On Secure Asymmetric Multilevel Diversity Coding Systems

Congduan Li*, Xuan Guang†, Chee Wei Tan*, Raymond W. Yeung†
*Department of Computer Science, City University of Hong Kong,
† Institute of Network Coding, The Chinese University of Hong Kong

***Abstract*—Whether superposition (source separation) is optimal for the asymmetric multilevel diversity coding systems (AMDCS) with perfect secrecy is answered in this paper by studying a non-trivial example. 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 can get nothing about the sources, as long as the size of the subset is not above the security level. The secure AMDCS (S-AMDCS) with five sources, four encoders and security level two is solved and it is shown that linear codes are optimal for this instance. However, in contrast with the secure symmetric multilevel diversity coding systems (S-SMDCS), superposition is shown to be not optimal for S-AMDCS in general from this counterexample.**

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

I. Introduction

As one of the earliest models of modern communication and storage networks, multilevel diversity coding systems (MDCS) were introduced in [1], [2], where the sources are assumed to be prioritized, and a source with higher priority must be decoded before a source with lower priority is decoded. The sources are coded and transmitted (or stored) by multiple encoders under the coding rates, and demanded by multiple sinks, where each sink has access to a certain subset of the transmissions (or storages) and require the first several sources. The applications of this model includes the transmission of images or videos, in which circumstance, the image and video sources may be coded at different levels of resolution and a sink demanding higher resolution may need to decode the lower-resolution part 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 [3] and it is shown that superposition (source separation) coding is optimal. In [4], a model without symmetry named 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., can decode different number of first sources. The case with only three encoders was solved in [4] and it is shown that superposition is not optimal. Some recent results on general MDCS with more than three encoders and further general multi-source networks can be found in [5], [6], where the optimality of different codes are examined, including superposition and simple linear codes.

These models focus on the rate regions, which characterize the relations between coding rates and source entropies for reliable communications, without consideration of secrecy. Nowadays, information security is as crucial as reliable communications [7], [8]. We are interested in the *perfect* or *information-theoretic* secrecy, proposed in [9], that the eavesdropper can get nothing about the source information with access to a wiretap set of channels. As will be shown, the wiretap channel II [10], which contains all subsets of the channels (encoders) with a fixed size (referred as security level in this paper), is considered in this paper. [11], [12] consider secure SMDCS (S-SMDCS) and showed that superposition is optimal for the sum-rate and furthermore the entire admissible rate region. We will investigate secure AMDCS (S-AMDCS) and see if the optimality of superposition still holds.

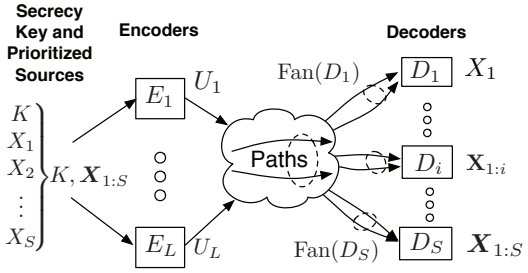


Figure 1: Diagram of an S-AMDCS.

The smallest non-trivial S-AMDCS with four sources, three encoders and security level 1 was studied initially in [13]. In this paper, we study a more complicated S-AMDCS example with five sources, four encoders and security level 2 (which actually includes the smallest non-trivial case as a special instance), and we show that the superposition secure rate region does not match with the full secure rate region. Thus, it indicates that optimality of superposition does not hold for this case and hence S-AMDCS in general. However, simple linear codes do suffice for the entire secure rate region of the example network.

II. Problem Formulation

We first introduce the system model and then define its secure rate region.

A. Secure Asymmetric Multilevel Diversity Coding Systems

In S-AMDCS, we add the threshold perfect secrecy constraints to the AMDCS model introduced in [4]. Specifically, in

978-1-5090-4096-4/17/$31.00 ©2017 IEEE

an S-AMDCS (Fig. 1), it is assumed to have L encoders (channels) $E_1, \ldots, E_L$ with associated output variables $U_1, \ldots, U_L$ and rates $R_1, \ldots, R_L$. Each encoder has access to all the independent prioritized sources $X_1, \ldots, X_S$ and the secrecy key K, which are i.i.d. in time. The eavesdropper may have access to any one but not more than one size-m subset of the encoders, where m is called the *security level*. Hence, a secure transmission must contain at least $m+1$ encoders. We consider the most general case that all the possible secure transmissions are used and each decoder has a distinct decoding level. Thus, there will be $S = \sum_{i=m+1}^{L} \binom{L}{i}$ decoders and a level-i decoder $D_i, i = 1, \ldots, S$ has access to a secure transmission $\mathrm{Fan(D_i)} \subseteq \{\mathrm{E_1}, \ldots, \mathrm{E_L}\}$ with $|\mathrm{Fan(D_i)}| > \mathrm{m}$ and is able to decode the first i sources $\mathbf{X}_{1:i}$.

