Fundamental Limits on a Class of Secure Asymmetric Multilevel Diversity Coding Systems

Congduan Li, *Member, IEEE*, Xuan Guang, *Member, IEEE*, Chee Wei Tan, *Senior Member, IEEE*, and Raymond W. Yeung, *Fellow, IEEE*

***Abstract*— In the future communication applications, users may obtain their messages that have different importance levels distributively from several available sources, such as distributed storage or even devices belonging to other users. This scenario is the best modeled by the multilevel diversity coding systems (MDCS). To achieve perfect (information-theoretic) secrecy against wiretap channels, this paper investigates the fundamental limits on the secure rate region of the asymmetric MDCS (AMDCS), which include the symmetric case as a special case. Threshold perfect secrecy is added to the AMDCS model. The eavesdropper may have access to any one but not more than one subset of the channels but know nothing about the sources, as long as the size of the subset is not above the security level. The question of whether superposition (source separation) coding is optimal for such an AMDCS with threshold perfect secrecy is answered. A class of secure AMDCS (S-AMDCS) with an arbitrary number of encoders is solved, and it is shown that linear codes are optimal for this class of instances. However, in contrast with the secure symmetric MDCS, superposition is shown to be not optimal for S-AMDCS in general. In addition, necessary conditions on the existence of a secrecy key are determined as a design guideline.**

***Index Terms*— Multilevel diversity coding, secrecy, wiretap channel, superposition, asymmetric, symmetric.**

Manuscript received September 16, 2017; revised January 31, 2018; accepted February 17, 2018. Date of publication April 11, 2018; date of current version July 9, 2018. This work was supported in part by the Science, Technology and Innovation Commission of Shenzhen Municipality under Project JCYJ20170818094955771, Project JCYJ20160229165220746, Project JCYJ20170307090810981, and Project JSGG20160301170514984, in part by the National Natural Science Foundation of China under Grant 61771018 and Grant 61771259, in part by the Research Grants Council of Hong Kong under Grant 11207615, in part by the Hong Kong Scholars Program under Grant XJ2016028, in part by the University Grants Committee of the Hong Kong SAR, China, under Project AoE/E-02/08, and in part by the Vice-Chancellor's One-off Discretionary Fund of CUHK under Project VCF2014030 and Project VCF2015007. This paper was presented at the IEEE International Symposium on Information Theory, Aachen, Germany, in 2017. *(Corresponding authors: Congduan Li; Xuan Guang.)*

C. Li is with the Department of Computer Science, City University of Hong Kong, Hong Kong (e-mail: congduan.li@gmail.com; congduan.li@cityu.edu.hk).

X. Guang is with the School of Mathematical Sciences and LPMC, Nankai University, Tianjin 300071, China, and also with the Institute of Network Coding, The Chinese University of Hong Kong, Hong Kong (e-mail: xguang@nankai.edu.cn).

C. W. Tan is with the Department of Computer Science, City University of Hong Kong, Hong Kong (e-mail: cheewtan@cityu.edu.hk).

R. W. Yeung is with the Institute of Network Coding, The Chinese University of Hong Kong, Hong Kong, and also with the School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen 518172, China (e-mail: whyeung@ie.cuhk.edu.hk).

Digital Object Identifier 10.1109/JSAC.2018.2825838

I. Introduction

In FUTURE communication networks, say next-generation wireless cellular networks, users may like to receive their desired messages at high speed. To achieve this goal, the network may store information in a distributed manner at many data servers (e.g., base stations or data-center caches) and, possibly, even at devices belonging to other nearby users so that a particular user can get the information from a subset of the available sources. Among the desired messages in the information stream of a user, they may have different importance levels. For instance, multimedia data such as videos or images are usually coded at different levels of resolutions to satisfy the different user requirements or to meet performance specifications. Some messages may be encoded in data packets with a minimal resolution and are typically considered more important since a higher resolution can be obtained after getting additional data packets. Since information may be stored at devices belonging to other users, another crucial issue is network security [1]–[4]. As increasingly more devices are connected to the network, the challenge of preventing wiretapping and protecting the privacy of users draws increasing attentions. This is also important due to the broadcast nature of wireless networks, where transmitted messages can be easily wiretapped. Even for wired networks, the risk of being wiretapped also exists.

In this paper, we study the information-theoretic security issue in such a distributed communication network with sources of different importance. Perfect secrecy is of essence since with the rapid development of large-scale computing and data analytics, it is possible to decrypt a secrecy message by brute force. For instance, a wiretapper may collect data for a sufficiently long time period and then apply statistical inference techniques to glimpse the protected information. Perfect or information-theoretic security guarantees that wiretapped messages do not leak any information of the sources. We will provide fundamental limits on the secure transmission rates and the size of the secrecy key for asymmetric transmission, which is a key feature in future 5G systems. These fundamental limits may provide a guiding principle on the design of network security and the distribution of secrecy key.

The scenario of distributively communicating or storing information with different importance levels is best modeled by the multilevel diversity coding systems (MDCS). As one of the earliest models of modern communication and storage

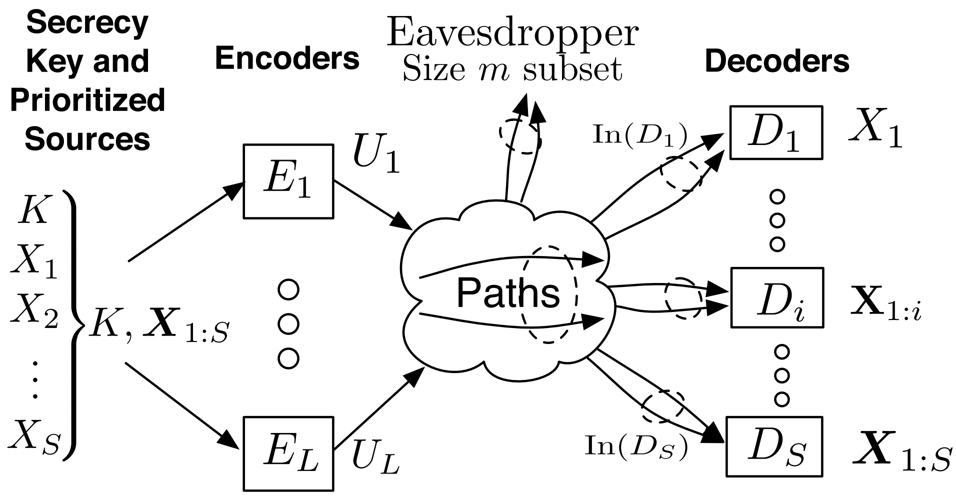


Fig. 1. A Secure Asymmetric Multilevel Diversity Coding System (S-AMDCS). The secrecy key K and prioritized sources $X_1, X_2, \ldots, X_S$ are coded by L encoders and the eavesdropper can access a size-m subset of the coded messages. Each decoder has a distinct decoding level, i.e., decoder D_i can decode the first i sources, $X_1, X_2, \ldots, X_i$, $i = 1$, 2, …, S.

networks, MDCS were introduced in [5] and [6], where the sources are prioritized in a way such that a source with higher priority first gets decoded before sources with lower priority. The sources are coded and transmitted (or stored) by multiple encoders, and are demanded by multiple sinks where each sink has access to a certain subset of the transmissions (or storages) and requires the first several sources. Early applications of MDCS include the transmission of multimedia, e.g., videos or images, that are encoded at different levels of resolution and a sink demanding a higher resolution may need to decode the lower-resolution parts first.

If full symmetry of encoders exists in the system, that is, decoders with input from any l encoders can decode the first l sources, the system is called symmetric MDCS (SMDCS). The rate region of SMDCS is solved in [7] and it is shown that superposition (source separation) coding is optimal. In [8], a model without symmetry called asymmetric MDCS (AMDCS) was proposed, where all $2^L - 1$ access structure for L encoders are considered at the decoder side and each decoder is assigned a different level, i.e., the decoder can decode different number of first sources. The case with only three encoders was solved in [8] and it is shown that the superposition strategy is not optimal. Some recent results on general MDCS with more than three encoders and further general multi-source networks can be found in [9] and [10], where the optimality of different codes are examined, including superposition and simple linear codes associated with representable matroids [11].

The standard MDCS models focus on the rate regions, which characterize the relations between coding rates and source entropies for reliable communications without any consideration of secrecy. However, future networks such as 5G system may demand specifications on both information security as well as reliable communications [12], [13]. We are interested in *perfect* or *information-theoretic* secrecy, proposed in [14], where the eavesdropper obtains nothing about the source information even after accessing a subset of channels, called a *wiretap set*. As will be shown, the wiretap channel II [15], which contains all subsets of the channels (encoders) with a fixed size (referred as security level in this paper), is considered in this paper. In [16] and [17], secure SMDCS (S-SMDCS) is considered and it is shown that superposition is optimal for the sum-rate and furthermore the entire admissible rate region. We propose a secure AMDCS (S-AMDCS) and study the optimality of superposition.

Two smallest non-trivial S-AMDCS with i) four sources, three encoders, security level 1 (i.e., at most one encoder is wiretapped) and ii) five sources, four encoders, security level 2 (i.e., at most two encodes are wiretapped), were studied initially in [18] and [19], where it was shown that superposition coding is not optimal for these two special cases and thus for general S-AMDCS. In this paper, we will show the fundamental limits on a class of S-AMDCS with arbitrary number (say L) of encoders, $L+1$ sources and security level $L - 2$. We prove the non-optimality by showing that the *superposition secure rate region* does not match with the full *secure rate region* for this class of problems. However, simple linear codes do suffice to achieve the full secure rate region for this class of networks. In addition, we give fundamental limits on the size of secrecy keys to achieve the security constraints.

The rest of this paper is organized as follows. The secure rate region of AMDCS with perfect secrecy is formulated in Section II. Then, the secure rate regions of a class of networks are presented in Section III, which includes the characterization of superposition and full secure rate region. The proofs are presented in Section IV and we conclude the paper in Section V.

II. Problem Formulation

Let us start with the problem formulation for S-AMDCS and then introduce several definitions of its secure rate region.

