and transmitted through the network.

In this setting over the coherent network coding system, the universal error correction capability of the nested coset coding scheme is exactly expressed in terms of the first RGRW  $M_{R,1}(C_1, C_2)$  as follows.

**Theorem 38.** Consider the  $t$ -error  $(n \times m)_q$  linear network in Definition 20. Then, the nested coset coding scheme with  $C_1, C_2$  in Definition 21 is universally (i.e., simultaneously for all  $A \in \mathbb{F}_q^{N \times n}$  with rank deficiency at most  $\rho$ )  $t$ -error- $\rho$ -erasure-correcting if and only if  $M_{R,1}(C_1, C_2) > 2t + \rho$ .

*Proof:* See Appendix C, where the detailed proof itself is given in Appendix C-B. ■

##### B. Case of Noncoherent System

As described in Section III-A, the transfer matrix  $A$  is unknown to the sink node in the case of a noncoherent network coding system. In this case, the source node appends appropriate packet headers to the packets generated by the nested coset coding scheme. The addition of packet headers is called the *lifting construction* [38]. Since the information of global coding vectors are carried by the packet headers in the lifting construction, this allows the scheme to be decoded when  $A$  is unknown.

The lifting construction [38] of the nested coset coding scheme is described in detail as follows. Let  $\tilde{m}$  be the degree

of a field extension  $\mathbb{F}_{q^{\tilde{m}}}$ , and let  $\phi_{\tilde{m}} : \mathbb{F}_{q^{\tilde{m}}} \rightarrow \mathbb{F}_q^{\tilde{m} \times 1}$  be an  $\mathbb{F}_q$ -linear isomorphism that expands an element of  $\mathbb{F}_{q^{\tilde{m}}}$  to a column vector over  $\mathbb{F}_q$  with respect to some fixed basis for  $\mathbb{F}_{q^{\tilde{m}}}$  over  $\mathbb{F}_q$ . Suppose  $m > n$ . Let  $\tilde{m} \triangleq m - n$ , and let  $C_1 \subseteq \mathbb{F}_{q^{\tilde{m}}}^n$  and  $C_2 \subsetneq C_1$  be a linear code and its subcode, respectively. By the nested coset coding scheme with  $C_1, C_2$ , we generate  $\tilde{X} \in \mathbb{F}_{q^{\tilde{m}}}^n$  from a secret message  $S \in \mathcal{S} = \mathbb{F}_{q^{\tilde{m}}}^l$ . Then, expanding  $\tilde{X} = [X_1, \dots, X_n] \in \mathbb{F}_{q^{\tilde{m}}}^n$  to an  $\tilde{m} \times n$  matrix  $\phi_{\tilde{m}}(\tilde{X}) \triangleq [\phi_{\tilde{m}}(\tilde{X}_1), \dots, \phi_{\tilde{m}}(\tilde{X}_n)] \in \mathbb{F}_q^{\tilde{m} \times n}$  over the base field  $\mathbb{F}_q$ , we construct  $X \in \mathbb{F}_q^{n \times m}$  of transmitted  $n$  packets that is represented as  $X^T = \begin{bmatrix} I & \phi_{\tilde{m}}(\tilde{X})^T \end{bmatrix} \in \mathbb{F}_q^{n \times m}$  as a matrix over  $\mathbb{F}_q$ , where the identity matrix  $I \in \mathbb{F}_q^{n \times n}$  is the packet header. Hence,  $\mathcal{X}_S$  and  $\mathcal{P}_S$  is given by

$$\begin{aligned} \mathcal{X}_S &= \mathcal{X}_{S, \text{lift}} \triangleq \left\{ X = \begin{bmatrix} I \\ \phi_{\tilde{m}}(\tilde{X}) \end{bmatrix} : \tilde{X} \in \psi(S) \right\}, \\ \mathcal{P}_S &= \mathcal{P}_{\text{lift}} \triangleq \left\{ X \in \mathcal{X}_{S, \text{lift}} : S \in \mathbb{F}_{q^{\tilde{m}}}^l \right\}, \end{aligned} \quad (23)$$

where  $X \in \mathbb{F}_q^{n \times m}$  is regarded as an  $m \times n$  matrix over  $\mathbb{F}_q$ . Here, recall that we defined  $\mathfrak{S}(X) \subseteq \mathbb{F}_{q^{\tilde{m}}}^n$  for  $X = [X_1, \dots, X_n] \in \mathbb{F}_q^{n \times m}$  as an  $\mathbb{F}_q$ -linear subspace of  $\mathbb{F}_{q^{\tilde{m}}}^n$  spanned by  $X_1, \dots, X_n$ , and note that  $\dim_{\mathbb{F}_q} \mathfrak{S}(X) = n$  is always guaranteed for all  $X \in \mathcal{X}_{S, \text{lift}}$  and all  $\mathcal{X}_{S, \text{lift}} \in \mathcal{P}_{\text{lift}}$  by the packet header  $I$ .

**Remark 39.** The packet headers of the lifting construction do not convey the information generated from the secret message, and convey only the information of the global coding vectors (and errors). Thus, appending packet headers does not affect the security given in Section III.

The following proposition shows that in this setting of the lifting construction of the nested coset coding scheme in the noncoherent system, the universal error correction capability is exactly expressed in terms of the first RGRW  $M_{R,1}(C_1, C_2)$  as in the coherent system.

**Proposition 40.** Assume  $m > n$ , and consider the  $t$ -error  $(n \times m)_q$  linear network in Definition 20. Consider the lifting construction of the nested coset coding scheme with  $C_1 \subseteq \mathbb{F}_{q^{\tilde{m}}}^n$  and  $C_2 \subsetneq C_1$  for  $\tilde{m} = m - n$ , as described in Section IV-B. Then, the scheme is universally  $t$ -error- $\rho$ -erasure-correcting if and only if  $M_{R,1}(C_1, C_2) > 2t + \rho$ .

*Proof:* See Appendix C, where the detailed proof itself is given in Appendix C-C. ■

This proposition also implies that by applying the lifting construction, the correction capability of the nested coset coding scheme is maintained even over the noncoherent network coding system.

## V. A CONSTRUCTION OF SECURE NETWORK CODING AND ITS ANALYSIS

This section proposes a construction of the nested coset coding scheme with  $C_1$  and  $C_2$ . We also show its universal security performance and universal error correction capability as an example of the analyses in Section III and Section IV using the RDLP and the RGRW. By adding the error correction, the proposed scheme is an extension of the universal strongly secure network coding scheme based on an MRD

code with a systematic generator matrix, presented in our earlier conference paper [21]. As well as the scheme of Silva and Kschischang [37], the proposed scheme guarantees the universal equivocation  $\Theta_{\dim C_1 - l, P_{S,X}} = H(S)$  when the conditional distribution of  $X$  given  $S$  is uniform on  $\psi(S)$ , and it is universally  $t$ -error- $\rho$ -erasure-correcting when  $n - \dim C_1 + 1 > 2t + \rho$ . Moreover, unlike Silva et al.'s scheme, our scheme guarantees the universal maximum strength  $\Omega = \dim C_1 - 1$ , which means that no part of the secret message is deterministically revealed from the eavesdropped information observed from at most  $\dim C_1 - 1$  links over any underlying network code. An explicit construction of the nested coset coding scheme satisfying  $\Omega = \dim C_1 - 1$  had remained an open question [38], and hence we solve this open question by the proposed scheme.

For the sake of simplicity, this section considers the fundamental case of a coherent network coding system. In the case of noncoherent network coding, we can simply customize the proposed scheme by the lifting construction as we described in Section IV-B.

### A. Theorems for Nested Coset Coding Scheme with MRD codes

In this subsection, we first introduce some theorems for the nested coset coding scheme using MRD codes  $C_1 \subseteq \mathbb{F}_{q^{\tilde{m}}}^n$  and  $C_2 \subsetneq C_1$ . These theorems will be used in the next subsection to clarify the security performance and error correction capability of our proposed scheme. We note that they can be also used to reveal the performance of the scheme proposed by Silva and Kschischang [37]. This will be briefly explained in Section V-C3.

First, we present the following two theorems that are established regardless of the choice of  $\psi$  in the nested coset coding scheme. For an arbitrary linear code  $C_1 \subseteq \mathbb{F}_{q^{\tilde{m}}}^n$  and an MRD code  $C_2 \subsetneq C_1$  with  $m \geq n$ , since the dual of an MRD code is also MRD [15], [24], we have  $K_{R,\mu}(C_2^\perp, C_1^\perp) = [\mu - \dim C_2]^+$  ( $0 \leq \mu \leq \dim C_1$ ) by Proposition 19. Thus, for the universal equivocation  $\Theta_{\mu, P_{S,X}}$ , we immediately have the following theorem from Proposition 27.

**Theorem 41.** Assume  $m \geq n$ . Let  $C_1 \subseteq \mathbb{F}_{q^{\tilde{m}}}^n$  be an arbitrary linear code and let  $C_2 \subsetneq C_1$  be its subcode. Suppose that  $C_2$  is an MRD code. Write  $l = \dim C_1 - \dim C_2$ . Then, for the nested coset coding scheme with  $C_1$  and  $C_2$  in Definition 21, the universal equivocation is in the range of

$$\begin{aligned} H(S) - D(X \| U_{\psi(S)} | S) &= [\mu - \dim C_2]^+ \\ &\leq \Theta_{\mu, P_{S,X}} \\ &\leq l - [\mu - \dim C_2]^+, \end{aligned}$$

for  $0 \leq \mu \leq \dim C_1$ . ■

This theorem shows that if  $X$  is uniform, the universal equivocation is  $\Theta_{\dim C_2, P_{S,X}} = H(S)$ . Also for the universal error correction capability, we immediately have the following theorem from Corollary 16 and Theorem 38.

**Theorem 42.** Assume  $m \geq n$ . Let  $C_1 \subseteq \mathbb{F}_{q^{\tilde{m}}}^n$  be a linear code and let  $C_2 \subsetneq C_1$  be its subcode. Suppose that  $C_1$  is an MRD code. Then, the nested coset coding scheme with  $C_1$  and  $C_2$  in

Definition 21 is universally  $t$ -error- $\rho$ -erasure-correcting if and only if  $2t + \rho < n - \dim C_1 + 1$ . ■

Next, we present a theorem for the universal maximum strength, which is dependent on the setting of  $\psi$  unlike Theorem 41 and Theorem 42. We have the following theorem immediately from Corollary 16 and Theorem 31 since the dual of an MRD code is also MRD.

**Theorem 43.** Assume  $m \geq n$ . Let  $C_1 \subseteq \mathbb{F}_{q^m}^n$  be a linear code and let  $C_2 \subsetneq C_1$  be its subcode. Write  $l = \dim C_1 - \dim C_2$ . Let a bijective function  $\psi : \mathbb{F}_{q^m}^l \rightarrow C_1/C_2$  be fixed in such a way that for all  $\mathcal{Z} \subseteq \{1, \dots, l\}$ , an  $\mathbb{F}_{q^m}$ -linear subspace  $C_{3,\mathcal{Z}}$  defined in (19) is an MRD code with  $\dim C_{3,\mathcal{Z}} = \dim C_1 - |\mathcal{Z}|$  and  $d_R(C_{3,\mathcal{Z}}) = n - \dim C_1 - |\mathcal{Z}| + 1$ . Then, the nested coset coding scheme with  $C_1$ ,  $C_2$  and  $\psi$  in Definition 21 guarantees the universal maximum strength  $\Omega = \dim C_1 - 1$ . ■

In the next subsection, we present an explicit construction of the nested coset coding scheme that satisfies all the assumptions in Theorems 41, 42 and 43 simultaneously.