Note that not all bipartite matchings between secure transmissions and decoders are valid. For instance, if $\mathrm{Fan(D_i)} \subsetneq \mathrm{Fan(D_j)}, \mathrm{i} \neq \mathrm{j}$, we usually have that the level of D_j is larger than that of D_i. Precisely, we define a valid *ordering* for the bipartite matching as follows.

Definition 1. *Let $\mathcal{P} = \{\mathcal{A} \subseteq \{E_1, \ldots, E_L\} : |\mathcal{A}| > m\}$ be all secure transmissions and $S = |\mathcal{P}|$. A valid ordering is an one-to-one mapping $\mathcal{L}$: $\mathcal{P} \to \{1, \ldots, S\}$ such that $\mathcal{B} \subset \mathcal{C}$ implies $\mathcal{L}(\mathcal{B}) < \mathcal{L}(\mathcal{C})$.*

An S-AMDCS instance can be determined by the tuple $(L, m, \mathcal{L})$ of the number of encoders, security level and ordering of secure transmissions. This is a general model so that the symmetric case is actually included in it. For example, the symmetric case of the 4-encoder MDCS with security level 2 can be obtained by letting X_2, X_3, X_4 be empty variables in Fig. 2.

B. Secure Rate Region Formulation

After introducing the system model, we now define a block code for it and then the secure rate region. For an $(L, m, \mathcal{L})$ S-AMDCS, we define an $(n, \boldsymbol{\omega}, \boldsymbol{r})$ block code, with $\boldsymbol{\omega} = [H(X_1), \ldots, H(X_S)]$, $\boldsymbol{r} = [R_1, \ldots, R_L]$.

(i) There exist a series of mutually independent sources $X_i^{(n)}, i \in \{1, \ldots, S\}$ distributed in $\mathcal{W} = \{1, \ldots, \lceil 2^{nH(X_i)} \rceil\}$, and secrecy keys $K^{(n)}$ distributed in $\mathcal{K} = \{1, \ldots, \lceil 2^{nH(K)} \rceil\}$.

(ii) The block encoders, one for each encoder i, are functions that map a block of n source observations from all sources and the secrecy key to one of $\lceil 2^{nR_i} \rceil$ different descriptions in $\mathcal{U}_i = \{0, 1, \ldots, \lceil 2^{nR_i} \rceil - 1\}$,

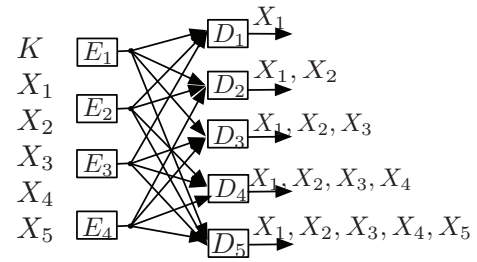
$$\phi_i^{(n)} : \prod_{j \in \{1,\ldots,S\}} \mathcal{X}_j \times \mathcal{K} \to \mathcal{U}_i, i \in \{1, \ldots, L\}. \quad (1)$$

(iii) The perfect secrecy constraints that when any size-m subset of the encoders are accessed, the eavesdropper can get nothing. That is,

$$I(\mathbf{X}_{1:S}^n; \mathbf{U}_{\mathcal{A}}) = 0, \mathcal{A} \subset \{E_1, \ldots, E_L\}, |\mathcal{A}| = m, \quad (2)$$

(iv) The block decoders are functions that map observations of $\mathrm{Fan(D_i)}$ to the files $\mathcal{X}_{1:i}$,

$$\mu_i^{(n)} : \prod_{j \in \mathrm{Fan(D_i)}} \mathcal{U}_j \to \prod_{k=1}^{i} \mathcal{X}_k. \quad (3)$$



$$security : I(\mathbf{X}_{1:5}; \mathbf{E}_{i,j}) = 0, i, j \in \{1, 2, 3, 4\}$$

Figure 2: The 4-encoder AMDCS with security level 2.

(v) Denote the estimate at sink side as $\hat{\mathbf{X}}_{1:i} \triangleq \mu_i^{(n)}(\mathrm{Fan(D_i)})$. Consider all the sinks and define the maximum probability of block error as

$$p^{(n)} = \max_{i \in \{1,\ldots,S\}} \mathbb{P}(\hat{\mathbf{X}}_{1:i} \neq \mathbf{X}_{1:i}). \quad (4)$$

After defining a code, we now define the secure rate region.