A. Secure Asymmetric Multilevel Diversity Coding Systems

In S-AMDCS (see Fig. 1), we add threshold perfect secrecy constraints to the AMDCS model introduced in [8]. Specifically, an S-AMDCS has L encoders (channels) $E_1, E_2, \cdots, E_L$ and T decoders $D_1, D_2, \cdots D_T$. Each encoder E_i has access to all the independent prioritized sources $X_1, X_2, \cdots, X_S$ and the secrecy key K, which are i.i.d. in time. Each decoder D_j has access a subset of encoders $\mathrm{In}(D_j) \subseteq \{E_1, E_2, \cdots, E_L\}$, and we say that D_j has a *decoding level* n, denoted by $\mathcal{L}(D_j)$, if the first n sources $\mathbf{X}_{1:n}^{(n)} \triangleq (X_1, X_2, \cdots, X_n)$ can be decoded at D_j by accessing all outputs of the encoders in $\mathrm{In}(D_j)$. This function $\mathcal{L}(\cdot)$ is called the decoding level of the S-AMDCS. There is an eavesdropper who can wiretap any one but not more than one size-m subset of the encoders, where m is called the *security level*. Now, if a decoder D_j can achieve the secure transmission, $\mathrm{In}(D_j)$ must contain at least $m+1$ encoders, i.e., $|\mathrm{In}(D_j)| \geq m+1$, because otherwise D_j cannot obtain any private information of the sources under the security level m.

In this paper, we consider all possible secure transmissions, i.e., the number of the decoders is $T = \sum_{l=m+1}^{L} \binom{L}{l}$ and assume that all the decoders have distinct decoding levels with a strict partial order as follows: for any two decoders D_i and D_j with $\mathrm{In}(D_i) \supsetneq \mathrm{In}(D_j)$, the decoding level of D_i is strictly larger than that of D_j, i.e., $\mathcal{L}(D_i) > \mathcal{L}(D_j)$. In this paper, we consider the case that the number of the sources S achieves the minimum, i.e.,

$$S = T = \sum_{l=m+1}^{L} \binom{L}{l}.$$

Such a decoding level $\mathcal{L}(\cdot)$ is called *valid* and so it can be regarded as a one-to-one mapping with the foregoing strict partial order from the set of all the subsets of encoders of size larger than m to the set $\{1, 2, \cdots, S\}$. Thus, an S-AMDCS instance can be determined by the tuple $(L, m, \mathcal{L})$ of the number of encoders L, the security level m, and the decoding levels $\mathcal{L}$. This is a general model and includes the symmetric case as a special case. In the sequel, we sometimes use the indices of the encoders in $\mathrm{In}(D_i)$ only for notational simplicity, if there is no ambiguity.

B. Secure Rate Region

In this subsection, we define a block code and give the secure rate region for an S-AMDCS.

Definition 1: For an $(L, m, \mathcal{L})$ S-AMDCS with S mutually independent prioritized sources $X_1, X_2, \cdots, X_S$. Let $\boldsymbol{\omega} = \big(H(X_1), H(X_2), \cdots, H(X_S)\big)$ be the vector of the source entropies and $\boldsymbol{r} = (R_1, R_2, \cdots, R_L)$ be a nonnegative real vector. Then, an $(n, \boldsymbol{\omega}, \boldsymbol{r})$ block code, where n is block length, is defined as follows:

(i) Define a series of mutually independent sources $X_j^{(n)}$, $j = 1, 2, \cdots, S$, uniformly distributed on the alphabet $\mathcal{X}_j = \{0, 1, \cdots, \lceil 2^{nH(X_j)} \rceil - 1\}$, and a secrecy key $\mathbf{K}^{(n)}$ uniformly distributed on the alphabet $\mathcal{K} = \{0, 1, \cdots, \lceil 2^{nH(K)} \rceil - 1\}$;

(ii) For each encoder E_i, $i = 1, 2, \cdots, L$, define its block encoder as an encoding function mapping from the Cartesian product of all the alphabets $\mathcal{X}_j$, $j = 1, 2, \cdots, S$ and the alphabet $\mathcal{K}$ to an alphabet $\mathcal{U}_i = \{0, 1, \cdots, \lceil 2^{nR_i} \rceil - 1\}$, i.e.,

$$\phi_i^{(n)} : \prod_{j=1}^{S} \mathcal{X}_j \times \mathcal{K} \to \mathcal{U}_i; \tag{1}$$

(iii) For each decoder D_j, $j = 1, 2, \cdots, S$, define its block decoder as a decoding function mapping from the Cartesian product of the alphabets $\mathcal{U}_k$, $k \in \mathrm{In}(D_j)$, to the Cartesian product of the first $\mathcal{L}(D_j)$ alphabets $\mathcal{X}_k$, $k = 1, 2, \cdots, \mathcal{L}(D_j)$, i.e.,

$$\mu_j^{(n)} : \prod_{k \in \mathrm{In}(D_j)} \mathcal{U}_k \to \prod_{k=1}^{\mathcal{L}(D_j)} \mathcal{X}_k; \tag{2}$$

(iv) The perfect secrecy constraint is that when any size-m subset of encoders are fully accessed, the eavesdropper obtains nothing on all sources, i.e.,

$$I(\mathbf{X}_{1:S}^{(n)}; \mathbf{U}_{\mathcal{A}}) = 0, \quad \forall\, \mathcal{A} \subseteq \{1, 2, \cdots, L\} \text{ with } |\mathcal{A}| = m, \tag{3}$$

where $\mathbf{X}_{1:S}^{(n)} \triangleq (X_1^{(n)}, X_2^{(n)}, \cdots, X_S^{(n)})$, and $\mathbf{U}_{\mathcal{A}} \triangleq (U_i : i \in \mathcal{A})$ with U_i representing the random variable of the output of the ith block encoder, i.e., $U_i = \phi_i^{(n)}\big(\mathbf{X}_{1:S}^{(n)}, \mathbf{K}^{(n)}\big)$;

For such an $(n, \boldsymbol{\omega}, \boldsymbol{r})$ block code, $\hat{\mathbf{X}}_{1:\mathcal{L}(D_j)}^{(n)} \triangleq \mu_j^{(n)}\big(U_k, k \in \mathrm{In}(D_j)\big)$ is the estimate of the decoder D_j. Considering all the decoders, we define the *maximum probability of block error* as

$$p^{(n)} \triangleq \max_{j=1,2,\cdots,S} \mathbb{P}\Big(\hat{\mathbf{X}}_{1:\mathcal{L}(D_j)}^{(n)} \neq \mathbf{X}_{1:\mathcal{L}(D_j)}^{(n)}\Big). \tag{4}$$

Now, we define an achievable $(n, \boldsymbol{\omega}, \boldsymbol{r})$ block code as follows.

Definition 2: Let $X_1, X_2, \cdots, X_S$ be S mutual independent prioritized sources with entropies $H(X_j)$, $j = 1, 2, \cdots, S$. Let $\boldsymbol{\omega} = \big(H(X_1), H(X_2), \cdots, H(X_S)\big)$ and $\boldsymbol{r} = (R_1, R_2, \cdots, R_L)$ be a nonnegative real vector. We say $\boldsymbol{r}$ is achievable, if $\forall\, \epsilon > 0$, there exists an $(n, \boldsymbol{\omega}, \boldsymbol{r})$ block code for n sufficiently large, i.e., a sequence of block encoders $\phi^{(n)} \triangleq (\phi_i^{(n)} : i = 1, 2, \cdots, L)$ and a sequence of block decoders $\mu^{(n)} \triangleq (\mu_j^{(n)} : j = 1, 2, \cdots, S)$, such that

i) $p^{(n)} < \epsilon$, called the decoding condition; and

ii) the secure condition (3) is satisfied.

Note that the achievability of a rate vector $\boldsymbol{r}$ is related to the source entropy vector $\boldsymbol{\omega}$. So, we usually say that $(\boldsymbol{\omega}, \boldsymbol{r})$ is achievable, if $\boldsymbol{r}$ is achievable for an $(L, m, \mathcal{L})$ S-AMDCS with the source entropy vector $\boldsymbol{\omega}$. Now, we define the secure rate region.

Definition 3: For an $(L, m, \mathcal{L})$ S-AMDCS with S mutual independent prioritized sources $X_1, X_2, \cdots, X_S$, the closure of the set of all achievable $(\boldsymbol{\omega}, \boldsymbol{r})$ is defined as the secure rate region, denoted by $\mathcal{R}_{(L,m,\mathcal{L})}$.

In the next section, we will follow the formulation above to study the secure rate region of a class of networks.

III. Main Results

In this section, we fully characterize the secure rate region of the S-AMDCS with L encoders, security level $L-2$, and a valid decoding level $\mathcal{L}(\cdot)$, which is the next nontrivial class of problems to be tackled, since the problems with security level $L-1$ are equivalent to single source threshold security problems and have been solved in [12] and [20].

For a S-AMDCS with L encoders and security level $L-2$, we see that there are total $L+1$ secure transmissions, and thus $L+1$ decoders $D_1, D_1, \cdots, D_{L+1}$, where L decoders, say $D_1, D_2, \cdots, D_L$, access L size-$(L-1)$ subsets of the encodes, respectively, and another decoder D_{L+1} access the whole set of all encoders. Since we only consider the valid decoding level, we have $S = L+1$, the number of the sources, and we let

$$\begin{aligned} \mathrm{In}(D_j) &= \{E_1, E_2, \cdots, E_L\} \setminus \{E_{L-j+1}\},\ 1 \le j \le L, \\ \mathrm{In}(D_{L+1}) &= \{E_1, E_2, \cdots, E_L\}, \end{aligned} \tag{5}$$

and without loss of generality we assume that D_j is required to decode the sources $(X_1, X_2, \cdots, X_j)$, i.e., $\mathcal{L}(D_j) = j,\ \forall\, j = 1, 2, \cdots, L+1$. Note that in this case each valid decoding level is equivalent to the one we considered here, and so it suffices to consider the above decoding level $\mathcal{L}(\cdot)$, and we write the secure rate region as $\mathcal{R}_{L,L-2}$ for notational simplicity.

