Collective Secrecy Over the K-Transmitter Multiple Access Channel

Yanling Chen, O. Ozan Koyluoglu, and A. J. Han Vinck

***Abstract*— This paper studies the problem of secure communication over a K-transmitter multiple access channel (MAC) in the presence of an external eavesdropper, subject to a collective secrecy constraint (i.e., information leakage rate to an eavesdropper on a collection of messages that are from a pre-specified subset of the K transmitters, say $\mathcal{S} \subseteq \mathcal{K} = \{1, 2, \ldots, K\}$, is made vanishing). Since secrecy is of concern only to transmitters $\{i|i \in \mathcal{S}\}$ but not to transmitters $\{i|i \in \mathcal{S}^c\}$, where $\mathcal{S}^c = \mathcal{K}\backslash\mathcal{S}$, different transmission strategies could be employed at transmitters $\{i|i \in \mathcal{S}^c\}$. Consider the following two scenarios: 1) transmitters $\{i|i \in \mathcal{S}^c\}$ use deterministic encoders (which are conventionally used for MAC without secrecy), competing for the channel resource (i.e., being competitive) and 2) transmitters $\{i|i \in \mathcal{S}^c\}$ use stochastic encoders, helping to hide other transmitters' messages from the eavesdropper (i.e., being cooperative). As a result, we establish the respective $\mathcal{S}$-collective secrecy achievable rate regions and demonstrate the advantage of being cooperative theoretically and numerically. To this end, in addition to the standard techniques, our results build upon two techniques. The first is a generalization of Chia-El Gamal's lemma on entropy bound for a set of codewords given partial information. The second is to utilize a compact representation of a list of sets that, together with submodular properties of mutual information functions involved, leads to an efficient Fourier-Motzkin elimination. These two approaches allow us to derive achievable regions in this work, and could also be of independent interest in other context.**

***Index Terms*— Mulitiple access channel, capacity region, secrecy, Fourier-Motzkin elimination, submodular function.**

I. Introduction

MULTIPLE access channel (MAC) is an important branch in the extensive field of the multiple-user communication. It is particularly of interest in wireless communications, as it corresponds to the scenario where a single physical channel is utilized by multiple transmitters such as in an ad-hoc network. For the problem of communicating independent sources over an MAC without any secrecy constraint, Ahlswede [2] first studied the 2-transmitter and 3-transmitter cases and determined the respective capacity regions; whilst Liao [3] considered the general K-transmitter MAC and fully characterized its capacity region. There are also many studies on different extensions of MAC, such as MAC with correlated sources [4]–[6], and MAC with feedback [7], [8]. An extensive survey on the information-theoretic aspects of MAC was given by van der Meulen [9].

Inspired by the pioneering works of Wyner [10] and Csiszár and Körner [11] that studied the information theoretic secrecy of a point-to-point communication in the presence of an external eavesdropper, MAC with an external eavesdropper was first introduced in [12]. In particular, [12] focused on a degraded Gaussian MAC with K-transmitters and established achievable rate regions subject to a pre-specified secrecy measure; while a discrete memoryless 2-transmitter MAC with an external eavesdropper was considered in [13]. In addition to the (*joint*) secrecy constraint at the eavesdropper, the model in [13] also takes into account the generalized feedback that may enable cooperation between trusted transmitters. Achievable secrecy rate regions were derived. Further works on MAC with an external eavesdropper include but not limited to [14]–[16] that focused on the Gaussian scenario; References [17] and [18] that investigated MAC with a stronger secrecy criteria (i.e., the *amount* of information leakage from both messages to the eavesdropper is made vanishing). Note that [18] considered an MAC where encoders have limited access to common randomness or they may share a conferencing link. However, the secrecy capacity region of the MAC with an external eavesdropper, even for the 2-transmitter case, still remains open. Besides, there is a relevant direction, i.e., the 2-transmitter MAC with confidential messages (without an external eavesdropper) [19]–[21], worth mentioning. More specifically, the MAC with one (resp. two) confidential message (resp. messages) that was introduced in [19] (resp. in [20]), generalizes the classic MAC in that one (resp. each) user receives also channel output, and views the other as an eavesdropper. Note that both models were well studied in [21].

In this paper, we consider the secure communication over a K-transmitter MAC subject to a collective secrecy constraint (i.e., information leakage rate on a collection of messages that are from a pre-specified subset of the K transmitters, say $\mathcal{S} \subseteq \mathcal{K} = \{1, 2, \ldots, K\}$, to an eavesdropper is made vanishing). The channel model is shown in Fig. 1. The motivation of this collective secrecy comes from the fact that in a multi-

Manuscript received August 4, 2017; revised January 26, 2018 and March 5, 2018; accepted March 6, 2018. Date of publication March 21, 2018; date of current version May 1, 2018. This work was supported in part by DFG under grant CH 601/2-1 and in part by NSF under Award CNS-1748692. This paper was presented at the 2017 IEEE Information Theory Workshop, Kaohsiung, Taiwan, Nov. 2017 [1]. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Walid Saad. *(Corresponding author: Yanling Chen.)*

Y. Chen and A. J. H. Vinck are with the Institute of Digital Signal Processing, University of Duisburg-Essen, 47057 Duisburg, Germany (e-mail: yanling.chen@uni-due.de; han.vinck@uni-due.de).

O. O. Koyluoglu is with the Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, Berkeley, CA 94720, USA (e-mail: ozan.koyluoglu@berkeley.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2018.2818067

1556-6013 © 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

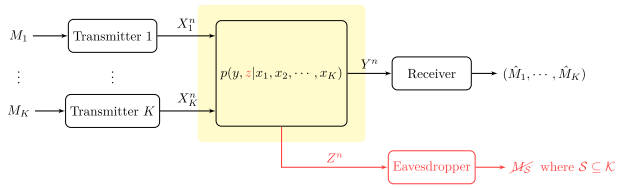


Fig. 1. K-transmitter DM-MAC with an external eavesdropper.

user setting, the secrecy of the respective messages is of great concern only to some users, but not to all. Just as the social network users could configure their privacy settings, the K transmitters in the MAC scenario could also decide whether they would like to keep their messages secret from the eavesdropper (i.e., vote for secrecy) or not (i.e., vote for efficiency). The goal is to find the fundamental trade-off between the efficiency and secrecy subject to the concerns of the K transmitters. Since secrecy is of concern only to transmitters $\{i|i \in \mathcal{S}\}$ but not to transmitters $\{i|i \in \mathcal{S}^c\}$, where $\mathcal{S}^c = \mathcal{K}\backslash\mathcal{S}$, different transmission strategies could be employed at transmitters $\{i|i \in \mathcal{S}^c\}$. More specifically, we consider the following two scenarios: 1) transmitters $\{i|i \in \mathcal{S}^c\}$ use deterministic encoders (which are conventionally used for MAC without secrecy), competing for the channel resource (i.e., being competitive); and 2) transmitters $\{i|i \in \mathcal{S}^c\}$ use stochastic encoders, helping to hide other transmitters' messages from the eavesdropper (i.e., being cooperative). As a general result, we establish the respective collective secrecy achievable rate regions and demonstrate the advantage of being cooperative theoretically and numerically. To this end, in addition to the standard methods (e.g., secrecy coding with a stochastic encoder and a joint typical decoder), our results build upon two techniques. The first is a generalization of Chia-El Gamal's lemma [22, Lemma 1] on entropy bound for a set of codewords given partial information. The second is to utilize a compact representation of a list of sets that, together with the submodular properties of mutual information functions involved, leads to an efficient Fourier-Motzkin elimination. These two approaches allow to derive achievable regions in this work, and could also be of independent interest in other context. An interesting observation is that, our general result includes a joint secrecy rate region as a special case result (i.e., K transmitter all vote for secrecy). Moreover, the obtained joint secrecy rate region is a submodular polyhedron (similar to the capacity region of the K-transmitter MAC [3], [5], [23, Th. 4.5]). Note that one important property of the submodular polyhedron is that, although the polyhedron itself is described by an exponential number of inequalities (i.e., $2^K - 1$), the extreme points and facets can be easily characterized. And, a game-theoretic interpretation of the joint secrecy rate region can be easily developed by following a similar argument to [24].

The rest of the paper is organized as follows. Section II introduces the system model; Section III presents the necessary mathematical tools; Section IV gives the main results, i.e., the $\mathcal{S}$-collective secrecy rate region, detailed proofs of which are provided in Section IV-A (for the achievability) and Section IV-B (for the efficient elimination); Additionally, some numerical results are provided in Section V. Section VI discusses how to extend our results to other settings, and Section VII concludes the paper. To enhance the flow, some details are relegated to the appendix.

II. System Model

Consider a discrete memoryless MAC (DM-MAC) with K transmitters, one legitimate receiver, and one passive eavesdropper, which is defined by $p(y, z|x_1, x_2, \ldots, x_K)$. The transmitter i, aims to send message m_i, to the legitimate receiver, where $i \in \mathcal{K} = \{1, 2, \ldots, K\}$. Define rate R_i at transmitter i by

$$R_i = \frac{1}{n}H(M_i), \quad \text{for } i \in \mathcal{K}.$$

Suppose that x_i^n is the channel input at transmitter i, and the channel outputs at the legitimate receiver and eavesdropper are y^n and z^n, respectively. By the *discrete memoryless* nature of the channel (without any feedback), we have

$$p(y^n, z^n|x_1^n, x_2^n, \ldots, x_K^n) = \prod_{i=1}^{n} p(y_i, z_i|x_{1,i}, x_{2,i}, \ldots, x_{K,i}).$$

A $(2^{nR_1}, 2^{nR_2}, \ldots, 2^{nR_K}, n)$ secrecy code $\mathcal{C}_n$ for the DM-MAC consists of

- K message sets $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_K$, where $m_i \in \mathcal{M}_i = [1 : 2^{nR_i}]$ for $i \in \mathcal{K}$;
- K encoders each assigning a codeword x_i^n to message m_i for $i \in \mathcal{K}$; and
- One decoder at the legitimate receiver that declares an estimate of $(m_1, m_2, \ldots, m_K)$ say $(\hat{m}_1, \hat{m}_2, \ldots, \hat{m}_K)$ or an error to the received sequence y^n.

Following the conventional definition as given in [25, (7.31)], we define the *average probability of decoding error* at the legitimate receiver by

$$P_e^n(\mathcal{C}_n) = \frac{1}{2^{n[R_1+\cdots+R_K]}} \Pr\left\{\bigcup_{i\in\mathcal{K}}\{m_i \neq \hat{m}_i\}|\mathcal{C}_n\right\}. \tag{1}$$

Note that $P_e^n(\mathcal{C}_n) = \Pr\left\{\bigcup_{i\in\mathcal{K}}\{M_i \neq \hat{M}_i\}|\mathcal{C}_n\right\}$ if $M_1, M_2, \ldots, M_K$ are uniformly distributed over their corresponding message sets. For any fixed $\mathcal{S} \subseteq \mathcal{K}$ of size $|\mathcal{S}| = S$, denote $M_{\mathcal{S}} = \{M_i|i \in \mathcal{S}\}$. Define the $\mathcal{S}$-*collective* information leakage rate of the messages from transmitters that belong to the set $\mathcal{S}$ by

$$R_{L,\mathcal{S}}(\mathcal{C}_n) = \frac{1}{n}I(M_{\mathcal{S}}; Z^n|\mathcal{C}_n).$$

The rate pair $(R_1, R_2, \ldots, R_K)$ is said to be *achievable under the $\mathcal{S}$-collective secrecy constraint*, if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, \ldots, 2^{nR_K}, n)$ codes $\{\mathcal{C}_n\}$ such that

$$P_e^n(\mathcal{C}_n) \leq \epsilon_n, \tag{2}$$

$$R_{L,\mathcal{S}}(\mathcal{C}_n) \leq \tau_n, \tag{3}$$

$$\lim_{n\to\infty} \epsilon_n = 0 \quad \text{and} \quad \lim_{n\to\infty} \tau_n = 0. \tag{4}$$

Clearly, the $\mathcal{S}$-collective secrecy implies the $\mathcal{T}$-collective secrecy for any $\mathcal{T} \subseteq \mathcal{S}$. Remarkably, in case of $\mathcal{S} = \mathcal{K}$, (3) corresponds to the *joint* secrecy constraint that is well studied in the literature.

Remark 1: The $\mathcal{S}$-collective secrecy defined by (3)*, together with* (4)*, guarantees a kind of asymptotic perfect secrecy for a specific subset of users $\mathcal{S}$ (in the manner that $\lim_{n\to\infty} R_{L,\mathcal{S}}(\mathcal{C}_n) = 0$, unlike the perfect secrecy that requires $R_{L,\mathcal{S}}(\mathcal{C}_n) = 0$ [26]). We note that this definition is different from the δ-collective secrecy defined in [12], which measures the normalized equivocations, requires that*

$$\Delta_{\mathcal{T}} = \frac{H(M_{\mathcal{T}}|Z^n)}{H(M_{\mathcal{T}})} \geq \delta, \quad \forall \mathcal{T} \subseteq \mathcal{K}, \tag{5}$$

and guarantees a certain degree of secrecy for all subsets of users. Nevertheless, as δ approaches to 1, then the δ-collective secrecy by (5) *guarantees the asymptotic perfect secrecy for the ensemble of users ([14, Definition 2]), which is equivalent to the $\mathcal{K}$-collective secrecy (i.e., joint secrecy) in our definition. Therefore, [14, Definition 3] actually established a joint secrecy rate region for the K-transmitter Gaussian MAC.*

Remark 2: We remark that the $\mathcal{S}$-collective secrecy defined by (3)*, is a weak secrecy metric. It is actually possible to strengthen our weak secrecy results under some stronger alternatives without any rate loss on the achievable regions. This will be discussed in more details in Section VI-B.*

In this paper, we are interested in the achievable $\mathcal{S}$-collective secrecy rate region of the K-transmitter DM-MAC with an external eavesdropper. For convenience, for any random variables W_j for $j \in \mathcal{J}$, and any fixed $\mathcal{J} \subseteq \mathcal{K}$, we denote $W_{\mathcal{J}} = \{W_i | i \in \mathcal{J}\}$.

III. Preliminary Definitions and Lemmas

Compared to the problem of reliable communication over the K-transmitter DM-MAC, the challenges of secure communication are twofold.

- First, an additional secrecy constraint is taken into account. Previous studies on secure communication over DM-MAC [13], [27] mainly focused on the 2-transmitter case, and sub-binning techniques are used therein for secrecy proofs (especially for deriving the sufficient rate constraints for the pre-specified secrecy, which reflects the resolvability of the eavesdropper's channel). In general, if using sub-binning techniques for the secrecy analysis for the K-transmitter DM-MAC, it needs $\mathcal{O}(2K)$ times sub-binning the codebooks and $\mathcal{O}(2^K)$ cases analysis due to the size of the sub-binned codebooks. The secrecy proof soon becomes cumbersome for $K > 2$ (nevertheless, such a proof is available upon request). Besides, the resolvability techniques, to best of our knowledge, are developed only for the 2-transmitter case by Steinberg [28].
- Secondly, stochastic encoders are often used in the random coding stage for secure communication (differently from the deterministic encoders for reliable communication). To obtain a concise form of secrecy rate region (in terms of the system's parameters only), the variables added due to the randomness for secrecy need to be eliminated. Standardly, this can be done by Fourier-Motzkin elimination procedure. However, it is known that the Fourier-Motzkin elimination has a double exponential complexity, which soon becomes infeasible even by software [29] (e.g., for $K \geq 4$ in our problem setting).

In this section, we present the mathematical tools needed to overcome these two challenges. Together with the standard methods, they will be used in the next section to derive the achievable $\mathcal{S}$-collective secrecy rate region for the K-transmitter DM-MAC with an external eavesdropper.

A. Conditional Entropy Bound

Differently from the deterministic encoder that is often sufficient for a reliable communication, a stochastic encoder is preferred for a reliable and secure communication. The basic idea is to trade rates for secrecy, by adding appropriate amount of randomness in the codewords generation. Theoretically, it is of great interest to find out the right amount of randomness that gives the best trade off.

Typically, the sufficient amount of randomness is indicated by a few rate conditions that are derived in the respective secrecy analysis. Such examples include but are not limited to [23, Lemma 22.1] for the wiretap channel, [22, Lemma 1] for the broadcast channel with an external eavesdropper, [27, Lemma 4] for the 2-transmitter DM-MAC with an external eavesdropper. As a generalization, we give in the following Lemma 1 for the K-transmitter DM-MAC with an external eavesdropper. For convenience of comparison, we list them (except [23, Lemma 22.1], since it is implied by [22, Lemma 1]) in Table I.