### B. Description of the Proposed Scheme

Recall that the punctured code and shortened code of a code  $C \in \mathbb{F}_{q^m}^N$  to  $\mathcal{J} \subseteq \{1, \dots, N\}$  are respectively defined by  $P_{\mathcal{J}}(C) = \{P_{\mathcal{J}}(c) : c \in C\}$  and  $C_{\mathcal{J}} = \{P_{\mathcal{J}}(c) : c = [c_1, \dots, c_N] \in C, c_i = 0 \text{ for } i \notin \mathcal{J}\}$ , where  $P_{\mathcal{J}}(c)$  for  $c \in \mathbb{F}_{q^m}^N$  represents a vector of length  $|\mathcal{J}|$  obtained by removing the  $t$ -th components of  $c$  for  $t \notin \mathcal{J}$ . Assume that the degree  $m$  of the field extension  $\mathbb{F}_{q^m}$  satisfies  $m \geq l + n$ . Then, the proposed scheme generates the transmitted  $n$  packets  $X \in \mathbb{F}_{q^m}^n$  by the following setting of the nested coset coding scheme.

First, we set the linear codes  $C_1, C_2 \subseteq \mathbb{F}_{q^m}^n$ . Let  $\mathcal{D}$  be an  $[l + n, k]$  MRD code over  $\mathbb{F}_{q^m}$  with  $\dim \mathcal{D} = k (\geq l)$  and a systematic generator matrix  $G = \begin{bmatrix} I & P \end{bmatrix} \in \mathbb{F}_{q^m}^{(l+n) \times k}$ . Let  $\mathcal{L} \triangleq \{l + 1, \dots, l + n\}$  be an index set. Define  $C_1 \triangleq P_{\mathcal{L}}(\mathcal{D})$  as a punctured code of  $\mathcal{D}$  to the index set  $\mathcal{L}$ . Also define  $C_2 \triangleq \mathcal{D}_{\mathcal{L}}$  as a shortened code of  $\mathcal{D}$  to the index set  $\mathcal{L}$ . Here we note the following facts for  $C_1, C_2$ . Since an MRD code over  $\mathbb{F}_{q^m}^N$  with  $m \geq N$  is also an MDS code over  $\mathbb{F}_{q^m}$  [15], a  $k \times k$  matrix over  $\mathbb{F}_{q^m}$  consisting of arbitrary  $k$  columns of  $G$  is always nonsingular, and hence  $\dim P_{\mathcal{L}}(\mathcal{D}) = \dim C_1 = k$ . Also, since the MRD code  $\mathcal{D}$  is also MDS [15], the shortening of  $\mathcal{D}$  to  $\mathcal{L}$  simply reduces the dimension of  $\mathcal{D}$  over  $\mathbb{F}_{q^m}$  by  $l$ , i.e.,  $\dim \mathcal{D}_{\mathcal{L}} = \dim C_2 = k - l$ . Also, we should note that from the definition of the punctured code and shortened code, we have  $C_2 \subseteq C_1$ , and  $\dim C_1 - \dim C_2 = \dim C_1/C_2 = l$ .

Next, we set the bijective function  $\psi : \mathbb{F}_{q^m}^l \rightarrow C_1/C_2$ . We define submatrices of the systematic generator matrix  $G$  of  $\mathcal{D}$  as follows.

$$G \triangleq \left[ \begin{array}{c|c} I & \Delta G \\ \hline O & G_2 \end{array} \right] \left\{ \begin{array}{l} l \text{ rows} \\ k - l \text{ rows} \end{array} \right\}$$

$\underbrace{\hspace{1.5cm}}_{l \text{ columns}} \quad \underbrace{\hspace{1.5cm}}_{n \text{ columns}}$

Then, we set  $\psi$  by  $\Delta G \in \mathbb{F}_{q^m}^{l \times n}$  as follows.

$$\psi(S) \triangleq S \Delta G + C_2 \in C_1/C_2. \quad (24)$$

We note that  $G_1 \triangleq \begin{bmatrix} \Delta G \\ G_2 \end{bmatrix} \in \mathbb{F}_{q^m}^{k \times n}$  is the generator matrix of  $C_1$ , and  $G_2 \in \mathbb{F}_{q^m}^{(k-l) \times n}$  is the generator matrix of  $C_2$ . Also note that since  $\text{rank } \Delta G = l$  from  $\dim C_1 - \dim C_2 = \text{rank } G_1 - \text{rank } G_2 = l$ ,  $\psi$  is bijective.

In our scheme, we execute the nested coset coding scheme with these settings of  $C_1$ ,  $C_2$  and  $\psi$ , and generate the transmitted packets  $X$ . Then, the source node transmits  $X$  over the network as described in Section III-A, and the sink node receives  $Y$  and attempts to obtain the secret message from  $Y$ . The universal security performance and the universal error correction capability of our scheme is clarified in the next subsection.

**Remark 44.** Consider the case where  $\mathcal{D}$  and  $G$  are not an MRD code and its systematic generator matrix but a Reed-Solomon code and its systematic one respectively in the above settings. Then, this nested coset coding scheme becomes the strongly-secure secret sharing scheme of Nishara and Takizawa [30]. Similarly to the relation between the wiretap channel II and secure network coding, our scheme can be viewed as a generalization of their scheme [30] for network coding.

### C. Analyses on the Proposed Scheme

As an example of applications of the analyses of Section III and Section IV using the RDIP and the RGRW, this subsection presents the analyses on the proposed scheme described in the previous subsection. We first reveal the security performance and error correction capability of our scheme. Next, we discuss the required packet length in our scheme. Finally, we summarize the comparison of the proposed scheme with the scheme of Silva and Kschischang [37].

1) *Security Performance and Error Correction Capability of the Proposed Scheme:* Here, we analyze the security performance and the error correction capability of the proposed scheme using the theorems presented in Section V-A.

First, in order to show that assumptions in Theorems 41–43 are satisfied in our scheme, we introduce the following lemmas about a shortened code and a punctured code of an MRD code.

**Lemma 45.** Let  $m \geq N$ , and  $C \subseteq \mathbb{F}_{q^m}^N$  be an MRD code of length  $N$  over  $\mathbb{F}_{q^m}$ . For a subset  $\mathcal{I} \subseteq \{1, \dots, N\}$  satisfying  $\mathcal{I} \supseteq \{\dim C + 1, \dots, N\}$ , let  $C_{\mathcal{I}} \subseteq \mathbb{F}_{q^m}^{|\mathcal{I}|}$  be a shortened code of  $C \subseteq \mathbb{F}_{q^m}^N$  to  $\mathcal{I}$ . Then,  $C_{\mathcal{I}}$  is an MRD code with  $\dim C_{\mathcal{I}} = \dim C - N + |\mathcal{I}|$  and  $d_R(C_{\mathcal{I}}) = N - \dim C + 1$ .

*Proof:* Since the MRD code  $C$  is also MDS [15] and  $\mathcal{I} \supseteq \{\dim C + 1, \dots, N\}$ , the shortening of  $C$  to  $\mathcal{I}$  simply reduces the dimension of  $C$  over  $\mathbb{F}_{q^m}$  by  $N - |\mathcal{I}|$ , i.e.,  $\dim C_{\mathcal{I}} = \dim C - N + |\mathcal{I}|$ .

Since  $m \geq N$  and shortened codes can be viewed as subcodes, we have

$$\begin{aligned} d_R(C_{\mathcal{I}}) &\geq d_R(C) \\ &= N - \dim C + 1. \end{aligned}$$

On the other hand, from  $m \geq N$  and the Singleton-type bound



for the rank distance given in Proposition 14, we have

$$\begin{aligned} d_R(C_I) &\leq |I| - \underbrace{\dim C_I}_{=\dim C - N + |I|} + 1 \\ &= N - \dim C + 1. \end{aligned}$$

Therefore, we have  $d_R(C_I) = N - \dim C + 1$ . ■

**Lemma 46.** Let  $m \geq N$ , and  $C \subseteq \mathbb{F}_{q^m}^N$  be an MRD code of length  $N$  over  $\mathbb{F}_{q^m}$ . For a set  $I \subseteq \{1, \dots, N\}$  satisfying  $|I| \geq N - \dim C$  and  $|I| \geq \dim C$ , let  $P_I(C) \subseteq \mathbb{F}_{q^m}^{|I|}$  be a punctured code of  $C$  to  $I$ . Then,  $P_I(C)$  is an MRD code with  $\dim P_I(C) = \dim C$  and  $d_R(P_I(C)) = |I| - \dim C + 1$ .

*Proof:* Since an MRD code is also MDS, a  $\dim C \times \dim C$  matrix over  $\mathbb{F}_{q^m}$  consisting of arbitrary  $\dim C$  columns of the generator matrix of  $C$  is always nonsingular. Thus, the dimension of a punctured code  $P_I(C)$  of length  $|I| (\geq \dim C)$  is  $\dim P_I(C) = \dim C$ .

The puncturing of  $C$  to  $I$  reduces the minimum rank distance of  $C$  by at most  $N - |I| (\leq \dim C)$  from the definition of rank distance [15]. This implies that  $d_R(P_I(C)) \geq d_R(C) - N + |I|$ . From  $m \geq N$ , we thus have

$$\begin{aligned} d_R(P_I(C)) &\geq d_R(C) - N + |I| \\ &= |I| - \dim C + 1. \end{aligned}$$

On the other hand, from  $m \geq N$  and the Singleton-type bound for the rank distance given in Proposition 14, we have

$$\begin{aligned} d_R(P_I(C)) &\leq |I| - \dim P_I(C) + 1 \\ &= |I| - \dim C + 1. \end{aligned}$$

Therefore, we have  $d_R(P_I(C)) = |I| - \dim C + 1$ . ■

By the above lemmas, we finally derive the following propositions for the universal security performance and the universal error correction capability in our scheme, and show that our scheme satisfies Theorems 41, 42 and 43 simultaneously.

**Proposition 47.** Consider the nested coset coding scheme proposed in Section V-B. Then, the universal equivocation  $\Theta_{\mu, P_{S,X}}$  of the scheme is in the range of

$$\begin{aligned} H(S) - D(X \| U_{\psi(S)} | S) - [\mu - \dim C_2]^+ \\ \leq \Theta_{\mu, P_{S,X}} \\ \leq l - [\mu - \dim C_2]^+, \end{aligned}$$

for  $0 \leq \mu \leq \dim C_1 = k$ .

*Proof:* From Lemma 45, since  $m \geq l + n$ , we have  $\dim C_2 = k - l$ , and  $C_2$  is an MRD code with  $d_R(C_2) = n + l - k + 1$ . Thus, from Theorem 41, we have the proposition. ■

**Proposition 48.** The nested coset coding scheme proposed in Section V-B is universally  $t$ -error- $\rho$ -erasure-correcting if and only if  $2t + \rho < n - k + 1$ .

*Proof:* From Lemma 46, since  $m \geq l + n$ , we have  $\dim C_1 = \dim \mathcal{D} = k$ , and  $C_1$  is an MRD code with  $d_R(C_1) = n - k + 1$ . Therefore, the proposition is proved from Theorem 42. ■

**Proposition 49.** The nested coset coding scheme proposed in Section V-B has the universal maximum strength  $\Omega = k - 1$ .