Definition 2. *The secure rate region $\mathcal{R}_{L,m}$ of an S-AMDCS with ordering $\mathcal{L}$ is the closure of the set of all achievable vectors $(\boldsymbol{\omega}, \boldsymbol{r})$, where a vector is achievable if there exist a sequence of encoders $\{\phi^{(n)} = [\phi_i^{(n)} | i = 1, \ldots, L]\}$ satisfying rate constraints that $\frac{1}{n} \log |\mathcal{U}_i| \leq R_l + \epsilon_n$, perfect secrecy constraints* (2)*, and decoders $\{\mu^{(n)} = [\mu_i^{(n)} | i = 1, \ldots, S]\}$ such that $\epsilon_n \to 0$, $p^{(n)} \to 0$ as $n \to \infty$.*

In the next section, we will follow the formulation above to study a particular example.

III. Main Results

In this section, we fully characterize the rate region $\mathcal{R}_{4,2}$ of the 4-encoder S-AMDCS security level 2. It is not difficult to see that there are five possible secure transmissions and thus we have five sources. Furthermore, it suffices to consider the case with the following ordering $\mathcal{L}_1(E_1E_2E_3) = 1, \mathcal{L}_1(E_1E_2E_4) = 2, \mathcal{L}_1(E_1E_3E_4) = 3, \mathcal{L}_1(E_2E_3E_4) = 4, \mathcal{L}_1(E_1E_2E_3E_4) = 5$, as shown in Fig. 2, since all the other orderings are simply permutations of this case on the encoders.

Before presenting the exact rate region $\mathcal{R}_{4,2}$, we first present an inner bound on it, namely the superposition rate region $\mathcal{R}_{4,2}^s$, which can be achieved by coding the sources separately [3]. Since the sources are coded separately, each encoder can be divided into several sub-encoders and thus, the rate constraints on each encoder is

$$R_i = r_i^1 + r_i^2 + r_i^3 + r_i^4 + r_i^5, \quad 1 \leq i \leq 4 \quad (5)$$

where, $r_i^1, \ldots, r_i^5$ are the sub-rate constraints for sources $X_1, \ldots, X_5$ respectively.

From the literature (e.g. [14], [7]), we know that the secure rate for single source with threshold secrecy is solved. Thus, for a decoder D_d with input $\mathrm{Fan}(D_d)$ and output $X_1, \ldots, X_d$, where d indicates up to which level of source this decoder can recover, we can write the secrecy rate constraints for security level as follows.

$$\sum_{i \in \binom{\mathrm{Fan}(D_d)}{|\mathrm{Fan}(D_d)|-2}} r_i^j \geq H(X_j), \forall j = 1, \ldots, d, \quad (6)$$

where $\binom{\mathrm{Fan}(D_d)}{|\mathrm{Fan}(D_d)|-2}$ indicate all possible selections of encoders in the input excluding two of them, since the security level is 2.

Specifically, from the decoder D_1 in Fig. 2, we will have the constraints $r_i^1 \geq H(X_1), i = 1, 2, 3$. From the decoder D_2 in Fig. 2, we will have the following constraints for sources $X_j, j = 1, 2$,

$$r_i^j \geq H(X_j), i = 1, 2, 4. \tag{7}$$

Then, from the decoder D_3 in Fig. 2, we will have the following constraints for sources $X_j, j = 1, \ldots, 3$,

$$r_i^j \geq H(X_j), i = 1, 3, 4. \tag{8}$$

Similarly, from the decoder D_4 in Fig. 2, we will have the following constraints for sources $X_j, j = 1, \ldots, 4$,

$$r_i^j \geq H(X_j), i = 2, 3, 4. \tag{9}$$

Finally, from the decoder D_5, we will have the following constraints for sources $X_j, j = 1, \ldots, 5$,

$$r_1^j + r_i^j \geq H(X_j), i = 2, 3, 4 \tag{10}$$

$$r_2^j + r_i^j \geq H(X_j), i = 3, 4 \tag{11}$$

$$r_3^j + r_4^j \geq H(X_j). \tag{12}$$

By taking into account all constraints from all decoders and eliminating the sub-rate variables, we can characterize the $\mathcal{R}_{4,2}^s$ as follows.