A. Superposition Secure Rate Region

Before presenting the exact rate region $\mathcal{R}_{L,L-2}$, we first give an inner bound, the *superposition rate region* $\mathcal{R}^s_{L,L-2}$, which can be achieved by encoding the sources separately [7]. To be specific, each encoder can be divided into several sub-encoders, and we let $r_i^1, r_i^2, \cdots, r_i^{L+1}$ be the sub-rate constraints of the encoder E_i for sources $X_1, X_2, \cdots, X_{L+1}$, respectively, so that the rate constraint on each encoder E_i is

$$R_i = \sum_{j=1}^{L+1} r_i^j, \qquad i = 1, 2, \cdots, L. \tag{6}$$

The secure rate for single source with threshold secrecy was solved (e.g. [12], [20]). Consider each decoder D_d required to decode $X_1, X_2, \cdots, X_d$. Together with the security level $L-2$, we obtain that for each subset $\mathcal{A} \subseteq \mathrm{In}(D_d)$ with $|\mathcal{A}| = L-2$,

$$\sum_{i \in \mathrm{In}(D_d) \setminus \mathcal{A}} r_i^j \ge H(X_j), \quad \forall\, j = 1, 2, \cdots, d. \tag{7}$$

By (7), for decoders D_d, $d = 1, 2, \cdots, L$,

$$r_k^j \ge H(X_j), \quad j = 1, 2, \cdots, d, \quad \text{and} \ \ \forall\, k \in \mathrm{In}(D_d). \tag{8}$$

For the last decoder D_{L+1}, by (7) we have

$$r_i^j + r_k^j \ge H(X_j), \quad j = 1, 2, \cdots, L+1,$$

and

$$i, k \in \mathrm{In}(D_{L+1}) \text{ with } i \ne k. \tag{9}$$

The following theorem characterize the superposition secure rate region $\mathcal{R}^s_{L,L-2}$.

Theorem 1: The superposition secure rate region $\mathcal{R}^s_{L,L-2}$ of the S-AMDCS with L encoders and the security level $L-2$ contains all rate tuples characterized by the following inequalities:

$$R_1 \ge \sum_{i=1}^{L-1} H(X_i); \tag{10}$$

$$R_i \ge \sum_{j=1}^{L} H(X_j), \quad \forall\ 2 \le i \le L; \tag{11}$$

$$R_1 + R_i \ge 2\sum_{j=1}^{L-1} H(X_j) + H(X_L) + H(X_{L+1}), \forall 2 \le i \le L; \tag{12}$$

$$R_i + R_k \ge 2\sum_{j=1}^{L} H(X_j) + H(X_{L+1}), \qquad \forall\ i, k \in \mathrm{In}(D_L) \text{ with } i \ne k. \tag{13}$$

As mentioned in Section I, the superposition coding is optimal for the entire secure rate region for symmetric MDCS. One natural question is whether it is still optimal for the asymmetric case. The answer is negative. In particular, the superposition secure rate region $\mathcal{R}^s_{L,L-2}$ here is not a tight inner bound on $\mathcal{R}_{L,L-2}$, i.e.,

$$\mathcal{R}^s_{L,L-2} \subsetneq \mathcal{R}_{L,L-2}. \tag{14}$$

B. Exact Secure Rate Region

Now, we give the exact secure rate region $\mathcal{R}_{L,L-2}$ as follows.

Theorem 2: The secure rate region $\mathcal{R}_{L,L-2}$ of the S-AMDCS with L encoders and security level $L-2$ contains all rate tuples characterized by the following inequalities:

$$R_1 \ge \sum_{i=1}^{L-1} H(X_i); \tag{15}$$

$$R_i \ge \sum_{j=1}^{L} H(X_j),\ \forall\ 2 \le i \le L; \tag{16}$$

$$R_1 + R_i \ge 2\sum_{j=1}^{L-1} H(X_j) + H(X_L) + H(X_{L+1}), \qquad \forall\ 2 \le i \le L; \tag{17}$$

$$R_2 + R_i \ge 2\sum_{j=1}^{L-1} H(X_j) + H(X_L) + H(X_{L+1}), \qquad \forall\ 3 \le i \le L; \tag{18}$$

$$R_i + R_j \ge 2\sum_{k=1}^{L-i+1} H(X_k) + \sum_{l=L-i+2}^{L+1} H(X_l), \qquad \forall 3 \le i < j \le L. \tag{19}$$

Note that the two classes of extreme rays that are outside $\mathcal{R}^s_{L,L-2}$ cannot be achieved by superposition coding since one has to encode the two sources together instead of separately encoding. Nevertheless, as shown in the achievability proof of Theorem 2 (cf. Section IV), they can be achieved by linear codes. Together with the fact that all the extreme rays of

$\mathcal{R}^s_{L,L-2}$ are achievable by linear codes, according to the proof of Theorem 1, we have the following corollary.

Corollary 1: Main conclusions:

1) Superposition coding in general is not sufficient to achieve the secure rate region of an S-AMDCS and source-crossing coding is necessary.
2) Linear codes are optimal to achieve the secure rate region of the S-AMDCS with L encoders and security level $L-2$.

Note that the region $\mathcal{R}_{L,L-2}$ does not consider the size of the secrecy key K. In fact, there exist basic constraints on the size of the secrecy key to guarantee that the amount of the randomness is sufficient for the required security level. We also investigate the key size for the region $\mathcal{R}_{L,L-2}$ as stated in the following theorem. However, bounds obtained are loose. We leave the issue of finding tighter bounds on the size of the secrecy key as one future work.

Theorem 3: The secrecy key K for the secure rate region $\mathcal{R}_{L,L-2}$ of the S-AMDCS with L encoders and security level $L-2$ satisfies the following inequalities: for $j=1,2$ and $3 \le l \le L$,

$$\frac{1}{L-2}H(K) \ge \sum_{i=1}^{L} H(X_i); \tag{20}$$

$$R_j + \frac{1}{L-2}H(K) \ge 2\sum_{i=1}^{L-1} H(X_i) + H(X_L) + H(X_{L+1}); \tag{21}$$

$$R_l + \frac{1}{L-2}H(K) \ge 2\sum_{i=1}^{L+1-l} H(X_i) + \sum_{k=L+2-l}^{L+1} H(X_k). \tag{22}$$

Furthermore, for $L \le 4$, the secrecy key K also satisfies

$$\frac{2}{L-2}H(K) \ge 2\sum_{i=1}^{L-1} H(X_i) + H(X_L) + H(X_{L+1}). \tag{23}$$

Notably, there is a recent trend of employing a computer-aided approach to solve large-scale information-theoretic problems [9], [10], [21]–[25] and to prove or disprove information inequalities [26]. In particular, these computer-aided software can be used to verify the results for some example networks with the small number of encoders [18], [19].

IV. Proofs

We will prove Theorems 1–3 in this section.

A. Proof of Theorem 1

Converse: We show that (6), (8), and (9) imply (10)–(13) by eliminating the sub-rate variables.

For (10), note that besides the decoder D_{L+1}, the encoder E_1 is only accessible by the decoders $D_1, D_2, \cdots, D_{L-1}$. By (8), we have

$$r_1^j \ge H(X_j),\ j = 1,2,\cdots,L-1. \tag{24}$$

Immediately, we obtain (10) by (6). Similarly, for other encoders E_i, $2 \le i \le L$, which are accessible by D_L, the associated constraints will be

$$r_i^j \ge H(X_j),\ j = 1,2,\cdots,L. \tag{25}$$

This implies (11) by (6).

According to the constraints from the decoder D_{L+1} as shown in (9), for $j = 1,2,\cdots,L+1$, we have

$$r_1^j + r_k^j \ge H(X_j),\ \forall\ 2 \le k \le L. \tag{26}$$

However, since we have the constraints in (24) and (25), the constraints in (26) become redundant for $j=1,2,\cdots,L-1$. In other words, the constraints for $j=1,2,\cdots,L-1$ are

$$r_1^j + r_k^j \ge 2H(X_j),\ \forall\ 2 \le k \le L. \tag{27}$$

Note that (26) is not redundant for $j = L, L+1$. Together with (6), we immediately obtain (12).

Similarly, for $i,k \in \mathrm{In}(D_L) = \{2,3,\cdots,L\}$ with $i \ne k$, applying (25) will make the constraints (9) redundant for $j = 1,2,\cdots,L$ but not redundant for $j = L+1$. Together with (6), we obtain (13).

Achievability: We show that the superposition secure rate region is indeed achievable by superposition coding. In particular, note that the inequalities (10)–(13) form a polyhedral cone. It suffices to prove that (the representative of) each extreme ray of $\mathcal{R}^s_{L,L-2}$ can be achieved by superposition. We know that one extreme ray needs to satisfy all inequalities and make some of them hold with equality. By analyzing (10)–(13) and forcing different subsets of inequalities to hold at equality, we get three classes of non-trivial extreme rays and the achieving codes are as follows.

1) The first class includes $(R_1 = 0, R_i = 1, 2 \le i \le L, H(X_j) = 0, 1 \le j \le L-1, H(X_L) = 1, H(X_{L+1}) = 0)$, $(R_1 = 0,\ R_i = 1,\ 2 \le i \le L,\ H(X_j) = 0, 1 \le j \le L, H(X_{L+1}) = 1)$, and $(R_i = 0,$ for one $i \in \{2,3,\cdots,L\}, R_j = 1, j \ne i, 1 \le j \le L, H(X_j) = 0, 1 \le j \le L, H(X_{L+1}) = 1)$. The first extreme ray can be achieved by using a secrecy key K with size of $L-2$ bits and then let $U_i = X_L + K_{i-1}, 2 \le i \le L-1$ and $U_L = X_L + \sum_{i=1}^{L-2} K_i$, where K_i, $1 \le i \le L-2$ are the bits in the key and the sum is in binary. It is not difficult to check that this achieving code satisfies all the reconstruction and security constraints. The other extreme rays can be achieved by a similar code.
2) The second class includes the following extreme rays: $(R_i = 1, 1 \le i \le L, H(X_j) = 1,$ for one $j \in \{1,2,\cdots,L-1\}, H(X_L) = 0, H(X_{L+1}) = 0)$. It suffices to construct the code for the extreme ray when $H(X_1) = 1$, since this requires the most strict constraints and the other ones can be achieved similarly. The field size of the code to achieve this extreme ray needs to be larger than or equal to $L-1$, because the security constraints require that when the eavesdropper has access to any $L-2$ encoded messages, no information should be released, which means that any $L-2$ messages should be independent. Actually, the code could be $U_i = X_1 + K_i$, $1 \le i \le L-2$, $U_{L-1} = X_1 + \sum_{i=1}^{L-2} K_i$, and $U_L = X_1 + \sum_{i=1}^{L-2} iK_i$,

where the size of the secrecy key is $L-2$. One can check that any $L-2$ messages will not release any information but with $L-1$ messages, the decoder can successfully decode the source.