*Proof:* Recall  $\dim \mathcal{D} = k$ . For a subset  $\mathcal{Z} \subseteq \{1, \dots, l\}$ , let  $\overline{\mathcal{Z}} \triangleq \{1, \dots, l, l+1, \dots, l+n\} \setminus \mathcal{Z}$ . Denote by  $\mathcal{D}_{\overline{\mathcal{Z}}} \subseteq \mathbb{F}_{q^m}^{l+n-|\mathcal{Z}|}$  a shortened code of  $\mathcal{D}$  to  $\overline{\mathcal{Z}}$ . Since  $\mathcal{D} \subseteq \mathbb{F}_{q^m}^{l+n}$  is an MRD code with  $m \geq l + n$  and  $\overline{\mathcal{Z}} \supseteq \{l+1, \dots, l+n\} \supseteq \{k+1, \dots, l+n\}$  from  $l \leq k$ ,  $\mathcal{D}_{\overline{\mathcal{Z}}}$  is an MRD code with  $\dim \mathcal{D}_{\overline{\mathcal{Z}}} = k - |\mathcal{Z}|$  and  $d_R(\mathcal{D}_{\overline{\mathcal{Z}}}) = l+n-k+1$  from Lemma 45. Since  $\psi$  in the proposed scheme is specified by the systematic generator matrix  $G$  of  $\mathcal{D}$  as (24), we can see that for  $\mathcal{Z}$ ,  $C_{3,\mathcal{Z}}$  in (19) can be defined as a punctured code of  $\mathcal{D}_{\overline{\mathcal{Z}}}$  to an index set  $\{l+1-|\mathcal{Z}|, \dots, l+n-|\mathcal{Z}|\}$ , i.e., it is obtained by eliminating first  $l - |\mathcal{Z}|$  coordinates of codewords in  $\mathcal{D}_{\overline{\mathcal{Z}}}$ . Hence, from Lemma 46,  $C_{3,\mathcal{Z}} \subseteq \mathbb{F}_{q^m}^n$  is an MRD code with  $\dim C_{3,\mathcal{Z}} = k - |\mathcal{Z}|$  and  $d_R(C_{3,\mathcal{Z}}) = n - k - |\mathcal{Z}| + 1$ . Therefore, we have the proposition from Theorem 43. ■

Here we note that in the proposed scheme, the exact value of  $\Omega$  derived in Proposition 49 coincides with the upper and lower bounds of  $\Omega$  that are respectively given by Proposition 32 and Proposition 33. The reason is as follows. For  $i \in \{1, \dots, l\}$  and  $\{i\} = \{1, \dots, l+n\} \setminus \{i\}$ , define the punctured code  $\mathcal{D}_{1,i} \triangleq P_{\{i\}}(\mathcal{D})$  and the shortened code  $\mathcal{D}_{2,i} \triangleq \mathcal{D}_{\overline{\{i\}}}$ . Then,  $\mathcal{D}_{2,i}$  is MRD with  $\dim \mathcal{D}_{2,i} = k - 1$  from Lemma 45. Since the dual of an MRD code is also MRD, we have  $M_{R,1}(\mathcal{D}_{2,i}^\perp, \mathcal{D}_{1,i}^\perp) = n - \dim \mathcal{D}_{2,i}^\perp + 1 = k$  from Corollary 16. Thus, we obtain  $\Omega \geq k - 1$  from Proposition 33. On the other hand, the subcode  $C_{3,\{i\}}$  is MRD with  $\dim C_{3,\{i\}} = k - 1$  as shown in the proof of Proposition 49. We thus have  $M_{R,1}(C_{3,\{i\}}^\perp, C_1^\perp) = n - \dim C_{3,\{i\}}^\perp + 1 = k$ . Therefore  $\Omega \leq k - 1$  holds from Proposition 32.

2) *Required Packet Length  $m$ :* Assume that  $m < N$  in Lemma 45 and Lemma 46. Then, Lemma 45 and Lemma 46 do not always hold. We give here a specific case in which Lemma 45 and Lemma 46 do not hold. Considering the case where  $m < N$  and additionally  $m < |I|$  in Lemma 45, we have

$$d_R(C_I) \leq \frac{m}{|I|}(|I| - \dim C_I) + 1 = \frac{m}{|I|}(N - \dim C) + 1,$$

by the Singleton-type bound for rank distance. Since  $m < |I|$ , this clearly shows that Lemma 45 does not hold in the case. Also, when  $m < N$  and  $m < |I|$  in Lemma 46, we have

$$d_R(P_I(C)) \leq \frac{m}{|I|}(|I| - \dim P_I(C)) + 1 = \frac{m}{|I|}(|I| - \dim C) + 1,$$

and hence Lemma 46 does not hold in the case. Hence, we can see that  $m \geq N$  is a necessary condition for Lemma 45 and Lemma 46 to hold. This also implies that Propositions 47–49 do not always hold if the packet length is  $m < l + n$  in our scheme. Thus, the assumption  $m \geq l + n$  is a necessary condition for our scheme to always satisfy Propositions 47–49 simultaneously.

3) *A Comparison of the Security and the Error-Correction Capability:* Here we summarize the comparison of our scheme with the scheme of Silva and Kschischang. First we present a comparison about the security and error correction capability. The scheme of Silva and Kschischang [37] is the nested coset coding scheme using a linear code  $C_1 \subseteq \mathbb{F}_{q^m}^n$  and its subcode  $C_2 \subsetneq C_1$  where both  $C_1$  and  $C_2$  are MRD with  $m \geq n$ .

This immediately yields that Theorem 41 and Theorem 42 are simultaneously established in their scheme as in our scheme. However, their scheme does not specify the bijective function  $\psi$  in such a way that the condition in Theorem 43 is always satisfied, and hence their scheme does not always guarantee the universal maximum strength  $\Omega = \dim C_1 - 1$ . On the other hand, our scheme simultaneously satisfies Theorems 41–43 as shown in Propositions 47–49. Especially, one specific reason why our scheme satisfies Proposition 49 is that the bijective function  $\psi$  in our scheme is specified by the systematic generator matrix  $G$  of  $\mathcal{D}$  as (24). Therefore, we can see that our scheme clearly has the advantage over their scheme in terms of the strong security.

Next we give a comparison about the required packet length. In [36, Theorem 8], Silva et al. showed that there exist cases where their scheme in [37] satisfies the universal maximum strength  $\Omega = \dim C_1 - 1$ , and that the sufficient condition on the existence of such a case is  $m \geq (l+n)^2/8 + \log_q 16l$  for packet length. In contrast, we have demonstrated an explicit construction of the nested coset coding scheme satisfying  $\Omega = \dim C_1 - 1$  whenever  $m \geq l+n$  is satisfied. Furthermore, we always have  $l+n < (l+n)^2/8 + \log_q 16l$  for  $l \geq 1$  and  $n \geq 2$ . Therefore, our condition for the packet length is less demanding than that of Silva et al.’s sufficient condition.

## VI. CONCLUSION

In this paper, we have introduced two relative code parameters, the relative dimension/intersection profile (RDIP) of a linear code  $C_1 \subseteq \mathbb{F}_{q^m}^n$  and its subcode  $C_2 \subsetneq C_1$  and the relative generalized rank weight (RGRW) of  $C_1$  and  $C_2$ . We have also elucidated some basic properties of the RDIP and the RGRW. We have clarified the relation between the RGRW and the Gabidulin’s rank distance [15], that between the RGRW and the relative generalized Hamming weight [25], and that between the RGRW and the relative network generalized Hamming weight [46]. As applications of the RDIP and the RGRW, the security performance and the error correction capability of secure network coding based on the nested coset coding scheme with  $C_1$  and  $C_2$  have been analyzed and clarified. We have revealed that the security performance and the error correction capability, guaranteed independently of the underlying network code, are expressed in terms of the RDIP and the RGRW. Further, we have proposed an explicit construction of the nested coset coding scheme, and have analyzed its universal security performance and universal error correction capability by using the RDIP and the RGRW. As well as the scheme of Silva and Kschischang [37], the proposed scheme guarantees, independently of the underlying network code, that no information of the secret message is obtained from any  $\mu \leq \dim C_2$  tapped links when the transmitted packets are uniformly distributed over  $C_1$ , and that the secret message is correctly decodable against any  $t$  error packets injected somewhere in the network and  $\rho$  rank deficiency of the transfer matrix of the sink node whenever  $n - \dim C_1 + 1 < 2t + \rho$  holds. Moreover, our scheme also always guarantees that no part of the secret message is revealed to the adversary with  $\mu \leq \dim C_1 - 1$  tapped links when the secret

message and transmitted packets are uniformly distributed, unlike Silva et al.’s scheme [36], [37].

Section V of this paper presented only one instance of the nested coset coding scheme that has specific universal security performance and universal error correction capability, i.e., specific values of RDIP and RGRW. We believe that the security scheme should be designed according to the system requirements and environments. Hence, how to design a pair of a linear code  $C_1$  and its subcode  $C_2$  from arbitrarily given RDIP and RGRW is left as an important open problem for future work. Another possible avenue is to derive other types of bounds of the RGRW, e.g., generalizing the Gilbert-Varshamov bound of the rank distance [16] for the RGRW, etc.

Recall that the theory of the RDIP and RGRW established in this paper is similar to the theory of the GHW [42] that was proposed to investigate the security performance of coding schemes on the Wiretap Channel II [32]. The specific coding schemes based on maximum distance separable codes have been already known as optimal ones in the Wiretap Channel II. However, the theory of the GHW is not regarded as unnecessary, because it is important and required to reveal the security performance of *any* coding schemes on the Wiretap Channel II. As a conclusion of this paper, we allege that this importance of the GHW is exactly same as what we have established in this paper about the RDIP and RGRW for network coding.

## APPENDIX A

### PROOF OF LEMMA 25

We first give the following lemma that will be used to prove Lemma 25.

**Lemma 50.** Let  $C_1 \subseteq \mathbb{F}_{q^m}^n$  be a linear code and  $C_2 \subsetneq C_1$  be its subcode. For an arbitrary subspace  $V \subseteq \mathbb{F}_{q^m}^n$ , we have

$$\begin{aligned} \dim(C_1 \cap V) - \dim(C_2 \cap V) \\ = \dim C_1 / C_2 - \dim(C_2^\perp \cap V^\perp) + \dim(C_1^\perp \cap V^\perp). \end{aligned}$$

*Proof:* For a linear subspace  $C \subseteq \mathbb{F}_{q^m}^n$ , we have  $\dim C + \dim(C^\perp \cap V^\perp) = \dim V^\perp + \dim(C \cap V)$ . Thus, by letting  $C = C_1$  and  $C = C_2$  in this equation, we obtain

$$0 = \dim C_1 + \dim(C_1^\perp \cap V^\perp) - \dim V^\perp - \dim(C_1 \cap V),$$

and

$$0 = \dim C_2 + \dim(C_2^\perp \cap V^\perp) - \dim V^\perp - \dim(C_2 \cap V),$$

respectively. Therefore, the lemma is established by these equalities since  $\dim C_1 - \dim C_2 = \dim C_1 / C_2$ . ■

Next we recall that for random variables  $A \in \mathcal{A}$  and  $B \in \mathcal{B}$ , we have the following relations among the conditional entropy and the (conditional) relative entropy [8, Ch. 2, p. 27]:

$$H(A) = \log |\mathcal{A}| - D(A \| U_{\mathcal{A}}), \quad (25)$$

$$H(A|B) = E_B [\log |\mathcal{A}(B)|] - D(A \| U_{\mathcal{A}(B)} | B), \quad (26)$$

where  $A \in \mathcal{A}(b)$  with probability one given  $B = b$  and  $E_B$  denotes the expectation over the probability distribution  $P_B$ .

In the following, we will use these relationships to prove the lemma.