Theorem 1. *With the ordering $\mathcal{L}_1$, the superposition rate region $\mathcal{R}_{4,2}^s$ of the 4-encoder AMDCS with security level 2 contains all rate tuples characterized by the following inequalities:*

$$R_i \geq \sum_{i=j}^{3} H(X_j), \quad i = 1, 2, 3, 4 \tag{13}$$

$$R_1 + R_i \geq 2\sum_{j=1}^{3} H(X_j) + \sum_{l=4}^{5} H(X_l), \ i = 2, 3, 4 \tag{14}$$

$$R_2 + R_i \geq 2\sum_{j=1}^{4} H(X_j) + H(X_5), i = 3, 4 \tag{15}$$

$$R_3 + R_4 \geq 2\sum_{i=1}^{4} H(X_i) + H(X_5) \tag{16}$$

Proof: It is not difficult to show that (7)–(12) imply (13)–(16). We only need to show that the rate region is indeed superposition achievable. Note that the inequalities (13)–(16) form a polyhedral cone. It suffices to prove (the representative of) each extreme ray of $\mathcal{R}_{4,2}^s$ can be achieved by superposition. The non-trivial extreme rays of $\mathcal{R}_{4,2}^s$ are listed in Table I, where each row represents an extreme ray. They are all superposition coding achievable. For those extreme rays with only one non-zero value for the source entropies, in order to add sufficient randomness for the security purpose, one needs $H(K) = 2$. These extreme rays can easily be achieved. For instance, $(1, 1, 1, 0, 0, 0, 0, 0, 1)$ can be achieved with $H(K) = 2$ by letting $U_1 = X_5 + K_1, U_2 = X_5 + K_2$, and $U_3 = X_5 + K_2 + K_1$, where K_1, K_2 are the two bits of K. Similar constructions can achieve the other extreme rays with only one non-zero entry at source entropies. For the ray $(1, 1, 1, 1, 0, 0, 0, 0, 2)$, one may still need $H(K) = 2$ to guarantee the security. Actually, with $H(K) = 2$, it can be achieved by letting $U_1 = X_5^1 + K_1, U_2 = X_5^2 + K_2, U_3 = X_5^1 + K_2 + K_1$ and $U_4 = X_5^2 + K_1 + K_2$, where X_5^1, X_5^2 are the two bits of X_5. ■

Table I: Extreme rays of $\mathcal{R}_{4,2}$.

R_1	R_2	R_3	R_4	$H(X_1)$	$H(X_2)$	$H(X_3)$	$H(X_4)$	$H(X_5)$
1	1	1	1	0	0	1	0	0
1	1	1	1	1	0	0	0	0
1	1	1	1	0	1	0	0	0
1	1	0	1	0	0	0	0	1
1	1	1	1	0	0	0	0	2
1	0	1	1	0	0	0	0	1
0	1	1	1	0	0	0	1	0
0	1	1	1	0	0	0	0	1
1	1	1	0	0	0	0	0	1

As mentioned in §I, superposition is optimal for the entire secure rate region for symmetric MDCS. One natural question is if it is still optimal for the asymmetric case. It turns out to be not the case. The superposition rate region $\mathcal{R}_{4,2}^s$ is actually an inner bound on $\mathcal{R}_{4,2}$, i.e., $\mathcal{R}_{4,2}^s \subsetneq \mathcal{R}_{4,2}$.

We give the exact secure rate region $\mathcal{R}_{4,2}$ as follows.

Theorem 2. *With the ordering $\mathcal{L}_1$, the rate region $\mathcal{R}_{4,2}$ of the 4-encoder AMDCS with security level 2 contains all rate tuples characterized by the following inequalities:*

$$R_1 \geq \sum_{i=1}^{3} H(X_i) \tag{17}$$

$$R_j \geq \sum_{i=1}^{4} H(X_i), \ j = 2, 3, 4 \tag{18}$$

$$R_1 + R_j \geq 2\sum_{i=1}^{3} H(X_i) + \sum_{k=4}^{5} H(X_k), j = 2, 3, 4 \tag{19}$$

$$R_2 + R_j \geq 2\sum_{i=1}^{3} H(X_i) + \sum_{k=4}^{5} H(X_k), j = 3, 4 \tag{20}$$

$$R_3 + R_4 \geq 2\sum_{i=1}^{2} H(X_i) + H(X_3) + H(X_4) + H(X_5) \tag{21}$$

Proof: **Converse:** We will prove the inequalities (17) – (21) one by one. Suppose a point $\boldsymbol{r} \in \mathcal{R}_{4,2}$, there exists a block $(n, \boldsymbol{r})$ code to achieve it with $\epsilon \to 0$. By Fano's inequality, for a decoder D_d with input $\mathrm{Fan}(D_d)$ and output $\mathbf{X}_{1:d}$ we have

$$H(\mathbf{X}_{1:d}^n | U_{\mathrm{Fan}(D_d)}) \leq n\delta_d(n, \epsilon), \tag{22}$$

where $\delta_d(n, \epsilon) = \frac{1}{n} + \epsilon \sum_{i=1}^{d} \log |\mathcal{X}_i|$, and we use δ to represent it if there is no confusion.