3) The third class includes the following extreme ray ($R_i = 1, 1 \leq i \leq L, H(X_j) = 0, 1 \leq j \leq L, H(X_{L+1}) = 2$). The achieving code can be $U_i = X_{L+1}^1 + K_i, 1 \leq i \leq L-2$, $U_{L-1} = X_{L+1}^1 + \sum_{i=1}^{L-2} K_i$, and $U_L = X_{L+1}^2 + \sum_{i=1}^{L-2} K_i$, where the size of the secrecy key is $L-2$ and the summation is in arithmetic modulo 2.

This completes the proof. ■

B. Proof of Theorem 2

Converse: We will prove the inequalities (15)–(19) in order. For any point $(\boldsymbol{\omega}, \boldsymbol{r}) \in \mathcal{R}_{L,L-2}$, there exists an $(n, \boldsymbol{\omega}, \boldsymbol{r})$ block code to achieve it with $\epsilon \to 0$. By Fano's inequality, for the decoder $D_j, j = 1, 2, \cdots, L+1$ with input $\text{In}(D_j)$ and output $\mathbf{X}_{1:j}^{(n)}$ we have

$$H(\mathbf{X}_{1:j}^{(n)} | \mathbf{U}_{\text{In}(D_j)}) \leq n\delta_j(n, \epsilon), \tag{28}$$

where $\delta_j(n,\epsilon) = \frac{H(p^{(n)})}{n} + \epsilon \sum_{k=1}^{j} H(X_k)$, denoted by δ_j for notational simplicity if there is no confusion. With $n \to \infty$, we will have $H(\mathbf{X}_{1:j}^{(n)} | \mathbf{U}_{\text{In}(D_j)}) \to 0$.

Recall that, by (5), the decoder D_{L-i+1} has input $\text{In}(D_{L-i+1}) = \{E_1, E_2, \cdots, E_L\} \setminus \{E_i\}$ and output $\mathbf{X}_{1:L-i+1}^{(n)}$, for $i = 1, \ldots, L$. For instance, D_{L-1}, D_L have input $\text{In}(D_{L-1}) = \{E_1, E_2, \cdots, E_L\} \setminus \{E_2\}$, $\text{In}(D_L) = \{E_1, E_2, \cdots, E_L\} \setminus \{E_1\}$ and output $\mathbf{X}_{1:L-1}^{(n)}$, $\mathbf{X}_{1:L}^{(n)}$, respectively. Meanwhile, the decoder D_{L+1} has input $\text{In}(D_{L+1}) = \{E_1, E_2, \cdots, E_L\}$ and output $\mathbf{X}_{1:L+1}^{(n)}$.

For (15), following the constraints on the decoder D_{L-1}, we have

$$\begin{aligned}
n(R_1 + \epsilon) &\geq H(U_1) \geq H(U_1 | \mathbf{U}_{3:L}) && (29)\\
&\geq H(\mathbf{U}_{\text{In}(D_{L-1})}) - H(\mathbf{U}_{3:L}) && (30)\\
&= H(\mathbf{U}_{\text{In}(D_{L-1})}) + H(\mathbf{X}_{1:L+1}^{(n)}) - H(\mathbf{X}_{1:L+1}^{(n)} \mathbf{U}_{3:L}) && (31)\\
&= H(\mathbf{X}_{1:L-1}^{(n)} \mathbf{U}_{\text{In}(D_{L-1})}) - H(\mathbf{X}_{1:L-1}^{(n)} | \mathbf{U}_{\text{In}(D_{L-1})}) \\
&\quad + H(\mathbf{X}_{1:L+1}^{(n)}) - H(\mathbf{X}_{1:L+1}^{(n)} \mathbf{U}_{3:L}) \\
&\geq H(\mathbf{X}_{1:L-1}^{(n)} \mathbf{U}_{\text{In}(D_{L-1})}) + H(\mathbf{X}_{1:L+1}^{(n)}) \\
&\quad - H(\mathbf{X}_{1:L+1}^{(n)} \mathbf{U}_{3:L}) - n\delta_{L-1} && (32)\\
&\geq H(\mathbf{X}_{1:L-1}^{(n)} \mathbf{U}_{3:L}) + H(\mathbf{X}_{1:L+1}^{(n)}) \\
&\quad - H(\mathbf{X}_{1:L+1}^{(n)} \mathbf{U}_{3:L}) - n\delta_{L-1} && (33)\\
&= H(\mathbf{X}_{1:L-1}^{(n)}) + I(\mathbf{U}_{3:L}; X_L^{(n)} X_{L+1}^{(n)} | \mathbf{X}_{1:L-1}^{(n)}) - n\delta_{L-1} \\
&\geq H(\mathbf{X}_{1:L-1}^{(n)}) - n\delta_{L-1} && (34)\\
&= n \sum_{i=1}^{L-1} H(X_i) - n\delta_{L-1}, && (35)
\end{aligned}$$

where (29) follows from the coding rate constraint, (31) follows from the secrecy constraint that $I(\mathbf{X}_{1:L+1}^{(n)}; \mathbf{U}_{3:L}) = 0$, i.e., the eavesdropper obtain nothing on $\mathbf{X}_{1:L+1}^{(n)}$ when he has access to $\mathbf{U}_{3:L}$, (32) is due to the decoding condition (28) for the decoder D_{L-1}, (33) follows from $\text{In}(D_{L-1}) \supseteq \{3, 4, \cdots, L\}$, and (35) is due to the source independence.

Similarly, for (16), by taking into account the constraints on the decoder D_L, we have for $i = 2, 3, \cdots, L$ that

$$\begin{aligned}
n(R_i + \epsilon) &\geq H(U_i) \geq H(U_i | \mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) && (36)\\
&= H(\mathbf{U}_{\text{In}(D_L)}) - H(\mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) \\
&\quad + I(\mathbf{X}_{1:L+1}^{(n)}; \mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) && (37)\\
&= H(\mathbf{U}_{\text{In}(D_L)}) + H(\mathbf{X}_{1:L+1}^{(n)}) \\
&\quad - H(\mathbf{X}_{1:L+1}^{(n)} \mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) && (38)\\
&\geq H(\mathbf{X}_{1:L}^{(n)} \mathbf{U}_{\text{In}(D_L)}) + H(\mathbf{X}_{1:L+1}^{(n)}) \\
&\quad - H(\mathbf{X}_{1:L+1}^{(n)} \mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) - n\delta_L && (39)\\
&\geq H(\mathbf{X}_{1:L}^{(n)} \mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) + H(\mathbf{X}_{1:L+1}^{(n)}) \\
&\quad - H(\mathbf{X}_{1:L+1}^{(n)} \mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) - n\delta_L && (40)\\
&= H(\mathbf{X}_{1:L}^{(n)}) + I(\mathbf{X}_{L+1}^{(n)}; \mathbf{U}_{\text{In}(D_L) \setminus \{i\}} | \mathbf{X}_{1:L}^{(n)}) - n\delta_L && (41)\\
&\geq H(\mathbf{X}_{1:L}^{(n)}) - n\delta_L && (42)\\
&= n \sum_{j=1}^{L} H(X_j) - n\delta_L, && (43)
\end{aligned}$$

where the first inequality in (36) is the coding rate constraint, (37) follows from the security level $L-2$, i.e., $I(\mathbf{X}_{1:L+1}^{(n)}; \mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) = 0$, (39) follows from the decoding condition for the decoder D_L, and (43) follows from the source independence.

For (17), with $i = 2, 3, \cdots, L$, we have

$$\begin{aligned}
&nR_1 + nR_i + 2n\epsilon \\
&\geq H(U_1) + H(U_i) && (44)\\
&\geq H(U_1 | \mathbf{U}_{3:L}) + H(U_i | \mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) \\
&\geq H(U_1 \mathbf{U}_{3:L}) - H(\mathbf{U}_{3:L}) + H(\mathbf{U}_{\text{In}(D_L)}) \\
&\quad - H(\mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) && (45)\\
&\geq \left[H(\mathbf{X}_{1:L-1}^{(n)} \mathbf{U}_{\text{In}(D_{L-1})}) - n\delta_{L-1}\right] \\
&\quad + \left[H(\mathbf{X}_{1:L}^{(n)} \mathbf{U}_{\text{In}(D_L)}) - n\delta_L\right] \\
&\quad - H(\mathbf{U}_{3:L}) - H(\mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) && (46)\\
&= H(\mathbf{X}_{1:L-1}^{(n)} U_1 \mathbf{U}_{3:L}) + H(\mathbf{X}_{1:L}^{(n)} \mathbf{U}_{\text{In}(D_L)}) \\
&\quad - H(\mathbf{U}_{3:L}) - H(\mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) - n\delta_{L-1} - n\delta_L && (47)\\
&= H(\mathbf{X}_{1:L-1}^{(n)} \mathbf{U}_{\text{In}(D_{L-1})}) + H(\mathbf{X}_{1:L}^{(n)} \mathbf{U}_{\text{In}(D_L)}) - n\delta_{L-1} - n\delta_L \\
&\quad + 2H(\mathbf{X}_{1:L+1}^{(n)}) - H(\mathbf{X}_{1:L+1}^{(n)} \mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) \\
&\quad - H(\mathbf{X}_{1:L+1}^{(n)} \mathbf{U}_{\text{In}(D_{L-1}) \setminus \{1\}}) && (48)\\
&\geq H(\mathbf{X}_{1:L-1}^{(n)} \mathbf{U}_{\text{In}(D_{L-1})}) + H(\mathbf{X}_{1:L}^{(n)} \mathbf{U}_{\text{In}(D_L)}) + H(\mathbf{X}_{1:L+1}^{(n)}) \\
&\quad - H(\mathbf{X}_{1:L+1}^{(n)} \mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) + H(\mathbf{X}_{1:L-1}^{(n)}) \\
&\quad - H(\mathbf{X}_{1:L-1}^{(n)} \mathbf{U}_{\text{In}(D_{L-1}) \setminus \{1\}}) - n\delta_{L-1} - n\delta_L && (49)\\
&\geq H(\mathbf{X}_{1:L}^{(n)} \mathbf{U}_{\text{In}(D_L) \cup \{1\}}) - H(\mathbf{X}_{1:L+1}^{(n)} \mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) \\
&\quad + H(\mathbf{X}_{1:L-1}^{(n)}) + H(\mathbf{X}_{1:L+1}^{(n)}) - n\delta_{L-1} - n\delta_L && (50)\\
&\geq \left[H(\mathbf{X}_{1:L+1}^{(n)} \mathbf{U}_{1:L}) - n\delta_{L+1}\right] - H(\mathbf{X}_{1:L+1}^{(n)} \mathbf{U}_{\text{In}(D_L) \setminus \{i\}}) \\
&\quad + H(\mathbf{X}_{1:L-1}^{(n)}) + H(\mathbf{X}_{1:L+1}^{(n)}) - n\delta_{L-1} - n\delta_L && (51)\\
&\geq H(\mathbf{X}_{1:L-1}^{(n)}) + H(\mathbf{X}_{1:L+1}^{(n)}) - n\delta_{L-1} - n\delta_L - n\delta_{L+1} && (52)\\
&= 2n \sum_{j=1}^{L-1} H(X_j) + n[H(X_L) + H(X_{L+1})] \\
&\quad - n\delta_{L-1} - n\delta_L - n\delta_{L+1}, && (53)
\end{aligned}$$