Lemma 1: Let $(Q, V_1, V_2, \ldots, V_K, Z) \sim p(q) \prod_{i\in\mathcal{K}} p(v_i|q)$ $p(z|v_1, \ldots, v_K)$, $R_{v,i} \geq 0$ for $i \in \mathcal{K}$, and $\epsilon > 0$. Let Q^n be a random sequence and each $q^n = (q(1), \ldots, q(n))$ distributed according to $\prod_{t=1}^{n} p(q(t))$. For $i \in \mathcal{K}$, let $V_i^n(l_i)$, $l_i \in [1 : 2^{nR_{v,i}}]$, be a set of random sequences that are conditionally independent given Q^n and each $v_i^n = (v_i(1), \ldots, v_i(n))$ distributed according to $\prod_{t=1}^{n} p(v_i(t)|q(t))$, and let $\mathcal{C}$ be the codebook of $(Q^n, V_1^n(1), \ldots, V_K^n(2^{nR_{v,K}})$. Let L_i be the random index with an arbitrary probability mass function for $i \in \mathcal{K}$. Then, if $\Pr\{(Q^n, V_1^n(L_1), \ldots, V_K^n(L_K), Z^n) \in \mathcal{T}_\epsilon^n(Q, V_1, \ldots, V_K, Z)\} \to 1$ as $n \to \infty$ and

$$\sum_{j\in\mathcal{J}} R_{v,j} \geq I(V_{\mathcal{J}}; Z|Q), \quad \forall \mathcal{J} \subseteq \mathcal{K} \tag{6}$$

there exists a $\delta_n(\epsilon) \to 0$ as $\epsilon \to 0$ and $n \to \infty$, such that for n sufficiently large

$$H(L_1, L_2, \ldots, L_K|Z^n, Q^n, \mathcal{C}) \leq n\left[\sum_{j\in\mathcal{K}} R_{v,j} - I(V_1, V_2, \ldots, V_K; Z|Q)\right] + n\delta(\epsilon).$$

Proof: See a detailed proof in Appendix A. ■

Remark 3: We observe that the resolvability for the 2-transmitter MAC as discussed in [28] has a similar form as

TABLE I

ENTROPY BOUNDS BY [22, LEMMA 1], [27, LEMMA 4] AND LEMMA 1

	[22, Lemma 1]	[27, Lemma 4]	Lemma 1
Variables	$Q^n \sim \prod_{t=1}^{n} p(q(t))$ $V^n \sim \prod_{t=1}^{n} p(v(t)\|q(t))$ $(Q,V,Z) \sim p(q,v,z)$ L : index of V^n, $l \in [1:2^{nR_v}]$	$Q^n \sim \prod_{t=1}^{n} p(q(t))$ $V_i^n \sim \prod_{t=1}^{n} p(v_i(t)\|q(t))$, $i=1,2$ $(Q,V_1,V_2,Z) \sim p(q)\prod_{i=1}^{2} p(v_i\|q)p(z\|v_1,v_2)$ L_i : index of V_i^n, $l_i \in [1:2^{nR_{v,i}}]$	$Q^n \sim \prod_{t=1}^{n} p(q(t))$ $V_i^n \sim \prod_{t=1}^{n} p(v_i(t)\|q(t))$, $i=1,\cdots,K$ $(Q,V_1,\cdots,V_K,Z) \sim p(q)\prod_{i=1}^{n} p(v_i\|q)p(z\|v_1,\cdots,v_K)$ L_i : index of V_i^n, $l_i \in [1:2^{nR_{v,i}}]$
Codebook $\mathcal{C}$	$\{(Q^n,V^n(l))\|l \in [1:2^{nR_v}]\}$	$\{(Q^n,V_1^n(l_1),V_2^n(l_2))\|$ $l_i \in [1:2^{nR_{v,i}}], i=1,2\}$	$\{(Q^n,V_1^n(l_1),\cdots,V_K^n(l_K))\|$ $l_i \in [1:2^{nR_{v,i}}], i=1,\cdots,K\}$
Condition	$\Pr\{(Q^n,V^n(L),Z^n) \in \mathcal{T}_\epsilon^n(U,V,Z)\} \to 1$	$\Pr\{(Q^n,V_1^n(L_1),V_2^n(L_2),Z^n)$ $\in \mathcal{T}_\epsilon^n(Q,V_1,V_2,Z)\} \to 1$	$\Pr\{(Q^n,V_1^n(L_1),\cdots,V_K^n(L_K),Z^n)$ $\in \mathcal{T}_\epsilon^n(Q,V_1,\cdots,V_K,Z)\} \to 1$
	$R_v \geq I(V;Z\|Q)$	$R_{v,1} \geq I(V_1;Z\|Q)$ $R_{v,2} \geq I(V_2;Z\|Q)$ $R_{v,1}+R_{v,2} \geq I(V_1,V_2;Z\|Q)$	$\sum_{j\in\mathcal{J}} R_{v,j} \geq I(V_{\mathcal{J}};Z\|Q), \forall \mathcal{J} \subseteq \{1,\cdots,K\}$
Bound	$H(L\|Z^n,Q^n,\mathcal{C})$ $\leq n[R_v - I(V;Z\|Q)] + n\mathcal{O}(\epsilon)$	$H(L_1,L_2\|Z^n,Q^n,\mathcal{C})$ $\leq n[R_{v,1}+R_{v,2} - I(V_1,V_2;Z\|Q)] + n\mathcal{O}(\epsilon)$	$H(L_1,\cdots,L_K\|Z^n,Q^n,\mathcal{C})$ $\leq n\left[\sum_{i\in\{1,\cdots,K\}} R_{v,i} - I(V_1,\cdots,V_K;Z\|Q)\right] + n\mathcal{O}(\epsilon)$

the required randomness for weak secrecy in [27, Lemma 4]. Therefore, we believe that Lemma 1 will shed light on the resolvability theory for the K-transmitter MAC.

B. Compact Representation of a List of Sets

In this subsection, we introduce a compact representation of a list of sets and explore its properties. Together with the submodular properties of the mutual information functions that are explored in the next subsection, the representation developed here will help us to significantly reduce the tremendous computational complexity of the Fourier-Motzkin elimination procedure in the next section.

Recall that $\mathcal{K} = \{1,2,\ldots,K\}$. We have the following definitions.

Definition 1: The indicator vector of a subset $\mathcal{T}$ of set $\mathcal{K}$, denoted by $1_{\mathcal{T}}$, is a $1 \times K$ vector, with the i-th element equal to 1 if $i \in \mathcal{T}$ and 0 if $i \notin \mathcal{T}$, for $1 \leq i \leq K$.

For instance, for $K = 5$, $\mathcal{K} = \{1,2,3,4,5\}$ and $\mathcal{T} = \{1,3,5\}$, we have $1_{\mathcal{T}} = [1\ 0\ 1\ 0\ 1]$, and $1_{\emptyset} = [0\ 0\ 0\ 0\ 0]$.

Let $\{\mathcal{T}_i | 1 \leq i \leq t\}$ be a list of t subsets of $\mathcal{K}$.

Definition 2: The presence vector of $\{\mathcal{T}_i | 1 \leq i \leq t\}$ is defined to be $\mathrm{t}_\# = \sum_{i=1}^{t} 1_{\mathcal{T}_i}$, which counts the number of presences of each element of $\mathcal{K}$ over $\{\mathcal{T}_i | 1 \leq i \leq t\}$.

Definition 3: A compact form of the element rearrangement for $\{\mathcal{T}_i | 1 \leq i \leq t\}$ is defined to be $\{\mathcal{T}_{t,i}^* | 1 \leq i \leq t\}$, where $\mathcal{T}_{t,i}^*$ contains the elements that present at least i times from all these t subsets, i.e.,

$$\mathcal{T}_{t,i}^* = \bigcup_{\{j_1,\ldots,j_i\}\subseteq[1:t]} \left(\bigcap_{k=1}^{i} \mathcal{T}_{j_k}\right).$$

Clearly, $\mathcal{T}_{t,t}^* \subseteq \mathcal{T}_{t,t-1}^* \subseteq \cdots \subseteq \mathcal{T}_{t,1}^*$. And, $\mathcal{T}_{t,i}^* = \emptyset$ for $i > t_{\max}$, where $t_{\max}$ is the largest element of $\mathrm{t}_\#$. So $\{\mathcal{T}_{t,i}^* | 1 \leq i \leq t_{\max}\}$ is the compact form without the empty sets.

For instance, for $K = 3$, $\mathcal{K} = \{1,2,3\}$ and $\{\mathcal{T}_i | 1 \leq i \leq 3\}$ with $\mathcal{T}_1 = \{1\}, \mathcal{T}_2 = \{1,2\}$, $\mathcal{T}_3 = \{2,3\}$. We have $\mathrm{t}_\# = (2,2,1)$, $t_{\max} = 2$, $\mathcal{T}_{3,1}^* = \{1,2,3\}, \mathcal{T}_{3,2}^* = \{1,2\}, \mathcal{T}_{3,3}^* = \emptyset$.

Note that the compact form without the empty sets is uniquely determined by the presence vector $\mathrm{t}_\#$. Suppose that $\mathrm{t}_\# = \{n_1,\ldots,n_K\}$, with $t_{\max}$ as the largest element of $\mathrm{t}_\#$. By Definition 3, the list of sets $\{\mathcal{T}_{t,i}^* | 1 \leq i \leq t_{\max}\}$ can be uniquely determined by taking $\mathcal{T}_{t,i}^*$ to be a set that contains elements $k \in \mathcal{K}$ with $n_k \geq i$. As a direct consequence, $\{\mathcal{T}_{t,i}^* | 1 \leq i \leq t_{\max}\}$ is the compact form without the empty sets for all lists that share the same presence vector $\mathrm{t}_\#$. Straightforwardly, we have the following lemmas.

Lemma 2: $\mathrm{t}_\# = \sum_{i=1}^{t} 1_{\mathcal{T}_i} = \sum_{i=1}^{t} 1_{\mathcal{T}_{t,i}^*} = \sum_{i=1}^{t_{\max}} 1_{\mathcal{T}_{t,i}^*}$.

Lemma 3: Given two lists of sets $\{\mathcal{T}_{1i} | 1 \leq i \leq t_1\}$ and $\{\mathcal{T}_{2i} | 1 \leq i \leq t_2\}$, suppose their compact forms of the element rearrangement are $\{\mathcal{T}_{t_1,1i}^* | 1 \leq i \leq t_1\}$ and $\{\mathcal{T}_{t_2,2i}^* | 1 \leq i \leq t_2\}$, and their presence vectors are $\mathrm{t}_{1\#}$ and $\mathrm{t}_{2\#}$, respectively.

1) *If $\mathrm{t}_{1\#} = \mathrm{t}_{2\#}$, with $t_{\max}$ as the largest element, then we have $\mathcal{T}_{t_1,1i}^* = \mathcal{T}_{t_2,2i}^*$ for $1 \leq i \leq t_{\max}$ and $\mathcal{T}_{t_1,1j}^* = \mathcal{T}_{t_2,2k}^* = \emptyset$ for $t_{\max} \leq j \leq t_1$ and $t_{\max} \leq k \leq t_2$.*
2) *If $\mathrm{t}_{2\#}$ is less than or equal to $\mathrm{t}_{1\#}$ (i.e., each component of $\mathrm{t}_{2\#}$ is less than or equal to its corresponding component of $\mathrm{t}_{1\#}$), then we have $\mathcal{T}_{t_2,2i}^* \subseteq \mathcal{T}_{t_1,1i}^*$ for $1 \leq i \leq \min\{t_1,t_2\}$.*

Proof: See a detailed proof in Appendix B. ■

Lemma 4: Given a list of sets $\{\mathcal{T}_i | 1 \leq i \leq t-1\}$ and another list (with one more set $\mathcal{T}_t$ included), i.e., $\{\mathcal{T}_i | 1 \leq i \leq t\}$, let $\{\mathcal{T}_{t-1,i}^* | 1 \leq i \leq t-1\}$ and $\{\mathcal{T}_{t,i}^* | 1 \leq i \leq t\}$ be their compact forms of the element rearrangement, respectively. We have

$$\mathcal{T}_{t,i}^* = \begin{cases} \mathcal{T}_{t-1,1}^* \bigcup \mathcal{T}_t & i = 1 \\ \mathcal{T}_{t-1,i}^* \bigcup \left(\mathcal{T}_{t-1,i-1}^* \bigcap \mathcal{T}_t\right) & 1 < i < t \\ \mathcal{T}_{t-1,t-1}^* \bigcap \mathcal{T}_t & i = t. \end{cases}$$

Proof: See a detailed proof in Appendix C. ■

Lemma 5: Given a list of sets $\{\mathcal{T}_i | 1 \leq i \leq t\}$, and its compact form of the element rearrangement $\{\mathcal{T}_{t,i}^* | 1 \leq i \leq t\}$, for any $\mathcal{S} \subseteq \mathcal{K}$, the compact form of the list of sets $\{\mathcal{T}_i \cap \mathcal{S} | 1 \leq i \leq t\}$ is $\{\mathcal{T}_{t,i}^* \cap \mathcal{S} | 1 \leq i \leq t\}$.

Proof: See a detailed proof in Appendix D. ■

Lemma 6: Let $\{\mathcal{T}_{t,0i}^* | 1 \leq i \leq t\}$ and $\{\mathcal{T}_{t,1i}^* | 1 \leq i \leq t\}$ be the compact forms of the element rearrangement *for $\{\mathcal{T}_{0i} | 1 \leq i \leq t\}$ and $\{\mathcal{T}_{1i} | 1 \leq i \leq t\}$, respectively. If for all $1 \leq i \leq t$, $\mathcal{T}_{0i} \subseteq \mathcal{S} \subseteq \mathcal{K}$ and $\mathcal{T}_{1i} \subseteq \mathcal{S}^c = \mathcal{K} \backslash \mathcal{S}$, then $\{\mathcal{T}_{t,0i}^* \cup \mathcal{T}_{t,1i}^* | 1 \leq i \leq t\}$ is the compact form of the element rearrangement for $\{\mathcal{T}_{0i} \cup \mathcal{T}_{1i} | 1 \leq i \leq t\}$.*

Proof: See a detailed proof in Appendix E. ■

C. Property of Submodular Set Functions

Denote the *power set* of $\mathcal{K}$, i.e., the set of all subsets of $\mathcal{K}$, as $\mathcal{P}_{\mathcal{K}}$. We have the following definitions.

Definition 4: A set function $f : \mathcal{P}_{\mathcal{K}} \to \mathbb{R}$, assigns each subset $\mathcal{T} \subseteq \mathcal{K}$ a value $f_{\mathcal{T}}$.

Definition 5: A set function f is submodular if for every $\mathcal{T}_1, \mathcal{T}_2 \subseteq \mathcal{K}$, we have

$$f_{\mathcal{T}_1} + f_{\mathcal{T}_2} \geq f_{\mathcal{T}_1 \cap \mathcal{T}_2} + f_{\mathcal{T}_1 \cup \mathcal{T}_2}.$$

And, a function f is called supermodular if $-f$ is submodular. A function that is both submodular and supermodular is called a modular function.

Lemma 7: Given $\{\mathcal{T}_i | 1 \leq i \leq t\}$ as a list of t subsets of $\mathcal{K}$, its compact form of the element rearrangement $\{\mathcal{T}^*_{t,i} | 1 \leq i \leq t\}$, and a submodular function $f : \mathcal{P}_{\mathcal{K}} \to \mathbb{R}$, we have

$$\sum_{i=1}^{t} f_{\mathcal{T}_i} \geq \sum_{i=1}^{t} f_{\mathcal{T}^*_{t,i}}.$$

Proof: The proof can be done by induction. A detailed proof is given in Appendix F. ■

Remark 4: Lemma 7 considers the sum value of f over a list of sets. In particular, over all the lists of sets which share the same compact form (see Definition 3), it finds the local minimum extreme point at the list of sets in the compact form. As submodular functions have found immense applications in economics, game theory, electrical networks and machine learning and so on, we believe that Lemma 7 could be of interest also in those domains.

