Multiple Linear-Combination Security Network Coding

Yang Bai, Xuan Guang, and Raymond W. Yeung

Abstract

In this paper, we put forward the model of multiple linear-combination security multicast network coding, where the wiretapper desires to obtain some information on a predefined set of multiple linear combinations of the source symbols by eavesdropping any one but not more than one channel subset up to a certain size r, referred to as the *security level*. More precisely, in this model, i) the single source node generates source symbols over a finite field F and all the source symbols are required to be correctly decoded at all the sink nodes; and ii) the wiretapper, who can fully access any channel subset of size not larger than r, is not allowed to obtain any information about these linear combinations of the source symbols. For such a linear-combination security model, the security capacity is defined as the maximum average number of source symbols that can be securely multicast to all sink nodes for one use of the network under the linear-combination security constraint. We first show that $C_{\min}-1$ is the maximum security level such that the source symbols can be securely transmitted with a positive rate, where $C_{\min}$ denotes the smallest minimum cut capacity separating a sink node from the source node. For any nontrivial security level $1 \leq r \leq C_{\min}-1$, we prove upper bounds on the security capacity in terms of the ratio of the rank of the linear-combination security constraint to the number of source symbols. Further, we develop a general construction of linear security network codes. Based on the upper bounds obtained and the code construction, we fully characterize the security capacity for any security level and any linear-combination security constraint. Finally, we investigate the asymptotic behavior of the security capacity for a sequence of linear-combination security models and discuss the asymptotic optimality of our code construction.

Keywords: information-theoretical security; linear-combination security; network coding; secure network coding; security capacity; code construction; asymptotic behavior

I. Introduction

In 2000, Ahlswede *et al.* [1] proposed the general concept of network coding. In particular, they investigated the single-source multicast network coding problem, where the source symbols generated by a single source node are required to multicast to multiple sink nodes through a noiseless network

while the nodes in the network are allowed to process the received information. It was proved in [1] that if coding is applied at the intermediate nodes (rather than routing only), the source node can multicast source symbols to all the sink nodes at the theoretically maximum rate, i.e., the smallest minimum cut capacity separating a sink node from the source node, as the alphabet size of both the information source and the channel transmission symbol tends to infinity. In 2003, Li *et al.* [2] proved that linear network coding over a finite alphabet is sufficient for optimal multicast by means of a vector space approach. Independently, Koetter and Médard [3] developed an algebraic characterization of the linear network coding by means of a matrix approach. Jaggi *et al.* [4] further presented a deterministic polynomial-time algorithm for constructing a linear network code. For comprehensive discussions of network coding, we refer the reader to [5]–[10].

In the paradigm of network coding, information-theoretic security in network coding with the presence of a wiretapper is naturally considered (cf. [11]–[19], [21]–[25]), called the *secure network coding* problem. In the model of secure network coding over a wiretap network, i) the source node multicasts the source symbols to all the sink nodes which as legal users are required to correctly decode the source symbols; and ii) the wiretapper, who can access any one but not more than one wiretap set of communication channels, is not allowed to obtain any information about the source symbols. The classical information-theoretically secure models, e.g., Shannon's cipher system [26], secret sharing [27], [28] and the wiretap channel II [29], can be regarded as special cases of the secure network coding model. In particular, a wiretap network is called an *r-wiretap network* if the wiretapper can fully access an arbitrary subset of at most r edges, where the nonnegative integer r is called the *security level*.

In the model of secure network coding, to guarantee the required information-theoretic security, it is necessary to randomize the source symbols to combat the wiretapper. Cai and Yeung [11] presented a code construction for the r-wiretap network. El Rouayheb *et al.* [12] further showed that the Cai-Yeung code construction can be viewed as a network generalization of the code construction for wiretap channel II in [29]. Motivated by El Rouayheb *et al.*, Silva and Kschischang [13] proposed a universal design of security network codes based on rank-metric codes. For the constructions of security network codes in [11]–[13], the existing upper bounds on the minimum required alphabet size may be too large for implementation for certain applications in terms of computational complexity and storage requirement. Feldman *et al.* [30] showed that for a given security level, the alphabet size can be reduced by sacrificing a small fraction of the information rate. However, if the information rate is not sacrificed, whether it is possible to reduce the required alphabet size is considered as an open problem [12], [17]. Recently, Guang and Yeung [18] developed a systematic graph-theoretic approach to improve the upper bound on the minimum required alphabet size for the existence of secure network codes and the improvement is in general significant.

Subsequently, in order to tackle the problem of secure network coding when the information rate and the secure level may vary over time, Guang *et al.* [19] put forward local-encoding-preserving secure network coding where a family of secure linear network codes is called local-encoding-preserving if all the codes in this family use a common local encoding operation at each intermediate node in the network. They also constructed a family of local-encoding-preserving secure linear network codes applicable for all possible pairs of rate and security level. We note that the variable-rate linear network coding problem without security consideration was previously investigated by Fong and Yeung [20].

In this paper, we put forward the model of multiple linear-combination security network coding, where multiple linear combinations of the source symbols are required to be protected from the wiretapper. More precisely, in this model over an r-wiretap network, i) the single source node generates source symbols over a finite field F and all the source symbols are required to be correctly decoded at all the sink nodes; and ii) for a predefined set of linear combinations of the source symbols, the wiretapper, who can fully access any channel subset of size not larger than r, is not allowed to obtain any information about these linear combinations. For the above security model with the security level r, the (linear-combination) security capacity is defined as the maximum average number of source symbols that can be securely multicast to all the sink nodes for one use of the network under the above linear-combination security constraint. A model related to the current work is the one considered by Bhattad and Narayanan [24], which contains weakly secure network coding as a special case. The relation between the current work and Bhattad and Narayanan [24] will be discussed in Appendix A.

In this paper, we investigate the security capacity and the code construction for this model, and also analyze the asymptotic behavior of the security capacity and code construction for a sequence of linear-combination security models. The main contributions and organization of the paper are:

- In Section II, we formally present the model of linear-combination security network coding and also the preliminaries including the necessary notation and definitions.
- In Section III, we characterize the security capacity by considering different cases of the security level r. We first prove that $C_{\min}-1$ is the maximum security level such that the source symbols can be securely multicast to all sink nodes with a positive rate, where $C_{\min}$ is the smallest minimum cut capacity separating a sink node from the source node. So, the security capacity is zero for $r \geq C_{\min}$. For any nontrivial security level $1 \leq r \leq C_{\min}-1$, we prove upper bounds on the security capacity in terms of the ratio τ of the rank of the linear-combination security constraint to the number of source symbols.

  We further develop a systematic construction of linear security network codes, which is applicable

to an arbitrary linear-combination security model. Based on the obtained upper bounds and the developed code construction, we fully characterize the security capacity for any possible pair of the number of the source symbols and the linear-combination security constraint. We also determine the threshold value τ_0 such that there is no penalty on the security capacity compared with the capacity without any security consideration when the ratio τ is not larger than τ_0.

- In Section IV, we fully characterize the asymptotic behavior of the security capacity for a sequence of linear-combination security models and prove that our code construction is asymptotically optimal.
- We conclude in Section V with a summary of our results.

II. Preliminaries

Consider a communication network whose communication channels are point-to-point. The network is represented by a directed acyclic graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ and $\mathcal{E}$ are finite sets of nodes and edges, respectively. Here, an edge in the graph $\mathcal{G}$ corresponds to a point-to-point channel in the network. In the graph $\mathcal{G}$, multiple edges between two nodes are allowed. We assume that an element in a finite field F can be reliably transmitted on each edge for each use. We use $\mathrm{tail}(e)$ and $\mathrm{head}(e)$ to denote the *tail* node and the *head* node of an edge e, respectively. For a node $v \in \mathcal{V}$, we let $\mathrm{In}(v) = \{e \in \mathcal{E} : \mathrm{head}(e) = v\}$ and $\mathrm{Out}(v) = \{e \in \mathcal{E} : \mathrm{tail}(e) = v\}$, i.e., $\mathrm{In}(v)$ and $\mathrm{Out}(v)$ are the set of input edges and the set of output edges, respectively. Further, a sequence of edges $(e_1, e_2, \cdots, e_m)$ is called a (directed) *path* from the node $\mathrm{tail}(e_1)$ to the node $\mathrm{head}(e_m)$ if $\mathrm{tail}(e_i) = \mathrm{head}(e_{i-1})$ for $i = 2, 3, \cdots, m$. For two nodes u and v with $u \neq v$, an edge subset $C \subseteq \mathcal{E}$ is called a *cut* separating v from u if no path exists from u to v upon removing the edges in C. The *capacity* of a cut separating v from u is defined as the size of this cut. A cut C separating v from u is called a *minimum cut* separating v from u if there does not exist a cut C' separating v from u such that $|C'| < |C|$. The capacity of a minimum cut separating v from u is called the *minimum cut capacity* separating v from u, denoted by $\mathrm{mincut}(u, v)$. There is a single *source node* $s \in \mathcal{V}$ and a set of *sink nodes* $T \subseteq \mathcal{V} \setminus \{s\}$ on the graph $\mathcal{G}$. Without loss of generality, we assume that the source node s has no input edges and every sink node $t \in T$ has no output edges, i.e., $\mathrm{In}(s) = \mathrm{Out}(t) = \emptyset,\ \forall\ t \in T$. The graph $\mathcal{G}$, together with s and T, forms a *network* $\mathcal{N}$, denoted by $\mathcal{N} = (\mathcal{G}, s, T)$.

The source node s generates L *source symbols* $B_1, B_2, \cdots, B_L$ that are independent and identically distributed (i.i.d.) random variables with the uniform distribution on the finite field F. All the source symbols are required to be multicast to every sink node t in T by using the network $\mathcal{N}$ multiple times, i.e., transmitting multiple elements in F on each edge by using the edge multiple times. There is a

wiretapper who can eavesdrop any edge subset of size up to the security level r, while, for a positive integer $m_{_L}$, the $m_{_L}$ linear combinations of the source symbols

$$\sum_{i=1}^{L} a_{i,j} \cdot B_i, \quad j = 1, 2, \cdots, m_{_L} \tag{1}$$

over the finite field F are required to be protected from the wiretapper, where $a_{i,j},\ 1 \leq i \leq L, 1 \leq j \leq m_{_L}$ are constants in F. That is, the wiretapper is not allowed to obtain any information about the multiple linear combinations of the source symbols given in (1). Further, we let $\mathbf{B} = (B_1, B_2, \cdots, B_L)$ and

$$M_L = \Big[a_{i,j}\Big]_{1 \leq i \leq L,\ 1 \leq j \leq m_{_L}},$$

an $L \times m_{_L}$ matrix. Then, the $m_{_L}$ linear combinations in (1) can be written as $\mathbf{B} \cdot M_L$. Without loss of generality, we assume that $m_{_L} \leq L$ and the matrix M_L has full column rank, i.e.,

$$\mathrm{Rank}(M_L) = m_{_L}.$$

In this model, the security level r is known by the source node and sink nodes but which edge subset is eavesdropped by the wiretapper is unknown. It suffices to consider only the wiretap sets of size exactly equal to r. Then we let

$$\mathcal{W}_r \triangleq \{W \subseteq \mathcal{E} :\ |W| = r\},$$

where each edge subset $W \in \mathcal{W}_r$ is called a *wiretap set*. We use $\{(L, M_L), r\}$ to denote the above linear-combination security model.