Recall that for each  $S = s$ , a coset  $\psi(s) \in C_1/C_2$  is uniquely determined. Also observe that for given  $W = w$  as a realization of  $W$ , there exists a unique coset  $\mathcal{X}(w) = \{x \in C_1 : Bx^T = w^T\} \in C_1/(\text{row}(B)^\perp \cap C_1)$ . Observe that  $X$  belongs to  $\psi(s) \cap \mathcal{X}(w)$  when  $S = s$  and  $W = w$ , and that

$$|\psi(s) \cap \mathcal{X}(w)| = |\psi(0) \cap \mathcal{X}(0)| = |C_2 \cap (\text{row}(B)^\perp \cap C_1)| \\ = |C_2 \cap \text{row}(B)^\perp|.$$

Hence we have

$$\log_{q^m} |\psi(s) \cap \mathcal{X}(w)| = \log_{q^m} |C_2 \cap \text{row}(B)^\perp| \\ = \dim(C_2 \cap \text{row}(B)^\perp),$$

for any  $s$  and  $w$ . Thus, by (26), we have

$$H(X|S, W) = \dim(C_2 \cap \text{row}(B)^\perp) - D(X||U_{\psi(S) \cap \mathcal{X}(W)}|S, W). \quad (27)$$

Also observe that  $X$  is distributed over  $\mathcal{X}(w)$  when  $W = w$ , and that

$$\log_{q^m} |\mathcal{X}(w)| = \log_{q^m} |C_1 \cap \text{row}(B)^\perp| = \dim(C_1 \cap \text{row}(B)^\perp),$$

for any  $w$ . Thus, by (26), we obtain

$$H(X|W) = \dim(C_1 \cap \text{row}(B)^\perp) - D(X||U_{\mathcal{X}(W)}|W). \quad (28)$$

Recall that  $X$  is distributed over a coset  $\psi(s) \in C_1/C_2$  for fixed  $S = s$ , and  $\log_{q^m} |\psi(s)| = \dim C_2$  for any  $s$ . Thus, by (26), we have

$$H(X|S) = \dim C_2 - D(X||U_{\psi(S)}|S). \quad (29)$$

Let a subspace  $\mathcal{W} = \{xB^T : x \in C_1\}$ . For the cardinality of  $\mathcal{W}$ , we have

$$\log_{q^m} |\mathcal{W}| = \dim \mathcal{W} = \dim C_1 - \dim(C_1 \cap \text{row}(B)^\perp).$$

Thus, by (25), we have

$$H(W) = \log_{q^m} |\mathcal{W}| - D(W||U_{\mathcal{W}}) \\ = \dim C_1 - \dim(C_1 \cap \text{row}(B)^\perp) - D(W||U_{\mathcal{W}}). \quad (30)$$

Recall that for given  $B$  and fixed  $X = x$ ,  $W = xB^T$  is uniquely determined. This implies  $H(W|X) = 0$ . Thus, by  $H(W|S, X) \leq H(W|X) = 0$  and the nonnegativity of the entropy function [8, Ch. 2, p. 14], we have

$$H(W|S, X) = 0. \quad (31)$$

By expanding  $I(S; W)$  and substituting (27), (29), (30) and

(31) into the expanded equation (32), we obtain

$$\begin{aligned} I(S; W) &= \underbrace{I(S, X; W)}_{=H(W)-H(W|S, X)} - \underbrace{I(X; W|S)}_{=H(X|S)-H(X|S, W)} \\ &= \underbrace{H(W)}_{=\dim C_1 - \dim(C_1 \cap \text{row}(B)^\perp) - D(W||U_{\mathcal{W}})} - \underbrace{H(W|S, X)}_{=0 \text{ (by (31))}} \\ &\quad - \underbrace{H(X|S)}_{=\dim C_2 - D(X||U_{\psi(S)}|S) \text{ (by (29))}} + \underbrace{H(X|S, W)}_{=\dim(C_2 \cap \text{row}(B)^\perp) - D(X||U_{\psi(S) \cap \mathcal{X}(W)}|S, W) \text{ (by (27))}} \\ &= \underbrace{\dim C_1 - \dim C_2}_{=l} - \dim(C_1 \cap \text{row}(B)^\perp) + \dim(C_2 \cap \text{row}(B)^\perp) \\ &\quad + D(X||U_{\psi(S)}|S) - D(W||U_{\mathcal{W}}) - D(X||U_{\psi(S) \cap \mathcal{X}(W)}|S, W) \\ &\leq \underbrace{l - \dim(C_1 \cap \text{row}(B)^\perp) + \dim(C_2 \cap \text{row}(B)^\perp)}_{=\dim(C_2^\perp \cap \text{row}(B)) - \dim(C_1^\perp \cap \text{row}(B)) \text{ (by Lemma 50)}} + D(X||U_{\psi(S)}|S), \end{aligned} \quad (32)$$

which proves (11).

On the other hand, observe that the number of possible  $S$  for any given  $W = w$  is exactly equal to  $q^{m \cdot \dim(C_1 \cap \text{row}(B)^\perp)} / q^{m \cdot \dim(C_2 \cap \text{row}(B)^\perp)}$ . Also recall that the relative entropy is nonnegative [8, Ch. 2, p. 26]. Thus, by applying (26) to the set  $\{s \in \mathbb{F}_{q^m}^l : w = xB^T, x \in \psi(s)\}$  that depends on the realization  $W = w$ , we have the following inequality.

$$H(S|W) \leq \dim(C_1 \cap \text{row}(B)^\perp) - \dim(C_2 \cap \text{row}(B)^\perp).$$

Thus,

$$\begin{aligned} I(S; W) &= H(S) - H(S|W) \\ &\geq H(S) - \dim(C_1 \cap \text{row}(B)^\perp) - \dim(C_2 \cap \text{row}(B)^\perp) \\ &= H(S) - l + \dim(C_2^\perp \cap \text{row}(B)) - \dim(C_1^\perp \cap \text{row}(B)) \\ &\quad \text{(by Lemma 50)} \\ &= \dim(C_2^\perp \cap \text{row}(B)) - \dim(C_1^\perp \cap \text{row}(B)) - D(S||U_{\mathbb{F}_{q^m}^l}), \\ &\quad \text{(by (25))} \end{aligned}$$

which proves (12). Thus, we have the statement 1) in the lemma.

Here, we show the equalities in (11) and (12) for the uniformly distributed  $S$  and  $X$ . Assume that  $S$  is uniform over  $\mathbb{F}_{q^m}^l$ . Then, from (25), we have  $D(S||U_{\mathbb{F}_{q^m}^l}) = l - H(S) = 0$ . Also, when  $X$  is uniform over  $C_1$ , i.e., uniform over  $\psi(S)$ , we have  $H(X|S) = \dim C_2$  and hence  $D(X||U_{\psi(S)}|S) = \dim C_2 - H(X|S) = 0$  from (26). Therefore, the equalities in (11) and (12) hold, and we have the statement 2) in the lemma.

Finally, we show the statement 3) for the distribution of  $S$  that assigns a positive probability to every element in  $\mathbb{F}_{q^m}^l$ . Let  $P_S$  be a distribution of  $S$  such that all elements in  $\mathbb{F}_{q^m}^l$  have positive probabilities, and assume that  $I(S; W) = 0$  holds for  $P_S$ . Recall that the mutual information is expressed in terms of the relative entropy [8, Ch. 2, pp. 18–19] as

$$0 = I(S; W) = \sum_s P_S(s) D(W_{S=s} || W).$$

where  $W_{S=s}$  is the random variable with the distribution  $P_{W|S=s}$ . Thus,  $D(W_{S=s}||W) = 0$ , i.e.,  $P_{W|S=s} = P_W$ , simultaneously holds for all  $s \in \mathbb{F}_{q^m}^l$  from the nonnegativity of relative entropy [8, Ch. 2, p. 26].

Here, consider another random variable  $S'$  with an arbitrary distribution  $P_{S'}$ , and the corresponding random variable  $W'$ . Here we assume that the conditional probability of  $W'$  given  $S'$  is the same as that of  $W$  given  $S$ , which means that  $P_{W'|S'=s} = P_{W|S=s} = P_W = P_{W'}$  for all  $s$ . By  $I(S'|W') = \sum_s P_{S'}(s)D(W'_{S'=s}||W')$ , we see  $I(S'|W') = 0$ . In particular, for the uniformly distributed  $S'$  we have  $I(S'; W') = 0$  and  $D(S' || U_{\mathbb{F}_{q^m}^l}) = 0$ , and hence we have

$$0 = I(S'; W') \geq \dim(C_2^\perp \cap \text{row}(B)) - \dim(C_1^\perp \cap \text{row}(B)),$$

from (12). Therefore, since

$$\dim(C_2^\perp \cap \text{row}(B)) - \dim(C_1^\perp \cap \text{row}(B)) \geq 0,$$

holds, we have  $\dim(C_2^\perp \cap \text{row}(B)) - \dim(C_1^\perp \cap \text{row}(B)) = 0$ . ■

## APPENDIX B PROOF OF PROPOSITION 33

From the definition of  $C'_1$ ,  $\mathcal{D}_{2,i}$  is a subcode of  $\mathcal{D}_{1,i}$  with dimension  $\dim \mathcal{D}_{2,i} = \dim \mathcal{D}_{1,i} - 1 = \dim C_1 - 1$  over  $\mathbb{F}_{q^m}$  for each  $i \in \{1, \dots, l\}$ . Let  $\mathcal{L} \triangleq \{1, \dots, l\}$  and  $S_{\mathcal{L} \setminus \{i\}} \triangleq [S_1, \dots, S_{i-1}, S_{i+1}, \dots, S_l]$  for  $1 \leq i \leq l$ . For  $S_i \in \mathbb{F}_{q^m}$ , define a coset

$$\tau(S_i) \triangleq \{[S_{\mathcal{L} \setminus \{i\}}, X] : S_{\mathcal{L} \setminus \{i\}} \in \mathbb{F}_{q^m}^{l-1} \text{ and } X \in \psi([S_1, \dots, S_l])\} \\ \in \mathcal{D}_{1,i} / \mathcal{D}_{2,i}.$$

Here we define  $Z_{\overline{\{i\}}} \triangleq P_{\overline{\{i\}}}([S, X]) = [S_{\mathcal{L} \setminus \{i\}}, X] \in \mathcal{D}_{1,i}$ . Recall that  $S_1, \dots, S_l$  are mutually independent and uniformly distributed over  $\mathbb{F}_{q^m}$ . Thus,  $Z_{\overline{\{i\}}}$  can be regarded as the one generated from a secret message  $S_i \in \mathbb{F}_{q^m}$  by a nested coset coding scheme with  $\mathcal{D}_{1,i}$  and  $\mathcal{D}_{2,i}$  according to the uniform distribution over  $\tau(S_i)$ , that is,  $Z_{\overline{\{i\}}} \in \tau(S_i)$  is chosen uniformly at random from  $\tau(S_i) \in \mathcal{D}_{1,i} / \mathcal{D}_{2,i}$ . Therefore, we have  $I(S_i; DZ_{\overline{\{i\}}}^T) = 0$  for any  $D \in \mathbb{F}_q^{\mu \times (n+l-1)}$  whenever  $\mu < M_{R,1}(\mathcal{D}_{2,i}^\perp, \mathcal{D}_{1,i}^\perp)$  from Corollary 28.