where (44) follows from the coding rate constraints of E_1 and E_i, (45) is due to $I(U_1;\mathbf{U}_{3:L})\geq 0$ and $I(U_i;\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})\geq 0$, (46) follows from $U_1\mathbf{U}_{3:L}=\mathbf{U}_{\mathrm{In}(D_{L-1})}$ and the decoding condition (28) for the decoders D_{L-1} and D_L, (48) is due to the security level $L-2$ and $I(\mathbf{X}^{(n)}_{1:L+1};\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{1\}})=0$, (49) follows from $I(\mathbf{X}^{(n)}_L\mathbf{X}^{(n)}_{L+1};\mathbf{U}_{3:L}|\mathbf{X}^{(n)}_{1:L-1})\geq 0$, (50) holds because of the following inequality

$$\begin{aligned}&[H(\mathbf{X}^{(n)}_{1:L-1}\mathbf{U}_{\mathrm{In}(D_{L-1})})-H(\mathbf{X}^{(n)}_{1:L-1}\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{1\}})]\\&\quad-[H(\mathbf{X}^{(n)}_{1:L}\mathbf{U}_{\mathrm{In}(D_L)\cup\{1\}})-H(\mathbf{X}^{(n)}_{1:L}\mathbf{U}_{\mathrm{In}(D_L)})]\\&=H(U_1|\mathbf{X}^{(n)}_{1:L-1}\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{1\}})-H(U_1|\mathbf{X}^{(n)}_{1:L}\mathbf{U}_{\mathrm{In}(D_L)})\geq 0,\end{aligned}$$

and (51) follows from

$$\begin{aligned}H(\mathbf{X}^{(n)}_{1:L}\mathbf{U}_{1:L})&=H(\mathbf{X}^{(n)}_{1:L+1}\mathbf{U}_{1:L})-H(\mathbf{X}^{(n)}_{L+1}|\mathbf{X}^{(n)}_{1:L}\mathbf{U}_{1:L})\\&=H(\mathbf{X}^{(n)}_{1:L+1}\mathbf{U}_{1:L})-H(\mathbf{X}^{(n)}_{L+1}|\mathbf{U}_{1:L})\\&\geq H(\mathbf{X}^{(n)}_{1:L+1}\mathbf{U}_{1:L})-n\delta_{L+1},\end{aligned}$$

where the last inequality holds due to $\mathrm{In}(D_L)\cup\{1\}=\mathrm{In}(D_{L+1})$ and the decoding condition (28) for the decoder D_{L+1}.

For (18), with $i=3,4,\cdots,L$, we have

$$\begin{aligned}&nR_2+nR_i+2n\epsilon\\&\geq H(U_2)+H(U_i) &(54)\\&\geq H(U_2|\mathbf{U}_{\mathrm{In}(D_L)\setminus\{2\}})+H(U_i|\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{i\}})\\&=H(\mathbf{U}_{\mathrm{In}(D_L)})+H(\mathbf{U}_{\mathrm{In}(D_{L-1})})-H(\mathbf{U}_{\mathrm{In}(D_L)\setminus\{2\}})\\&\quad-H(\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{i\}}) &(55)\\&=H(\mathbf{X}^{(n)}_{1:L}\mathbf{U}_{\mathrm{In}(D_L)})+H(\mathbf{X}^{(n)}_{1:L-1}\mathbf{U}_{\mathrm{In}(D_{L-1})})\\&\quad-H(\mathbf{U}_{\mathrm{In}(D_L)\setminus\{2\}})-H((\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{i\}})-n\delta_{L-1}-n\delta_L &(56)\\&\geq H(\mathbf{X}^{(n)}_{1:L}\mathbf{U}_{\mathrm{In}(D_L)})+H(\mathbf{X}^{(n)}_{1:L-1}\mathbf{U}_{\mathrm{In}(D_{L-1})})\\&\quad+2H(\mathbf{X}^{(n)}_{1:L+1})-H(\mathbf{X}^{(n)}_{1:L+1}\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{i\}})\\&\quad-H(\mathbf{X}^{(n)}_{1:L+1}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{2\}})-n\delta_{L-1}-n\delta_L &(57)\\&\geq H(\mathbf{X}^{(n)}_{1:L}\mathbf{U}_{\mathrm{In}(D_L)})+H(\mathbf{X}^{(n)}_{1:L-1}\mathbf{U}_{\mathrm{In}(D_{L-1})})+H(\mathbf{X}^{(n)}_{1:L+1})\\&\quad-H(\mathbf{X}^{(n)}_{1:L+1}\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{i\}})+H(\mathbf{X}^{(n)}_{1:L-1})\\&\quad-H(\mathbf{X}^{(n)}_{1:L-1}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{2\}})-n\delta_{L-1}-n\delta_L &(58)\\&\geq H(\mathbf{X}^{(n)}_{1:L}\mathbf{U}_{1:L})-H(\mathbf{X}^{(n)}_{1:L+1}\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{i\}})\\&\quad+H(\mathbf{X}^{(n)}_{1:L-1})+H(\mathbf{X}^{(n)}_{1:L+1})-n\delta_{L-1}-n\delta_L &(59)\\&\geq 2n\sum_{j=1}^{L-1}H(X_j)+n[H(X_L)+H(X_{L+1})]\\&\quad-n\delta_{L-1}-n\delta_L-n\delta_{L+1}, &(60)\end{aligned}$$

where (54) follows from the coding rate constraints of E_2 and E_i, (56) is due to the decoding condition (28) for the decoders D_{L-1} and D_L, (57) is due to the security level $L-2$, i.e., $I(\mathbf{X}^{(n)}_{1:L+1};\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{i\}})=0$ and $I(\mathbf{X}^{(n)}_{1:L+1};\mathbf{U}_{\mathrm{In}(D_L)\setminus\{2\}})=0$, (58) follows from $I(\mathbf{X}^{(n)}_L\mathbf{X}^{(n)}_{L+1};\mathbf{U}_{\mathrm{In}(D_L)\setminus\{2\}}|\mathbf{X}^{(n)}_{1:L-1})\geq 0$, (59) follows from the submodularity property of the entropy function and (60) holds following from (50)–(53).

For (19), consider i,j with $3\leq i<j\leq L$. Without loss of generality, we let $i=3,4,\cdots,L$ and $j=4,5,\cdots,L$ with $i<j$. As such, we have i (i.e., U_i) in $\mathrm{In}(D_L)$ and j (i.e., U_j) in $\mathrm{In}(D_{L-2})$. Then, we obtain

$$\begin{aligned}&nR_i+nR_j+2n\epsilon\\&\geq H(U_i)+H(U_j) &(61)\\&\geq H(U_i|\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})+H(U_j|\mathbf{U}_{\mathrm{In}(D_{L-i+1})\setminus\{j\}})\\&=H(\mathbf{U}_{\mathrm{In}(D_L)})-H(\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})\\&\quad+H(\mathbf{U}_{\mathrm{In}(D_{L-2})})-H(\mathbf{U}_{\mathrm{In}(D_{L-i+1})\setminus\{j\}}) &(62)\\&=H(\mathbf{X}^{(n)}_{1:L}\mathbf{U}_{\mathrm{In}(D_L)})+H(\mathbf{X}^{(n)}_{1:L-i+1}\mathbf{U}_{\mathrm{In}(D_{L-i+1})})\\&\quad-H(\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})-H(\mathbf{U}_{\mathrm{In}(D_{L-i+1})\setminus\{j\}})\\&\quad-n\delta_{L-i+1}-n\delta_L &(63)\\&\geq H(\mathbf{X}^{(n)}_{1:L-i+1}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})+H(\mathbf{X}^{(n)}_{1:L}\mathbf{U}_{1:L})\\&\quad-H(\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})-H(\mathbf{U}_{\mathrm{In}(D_{L-i+1})\setminus\{j\}})\\&\quad-n\delta_{L-i+1}-n\delta_L &(64)\\&\geq H(\mathbf{X}^{(n)}_{1:L-i+1}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})+H(\mathbf{X}^{(n)}_{1:L}\mathbf{U}_{1:L})\\&\quad+H(\mathbf{X}^{(n)}_{1:L-i+1})+H(\mathbf{X}^{(n)}_{1:L+1})-H(\mathbf{X}^{(n)}_{1:L-i+1}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})\\&\quad-H(\mathbf{X}^{(n)}_{1:L+1}\mathbf{U}_{\mathrm{In}(D_{L-i+1})\setminus\{j\}})-n\delta_{L-i+1}-n\delta_L &(65)\\&\geq H(\mathbf{X}^{(n)}_{1:L+1}\mathbf{U}_{1:L})+H(\mathbf{X}^{(n)}_{1:L-i+1})+H(\mathbf{X}^{(n)}_{1:L+1})\\&\quad-H(\mathbf{X}^{(n)}_{1:L+1}\mathbf{U}_{\mathrm{In}(D_{L-i+1})\setminus\{j\}})-n\delta_{L-i+1}-n\delta_L &(66)\\&\geq H(\mathbf{X}^{(n)}_{1:L-2})+H(\mathbf{X}^{(n)}_{1:L+1})-n\delta_{L-i+1}-n\delta_L &(67)\\&=2n\sum_{k=1}^{L-i+1}H(X_k)+n\sum_{l=L-i+2}^{L+1}H(X_l)-n\delta_{L-i+1}-n\delta_L, &(68)\end{aligned}$$

where (61) is the coding rate constraints, (62) follows from basic entropy properties, (63) follows from the decoding conditions for the decoders D_{L-i+1} and D_L, (64) follows from $I(U_1;U_i\mathbf{X}_{L-i+2:L+1}|\mathbf{X}^{(n)}_{1:L-i+1}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})\geq 0$, (65) follows from the security level $L-2$, and specifically, $I(\mathbf{X}^{(n)}_{1:L-i+1};\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})=0$ and $I(\mathbf{X}^{(n)}_{1:L+1};\mathbf{U}_{\mathrm{In}(D_{L-i+1})\setminus\{j\}})=0$, (66) follows from the decoding constraints at decoder D_{L+1}, (67) follows from $H(U_iU_j|\mathbf{X}^{(n)}_{1:L+1}\mathbf{U}_{\mathrm{In}(D_{L-i+1})\setminus\{j\}})\geq 0$, and (68) follows from the source independence.