Next, we define a *(linear-combination) security network code* for the security model $\{(L, M_L), r\}$. In order to combat the wiretapper, we may need randomness to randomize the source symbols.[1] As part of the code to be defined, we assume that the *key* $\mathbf{K}$ is a random variable uniformly distributed over a finite set $\mathcal{K}$, which is available only at the source node s. The key $\mathbf{K}$ and the source symbols $B_i,\ i = 1, 2, \cdots, L$ are assumed to be mutually independent. An (L, M_L) security network code is defined as follows. First, we let $b_i \in F$ and $\mathbf{k} \in \mathcal{K}$ be arbitrary outputs of the source symbol B_i and the key $\mathbf{K}$, respectively, $i = 1, 2, \cdots, L$. We further let $\mathbf{b} = (b_1, b_2, \cdots, b_{_L})$, which is the output of the vector of source symbols $\mathbf{B} = (B_1, B_2, \cdots, B_L)$. An (L, M_L) security network code $\widehat{\mathbf{C}}$ consists of

- a *local encoding function* $\widehat{\theta}_e$ for each edge $e \in \mathcal{E}$, where

$$\widehat{\theta}_e : \begin{cases} F^L \times \mathcal{K} \to \mathrm{Im}(\widehat{\theta}_e), & \text{if } \mathrm{tail}(e) = s; \\ \prod\limits_{d \in \mathrm{In}(\mathrm{tail}(e))} \mathrm{Im}(\widehat{\theta}_d) \to \mathrm{Im}(\widehat{\theta}_e), & \text{otherwise}; \end{cases} \tag{2}$$

[1] As we will show, it is not always necessary to randomize the source symbols.

with $\mathrm{Im}(\widehat{\theta}_e)$ denoting the image set of $\widehat{\theta}_e$;

- a decoding function for each sink node $t \in T$:

$$\widehat{\varphi}_t : \prod_{e\in \mathrm{In}(t)} \mathrm{Im}(\widehat{\theta}_e) \to F^L$$

to decode the source symbols $b_1, b_2, \cdots, b_L$ at t.

Further, we use $y_e \in \mathrm{Im}(\widehat{\theta}_e)$ to denote the message transmitted on each edge $e \in \mathcal{E}$ by using the code $\widehat{\mathbf{C}}$ under $\mathbf{b}$ and $\mathbf{k}$. With the encoding mechanism as described in (2), we readily see that y_e is a function of $\mathbf{b}$ and $\mathbf{k}$, denoted by $\widehat{h}_e\big(\mathbf{b}\ \mathbf{k}\big)$ (i.e., $y_e = \widehat{h}_e\big(\mathbf{b}\ \mathbf{k}\big)$), where $\widehat{h}_e$ can be obtained by recursively applying the local encoding functions $\widehat{\theta}_e, e \in \mathcal{E}$ according to any ancestral order of the edges in $\mathcal{E}$. More precisely, for each $e \in \mathcal{E}$, we have

$$\widehat{h}_e\big(\mathbf{b}\ \mathbf{k}\big) = \begin{cases} \widehat{\theta}_e\big(\mathbf{b}\ \mathbf{k}\big), & \text{if } \mathrm{tail}(e) = s; \\ \widehat{\theta}_e\big(\widehat{h}_{\mathrm{In}(u)}(\mathbf{b}\ \mathbf{k})\big), & \text{otherwise;} \end{cases}$$

where $u = \mathrm{tail}(e)$ and $\widehat{h}_E(\mathbf{b}\ \mathbf{k}) \triangleq \big(\widehat{h}_e(\mathbf{b}\ \mathbf{k}) : e \in E\big)$ for an edge subset $E \subseteq \mathcal{E}$ so that $\widehat{h}_{\mathrm{In}(u)}(\mathbf{b}\ \mathbf{k}) = \big(\widehat{h}_e(\mathbf{b}\ \mathbf{k}) : e \in \mathrm{In}(u)\big)$. We call $\widehat{h}_e$ the *global encoding function* of the edge e for the code $\widehat{\mathbf{C}}$.

For the security model $\{(L, M_L), r\}$, an (L, M_L) security network code $\widehat{\mathbf{C}} = \{\widehat{\theta}_e : e \in \mathcal{E};\ \widehat{\varphi}_t : t \in T\}$ is *admissible* if the following *decoding* and *security conditions* are satisfied:

- ***decoding condition***: all the source symbols are correctly decoded for each sink node $t \in T$, i.e., for each $t \in T$,

$$\widehat{\varphi}_t\big(\widehat{h}_{\mathrm{In}(t)}(\mathbf{b}\ \mathbf{k})\big) = \mathbf{b}, \quad \forall\ \mathbf{b} \in F^L \ \text{ and } \ \forall\ \mathbf{k} \in \mathcal{K}; \tag{3}$$

- ***security condition***: for each wiretap set $W \in \mathcal{W}_r$,

$$I\Big(\mathbf{Y}_W;\ \mathbf{B}\cdot M_L\Big) = 0, \tag{4}$$

where $\mathbf{Y}_W \triangleq (Y_e : e \in W)$ with $Y_e \triangleq \widehat{h}_e(\mathbf{B}, \mathbf{K})$ being the random variable transmitted on the edge e.

For an admissible (L, M_L) security network code $\widehat{\mathbf{C}} = \{\widehat{\theta}_e : e \in \mathcal{E};\ \widehat{\varphi}_t : t \in T\}$, we let

$$n_e = \lceil \log_{|F|} |\mathrm{Im}(\widehat{\theta}_e)| \rceil$$

for each edge e in $\mathcal{E}$, which is regarded as the number of times the edge e is used for transmission when applying the code $\widehat{\mathbf{C}}$. We further let $n(\widehat{\mathbf{C}}) \triangleq \max_{e\in\mathcal{E}} n_e$. Then, the *rate* of $\widehat{\mathbf{C}}$ is defined by

$$R(\widehat{\mathbf{C}}) = \frac{L}{n(\widehat{\mathbf{C}})}, \tag{5}$$

which is the average number of source symbols that can be securely multicast to all the sink nodes for one use of the network by using the code $\widehat{\mathbf{C}}$.

Furthermore, the *security capacity* for this model $\{(L, M_L), r\}$ is defined as the maximum rate of all the admissible (L, M_L) security network codes, i.e.,

$$\mathcal{C} = \max\left\{R(\widehat{\mathbf{C}}) : \widehat{\mathbf{C}} \text{ is an admissible } (L, M_L) \text{ security network code for } \{(L, M_L), r\}\right\}.$$

By the definition of the rate in (5), characterizing the security capacity $\mathcal{C}$ is equivalent to determining the minimum $n(\widehat{\mathbf{C}})$ over all the admissible (L, M_L) security network codes, i.e.,

$$n^* \triangleq \min\left\{n(\widehat{\mathbf{C}}) : \widehat{\mathbf{C}} \text{ is an admissible } (L, M_L) \text{ security network code for } \{(L, M_L), r\}\right\}.$$

For instance, a special case of the linear-combination security model $\{(L, M_L), r\}$ is the algebraic-sum security network coding, as elaborated below. In this model, the source node s generates L source symbols $B_1, B_2, \cdots, B_L$, which are required to be multicast to every sink node $t \in T$; and the wiretapper, who can eavesdrop any edge subset of size r, is not allowed to obtain any information on the m algebraic sums of the source symbols

$$\sum_{\substack{i\in[L]:\\ i\equiv j(\mathrm{mod}\ m)}} B_i, \quad j = 1, 2, \cdots, m, \tag{6}$$

where $1 \le m \le L$ and $[L] \triangleq \{1, 2, \cdots, L\}$. For this algebraic-sum security model, when $m = 1$, we adopt the convention that $i \equiv 1(\mathrm{mod}\ 1)$ for all $i = 1, 2, \cdots, L$. Then the equation (6) becomes $\sum_{i=1}^{L} B_i$, i.e., the algebraic sum $\sum_{i=1}^{L} B_i$ of all the L source symbols is required to be protected from the wiretapper. When $m = L$, we have $i \not\equiv i'(\mathrm{mod}\ m),\ \forall\ i, i' \in [L]$ with $i \neq i'$, and thus all the source symbols $B_1, B_2, \cdots, B_L$ are required to be protected from the wiretapper. This is the standard model of secure network coding, which has been widely studied in the literature, e.g. [11]–[19], [21]–[25].

III. Characterization of the Capacity for the Security Model $\{(L, M_L), r\}$

A. Upper Bounds on the Security Capacity

Consider a linear-combination security model $\{(L, M_L), r\}$. We first consider the trivial case of $r \ge C_{\min}$, where $C_{\min} \triangleq \min_{t\in T} \mathrm{mincut}(s, t)$. In this case, for a sink node $t \in T$ such that $\mathrm{mincut}(s, t) = C_{\min}$, the wiretapper is able to decode the source symbols provided that the sink node t correctly decodes them. This thus shows that the security capacity $\mathcal{C} = 0$ for $r \ge C_{\min}$, which implies that $C_{\min} - 1$ is an upper bound on the maximum security level for which the source symbols can be multicast with a positive rate. For another trivial case $r = 0$, the security model $\{(L, M_L), 0\}$ becomes a single-source multicast network coding problem without any security consideration. Following the fact that the maximum rate at which the source symbols can be correctly multicast to all the sink nodes is $C_{\min}$ (cf. [1], [6]), we thus obtain that

$$n^* = \left\lceil \frac{L}{C_{\min}} \right\rceil, \tag{7}$$

or equivalently,

$$\mathcal{C} = \frac{L}{n^*} = \frac{L}{\lceil L/C_{\min} \rceil}. \tag{8}$$

Next, we consider $0 < r < C_{\min}$. We readily see that an admissible (L, M_L) security network code $\widehat{\mathbf{C}}$ is also a network code such that all the L source symbols can be correctly decoded at each $t \in T$. This immediately implies that n^* can be lower bounded by $\lceil L/C_{\min} \rceil$ for any security level $0 < r < C_{\min}$, i.e.,

$$n^* \geq \left\lceil \frac{L}{C_{\min}} \right\rceil. \tag{9}$$

Furthermore, we present the following lemma which asserts a non-trivial lower bound on n^*.

Lemma 1. *Consider a linear-combination security model $\{(L, M_L), r\}$ with the security level $0 < r < C_{\min}$, where $\mathrm{Rank}(M_L) = m_{\scriptscriptstyle L}$. Let $\tau = m_{\scriptscriptstyle L}/L$. Then,*

$$n^* \geq \left\lceil \frac{\tau L}{C_{\min} - r} \right\rceil. \tag{10}$$

Proof. First, we claim that

$$H(\mathbf{B} \cdot M_L) = \tau L \cdot \log |F|, \tag{11}$$

where $\tau L = m_{\scriptscriptstyle L}$. To see this, we consider an arbitrary row vector $\vec{x} \in F^{\tau L}$ and obtain that

$$\begin{aligned} \Pr\left(\mathbf{B} \cdot M_L = \vec{x}\right) &= \sum_{\mathbf{b} \in F^L:\ \mathbf{b} \cdot M_L = \vec{x}} \Pr\left(\mathbf{B} = \mathbf{b}\right) \\ &= \#\left\{\mathbf{b} \in F^L : \mathbf{b} \cdot M_L = \vec{x}\right\} \cdot \frac{1}{|F|^L} = \frac{1}{|F|^{\tau L}}, \end{aligned} \tag{12}$$

where the equality $\Pr\left(\mathbf{B} = \mathbf{b}\right) = \frac{1}{|F|^L}$ holds because the source symbols $B_i, 1 \leq i \leq L$ are i.i.d. with the uniform distribution on F.