For (17), we have

$$\begin{aligned}
n(R_1+\epsilon)\geq& H(U_1) && (23)\\
\geq& H(U_1U_3U_4)-H(U_3U_4) && (24)\\
=& H(U_1U_3U_4)+H(\mathbf{X}_{1:5}^n)\\
&-H(\mathbf{X}_{1:5}^nU_3U_4) && (25)\\
\geq& H(\mathbf{X}_{1:3}^nU_1U_3U_4)+H(\mathbf{X}_{1:5}^n)\\
&-H(\mathbf{X}_{1:5}^nU_3U_4)-n\delta && (26)\\
\geq& H(\mathbf{X}_{1:3}^nU_3U_4)+H(\mathbf{X}_{1:5}^n)\\
&-H(\mathbf{X}_{1:5}^nU_3U_4)-n\delta && (27)\\
\geq& H(\mathbf{X}_{1:3}^n)-n\delta && (28)\\
=& nH(X_1)+nH(X_2)+nH(X_3)-n\delta, && (29)
\end{aligned}$$

where (23) is the coding rate constraint, (24) is due to $I(U_1;U_3U_4)\geq 0$, (25) is due to the secrecy constraint that $I(\mathbf{X}_{1:5}^n;U_3U_4)=0$ when U_3,U_4 are accessed by the eavesdropper, (26) is due to the decoding constraint at decoder D_3 in Fig. 2, (27) is due to the non-increasing property of entropy when dropping variables, (28) is due to the non-negativity of $I(U_3U_4;X_4^nX_5^n|X_1^nX_2^nX_3^n)$, and (29) is due to the source independence.

For (18), we have

$$\begin{aligned}
n(R_2+\epsilon)\geq& H(U_2) && (30)\\
\geq& H(U_2U_3U_4)-H(U_3U_4) && (31)\\
=& H(U_2U_3U_4)+H(\mathbf{X}_{1:5}^n)\\
&-H(\mathbf{X}_{1:5}^nU_3U_4) && (32)\\
=& H(\mathbf{X}_{1:4}^nU_2U_3U_4)+H(\mathbf{X}_{1:5}^n)\\
&-H(\mathbf{X}_{1:5}^nU_3U_4)-n\delta && (33)\\
\geq& H(\mathbf{X}_{1:4}^nU_3U_4)+H(\mathbf{X}_{1:5}^n)\\
&-H(\mathbf{X}_{1:5}^nU_3U_4)-n\delta && (34)\\
\geq& H(\mathbf{X}_{1:4}^n)-n\delta && (35)\\
=& nH(X_1)+nH(X_2)+nH(X_3)\\
&+nH(X_4)-n\delta, && (36)
\end{aligned}$$

where (30) is the coding rate constraint, (31) is due to $I(U_2;U_3U_4)\geq 0$, (32) is due to the secrecy constraint that $I(\mathbf{X}_{1:5}^n;U_3U_4)=0$ when U_3,U_4 are accessed by the eavesdropper, (33) is due to the decoding constraint at decoder D_4 in Fig. 2, (34) is due to the non-increasing property of entropy when dropping variables, (35) is due to the non-negativity of $I(U_3U_4;X_5^n|\mathbf{X}_{1:4}^n)$, and (36) is due to the source independence.

Similar as the proof of (18), we can prove $R_3\geq\sum_{i=1}^4H(X_i)$ and $R_4\geq\sum_{i=1}^4H(X_i)$.