For an arbitrary subset  $\mathcal{R} \subseteq \mathcal{L} \setminus \{i\}$ , define a matrix  $F_{\mathcal{R}}$  that consists of  $|\mathcal{R}|$  rows of an  $(l-1) \times (l-1)$  identity matrix, satisfying  $[S_j : j \in \mathcal{R}]^T = F_{\mathcal{R}} S_{\mathcal{L} \setminus \{i\}}^T$ . Here we note that  $F_{\mathcal{R}} \in \mathbb{F}_{q^m}^{|\mathcal{R}| \times (n+l-1)}$  is defined as a matrix over the base field  $\mathbb{F}_q$ . For an arbitrary matrix  $B \in \mathbb{F}_q^{k \times n}$  ( $0 \leq k \leq n$ ), let  $\mu = |\mathcal{R}| + k$  and  $D = \begin{bmatrix} F_{\mathcal{R}} & O \\ O & B \end{bmatrix} \in \mathbb{F}_q^{(|\mathcal{R}|+k) \times (n+l-1)}$ . Then, since  $DZ_{\overline{\{i\}}}^T = \begin{bmatrix} [S_j : j \in \mathcal{R}]^T \\ BX^T \end{bmatrix}$ , we have the following equality from the foregoing proof.

$$0 = I(S_i; DZ_{\overline{\{i\}}}^T) = I(S_i; S_{\mathcal{R}}, BX^T), \quad (33)$$

whenever  $|\mathcal{R}| + k < M_1(\mathcal{D}_{2,i}^\perp, \mathcal{D}_{1,i}^\perp)$ . Let  $\mathcal{R}' \triangleq \mathcal{R} \cup \{i\} = \{r_1, \dots, r_{|\mathcal{R}+1|}\}$ . Since  $S_1, \dots, S_l$  are mutually independent, the mutual information between  $S_{\mathcal{R}'}$  and  $BX^T$  is

given by

$$I(S_{\mathcal{R}'}; BX^T) = H(S_{\mathcal{R}'}) - H(S_{\mathcal{R}'} | BX^T) \\ = \sum_{j=1}^{|\mathcal{R}|+1} H(S_{r_j}) - \sum_{j=1}^{|\mathcal{R}|+1} H(S_{r_j} | BX^T, S_{\{r_1, \dots, r_{j-1}\}}) \\ = \sum_{j=1}^{|\mathcal{R}|+1} I(S_{r_j}; BX^T, S_{\{r_1, \dots, r_{j-1}\}}),$$

from the chain rule [8, Ch. 2, p. 16]. Since the mutual information is nonnegative [8, Ch. 2, p. 27], we have  $I(S_{\mathcal{R}'}; BX^T) = 0$  if and only if  $I(S_{r_j}; BX^T, S_{\{r_1, \dots, r_{j-1}\}}) = 0$  for all  $r_j \in \mathcal{R}'$ . By substituting  $i = r_j$  in (33), we always have  $I(S_{r_j}; BX^T, S_{\{r_1, \dots, r_{j-1}\}}) = 0$  only for  $r_j$  if  $|\mathcal{R}| + k < M_1(\mathcal{D}_{2,r_j}^\perp, \mathcal{D}_{1,r_j}^\perp)$ . Thus, we always have  $I(S_{\mathcal{R}'}; BX^T) = 0$  for arbitrary  $k$  and  $\mathcal{R}'$  whenever  $|\mathcal{R}| + k < \min\{M_1(\mathcal{D}_{2,i}^\perp, \mathcal{D}_{1,i}^\perp) : 1 \leq i \leq l\}$  holds. Therefore, we prove that the universal  $\omega$ -security is attained whenever  $\omega < \min\{M_{R,1}(\mathcal{D}_{2,i}^\perp, \mathcal{D}_{1,i}^\perp) : 1 \leq i \leq l\}$ , and we have (22). ■

## APPENDIX C DERIVATION OF THE MAIN THEOREMS OF UNIVERSAL ERROR-CORRECTION CAPABILITY

In this appendix, we first briefly review Silva et al.'s approach [35, Section III]. Next, by using their approach, we analyze the error correction capability of the nested coset coding scheme over the coherent network coding system and derive Theorem 38. We finally extend the analysis to the noncoherent systems and also derive Proposition 40. Here we note that these derivations of theorems in Section IV are natural generalizations of the work in [35] to the error correction of the nested coset coding scheme.

### A. Brief Review of Silva et al.'s Approach

First we give a brief review of the approach of [35, Section III]. Consider a transmission of data over a channel in which there exists an adversary. Let the channel be specified by a finite input alphabet  $\mathcal{P}$  (e.g., a code), a finite output alphabet  $\mathcal{Q}$  (e.g., a vector space), and a collection of fan-out sets  $\mathcal{Q}_P \subseteq \mathcal{Q}$  for all  $P \in \mathcal{P}$  (e.g., a collection of cosets). For each input  $P \in \mathcal{P}$ , the output  $Q$  of the channel is constrained to be in  $\mathcal{Q}_P$  but is otherwise arbitrarily chosen by an adversary. A decoder for  $\mathcal{P}$  is any function  $\hat{P} : \mathcal{Q} \rightarrow \mathcal{P} \cup \{f\}$ , where  $f \notin \mathcal{P}$  denotes a decoding failure, i.e., detected errors. When  $P \in \mathcal{P}$  is transmitted and  $Q \in \mathcal{Q}_P$  is received, a decoder is said to be *successful* if  $\hat{P}(Q) = P$ . We also say that a decoder is *infallible* if it is successful for all  $Q \in \mathcal{Q}_P$  and all  $P \in \mathcal{P}$ .

Assume that the fan-out sets for a input  $P$  is given as

$$\mathcal{Q}_P = \{Q \in \mathcal{Q} : \Delta(P, Q) \leq t\},$$

for some  $\Delta : \mathcal{P} \times \mathcal{Q} \rightarrow \mathbb{N}$ . The value  $\Delta(P, Q)$  is called the *discrepancy* between  $P$  and  $Q$  for the given channel, which represents the minimum effort required for an adversary in the channel to transform  $P$  to  $Q$ . The value  $t$  represents the maximum effort of the adversary allowed in the channel. The problem is to decode  $P$  from  $Q$  by correcting at most

$t$  discrepancy. Then, the *minimum-discrepancy decoder* is defined by

$$\hat{P} = \arg \min_{P \in \mathcal{P}} \Delta(P, Q).$$

The relation between the discrepancy function and the error correction capability of this decoder was given in [35] as follows.

**Definition 51** ([35, Definition 1]). For a discrepancy function  $\Delta : \mathcal{P} \times \mathcal{Q} \rightarrow \mathbb{N}$ , let  $\delta(P, P') = \min \{\Delta(P, Q) + \Delta(P', Q) : Q \in \mathcal{Q}\}$ . Then,  $\Delta$  is said to be *normal* if, for all  $P, P' \in \mathcal{P}$  and all  $0 \leq i \leq \delta(P, P')$ , there exists some  $Q \in \mathcal{Q}$  such that  $\Delta(P, Q) = i$  and  $\Delta(P', Q) = \delta(P, P') - i$ .

**Theorem 52** ([35, Proposition 1, Theorem 3]). Let  $\delta(\mathcal{P}) = \min \{\delta(P, P') : P, P' \in \mathcal{P}, P \neq P'\}$ . Suppose  $\Delta(\cdot, \cdot)$  is normal. Then, the minimum discrepancy decoder  $\hat{P}$  is infallible if and only if  $t \leq \lfloor (\delta(\mathcal{P}) - 1)/2 \rfloor$ .

### B. How to Prove Theorem 38

By applying the above approach [35, Section III] to the secure network coding over the coherent network coding system in Section IV-A, this subsection derives Theorem 38, i.e., the universal error correction capability of the nested coset coding scheme with  $C_1, C_2$  for given  $A$ , expressed in terms of the first RGRW.

Recall that the received packets  $Y$  are given by  $Y^T = AX^T + DZ^T$  in the setup of Section III-B, and that  $X \in \mathbb{F}_{q^m}^n$  is chosen from a set  $\mathcal{X}_S \in \mathcal{P}_S$  corresponding to  $S \in \mathcal{S}$  by a certain coding scheme defined in Definition 36. Note that we do not restrict the coding scheme to the nested coset coding scheme here. From now on, we write  $\mathcal{X} \triangleq \mathcal{X}_S$  for the sake of simplicity. Suppose that the transfer matrix  $A$  is known to the sink node as in Section IV-A. Here, we define the discrepancy function between  $\mathcal{X}$  and  $Y$  for given  $A$  by

$$\begin{aligned} \Delta_A(\mathcal{X}, Y) \\ \triangleq \min \left\{ r \in \mathbb{N} : \exists D \in \mathbb{F}_q^{N \times r}, \exists Z \in \mathbb{F}_{q^m}^r, \exists X \in \mathcal{X}, Y^T = AX^T + DZ^T \right\}. \end{aligned} \quad (34)$$

This definition of  $\Delta_A(\mathcal{X}, Y)$  represents the minimum number  $r$  of error packets  $Z$  required to be injected in order to transform at least one element of  $\mathcal{X}$  into  $Y$ , as [35, (9)]. For the discrepancy function  $\Delta_A(\mathcal{X}, Y)$ , the minimum discrepancy decoder is given as

$$\hat{\mathcal{X}} = \arg \min_{\mathcal{X} \in \mathcal{P}_S} \Delta_A(\mathcal{X}, Y).$$

Note that “the minimum discrepancy decoder  $\hat{P}$  is infallible” in Theorem 52 means that for the discrepancy function  $\Delta_A(\mathcal{X}, Y)$ , “any  $t$  error packets can be corrected by the coding scheme for given  $A$  using the minimum discrepancy decoder  $\hat{\mathcal{X}}$ .” In the following, we will show that  $\Delta_A(\mathcal{X}, Y)$  is normal.

We define the  $\Delta$ -distance [35] between  $\mathcal{X}$  and  $\mathcal{X}'$ , induced by  $\Delta_A(\mathcal{X}, Y)$ , as

$$\delta_A(\mathcal{X}, \mathcal{X}') \triangleq \min \left\{ \Delta_A(\mathcal{X}, Y) + \Delta_A(\mathcal{X}', Y) : Y \in \mathbb{F}_{q^m}^N \right\}, \quad (35)$$

for  $\mathcal{X}, \mathcal{X}' \in \mathcal{P}_S$ . Let  $\delta_A(\mathcal{P}_S)$  be the minimum  $\Delta$ -distance given by

$$\delta_A(\mathcal{P}_S) \triangleq \min \{ \delta_A(\mathcal{X}, \mathcal{X}') : \mathcal{X}, \mathcal{X}' \in \mathcal{P}_S, \mathcal{X} \neq \mathcal{X}' \}.$$

**Lemma 53** ([35, Lemma 4]).

$$\min \left\{ r \in \mathbb{N} : D \in \mathbb{F}_q^{N \times r}, Z \in \mathbb{F}_{q^m}^r, Y^T = AX^T + DZ^T \right\} = d_R(XA^T, Y).$$

**Lemma 54.**  $\Delta_A(\mathcal{X}, Y) = \min \{ d_R(XA^T, Y) : X \in \mathcal{X} \}$ .

*Proof:* From Lemma 53, we have

$$\begin{aligned} \Delta_A(\mathcal{X}, Y) \\ &= \min \left\{ r \in \mathbb{N} : D \in \mathbb{F}_q^{N \times r}, Z \in \mathbb{F}_{q^m}^r, X \in \mathcal{X}, Y^T = AX^T + DZ^T \right\} \\ &= \min \left\{ \min \left\{ r \in \mathbb{N} : D \in \mathbb{F}_q^{N \times r}, Z \in \mathbb{F}_{q^m}^r, Y^T = AX^T + DZ^T \right\} : X \in \mathcal{X} \right\} \\ &= \min \left\{ d_R(XA^T, Y) : X \in \mathcal{X} \right\}. \end{aligned}$$

■

**Lemma 55.** For  $\mathcal{X}, \mathcal{X}' \in \mathcal{P}_S$ , we have

$$\delta_A(\mathcal{X}, \mathcal{X}') = \min \left\{ d_R(XA^T, X'A^T) : X \in \mathcal{X}, X' \in \mathcal{X}' \right\}. \quad (36)$$