We now consider an arbitrary admissible (L, M_L) security network code $\widehat{\mathbf{C}} = \{\widehat{\theta}_e : e \in \mathcal{E};\ \widehat{\varphi}_t : t \in T\}$. For an edge subset C that separates a sink node $t \in T$ from the source node s, it follows from the decoding condition (3) that $H(\mathbf{B}|\mathbf{Y}_C) = 0$. This immediately implies that

$$H\big(\mathbf{B} \cdot M_L \big| \mathbf{Y}_C\big) = 0. \tag{13}$$

Further, for any wiretap set $W \in \mathcal{W}_r$ with $W \subseteq C$, it follows from the security condition (4) that

$$H\big(\mathbf{B} \cdot M_L\big) = H\big(\mathbf{B} \cdot M_L \big| \mathbf{Y}_W\big). \tag{14}$$

Combining (13) and (14), we obtain that

$$\begin{aligned} H\big(\mathbf{B} \cdot M_L\big) &= H\big(\mathbf{B} \cdot M_L \big| \mathbf{Y}_W\big) - H\big(\mathbf{B} \cdot M_L \big| \mathbf{Y}_C\big) \\ &= I\big(\mathbf{B} \cdot M_L;\ \mathbf{Y}_{C \setminus W} \big| \mathbf{Y}_W\big) \end{aligned}$$

$$
\begin{aligned}
&\leq H\big(\mathbf{Y}_{C\setminus W}\big|\mathbf{Y}_W\big)\\
&\leq H\big(\mathbf{Y}_{C\setminus W}\big)\\
&\leq \sum_{e\in C\setminus W} H(Y_e)\\
&\leq \sum_{e\in C\setminus W} \log\big|\mathrm{Im}(\widehat{\theta}_e)\big| \qquad (15)\\
&\leq \sum_{e\in C\setminus W} n_e\cdot\log|F| \qquad (16)\\
&\leq n(\widehat{\mathbf{C}})\cdot|C\setminus W|\cdot\log|F|, \qquad (17)
\end{aligned}
$$

where the inequality (15) holds because Y_e takes values in $\mathrm{Im}(\widehat{\theta}_e)$, the inequality (16) follows from

$$n_e=\big\lceil\log_{|F|}|\mathrm{Im}(\widehat{\theta}_e)|\big\rceil\geq\log_{|F|}|\mathrm{Im}(\widehat{\theta}_e)|,$$

and the inequality (17) follows from $n(\widehat{\mathbf{C}})=\max_{e\in\mathcal{E}}n_e$.

Combining (11) and (17), we obtain that

$$n(\widehat{\mathbf{C}})\geq\frac{H\big(\mathbf{B}\cdot M_L\big)}{|C\setminus W|\cdot\log|F|}=\frac{\tau L}{|C\setminus W|}.$$

Note that the above inequality is true for each sink node $t\in T$ and all the pairs (C,W) of the cut C separating t from s and the wiretap set $W\in\mathcal{W}_r$ such that $W\subseteq C$. We thus obtain that

$$n(\widehat{\mathbf{C}})\geq\max_{t\in T}\max_{\substack{(W,C)\in\mathcal{W}_r\times\Lambda_t:\\ W\subseteq C}}\frac{\tau L}{|C\setminus W|},$$

where $\Lambda_t\triangleq\big\{C\subseteq\mathcal{E}: C \text{ is a cut separating } t \text{ from } s\big\}$. For each $t\in T$, we have

$$|C\setminus W|\geq C_{\min}-r,\quad\forall\ (W,C)\in\mathcal{W}_r\times\Lambda_t \text{ with } W\subseteq C.$$

By the definition of $C_{\min}$, this lower bound is achievable for some $t\in T$ and $(W,C)\in\mathcal{W}_r\times\Lambda_t$ such that $W\subseteq C$. It then follows that

$$n(\widehat{\mathbf{C}})\geq\frac{\tau L}{C_{\min}-r}.$$

Further, since $n(\widehat{\mathbf{C}})$ is an integer, we have

$$n(\widehat{\mathbf{C}})\geq\left\lceil\frac{\tau L}{C_{\min}-r}\right\rceil. \qquad (18)$$

In addition, because the above lower bound (18) on $n(\widehat{\mathbf{C}})$ is valid for any admissible (L,M_L) security network code $\widehat{\mathbf{C}}$, we obtain that

$$n^*\geq\left\lceil\frac{\tau L}{C_{\min}-r}\right\rceil. \qquad (19)$$

The lemma is thus proved. □

The lower bounds in (9) and (10) on n^* applies to all $0 < r < C_{\min}$. For a specific value of τ, one of them can be tighter than the other. By comparing these bounds, we can readily obtain the upper bounds on the security capacity $\mathcal{C}$ as stated in the following theorem.

Theorem 1. *Consider a linear-combination security model $\{(L, M_L), r\}$ with the security level $0 < r < C_{\min}$, where $\mathrm{Rank}(M_L) = m_{_L}$. Let*

$$\tau = \frac{m_{_L}}{L} \quad \textit{and} \quad \tau_0 = \frac{C_{\min} - r}{C_{\min}}.$$

- *If $0 \le \tau \le \tau_0$, then*

$$\mathcal{C} \le \frac{L}{\lceil L/C_{\min} \rceil}. \tag{20}$$

- *If $\tau_0 < \tau \le 1$, then*

$$\mathcal{C} \le \frac{L}{\lceil \tau L/(C_{\min} - r) \rceil}. \tag{21}$$

Proof. By comparing the lower bounds (9) and (10) on n^*, we immediately obtain that

• if $0 \le \tau \le \tau_0$, then

$$n^* \ge \left\lceil \frac{L}{C_{\min}} \right\rceil \ge \left\lceil \frac{\tau L}{C_{\min} - r} \right\rceil \tag{22}$$

implying that

$$\mathcal{C} \le \frac{L}{\lceil L/C_{\min} \rceil};$$

• if $\tau_0 < \tau \le 1$, we have

$$n^* \ge \left\lceil \frac{\tau L}{C_{\min} - r} \right\rceil \ge \left\lceil \frac{L}{C_{\min}} \right\rceil \tag{23}$$

implying that

$$\mathcal{C} \le \frac{L}{\lceil \tau L/C_{\min} \rceil}.$$

We thus have proved the theorem. □

In the next subsection, we will present a code construction for the security model $\{(L, M_L), r\}$ with $0 < r < C_{\min}$, which shows that the upper bounds in Theorem 1 for both cases of τ are tight. This reveals the somewhat surprising fact that for the case $0 \le \tau \le \tau_0$, there is no penalty on the security capacity compared with the capacity without any security consideration. We thus obtain a full characterization of the security capacity for the security model $\{(L, M_L), r\}$, as stated in the following theorem.

Theorem 2. *Consider a linear-combination security model $\{(L, M_L), r\}$ over the finite field F, where $0 < r < C_{\min}$ and $|F| > \max\left\{|T|, \binom{|\mathcal{E}|}{r}\right\}$. Let*

$$\tau = \frac{m_{_L}}{L} \quad \textit{and} \quad \tau_0 = \frac{C_{\min} - r}{C_{\min}}.$$

- *If* $0 \leq \tau \leq \tau_0$, *then*

$$\mathcal{C} = \frac{L}{\lceil L/C_{\min} \rceil}. \tag{24}$$

- *If* $\tau_0 < \tau \leq 1$, *then*

$$\mathcal{C} = \frac{L}{\lceil \tau L/(C_{\min} - r) \rceil}. \tag{25}$$

In Section IV, we will further investigate the asymptotic behavior of the security capacity for a sequence of the security models as L tends to infinity. We will not only characterize the asymptotic behavior of the security capacity but also show the asymptotic optimality of our construction.

B. Code Construction

We first define a linear security network code for the security model $\{(L, M_L), r\}$. Briefly speaking, an (L, M_L) security network code $\widehat{\mathbf{C}}$ is *linear* if the local encoding functions for all the edges are linear. To be specific, we recall that $\mathbf{b} = (b_1, b_2, \cdots, b_{\scriptscriptstyle L}) \in F^L$ is an arbitrary output of the vector of source symbols $\mathbf{B} = (B_1, B_2, \cdots, B_L)$. Let $\mathcal{K} = F^z$, where the nonnegative integer z will be specified later. Then, the key $\mathbf{K}$ is a random row vector uniformly distributed on F^z. We further let $\mathbf{k} \in F^z$ be an arbitrary output of $\mathbf{K}$. Consequently, for an (L, M_L) linear security network code $\widehat{\mathbf{C}}$, all the global encoding functions $\widehat{h}_e,\ e \in \mathcal{E}$ are linear functions of $\mathbf{b}$ and $\mathbf{k}$. So, there exists an F-valued $(L+z) \times n$ matrix $H_e = \left[\vec{h}_e^{(1)}\ \vec{h}_e^{(2)}\ \cdots\ \vec{h}_e^{(n)}\right]$ for each $e \in \mathcal{E}$ such that

$$\widehat{h}_e(\mathbf{b}\ \mathbf{k}) = (\mathbf{b}\ \mathbf{k}) \cdot H_e,$$

where $n \triangleq n(\widehat{\mathbf{C}})$ and H_e is called the *global encoding matrix* of the edge e for the code $\widehat{\mathbf{C}}$. In particular, if $n(\widehat{\mathbf{C}}) = 1$, then the code $\widehat{\mathbf{C}}$ is called an (L, M_L) *scalar-linear* security network code.

In the following, for the nontrivial case of the security model $\{(L, M_L), r\}$ with security level $0 < r < C_{\min}$, we will develop a construction of admissible (L, M_L) linear security network codes which can be applied to any pair (L, M_L).

Theorem 3. *Consider a linear-combination security model* $\{(L, M_L), r\}$ *over the finite field* F, *where* $\mathrm{Rank}(M_L) = m_{\scriptscriptstyle L}$, $0 < r < C_{\min}$ *and* $|F| > \max\left\{|T|, \binom{|\mathcal{E}|}{r}\right\}$. *Let*

$$\tau = \frac{m_{\scriptscriptstyle L}}{L} \quad \textit{and} \quad \tau_0 = \frac{C_{\min} - r}{C_{\min}}.$$

Then, there exists an admissible (L, M_L) *linear security network code* $\widehat{\mathbf{C}}$ *such that*

- *if* $0 \leq \tau \leq \tau_0$, *then*

$$n(\widehat{\mathbf{C}}) = \left\lceil \frac{L}{C_{\min}} \right\rceil; \tag{26}$$

- *if* $\tau_0 < \tau \leq 1$*, then*

$$n(\widehat{\mathbf{C}}) = \left\lceil \frac{\tau L}{C_{\min} - r} \right\rceil. \tag{27}$$

The proof of Theorem 3, including the code construction and the verification of the decoding and security conditions, will be deferred to Section III-C.

C. Proof of Theorem 3

Code construction:

We consider a linear-combination security model $\{(L, M_L), r\}$ over the finite field F, where $0 < r < C_{\min}$ and $|F| > \max\left\{|T|, \binom{|\mathcal{E}|}{r}\right\}$. In the following, we will construct an admissible (L, M_L) linear security network code such that the L source symbols can be securely multicast to all the sink nodes by transmitting n symbols on each edge, i.e., using the network n times, where

$$n = \begin{cases} \left\lceil \frac{L}{C_{\min}} \right\rceil, & \text{if } 0 \leq \tau \leq \tau_0, \\ \left\lceil \frac{\tau L}{C_{\min} - r} \right\rceil. & \text{if } \tau_0 < \tau \leq 1, \end{cases} \tag{28}$$

(cf. (26) and (27)). For any $0 \leq \tau \leq 1$, we let

$$z = \begin{cases} 0, & \text{if } L \geq nr + \tau L, \\ nr + \tau L - L, & \text{if } L < nr + \tau L, \end{cases} \tag{29}$$

i.e.,

$$\mathcal{K} = \begin{cases} \emptyset, & \text{if } L \geq nr + \tau L, \\ F^{nr+\tau L-L}, & \text{if } L < nr + \tau L. \end{cases}$$

According to (29), when $L \geq nr + \tau L$, it is unnecessary to randomize the source symbols to guarantee the linear-combination security. Furthermore, for any pair (L, z) satisfying (29), we observe that

$$nr + \tau L \leq L + z \leq nC_{\min}. \tag{30}$$

The first inequality in (30) is straightforward. To prove the second inequality, we consider two cases below.

Case 1: $L \geq nr + \tau L$.

By (29) we have $z = 0$ and thus

$$L + z = L. \tag{31}$$

Further, it follows from (28) that for $0 \leq \tau \leq \tau_0$,

$$n = \left\lceil \frac{L}{C_{\min}} \right\rceil \geq \frac{L}{C_{\min}};$$

and for $\tau_0 < \tau \leq 1$,

$$n = \left\lceil \frac{\tau L}{C_{\min} - r} \right\rceil \geq \left\lceil \frac{L}{C_{\min}} \right\rceil \geq \frac{L}{C_{\min}}$$

(cf. (23) for the first inequality in the above equation). Together with (31), we immediately prove that $L + z = L \leq nC_{\min}$ for this case.

Case 2: $L < nr + \tau L$.