1) Some Submodular Mutual Information Functions: Consider a set of discrete random variables $(Q, V_1, V_2, \ldots, V_K, Y, Z)$. The values of $I(V_{\mathcal{T}}; Y | V_{\mathcal{T}^c}, Q)$ and $I(V_{\mathcal{T}}; Z | Q)$, for a fixed $\mathcal{T} \subseteq \mathcal{K}$ and $\mathcal{T}^c = \mathcal{K} \backslash \mathcal{T}$, are functions of the probability distributions for $(Q, V_{\mathcal{K}}, Y)$ and $(Q, V_{\mathcal{T}}, Z)$, respectively. Their properties as a function of the probability distribution are well understood.

On the other hand, once the probability distribution for random variables $(Q, V_1, V_2, \ldots, V_K, Y, Z)$ is given and fixed, e.g., $(Q, V_1, V_2, \ldots, V_K, Y, Z) \sim p(q) \prod_{i \in \mathcal{K}} p(v_i | q) p(y, z | v_1, \ldots, v_K)$, then we have 2^K conditional mutual information by $I(V_{\mathcal{T}}; Y | V_{\mathcal{T}^c}, Q)$ and 2^K mutual information by $I(V_{\mathcal{T}}; Z | Q)$, for all $\mathcal{T} \in \mathcal{P}_{\mathcal{K}}$. More specifically, we define for any $\mathcal{T} \in \mathcal{P}_{\mathcal{K}}$,

$$b^+_{\mathcal{T}} = I(V_{\mathcal{T}}; Y | V_{\mathcal{T}^c}, Q), \tag{7}$$

$$b^-_{\mathcal{T}} = I(V_{\mathcal{T}}; Z | Q), \tag{8}$$

$$b_{\mathcal{T}} = I(V_{\mathcal{T}}; Y | V_{\mathcal{T}^c}, Q) - I(V_{\mathcal{T}}; Z | Q). \tag{9}$$

Thus, we can regard b^+, b^- and b as set functions from the set $\mathcal{P}_{\mathcal{K}}$ into the set of real numbers. In particular, we put $b^+_{\emptyset} = b^-_{\emptyset} = 0$ (and thus $b_{\emptyset} = 0$). Properties of the thus defined (conditional) mutual information as set functions (i.e., b^+, b^-) need to be further explored. Note that the non-negativity of b^+, b^- in Shannon's sense and the submodularity of b^+ have been recognized [5]. Interestingly, $-b^-$ and b are also submodular.

Lemma 8: For $\forall \mathcal{T}_1, \mathcal{T}_2 \subseteq \mathcal{K}$, we have

1) *(Submodularity of b^+) $b^+_{\mathcal{T}_1} + b^+_{\mathcal{T}_2} \geq b^+_{\mathcal{T}_1 \cap \mathcal{T}_2} + b^+_{\mathcal{T}_1 \cup \mathcal{T}_2}$;*
2) *(Supermodularity of b^-) $b^-_{\mathcal{T}_1} + b^-_{\mathcal{T}_2} \leq b^-_{\mathcal{T}_1 \cap \mathcal{T}_2} + b^-_{\mathcal{T}_1 \cup \mathcal{T}_2}$;*
3) *(Submodularity of b) $b_{\mathcal{T}_1} + b_{\mathcal{T}_2} \geq b_{\mathcal{T}_1 \cap \mathcal{T}_2} + b_{\mathcal{T}_1 \cup \mathcal{T}_2}$.*

Proof: Note that Lemma 8-1), i.e., the submodularity of b^+, has been discussed in [5, Lemma 3.1]. We include it here for the sake of completeness. A detailed proof of Lemma 8-2) is given in Appendix G. And, Lemma 8-3) is, by defintion, a direct consequence of Lemma 8-1) and Lemma 8-2). ■

As a direct consequence of Lemma 7 and Lemma 8, we have the following corollary.

Corollary 1: Given $\{\mathcal{T}_i | 1 \leq i \leq t\}$ as a list of t subsets of $\mathcal{K}$, and its compact form of the element rearrangement $\{\mathcal{T}^*_{t,i} | 1 \leq i \leq t\}$, we have

1) $\sum_{i=1}^{t} b^+_{\mathcal{T}_i} \geq \sum_{i=1}^{t} b^+_{\mathcal{T}^*_{t,i}}$;
2) $\sum_{i=1}^{t} b^-_{\mathcal{T}_i} \leq \sum_{i=1}^{t} b^-_{\mathcal{T}^*_{t,i}}$;
3) $\sum_{i=1}^{t} b_{\mathcal{T}_i} \geq \sum_{i=1}^{t} b_{\mathcal{T}^*_{t,i}}$.

Remark 5: Note that the polymatroidal property of the conditional mutual information function b^+, i.e., submodularity together with $b^+_{\emptyset} = 0$ and monotonicity ($b^+_{\mathcal{T}_1} \leq b^+_{\mathcal{T}_2}$ for $\mathcal{T}_1 \subseteq \mathcal{T}_2$), was discussed in [5, Lemma 3.1]; while the polymatroidal property of the entropy functions was discussed in [30]. Both were pointed out explicitly to be fundamental when we deal with the interdependence of random variables in the analysis of multiple-user communication networks. To this end, we believe the submodularity of $-b^-, b$ and Corollary 1 (i.e., the generalized submodularity of $b^+, -b^-$ and b), could be a valuable addition.

Remarkably, b^+ (as defined in (7)) is used to describe the polymatroidal structure of the capacity region of the K-transmitter MAC with correlated sources in [5]. And in this paper, as we show in Corollary 2, the joint secrecy rate region of the K-transmitter MAC with an external eavesdropper is a submodular polyhedron associated with the submodular function b (as defined in (9)).

IV. K-Transmitter DM-MAC With an External Eavesdropper

In this section, we give achievable $\mathcal{S}$-collective secrecy rate regions of the K-transmitter DM-MAC with an external eavesdropper for the following two scenarios:

1) with *competitive* transmitters $\{i | i \in \mathcal{S}^c\}$, where transmitters $\{i | i \in \mathcal{S}^c\}$ use deterministic encoders (which are conventionally used for MAC without secrecy), competing for the channel resource;
2) with *cooperative* transmitters $\{i | i \in \mathcal{S}^c\}$, where transmitters $\{i | i \in \mathcal{S}^c\}$ use stochastic encoders, helping to hide other transmitters' messages from the eavesdropper.

As a general result, we have the following theorem.

Theorem 4.1: An achievable $\mathcal{S}$-collective secrecy rate region of the K-transmitter DM-MAC with an external eavesdropper is given by the union of non-negative rate pairs $(R_1, R_2, \ldots, R_K)$ that are defined by

1) *for the case with competitive transmitters* $\{i|i \in \mathcal{S}^c\}$:

$$\sum_{j\in\mathcal{T}_0\cup\mathcal{T}_1} R_j - \sum_{j\in\mathcal{T}_2} R_j \leq I(V_{\mathcal{T}_0\cup\mathcal{T}_1}; Y|V_{(\mathcal{T}_0\cup\mathcal{T}_1)^c}, Q) - I(V_{\mathcal{T}_0\cup\mathcal{T}_2}; Z|Q), \quad \forall \mathcal{T}_0 \subseteq \mathcal{S} \ \& \ \mathcal{T}_1, \quad \mathcal{T}_2 \subseteq \mathcal{S}^c, \tag{10}$$

2) *for the case with cooperative transmitters* $\{i|i \in \mathcal{S}^c\}$:

$$\sum_{j\in\mathcal{T}_0\cup\{\mathcal{T}_1\setminus\mathcal{T}_2\}} R_j \leq I(V_{\mathcal{T}_0\cup\mathcal{T}_1}; Y|V_{(\mathcal{T}_0\cup\mathcal{T}_1)^c}, Q) - I(V_{\mathcal{T}_0\cup\mathcal{T}_2}; Z|Q), \quad \forall \mathcal{T}_0 \subseteq \mathcal{S} \ \& \ \mathcal{T}_2 \subseteq \mathcal{T}_1 \subseteq \mathcal{S}^c, \tag{11}$$

where the union is over input probability distributions that factor as $p(q)\prod_{i\in\mathcal{K}} p(v_i|q)p(x_i|v_i)$.

Remark 6: It is easy to see that (10) *and* (11) *differ only at the choices of* $\mathcal{T}_1, \mathcal{T}_2$, *where the choices for the former include the ones for the later. As a direct consequence, the region defined by* (10) *is in general smaller than the one defined by* (11). *In other words, transmitters* $\{i|i \in \mathcal{S}^c\}$, *although they do not demand to keep their messages secret from the eavesdropper, they could help the secure transmission of the messages from other transmitters (in achieving a larger secrecy region), by using the stochastic encoders instead of the deterministic ones. In particular, at* $\mathcal{S} = \mathcal{K}$, *both regions in* (10) *and* (11) *reduce to an achievable joint secrecy rate region as given in the following corollary.*

Corollary 2: [1, Th. 7] An achievable joint secrecy rate region of the K*-transmitter DM-MAC with an external eavesdropper is given by the union of non-negative rate pairs* $(R_1, R_2, \ldots, R_K)$ *defined by*

$$\sum_{j\in\mathcal{T}} R_j \leq I(V_{\mathcal{T}}; Y|V_{\mathcal{T}^c}, Q) - I(V_{\mathcal{T}}; Z|Q), \quad \forall \mathcal{T} \subseteq \mathcal{K},$$

where the union is over input probability distributions that factor as $p(q)\prod_{i\in\mathcal{K}} p(v_i|q)p(x_i|v_i)$.

Remark 7: Setting $Z = \emptyset$ *and taking* $V_i = X_i$ *for* $i \in \mathcal{K}$, *Corollary 2 reduces to the capacity region of the* K*-transmitter MAC [3], [23, Th. 4.5]. Moreover, applying the standard discretization procedure [23], one can extend Corollary 2 to the Gaussian case. Further taking* $V_i = X_i$ *for* $i \in \mathcal{K}$, *one recovers the joint secrecy rate region for the* K*-transmitter Gaussian MAC that is established in [14, Definition 3]. Besides, Corollary 2 generalizes the joint secrecy result for 2-transmitter DM-MAC in [27, Th. 2] that improves [13, (8)] with channel prefixing as demonstrated in [27].*

A. Achievability Proof of Theorem 4.1

Fix $p(q)$ and $p(v_i|q), p(x_i|v_i)$ for $i \in \mathcal{K}$. Generate a random sequence q^n, where $p(q^n) = \prod_{t=1}^{n} p(q(t))$ with each entry chosen as i.i.d. $p(q)$. The sequence q^n is given to every node in the system.

1) Codebook Generation: To construct codebook $\mathcal{C}_i$ for $i \in \mathcal{K}$, randomly generate $2^{n[R_i+R_{i,r}]}$ i.i.d. sequences $v_i^n(m_i, m_{i,r})$, with $(m_i, m_{i,r}) \in [1 : 2^{nR_i}] \times [1 : 2^{nR_{i,r}}]$, each with probability $p(v_i^n|q^n) = \prod_{t=1}^{n} p(v_i(t)|q(t))$. Every node in the network knows these codebooks. Denote the overall codebook as $\mathcal{C}$. Note that for the case of *competitive* transmitters $\{i|i \in \mathcal{S}^c\}$, we have $R_{i,r} = 0$ for those $i \in \mathcal{S}^c$.

2) Encoding: For $i \in \mathcal{K}$, transmitter i, to send message m_i, randomly and uniformly chooses $m_{i,r} \in [1 : 2^{nR_{i,r}}]$ and finds $v_i^n(m_i, m_{i,r})$. Then, given the codeword $v_i^n(m_i, m_{i,r})$, it generates x_i^n according to $\sum_{t=1}^{n} p(x_i(t)|v_i(t))$ and transmits this sequence to the channel.

3) Decoding: The legitimate receiver, upon receiving y^n, finds $v_1^n(\hat{m}_1, \hat{m}_{1,r}), \ v_2^n(\hat{m}_2, \hat{m}_{2,r}), \ldots, v_K^n(\hat{m}_K, \hat{m}_{K,r})$ such that $(v_1^n(\hat{m}_1, \hat{m}_{1,r}), v_2^n(\hat{m}_2, \hat{m}_{2,r}), \ldots, v_K^n(\hat{m}_K, \hat{m}_{K,r}), y^n)$ is jointly typical.

4) Analysis of the Error Probability of Decoding: Consider the expected value of the error probability of decoding over the ensemble of random codes $\mathcal{C}$, i.e., $P_e = \mathbb{E}[P_e(\mathcal{C})]$. Note that here $\mathcal{C}$ denotes the random variable that represents the randomly generated codebook that adhere to the above scheme. From the decoding analysis for the multiple access channel, see, e.g., [23], P_e can be made approximately zero as $n \to \infty$ if

$$\sum_{j\in\mathcal{J}} [R_j + R_{j,r}] \leq I(V_{\mathcal{J}}; Y|V_{\mathcal{J}^c}, Q), \quad \forall \mathcal{J} \subseteq \mathcal{K}. \tag{12}$$

5) Analysis of $\mathcal{S}$*-Collective Secrecy:* For the $\mathcal{S}$-collective secrecy as defined in (3), we need to show that $\mathbb{E}\left[R_{L,\mathcal{S}}(\mathcal{C})\right] \leq \tau_n$, for given $\mathcal{S} \subseteq \mathcal{K}$. To this end, we show its equivalent form that $H(M_{\mathcal{S}}|Z^n, Q^n, \mathcal{C}) \geq n\sum_{j\in\mathcal{S}} R_j - n\tau_n$ as this implies $I(M_{\mathcal{S}}; Z^n|\mathcal{C}) \leq I(M_{\mathcal{S}}; Z^n, Q^n|\mathcal{C}) \leq n\tau_n$. This can be done by applying the following lemma:

Lemma 9: For a fixed $\mathcal{S} \subseteq \mathcal{K}$, *we have* $H(M_{\mathcal{S}}|Z^n, Q^n, \mathcal{C}) \geq n\sum_{i\in\mathcal{S}} R_i - n\tau_n$ *if*

$$\sum_{j\in\mathcal{J}\cap\mathcal{S}^c} R_j + \sum_{j\in\mathcal{J}} R_{j,r} \geq I(V_{\mathcal{J}}; Z|Q), \quad \forall \mathcal{J} \subseteq \mathcal{K}. \tag{13}$$

Proof: See a detailed proof in Appendix H. ■

Summarizing the requirements for a reliable communication under the S-collective secrecy constraint, we have the following rate conditions:

- the non-negativity for rates;
- the conditions for a reliable communication to the legitimate receiver, i.e., (12); and
- the conditions for S-collective secrecy of the messages at the eavesdropper, i.e., (13).

That is, we have the following system of inequalities:

$$\begin{aligned} &R_i, R_{j,r} \geq 0, \ \forall i \in \mathcal{K}, \ \forall j \in \mathcal{S}^c; \\ &\sum_{j\in\mathcal{J}} R_j + \sum_{j\in\mathcal{J}} R_{j,r} \leq I(V_{\mathcal{J}}; Y|V_{\mathcal{J}^c}, Q), \ \forall \mathcal{J} \subseteq \mathcal{K}; \\ &\sum_{j\in\mathcal{J}\cap\mathcal{S}^c} R_j + \sum_{j\in\mathcal{J}} R_{j,r} \geq I(V_{\mathcal{J}}; Z|Q), \ \forall \mathcal{J} \subseteq \mathcal{K}. \end{aligned} \tag{14}$$

(Note that $R_{i,r} \geq 0$ for $i \in \mathcal{S}$ are redundant due to the last inequality in (14) with $\mathcal{J} = \{i\}$ for $i \in \mathcal{S}$ and the non-negativity of mutual information $I(V_{\{i\}}; Z|Q)$ for those $i \in \mathcal{S}$.) To obtain the desired region of $\{R_i | i \in \mathcal{K}\}$, the variables of $\{R_{i,r} | i \in \mathcal{K}\}$ are to be eliminated. To do that, we first eliminate the variables of $\{R_{i,r} | i \in \mathcal{S}\}$ and then the variables of $\{R_{i,r} | i \in \mathcal{S}^c\}$.

B. Efficient Elimination

In this subsection, we first eliminate the variables of $\{R_{i,r} | i \in \mathcal{S}\}$. Note that this is sufficient to derive the region for the case of competitive transmitters $\{i | i \in \mathcal{S}^c\}$ where $R_{j,r} = 0$ for $j \in \mathcal{S}^c$; while to derive the region for the case of cooperative transmitters $\{i | i \in \mathcal{S}^c\}$, we need to further eliminate the variables of $\{R_{i,r} | i \in \mathcal{S}^c\}$.