For (19), we have

$$\begin{aligned}
&nR_1+nR_2+2n\epsilon\\
\geq& H(U_1)+H(U_2) && (37)\\
\geq& H(U_1U_3U_4)+H(U_2U_3U_4)-2H(U_3U_4) && (38)\\
=& H(\mathbf{X}_{1:3}^nU_1U_3U_4)+H(\mathbf{X}_{1:4}^nU_2U_3U_4)\\
&-2H(U_3U_4)-n\delta_3-n\delta_4 && (39)\\
\geq& H(\mathbf{X}_{1:3}^nU_1U_3U_4)+H(\mathbf{X}_{1:4}^nU_2U_3U_4)\\
&+2H(\mathbf{X}_{1:5}^n)-2H(\mathbf{X}_{1:5}^nU_3U_4)-n\delta_3-n\delta_4 && (40)\\
\geq& H(\mathbf{X}_{1:3}^nU_1U_3U_4)+H(\mathbf{X}_{1:4}^nU_2U_3U_4)+H(\mathbf{X}_{1:5}^n)\\
&-H(\mathbf{X}_{1:5}^nU_3U_4)+H(\mathbf{X}_{1:3}^n)-H(\mathbf{X}_{1:3}^nU_3U_4)\\
&-n\delta_3-n\delta_4 && (41)\\
\geq& H(\mathbf{X}_{1:4}^nU_1U_2U_3U_4)-H(\mathbf{X}_{1:5}^nU_3U_4)\\
&+H(\mathbf{X}_{1:3}^n)+H(\mathbf{X}_{1:5}^n)-n\delta_3-n\delta_4 && (42)\\
\geq& H(\mathbf{X}_{1:5}^nU_1U_2U_3U_4)-H(\mathbf{X}_{1:5}^nU_3U_4)\\
&+H(\mathbf{X}_{1:2}^n)+H(\mathbf{X}_{1:4}^n)-n\delta_3-n\delta_4 && (43)\\
\geq& H(\mathbf{X}_{1:3}^n)+H(\mathbf{X}_{1:5}^n)-n\delta_3-n\delta_4 && (44)\\
=& 2nH(X_1)+2nH(X_2)+2nH(X_3)\\
&+nH(X_4)+nH(X_5)-n\delta_3-n\delta_4, && (45)
\end{aligned}$$

where (37) is the coding rate constraint, (38) is due to $I(U_2;U_3U_4)\geq 0$ and $I(U_1;U_3U_4)\geq 0$, (39) is due to the decoding constraints at decoders D_3,D_4 in Fig. 2, (40) is due to the secrecy constraint that $I(\mathbf{X}_{1:5}^n;U_3U_4)=0$ when U_3,U_4 are accessed by the eavesdropper, (41) is due to the non-negativity of $I(\mathbf{X}_{4:5}^n;U_3U_4|\mathbf{X}_{1:3}^n)$, (42) is due to the sub-modularity that $H(\mathbf{X}_{1:3}^nU_1U_3U_4)+H(\mathbf{X}_{1:5}^nU_2U_3U_4)\geq H(\mathbf{X}_{1:5}^nU_1U_2U_3U_4)+H(\mathbf{X}_{1:3}^nU_3U_4)$, (43) to (44) are due to the decoding constraint at decoder D_5 and the non-negativity of $H(U_1U_2|\mathbf{X}_{1:5}^nU_3U_4)$, and (45) is due to the source independence.

Next, we have

$$\begin{aligned}
&nR_1+nR_3+2n\epsilon\\
\geq& H(U_1)+H(U_3) && (46)\\
\geq& H(U_1U_3U_4)-H(U_3U_4)\\
&+H(U_2U_3U_4)-H(U_2U_4) && (47)\\
=& H(\mathbf{X}_{1:3}^nU_1U_3U_4)+H(\mathbf{X}_{1:4}^nU_2U_3U_4)\\
&-H(U_2U_4)-H(U_3U_4)-n\delta_3-n\delta_4 && (48)\\
\geq& H(\mathbf{X}_{1:3}^nU_1U_3U_4)+H(\mathbf{X}_{1:4}^nU_2U_3U_4)+2H(\mathbf{X}_{1:5}^n)\\
&-H(\mathbf{X}_{1:5}^nU_2U_4)-H(\mathbf{X}_{1:5}^nU_3U_4)-n\delta_3-n\delta_4 && (49)\\
\geq& H(\mathbf{X}_{1:4}^nU_1U_2U_3U_4)+H(\mathbf{X}_{1:5}^n)\\
&-H(\mathbf{X}_{1:5}^nU_2U_4)+H(\mathbf{X}_{1:3}^n)-n\delta_3-n\delta_4 && (50)\\
\geq& H(\mathbf{X}_{1:5}^nU_1U_2U_3U_4)-H(\mathbf{X}_{1:5}^nU_2U_4)\\
&+H(\mathbf{X}_{1:3}^n)+H(\mathbf{X}_{1:5}^n)-n\delta_3-n\delta_4 && (51)\\
\geq& H(\mathbf{X}_{1:3}^n)+H(\mathbf{X}_{1:5}^n)-n\delta_3-n\delta_4 && (52)\\
=& 2nH(X_1)+2nH(X_2)+2nH(X_3)\\
&+nH(X_4)+nH(X_5)-n\delta_3-n\delta_4, && (53)
\end{aligned}$$

where (46) is the coding rate constraint, (47) is due to $I(U_2;U_3U_4)\geq 0$ and $I(U_1;U_3U_4)\geq 0$, (48) is due to the decoding constraints at decoders D_3,D_4 in Fig. 2,