By (29) we have

$$L + z = nr + \tau L. \tag{32}$$

Further, it follows from (28) that for $0 \leq \tau \leq \tau_0$,

$$n = \left\lceil \frac{L}{C_{\min}} \right\rceil \geq \left\lceil \frac{\tau L}{C_{\min} - r} \right\rceil \geq \frac{\tau L}{C_{\min} - r}$$

(cf. (22) for the first inequality in the above equation), and for $\tau_0 < \tau \leq 1$,

$$n = \left\lceil \frac{\tau L}{C_{\min} - r} \right\rceil \geq \frac{\tau L}{C_{\min} - r}.$$

Together with (32), we immediately obtain that $L + z = nr + \tau L \leq nC_{\min}$ for this case. Combining the two cases, we have proved the second inequality in (30).

By (30), we have $L + z \leq nC_{\min}$. This implies that the $L + z$ symbols in F generated by the source node s, which contain the L source symbols and the key of z symbols, can be multicast to all the sink nodes in T by using the network n times. To elaborate this, we first claim that

$$L + z > (n-1)C_{\min}. \tag{33}$$

- When $0 \leq \tau \leq \tau_0$, it follows from (28) that

$$\begin{aligned}(n-1)C_{\min} &= \left(\left\lceil \frac{L}{C_{\min}} \right\rceil - 1 \right) \cdot C_{\min} \\ &< \frac{L}{C_{\min}} \cdot C_{\min} = L \leq L + z.\end{aligned}$$

- When $\tau_0 < \tau \leq 1$, by (28) we obtain that

$$\begin{aligned}(n-1)C_{\min} &= \left(\left\lceil \frac{\tau L}{C_{\min} - r} \right\rceil - 1 \right) \cdot C_{\min} \\ &< \frac{\tau L}{C_{\min} - r} \cdot C_{\min} \\ &= \tau L + \frac{\tau L}{C_{\min} - r} \cdot r \\ &\leq \tau L + nr \leq L + z,\end{aligned}$$

  where the last two inequalities follow from (28) and (30), respectively.

Thus, we have proved (33).

Now, we let $b'_1, b'_2, \cdots, b'_{L+z}$ be the $L+z$ source symbols and divide them into n groups $\mathbf{b}'_1, \mathbf{b}'_2, \cdots, \mathbf{b}'_{n-1}$ and $\mathbf{b}'_n$, where for $i = 1, 2, \cdots, n-1$, $\mathbf{b}'_i$ contains $C_{\min}$ source symbols, and $\mathbf{b}'_n$ contains the remaining $L+z-(n-1)C_{\min}$ source symbols. Here, we note from (30) and (33) that

$$1 \le L+z-(n-1)C_{\min} \le C_{\min}.$$

Thus, it suffices to construct at most 2 scalar-linear network codes of dimensions $C_{\min}$ and $\omega \triangleq L+z-(n-1)C_{\min}$, respectively, to multicast the $L+z$ source symbols to all the sink nodes.

Let $\mathbf{C}_1$ be a $C_{\min}$-dimensional scalar-linear network code on the network $\mathcal{N}$, of which the global encoding vectors are column vectors $\vec{f}_e$ in $F^{C_{\min}}$ for all $e \in \mathcal{E}$, and $\mathbf{C}_2$ be an ω-dimensional scalar-linear network code on $\mathcal{N}$, of which the global encoding vectors are column vectors $\vec{f}'_e$ in F^{ω} for all $e \in \mathcal{E}$ (cf. [1], [2] and [6]). We use the two codes $\mathbf{C}_1$ and $\mathbf{C}_2$ to construct an $(L+z)$-dimensional (vector-) linear network code $\mathbf{C}$ on the network $\mathcal{N}$ such that n symbols are transmitted on each edge $e \in \mathcal{E}$. To be specific, for each $e \in \mathcal{E}$, we let

$$\begin{aligned} G_e &= \Big[\vec{g}_e^{(1)}\ \vec{g}_e^{(2)}\ \cdots\ \vec{g}_e^{(n)}\Big] \\ &= \begin{bmatrix} \vec{f}_e & \vec{0} & \cdots & \vec{0} & \vec{0} \\ \vec{0} & \vec{f}_e & \cdots & \vec{0} & \vec{0} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vec{0} & \vec{0} & \cdots & \vec{f}_e & \vec{0} \\ \vec{0} & \vec{0} & \cdots & \vec{0} & \vec{f}'_e \end{bmatrix}, \end{aligned}$$

which is an F-valued $(L+z)\times n$ matrix regarded as the global encoding matrix for the code $\mathbf{C}$.

Next, for an edge $e \in \mathcal{E}$, we use $\big\langle G_e \big\rangle$ to denote the vector space spanned by the column vectors of the matrix G_e, i.e.,

$$\big\langle G_e \big\rangle \triangleq \big\langle \vec{g}_e^{(1)}, \vec{g}_e^{(2)}, \cdots, \vec{g}_e^{(n)} \big\rangle.$$

Further, for a wiretap set $W \in \mathcal{W}_r$, we use G_W to denote the $(L+z)\times nr$ matrix whose column vectors are the column vectors of G_e for all the edges $e \in W$, i.e.,

$$G_W = \Big[G_e :\ e \in W\Big] = \Big[\vec{g}_e^{(1)}\ \ \vec{g}_e^{(2)}\ \ \cdots\ \ \vec{g}_e^{(n)} :\ e \in W\Big],$$

and then similarly use $\big\langle G_W \big\rangle$ to denote the vector space spanned by the column vectors of the matrix G_W, i.e.,

$$\big\langle G_W \big\rangle \triangleq \big\langle \vec{g}_e^{(1)}, \vec{g}_e^{(2)}, \cdots, \vec{g}_e^{(n)} :\ e \in W \big\rangle.$$

Hence, we readily see that

$$\big\langle G_W \big\rangle = \sum_{e\in W} \big\langle G_e \big\rangle.$$

Now, we claim that there exist F-valued column $(L+z)$-vectors $\vec{u}_i,\ i=1,2,\cdots,\tau L$ such that

$$\big\langle \vec{u}_i : 1\le i\le \tau L\big\rangle \bigcap \big\langle G_W\big\rangle = \{\vec{0}\},\ \ \forall\ W\in\mathcal{W}_r. \tag{34}$$

To see this, we will prove by induction on $1\le j\le \tau L$ that if we have $j-1$ linearly independent column vectors $\vec{u}_1,\vec{u}_2,\cdots,\vec{u}_{j-1}$ in F^{L+z} such that

$$\big\langle \vec{u}_i : 1\le i\le j-1\big\rangle \bigcap \big\langle G_W\big\rangle = \{\vec{0}\},\ \ \forall\ W\in\mathcal{W}_r, \tag{35}$$

then we can choose a column vector $\vec{u}_j\in F^{L+z}\setminus \big\langle \vec{u}_i : 1\le i\le j-1\big\rangle$ such that

$$\big\langle \vec{u}_i : 1\le i\le j\big\rangle \bigcap \big\langle G_W\big\rangle = \{\vec{0}\},\ \ \forall\ W\in\mathcal{W}_r, \tag{36}$$

provided that $|F|>\binom{|\mathcal{E}|}{r}$. We consider

$$\begin{aligned}
&\Big|F^{L+z}\setminus \bigcup_{W\in\mathcal{W}_r} \big\langle G_W,\ \vec{u}_1,\vec{u}_2,\cdots,\vec{u}_{j-1}\big\rangle\Big| \\
&\ge |F|^{L+z} - |\mathcal{W}_r|\cdot|F|^{nr+j-1} &(37)\\
&\ge |F|^{nr+\tau L} - |\mathcal{W}_r|\cdot|F|^{nr+\tau L-1} &(38)\\
&\ge |F|^{nr+\tau L-1}\cdot\big(|F|-|\mathcal{W}_r|\big)>0, &(39)
\end{aligned}$$

where the inequality (37) follows because

$$\begin{aligned}
\dim\big(\big\langle G_W,\ \vec{u}_1,\vec{u}_2,\cdots,\vec{u}_{j-1}\big\rangle\big) &\le \dim\big(\big\langle G_W\big\rangle\big)+j-1\\
&\le n|W|+j-1 = nr+j-1,\ \ \forall\ W\in\mathcal{W}_r;
\end{aligned}$$

the inequality (38) follows from $L+z\ge nr+\tau L$ by (30) and the inequality (39) follows from

$$|F|>\binom{|\mathcal{E}|}{r}=|\mathcal{W}_r|.$$

Thus, we have proved the existence of such vectors $\vec{u}_i,\ 1\le i\le \tau L$ that satisfies the condition (34).

With the vectors $\vec{u}_i,\ 1\le i\le\tau L$, we let U be an F-valued $(L+z)\times(L+z)$ invertible matrix such that $\vec{u}_i,\ 1\le i\le\tau L$ are the first τL column vectors of U. Further, we consider an $(L+z)\times\tau L$ matrix

$$\widehat{M}_L \triangleq \begin{bmatrix} M_L \\ \mathbf{0}\end{bmatrix}, \tag{40}$$

where $\mathbf{0}$ is the $z\times\tau L$ zero matrix. In particular, when $z=0$ (cf. (29)), $\widehat{M}_L = M_L$. Recalling that M_L has full column rank, we readily see that $\widehat{M}_L$ has full column rank, too. With the full-column-rank

matrix $\widehat{M_L}$, we let Γ be an F-valued $(L+z)\times(L+z)$ invertible matrix such that the column vectors of $\widehat{M_L}$ are the first τL column vectors of Γ. Then, we define the matrix

$$Q \triangleq \Gamma \cdot U^{-1}, \tag{41}$$

which is of size $(L+z)\times(L+z)$ and also invertible over F.

Now, we consider the transformation $Q\cdot\mathbf{C}$ of the code $\mathbf{C}$ by the matrix Q, i.e., $Q\cdot\mathbf{C}$ is an F-valued $(L+z)$-dimensional linear network code on the network $\mathcal{N}$, of which all the global encoding matrices are

$$H_e \triangleq Q\cdot G_e,\ \forall\ e\in\mathcal{E}, \tag{42}$$

(cf. the transformation of a scalar-linear network code in [6, Section 19.3.1] and [19, Theorem 2]). Next, we will show that $\widehat{\mathbf{C}} \triangleq Q\cdot\mathbf{C}$ is an admissible F-valued (L, M_L) linear security network code for the security model $\{(L, M_L), r\}$ by verifying the decoding and security conditions.

Verification of the decoding condition:

We continue to consider the output of the source $(\mathbf{b}, \mathbf{k})$, where $\mathbf{b}\in F^L$ is the vector of source symbols and $\mathbf{k}\in F^z$ is the key. In using the code $\widehat{\mathbf{C}}$, the implementation of the global encoding matrices $H_e,\ e\in\mathcal{E}$ is equivalent to linearly transforming $(\mathbf{b}\ \mathbf{k})$ into $\boldsymbol{x}\triangleq(\mathbf{b}\ \mathbf{k})\cdot Q$ and then using the code $\mathbf{C}$ to multicast $\boldsymbol{x}$ to all the sink nodes in T.

Since the vector $\boldsymbol{x}$ can be correctly decoded at each $t\in T$ when applying the code $\mathbf{C}$, $(\mathbf{b}\ \ \mathbf{k})$ can be also correctly decoded at each $t\in T$ and so does the vector $\mathbf{b}$ of source symbols. Thus, we have verified the decoding condition.