1) Eliminating the Variables of $\{R_{i,r} | i \in \mathcal{S}\}$*:* Let $\mathrm{x}' = [R_1 \ R_2 \ \cdots \ R_K]^T$, $\mathrm{x}'' = [R_{1,r} \ R_{2,r} \ \cdots \ R_{K,r}]^T$. A representation of the system (14) (without the rate conditions $R_i, R_{j,r} \geq 0$ for $i \in \mathcal{K}$ and $j \in \mathcal{S}^c$, since they will not be involved in the elimination but will be included in the final derived region) can be written as follows:

$$1_{\mathcal{J}}\mathrm{x}' + 1_{\mathcal{J}\cap\mathcal{S}^c}\mathrm{x}'' + 1_{\mathcal{J}\cap\mathcal{S}}\mathrm{x}'' \leq b^+_{\mathcal{J}}, \quad \forall \mathcal{J} \subseteq \mathcal{K}; \tag{15}$$

$$-1_{\mathcal{J}\cap\mathcal{S}^c}\mathrm{x}' - 1_{\mathcal{J}\cap\mathcal{S}^c}\mathrm{x}'' - 1_{\mathcal{J}\cap\mathcal{S}}\mathrm{x}'' \leq -b^-_{\mathcal{J}}, \quad \forall \mathcal{J} \subseteq \mathcal{K}, \tag{16}$$

where

- $1_{\mathcal{J}}$ is the $1 \times K$ indicator vector of the subset $\mathcal{J}$ of the set $\mathcal{K}$ (as defined in Definition 1);
- $b^+_{\mathcal{J}_i} = I(V_{\mathcal{J}_i}; Y | V_{\mathcal{J}_i^c}, Q)$ (as defined in (7));
- $b^-_{\mathcal{J}_i} = I(V_{\mathcal{J}_i}; Z | Q)$ (as defined in (8)).

Note that $1_{\mathcal{J}\cap\mathcal{S}^c}\mathrm{x}''$ involves only variables of $\{R_{i,r} | i \in \mathcal{S}^c\}$; whilst $1_{\mathcal{J}\cap\mathcal{S}}\mathrm{x}''$ involves only variables of $\{R_{i,r} | i \in \mathcal{S}\}$. To eliminate the variables of $\{R_{i,r} | i \in \mathcal{S}\}$, according to [31], we are looking for a final system (in terms of $\{R_i | i \in \mathcal{K}\}$ and $\{R_{i,r} | i \in \mathcal{S}^c\}$ only), where each inequation of the final system is a linear combinatory with positive coefficients of inequations of initial system (as a consequence of Fourier's elimination). For the system defined by (14), we find that the final system (after eliminating $\{R_{i,r} | i \in \mathcal{S}\}$) is the following (together with the non-negativity of rates):

$$1_{\mathcal{J}_1}\mathrm{x}' - 1_{\mathcal{J}_2\cap\mathcal{S}^c}\mathrm{x}' + 1_{\mathcal{J}_1\cap\mathcal{S}^c}\mathrm{x}'' - 1_{\mathcal{J}_2\cap\mathcal{S}^c}\mathrm{x}'' \leq b^+_{\mathcal{J}_1} - b^-_{\mathcal{J}_2}, \quad \forall \mathcal{J}_1, \mathcal{J}_2 \subseteq \mathcal{K}, \quad \mathcal{J}_1 \cap \mathcal{S} = \mathcal{J}_2 \cap \mathcal{S}, \tag{17}$$

where (17) is obtained by summing up the realizations of (15) at $\mathcal{J} = \mathcal{J}_1$ and (16) at $\mathcal{J} = \mathcal{J}_2$, where $\mathcal{J}_1, \mathcal{J}_2 \subseteq \mathcal{K}$ with $\mathcal{J}_1 \cap \mathcal{S} = \mathcal{J}_2 \cap \mathcal{S}$. To prove that (17) defines the final system, we show in the following that any other linear combinatory with positive coefficients of inequations of initial system, will produce only redundant inequations.

Without loss of generality, we consider a linear combinatory with positive coefficients of inequations of the initial system as a summation of realizations of (15) at $\{\mathcal{J}_i^+ | 1 \leq i \leq n^+\}$ and (16) at $\{\mathcal{J}_i^- | 1 \leq i \leq n^-\}$. To result in an inequation not involving the variables of $\{R_{i,r} | i \in \mathcal{S}\}$, we have

$$\sum_{i=1}^{n^+} 1_{\mathcal{J}_i^+\cap\mathcal{S}} = \sum_{i=1}^{n^-} 1_{\mathcal{J}_i^-\cap\mathcal{S}}. \tag{18}$$

And, the resulting inequation is

$$\sum_{i=1}^{n^+} 1_{\mathcal{J}_i^+}\mathrm{x}' - \sum_{i=1}^{n^-} 1_{\mathcal{J}_i^-\cap\mathcal{S}^c}\mathrm{x}' + \sum_{i=1}^{n^+} 1_{\mathcal{J}_i^+\cap\mathcal{S}^c}\mathrm{x}'' - \sum_{i=1}^{n^-} 1_{\mathcal{J}_i^-\cap\mathcal{S}^c}\mathrm{x}'' \leq \sum_{i=1}^{n^+} b^+_{\mathcal{J}_i^+} - \sum_{i=1}^{n^-} b^-_{\mathcal{J}_i^-}. \tag{19}$$

Let $\{\mathcal{J}^*_{n^+,i} | 1 \leq i \leq n^+\}$ and $\{\mathcal{J}^*_{n^-,i} | 1 \leq i \leq n^-\}$ be the compact forms of the element rearrangement (definition of which is given in Definition 3) for $\{\mathcal{J}_i^+ | 1 \leq i \leq n^+\}$ and $\{\mathcal{J}_i^- | 1 \leq i \leq n^-\}$, respectively. Then, according to Lemma 5, $\{\mathcal{J}^*_{n^+,i} \cap \mathcal{S} | 1 \leq i \leq n^+\}$ and $\{\mathcal{J}^*_{n^-,i} \cap \mathcal{S} | 1 \leq i \leq n^-\}$ are the compact forms of the element rearrangement for $\{\mathcal{J}_i^+ \cap \mathcal{S} | 1 \leq i \leq n^+\}$ and $\{\mathcal{J}_i^- \cap \mathcal{S} | 1 \leq i \leq n^-\}$, respectively. Note that (18) implies that $\{\mathcal{J}_i^+ \cap \mathcal{S} | 1 \leq i \leq n^+\}$ and $\{\mathcal{J}_i^- \cap \mathcal{S} | 1 \leq i \leq n^-\}$ share the same presence vector (according to Definition 2), say $\mathrm{c}_\#$. Denote the largest element of $\mathrm{c}_\#$ to be $c_{\max}$. Then, according to Lemma 3-1), we have

$$\mathcal{J}^*_{n^+,i} \cap \mathcal{S} = \mathcal{J}^*_{n^-,i} \cap \mathcal{S}, \quad \text{for } 1 \leq i \leq c_{\max}, \tag{20}$$

$$\mathcal{J}^*_{n^+,i} \cap \mathcal{S} = \emptyset, \text{ i.e., } \mathcal{J}^*_{n^+,i} = \mathcal{J}^*_{n^+,i} \cap \mathcal{S}^c, \quad \text{for } c_{\max} + 1 \leq i \leq n^+, \tag{21}$$

$$\mathcal{J}^*_{n^-,i} \cap \mathcal{S} = \emptyset, \text{ i.e., } \mathcal{J}^*_{n^-,i} = \mathcal{J}^*_{n^-,i} \cap \mathcal{S}^c, \quad \text{for } c_{\max} + 1 \leq i \leq n^-. \tag{22}$$

Now consider the system defined by (17). We have the followings.

- Taking $(\mathcal{J}_1, \mathcal{J}_2) = (\mathcal{J}^*_{n^+,i}, \mathcal{J}^*_{n^-,i})$ in (17) for $1 \leq i \leq c_{\max}$ and summing them up, we obtain

$$\sum_{i=1}^{c_{\max}} 1_{\mathcal{J}^*_{n^+,i}}\mathrm{x}' - \sum_{i=1}^{c_{\max}} 1_{\mathcal{J}^*_{n^-,i}\cap\mathcal{S}^c}\mathrm{x}' + \sum_{i=1}^{c_{\max}} 1_{\mathcal{J}^*_{n^+,i}\cap\mathcal{S}^c}\mathrm{x}'' - \sum_{i=1}^{c_{\max}} 1_{\mathcal{J}^*_{n^-,i}\cap\mathcal{S}^c}\mathrm{x}'' \leq \sum_{i=1}^{c_{\max}} \left[b^+_{\mathcal{J}^*_{n^+,i}} - b^-_{\mathcal{J}^*_{n^-,i}} \right]. \tag{23}$$

- Taking $(\mathcal{J}_1, \mathcal{J}_2) = (\mathcal{J}^*_{n^+,i}, \emptyset)$ in (17) for $c_{\max} + 1 \leq i \leq n^+$ and summing them up, we obtain

$$\begin{aligned} &\sum_{i=c_{\max}+1}^{n^+} 1_{\mathcal{J}^*_{n^+,i}}\mathrm{x}' + \sum_{i=c_{\max}+1}^{n^+} 1_{\mathcal{J}^*_{n^+,i}}\mathrm{x}'' \\ &\overset{(a)}{=} \sum_{i=c_{\max}+1}^{n^+} 1_{\mathcal{J}^*_{n^+,i}}\mathrm{x}' + \sum_{i=c_{\max}+1}^{n^+} 1_{\mathcal{J}^*_{n^+,i}\cap\mathcal{S}^c}\mathrm{x}'' \\ &\leq \sum_{i=c_{\max}+1}^{n^+} b^+_{\mathcal{J}^*_{n^+,i}}, \end{aligned} \tag{24}$$

where (a) is due to (21).

- Taking $(\mathcal{J}_1, \mathcal{J}_2) = (\emptyset, \mathcal{J}^*_{n^-,i})$ in (17) for $c_{\max}+1 \le i \le n^-$ and summing them up, we obtain

$$\begin{aligned} &-\sum_{i=c_{\max}+1}^{n^-} 1_{\mathcal{J}^*_{n^-,i}} \mathrm{x}' - \sum_{i=c_{\max}+1}^{n^-} 1_{\mathcal{J}^*_{n^-,i}} \mathrm{x}'' \\ &\overset{(b)}{=} -\sum_{i=c_{\max}+1}^{n^-} 1_{\mathcal{J}^*_{n^-,i}\cap\mathcal{S}^c} \mathrm{x}' - \sum_{i=c_{\max}+1}^{n^-} 1_{\mathcal{J}^*_{n^-,i}\cap\mathcal{S}^c} \mathrm{x}'' \\ &\le -\sum_{i=c_{\max}+1}^{n^-} b^-_{\mathcal{J}^*_{n^-,i}}, \end{aligned} \tag{25}$$

where (b) is due to (22).

Putting (23), (24) and (25) together, we obtain:

$$\begin{aligned} &\sum_{i=1}^{n^+} 1_{\mathcal{J}^*_{n^+,i}} \mathrm{x}' - \sum_{i=1}^{n^-} 1_{\mathcal{J}^*_{n^-,i}\cap\mathcal{S}^c} \mathrm{x}' + \sum_{i=1}^{n^+} 1_{\mathcal{J}^*_{n^+,i}\cap\mathcal{S}^c} \mathrm{x}'' \\ &\quad - \sum_{i=1}^{n^-} 1_{\mathcal{J}^*_{n^-,i}\cap\mathcal{S}^c} \mathrm{x}'' \le \sum_{i=1}^{n^+} b^+_{\mathcal{J}^*_{n^+,i}} - \sum_{i=1}^{n^-} b^-_{\mathcal{J}^*_{n^-,i}}. \end{aligned} \tag{26}$$

Comparing (19) and (26), we notice that

- the LHS of (19) is the same as the LHS of (26):

$$\begin{aligned} \text{LHS of (19)} &= \sum_{i=1}^{n^+} 1_{\mathcal{J}_i^+} \mathrm{x}' - \sum_{i=1}^{n^-} 1_{\mathcal{J}_i^-\cap\mathcal{S}^c} \mathrm{x}' \\ &\quad + \sum_{i=1}^{n^+} 1_{\mathcal{J}_i^+\cap\mathcal{S}^c} \mathrm{x}'' - \sum_{i=1}^{n^-} 1_{\mathcal{J}_i^-\cap\mathcal{S}^c} \mathrm{x}'' \\ &\overset{(c)}{=} \sum_{i=1}^{n^+} 1_{\mathcal{J}^*_{n^+,i}} \mathrm{x}' - \sum_{i=1}^{n^-} 1_{\mathcal{J}^*_{n^-,i}\cap\mathcal{S}^c} \mathrm{x}' \\ &\quad + \sum_{i=1}^{n^+} 1_{\mathcal{J}^*_{n^+,i}\cap\mathcal{S}^c} \mathrm{x}'' - \sum_{i=1}^{n^-} 1_{\mathcal{J}^*_{n^-,i}\cap\mathcal{S}^c} \mathrm{x}'' \\ &= \text{LHS of (26)}, \end{aligned}$$

where (c) is due to Lemma 2 and Lemma 5.

- the RHS of (19) is always equal to or larger than the RHS of (26):

$$\begin{aligned} \text{RHS of (19)} &= \sum_{i=1}^{n^+} b^+_{\mathcal{J}_i^+} - \sum_{i=1}^{n^-} b^-_{\mathcal{J}_i^-} \\ &\overset{(d)}{\ge} \sum_{i=1}^{n^+} b^+_{\mathcal{J}^*_{n^+,i}} - \sum_{i=1}^{n^-} b^-_{\mathcal{J}^*_{n^-,i}} \\ &= \text{RHS of (26)}, \end{aligned}$$

where (d) is according to Corollary 1.

That is, (19) is redundant since it is already implied by (26), which is derived as a linear combinatory with positive coefficients of inequations of the system defined by (17). So far, (17) together with the non-negativity of rates establish the desired final system (after eliminating $\{R_{i,r}|i \in \mathcal{S}\}$). Letting $\mathcal{T}_0 = \mathcal{J}_1 \cap \mathcal{S} = \mathcal{J}_2 \cap \mathcal{S}$, $\mathcal{T}_1 = \mathcal{J}_1 \cap \mathcal{S}^c$ and $\mathcal{T}_2 = \mathcal{J}_2 \cap \mathcal{S}^c$, (17) can be rewritten in the following form:

$$\begin{aligned} &1_{\mathcal{T}_0\cup\mathcal{T}_1}\mathrm{x}' - 1_{\mathcal{T}_2}\mathrm{x}' + 1_{\mathcal{T}_1}\mathrm{x}'' - 1_{\mathcal{T}_2}\mathrm{x}'' \le b^+_{\mathcal{T}_0\cup\mathcal{T}_1} - b^-_{\mathcal{T}_0\cup\mathcal{T}_2}, \\ &\qquad \forall \mathcal{T}_0 \subseteq \mathcal{S} \ \&\ \mathcal{T}_1, \quad \mathcal{T}_2 \subseteq \mathcal{S}^c. \end{aligned} \tag{27}$$

Recall that for the case of competitive transmitters $\{i|i \in \mathcal{S}^c\}$, we have $R_{i,r} = 0$ for $i \in \mathcal{S}^c$ and thus $1_{\mathcal{T}_1}\mathrm{x}'' = 1_{\mathcal{T}_2}\mathrm{x}'' = 0$ for $\mathcal{T}_1, \mathcal{T}_2 \subseteq \mathcal{S}^c$ in (27). We obtain

$$\begin{aligned} &1_{\mathcal{T}_0\cup\mathcal{T}_1}\mathrm{x}' - 1_{\mathcal{T}_2}\mathrm{x}' \le b^+_{\mathcal{T}_0\cup\mathcal{T}_1} - b^-_{\mathcal{T}_0\cup\mathcal{T}_2}, \\ &\qquad \forall \mathcal{T}_0 \subseteq \mathcal{S} \ \&\ \mathcal{T}_1, \quad \mathcal{T}_2 \subseteq \mathcal{S}^c, \end{aligned}$$

i.e., (10), which defines the achievable secrecy region for the case of competitive transmitters $\{i|i \in \mathcal{S}^c\}$.

2) Eliminating the Variables of $\{R_{i,r}|i \in \mathcal{S}^c\}$: For the case of cooperative transmitters $\{i|i \in \mathcal{S}^c\}$, we have obtained so far a system defined by (27) together with the non-negativity of rates, i.e.,

$$-R_{j,r} \le 0, \quad \forall j \in \mathcal{S}^c. \tag{28}$$

The remaining task here is to further eliminate the variables of $\{R_{i,r}|i \in \mathcal{S}^c\}$.