Achievability: Note that the inequalities (15)–(19) form a polyhedral cone. It suffices to prove the achievability of (representative of) each extreme ray, since all the points in the cone can be achieved by time-sharing (conic combination) of the codes achieving the extreme rays. Further, as indicated in (14), the secure rate region $\mathcal{R}_{L,L-2}$ contains the superposition secure rate region $\mathcal{R}^s_{L,L-2}$. Actually, these two regions share some extreme rays. Thus, we only need to focus on the achievability of those extreme rays outside $\mathcal{R}^s_{L,L-2}$.

Note that the two regions, $\mathcal{R}_{L,L-2}$ and $\mathcal{R}^s_{L,L-2}$, have different coefficients in (13), (18), and (19). By analyzing the extreme rays of $\mathcal{R}_{L,L-2}$, we have the two classes outside $\mathcal{R}^s_{L,L-2}$ as follows.

1) The first extreme ray is $(R_i=1, 1\leq i\leq L, H(X_j)=0, 1\leq j\leq L-1, H(X_L)=H(X_{L+1})=1)$. It can be

achieved with $H(K) = L-2$ by letting $U_1 = X_L + X_{L+1} + \sum_{j=1}^{L-2} K_j, U_2 = X_{L+1} + K_1, U_i = X_{L+1} + K_1 + K_{i-1}, 3 \le i \le L-1, U_L = X_L + \sum_{j=2}^{L-2} K_j$, where $K_1, K_2, \cdots, K_{L-2}$ are the $L-2$ bits of the secrecy key and the sum is in binary. It is not difficult to verify that this code can satisfy the decoding and security constraints.

2) The second class of extreme ray is $(R_1 = R_2 = \ldots = R_i = 2, R_j = 1, i+1 \le j \le L, H(X_{L-i+1}) = H(X_{L+1}) = 1, H(X_k) = 0, \forall k \neq L-i+1, L+1)$, where $i = 2, 3, \ldots, L-2$. It can be achieved with $H(K) = L-1$ by letting

$$\begin{aligned}
U_1 &= (X_{L-i+1} + K_1 + K_2 + \ldots + K_{i-1},\\
&\quad X_{L+1} + K_2 + K_3 + \ldots + K_i),\\
U_2 &= (X_{L-i+1} + K_3 + K_4 + \ldots + K_i + K_1,\\
&\quad X_{L+1} + K_4 + K_5 + \ldots + K_i + K_1 + K_2),\\
&\vdots\\
U_i &= (X_{L-i+1} + K_{i-1} + K_i + K_1 + \ldots + K_{i-3},\\
&\quad X_{L+1} + K_i + K_1 + \ldots + K_{i-2},\\
U_{i+1} &= X_{L+1} + \sum_{j=1}^{i+1} K_j\\
U_j &= K_{j-1} + K_j, i+2 \le j \le L-1\\
U_L &= K_{L-1},
\end{aligned}$$

where $K_1, K_2, \cdots, K_{L-1}$ are the $L-1$ bits of the secrecy key K and the sum is in binary. It is not difficult to verify that this code can satisfy the decoding and security constraints.

This completes the proof. ∎

C. Proof of Theorem 3

The following Shearer's lemma [27] is useful in establishing the proof of Theorem 3.

Lemma 1 (Shearer's Lemma): Let $\mathcal{F}$ be a family of subsets of $\{1, 2, \cdots, n\}$ (possibly with repeats) with each $i \in \{1, 2, \cdots, n\}$ included in at least t members of $\mathcal{F}$. For random vector $(X_1, \cdots, X_n)$,

$$tH(X_1, \cdots, X_n) \le \sum_{F \in \mathcal{F}} H(\mathbf{X}_F), \tag{69}$$

where $\mathbf{X}_F$ is the vector $(X_i : i \in F)$.

Now we use it to prove the Theorem 3.

Proof of Theorem 3: We will prove the inequalities (20)–(23) one by one.

For (20), we first have

$$\begin{aligned}
&nH(K)\\
&= H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)}) - H(\mathbf{X}_{1:L+1}^{(n)}) \qquad (70)\\
&= H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)}) + (L-2)H(\mathbf{X}_{1:L}^{(n)})\\
&\quad + \sum_{i=2}^{L}\Big(H(\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}) - H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})\Big)\\
&\quad + \frac{L-2}{L-1}\sum_{i=2}^{L} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})\\
&\quad - \frac{L-2}{L-1}\sum_{i=2}^{L} H(\mathbf{X}_{1:L}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}) \qquad (71)\\
&\ge H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)}) + (L-2)H(\mathbf{X}_{1:L}^{(n)})\\
&\quad + (L-2)H(\mathbf{U}_{\mathrm{In}(D_L)}) - \sum_{i=2}^{L} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})\\
&\quad + \frac{L-2}{L-1}\sum_{i=2}^{L} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})\\
&\quad - \frac{L-2}{L-1}\sum_{i=2}^{L} H(\mathbf{X}_{1:L}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}) \qquad (72)\\
&= H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)}) + (L-2)H(\mathbf{X}_{1:L}^{(n)})\\
&\quad + (L-2)\Big[H(\mathbf{X}_{1:L}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)}) - n\delta_L\Big]\\
&\quad - \frac{1}{L-1}\sum_{i=2}^{L} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})\\
&\quad - \frac{L-2}{L-1}\sum_{i=2}^{L} H(\mathbf{X}_{1:L}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}) \qquad (73)\\
&\ge (L-2)\Big[H(\mathbf{X}_{1:L}^{(n)}) - n\delta\Big] \qquad (74)\\
&\ge (L-2)\Big[n\sum_{i=1}^{L} H(X_i) - n\delta\Big]. \qquad (75)
\end{aligned}$$

Here, (70) follows from the independence between $\mathbf{X}_{1:L+1}^{(n)}$ and $\mathbf{K}^{(n)}$.

Then, we note that, due to the secrecy constraints when $L-2$ encoders are wiretapped,

$$\sum_{i=2}^{L}\Big(H(\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}) - H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})\Big) = -(L-1)H(\mathbf{X}_{1:L+1}^{(n)}), \tag{76}$$

and

$$\begin{aligned}
&\frac{L-2}{L-1}\sum_{i=2}^{L} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})\\
&\quad - \frac{L-2}{L-1}\sum_{i=2}^{L} H(\mathbf{X}_{1:L}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}})\\
&= (L-2)(H(\mathbf{X}_{1:L+1}^{(n)}) - H(\mathbf{X}_{1:L}^{(n)})). \qquad (77)
\end{aligned}$$

By summing (76) and (77) and adding a term $(L-2)H(\mathbf{X}_{1:L}^{(n)})$ to keep the balance of equality, we get (71). Eq. (72) follows from Shearer's lemma that

$$\sum_{i=2}^{L} H(\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}) \ge (L-2)H(\mathbf{U}_{\mathrm{In}(D_L)}). \tag{78}$$

Eq. (73) follows from the decoding constraints at the decoder D_L and (28) that $H(\mathbf{X}_{1:L}^{(n)}|\mathbf{U}_{\mathrm{In}(D_L)}) \le n\delta_L$. To obtain (74), we apply the constraints that

$$H(\mathbf{X}_{1:L}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}) \le H(\mathbf{X}_{1:L}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)})$$
$$H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}) \le H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)})$$
$$H(\mathbf{X}_{1:L+1}^{(n)}K) = H(\mathbf{X}_{1:L+1}^{(n)}K\mathbf{U}_{1:L}) \ge H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}).$$

Eq. (75) follows from the source independence.

For (21), let $j = \{1,2\}\setminus\{i\}, i = 1$ or 2, then

$$\begin{aligned}
&(L-2)n(R_j+\epsilon) + nH(K)\\
&\ge (L-2)H(U_j) + H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)}) - H(\mathbf{X}_{1:L+1}^{(n)}) &(79)\\
&\ge (L-2)\left[H(U_j\mathbf{U}_{3:L}) - H(\mathbf{U}_{3:L})\right] + H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)})\\
&\quad -H(\mathbf{X}_{1:L+1}^{(n)}) &(80)\\
&\ge (L-2)\left[H(U_j\mathbf{U}_{3:L}) - H(\mathbf{U}_{3:L})\right] + (L-2)H(U_i\mathbf{U}_{3:L})\\
&\quad - \sum_{k\in\{i,3:L\}} H(\mathbf{U}_{\{i,3:L\}\setminus k}) + H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)}) - H(\mathbf{X}_{1:L+1}^{(n)}) &(81)\\
&\ge (L-2)\Big[H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{1:L}) + H(\mathbf{X}_{1:L-1}^{(n)}\mathbf{U}_{3:L})\\
&\quad -n\delta_{L-1} - n\delta_L\Big] - \sum_{k\in\{i,3:L\}} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\{i,3:L\}\setminus\{k\}})\\
&\quad -(L-2)H(\mathbf{U}_{3:L}) + H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)})\\
&\quad +(L-2)H(\mathbf{X}_{1:L+1}^{(n)}) &(82)\\
&\ge (L-2)\Big[H(\mathbf{X}_{1:L-1}^{(n)}) + H(\mathbf{X}_{1:L+1}^{(n)}) - n\delta_{L-1} - n\delta_L\Big] &(83)\\
&= (L-2)n\left[2\sum_{k=1}^{L-1} H(X_k) + \sum_{l=L}^{L+1} H(X_l) - \delta_{L-1} - \delta_L\right]. &(84)
\end{aligned}$$

Here, (79) follows from the rate constraint and independence between sources and secrecy key, (80) follows from $I(U_j;\mathbf{U}_{3:L}) \ge 0$, (81) follows from Shearer's lemma that

$$(L-2)H(U_i\mathbf{U}_{3:L}) - \sum_{k\in\{i,3:L\}} H(\mathbf{U}_{\{i,3:L\}\setminus\{k\}}) \le 0. \quad (85)$$

Eq. (82) follows from the decoding conditions of D_{L-1} and D_L and the secrecy constraints.