*Proof:* First we have

$$\begin{aligned} \delta_A(\mathcal{X}, \mathcal{X}') \\ &= \min \left\{ \Delta_A(\mathcal{X}, Y) + \Delta_A(\mathcal{X}', Y) : Y \in \mathbb{F}_{q^m}^N \right\} \\ &= \min \left\{ \min \left\{ d_R(XA^T, Y) : X \in \mathcal{X} \right\} + \right. \\ &\quad \left. \min \left\{ d_R(X'A^T, Y) : X' \in \mathcal{X}' \right\} : Y \in \mathbb{F}_{q^m}^N \right\} \\ &= \min \left\{ d_R(XA^T, Y) + d_R(X'A^T, Y) : X \in \mathcal{X}, X' \in \mathcal{X}', Y \in \mathbb{F}_{q^m}^N \right\}. \end{aligned} \quad (37)$$

The rank distance satisfies the triangle inequality  $d_R(XA^T, X'A^T) \leq d_R(XA^T, Y) + d_R(X'A^T, Y)$  for  $\forall Y \in \mathbb{F}_{q^m}^N$  [15]. This lower bound can be achieved by choosing, e.g.,  $Y = XA^T$ . Therefore, from (37), we have (36). ■

**Lemma 56.** The discrepancy function  $\Delta_A(\mathcal{X}, Y)$  is normal.

*Proof:* Let  $\mathcal{X}, \mathcal{X}' \in \mathcal{P}_S$  and let  $0 \leq i \leq d = \delta_A(\mathcal{X}, \mathcal{X}')$ . Then,  $d = \min \{ d_R(XA^T, X'A^T) : X \in \mathcal{X}, X' \in \mathcal{X}' \}$  from Lemma 55. Let  $\bar{X} \in \mathcal{X}$  and  $\bar{X}' \in \mathcal{X}'$  be vectors satisfying  $d = d_R(\bar{X}A^T, \bar{X}'A^T)$ . Here, we can always find two vectors  $W, W' \in \mathbb{F}_{q^m}^N$  such that  $W + W' = (\bar{X}' - \bar{X})A^T$ ,  $\dim_{\mathbb{F}_q} \mathfrak{S}(W) = i$  and  $\dim_{\mathbb{F}_q} \mathfrak{S}(W') = d - i$ , as shown in the proof of [35, Theorem 6]. Taking  $\bar{Y} = \bar{X}A^T + W = \bar{X}'A^T - W'$ , we have  $d_R(\bar{X}A^T, \bar{Y}) = i$  and  $d_R(\bar{X}'A^T, \bar{Y}) = d - i$ . We thus obtain  $\Delta_A(\mathcal{X}, \bar{Y}) \leq i$  and  $\Delta_A(\mathcal{X}', \bar{Y}) \leq d - i$  from Lemma 54. On the other hand, since  $\delta_A(\mathcal{X}, \mathcal{X}') = d$ , we have  $\Delta_A(\mathcal{X}, Y) + \Delta_A(\mathcal{X}', Y) \geq d$  for any  $Y \in \mathbb{F}_{q^m}^N$  from (35). Therefore,  $\Delta_A(\mathcal{X}, \bar{Y}) = i$  and  $\Delta_A(\mathcal{X}', \bar{Y}) = d - i$  hold. ■

As [35, Theorem 7] obtained by [35, Theorems 3 and 6], we have Proposition 57 from Theorem 52 and Lemma 56 by the approach of Appendix C-A.

**Proposition 57.** Consider the  $t$ -error  $(n \times m)_q$  linear network in Definition 20. Suppose that for a secret message  $S \in \mathbb{F}_{q^m}^l$ , the

transmitted  $n$  packets  $X \in \mathcal{X}$  are generated by a coding scheme defined in Definition 36. Then, the minimum discrepancy decoder for  $\Delta_A(\mathcal{X}, Y)$  is infallible for any fixed  $A$  if and only if  $t \leq \lfloor (\delta_A(\mathcal{P}_S) - 1)/2 \rfloor$ . ■

This proposition implies that the coding scheme given in Definition 36 is guaranteed to determine the unique set  $\mathcal{X}$  against any  $t$  packet errors for any fixed  $A$  if and only if  $\delta_A(\mathcal{P}_S) > 2t$ . Here we note that if  $\mathcal{X}$  is uniquely determined,  $S$  is also uniquely determined from Definition 36.

In the following, we restrict the coding scheme to the nested coset coding scheme with  $C_1$  and  $C_2$ , and present a special case of Proposition 57 expressed in terms of the RGRW. That is, we set  $\mathcal{S} = \mathbb{F}_{q^m}^l$  and  $\mathcal{P}_S = C_1/C_2$  as defined in Definition 21.

**Lemma 58.**

$$\delta_A(C_1/C_2) = \min\{d_R(XA^T, X'A^T) : X, X' \in C_1, X' - X \notin C_2\}.$$

*Proof:*

$$\begin{aligned} \delta_A(C_1/C_2) &= \min\{\delta_A(\mathcal{X}, \mathcal{X}') : \mathcal{X}, \mathcal{X}' \in C_1/C_2, \mathcal{X} \neq \mathcal{X}'\} \\ &= \min\left\{\min\{d_R(XA^T, X'A^T) : X \in \mathcal{X}, X' \in \mathcal{X}'\} : \right. \\ &\quad \left. \mathcal{X}, \mathcal{X}' \in C_1/C_2, \mathcal{X} \neq \mathcal{X}'\right\} \\ &= \min\{d_R(XA^T, X'A^T) : X \in \mathcal{X} \in C_1/C_2, X' \in \mathcal{X}' \in C_1/C_2, \mathcal{X} \neq \mathcal{X}'\} \\ &= \min\{d_R(XA^T, X'A^T) : X, X' \in C_1, X' - X \notin C_2\}. \end{aligned}$$

**Lemma 59** ([28, Ch. 4, p. 211], [35]). For an arbitrary vector  $x \in \mathbb{F}_{q^m}^n$  and an arbitrary matrix  $A \in \mathbb{F}_q^{N \times n}$ , we have  $\dim_{\mathbb{F}_q} \mathfrak{S}(xA^T) \geq [\dim_{\mathbb{F}_q} \mathfrak{S}(x) + \text{rank } A - n]^+$ .

**Lemma 60.** Fix  $x \in \mathbb{F}_{q^m}^n$  and  $\rho \in \{0, \dots, n\}$  arbitrarily. Then, there always exists  $A \in \mathbb{F}_q^{N \times n}$  with  $\text{rank } A = n - \rho$  that satisfies the equality  $\dim_{\mathbb{F}_q} \mathfrak{S}(xA^T) = [\dim_{\mathbb{F}_q} \mathfrak{S}(x) - \rho]^+$  in Lemma 59.

*Proof:* First represent an  $n$ -dimensional vector  $x \in \mathbb{F}_{q^m}^n$  over  $\mathbb{F}_{q^m}$  as an  $m \times n$  matrix over the base field  $\mathbb{F}_q$ , denoted by  $M_x \in \mathbb{F}_q^{m \times n}$ . Here we note that  $\dim_{\mathbb{F}_q} \mathfrak{S}(xA^T) = \text{rank } M_x A^T$ . We define by  $\langle M_x \rangle \subseteq \mathbb{F}_q^n$  and  $\langle A \rangle \subseteq \mathbb{F}_q^n$  row spaces of  $M_x$  and  $A$  over  $\mathbb{F}_q$ , respectively. The rank of  $M_x A^T$  is given by  $\text{rank } M_x A^T = \text{rank } A - \dim(\langle M_x \rangle^\perp \cap \langle A \rangle)$  [28, Ch. 4, p. 210], where  $\langle M_x \rangle^\perp \in \mathbb{F}_q^n$  is the dual of  $\langle M_x \rangle$  over  $\mathbb{F}_q^n$ . If  $\dim \langle M_x \rangle^\perp \leq n - \rho$ , i.e., if  $\text{rank } M_x = \dim_{\mathbb{F}_q} \mathfrak{S}(x) \geq \rho$ , we can always choose  $A$  satisfying  $\text{rank } A = n - \rho$  and  $\langle A \rangle \supseteq \langle M_x \rangle^\perp$ . Then, for such  $A$ , we have  $\langle M_x \rangle^\perp = \langle M_x \rangle^\perp \cap \langle A \rangle$  and hence

$$\begin{aligned} \text{rank } M_x A^T &= \underbrace{\text{rank } A}_{n-\rho} - \underbrace{\dim(\langle M_x \rangle^\perp \cap \langle A \rangle)}_{=\langle M_x \rangle^\perp} \\ &= n - \rho - \underbrace{\dim \langle M_x \rangle^\perp}_{=n-\text{rank } M_x} \\ &= \text{rank } M_x - \rho \\ &= \dim_{\mathbb{F}_q} \mathfrak{S}(x) - \rho. \end{aligned}$$

On the other hand, if  $\dim \langle M_x \rangle^\perp > n - \rho$ , i.e., if  $\text{rank } M_x = \dim_{\mathbb{F}_q} \mathfrak{S}(x) < \rho$ , we can always choose  $A$  satisfying

$\text{rank } A = n - \rho$  and  $\langle A \rangle \subsetneq \langle M_x \rangle^\perp$ . Then, for such  $A$ , we have  $\langle A \rangle = \langle M_x \rangle^\perp \cap \langle A \rangle$  and hence

$$\text{rank } M_x A^T = \text{rank } A - \underbrace{\dim(\langle M_x \rangle^\perp \cap \langle A \rangle)}_{=\text{rank } A} = 0.$$

Therefore, the lemma is established. ■

For the rank deficiency  $\rho = n - \text{rank } A$ , we have  $[d_R(X, X') - \rho]^+ \leq d_R(XA^T, X'A^T)$  from Lemma 59, and there always exists  $A \in \mathbb{F}_q^{N \times n}$  depending on  $(X, X')$  such that the equality holds from Lemma 60. Thus, from Lemma 58, we have the following inequalities for an arbitrarily fixed  $A$  with  $\text{rank } A = n - \rho$ .

$$\begin{aligned} \min_{A \in \mathbb{F}_q^{N \times n} : \text{rank } A = n - \rho} \delta_A(C_1/C_2) &= [\min\{d_R(X, X') : X, X' \in C_1, X' - X \notin C_2\} - \rho]^+ \\ &= [\min\{d_R(X, 0) : X \in C_1, X \notin C_2\} - \rho]^+ \\ &= [M_{R,1}(C_1, C_2) - \rho]^+. \quad (\text{by Lemma 12}) \end{aligned}$$

Thus, for  $1 \leq i \leq \rho$ , we have

$$\min_{A : \text{rank } A = n - \rho} \delta_A(C_1/C_2) < \min_{A : \text{rank } A = n - (\rho - i)} \delta_A(C_1/C_2),$$

and hence we obtain

$$\begin{aligned} \min_{A : \text{rank } A \geq n - \rho} \delta_A(C_1/C_2) &= \min_{A : \text{rank } A = n - \rho} \delta_A(C_1/C_2) \\ &= [M_{R,1}(C_1, C_2) - \rho]^+. \end{aligned}$$

Therefore, from Proposition 57 for  $\mathcal{P}_S = C_1/C_2$ , Theorem 38 is proved. ■

### C. How to Prove Proposition 40

In this subsection, we extend the analysis for the coherent network coding system, given in Appendix C-B, to one for the noncoherent system in the setup of Section IV-B. We derive Proposition 40, i.e., an expression for the error correction capability of the lifting construction [38] of the nested coset coding scheme in terms of the RGRW. Here we recall that only one sink node has been assumed without loss of generality.