Having a close look into (27), if taking $\mathcal{T}_2 \subseteq \mathcal{T}_1$ in (27), we obtain

$$\begin{aligned} &1_{\mathcal{T}_0\cup\{\mathcal{T}_1\setminus\mathcal{T}_2\}}\mathrm{x}' \le b^+_{\mathcal{T}_0\cup\mathcal{T}_1} - b^-_{\mathcal{T}_0\cup\mathcal{T}_2}, \\ &\qquad \forall \mathcal{T}_0 \subseteq \mathcal{S} \ \&\ \mathcal{T}_1 \subseteq \mathcal{T}_2 \subseteq \mathcal{S}^c. \end{aligned} \tag{29}$$

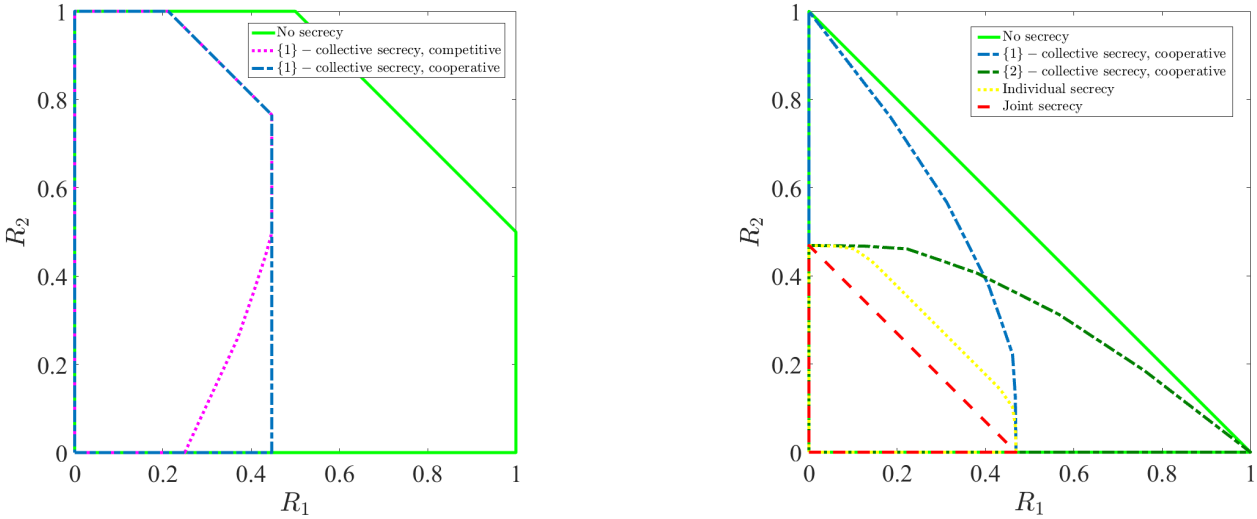
In the following, we show that (29) establishes the final system after eliminating the variables of $\{R_{i,r}|i \in \mathcal{S}^c\}$.

Consider a linear combinatory with positive coefficients of inequations of (27) and (28) (that results in an inequation not involving the variables of $\{R_{i,r}|i \in \mathcal{S}^c\}$) as a summation of realizations of (27) at $(\mathcal{T}_0, \mathcal{T}_1, \mathcal{T}_2) = (\mathcal{T}_{0i}, \mathcal{T}_{1i}, \mathcal{T}_{2i})$, where $\mathcal{T}_{0i} \subseteq \mathcal{S}$ and $\mathcal{T}_{1i}, \mathcal{T}_{2i} \in \mathcal{S}^c$ for $1 \le i \le t$ and (28) (if necessary). Let $\mathrm{t}_{1\#}$ and $\mathrm{t}_{2\#}$ be the presence vectors (as defined in Definition 2) of $\{\mathcal{T}_{1i}|1 \le i \le t\}$ and $\{\mathcal{T}_{2i}|1 \le i \le t\}$, respectively. To result in an inequation not involving the variables of $\{R_{i,r}|i \in \mathcal{S}^c\}$, $\mathrm{t}_{2\#}$ must be less than or equal to $\mathrm{t}_{1\#}$. More specifically, let $\mathrm{t}_{1\#} - \mathrm{t}_{2\#} = [n_1 \ n_2 \ \cdots \ n_K]$. We have $n_j = 0$ for $j \in \mathcal{S}$ (since $T_{1i}, T_{2i} \subseteq \mathcal{S}^c$) and $n_j \ge 0$ for $j \in \mathcal{S}^c$. Multiplying n_j to (28) for $j \in \mathcal{S}^c$, summing them up together with realizations of (27) at $(\mathcal{T}_0, \mathcal{T}_1, \mathcal{T}_2) = (\mathcal{T}_{0i}, \mathcal{T}_{1i}, \mathcal{T}_{2i})$ for $1 \le i \le t$, we obtain

$$\sum_{i=1}^{t} 1_{\mathcal{T}_{0i}\cup\mathcal{T}_{1i}}\mathrm{x}' - \sum_{i=1}^{t} 1_{\mathcal{T}_{2i}}\mathrm{x}' \le \sum_{i=1}^{t} b^+_{\mathcal{T}_{0i}\cup\mathcal{T}_{1i}} - \sum_{i=1}^{t} b^-_{\mathcal{T}_{0i}\cup\mathcal{T}_{2i}}. \tag{30}$$

Let $\{\mathcal{T}^*_{t,0i}|1 \le i \le t\}$, $\{\mathcal{T}^*_{t,1i}|1 \le i \le t\}$ and $\{\mathcal{T}^*_{t,2i}|1 \le i \le t\}$ be the compact forms of the element rearrangement for $\{\mathcal{T}_{0i}|1 \le i \le t\}$, $\{\mathcal{T}_{1i}|1 \le i \le t\}$ and $\{\mathcal{T}_{2i}|1 \le i \le t\}$, respectively. Then, according to Lemma 6, $\{\mathcal{T}^*_{t,0i} \cup \mathcal{T}^*_{t,1i}|1 \le i \le t\}$, $\{\mathcal{T}^*_{t,0i} \cup \mathcal{T}^*_{t,2i}|1 \le i \le t\}$ are the compact forms of the element rearrangement for $\{\mathcal{T}_{0i} \cup \mathcal{T}_{1i}|1 \le i \le t\}$ and $\{\mathcal{T}_{0i} \cup \mathcal{T}_{2i}|1 \le i \le t\}$, respectively. Since $\mathrm{t}_{2\#}$ is less than or equal to $\mathrm{t}_{1\#}$, according to Lemma 3-2), we have $\mathcal{T}^*_{t,2i} \subseteq \mathcal{T}^*_{t,1i}$. Now consider (29). If we sum up its realizations at $(\mathcal{T}_0, \mathcal{T}_1, \mathcal{T}_2) = (\mathcal{T}^*_{t,0i}, \mathcal{T}^*_{t,1i}, \mathcal{T}^*_{t,2i})$ for $1 \le i \le t$, we obtain

$$\sum_{i=1}^{t} 1_{\mathcal{T}^*_{t,0i}\cup\{\mathcal{T}^*_{t,1i}\setminus\mathcal{T}^*_{t,2i}\}}\mathrm{x}' \le \sum_{i=1}^{t} b^+_{\mathcal{T}^*_{t,0i}\cup\mathcal{T}^*_{t,1i}} - \sum_{i=1}^{t} b^-_{\mathcal{T}^*_{t,0i}\cup\mathcal{T}^*_{t,2i}}. \tag{31}$$



(a) Impact by being competitive/cooperative

(b) Impact by different secrecy constraints

Fig. 2. Achievable rate regions under different transmission strategies and secrecy constraints: (a) a binary input adder 2-transmitter MAC with a degraded eavesdropper, with fixed $\mathcal{S} = \{1\}$ but different transmission strategies; (b): a binary multiplier 2-transmitter MAC with a degraded eavesdropper, with different $\mathcal{S}$ but cooperative transmitters $\mathcal{S}^c$.

Comparing (30) and (31), we notice that

- the LHS of (30) is the same as the LHS of (31):

$$\begin{aligned}\text{LHS of (30)} &= \sum_{i=1}^{t} 1_{\mathcal{T}_{0i}\cup\mathcal{T}_{1i}}\mathrm{x}' - \sum_{i=1}^{t} 1_{\mathcal{T}_{2i}}\mathrm{x}' \\ &\overset{(e)}{=} \sum_{i=1}^{t} 1_{\mathcal{T}^*_{t,0i}\cup\mathcal{T}^*_{t,1i}}\mathrm{x}' - \sum_{i=1}^{t} 1_{\mathcal{T}^*_{t,2i}}\mathrm{x}' \\ &\overset{(f)}{=} 1_{\mathcal{T}^*_{t,0i}\cup\{\mathcal{T}^*_{t,1i}\setminus\mathcal{T}^*_{t,2i}\}}\mathrm{x}' \\ &= \text{LHS of (31)},\end{aligned}$$

  where (e) is due to Lemma 2 and Lemma 6; and (f) is due to the fact that for $1 \le i \le t$, $\mathcal{T}^*_{t,0i} \subseteq \mathcal{S}$ and $\mathcal{T}^*_{t,2i} \subseteq \mathcal{T}^*_{t,1i} \subseteq \mathcal{S}^c$.
- the RHS of (30) is always equal to or larger than the RHS of (31):

$$\begin{aligned}\text{RHS of (30)} &= \sum_{i=1}^{t} b^+_{\mathcal{T}_{0i}\cup\mathcal{T}_{1i}} - \sum_{i=1}^{t} b^-_{\mathcal{T}_{0i}\cup\mathcal{T}_{2i}} \\ &\overset{(g)}{\ge} \sum_{i=1}^{t} b^+_{\mathcal{T}^*_{t,0i}\cup\mathcal{T}^*_{t,1i}} - \sum_{i=1}^{t} b^-_{\mathcal{T}^*_{t,0i}\cup\mathcal{T}^*_{t,2i}} \\ &= \text{RHS of (31)},\end{aligned}$$

  where (g) is according to Lemma 6 and Corollary 1.

That is, (30) is redundant since it is already implied by (31), which is derived as a linear combinatory with positive coefficients of inequations of the system defined by (29). As a conclusion, (29) establishes the desired secrecy rate region for the case of cooperative transmitters $\{i|i \in \mathcal{S}^c\}$.

V. Numerical Results

In this section, we provide some numerical results to illustrate the impact on the respective achievable rate regions by employing different transmission strategies at transmitters $\{i|i \in \mathcal{S}^c\}$ and imposing different secrecy constraints.

A. Impact by Different Transmission Strategies at Transmitters $\{i|i \in \mathcal{S}^c\}$

For simplicity, we take $K = 2$ and $\mathcal{S} = \{1\}$, i.e., transmitter 1 would like to keep its message secret from the eavesdropper; while transmitter 2 not. In particular, transmitter 1 uses a stochastic encoder for the purpose of secrecy; while transmitter 2 may take a conventional deterministic encoder for being competitive for the same channel resource; or take a stochastic encoder for being cooperative to help to hide transmitter 1's message from the eavesdropper. According to Theorem 1, we have two achievable regions corresponding to these two different transmission strategies at transmitter 2, and we provide them in Table II. Note that the same regions can be derived by applying Fourier-Motzkin elimination via [29].

As pointed out in Remark 6, a larger secrecy rate region is expected in case of transmitter 2 being cooperative. In Fig. 2(a), we graphically demonstrate the advantage of transmitter 2 being cooperative by a concrete example. Consider a 2-transmitter DM-MAC with an external eavesdropper, where the channel from (X_1, X_2) to Y is a binary input adder MAC, and Z is a degraded version of Y with $p(z|y) = 1 - p$ for $z = y$ and $p(z|y) = p$ for $z = y + 1 \pmod 3$, where $p = 0.1$. In Fig. 2(a), we depict the respective achievable regions (with binary V_1, V_2 for the calculations), where the one enclosed by (magenta) dotted lines is for the case of transmitter 2 being competitive; and the one enclosed by (blue) dash-dotted lines is for the case of transmitter 2 being cooperative. The capacity region (without secrecy constraint) is also plotted for reference purpose, which is enclosed by the (green) solid lines.

As expected, we see that in case of transmitter 2 being cooperative, the region is strictly larger than the case of transmitter 2 being competitive. In particular, a big gap in the achievable secret rate R_1 can be observed at $R_2 = 0$. The gap indicates that transmitter 2 can indeed help the secret transmission of transmitter 1 by sending random signals to jam

TABLE II

2-TRANSMITTER DM-MAC WITH AN EXTERNAL EAVESDROPPER: {1}-COLLECTIVE SECRECY

	Competitive Transmitter 2, by (10)	Cooperative Transmitter 2, by (11)
Rate region	$R_2 \geq I(V_2;Z\|Q)$ $R_2 \leq I(V_2;Y\|V_1,Q)$ $R_1 \leq \min\left\{\begin{array}{l} I(V_1;Y\|V_2,Q)-I(V_1;Z\|Q) \\ I(V_1,V_2;Y\|Q)-I(V_1,V_2;Z\|Q)\end{array}\right\}$ $R_1-R_2 \leq I(V_1;Y\|V_2,Q)-I(V_1,V_2;Z\|Q)$ $R_1+R_2 \leq I(V_1,V_2;Y\|Q)-I(V_1;Z\|Q)$	$R_2 \leq I(V_2;Y\|V_1,Q)$ $R_1 \leq \min\left\{\begin{array}{l} I(V_1;Y\|V_2,Q)-I(V_1;Z\|Q) \\ I(V_1,V_2;Y\|Q)-I(V_1,V_2;Z\|Q)\end{array}\right\}$ $R_1+R_2 \leq I(V_1,V_2;Y\|Q)-I(V_1;Z\|Q)$
Input distribution	$(Q,V_1,V_2,X_1,X_2) \sim p(q)\prod_{i=1}^{2} p(v_i\|q)p(x_i\|v_i)$ such that $I(V_2;Z\|Q) \leq I(V_2;Y\|V_1,Q)$	

TABLE III

2-TRANSMITTER DM-MAC WITH AN EXTERNAL EAVESDROPPER: (11) UNDER DIFFERENT SECRECY CONSTRAINTS

		Rate region	Input distribution
$\mathcal{C}$:	No secrecy [23, Theorem 4.3]	$R_1 \leq I(X_1;Y\|X_2,Q)$ $R_2 \leq I(X_2;Y\|X_1,Q)$ $R_1+R_2 \leq I(X_1,X_2;Y\|Q)$	$(Q,X_1,X_2) \sim p(q)p(x_1\|q)p(x_2\|q)$
$\mathcal{R}_{\{1\}}$:	$\{1\}-$ collective secrecy $\frac{1}{n}I(M_1;Z^n) \to 0$	$R_2 \leq I(V_2;Y\|V_1,Q)$ $R_1 \leq \min\left\{\begin{array}{l} I(V_1;Y\|V_2,Q)-I(V_1;Z\|Q) \\ I(V_1,V_2;Y\|Q)-I(V_1,V_2;Z\|Q)\end{array}\right\}$ $R_1+R_2 \leq I(V_1,V_2;Y\|Q)-I(V_1;Z\|Q)$	$(Q,V_1,V_2,X_1,X_2) \sim p(q)\prod_{i=1}^{2} p(v_i\|q)p(x_i\|v_i)$ such that $I(V_2;Z\|Q) \leq I(V_2;Y\|V_1,Q)$
$\mathcal{R}_{\{2\}}$:	$\{2\}-$ collective secrecy $\frac{1}{n}I(M_2;Z^n) \to 0$	$R_1 \leq I(V_1;Y\|V_2,Q)$ $R_2 \leq \min\left\{\begin{array}{l} I(V_2;Y\|V_1,Q)-I(V_2;Z\|Q) \\ I(V_1,V_2;Y\|Q)-I(V_1,V_2;Z\|Q)\end{array}\right\}$ $R_1+R_2 \leq I(V_1,V_2;Y\|Q)-I(V_2;Z\|Q)$	$(Q,V_1,V_2,X_1,X_2) \sim p(q)\prod_{i=1}^{2} p(v_i\|q)p(x_i\|v_i)$ such that $I(V_1;Z\|Q) \leq I(V_1;Y\|V_2,Q)$
$\mathcal{R}_{\{1\},\{2\}}$:	Individual secrecy [27, Theorem 1] $\frac{1}{n}I(M_1;Z^n) \to 0$ $\frac{1}{n}I(M_2;Z^n) \to 0$	$R_1 \leq I(V_1;Y\|V_2,Q)-I(V_1;Z\|Q)$ $R_2 \leq I(V_2;Y\|V_1,Q)-I(V_2;Z\|Q)$ $\max\{R_1,R_2\} \leq I(V_1,V_2;Y\|Q)-I(V_1,V_2;Z\|Q)$ $R_1+R_2 \leq I(V_1,V_2;Y\|Q)-I(V_1;Z\|Q)-I(V_2;Z\|Q)$	$(Q,V_1,V_2,X_1,X_2) \sim p(q)\prod_{i=1}^{2} p(v_i\|q)p(x_i\|v_i)$
$\mathcal{R}_{\{1,2\}}$:	$\{1,2\}-$ collective secrecy i.e., joint secrecy [27, Theorem 2] $\frac{1}{n}I(M_1,M_2;Z^n) \to 0$	$R_1 \leq I(V_1;Y\|V_2,Q)-I(V_1;Z\|Q)$ $R_2 \leq I(V_2;Y\|V_1,T)-I(V_2;Z\|Q)$ $R_1+R_2 \leq I(V_1,V_2;Y\|Q)-I(V_1,V_2;Z\|Q)$	$(Q,V_1,V_2,X_1,X_2) \sim p(q)\prod_{i=1}^{2} p(v_i\|q)p(x_i\|v_i)$

the eavesdropper. (This is similar to the cooperative jamming observed in the Gaussian scenario [14], but as its counterpart in the discrete setting.) Even in case that transmitter 2 uses a deterministic encoder, its transmission at low rates to some extent, could help transmitter 1 to achieve a larger secrecy rate. However, the advantage of using cooperative transmission strategy at transmitter 2, diminishes or even vanishes especially when R_2 is at high rates. This is because of the bounded sum rate capacity, due to the fact that both transmitters share the same channel resource.