To obtain (83), by the security level $L-2$, we have

$$H(\mathbf{X}_{1:L-1}^{(n)}\mathbf{U}_{3:L}) = H(\mathbf{X}_{1:L-1}^{(n)}) + H(\mathbf{U}_{3:L}), \quad (86)$$

and

$$\begin{aligned}
&(L-2)H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{1:L}) + H(\mathbf{X}_{1:L+1}^{(n)})\\
&\quad = (L-2)H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{1:L}) + H(\mathbf{U}_{1:L}\mathbf{X}_{1:L+1}^{(n)}) &(87)\\
&\quad \ge \sum_{k\in\{i,3:L\}} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\{i,3:L\}\setminus\{k\}}), &(88)
\end{aligned}$$

where (86) follows from the secrecy constraints, and (87) follows from the fact that all coded messages are functions of sources and secrecy key. Finally, (84) follows from the source independence.

For (22), let $\mathcal{A} = \{3,\cdots,L\}\setminus\{i\}, i = 3,4,\cdots,L$, then, we have

$$\begin{aligned}
&(L-2)n(R_i+\epsilon) + nH(K)\\
&\ge (L-2)H(U_i) + H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)}) - H(\mathbf{X}_{1:L+1}^{(n)}) &(89)\\
&\ge (L-2)\left[H(U_2\mathbf{U}_{3:L}) - H(U_2\mathbf{U}_{\mathcal{A}})\right] + H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)})\\
&\quad -H(\mathbf{X}_{1:L+1}^{(n)}) &(90)\\
&\ge (L-2)\left[H(U_2\mathbf{U}_{3:L}) - H(U_2\mathbf{U}_{\mathcal{A}})\right]\\
&\quad +(L-2)H(U_1U_2\mathbf{U}_{\mathcal{A}}) - \sum_{k\in\mathcal{A}\cup\{1,2\}} H(\mathbf{U}_{\mathcal{A}\cup\{1,2\}\setminus\{k\}})\\
&\quad +H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)}) - H(\mathbf{X}_{1:L+1}^{(n)}) &(91)\\
&\ge (L-2)\Big[H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{1:L}) + H(\mathbf{X}_{1:L+1-i}^{(n)}U_2\mathbf{U}_{\mathcal{A}})\\
&\quad -H(U_2\mathbf{U}_{\mathcal{A}}) - n\delta_{L+1-i} - n\delta_L\Big]\\
&\quad - \sum_{k\in\mathcal{A}\cup\{1,2\}} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathcal{A}\cup\{1,2\}\setminus\{k\}})\\
&\quad +H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)}) + (L-2)H(\mathbf{X}_{1:L+1}^{(n)}) &(92)\\
&\ge (L-2)\Big[H(\mathbf{X}_{1:L+1-i}^{(n)}) + H(\mathbf{X}_{1:L+1}^{(n)})\Big]\\
&\quad -(L-2)n\left[\delta_{L+1-i} - \delta_L\right] &(93)\\
&= (L-2)n\left[2\sum_{k=1}^{L+1-i} H(X_k) + \sum_{l=L+2-i}^{L+1} H(X_l)\right]\\
&\quad -(L-2)n\left[\delta_{L+1-i} - \delta_L\right]. &(94)
\end{aligned}$$

Here, (89) follows from the rate constraint and independence between sources and secrecy key, (90) follows from basic entropy inequality that $I(U_i;U_2\mathbf{U}_{\mathcal{A}}) \ge 0$. Eq. (91) follows from Shearer's lemma that

$$(L-2)H(U_1U_2\mathbf{U}_{\mathcal{A}}) - \sum_{k\in\mathcal{A}\cup\{1,2\}} H(\mathbf{U}_{\mathcal{A}\cup\{1,2\}\setminus\{k\}}) \le 0. \quad (95)$$

Eq. (92) follows from the decoding conditions of D_{L+1-i} and D_L, the security level $L-2$, and submodularity that

$$\begin{aligned}
H(U_2\mathbf{U}_{3:L}) &\ge H(\mathbf{X}_{1:L}^{(n)}U_2\mathbf{U}_{3:L}) - n\delta_L,\\
H(U_1U_2\mathbf{U}_{\mathcal{A}}) &\ge H(\mathbf{X}_{1:L+1-i}^{(n)}U_1U_2\mathbf{U}_{\mathcal{A}}) - n\delta_{L+1-i},\\
H(\mathbf{X}_{1:L}^{(n)}U_2\mathbf{U}_{3:L}) &+ H(\mathbf{X}_{1:L+1-i}^{(n)}U_1U_2\mathbf{U}_{\mathcal{A}})\\
&\ge H(\mathbf{X}_{1:L}^{(n)}\mathbf{U}_{1:L}) + H(\mathbf{X}_{1:L+1-i}^{(n)}U_2\mathbf{U}_{\mathcal{A}}),\\
H(\mathbf{X}_{1:L}^{(n)}\mathbf{U}_{1:L}) &= H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{1:L}).
\end{aligned}$$

Eq. (93) follows from the secrecy constraint that

$$H(\mathbf{X}_{1:L+1-i}^{(n)}U_2\mathbf{U}_{\mathcal{A}}) = H(\mathbf{X}_{1:L+1-i}^{(n)}) + H(U_2\mathbf{U}_{\mathcal{A}}).$$

Eq. (94) follows from the source independence.

For (23), we have

$$\begin{aligned}
&2nH(K)\\
&= 2H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)}) - 2H(\mathbf{X}_{1:L+1}^{(n)}) &(96)\\
&= 2H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)}) - \sum_{i\in\{1,3:L\}} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{i\}})\\
&\quad -\sum_{i=2}^{L} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}) + \sum_{i\in\{1,3:L\}} H(\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{i\}})\\
&\quad +\sum_{i=2}^{L} H(\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}) + 2(L-2)H(\mathbf{X}_{1:L+1}^{(n)}) &(97)
\end{aligned}$$

$$\begin{aligned}
&\geq 2H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)}) - \sum_{i\in\{1,3:L\}} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{i\}}) \\
&\quad -\sum_{i=2}^{L} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}) + (L-2)H(\mathbf{U}_{\mathrm{In}(D_{L-1})}) \\
&\quad +(L-2)H(\mathbf{U}_{\mathrm{In}(D_L)}) + 2(L-2)H(\mathbf{X}_{1:L+1}^{(n)}) \qquad (98) \\
&\geq -\sum_{i\in\{1,3\}} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{i\}}) + 2(L-2)H(\mathbf{X}_{1:L+1}^{(n)}) \\
&\quad -\sum_{i\in\{2,3\}} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}) \\
&\quad +(L-2)\left[H(\mathbf{U}_{\mathrm{In}(D_{L-1})}) + H(\mathbf{U}_{\mathrm{In}(D_L)})\right] \qquad (99) \\
&\geq -\sum_{i\in\{1,3\}} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{i\}}) + 2(L-2)H(\mathbf{X}_{1:L+1}^{(n)}) \\
&\quad -\sum_{i\in\{2,3\}} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}) - (L-2)(n\delta_{L-1} - n\delta_L) \\
&\quad +(L-2)H(\mathbf{X}_{1:L-1}^{(n)}\mathbf{U}_{\mathrm{In}(D_{L-1})}) \\
&\quad +(L-2)H(\mathbf{X}_{1:L}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)}) \qquad (100) \\
&\geq -\sum_{i\in\{1,3\}} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{i\}}) + 2(L-2)H(\mathbf{X}_{1:L+1}^{(n)}) \\
&\quad -\sum_{i\in\{2,3\}} H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}) - (L-2)(n\delta_{L-1} - n\delta_L) \\
&\quad +(L-2)\left[H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{U}_{1:L}) + H(\mathbf{X}_{1:L-1}^{(n)}\mathbf{U}_{3:L})\right] \qquad (101) \\
&\geq (L-2)\left(H(\mathbf{X}_{1:L-1}^{(n)}) + H(\mathbf{X}_{1:L+1}^{(n)})\right) \\
&\quad -(L-2)(n\delta_{L-1} - n\delta_L) \qquad (102) \\
&= n(L-2)\left[2\sum_{i=1}^{L-1} H(X_i) + H(X_L) + H(X_{L+1})\right] \\
&\quad -(L-2)(n\delta_{L-1} - n\delta_L). \qquad (103)
\end{aligned}$$

Here, (96) follows from the independence between sources and secrecy key, (97) follows from the secrecy constraints $I(\mathbf{X}_{1:L+1}^{(n)}; \mathbf{U}_{\mathrm{In}(D_{L-1})\setminus\{i\}}) = 0$, $i = 1, 2, \cdots, L$ with $i \neq 2$ and $I(\mathbf{X}_{1:L+1}^{(n)}; \mathbf{U}_{\mathrm{In}(D_L)\setminus\{i\}}) = 0, i = 2, 3, \cdots, L$, and (98) follows from Shearer's lemma on the variables $\{U_1, U_3, U_4, \cdots, U_L\}$ and $\{U_2, U_3, \cdots, U_L\}$. To obtain (99), we note that every coded message is a function of the sources and the key. Thus, we have

$$H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)}) = H(\mathbf{X}_{1:L+1}^{(n)}\mathbf{K}^{(n)}\mathbf{U}_{1:L}). \qquad (104)$$

Eq. (100) follows from the decoding conditions for D_{L-1} and D_L that $H(\mathbf{X}_{1:L-1}^{(n)}|\mathbf{U}_{\mathrm{In}(D_{L-1})}) \geq n\delta_{L-1}$ and $H(\mathbf{X}_{1:L}^{(n)}|\mathbf{U}_{\mathrm{In}(D_L)}) \geq n\delta_L$. To obtain (101), we apply the submodularity and the decoding conditions for D_{L+1}. For $L \leq 4$, (102) naturally follows from the non-negativity of condition entropy. Eq. (103) follows from the source independence. ■

V. Conclusion

Motivated by the security requirements in future networks with sources of different levels of importance, we investigated the fundamental perfect secrecy limits on the secure rate region of a class of asymmetric multilevel diversity coding systems. We provide characterizations of superposition and full secure rate region for this class of AMDCS. In contrast to the symmetric case, it is shown that superposition coding is not optimal for the secure asymmetric case. Finally, fundamental limits on the size of the secrecy keys have been discussed.