Verification of the security condition:

In order to verify the security condition (4), we need the next lemma which plays a crucial role in our code construction. For an edge $e\in\mathcal{E}$, $\langle H_e\rangle$ denotes the vector space spanned by the column vectors of H_e, i.e.,

$$\langle H_e\rangle \triangleq \langle \vec{h}_e^{(1)}, \vec{h}_e^{(2)}, \cdots, \vec{h}_e^{(n)}\rangle.$$

Further, for a wiretap set $W\in\mathcal{W}_r$, we let H_W be the $(L+z)\times nr$ matrix that contains all the column vectors of the global encoding matrices H_e for all the edges $e\in W$, i.e.,

$$H_W = \Big[H_e:\ e\in W\Big] = \Big[\vec{h}_e^{(1)}\ \ \vec{h}_e^{(2)}\ \ \cdots\ \ \vec{h}_e^{(n)}:\ e\in W\Big].$$

We let

$$\langle H_W\rangle \triangleq \langle \vec{h}_e^{(1)}, \vec{h}_e^{(2)}, \cdots, \vec{h}_e^{(n)}:\ e\in W\rangle,$$

the vector space spanned by the column vectors of H_W. Evidently,

$$\big\langle H_W \big\rangle = \sum_{e\in W} \big\langle H_e \big\rangle.$$

Lemma 2. *For the security model $\{(L, M_L), r\}$ over the finite field F with $0 < r < C_{\min}$, let $\widehat{\mathbf{C}}$ be an F-valued (L, M_L) linear security network code, of which the global encoding matrices are $(L+z)\times n$ matrices $H_e = \Big[\vec{h}_e^{(1)}\ \vec{h}_e^{(2)}\ \cdots\ \vec{h}_e^{(n)}\Big],\ e\in\mathcal{E}$. Then, for the code $\widehat{\mathbf{C}}$, the security condition* (4) *is satisfied if and only if*

$$\big\langle \widehat{M}_L \big\rangle \bigcap \big\langle H_W \big\rangle = \{\vec{0}\},\quad \forall\ W\in\mathcal{W}_r, \tag{43}$$

where $\widehat{M}_L = \left[\begin{smallmatrix} M_L \\ \mathbf{0}\end{smallmatrix}\right]$ is an $(L+z)\times \tau L$ matrix as defined in (40).

Proof. We first prove the "only if" part by contradiction. Suppose the contrary that there exists a wiretap set $W\in\mathcal{W}_r$ such that

$$\big\langle \widehat{M}_L \big\rangle \bigcap \big\langle H_W \big\rangle \neq \{\vec{0}\}. \tag{44}$$

In the following, we will prove that

$$I\big(\mathbf{B}\cdot M_L;\ \mathbf{Y}_W\big) > 0, \tag{45}$$

which contradicts the security condition (4) for the code $\widehat{\mathbf{C}}$.

By (44), there exist two non-zero column vectors $\vec{w}\in F^{n|W|}$ $(=F^{nr})$ and $\vec{u}\in F^{\tau L}$ such that

$$H_W\cdot\vec{w} = \widehat{M}_L\cdot\vec{u}\neq\vec{0}, \tag{46}$$

where $\vec{0}$ is the zero column $(L+z)$-vector. Then, we obtain that

$$\begin{aligned}
&I\Big(\mathbf{B}\cdot M_L;\ \mathbf{Y}_W\Big)\\
&= I\Big(\mathbf{B}\cdot M_L;\ (\mathbf{B}\ \mathbf{K})\cdot H_W\Big) \qquad (47)\\
&= H\Big(\mathbf{B}\cdot M_L\Big) - H\Big(\mathbf{B}\cdot M_L\Big|(\mathbf{B}\ \mathbf{K})\cdot H_W\Big)\\
&= H\Big(\mathbf{B}\cdot M_L\Big) - H\Big(\mathbf{B}\cdot M_L\cdot\Big|(\mathbf{B}\ \mathbf{K})\cdot H_W, (\mathbf{B}\ \mathbf{K})\cdot H_W\cdot\vec{w}\Big)\\
&\geq H\Big(\mathbf{B}\cdot M_L\Big) - H\Big(\mathbf{B}\cdot M_L\Big|(\mathbf{B}\ \mathbf{K})\cdot H_W\cdot\vec{w}\Big)\\
&= I\Big(\mathbf{B}\cdot M_L;\ (\mathbf{B}\ \mathbf{K})\cdot H_W\cdot\vec{w}\Big)\\
&= I\Big(\mathbf{B}\cdot M_L;\ (\mathbf{B}\ \mathbf{K})\cdot\widehat{M}_L\cdot\vec{u}\Big) \qquad (48)\\
&= I\Big(\mathbf{B}\cdot M_L;\ \mathbf{B}\cdot M_L\cdot\vec{u}\Big)\\
&= H\Big(\mathbf{B}\cdot M_L\cdot\vec{u}\Big) - H\Big(\mathbf{B}\cdot M_L\cdot\vec{u}\Big|\mathbf{B}\cdot M_L\Big)
\end{aligned}$$

$$= H\Big(\mathbf{B}\cdot M_L\cdot\vec{u}\Big) > 0, \tag{49}$$

where the equality (47) follows from $\mathbf{Y}_W = (\mathbf{B}\ \mathbf{K})\cdot H_W$, the equality (48) follows from (46), the equality in (49) follows from $H\Big(\mathbf{B}\cdot M_L\cdot\vec{u}\big|\mathbf{B}\cdot M_L\Big) = 0$ and the inequality in (49) follows from $M_L\cdot\vec{u}\neq\vec{0}$ because $\vec{u}\neq\vec{0}$ and M_L has full column rank. Thus, the inequality (45) is proved.

Next, we prove the "if" part. By the security condition (4), we will prove that

$$H\Big(\mathbf{B}\cdot M_L\big|\mathbf{Y}_W\Big) = H\Big(\mathbf{B}\cdot M_L\Big),\quad \forall\ W\in\mathcal{W}_r \tag{50}$$

if the condition (43) is satisfied. To prove (50), it suffices to show that for each $W\in\mathcal{W}_r$, the equality

$$\Pr\Big(\mathbf{B}\cdot M_L=\vec{x}\big|\mathbf{Y}_W=\vec{y}\Big) = \Pr\Big(\mathbf{B}\cdot M_L=\vec{x}\Big) \tag{51}$$

is satisfied for any row vector $\vec{x}\in F^{\tau L}$ and any row vector $\vec{y}\in F^{nr}$ such that $\Pr\big(\mathbf{Y}_W=\vec{y}\big)>0$, i.e., there exists a pair $(\mathbf{b}\ \mathbf{k})$ of a vector of source symbols $\mathbf{b}\in F^L$ and a key $\mathbf{k}\in F^z$ such that $(\mathbf{b}\ \mathbf{k})\cdot H_W=\vec{y}$.

We recall that

$$\Pr\Big(\mathbf{B}\cdot M_L=\vec{x}\Big)=\frac{1}{|F|^{\tau L}},\quad\forall\ \vec{x}\in F^{\tau L}$$

(cf. (12)). Thus, we only need to prove that for each $W\in\mathcal{W}_r$,

$$\Pr\Big(\mathbf{B}\cdot M_L=\vec{x}\big|\mathbf{Y}_W=\vec{y}\Big)=\frac{1}{|F|^{\tau L}}$$

for any $\vec{x}\in F^{\tau L}$ and $\vec{y}\in F^{nr}$ such that $\Pr\big(\mathbf{Y}_W=\vec{y}\big)>0$. We now consider

$$\begin{aligned}
&\Pr\Big(\mathbf{B}\cdot M_L=\vec{x}\big|\mathbf{Y}_W=\vec{y}\Big)\\
&=\frac{\Pr\big(\mathbf{B}\cdot M_L=\vec{x},\mathbf{Y}_W=\vec{y}\big)}{\Pr\big(\mathbf{Y}_W=\vec{y}\big)}\\
&=\frac{\Pr\big((\mathbf{B}\ \mathbf{K})\cdot\widehat{M}_L=\vec{x},\ (\mathbf{B}\ \mathbf{K})\cdot H_W=\vec{y}\big)}{\Pr\big((\mathbf{B}\ \mathbf{K})\cdot H_W=\vec{y}\big)}\\
&=\frac{\Pr\big((\mathbf{B}\ \mathbf{K})\cdot\big[\widehat{M}_L\ H_W\big]=(\vec{x}\ \ \vec{y})\big)}{\Pr\big((\mathbf{B}\ \mathbf{K})\cdot H_W=\vec{y}\big)}\\
&=\frac{\sum_{(\mathbf{b}\ \mathbf{k})\in F^L\times F^z:\ (\mathbf{b}\ \mathbf{k})[\widehat{M}_L\ H_W]=(\vec{x}\ \vec{y})}\Pr\big(\mathbf{B}=\mathbf{b},\ \mathbf{K}=\mathbf{k}\big)}{\sum_{(\mathbf{b}'\ \mathbf{k}')\in F^L\times F^z:\ (\mathbf{b}'\ \mathbf{k}')H_W=\vec{y}}\Pr\big(\mathbf{B}=\mathbf{b}',\ \mathbf{K}=\mathbf{k}'\big)}\\
&=\frac{\#\big\{(\mathbf{b}\ \mathbf{k})\in F^L\times F^z:(\mathbf{b}\ \mathbf{k})\cdot\big[\widehat{M}_L\ H_W\big]=(\vec{x}\ \ \vec{y})\big\}}{\#\big\{(\mathbf{b}'\ \mathbf{k}')\in F^L\times F^z:(\mathbf{b}'\ \mathbf{k}')\cdot H_W=\vec{y}\big\}},
\end{aligned}\tag{52}$$

where we use "$\#\{\cdot\}$" to denote the cardinality of the set and the equality (52) follows because $\mathbf{B}$ and $\mathbf{K}$ are independently and uniformly distributed on F^L and F^z, respectively. Furthermore,

- for the dominator in (52), we have

$$\#\big\{(\mathbf{b}'\ \mathbf{k}') \in F^L \times F^z : (\mathbf{b}'\ \mathbf{k}')\cdot H_W = \vec{y}\big\} = |F|^{L+z-\mathrm{Rank}(H_W)}; \tag{53}$$

- for the numerator in (52), we have

$$\begin{aligned}&\#\big\{(\mathbf{b}\ \mathbf{k}) \in F^L \times F^z : (\mathbf{b}\ \mathbf{k})\cdot\big[\widehat{M}_L\ H_W\big] = (\vec{x}\ \ \vec{y})\big\}\\ &= |F|^{L+z-\mathrm{Rank}\left(\left[\widehat{M}_L\ H_W\right]\right)}\\ &= |F|^{L+z-\mathrm{Rank}(H_W)-\tau L},\end{aligned} \tag{54}$$

where the equality (54) follows from the condition that $\big\langle \widehat{M}_L\big\rangle \bigcap \big\langle H_W\big\rangle = \{\vec{0}\}$ (cf. (43)). Combining (53) and (54) with (52), we immediately prove that

$$\Pr\Big(\mathbf{B}\cdot M_L = \vec{x}\big|\mathbf{Y}_W = \vec{y}\Big) = \frac{1}{|F|^{\tau L}},$$

which implies the equality (51). The "if" part is also proved. We thus have proved the lemma. □

Now, we start to verify the security condition for our code construction. Toward this end, by Lemma 2 it suffices to verify (43). For the constructed (L, M_L) linear security network code $\widehat{\mathbf{C}}$, we have

$$\big\langle \vec{u}_i :\ 1 \le i \le \tau L\big\rangle \bigcap \big\langle G_W\big\rangle = \{\vec{0}\},\quad \forall\ W \in \mathcal{W}_r \tag{55}$$

(cf. (34)). We recall (41) that $Q = \Gamma \cdot U^{-1}$ is an $(L+z)\times(L+z)$ invertible matrix. Then, by (55), we immediately obtain that

$$\big\langle Q\cdot\vec{u}_i :\ 1 \le i \le \tau L\big\rangle \bigcap \big\langle Q\cdot G_W\big\rangle = \{\vec{0}\},\quad \forall\ W \in \mathcal{W}_r. \tag{56}$$

We note that

$$H_W = \Big[H_e :\ e \in W\Big] = Q\cdot\Big[G_e :\ e \in W\Big] = Q\cdot G_W,\quad \forall\ W \in \mathcal{W}_r. \tag{57}$$