B. Impact by Different Secrecy Constraints

For $K = 2$, there are 4 different secrecy strengths that are implied by different choices of $\mathcal{S} \subseteq \mathcal{K}$:

- as $\mathcal{S} = \emptyset$, it corresponds to the case of no secrecy;
- as $\mathcal{S} = \{1\}$ or $\{2\}$, it corresponds to $\{1\}$-collective secrecy or $\{2\}$-collective secrecy, respectively; and,
- as $\mathcal{S} = \{1, 2\}$, it corresponds to the joint secrecy.

Note that the individual secrecy is not included by $\mathcal{S}$-collective secrecy for any specific choice of $\mathcal{S}$; while it has been studied in [27] together with joint secrecy.

To ensure a fair comparison on the respective achievable regions, we use (11) for the calculations of the $\mathcal{S}$-collective secrecy rate regions (i.e., stochastic encoders are used at all transmitters, as in [27]). (Note that the regions for cases of no secrecy and joint secrecy can be calculated directly according to Corollary 2, see Remark 7.) Together with the individual secrecy rate region from [27, Th. 2], we provide in Table III the respective regions corresponding to these 5 different secrecy strengths. Denote the $\mathcal{S}$-collective secrecy region to be $\mathcal{R}_{\mathcal{S}}$ for $\mathcal{S} \neq \emptyset$ and $\mathcal{C}$ for $\mathcal{S} = \emptyset$, and the individual secrecy region for 2-transmitter MAC by $\mathcal{R}_{\{1\},\{2\}}$. From Table III, it is easy to see that both $\mathcal{C}$ and $\mathcal{R}_{\{1,2\}}$ are consistent with the existing results in the literature for the 2-transmitter DM-MAC (see [23, Th. 4.3] and [27, Th. 2]).

More specifically, in Fig. 2(b), we plotted all these regions for a 2-transmitter DM-MAC with an external eavesdropper, where the channel from (X_1, X_2) to Y is a binary multiplier MAC, and Z is a degraded version of Y through a binary symmetric channel (BSC) with crossover probability $p = 0.1$. Note that V_1, V_2 are taken as binary for the calculations. Not surprisingly, we observe that $\mathcal{R}_{\{1,2\}} \subseteq \mathcal{R}_{\{1\},\{2\}} \subseteq \mathcal{R}_{\{1\}}$ or $\mathcal{R}_{\{2\}} \subseteq \mathcal{C}$, where $\mathcal{R}_{\{1,2\}}$ is enclosed by (red) dashed lines; $\mathcal{R}_{\{1\},\{2\}}$ by (yellow) dotted lines; $\mathcal{R}_{\{1\}}$ and $\mathcal{R}_{\{2\}}$ by dash-dotted lines (blue for $\mathcal{R}_{\{1\}}$ and forest-green for $\mathcal{R}_{\{2\}}$, respectively); and $\mathcal{C}$ by (green) solid lines. Note that the inclusion relation of these regions is due to the correspondingly relaxed secrecy strengths. That is, more stringent is the secrecy requirement, smaller is the correspondingly achievable secrecy region.

VI. EXTENDING RESULTS TO OTHER SCENARIOS

A. Extending Results to Scenarios With More Than One Eavesdropper or Legitimate Receiver

In our model, we only consider the scenario with one legitimate receiver and one external eavesdropper. However, our analysis, (especially the secrecy analysis as given in Lemma 9), can be conveniently applied to scenarios in different settings to derive the desired rate conditions.

For instance, consider the discrete memoryless interference channel (DM-IC) with confidential messages that is defined

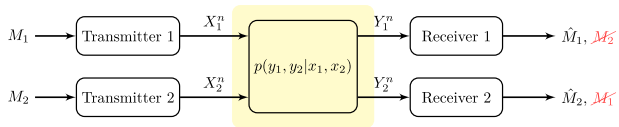


Fig. 3. DM-IC with confidential messages.

by $p(y_1, y_2|x_1, x_2)$, the model of which is shown in Fig. 3. Here two transmitters wish to send independent, confidential messages to their respective receivers (while treating the unintended receiver as an eavesdropper). This communication model was studied in [32].

At the transmitters, we use the same encoding scheme as given in Section IV-A, (this is different from [32], where $R_{1,r}, R_{2,r}$ are fixed therein); while at the legitimate receiver i, a typical set decoding is employed to decode M_i (by finding $v_i^n(\hat{m}_i, \hat{m}_{i,r})$ such that $(v_i^n(\hat{m}_i, \hat{m}_{i,r}), y_i^n)$ is joint typical). Following the standard argument as given in [32, Sec. V-A], if

$$\begin{aligned} R_1 + R_{1,r} &\leq I(V_1; Y_1|Q) \\ R_2 + R_{2,r} &\leq I(V_2; Y_2|Q) \end{aligned} \tag{32}$$

hold, then there exists a code $\mathcal{C}_n$, such that M_1, M_2 can be decoded at the respective receivers with an arbitrary small probability of decoding error. For the confidentiality of M_1 from receiver 2, (i.e., $\frac{1}{n}I(M_1; Y_2^n|\mathcal{C}_n) \to 0$), we have the following rate conditions according to Lemma 9 (by taking $\mathcal{K} = \{1, 2\}$, $\mathcal{S} = \{1\}$ and $Z = Y_2$):

$$\begin{aligned} R_{1,r} &\geq I(V_1; Y_2|Q) \\ R_2 + R_{2,r} &\geq I(V_2; Y_2|Q) \\ R_2 + R_{1,r} + R_{2,r} &\geq I(V_1, V_2; Y_2|Q) \end{aligned} \tag{33}$$

Similarly, for the confidentiality of M_2 from receiver 1, (i.e., $\frac{1}{n}I(M_2; Y_1^n|\mathcal{C}_n) \to 0$), we have by Lemma 9:

$$\begin{aligned} R_1 + R_{1,r} &\geq I(V_1; Y_1|Q) \\ R_{2,r} &\geq I(V_2; Y_1|Q) \\ R_1 + R_{1,r} + R_{2,r} &\geq I(V_1, V_2; Y_1|Q) \end{aligned} \tag{34}$$

Thus we obtain a secrecy rate region defined by the following constraints: the non-negativity for rates; the conditions for a reliable communication, i.e., (32); and the conditions for the confidentialty of the messages, i.e., (33) and (34). Eliminating $R_{1,r}, R_{2,r}$ (e.g., by applying Fourier-Motzkin procedure via [29]), we get

$$\begin{aligned} R_1 &\leq I(V_1; Y_1|Q) - I(V_1; Y_2|V_2, Q) \\ R_2 &\leq I(V_2; Y_2|Q) - I(V_2; Y_1|V_1, Q) \end{aligned}$$

which recovers the result given by [32, Th. 2].

B. Strengthening Secrecy Results From Weak to Strong

Note that we use the weak secrecy metric in this paper, i.e., a vanishing information leakage rate to the eavesdropper: $\frac{1}{n}I(M_{\mathcal{S}}; Z^n) \to 0$ as $n \to \infty$. The weakness of this metric from a cryptographic standpoint has been highlighted in [33] and [34]. Instead, several stronger alternatives have been advocated such as

- the one based on the variational distance [35]: $V(P_{M_{\mathcal{S}}Z^n}, P_{M_{\mathcal{S}}}P_{Z^n})$,
- the one based on the information leaked [33]: $I(M_{\mathcal{S}}; Z^n) = D(P_{M_{\mathcal{S}}Z^n}||P_{M_{\mathcal{S}}}P_{Z^n})$,
- the effective secrecy [36], [37] measured by the unnormalized informational divergence $D(P_{M_{\mathcal{S}}Z^n}||P_{M_{\mathcal{S}}}Q_{Z^n})$ (where Q_{Z^n} is the distribution that the eavesdropper expects to observe when the source is not communicating useful messages), and
- the semantic secrecy [38] defined by $\max_{P_M} I(M; Z^n)$.

To attain the strong secrecy, different methods have been proposed, such as graph-coloring techniques [33], privacy amplification [34], and channel resolvability/output statistics [35]–[37], [39]–[41]. However, the proofs for strong secrecy are often cumbersome (a reason why the weak secrecy is so far the most adopted secrecy metric, especially for the multi-user settings). In fact, the weak secrecy approach follows the pioneering works of [10] and [11]. The rather standard and direct analysis makes our result self-contained and more accessible to readers. It not only reveals insights into the structure of the secrecy rate region for K-transmitter MAC, but also lays a common foundation to scenarios that may have different criteria of strong secrecy.

Nevertheless, in the following we give an instance to strengthen our achievability result from weak to strong. For simplicity, we only consider the joint secrecy case and the strong secrecy is defined in terms of variational distance. The idea is to use the framework proposed in [40], which is based on the duality between channel and source coding problem and uses pmf (i.e., probability mass function) approximation arguments instead of typicality. Consider the dual source coding problem where a joint source is with distribution $P_{X_1\cdots X_K YZ} = P_{X_1}\cdots P_{X_K}P_{YZ|X_1\cdots X_K}$. For $i \in \mathcal{K}$, the realizations of X_i^n, are randomly binned twice, to form $M_i = \phi_i(X_i^n) \in [1 : 2^{nR_i}]$ and $M_{i,r} = \psi_i(X_i^n) \in [1 : 2^{nR_{i,r}}]$. (We ignore here the prefixing and time-sharing random variables that play no crucial role in the analysis.) By [40, Th. 1], if

$$\sum_{j\in\mathcal{J}}[R_j + R_{j,r}] \leq H(X_{\mathcal{J}}|Z), \quad \forall \mathcal{J} \subseteq \mathcal{K}, \tag{35}$$

then $\{M_j, M_{j,r}\}_{j=1}^K$ are nearly jointly uniformly distributed (hence independent) and independent of Z^n. Thus the strong joint secrecy in terms of variational distance can be fulfilled; whilst by [40, Lemma 1], if

$$\sum_{j\in\mathcal{J}} R_{j,r} \geq H(X_{\mathcal{J}}|X_{\mathcal{J}^c}, Y), \quad \forall \mathcal{J} \subseteq \mathcal{K}, \tag{36}$$

then $\{M_j\}_{j=1}^K$ will be nearly perfectly decoded from Y^n and $\{M_{j,r}\}_{j=1}^K$, thus fulfilling the reliability constraint. Denote $c_{\mathcal{J}}^+ = H(X_{\mathcal{J}}|Z)$ and $c_{\mathcal{J}}^- = H(X_{\mathcal{J}}|X_{\mathcal{J}^c}, Y)$. For fixed $(X_1, X_2, \ldots, X_K, Y, Z) \sim P_{X_1}\cdots P_{X_K}P_{YZ|X_1\cdots X_K}$, we note that $c_{\mathcal{J}}^+$ and $c_{\mathcal{J}}^-$ are submodular and supermodular set functions, respectively. This is similar to $b_{\mathcal{J}}^+$ and $b_{\mathcal{J}}^-$ as defined in (7) and (8). Therefore, we can apply the same approach as in this paper to eliminate $\{R_{j,r}|j \in \mathcal{K}\}$ on the system defined by (35) and (36). Further, taking into account the prefixing &

time sharing, one can then obtain Corollary 2 under a stronger secrecy criterion.

VII. Concluding Remarks

In this paper, we studied the problem of secure communication over a K-transmitter MAC subject to an $\mathcal{S}$-collective secrecy constraint. As a general result, we established the respective achievable secrecy rate regions by considering transmitters $\{i|i \in \mathcal{S}^c\}$ for being competitive or cooperative. Remarkably, our secrecy proof is based on a lemma that is a generalization of Chia-El Gamal's lemma [22, Lemma 1] on entropy bound for a set of codewords given partial information. And, a concise rate region (of system parameter only) is derived by utilizing a compact representation of a list of sets together with the submodularity of the mutual information functions (thus avoiding the double-exponential computational complexity of the Fourier-Motzkin elimination). We showed the effectiveness of these two approaches in deriving the secrecy rate region in this work. We believe these new tools could also be of independent interest in other context.

Appendix A
Proof of Lemma 1

To prove Lemma 1, we need to show that the inequality $H(L_1, L_2, \ldots, L_K|Z^n, Q^n, \mathcal{C}) \leq n \sum_{i\in\mathcal{K}} R_{v,i} - nI(V_1, V_2, \ldots, V_K; Z|Q) + n\delta_n(\epsilon)$ holds if the rates fulfill (6). To do this, given z^n, let us define $\mathcal{L}$ as the set of indices $(l_1, l_2, \ldots, l_K)$ such that

$$(q^n, v_1^n(l_1), v_2^n(l_2), \ldots, v_K^n(l_K), \ z^n) \in \mathcal{T}_\epsilon^n(Q, V_1, V_2, \ldots, V_K, Z).$$

Then we show that the expected size of this list, over all randomly generated codebooks, is upper bounded by

$$\mathbb{E}(|\mathcal{L}|) \leq 1 + \sum_{i=1}^{2^K-1} 2^{n[\mathrm{I}_i+\delta(\epsilon)]}, \tag{37}$$

where

$$\mathrm{I}_i = \sum_{j\in\mathcal{J}_i} R_{v,j} - I(V_{\mathcal{J}_i}; Z|V_{\mathcal{J}_i^c}, Q).$$

Here, $\{\mathcal{J}_i|i \in [1 : 2^K - 1]\}$ are the $2^K - 1$ non-empty subsets of $\mathcal{K}$, and $\mathcal{J}_i^c = \mathcal{K}\backslash\mathcal{J}_i$ for $i \in [1 : 2^K - 1]$.

To prove this, one can note that

$$\mathbb{E}(|\mathcal{L}|) = \Pr\{(L_1, L_2, \ldots, L_K) \in \mathcal{L}\} + \sum_{(l_1,l_2,\ldots,l_K)\neq(L_1,L_2,\ldots,L_K)} \Pr\{(l_1, l_2, \ldots, l_K) \in \mathcal{L}\},$$

where $(L_1, L_2, \ldots, L_K)$ are the true indices chosen by the sources. Since $\Pr\{(q^n, v_1^n(L_1), \ldots, v_K^n(L_K), z^n) \in \mathcal{T}_\epsilon^n(Q, V_1, \ldots, V_K, Z)\} \to 1$ as $n \to \infty$, the first term tends to 1 as $n \to \infty$. As for the second term, we can distinguish $(2^K - 1)$ cases according to the values of $(l_1, l_2, \ldots, l_K)$. More specifically, for each $\mathcal{J}_i$, $i \in [1 : 2^K - 1]$, we consider the following case:

- $l_j \neq L_j$ for $j \in \mathcal{J}_i$, and $l_j = L_j$ for $j \in \mathcal{J}_i^c$. In this case, in total there are at most $2^{n\sum_{j\in\mathcal{J}_i} R_{v,j}}$ possible $(l_1, l_2, \ldots, l_K)$. By the joint typicality lemma, we can show that

$$\Pr\{(l_1, l_2, \ldots, l_K) \in \mathcal{L}\} \leq 2^{-nI(V_{\mathcal{J}_i}; V_{\mathcal{J}_i^c}, Z|Q)+n\delta(\epsilon)} = 2^{-nI(V_{\mathcal{J}_i}; Z|V_{\mathcal{J}_i^c}, Q)+n\delta(\epsilon)},$$

  where the equality is due to the fact that $V_{\mathcal{J}_i}$ and $V_{\mathcal{J}_i^c}$ are conditionally independent given Q.
  Therefore, in this case, there are at most $2^{n[\mathrm{I}_i+\delta(\epsilon)]}$ number of $(l_1, l_2, \ldots, l_K)$ falling in the list $\mathcal{L}$.