It is interesting as future work to study problems with arbitrary security level, improve the fundamental limits on the key size, and their practical implications. These fundamental limits may provide a guiding principle on the design of network security and the distribution of secrecy key for many real applications, such as cognitive radio networks and wireless networks.

Acknowledgment

The authors would like to thank the editor and the anonymous reviewers for their valuable suggestions and comments that helped to greatly improve the paper.

References

[1] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[2] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao. (Jan. 2018). "A survey of physical layer security techniques for 5G wireless networks and challenges ahead." [Online]. Available: https://arxiv.org/abs/1801.05227

[3] C. W. Tan, *Cognitive Radio Networks: Performance, Applications and Technology*. New York, NY, USA: Nova, 2018.

[4] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.

[5] J. R. Roche, "Distributed information storage," Ph.D. dissertation, Dept. Statist., Stanford Univ., Stanford, CA, USA, Mar. 1992.

[6] R. W. Yeung, "Multilevel diversity coding with distortion," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 412–422, Mar. 1995.

[7] R. W. Yeung and Z. Zhang, "On symmetrical multilevel diversity coding," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 609–621, Mar. 1999.

[8] S. Mohajer, C. Tian, and S. N. Diggavi, "Asymmetric multilevel diversity coding and asymmetric Gaussian multiple descriptions," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4367–4387, Sep. 2010.

[9] C. Li, S. Weber, and J. M. Walsh, "Multilevel diversity coding systems: Rate regions, codes, computation, & forbidden minors," *IEEE Trans. Inf. Theory*, vol. 63, no. 1, pp. 230–251, Jan. 2017.

[10] C. Li, S. Weber, and J. M. Walsh, "On multi-source networks: Enumeration, rate region computation, and hierarchy," *IEEE Trans. Inf. Theory*, vol. 63, no. 11, pp. 7283–7303, Nov. 2017.

[11] C. Li, J. Walsh, and S. Weber, "Matroid bounds on the region of entropic vectors," in *Proc. 51st Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2013, pp. 796–803.

[12] N. Cai and R. W. Yeung, "Secure network coding on a wiretap network," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424–435, Jan. 2011.

[13] S. El Rouayheb, E. Soljanin, and A. Sprintson, "Secure network coding for wiretap networks of type II," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1361–1371, Mar. 2012.

[14] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[15] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *AT&T Bell Lab. Tech. J.*, vol. 63, no. 10, pp. 2135–2157, 1984.

[16] A. Balasubramanian, H. D. Ly, S. Li, T. Liu, and S. L. Miller, "Secure symmetrical multilevel diversity coding," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3572–3581, Jun. 2013.

[17] J. Jiang, N. Marukala, and T. Liu, "Symmetrical multilevel diversity coding and subset entropy inequalities," *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 84–103, Jan. 2014.

[18] C. Li and X. Guang, "Asymmetric multilevel diversity coding systems with perfect secrecy," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8558–8562, Sep. 2017.

[19] C. Li, X. Guang, C. W. Tan, and R. W. Yeung, "On secure asymmetric multilevel diversity coding systems," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2017, pp. 2138–2142.

[20] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[21] C. Li, J. M. Walsh, and S. Weber, "A computational approach for determining rate regions and codes using entropic vector bounds," in *Proc. 50th Annu. Allerton Conf. Commun., Control Comput.*, Oct. 2012, pp. 1580–1587.

[22] C. Li, J. Apte, J. M. Walsh, and S. Weber, "A new computational approach for determining rate regions and optimal codes for coded networks," in *Proc. IEEE Int. Symp. Netw. Coding*, Jun. 2013, pp. 1–6.

[23] C. Tian, "Characterizing the rate region of the (4,3,3) exact-repair regenerating codes," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 5, pp. 967–975, May 2014.

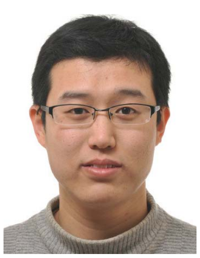
[24] C. Li, S. Weber, and J. M. Walsh, "Computer aided proofs for rate regions of independent distributed source coding problems," in *Proc. IEEE Int. Symp. Netw. Coding (NetCod)*, Jun. 2015, pp. 81–85.

[25] J. Apte and J. M. Walsh. (2016). "Explicit polyhedral bounds on network coding rate regions via entropy function region: Algorithms, symmetry, and computation." [Online]. Available: https://arxiv.org/abs/1607.06833

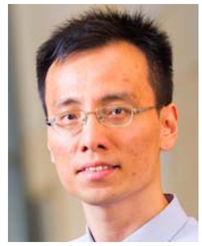
[26] S.-W. Ho, C. W. Tan, and R. W. Yeung, "Proving and disproving information inequalities," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2014, pp. 2814–2818.

[27] F. R. K. Chung, R. L. Graham, P. Frankl, and J. B. Shearer, "Some intersection theorems for ordered sets and graphs," *J. Combinat. Theory, A*, vol. 43, no. 1, pp. 23–37, 1986.

Congduan Li (S'11–M'15) received the B.S. degree from the University of Science and Technology Beijing, China, in 2008, the M.S. degree from Northern Arizona University, Flagstaff, AZ, USA, in 2011, and the Ph.D. degree from Drexel University, Philadelphia, PA, USA, in 2015, respectively, all in electrical engineering. From 2015 to 2016, he was a Post-Doctoral Research Fellow with the Institute of Network Coding, The Chinese University of Hong Kong. He is currently a Post-Doctoral Research Fellow with the Department of Computer Science, City University of Hong Kong. His research interests lie in the broad areas related with networks, such as coding, security, wireless, storage, and caching.



Xuan Guang (M'12) received the Ph.D. degree in mathematics from Nankai University, Tianjin, China, in 2012. From 2011 to 2012, he was a Visiting Researcher and a Post-Doctoral Research Fellow with the Ming Hsieh Department of Electrical Engineering, University of Southern California, Los Angeles, CA, USA. He is currently an Associate Professor with Nankai University. He is also with the Institute of Network Coding, The Chinese University of Hong Kong, by the Hong Kong Scholars Program. His research interests include network coding theory, network computation theory, and network information theory.



Chee Wei Tan (M'08–SM'12) received the M.A. and Ph.D. degrees in electrical engineering from Princeton University, Princeton, NJ, USA. He was a Post-Doctoral Scholar with the California Institute of Technology, Pasadena, CA, USA. He was a Visiting Faculty with Qualcomm R&D, San Diego, CA, USA, in 2011. He is currently an Associate Professor with the City University of Hong Kong. His research interests are in networks and graph analytics, statistical inference, cyber-security, convex optimization theory, and its applications. He was a recipient of the 2008 Princeton University Wu Prize for Excellence. He was the Chair of the IEEE Information Theory Society Hong Kong Chapter and received the 2015 Chapter of the Year Award. He was twice selected to participate at the U.S. National Academy of Engineering China-America Frontiers of Engineering Symposium in 2013 and 2015, respectively. He currently serves as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE/ACM TRANSACTIONS ON NETWORKING.

Raymond W. Yeung (S'85–M'88–SM'92–F'03) was born in Hong Kong in 1962. He received the B.S., M.Eng., and Ph.D. degrees in electrical engineering from Cornell University, Ithaca, NY, USA, in 1984, 1985, and 1988, respectively.

He was on leave at the Ecole Nationale Supérieure des Télécommunications, Paris, France, in 1986. He was a Member of Technical Staff of AT&T Bell Laboratories from 1988 to 1991. Since 1991, he has been with The Chinese University of Hong Kong, where he is currently a Choh-Ming Li Professor of information engineering and the Co-Director of the Institute of Network Coding. He has held visiting positions at Cornell University, Nankai University, the University of Bielefeld, the University of Copenhagen, the Tokyo Institute of Technology, the Munich University of Technology, and Columbia University. He was a Consultant in a project of the Jet Propulsion Laboratory, Pasadena, CA, USA, for salvaging the malfunctioning Galileo Spacecraft and a Consultant for NEC, USA. His 25-bit synchronization marker was used onboard the Galileo Spacecraft for image synchronization.

His research interests include information theory and network coding. He is the author of the textbooks *A First Course in Information Theory* (Kluwer Academic/Plenum, 2002) and its revision *Information Theory and Network Coding* (Springer, 2008), which have been adopted by over 100 institutions around the world. This book has also been published in Chinese (Higher Education Press, 2011) translation by Ning Cai *et al.*. In 2014, he gave the first MOOC on information theory that reached over 25 000 students.

Dr. Yeung was a member of the Board of Governors of the IEEE Information Theory Society from 1999 to 2001. He has served on the committees of a number of information theory symposiums and workshops. He was the General Chair of the First and Fourth Workshops on Network, Coding, and Applications (NetCod 2005 and 2008), a Technical Co-Chair for the 2006 IEEE International Symposium on Information Theory, a Technical Co-Chair for the 2006 IEEE Information Theory Workshop, Chengdu, China, and a General Co-Chair of the 2015 IEEE International Symposium on Information Theory. He was an Associate Editor for Shannon Theory of the *IEEE Transactions on Information Theory* from 2003 to 2005. He currently serves as an Editor-at-Large of *Communications in Information and Systems* and an Editor of *Foundation and Trends in Communications and Information Theory* and *Foundation and Trends in Networking*. From 2011 to 2012, he serves as a Distinguished Lecturer of the IEEE Information Theory Society.

He is a fellow of the Hong Kong Academy of Engineering Sciences and the Hong Kong Institution of Engineers. He was a recipient of the Croucher Foundation Senior Research Fellowship from 2000 to 2001, the Best Paper Award (Communication Theory) of the 2004 International Conference on Communications, Circuits and System, the 2005 IEEE Information Theory Society Paper Award, the Friedrich Wilhelm Bessel Research Award of the Alexander von Humboldt Foundation in 2007, and the 2016 IEEE Eric E. Sumner Award for pioneering contributions to the field of network coding. In 2015, he was named (together with Z. Zhang) an Outstanding Overseas Chinese Information Theorist by the China Information Theory Society.