As in Appendix C-B, we first consider the correction capability of the generalized coding scheme defined in Definition 36. Recall that in the noncoherent network coding system, the transfer matrix  $A$  at the sink node is unknown. Define the discrepancy function between  $\mathcal{X} = \mathcal{X}_S \in \mathcal{P}_S$  and  $Y$  for unknown  $A$  with at most  $\rho$  rank deficiency, as follows:

$$\begin{aligned} \Delta_\rho(\mathcal{X}, Y) &\triangleq \min\left\{r \in \mathbb{N} : \exists D \in \mathbb{F}_q^{N \times r}, \exists Z \in \mathbb{F}_{q^m}^r, \exists A \in \mathbb{F}_q^{N \times n}, \exists X \in \mathcal{X}, \right. \\ &\quad \left. Y^T = AX^T + DZ^T, \text{rank } A \geq n - \rho\right\} \\ &= \min\{\delta_A(\mathcal{X}, Y) : A \in \mathbb{F}_q^{N \times n}, \text{rank } A \geq n - \rho\}, \quad (38) \end{aligned}$$

where the second equality is obtained by (34). The definition of  $\Delta_\rho(\mathcal{X}, Y)$  represents the minimum number  $r$  of error packets  $Z$  required to be injected in order to transform at least one element of  $\mathcal{X}$  into  $Y$ , for at least one transfer matrix

$A$  satisfying  $\text{rank } A \geq n - \rho$ . For  $\Delta_\rho(X, Y)$ , the minimum discrepancy decoder is given as

$$\hat{X} = \arg \min_{X \in \mathcal{P}_S} \Delta_\rho(X, Y). \quad (39)$$

We also define  $\Delta$ -distance between  $X$  and  $X'$ , induced by  $\Delta_p(X, Y)$ , as

$$\begin{aligned} & \triangleq \min \left\{ \Delta_\rho(\mathcal{X}, Y) + \Delta_{\rho'}(\mathcal{X}', Y) : Y \in \mathbb{F}_{q^m}^N \right\} \\ & = \min \left\{ \Delta_A(\mathcal{X}, Y) + \Delta_{A'}(\mathcal{X}', Y) : A, A' \in \mathbb{F}_q^{N \times n}, Y \in \mathbb{F}_{q^m}^N, \right. \\ & \quad \left. \text{rank } A \geq n - \rho, \text{rank } A' \geq n - \rho' \right\}, \end{aligned}$$

where the second equality is obtained by (38). Let  $\delta_\rho(\mathcal{P}_S)$  be the minimum  $\Delta$ -distance given by

$$\delta_\rho(\mathcal{P}_S) \triangleq \min \left\{ \delta_\rho(\mathcal{X}, \mathcal{X}') : \mathcal{X}, \mathcal{X}' \in \mathcal{P}_S, \mathcal{X} \neq \mathcal{X}' \right\}.$$

Observe that from Lemma 54, we can rewrite  $\Delta_\rho(X, Y)$  as

$$\Delta_\rho(\mathcal{X}, Y) = \min \left\{ d_R(XA^T, Y) : X \in \mathcal{X}, A \in \mathbb{F}_q^{N \times n}, \text{rank } A \geq n - \rho \right\}. \quad (40)$$

Also, from Lemma 55, we have

$$\begin{aligned} & \delta_\rho(\mathcal{X}, \mathcal{X}') \\ &= \min \left\{ d_R(XA^T, X'A'^T) : X \in \mathcal{X}, X' \in \mathcal{X}', A, A' \in \mathbb{F}_q^{N \times n}, \right. \\ & \quad \left. \text{rank } A \geq n - \rho, \text{rank } A' \geq n - \rho \right\}. \end{aligned} \quad (41)$$

**Lemma 61.** The discrepancy function  $\Delta_\rho(\mathcal{X}, Y)$  is normal.

*Proof:* Let  $\mathcal{X}, \mathcal{X}' \in \mathcal{P}_{\mathcal{S}}$  and let  $0 \leq i \leq d = \delta_{\rho}(\mathcal{X}, \mathcal{X}')$ . Let  $A, A' \in \mathbb{F}_q^{N \times n}$  be fixed matrices that minimize (41), and then suppose that  $\bar{X} \in \mathcal{X}$  and  $\bar{X}' \in \mathcal{X}'$  are vectors satisfying  $d = d_R(\bar{X}A^T, \bar{X}'A'^T)$ . Here, we can always find two vectors  $W, W' \in \mathbb{F}_q^m$  such that  $W + W' = \bar{X}'A'^T - \bar{X}A^T$ ,  $\dim_{\mathbb{F}_q} \mathfrak{S}(W) = i$  and  $\dim_{\mathbb{F}_q} \mathfrak{S}(W') = d - i$ , as shown in the proof of [35, Theorem 13]. Taking  $\tilde{Y} = \bar{X}A^T + W = \bar{X}'A'^T - W'$ , we have  $d_R(\bar{X}A^T, \tilde{Y}) = i$  and  $d_R(\bar{X}'A'^T, \tilde{Y}) = d - i$ . We thus obtain  $\Delta_{\rho}(\mathcal{X}, \tilde{Y}) \leq i$  and  $\Delta_{\rho}(\mathcal{X}', \tilde{Y}) \leq d - i$  from (40). On the other hand, since  $\delta_{\rho}(\mathcal{X}, \mathcal{X}') = d$ , we have  $\Delta_{\rho}(\mathcal{X}, Y) + \Delta_{\rho}(\mathcal{X}', Y) \geq d$  for any  $Y \in \mathbb{F}_q^m$  from (38). Therefore,  $\Delta_{\rho}(\mathcal{X}, \tilde{Y}) = i$  and  $\Delta_{\rho}(\mathcal{X}', \tilde{Y}) = d - i$  hold.  $\blacksquare$

As [35, Theorem 14], we have Proposition 62 from Theorem 52 and Lemma 61 by the approach of Appendix C-A.

Then, we have the following proposition by the approach of Appendix C-A.

**Proposition 62.** Consider the  $t$ -error  $(n \times m)_q$  linear network in Definition 20. Suppose that for a secret message  $S \in \mathcal{S}$ , the transmitted  $n$  packets  $X \in \mathcal{X}$  are generated by a coding scheme defined in Definition 36. Then, the minimum discrepancy decoder for  $\Delta_\rho(X, Y)$  is infallible if and only if  $t \leq \lfloor (\delta_\rho(\mathcal{P}_S) - 1)/2 \rfloor$ . ■

This proposition implies that the coding scheme given in Definition 36 is guaranteed to determine the unique set  $X$  against any  $t$  packet errors if and only if  $\delta_\rho(\mathcal{P}_S) > 2t$ .

In the following, we restrict  $X$  to that generated by the lifting construction [38] of the nested coset coding scheme,

as described in Section IV-B, and we shall express the error correction capability given in Proposition 62 in terms of the RGRW. Recall that in the lifting construction of the nested coset coding scheme,  $C_1 \subseteq \mathbb{F}_{q^m}^n$  and  $C_2 \subsetneq C_1$  are a linear code and its subcode for  $\tilde{m} = m - n$ , respectively. Also recall that  $\mathcal{S} = \mathbb{F}_{q^m}^l$ ,  $\mathcal{X}_\mathcal{S} = \mathcal{X}_{\mathcal{S}, \text{lift}}$  and  $\mathcal{P}_\mathcal{S} = \mathcal{P}_{\text{lift}}$  defined in (23). We will consider the error correction capability in this setup. Here, we introduce the following proposition given in [35].

**Proposition 63** ([35, Proposition 18]). For  $X, X' \in \mathbb{F}_{q^m}^n$ , we have

$$\begin{aligned} & \min \left\{ d_R(XA^T, X'A'^T) : A, A' \in \mathbb{F}_q^{N \times n}, \right. \\ & \quad \left. \text{rank } A \geq n - \rho, \text{rank } A' \geq n - \rho \right\} \\ &= \left[ \dim_{\mathbb{F}_q} (\mathfrak{S}(X) + \mathfrak{S}(X')) - \min \left\{ \dim_{\mathbb{F}_q} \mathfrak{S}(X), \dim_{\mathbb{F}_q} \mathfrak{S}(X') \right\} - \rho \right]^+. \end{aligned}$$

From this proposition, we have the following lemma.

**Lemma 64.**

$$\delta_\rho(\mathcal{P}_{\text{lift}}) = \min \left\{ \left[ d_R(\tilde{X}, \tilde{X}') - \rho \right]^+ : \tilde{X}, \tilde{X}' \in C_1, \tilde{X}' - \tilde{X} \notin C_2 \right\}.$$

*Proof:* Since the transmitted packets are generated by the lifting construction of the nested coset coding scheme, we have  $\dim_{\mathbb{F}_q} \mathfrak{S}(X) = n$  for all  $X \in \mathcal{X}$  and for all  $X \in \mathcal{P}_{\text{lift}}$ . For  $X \in \mathcal{X} \in \mathcal{P}_{\text{lift}}$  and  $X' \in \mathcal{X}' \in \mathcal{P}_{\text{lift}}$ , we thus have

$$\begin{aligned}
& \dim_{\mathbb{F}_q}(\mathfrak{S}(X) + \mathfrak{S}(X')) - \min \left\{ \underbrace{\dim_{\mathbb{F}_q} \mathfrak{S}(X)}_{=n}, \underbrace{\dim_{\mathbb{F}_q} \mathfrak{S}(X')}_{=n} \right\} - \rho \\
&= \text{rank} \begin{bmatrix} I & I \\ \phi_{\bar{m}}(\tilde{X}) & \phi_{\bar{m}}(\tilde{X}') \end{bmatrix} - \min\{n, n\} - \rho \\
&= \text{rank} \underbrace{\begin{bmatrix} I & 0 \\ \phi_{\bar{m}}(\tilde{X}) & \phi_{\bar{m}}(\tilde{X}') - \phi_{\bar{m}}(\tilde{X}) \end{bmatrix}}_{=n + \text{rank}(\phi_{\bar{m}}(\tilde{X}') - \phi_{\bar{m}}(\tilde{X}))} - n - \rho \\
&= \text{rank} \underbrace{(\phi_{\bar{m}}(\tilde{X}') - \phi_{\bar{m}}(\tilde{X}))}_{=\phi_{\bar{m}}(\tilde{X}' - \tilde{X})} - \rho \\
&= \dim_{\mathbb{F}_q} \mathfrak{S}(\tilde{X}' - \tilde{X}) - \rho \\
&= d_R(\tilde{X}, \tilde{X}') - \rho,
\end{aligned}$$

where in the first equality,  $X$  and  $X' \in \mathbb{F}_{q^m}^{n \times m}$  are regarded as  $m \times n$  matrices over  $\mathbb{F}_q$ ,  $X^T = [I \quad \phi_m(\tilde{X})^T]$  and  $X'^T = [I \quad \phi_m(\tilde{X}')^T]$ , respectively. Thus, by combining Proposition 63 and (41), we have the following equation for  $X_{S, \text{lift}}, X_{S', \text{lift}} \in \mathcal{P}_{\text{lift}}$ .

$$\begin{aligned} & \delta_\rho(\mathcal{X}_{S,\text{lift}}, \mathcal{X}_{S',\text{lift}}) \\ &= \min \left\{ \left[ d_R(\widetilde{X}, \widetilde{X}') - \rho \right]^+ : X \in \mathcal{X}_{S,\text{lift}}, X' \in \mathcal{X}_{S',\text{lift}} \right\} \\ &= \min \left\{ \left[ d_R(\widetilde{X}, \widetilde{X}') - \rho \right]^+ : \widetilde{X} \in \psi(S), \widetilde{X}' \in \psi(S') \right\}. \text{ (by (23))} \end{aligned}$$