(49) is due to the secrecy constraint that $I(\mathbf{X}_{1:4}^n; U_2U_4) = 0$ ($I(\mathbf{X}_{1:4}^n; U_3U_4) = 0$) when U_2, U_4 (U_3, U_4) are accessed by the eavesdropper, (50) is due to the non-negativity of $I(\mathbf{X}_{4:5}^n; U_3U_4|\mathbf{X}_{1:3}^n)$ and the non-negativity of $I(U_1; U_2X_4|\mathbf{X}_{1:3}^nU_3U_4)$, (51) is due to the decoding constraint at decoder D_5, (52) is due to the non-negativity of $H(U_3|\mathbf{X}_{1:5}^nU_2U_4)$, and (53) is due to the source independence.

Following a similar argument as above by examining at decoders D_3, D_4 in Fig. 2, we can prove the other inequalities except the last one.

For (21), we have

$$\begin{aligned}
&nR_3 + nR_4 + 2n\epsilon \\
\geq& H(U_3) + H(U_4) && (54)\\
\geq& H(U_2U_3U_4) - H(U_2U_4) + H(U_1U_2U_4) - H(U_1U_2) && (55)\\
=& H(\mathbf{X}_{1:2}^nU_1U_2U_4) + H(\mathbf{X}_{1:4}^nU_2U_3U_4) \\
&- H(U_1U_2) - H(U_2U_4) - n\delta_2 - n\delta_4 && (56)\\
\geq& H(\mathbf{X}_{1:2}^nU_1U_2U_4) + H(\mathbf{X}_{1:4}^nU_2U_3U_4) + 2H(\mathbf{X}_{1:5}^n) \\
&- H(\mathbf{X}_{1:5}^nU_1U_2) - H(\mathbf{X}_{1:5}^nU_2U_4) - n\delta_2 - n\delta_4 && (57)\\
\geq& H(\mathbf{X}_{1:2}^nU_1U_2U_4) + H(\mathbf{X}_{1:4}^nU_2U_3U_4) - H(\mathbf{X}_{1:5}^nU_1U_2) \\
&+ H(\mathbf{X}_{1:5}^n) + H(\mathbf{X}_{1:2}^n) - H(\mathbf{X}_{1:2}^nU_2U_4) - n\delta_2 - n\delta_4 && (58)\\
\geq& H(\mathbf{X}_{1:4}^nU_1U_2U_3U_4) - H(\mathbf{X}_{1:5}^nU_1U_2) \\
&+ H(\mathbf{X}_{1:2}^n) + H(\mathbf{X}_{1:5}^n) - n\delta_2 - n\delta_4 && (59)\\
=& H(\mathbf{X}_{1:5}^nU_1U_2U_3U_4) - H(\mathbf{X}_{1:5}^nU_1U_2) \\
&+ H(\mathbf{X}_{1:2}^n) + H(\mathbf{X}_{1:5}^n) - n\delta_2 - n\delta_4 && (60)\\
\geq& H(\mathbf{X}_{1:2}^n) + H(\mathbf{X}_{1:4}^n) - n\delta_2 - n\delta_4 && (61)\\
=& 2nH(X_1) + 2nH(X_2) + nH(X_3) \\
&+ nH(X_4) + nH(X_5) - n\delta_2 - n\delta_4, && (62)
\end{aligned}$$

where (54) is the coding rate constraint, (55) is due to $I(U_3; U_2U_4) \geq 0$ and $I(U_4; U_1U_2) \geq 0$, (56) is due to the decoding constraints at decoders D_2, D_4 in Fig. 2, (57) is due to the secrecy constraint that $I(\mathbf{X}_{1:5}^n; U_1U_2) = 0$ ($I(\mathbf{X}_{1:4}^n; U_2U_4) = 0$) when U_1, U_2 (U_2, U_4) are accessed by the eavesdropper, (58) is due to the non-negativity of $I(\mathbf{X}_{3:5}^n; U_2U_4|\mathbf{X}_{1:2}^n)$, (59) is due to the non-negativity of $I(U_1; U_3X_3X_4|\mathbf{X}_{1:2}^nU_2U_4)$, (60) is due to the decoding constraint at decoder D_5, (61) is to the non-negativity of $H(U_3U_4|\mathbf{X}_{1:5}^nU_1U_2)$, and (62) is due to the source independence.