Summing up all the undetected errors for all these $(2^K - 1)$ cases that correspond to $\mathcal{J}_i$, $i \in [1 : 2^K - 1]$, we prove (37).

Furthermore, define the indicator variable $E = 1$ if $(L_1, L_2, \ldots, L_K) \in \mathcal{L}$, and $E = 0$ otherwise. We have

$$\begin{aligned} &H(L_1, L_2, \ldots, L_K|Z^n, Q^n, \mathcal{C}) \\ &\quad\leq H(L_1, L_2, \ldots, L_K, E|Z^n, Q^n, \mathcal{C}) \\ &\quad\leq H(E) + H(L_1, L_2, \ldots, L_K|Z^n, Q^n, E, \mathcal{C}) \\ &\quad\leq 1 + H(L_1, L_2, \ldots, L_K|Z^n, Q^n, E = 1, \mathcal{C}) \\ &\qquad + \Pr\{E = 0\}H(L_1, L_2, \ldots, L_K|\mathcal{C}), \end{aligned}$$

where the last inequality follows from the fact that $H(E) \leq 1$ since E is a binary random variable; $\Pr\{E = 1\} \leq 1$ and conditioning reduces the entropy, i.e., $H(L_1, L_2, \ldots, L_K|Z^n, Q^n, E = 0, \mathcal{C}) \leq H(L_1, L_2, \ldots, L_K|\mathcal{C})$.

Note that $\Pr\{E = 0\} = \Pr\{(L_1, L_2, \ldots, L_K) \notin \mathcal{L}\}$ can be made arbitrarily small as $n \to \infty$, since $\Pr\{(q^n, v_1^n(L_1), \ldots, v_K^n(L_K), z^n) \in \mathcal{T}_\epsilon^n(Q, V_1, \ldots, V_K, Z)\} \to 1$ as $n \to \infty$. Next, note that

$$\begin{aligned} &H(L_1, L_2, \ldots, L_K|Z^n, Q^n, E = 1, \mathcal{C}) \\ &\overset{(a)}{=} H(L_1, L_2, \ldots, L_K|Z^n, Q^n, E = 1, \mathcal{C}, \mathcal{L}, |\mathcal{L}|) \\ &\leq H(L_1, L_2, \ldots, L_K|E = 1, \mathcal{L}, |\mathcal{L}|) \\ &= \sum_{l\in\mathrm{supp}(|\mathcal{L}|)} \Pr\{|\mathcal{L}| = l\}H(L_1, L_2, \ldots, L_K|E=1, \mathcal{L}, |\mathcal{L}| = l) \\ &\overset{(b)}{\leq} \sum_{l\in\mathrm{supp}(|\mathcal{L}|)} \Pr\{|\mathcal{L}| = l\}\log_2(l) \\ &= \mathbb{E}(\log_2(|\mathcal{L}|)) \overset{(c)}{\leq} \log_2(\mathbb{E}(|\mathcal{L}|)) \\ &\overset{(d)}{\leq} n\max\{0, \max_{i\in[1:2^K-1]} \mathrm{I}_i\} + K + n\delta(\epsilon) \\ &\overset{(e)}{\leq} n\left[\sum_{i\in\mathcal{K}} R_{v,i} - I(V_1, V_2, \ldots, V_K; Z|Q)\right] + K + n\delta(\epsilon), \end{aligned}$$

where (a) follows from the fact that $\mathcal{L}$ and $|\mathcal{L}|$ are functions of the output Z^n, given the codebook $\mathcal{C}$ and Q^n; (b) is due to the fact that, knowing $E = 1$, the sent indices $(L_1, L_2, \ldots, L_K)$ belong to the list $\mathcal{L}$ and the uncertainty is upper bounded by the log cardinality of the list; (c) is due to the Jensen's inequality; (d) is by (37) along with an application of the log-sum-exp inequality: $\log_2\left(\sum_{x\in\mathcal{X}} 2^x\right) \leq \max_{x\in\mathcal{X}} x + \log_2(|\mathcal{X}|)$; and (e) follows if the rates satisfies (6), i.e., for each $\mathcal{J} \subseteq \mathcal{K}$: $\sum_{i\in\mathcal{J}} R_{v,i} \geq I(V_{\mathcal{J}}; Z)$. This, along with previous remarks

yields the desired inequality (by re-defining $\delta_n(\epsilon)$ to be the arbitrary small term $\mathcal{O}(\epsilon) + (K+1)/n$).

APPENDIX B
PROOF OF LEMMA 3

If $\mathrm{t}_{1\#} = \mathrm{t}_{2\#}$, i.e., $\{\mathcal{T}_{1i} | 1 \le i \le t_1\}$ and $\{\mathcal{T}_{2i} | 1 \le i \le t_2\}$ share the same presence vector with $t_{\max}$ as the largest element. By Definition 2, they have the same number of presences for each element of $\mathcal{K}$, thus the same compact form of the element rearrangement without the empty sets according to Definition 3. This implies that $\mathcal{T}^*_{t_1,1i} = \mathcal{T}^*_{t_2,2i}$ for $1 \le i \le t_{\max}$ and $\mathcal{T}^*_{t_1,1j} = \mathcal{T}^*_{t_2,2k} = \emptyset$ for $t_{\max} \le j \le t_1$ and $t_{\max} \le k \le t_2$.

Suppose that $\mathrm{t}_{1\#} = [n'_1 \ \cdots \ n'_K]$ and $\mathrm{t}_{2\#} = [n''_1 \ \cdots \ n''_K]$. By Definition 3, $\mathcal{T}^*_{t_1,1i}$ contains the elements k with $n'_k \ge i$ and $\mathcal{T}^*_{t_2,2i}$ contains the elements k with $n''_k \ge i$, for $1 \le i \le \min\{t_1, t_2\}$. If $\mathrm{t}_{2\#}$ is less than or equal to $\mathrm{t}_{1\#}$, i.e., $n''_k \le n'_k$ for each $k \in \mathcal{K}$, as a straightforward consequence, all the elements in $\mathcal{T}^*_{t_2,2i}$ belong to $\mathcal{T}^*_{t_1,1i}$ as well. This implies that $\mathcal{T}^*_{t_2,2i} \subseteq \mathcal{T}^*_{t_1,1i}$ for $1 \le i \le \min\{t_1, t_2\}$.

APPENDIX C
PROOF OF LEMMA 4

The proof for $i = 1, t$ is straightforward by definition. For $1 < i < t$, we have the proof as shown in (38), as shown at the bottom of this page, where (a) is by the definition of $\mathcal{T}^*_{t,i}$; (b) is due to the distributive law of the sets and (c) is by the definition of $\mathcal{T}^*_{t-1,i}$ and $\mathcal{T}^*_{t-1,i-1}$. This completes our proof of Lemma 4.

APPENDIX D
PROOF OF LEMMA 5

Let $\{\widetilde{\mathcal{T}}^*_{t,i} | 1 \le i \le t\}$ be the compact form of the list of sets $\{\mathcal{T}_i \cap \mathcal{S} | 1 \le i \le t\}$. We show in the following that $\widetilde{\mathcal{T}}^*_{t,i} = \mathcal{T}^*_{t,i} \cap \mathcal{S}$ for $1 \le i \le t$. Note that $\{\mathcal{T}^*_{t,i} | 1 \le i \le t\}$ is the compact form of the element rearrangement to the list $\{\mathcal{T}_i | 1 \le i \le t\}$.

$$\begin{aligned}
\widetilde{\mathcal{T}}^*_{t,i} &\overset{(a)}{=} \bigcup_{\{j_1,\ldots,j_i\}\subseteq[1:t]} \left(\bigcap_{k=1}^{i} \left(\mathcal{T}_{j_k} \bigcap \mathcal{S} \right) \right) \\
&\overset{(b)}{=} \bigcup_{\{j_1,\ldots,j_i\}\subseteq[1:t]} \left(\left(\bigcap_{k=1}^{i} \mathcal{T}_{j_k} \right) \bigcap \mathcal{S} \right) \\
&\overset{(c)}{=} \left(\bigcup_{\{j_1,\ldots,j_i\}\subseteq[1:t]} \left(\bigcap_{k=1}^{i} \mathcal{T}_{j_k} \right) \right) \bigcap \mathcal{S} \\
&\overset{(d)}{=} \mathcal{T}^*_{t,i} \bigcap \mathcal{S}
\end{aligned}$$

where (a) is by the definition of $\widetilde{\mathcal{T}}^*_{t,i}$, i.e., Definition 3; (b) is by the associative law of the sets; (c) is by the distributive law of the sets; and (d) is by the definition of $\mathcal{T}^*_{t,i}$ according to Definition 3. This completes our proof of Lemma 5.

APPENDIX E
PROOF OF LEMMA 6

Consider the list $\{\mathcal{T}_{0i} \cup \mathcal{T}_{1i} | 1 \le i \le t\}$. Suppose that $\{\mathcal{T}^*_{t,i} | 1 \le i \le t\}$ is its compact form of the element rearrangement. By Definition 3, we have

$$\begin{aligned}
\mathcal{T}^*_{t,i} &= \bigcup_{\{j_1,\ldots,j_i\}\subseteq[1:t]} \left(\bigcap_{k=1}^{i} \left(\mathcal{T}_{0j_k} \bigcup \mathcal{T}_{1j_k} \right) \right) \\
&\overset{(a)}{=} \bigcup_{\{j_1,\ldots,j_i\}\subseteq[1:t]} \left(\left(\bigcap_{k=1}^{i} \mathcal{T}_{0j_k} \right) \bigcup \left(\bigcap_{k=1}^{i} \mathcal{T}_{1j_k} \right) \right) \\
&= \left(\bigcup_{\{j_1,\ldots,j_i\}\subseteq[1:t]} \bigcap_{k=1}^{i} \mathcal{T}_{0j_k} \right) \bigcup \left(\bigcup_{\{j_1,\ldots,j_i\}\subseteq[1:t]} \bigcap_{k=1}^{i} \mathcal{T}_{1j_k} \right) \\
&\overset{(b)}{=} \mathcal{T}^*_{t,0i} \bigcup \mathcal{T}^*_{t,1i},
\end{aligned}$$

where (a) is due to the distributive law of the sets and the fact that for all $1 \le i \le t$, $\mathcal{T}_{0i} \subseteq \mathcal{S}$ and $\mathcal{T}_{1i} \subseteq \mathcal{S}^c$; and (b) is due to the fact that $\{\mathcal{T}^*_{t,0i} | 1 \le i \le t\}$ and $\{\mathcal{T}^*_{t,1i} | 1 \le i \le t\}$ are the compact forms of the element rearrangement for $\{\mathcal{T}_{0i} | 1 \le i \le t\}$ and $\{\mathcal{T}_{1i} | 1 \le i \le t\}$, respectively. As a conclusion, $\{\mathcal{T}^*_{t,0i} \cup \mathcal{T}^*_{t,1i} | 1 \le i \le t\}$ is the compact form of the element rearrangement for $\{\mathcal{T}_{0i} \cup \mathcal{T}_{1i} | 1 \le i \le t\}$.

APPENDIX F
PROOF OF LEMMA 7

We give the proof of Lemma 7 by induction as follows.

- For $t = 1$, we have by definition $\mathcal{T}^*_{1,1} = \mathcal{T}_1$. Thus, $f_{\mathcal{T}_1} = f_{\mathcal{T}^*_{1,1}}$ and the statement is true for $t = 1$.
- For $t = 2$, the statement is true by the submodularity of the set function f.
- Assume that the statement is true for some natural number $t-1$. That is, for any $\{\mathcal{T}_i | 1 \le i \le t-1\}$ as a list of $t-1$ subsets of $\mathcal{K}$, and its compact form of element rearrangement $\{\mathcal{T}^*_{t-1,i} | 1 \le i \le t-1\}$, we have $\sum_{i=1}^{t-1} f_{\mathcal{T}_i} \ge \sum_{i=1}^{t-1} f_{\mathcal{T}^*_{t-1,i}}$. Now we show that the statement is also true for t.

$$\begin{aligned}
\sum_{i=1}^{t} f_{\mathcal{T}_i} &= \sum_{i=1}^{t-1} f_{\mathcal{T}_i} + f_{\mathcal{T}_t} \\
&\overset{(a)}{\ge} \sum_{i=1}^{t-1} f_{\mathcal{T}^*_{t-1,i}} + f_{\mathcal{T}_t}
\end{aligned}$$

$$\begin{aligned}
\mathcal{T}^*_{t,i} &\overset{(a)}{=} \bigcup_{\{j_1,\ldots,j_i\}\subseteq[1:t]} \left(\bigcap_{k=1}^{i} \mathcal{T}_{j_k} \right) \overset{(a)}{=} \left\{ \bigcup_{\{j_1,\ldots,j_i\}\subseteq[1:t-1]} \left(\bigcap_{k=1}^{i} \mathcal{T}_{j_k} \right) \right\} \bigcup \left\{ \bigcup_{\{j_1,\ldots,j_{i-1}\}\subseteq[1:t-1]} \left(\left(\bigcap_{k=1}^{i-1} \mathcal{T}_{j_k} \right) \bigcap \mathcal{T}_t \right) \right\} \\
&\overset{(b)}{=} \left\{ \bigcup_{\{j_1,\ldots,j_i\}\subseteq[1:t-1]} \left(\bigcap_{k=1}^{i} \mathcal{T}_{j_k} \right) \right\} \bigcup \left\{ \left(\bigcup_{\{j_1,\ldots,j_{i-1}\}\subseteq[1:t-1]} \left(\bigcap_{k=1}^{i-1} \mathcal{T}_{j_k} \right) \right) \bigcap \mathcal{T}_t \right\} \\
&\overset{(c)}{=} \mathcal{T}^*_{t-1,i} \bigcup \left(\mathcal{T}^*_{t-1,i-1} \bigcap \mathcal{T}_t \right).
\end{aligned} \tag{38}$$

$$
\begin{aligned}
&= \sum_{i=2}^{t-1} f_{\mathcal{T}^*_{t-1,i}} + \left(f_{\mathcal{T}^*_{t-1,1}} + f_{\mathcal{T}_t}\right) \\
&\overset{(b_1)}{\geq} \sum_{i=2}^{t-1} f_{\mathcal{T}^*_{t-1,i}} + \left(f_{\mathcal{T}^*_{t-1,1}\cap\mathcal{T}_t} + f_{\mathcal{T}^*_{t-1,1}\cup\mathcal{T}_t}\right) \\
&\overset{(c_1)}{=} \sum_{i=3}^{t-1} f_{\mathcal{T}^*_{t-1,i}} + \left(f_{\mathcal{T}^*_{t-1,2}} + f_{\mathcal{T}^*_{t-1,1}\cap\mathcal{T}_t}\right) + f_{\mathcal{T}^*_{t,1}} \\
&\overset{(b_2)}{\geq} \sum_{i=3}^{t-1} f_{\mathcal{T}^*_{t-1,i}} + \left(f_{\mathcal{T}^*_{t-1,2}\cap\mathcal{T}_t} + f_{\mathcal{T}^*_{t-1,2}\cup\left(\mathcal{T}^*_{t-1,1}\cap\mathcal{T}_t\right)}\right) \\
&\quad + f_{\mathcal{T}^*_{t,1}} \\
&\overset{(c_2)}{=} \sum_{i=4}^{t-1} f_{\mathcal{T}^*_{t-1,i}} + \left(f_{\mathcal{T}^*_{t-1,3}} + f_{\mathcal{T}^*_{t-1,2}\cap\mathcal{T}_t}\right) + \sum_{i=1}^{2} f_{\mathcal{T}^*_{t,i}} \\
&\quad \vdots \\
&\overset{(b_{t-1})}{\geq} f_{\mathcal{T}^*_{t-1,t-1}\cap\mathcal{T}_t} + f_{\mathcal{T}^*_{t-1,t-1}\cup\left(\mathcal{T}^*_{t-1,t-2}\cap\mathcal{T}_t\right)} + \sum_{i=1}^{t-2} f_{\mathcal{T}^*_{t,i}} \\
&\overset{(c_{t-1})}{=} \sum_{i=1}^{t} f_{\mathcal{T}^*_{t,i}},
\end{aligned}
$$

where (a) is due to the fact that the statement is true for $t-1$; and for $1 \leq j \leq t-1$, step (b_j) holds by the submodularity of f and the fact that $\mathcal{T}^*_{t-1,j} \cap \left(\mathcal{T}^*_{t-1,j-1} \cap \mathcal{T}_t\right) = \mathcal{T}^*_{t-1,j} \cap \mathcal{T}_t$ for $2 \leq j \leq t-1$ (since $\mathcal{T}^*_{t-1,j} \subseteq \mathcal{T}^*_{t-1,j-1}$ by definition); step (c_j) is by applying Lemma 4. In particular, (c_1) is by the fact that $\mathcal{T}^*_{t,1} = \mathcal{T}^*_{t-1,1} \bigcup \mathcal{T}_t$; step (c_{t-1}) is by the fact that $\mathcal{T}^*_{t,t} = \mathcal{T}^*_{t-1,t-1} \bigcap \mathcal{T}_t$; and other intermediate steps are by the fact that $\mathcal{T}^*_{t-1,j} \cup \left(\mathcal{T}^*_{t-1,j-1} \cap \mathcal{T}_t\right) = \mathcal{T}^*_{t,j}$ for $1 < j < t$.