Therefore, we finally have

$$\begin{aligned}
& \delta_\rho(\mathcal{P}_{\text{lift}}) \\
&= \min \left\{ \delta_\rho(X, X') : X, X' \in \mathcal{P}_{\text{lift}}, X \neq X' \right\} \\
&= \min \left\{ \min \left\{ \left[ d_R(\tilde{X}, \tilde{X}') - \rho \right]^+ : \tilde{X} \in \psi(S), \tilde{X}' \in \psi(S') \right\} : \right. \\
&\quad \left. \psi(S), \psi(S') \in C_1/C_2, \psi(S) \neq \psi(S') \right\} \\
&= \min \left\{ \left[ d_R(\tilde{X}, \tilde{X}') - \rho \right]^+ : \tilde{X} \in \psi(S) \in C_1/C_2, \right. \\
&\quad \left. \tilde{X}' \in \psi(S') \in C_1/C_2, \psi(S) \neq \psi(S') \right\} \\
&= \min \left\{ \left[ d_R(\tilde{X}, \tilde{X}') - \rho \right]^+ : \tilde{X}, \tilde{X}' \in C_1, \tilde{X}' - \tilde{X} \notin C_2 \right\}.
\end{aligned}$$

From Lemma 64, we have

$$\begin{aligned}
\delta_\rho(\mathcal{P}_{\text{lift}}) + \rho &= \min \left\{ d_R(\tilde{X}, \tilde{X}') : \tilde{X}, \tilde{X}' \in C_1, \tilde{X}' - \tilde{X} \notin C_2 \right\} \\
&= \min \left\{ d_R(\tilde{X}, 0) : \tilde{X} \in C_1, \tilde{X} \notin C_2 \right\} \\
&= M_{R,1}(C_1, C_2). \quad (\text{by Lemma 12})
\end{aligned}$$

Thus, from Proposition 62 for  $\mathcal{P}_S = \mathcal{P}_{\text{lift}}$ , Proposition 40 is proved. ■

#### ACKNOWLEDGMENT

The authors would like to thank Prof. Terence H. Chan for pointing out the fact that the conditions for zero mutual information are independent of the probability distribution of secret messages. The authors would also like to thank the Associate Editor and the anonymous reviewers for their many helpful comments which have greatly improved the presentation of this paper. A part of this research was done during the first author's stay at Palo Alto Research Center (PARC), CA, USA. He greatly appreciates the support by Dr. Ersin Uzun. Another part of this research was also done during the second author's stay at Aalborg University, Denmark. He greatly appreciates the support by Profs. Olav Geil and Diego Ruano.

#### REFERENCES

- [1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.
- [2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. AFIPS 1979 National Computer Conf.*, vol. 48, 1979, pp. 313–317.
- [3] N. Cai, "Valuable messages and random outputs of channels in linear network coding," in *Proc. 2009 IEEE Int. Symp. Information Theory*, Seoul, Korea, Jun./Jul. 2009, pp. 413–417.
- [4] N. Cai and T. Chan, "Theory of secure network coding," *Proc. IEEE*, vol. 99, no. 3, pp. 421–437, Mar. 2011.
- [5] N. Cai and R. W. Yeung, "A security condition for multi-source linear network coding," in *Proc. 2007 IEEE Int. Symp. Information Theory*, Nice, France, Jun. 2007, pp. 561–565.
- [6] —, "Secure network coding on a wiretap network," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424–435, Jan. 2011.
- [7] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan, "Secure computation from random error correcting codes," in *Advances in Cryptology – EUROCRYPT 2007*, ser. Lecture Notes in Computer Science, vol. 4515. Heidelberg, Germany: Springer-Verlag, 2007, pp. 291–310.
- [8] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York, NY, USA: Wiley-Interscience, Jan. 2006.
- [9] J. Ducoat, "Generalized rank weights : duality and Griesmer bound," presented at 11th Int. Conf. Finite Fields and Their Appl., Magdeburg, Germany, Jul. 2013. [Online]. Available: arXiv:1306.3899 [cs.IT]
- [10] I. M. Duursma and S. Park, "Coset bounds for algebraic geometric codes," *Finite Fields Appl.*, vol. 16, no. 1, pp. 36–55, Jan. 2010.
- [11] S. Y. 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.
- [12] J. Feldman, T. Malkin, R. A. Servedio, and C. Stein, "On the capacity of secure network coding," in *Proc. 42nd Annu. Allerton Conf. Communication, Control, and Computing*, Monticello, IL, USA, Sep. 2004.
- [13] G. D. Forney, Jr., "Dimension/length profiles and trellis complexity of linear block codes," in *IEEE Trans. Inf. Theory*, vol. 40, no. 6, pp. 1741–1752, Mar. 1994.
- [14] C. Fragouli and E. Soljanin, *Network Coding Fundamentals*. Hanover, MA, USA: Now Publishers, 2007.
- [15] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Inf. Transm.*, vol. 21, no. 1, pp. 1–12, 1985.
- [16] M. Gadouleau and Z. Yan, "Properties of rank metric codes," Feb. 2007. [Online]. Available: arXiv:cs/0702077 [cs.IT]
- [17] K. Harada and H. Yamamoto, "Strongly secure linear network coding," *IEICE Trans. Fundamentals*, vol. E91-A, no. 10, pp. 2720–2728, Oct. 2008. [Online]. Available: http://dx.doi.org/10.1093/ietf/fec/e91-a.10.2720
- [18] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.
- [19] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, 2003.
- [20] 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*, vol. E95-A, no. 11, pp. 2067–2075, Nov. 2012. [Online]. Available: http://dx.doi.org/10.1587/transfun.E95.A.2067
- [21] —, "Explicit construction of universal strongly secure network coding via MRD codes," in *Proc. 2012 IEEE Int. Symp. Information Theory*, Cambridge, MA, USA, Jul. 2012, pp. 1488–1492.
- [22] —, "New parameters of linear codes expressing security performance of universal secure network coding," in *Proc. 50th Annu. Allerton Conf. Communication, Control, and Computing*, Monticello, IL, USA, Oct. 2012, pp. 533–540. [Online]. Available: arXiv:1207.1936 [cs.IT]
- [23] S.-Y. R. Li and R. W. Yeung, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.
- [24] P. Loidreau, "Properties of codes in rank metric," in *Proc. 11th Int. Workshop on Algebraic and Combinatorial Coding Theory*, Pamporovo, Bulgaria, 2008. [Online]. Available: arXiv:cs/0610057 [cs.DM]
- [25] Y. Luo, C. Mitpant, 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, Mar. 2005.
- [26] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
- [27] R. Matsumoto and M. Hayashi, "Secure multiplex network coding," in *Proc. 2011 Int. Symp. Network Coding*, Beijing, China, Jul. 2011, pp. 1–6.
- [28] C. D. Meyer, *Matrix Analysis and Applied Linear Algebra*. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, 2001.
- [29] 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.
- [30] M. Nishihara 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.
- [31] F. Oggier and A. Sboui, "On the existence of generalized rank weights," in *Proc. 2012 Int. Symp. Information Theory and Its Applications*, Honolulu, Hawaii, USA, Oct. 2012, pp. 406–410.
- [32] L. H. Ozarow and A. D. Wyner, "The wire-tap channel II," *AT&T Bell Labs. Tech. J.*, vol. 63, no. 10, pp. 2135–2157, Dec. 1984.
- [33] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [34] E. Shioji, R. Matsumoto, and T. Uyematsu, "Vulnerability of MRD-code-based universal secure network coding against stronger eavesdroppers," *IEICE Trans. Fundamentals*, vol. E93-A, no. 11, pp. 2026–2033, Nov. 2010. [Online]. Available: http://dx.doi.org/10.1587/transfun.E93.A.2026
- [35] D. Silva and F. R. Kschischang, "On metrics for error correction in network coding," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5479–5490, Dec. 2009.



- [36] —, “Universal weakly secure network coding,” in *Proc. 2009 IEEE Information Theory Workshop*, Volos, Greece, Jun. 2009, pp. 281–285.
- [37] —, “Universal secure network coding via rank-metric codes,” *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1124–1135, Feb. 2011.
- [38] D. Silva, F. R. Kschischang, and R. Koetter, “A rank-metric approach to error control in random network coding,” *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3951–3967, Sep. 2008.
- [39] H. Stichtenoth, “On the dimension of subfield subcodes,” *IEEE Trans. Inf. Theory*, vol. 36, no. 1, pp. 90–93, 1990.
- [40] W. R. Stevens, *TCP/IP Illustrated, Volume 1: The Protocols*. Boston, MA, USA: Addison-Wesley, 1994.
- [41] A. Subramanian and S. W. McLaughlin, “MDS codes on the erasure-erasure wiretap channel,” Feb. 2009. [Online]. Available: [arXiv:0902.3286 \[cs.IT\]](http://arxiv.org/abs/0902.3286)
- [42] V. K. Wei, “Generalized Hamming weights for linear codes,” *IEEE Trans. Inf. Theory*, vol. 37, no. 5, pp. 1412–1418, May 1991.
- [43] 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, 1985, [English translation: H. Yamamoto, “Secret sharing system using  $(k, L, n)$  threshold scheme,” *Electronics and Communications in Japan*, Part I, vol. 69, no. 9, pp. 46–54, (Scripta Technica, Inc.), Sep. 1986. [Online]. Available: <http://dx.doi.org/10.1002/ecja.4410690906>].
- [44] R. Zamir, S. Shamai, and U. Erez, “Nested linear/lattice codes for structured multiterminal binning,” *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1250–1276, Jun. 2002.
- [45] Z. Zhang and R. W. Yeung, “A general security condition for multi-source linear network coding,” in *Proc. 2009 IEEE Int. Symp. Information Theory*, Seoul, Korea, Jun./Jul. 2009, pp. 1155–1158.
- [46] Z. Zhang and B. Zhuang, “An application of the relative network generalized Hamming weight to erroneous wiretap networks,” in *Proc. 2009 IEEE Information Theory Workshop*, Taormina, Sicily, Italy, Oct. 2009, pp. 70–74.
- [47] Y. Zhu, B. Li, and J. Guo, “Multicast with network coding in application-layer overlay networks,” *IEEE J. Selected Areas in Comm.*, vol. 22, no. 1, pp. 107–120, Jan. 2004.

**Tomohiko Uyematsu** (M’95–SM’05) 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 Computer Engineering as professor. In 1992 and 1996, he was a visiting researcher at Supélec, France and Delft University of Technology, Netherlands, respectively. He was Technical Program Committee Co-Chair for the 2012 International Symposium on Information Theory and its Applications. He served as an Associate Editor for the IEEE Transactions on Information Theory in 2010–2013. He received the Achievement Award in 2008, and the Best Paper Award six times both from IEICE. His current research interests are in the areas of information theory, especially Shannon theory and multi-terminal information theory.

**Jun Kurihara** (M’13) received the B.E. degree in computer science, the M.E. degree in communication engineering and the Ph.D. degree in electrical and electronic engineering, all from Tokyo Institute of Technology, Tokyo, Japan, in 2004, 2006 and 2012 respectively. He joined KDDI Corp., Tokyo, Japan in April 2006. Since July 2006, he has been with KDDI R&D Laboratories, Inc., Saitama, Japan as a researcher. From 2013 to 2014, he was a visiting researcher at Palo Alto Research Center (PARC), Palo Alto, CA, USA. His research interests include coding theory, networking architecture and security. He received the Best Paper Award from IEICE in 2014.

**Ryutaroh Matsumoto** (M’00) 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 and 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 Computer Engineering, Tokyo Institute of Technology. His research interests include error-correcting codes, quantum information theory, information theoretic security, 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, 2011 and 2014.