Further, we write

$$\Big[\vec{u}_1\ \ \vec{u}_2\ \ \cdots\ \ \vec{u}_{\tau L}\Big] = U\cdot\begin{bmatrix} I_{\tau L}\\ \mathbf{0}\end{bmatrix},$$

where we recall that $\vec{u}_i,\ 1 \le i \le \tau L$ are the first τL column vectors of U, $I_{\tau L}$ is the $\tau L \times \tau L$ identity matrix and $\mathbf{0}$ is the $(L+z-\tau L)\times \tau L$ zero matrix. Then, we can see that

$$\begin{aligned}Q\cdot\Big[\vec{u}_1\ \ \vec{u}_2\ \ \cdots\ \ \vec{u}_{\tau L}\Big] &= Q\cdot U\cdot\begin{bmatrix} I_{\tau L}\\ \mathbf{0}\end{bmatrix}\\ &= \Gamma\cdot U^{-1}\cdot U\cdot\begin{bmatrix} I_{\tau L}\\ \mathbf{0}\end{bmatrix}\end{aligned} \tag{58}$$

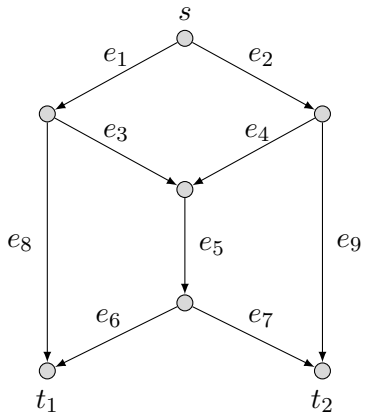

Fig. 1: The butterfly network $\mathcal{N} = (\mathcal{G}, s, T = \{t_1, t_2\})$.

$$= \Gamma \cdot \begin{bmatrix} I_{\tau L} \\ \mathbf{0} \end{bmatrix}$$
$$= \widehat{M}_L, \tag{59}$$

where (58) follows from $Q = \Gamma \cdot U^{-1}$ (cf. (41)) and (59) follows because the column vectors of $\widehat{M}_L$ are the first τL column vectors of Γ. Combining (57) and (59) with (56), we immediately prove that

$$\big\langle \widehat{M}_L \big\rangle \bigcap \big\langle H_W \big\rangle = \{\vec{0}\}, \quad \forall\ W \in \mathcal{W}_r.$$

Thus, by Lemma 2, we have verified the security condition.

D. An Example to Illustrate Our Code Construction

Let $\mathcal{N} = (\mathcal{G}, s, T = \{t_1, t_2\})$ be the butterfly network as depicted in Fig. 1. For the security model $r = 1$, we consider two linear-combination security models $\{(2, M_2), 1\}$ and $\{(3, M_3), 1\}$ over the field $\mathbf{F}_3 = \{0, 1, 2\}$, where

$$M_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad \text{and} \quad M_3 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}. \tag{60}$$

Namely, in the security model $\{(2, M_2), 1\}$, the algebraic sum $B_1 + B_2$ of the two source symbols is required to be protected from the wiretapper; and in the security model $\{(3, M_3), 1\}$, the algebraic sums $B_1 + B_2$ and $B_2 + B_3$ of the source symbols are required to be protected from the wiretapper.

• The security model $\{(2, M_2), 1\}$.

In this model, the source node s generates two source symbols b_1 and b_2 in $\mathbf{F}_3$ and the algebraic sum b_1+b_2 needs to be protected. From (60), we have

$$m_2 = \mathrm{Rank}(M_2) = 1, \quad \text{and} \quad \tau = \frac{m_2}{2} = \frac{1}{2} = \tau_0 = \frac{C_{\min}-r}{C_{\min}}.$$

Therefore, we have $0 \le \tau \le \tau_0$, i.e., the first case in Theorem 2. Next, we will construct an optimal $\mathbf{F}_3$-valued $(2, M_2)$ linear security network code for the security model $\{(2, M_2), 1\}$, which achieves the security capacity 2.

By our code construction, it follows from (28) and (29) that we take

$$n = \left\lceil \frac{L}{C_{\min}} \right\rceil = 1$$

and $z = 0$ because $L = 2 \ge nr + \tau L = 2$. We first consider an $\mathbf{F}_3$-valued 2-dimensional scalar-linear network code $\mathbf{C}_1$ on the network $\mathcal{N}$, which is used to multicast two source symbols b_1 and b_2 in $\mathbf{F}_3$ to the sink nodes t_1 and t_2. The global encoding matrices (vectors) of $\mathbf{C}_1$ are

$$G_{e_1} = G_{e_3} = G_{e_8} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad G_{e_2} = G_{e_4} = G_{e_9} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad \text{and} \quad G_{e_5} = G_{e_6} = G_{e_7} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

Clearly, the code $\mathbf{C}_1$ is not secure for the algebraic sum b_1+b_2 because the wiretapper can obtain b_1+b_2 by accessing the edge e_5 on which b_1+b_2 is transmitted. Based on the code $\mathbf{C}_1$, we now construct a $(2, M_2)$ scalar-linear security network code for the security model $\{(2, M_2), 1\}$.

Next, we let $\vec{u}_1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$, an $\mathbf{F}_3$-valued column 2-vector such that $\vec{u}_1 \notin \langle G_{e_i} \rangle, \ \forall\ 1 \le i \le 9$ (cf. (34)). Then, let $U = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$, a 2×2 invertible matrix on $\mathbf{F}_3$ such that $\vec{u}_1$ is the first column vector of U. Furthermore, since $z = 0$, we have $\widehat{M_2} = M_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ (cf. (40)), and let $\Gamma = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, which is a 2×2 invertible matrix on $\mathbf{F}_3$ such that $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ is the first column vector of Γ. By (41), we calculate $Q = \Gamma \cdot U^{-1} = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$. Now, we obtain an admissible $\mathbf{F}_3$-valued $(2, M_2)$ scalar-linear security network code $\widehat{\mathbf{C}}_1 = Q \cdot \mathbf{C}_1$, of which the global encoding matrices (vectors) are $H_{e_i} = Q \cdot G_{e_i}, \ 1 \le i \le 9$. Specifically,

$$H_{e_1} = H_{e_3} = H_{e_8} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad H_{e_2} = H_{e_4} = H_{e_9} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad \text{and} \quad H_{e_5} = H_{e_6} = H_{e_7} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

We use y_{e_i}, which takes values in $\mathbb{F}_3$, to denote the message transmitted on each edge $e_i, \ 1 \le i \le 9$. By the above global encoding matrices of $\widehat{\mathbf{C}}_1$, the messages $y_{e_i}\ (= (b_1, b_2) \cdot H_e)$ transmitted on the edges $e_i, \ 1 \le i \le 9$ are

$$y_{e_1} = y_{e_3} = y_{e_8} = b_1 + 2b_2, \quad y_{e_2} = y_{e_4} = y_{e_9} = b_2, \quad \text{and} \quad y_{e_5} = y_{e_6} = y_{e_7} = b_1,$$

as depicted in Fig. 2. We can readily verify the decoding and security conditions for the code $\widehat{\mathbf{C}}_1$. In particular, we see in this case that although no randomness is used to randomize the source symbols,

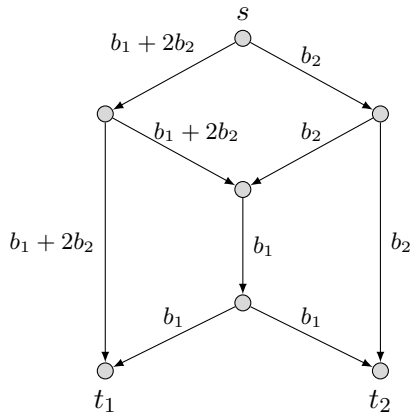

Fig. 2: An $\mathbf{F}_3$-valued $(2, M_2)$ scalar-linear security network code for $\{(2, M_2), 1\}$.

the wiretapper cannot obtain any information about the algebraic sum $b_1 + b_2$ when any one edge is eavesdropped.

• The security model $\{(3, M_3), 1\}$.

In this model, the source node s generates three source symbols b_1, b_2 and b_3 in $\mathbf{F}_3$ and two algebraic sums $b_1 + b_2$ and $b_2 + b_3$ need to be protected. By (60), we note that $m_3 = \mathrm{Rank}(M_3) = 2$, and so

$$\tau = \frac{m_3}{3} = \frac{2}{3} > \tau_0 = \frac{C_{\min} - r}{C_{\min}} = \frac{1}{2}.$$

Therefore, we have $\tau_0 < \tau \leq 1$, i.e., the second case in Theorem 2. Next, we will construct an optimal $\mathbf{F}_3$-valued $(3, M_3)$ linear security network code for the security model $\{(3, M_3), 1\}$, which achieves the security capacity $3/2$.

According to our code construction, it follows from (28) and (29) that we take

$$n = \left\lceil \frac{\tau L}{C_{\min} - r} \right\rceil = 2$$

and $z = 1$ because $L < nr + \tau L$ by $L = 3$ and $nr + \tau L = 4$. We consider an $\mathbf{F}_3$-valued 4-dimensional (where $4 = L + z$) linear network code $\mathbf{C}_2$ of rate 2, which is used to multicast the three source symbols b_1, b_2, b_3 and a key k in $\mathbf{F}_3$ to the sink nodes t_1 and t_2. The 4×2 global encoding matrices of $\mathbf{C}_2$ are

$$G_{e_1} = G_{e_3} = G_{e_8} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad G_{e_2} = G_{e_4} = G_{e_9} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad \text{and} \quad G_{e_5} = G_{e_6} = G_{e_7} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}.$$

We note that the code $\mathbf{C}_2$ is not secure because the wiretapper can obtain some information about b_1+b_2 by accessing the edge e_5 on which b_1+b_2 and b_3+k are transmitted. Based on the code $\mathbf{C}_2$, we now construct a linear secure network code for the security model $\{(3, M_3), 1\}$.

Let

$$\vec{u}_1 = \begin{bmatrix} 1 \\ 2 \\ 0 \\ 0 \end{bmatrix} \quad \text{and} \quad \vec{u}_2 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 2 \end{bmatrix}$$

be two $\mathbf{F}_3$-valued column 4-vectors such that $\left\langle \vec{u}_1, \vec{u}_2 \right\rangle \bigcap \left\langle G_{e_i} \right\rangle = \{\vec{0}\},\ \forall\ 1 \le i \le 9$ (cf. (34)). Then, let

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 1 \end{bmatrix},$$

a 4×4 invertible matrix on $\mathbf{F}_3$ such that $\vec{u}_1$ and $\vec{u}_2$ are the first two column vectors of U. Furthermore, since $z = 1$ as mentioned above, we have

$$\widehat{M_3} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$$

(cf. (40)), and let

$$\Gamma = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

which is a 4×4 invertible matrix on $\mathbf{F}_3$ such that the column vectors of $\widehat{M_L}$ are the first two column vectors of Γ. By (41), we calculate

$$Q = \Gamma \cdot U^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$

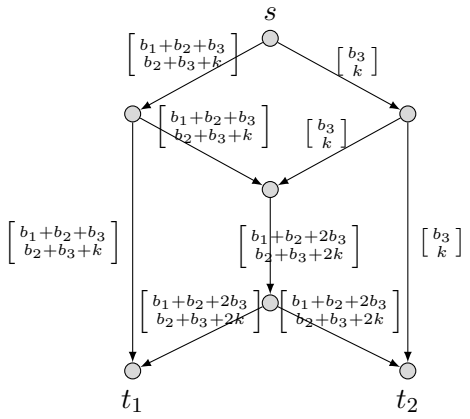

Fig. 3: An $\mathbf{F}_3$-valued $(3, M_3)$ linear security network code for $\{(3, M_3), 1\}$.