Achievability: Note that the inequalities (17)–(21) form a polyhedral cone. It suffices to prove the achievability of (representative of) each extreme ray of $\mathcal{R}_{4,2}$, since all the points in the cone can be achieved by time-sharing (conic combination) of the codes achieving the extreme rays. The non-trivial extreme rays of $\mathcal{R}_{4,2}$, that are not in $\mathcal{R}_{4,2}^s$, include the following two, with each row an extreme ray.

R_1	R_2	R_3	R_4	$H(X_1)$	$H(X_2)$	$H(X_3)$	$H(X_4)$	$H(X_5)$
1	1	1	1	0	0	0	1	1
2	2	1	1	0	0	1	0	1

They are all linear codes achievable. $(1, 1, 1, 1, 0, 0, 0, 1, 1)$ can be achieved with $H(K) = 2$ by letting $U_1 = X_4 + X_5, U_2 = X_5 + K_1 + K_2, U_3 = X_4 + K_2$ and $U_4 = X_5 + K_1$, where K_1, K_2 are the two bits of K. $(2, 2, 1, 1, 0, 0, 1, 0, 1)$ can be achieved with $H(K) = 3$ by letting $U_1 = [X_3 + K_1, X_5 + K_2], U_2 = [X_3 + K_2, X_5 + K_3], U_3 = K_1 + K_3$ and $U_4 = X_5 + K_2 + K_3$, where K_1, K_2, K_3 are the three bits of K. One can easily verify that the codes satisfy both the secrecy and decoding constraints. ■

Note that the two extreme rays $(1, 1, 1, 1, 0, 0, 0, 1, 1)$ and $(2, 2, 1, 1, 0, 0, 1, 0, 1)$ of $\mathcal{R}_{4,2}$ cannot be achieved by superposition coding since one has to encode the two sources together instead of separately. However, as shown in the achievability proof, they are linear codes achievable.

Corollary 1. *Linear codes suffice for the 4-encoder S-AMDCS with security level 2 but superposition coding does not. Hence, superposition does not suffice in general for S-AMDCS.*

Note that the region $\mathcal{R}_{4,2}$ does not consider the size of secrecy key. Due to space limit, we omit the constraints on secrecy key here.

IV. Conclusion

Motivated by the optimality of superposition coding for secure symmetric multilevel diversity coding systems, this paper tries to answer the question that if it is still optimal for the secure asymmetric case. A non-trivial example with five sources, four encoders and security level two is considered. Both the superposition and full secure rate region are proven and it is shown that superposition is not optimal for the asymmetric case, which is in contrast with the secure symmetric case. Further, it is shown that simple linear codes suffice for the entire secure rate region of the example network.

References

[1] J. R. Roche, "Distributed information storage," Ph.D. dissertation, Stanford University, March 1992.

[2] R. W. Yeung, "Multilevel diversity coding with distortion," *IEEE Trans. Information Theory*, vol. 41, pp. 412–422, 1995.

[3] R. Yeung and Z. Zhang, "On symmetrical multilevel diversity coding," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 609–621, 1999.

[4] S. Mohajer, C. Tian, and S. Diggavi, "Asymmetric multilevel diversity coding and asymmetric gaussian multiple descriptions," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4367–4387, 2010.

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

[6] C. Li, S. Weber, and J. MacLaren Walsh, "On Multi-source Networks: Enumeration, Rate Region Computation, and Hierarchy," *ArXiv e-prints*, Jul. 2015. [Online]. Available: http://arxiv.org/abs/1507.05728

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

[8] S. E. Rouayheb, E. Soljanin, and A. Sprintson, "Secure network coding for wiretap networks of type ii," *IEEE Transactions on Information Theory*, vol. 58, no. 3, pp. 1361–1371, March 2012.

[9] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[10] L. H. Ozarow and A. D. Wyner, "Wire-tap channel ii," *AT&T Bell Laboratories technical journal*, vol. 63, no. 10, pp. 2135–2157, 1984.

[11] A. Balasubramanian, H. D. Ly, S. Li, T. Liu, and S. L. Miller, "Secure symmetrical multilevel diversity coding," *IEEE Transactions on Information Theory*, vol. 59, no. 6, pp. 3572–3581, June 2013.

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

[13] C. Li and X. Guang, "Asymmetric Multilevel Diversity Coding Systems with Perfect Secrecy," *Submitted to IEEE Transactions on Vehicular Technology*, 2016. [Online]. Available: https://goo.gl/YOGLis

[14] A. Shamir, "How to share a secret," *Commu. Assoc. Comput.*, vol. 22, pp. 612–613, 1979.