Appendix G
Proof of Lemma 8-2)

Here we give the proof of Lemma 8-2) as follows:

$$
\begin{aligned}
& b^-_{\mathcal{T}_1} + b^-_{\mathcal{T}_2} \\
&\overset{(a)}{=} I(V_{\mathcal{T}_1}; Z|Q) + I(V_{\mathcal{T}_2}; Z|Q) \\
&\overset{(b)}{=} I(V_{\mathcal{T}_1\cap\mathcal{T}_2}, V_{\mathcal{T}_1\cap\mathcal{T}_2^c}; Z|Q) + I(V_{\mathcal{T}_2}; Z|Q) \\
&\overset{(c)}{=} I(V_{\mathcal{T}_1\cap\mathcal{T}_2}; Z|Q) + I(V_{\mathcal{T}_1\cap\mathcal{T}_2^c}; Z|V_{\mathcal{T}_1\cap\mathcal{T}_2}, Q) + I(V_{\mathcal{T}_2}; Z|Q) \\
&\overset{(d)}{\leq} I(V_{\mathcal{T}_1\cap\mathcal{T}_2}; Z|Q) + I(V_{\mathcal{T}_1\cap\mathcal{T}_2^c}; Z|V_{\mathcal{T}_2}, Q) + I(V_{\mathcal{T}_2}; Z|Q) \\
&\overset{(e)}{=} I(V_{\mathcal{T}_1\cap\mathcal{T}_2}; Z|Q) + I(V_{\mathcal{T}_1\cup\mathcal{T}_2}; Z|Q), \\
&\overset{(a)}{=} b^-_{\mathcal{T}_1\cap\mathcal{T}_2} + b^-_{\mathcal{T}_1\cup\mathcal{T}_2},
\end{aligned}
$$

where (a) is by the definition of $b^-_{\mathcal{T}}$; (b) is by the fact that $\mathcal{T}_1 = (\mathcal{T}_1 \cap \mathcal{T}_2) \cup (\mathcal{T}_1 \cap \mathcal{T}_2^c)$; (c) is by the chain rule of the mutual information; (d) is by the fact that $\mathcal{T}_2 = (\mathcal{T}_1 \cap \mathcal{T}_2) \cup (\mathcal{T}_1^c \cap \mathcal{T}_2)$ and

$$
\begin{aligned}
I(V_{\mathcal{T}_1\cap\mathcal{T}_2^c}; Z|V_{\mathcal{T}_2}, Q) &= I(V_{\mathcal{T}_1\cap\mathcal{T}_2^c}; V_{\mathcal{T}_1^c\cap\mathcal{T}_2}, Z|V_{\mathcal{T}_1\cap\mathcal{T}_2}, Q) \\
&\geq I(V_{\mathcal{T}_1\cap\mathcal{T}_2^c}; Z|V_{\mathcal{T}_1\cap\mathcal{T}_2}, Q),
\end{aligned}
$$

which holds since given $(Q, V_{\mathcal{T}_1\cap\mathcal{T}_2})$, $V_{\mathcal{T}_1\cap\mathcal{T}_2^c}$ and $V_{\mathcal{T}_1^c\cap\mathcal{T}_2}$ are independent of each other; and (e) is due to the facts that $\mathcal{T}_1 \cup \mathcal{T}_2 = \mathcal{T}_2 \cup (\mathcal{T}_1 \cap \mathcal{T}_2^c)$.

Appendix H
Proof of Lemma 9

For a fixed $\mathcal{S} \subseteq \mathcal{K}$, consider $H(M_{\mathcal{S}}|Z^n, Q^n, \mathcal{C})$. We have

$$
\begin{aligned}
& H(M_{\mathcal{S}}|Z^n, Q^n, \mathcal{C}) \\
&= H(M_{\mathcal{S}}, Z^n|Q^n, \mathcal{C}) - H(Z^n|Q^n, \mathcal{C}) \\
&= H(M_{\mathcal{K}}, M_{\mathcal{K},r}, Z^n|Q^n, \mathcal{C}) - H(M_{\mathcal{S}^c}, M_{\mathcal{K},r}|M_{\mathcal{S}}, Z^n, Q^n, \mathcal{C}) \\
&\quad - H(Z^n|Q^n, \mathcal{C}) \\
&= H(M_{\mathcal{K}}, M_{\mathcal{K},r}|Q^n, \mathcal{C}) + H(Z^n|M_{\mathcal{K}}, M_{\mathcal{K},r}, Q^n, \mathcal{C}) \\
&\quad - H(Z^n|Q^n, \mathcal{C}) - H(M_{\mathcal{S}^c}, M_{\mathcal{K}}|M_{\mathcal{S}}, Z^n, Q^n, \mathcal{C}) \\
&\overset{(a)}{=} H(M_{\mathcal{K}}, M_{\mathcal{K},r}|Q^n, \mathcal{C}) \\
&\quad + H(Z^n|V_1^n, V_2^n, \ldots, V_K^n, M_{\mathcal{K}}, M_{\mathcal{K},r}, Q^n, \mathcal{C}) \\
&\quad - H(Z^n|Q^n, \mathcal{C}) - H(M_{\mathcal{S}^c}, M_{\mathcal{K},r}|M_{\mathcal{S}}, Z^n, Q^n, \mathcal{C}) \\
&\overset{(b)}{=} n\sum_{i\in\mathcal{K}}[R_i + R_{i,r}] + H(Z^n|V_1^n, V_2^n, \ldots, V_K^n, Q^n, \mathcal{C}) \\
&\quad - H(Z^n|Q^n, \mathcal{C}) - H(M_{\mathcal{S}^c}, M_{\mathcal{K},r}|M_{\mathcal{S}}, Z^n, Q^n, \mathcal{C}) \\
&\overset{(c)}{\geq} n\sum_{i\in\mathcal{K}}[R_i + R_{i,r}] - I(V_1^n, V_2^n, \ldots, V_K^n; Z^n|Q^n, \mathcal{C}) \\
&\quad - n\left[\sum_{i\in\mathcal{S}^c} R_i + \sum_{i\in\mathcal{K}} R_{i,r} - I(V_1, V_2, \ldots, V_K; Z|Q) + \varepsilon_n\right] \\
&= n\sum_{i\in\mathcal{S}} R_i - n\varepsilon_n + \\
&\quad nI(V_1, V_2, \ldots, V_K; Z|Q) - I(V_1^n, V_2^n, \ldots, V_K^n; Z^n|Q^n, \mathcal{C}) \\
&\overset{(d)}{\geq} n\sum_{i\in\mathcal{S}} R_i - n\tau_n,
\end{aligned}
$$

where (a) follows from the fact that $V_1^n, V_2^n, \ldots, V_K^n$ are functions of $(M_1, M_{1,r})$, $(M_2, M_{2,r}), \ldots$, and $(M_K, M_{K,r})$, respectively, given Q^n and $\mathcal{C}$; (b) follows from the fact that $H(M_{\mathcal{K}}, M_{\mathcal{K},r}|Q^n, \mathcal{C}) = n\sum_{i\in\mathcal{K}}[R_i + R_{i,r}]$, and given Q^n and $\mathcal{C}$, the Markov chain:$(M_{\mathcal{K}}, M_{\mathcal{K}}) \to (V_1^n, V_2^n, \ldots, V_K^n) \to Z^n$; (c) follows from Lemma 1 (with $R_{v,j} = R_{j,r}$ for $j \in \mathcal{S}$, and $R_{v,j} = R_j + R_{j,r}$ for $j \in \mathcal{S}^c = \mathcal{K}\backslash\mathcal{S}$) by requiring $\sum_{j\in\mathcal{J}} R_{v,j} \geq I(V_{\mathcal{J}}; Z|Q), \forall\mathcal{J} \subseteq \mathcal{K}$, i.e., $\sum_{j\in\mathcal{J}\cap\mathcal{S}^c} R_j + \sum_{j\in\mathcal{J}} R_{j,r} \geq I(V_{\mathcal{J}}; Z|Q), \forall\mathcal{J} \subseteq \mathcal{K}$. (d) due to the fact that $I(V_1^n, V_2^n, \ldots, V_K^n; Z^n|Q^n, \mathcal{C}) \leq n[I(V_1, V_2, \ldots, V_K; Z|Q) + \varepsilon_n]$, the proof of which follows the proof of [32, Lemma 3], and taking $\tau_n = 2\varepsilon_n$.

Acknowledgement

The authors would like to thank Prof. Matthieu Bloch for pointing us the paper [40] and suggesting the example given in Section VI-B to achieve a stronger secrecy notion.

References

[1] Y. Chen, O. O. Koyluoglu, and H. Vinck, "Joint secrecy over the K-transmitter multiple access channel," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2017, pp. 394–398.

[2] R. Ahlswede, *Multi-Way Communication Channels*. Budapest, Hungary: Akadémiai Kiadó, 1973.

[3] H. H.-J. Liao, "Multiple access channels," Ph.D. dissertation, Dept. Elect. Eng., Univ. Hawaii, Honolulu, HI, USA, 1972.

[4] D. Slepian and J. K. Wolf, "A coding theorem for multiple access channels with correlated sources," *Bell Syst. Tech. J.*, vol. 52, no. 7, pp. 1037–1076, 1973.

[5] T. S. Han, "The capacity region of general multiple-access channel with certain correlated sources," *Inf. Control*, vol. 40, no. 1, pp. 37–60, 1979.

[6] T. M. Cover, A. El Gamal, and M. Salehi, "Multiple access channels with arbitrarily correlated sources," *IEEE Trans. Inf. Theory*, vol. IT-26, no. 6, pp. 648–657, Nov. 1980.

[7] N. Gaarder and J. Wolf, "The capacity region of a multiple-access discrete memoryless channel can increase with feedback (Corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-21, no. 1, pp. 100–102, Jan. 1975.

[8] T. Cover and C. Leung, "An achievable rate region for the multiple-access channel with feedback," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 3, pp. 292–298, May 1981.

[9] E. van der Meulen, "A survey of multi-way channels in information theory: 1961-1976," *IEEE Trans. Inf. Theory*, vol. 23, no. 1, pp. 1–37, Jan. 1977.

[10] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[11] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[12] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[13] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Multiple access channels with generalized feedback and confidential messages," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Sep. 2007, pp. 608–613.

[14] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[15] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 1014–1021.

[16] O. O. Koyluoglu and H. El Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5682–5694, Sep. 2011.

[17] M. H. Yassaee and M. R. Aref, "Multiple access wiretap channels with strong secrecy," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Sep. 2010, pp. 1–5.

[18] M. Wiese and H. Boche, "Strong secrecy for multiple access channels," in *Information Theory, Combinatorics, and Search Theory* (Lecture Notes in Computer Science), vol. 7777. Berlin, Germany: Springer, 2013, pp. 71–122.

[19] R. Liu, I. Marić, R. D. Yates, and P. Spasojević, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2006, pp. 957–961.

[20] Y. Liang and H. Poor, "Generalized multiple access channels with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2006, pp. 952–956.

[21] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[22] Y.-K. Chia and A. El Gamal, "Three-receiver broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2748–2765, May 2012.

[23] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. New York, NY, USA: Cambridge Univ. Press, 2012.

[24] M. Madiman, "Cores of cooperative games in information theory," *EURASIP J. Wireless Commun. Netw.*, vol. 2008, no. 1, p. 318704, 2008.

[25] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2006.

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

[27] Y. Chen, O. O. Koyluoglu, and H. Vinck, "On secure communication over the multiple access channel," in *Proc. IEEE Int. Symp. Inf. Theory Appl. (ISITA)*, Oct. 2016, pp. 355–359.

[28] Y. Steinberg, "Resolvability theory for the multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 472–487, Mar. 1998.

[29] I. B. Gattegno, Z. Goldfeld, and H. H. Permuter. (2016). "Fourier-motzkin elimination software for information theoretic inequalities." [Online]. Available: https://arxiv.org/abs/1610.03990

[30] S. Fujishige, "Polymatroidal dependence structure of a set of random variables," *Inf. Control*, vol. 39, no. 1, pp. 55–72, 1978.

[31] J.-l. Imbert, "Fourier's elimination: Which to choose?" in *Proc. PPCP*, 1993, pp. 117–129.

[32] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[33] I. Csiszár, "Almost independence and secrecy capacity," *Probl. Peredachi Inf.*, vol. 32, no. 1, pp. 48–57, 1996.

[34] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proc. Int. Conf. Theory Appl. Cryptogr. Techn. (Eurocrypt)*, 2000, pp. 351–368.

[35] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.

[36] T. S. Han, H. Endo, and M. Sasaki, "Reliability and secrecy functions of the wiretap channel under cost constraint," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6819–6843, Nov. 2014.

[37] J. Hou and G. Kramer, (Jan. 2014). "Effective secrecy: Reliability, confusion and stealth." [Online]. Available: https://arxiv.org/abs/1311.1411

[38] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Proc. Int. Cryptol. Conf. (CRYPTO)*, 2012, pp. 294–311.

[39] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1562–1575, Apr. 2006.

[40] M. H. Yassaee, M. R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6760–6786, Nov. 2014.

[41] M. Hayashi and R. Matsumoto, "Secure multiplex coding with dependent and non-uniform multiple messages," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2355–2409, May 2016.

Yanling Chen received the B.S. and M.S. degrees in applied mathematics from Nankai University, Tianjin, China, in 2001 and 2004, respectively, and the Ph.D. degree in engineering from the University of Duisburg-Essen (UDE), Germany, in 2007. She is currently a Researcher with the Institute of Digital Signal Processing, UDE. Her research interests include information and coding theory, cryptography, and their applications in communication networks, secure storage, and biometrics.

O. Ozan Koyluoglu received the B.S. degree in electrical and electronics engineering from Bilkent University, Ankara, Turkey, in 2005, and the M.S. and Ph.D. degrees in electrical and computer engineering from The Ohio State University, Columbus, OH, USA, in 2007 and 2010, respectively. Since 2017, he has been with the University of California at Berkeley. His current research interests are in the areas of information theory, machine learning, distributed storage/computing, networks, and computational neuroscience.

A. J. Han Vinck studied electrical engineering at the University of Eindhoven, The Netherlands, where he received the Ph.D. degree in 1980. From 1990 to 2014, he was a Professor in digital communications with the Institute for Experimental Mathematics, University of Essen, Germany. He has been a Senior Professor with the Institute of Digital Signal Processing, University of Duisburg-Essen, Germany, since 2014. He is the author of the book *Coding Concepts and Reed-Solomon Codes*. His interest is in information and communication theory, coding and network aspects in digital communications. Since 2014, he is a Co-Founder and President of the Leibniz Foundation. This foundation stimulates research in the field of information theory, neuroscience, and biology.