Now, we obtain an admissible $\mathbf{F}_3$-valued $(3, M_3)$ linear security network code $\widehat{\mathbf{C}}_2 = Q \cdot \mathbf{C}_2$, of which the 4×2 global encoding matrices are $H_{e_i} = Q \cdot G_{e_i},\ 1 \le i \le 9$; specifically,

$$H_{e_1} = H_{e_3} = H_{e_8} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad H_{e_2} = H_{e_4} = H_{e_9} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \text{and} \quad H_{e_5} = H_{e_6} = H_{e_7} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 2 & 1 \\ 0 & 2 \end{bmatrix}.$$

We use y_{e_i}, which takes values in $\mathbb{F}_3^2$, to denote the message transmitted on each edge $e_i,\ 1 \le i \le 9$. By the above global encoding matrices of $\widehat{\mathbf{C}}_2$, the messages $y_{e_i}\ (= (b_1, b_2, b_3, k) \cdot H_e)$ transmitted on the edges $e_i,\ 1 \le i \le 9$ are

$$y_{e_1} = y_{e_3} = y_{e_8} = (b_1 + b_2 + b_3,\ b_2 + b_3 + k),$$

$$y_{e_2} = y_{e_4} = y_{e_9} = (b_3,\ k), \quad \text{and} \quad y_{e_5} = y_{e_6} = y_{e_7} = (b_1 + b_2 + 2b_3,\ b_2 + b_3 + 2k),$$

as depicted in Fig. 3.

For the security models $\{(2, M_2), 1\}$ and $\{(3, M_3), 1\}$ as discussed in the above example, by Theorem 3, admissible linear security network codes of rate 2 and $3/2$, respectively, can be constructed if the field size $|F| > \max\left\{|T|, \binom{|\mathcal{E}|}{r}\right\} = 9$. However, we see in the example that the field $\mathbf{F}_3$ (of size 3) is sufficient for our code construction. This implies that the bound $\max\left\{|T|, \binom{|\mathcal{E}|}{r}\right\}$ in Theorem 3 on the field size is only sufficient but not necessary for our code construction.

IV. Asymptotic Behavior of the Security Capacity

In this section, we will investigate the asymptotic behavior of the security capacity. For a fixed network $\mathcal{N}$ and a security level r, we consider a sequence of the security models $\{(L, M_L), r\},\ L = 1, 2, \cdots$.

The following theorem characterizes the asymptotic behavior of the security capacity for a sequence of security models $\{(L, M_L), r\},\ L = 1, 2, \cdots$.

Theorem 4. *Consider a sequence of linear-combination security models $\{(L, M_L), r\}$ over a finite field F for $L = 1, 2, \cdots$, where $0 < r < C_{\min}$ and $|F| > \max\left\{|T|, \binom{|\mathcal{E}|}{r}\right\}$. Denote by $\mathcal{C}_{L,M_L}$ the security capacity for each model $\{(L, M_L), r\}$. Let*

$$\tau_{_L} = \frac{m_{_L}}{L},\ L = 1, 2, \cdots \quad \textit{and} \quad \tau_0 = \frac{C_{\min} - r}{C_{\min}},$$

where $m_{_L} = \mathrm{Rank}(M_L)$ for $L = 1, 2, \cdots$.

- *If $\tau_{_L} \leq \tau_0 + o(1)$, then,*

$$\lim_{L\to\infty} \mathcal{C}_{L,M_L} = C_{\min}.$$

- *If $\tau_{_L} = \kappa + o(1)$ with κ satisfying $\tau_0 < \kappa \leq 1$, then,*

$$\lim_{L\to\infty} \mathcal{C}_{L,M_L} = \kappa^{-1} \cdot (C_{\min} - r).$$

Proof. We first consider the case $\tau_{_L} \leq \tau_0 + o(1)$. Then, there exists a nonnegative sequence $a_{_L},\ L = 1, 2, \cdots$ with $\lim_{L\to\infty} a_{_L} = 0$ such that

$$\tau_{_L} \leq \tau_0 + a_{_L}, \quad L = 1, 2, \cdots. \tag{61}$$

We now use Theorem 2 to show that

$$\mathcal{C}_{L,M_L} \geq \frac{L}{\lceil (\tau_0 + a_{_L}) \cdot L/(C_{\min} - r) \rceil}. \tag{62}$$

To see this, consider the following two cases:

- if $0 \leq \tau_{_L} \leq \tau_0$, it follows from (24) that

$$\mathcal{C}_{L,M_L} = \frac{L}{\lceil L/C_{\min} \rceil} = \frac{L}{\lceil \tau_0 \cdot L/(C_{\min} - r) \rceil} \geq \frac{L}{\lceil (\tau_0 + a_{_L}) \cdot L/(C_{\min} - r) \rceil}; \tag{63}$$

- if $\tau_0 < \tau_{_L} \leq 1$, then we obtain that

$$\mathcal{C}_{L,M_L} = \frac{L}{\lceil \tau_{_L} \cdot L/(C_{\min} - r) \rceil} \geq \frac{L}{\lceil (\tau_0 + a_{_L}) \cdot L/(C_{\min} - r) \rceil}, \tag{64}$$

  where the equality follows from (25) and the inequality follows from (61).

Combining (62) and (9) above Lemma 1, we further obtain that for each pair (L, M_L),

$$\frac{L}{\lceil (\tau_0 + a_{_L}) \cdot L/(C_{\min} - r) \rceil} \leq \mathcal{C}_{L,M_L} \leq \frac{L}{\lceil L/C_{\min} \rceil} \leq C_{\min}. \tag{65}$$

We note that

$$\lim_{L\to\infty} \frac{L}{\lceil (\tau_0 + a_{_L}) \cdot L/(C_{\min} - r) \rceil} = C_{\min}.$$

Together with (65), we thus have proved that

$$\lim_{L\to\infty} \mathcal{C}_{L,M_L} = C_{\min}.$$

Next, we consider the case that $\tau_L = \kappa + o(1)$, where $\tau_0 < \kappa \leq 1$. Then, there exists a sequence b_L, $L = 1, 2, \cdots$ satisfying $\lim_{L\to\infty} b_L = 0$ such that

$$\tau_L = \kappa + b_L, \quad L = 1, 2, \cdots.$$

Here, we note that b_L may be negative. Together with $\kappa > \tau_0$ and $\lim_{L\to\infty} b_L = 0$, there exists a positive integer L_0 such that for each $L \geq L_0$,

$$|b_L| < \kappa - \tau_0, \quad \text{i.e.,} \quad \tau_0 - \kappa < b_L < \kappa - \tau_0,$$

which implies that

$$\tau_L = \kappa + b_L > \tau_0, \quad \forall\ L \geq L_0. \tag{66}$$

By (25) in Theorem 2, we have

$$\mathcal{C}_{L,M_L} = \frac{L}{\lceil (\kappa + b_L) \cdot L/(C_{\min} - r) \rceil},$$

so that

$$\lim_{L\to\infty} \mathcal{C}_{L,M_L} = \kappa^{-1} \cdot (C_{\min} - r).$$

Thus, the theorem is proved. □

By Theorem 4, we can see that for a sequence of security models $\{(L, M_L), r\},\ L = 1, 2, \cdots$ that satisfies $\tau_L \leq \tau_0 + o(1)$, or $\tau_L = \kappa + o(1)$ where $\tau_0 < \kappa \leq 1$, our code construction is *asymptotically optimal*, i.e.,

$$\lim_{L\to\infty} R(\widehat{\mathbf{C}}_{L,M_L}) = \lim_{L\to\infty} \mathcal{C}_{L,M_L}, \tag{67}$$

where $\widehat{\mathbf{C}}_{L,M_L}$ is the constructed code for each model $\{(L, M_L), r\}$ by our code construction. To illustrate this, we consider in the following several specific sequences of security models.

First, we consider a sequence of security models $\{(L, M_L), r\},\ L = 1, 2, \cdots$, where all the ranks $\mathrm{Rank}(M_L),\ L = 1, 2, \cdots$ are upper bounded by a constant, say m, e.g., the security constraint of multiple algebraic sums

$$\sum_{\substack{i\in[L]:\\ i\equiv j (\mathrm{mod}\ m)}} B_i, \quad j = 1, 2, \cdots, m$$

as discussed in the last paragraph of Section II. With this, we have

$$\lim_{L\to\infty} \frac{m_L}{L} = 0,$$

which implies the inequality $\tau_{_L} = m_{_L}/L \leq \tau_0 + o(1)$. It then follows from the first case of Theorem 4 that

$$\lim_{L\to\infty} \mathcal{C}_{L,M_{_L}} = C_{\min}.$$

Next, we will show that our code construction is asymptotically optimal. We first note that

$$\tau_{_L} = \frac{m_{_L}}{L} \leq \frac{C_{\min} - r}{C_{\min}} = \tau_0, \quad \forall\ L \geq C_{\min} \cdot \left\lceil \frac{m}{C_{\min} - r} \right\rceil.$$

Together with the first case of Theorem 3 (cf. (26)), the constructed code $\widehat{\mathbf{C}}_{L,M_{_L}}$ achieves the rate $R(\widehat{\mathbf{C}}_{L,M_{_L}}) = \frac{L}{\lceil L/C_{\min}\rceil}$. This immediately implies that the equality (67) is satisfied, namely that our code construction is asymptotically optimal for this example.

Next, we consider a sequence of security models $\{(L, M_L), r\},\ L = 1, 2, \cdots$, where all the ranks $m_{_L} = \mathrm{Rank}(M_L)$ satisfy

$$m_{_L} = \lceil \kappa \cdot L \rceil\,, \quad L = 1, 2, \cdots.$$

We note that the sequence of $m_{_L},\ L = 1, 2, \cdots$, is not upper bounded. By Theorem 4, we can obtain the asymptotic behavior of the security capacity for the sequence of models $\{(L, M_L), r\},\ L = 1, 2, \cdots$ as follows:

$$\lim_{L\to\infty} \mathcal{C}_{L,M_{_L}} = \begin{cases} C_{\min}, & \text{if } 0 < \kappa \leq \tau_0, \\ \kappa^{-1} \cdot (C_{\min} - r), & \text{if } \tau_0 < \kappa < 1. \end{cases} \tag{68}$$

Furthermore, it follows from Theorem 3 that

$$\lim_{L\to\infty} R(\widehat{\mathbf{C}}_{L,M_{_L}}) = \begin{cases} C_{\min}, & \text{if } 0 < \kappa \leq \tau_0, \\ \kappa^{-1} \cdot (C_{\min} - r), & \text{if } \tau_0 < \kappa < 1, \end{cases} \tag{69}$$

where $\widehat{\mathbf{C}}_{L,M_{_L}}$ is the code constructed for each model $\{(L, M_L), r\}$ by the code construction. Comparing (68) and (69), we immediately see that the equality (67) holds, which thus shows that our code construction is asymptotically optimal for this example.

Finally, we consider the special sequence of security models $\{(L, M_L), r\}$ for $L = 1, 2, \cdots$, where $m_{_L} = L$, i.e., $\tau_{_L} = m_{_L}/L = 1$ for all $L = 1, 2, \cdots$. This linear-combination security constraint is equivalent to protecting all the source symbols from the wiretapper, and so each model $\{(L, M_L), r\}$ is equivalent to the standard secure network coding model. Thus, we have

$$\lim_{L\to\infty} \mathcal{C}_{L,M_{_L}} = C_{\min} - r. \tag{70}$$

On the other hand, for each pair (L, M_L), it follows from $\tau_{_L} = 1$ and Theorem 3 that the (L, M_L) linear security network code $\widehat{\mathbf{C}}_{L,M_{_L}}$ constructed by our code construction has rate

$$R(\widehat{\mathbf{C}}_{L,M_{_L}}) = \frac{L}{\lceil L/(C_{\min} - r)\rceil}.$$

This implies that

$$\lim_{L\to\infty} R(\widehat{\mathbf{C}}_{L,M_L}) = C_{\min} - r. \tag{71}$$

Combining (70) and (71), we see that the equality (67) holds and thus our code construction is also asymptotically optimal for this example.

V. Conclusion

In this paper, we put forward the model of multiple linear-combination security network coding, which is specified by the security level, the number of source symbols, and the linear-combination security constraint. We fully characterized the security capacity for any such security model in terms of the ratio τ of the rank of the linear-combination security constraint to the number of source symbols. Also, we developed a construction of linear security network codes. The code construction is applicable to any security model, and the code constructed achieves the security capacity. We also determined a threshold value τ_0 such that there is no penalty on the security capacity compared with the capacity without any security consideration when the ratio τ is not larger than τ_0. Finally, we analyzed the asymptotic behavior of the security capacity for a sequence of linear-combination security models and fully characterized the asymptotic behavior of the security capacity. We also showed that our code construction is asymptotically optimal.

Appendix A
A Related Work by Bhattad and Narayanan

A model related to the current work is the one considered by Bhattad and Narayanan [24], of which the general case is given as follows. On the network $\mathcal{N}$, the single source node s generates L ($L \le C_{\min}$) source symbols, denoted by $X_1, X_2, \cdots, X_L$, over a finite field F that are required to be multicast to all the sink nodes in T. Let $U_p,\ 1 \le p \le P$ be P subsets of the L source symbols, and G_p, $1 \le p \le P$ be another P subsets of the L source symbols. The security requirement is specified by the P pairs $(U_p, G_p),\ 1 \le p \le P$ as follows. The wiretapper, who can access any one wiretap set W in a collection $\mathcal{W}$ of wiretap sets, is not allowed to obtain any information about U_p given G_p for each $p = 1, 2, \cdots, P$, i.e., for each $p = 1, 2, \cdots, P$,

$$I\big(U_p; Y_W \big| G_p\big) = 0 \quad \text{or} \quad H\big(U_p \big| G_p\big) = H\big(U_p \big| Y_W, G_p\big), \quad \forall\ W \in \mathcal{W}, \tag{72}$$

where $Y_W = (Y_e :\ e \in W)$ with Y_e being the random variable transmitted on the edge e. In particular, when taking $P = L$, and $U_p = \{X_p\}$ and $G_p = \emptyset$ for $1 \le p \le P$, the security requirement (72) becomes

$$I\big(X_p; Y_W\big) = 0, \quad \forall\ 1 \le p \le P \ \text{ and } \ W \in \mathcal{W}.$$

This type of security requirement is called *weak security* in [24].

For the above model, the main focus in [24] is on how to find a suitable linear transformation of the L source symbols for a given linear network code to obtain a secure linear network code such that the security requirement (72) is satisfied. Theorem 3 in [24], the most general result in the paper, asserts the existence of such a linear transformation when a given condition is satisfied. We state this theorem as follows.

Theorem A.1 ([24, Theorem 3])**.** *Consider an L-dimensional ($L \leq C_{\min}$) network code $\mathbf{C}$ over a finite field F and a collection of wiretap sets $\mathcal{W}$ in which $r = \max_{w\in\mathcal{W}} |W|$. Let $(U_p, G_p),\ 1 \leq p \leq P$ be P pairs of subsets U_p and G_p of the L source symbols, which specify the security requirement. If*

$$\max_{1\leq p\leq P} \big(|U_p| + |G_p|\big) \leq L - r, \tag{73}$$

then there exists a linear transformation of the source symbols as a precoding on the linear network code $\mathbf{C}$ such that the security requirement (72) *is satisfied.*

We now go back to the linear-combination security model $\{(L, M_L), r\}$ discussed in the current paper. Consider the first case $0 \leq \tau \leq \tau_0$ in Theorem 2, where we recall that $\tau = m_{\scriptscriptstyle L}/L$ with $m_{\scriptscriptstyle L} = \mathrm{Rank}(M_L)$ and $\tau_0 = (C_{\min} - r)/C_{\min}$. Then we can apply the approach of the linear transformation in Theorem A.1 (cf. [24] for details) to obtain an (L, M_L) linear security network code provided that the following two additional conditions on the model parameters are satisfied:

$$0 \leq \tau \leq \frac{L-r}{L}\ (\leq \tau_0) \quad \text{and} \quad L \leq C_{\min}. \tag{74}$$

To be specific, we consider a linear-combination security model $\{(L, M_L), r\}$ satisfying the conditions (74), where the L source symbols $B_1, B_2, \cdots, B_L$ are required to be multicast to all the sink nodes in T and the multiple linear combinations $\mathbf{B} \cdot M_L$ (where $\mathbf{B} = (B_1, B_2, \cdots, B_L)$) are required to be protected from the wiretapper. We first linearly transform $\mathbf{B} = (B_1, B_2, \cdots, B_L)$ to $(X_1, X_2, \cdots, X_L)$ by an $L \times L$ invertible matrix M whose left $L \times m_{\scriptscriptstyle L}$ submatrix is equal to M_L. Then we have

$$(X_1, X_2, \cdots, X_L) = (B_1, B_2, \cdots, B_L) \cdot M,$$

where

$$(X_1, X_2, \cdots, X_{m_{\scriptscriptstyle L}}) = (B_1, B_2, \cdots, B_L) \cdot M_L.$$

We now apply Theorem A.1 as follows. Take $X_1, X_2, \cdots, X_L$ as the source symbols. Let $U = \{X_1, X_2, \cdots, X_{m_{\scriptscriptstyle L}}\}$, $G = \emptyset$, and $\mathcal{W} = \mathcal{W}_r$. By $\tau \leq (L-r)/L$, we see that $|U| + |G| = m_{\scriptscriptstyle L} \leq L - r$, which satisfies the condition (73) in Theorem A.1. It thus follows from Theorem A.1 that we can construct

a linear secure network code such that $X_1, X_2, \cdots, X_L$ can be multicast to all the sink nodes in T and the wiretapper cannot obtain any information about U, i.e.,

$$I\big(X_1, X_2, \cdots, X_{m_L}; Y_W\big) = 0, \quad \forall\ W \in \mathcal{W}_r,$$

or equivalently,

$$I\big(\mathbf{B} \cdot M_L; Y_W\big) = 0, \quad \forall\ W \in \mathcal{W}_r.$$

Hence, we obtain an admissible (L, M_L) linear security network code for the security model $\{(L, M_L), r\}$.

However, the second case $\tau_0 < \tau \leq 1$ in Theorem 2 cannot be handled by the approach in [24]. To be specific, from $\tau > \tau_0$, we have

$$\frac{m_{\scriptscriptstyle L}}{L} = \tau > \tau_0 = \frac{C_{\min} - r}{C_{\min}} \geq \frac{L - r}{L}.$$

This implies that $|U| + |G| = m_{\scriptscriptstyle L} > L - r$, which does not satisfy the condition (73) in Theorem A.1. Hence, we cannot apply the linear transformation approach for the case $\tau_0 < \tau \leq 1$.

ACKNOWLEDGEMENT

A special case of the results in this paper was discussed in our submission to the 2023 IEEE Information Theory Workshop. We thank an anonymous reviewer for pointing out the relation between our submission and Bhattad and Narayanan [24].

REFERENCES

[1] Ahlswede, R.; Cai, N.; Li, S.-Y.; Yeung, R.W. Network Information Flow. *IEEE Trans. Inf. Theory* **2000**, 46, 1204–1216.

[2] Li, S.-Y.R.; Yeung, R.W.; Cai, N. Linear Network Coding. *IEEE Trans. Inf. Theory* **2003**, 49, 371–381.

[3] Koetter, R.; Médard, M. An Algebraic Approach to Network Coding. *IEEE/ACM transactions on networking* **2003**, 11, 782–795.

[4] Jaggi, S.; Sanders, P.; Chou, P.A.; Effros, M.; Egner, S.; Jain, K.; Tolhuizen, L.M. Polynomial Time Algorithms for Multicast Network Code Construction. *IEEE Trans. Inf. Theory* **2005**, 51, 1973–1982.

[5] Ho, T.; Lun, D. *Network Coding: An Introduction*; Cambridge University Press: Cambridge, UK, 2008.

[6] Yeung, R.W. *Information Theory and Network Coding*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2008.

[7] Yeung, R.W.; Li, S.-Y.R.; Cai, N.; Zhang, Z. Network Coding Theory Part I: Single Source. *Foundations and Trends in Communications and Information Theory* **2006**, 2, 241–329.

[8] Yeung, R.W.; Li, S.-Y.R.; Cai, N.; Zhang, Z. Network Coding Theory Part II: Multiple Source. *Foundations and Trends in Communications and Information Theory* **2006**, 2, 330–381.

[9] Fragouli, C.; Soljanin, E. Network Coding Fundamentals. *Foundations and Trends in Networking* **2007**, 2, 1–133.

[10] Fragouli, C.; Soljanin, E. Network Coding Applications. *Foundations and Trends in Networking* **2008**, 2, 135–269.

[11] Cai, N.; Yeung, R.W. Secure Network Coding on a Wiretap Network. *IEEE Trans. Inf. Theory* **2011**, 57, 424–435.

[12] El Rouayheb, S.; Soljanin, E.; Sprintson, A. Secure Network Coding for Wiretap Networks of Type II. *IEEE Trans. Inf. Theory* **2012**, 58, 1361–1371.

[13] Silva, D.; Kschischang, F.R. Universal Secure Network Coding via Rank-Metric Codes. *IEEE Trans. Inf. Theory* **2011**, 57, 1124–1135.

[14] Cai, N.; Chan, T. Theory of Secure Network Coding. *Proceedings of the IEEE* **2011**, 99, 421–437.

[15] Cui, T.; Ho, T.; Kliewer, J. On Secure Network Coding With Nonuniform or Restricted Wiretap Sets. *IEEE Trans. Inf. Theory* **2013**, 59, 166–176.

[16] Cheng, F.; Yeung, R.W. Performance Bounds on a Wiretap Network With Arbitrary Wiretap Sets. *IEEE Trans. Inf. Theory* **2014**, 60, 3345–3358.

[17] Fragouli, C.; Soljanin, E. (Secure) Linear Network Coding Multicast. *Designs, Codes and Cryptography* **2016**, 78, 269–310.

[18] Guang, X.; Yeung, R.W. Alphabet Size Reduction for Secure Network Coding: A Graph Theoretic Approach. *IEEE Trans. Inf. Theory* **2018**, 64, 4513–4529.

[19] Guang, X.; Yeung, R.W.; Fu, F.-W. Local-Encoding-Preserving Secure Network Coding. *IEEE Trans. Inf. Theory* **2020**, 66, 5965–5994.

[20] Fong S.-L.; Yeung, R.W. Variable-rate linear network coding, *IEEE Trans. Inf. Theory*, **2010**, 56, 2618-2625.

[21] Cai, N.; Yeung, R.W. A Security Condition for Multi-Source Linear Network Coding. In Proceedings of the 2007 IEEE International Symposium on Information Theory, Nice, France, 24–29 June 2007; pp. 561–565.

[22] Chan, T.; Grant, A. Capacity Bounds for Secure Network Coding. In Proceedings of the 2008 Australian Communications Theory Workshop, Christchurch, New Zealand, 30 January–1 February 2008; pp. 95–100.

[23] Zhang, Z.; Yeung, R.W. A General Security Condition for Multi-Source Linear Network Coding. In Proceedings of the 2009 IEEE International Symposium on Information Theory, Seoul, Korea (South), 28 June–3 July 2009; pp. 1155–1158.

[24] Bhattad, K.; Narayanan, K.R. Weakly Secure Network Coding. In Proceedings of the First Workshop on Network Coding, Theory and Applications, 4 April 2005; pp. 8-20.

[25] Harada, K.; Yamamoto, H. Strongly Secure Linear Network Coding. *IEICE transactions on fundamentals of electronics, communications and computer sciences* **2008**, 91, 2720–2728.

[26] Shannon, C.E. Communication Theory of Secrecy Systems. *The Bell System Technical Journal* **1949**, 28, 656–715.

[27] Blakley, G.R. Safeguarding Cryptographic Keys. In Proceedings of the Managing Requirements Knowledge, International Workshop on, NEW YORK, USA, 4–7 June 1979; p. 313.

[28] Shamir, A. How to Share a Secret. *Communications of the ACM* **1979**, 22, 612–613.

[29] Ozarow, L.H.; Wyner, A.D. Wire-Tap Channel II. *AT&T Bell Laboratories Technical Journal* **1984**, 63, 2135–2157.

[30] J. Feldman, T. Malkin, R. A. Servedio, and C. Stein. On the Capacity of Secure Network Coding. In Proceedings of 42nd Annual Allerton Conference on Communication, Control, and Computing, Monticello, USA, 29 September - 1 October, 2004.