A New Achievable Region of the K-User MAC Wiretap Channel with Confidential and Open Messages Under Strong Secrecy

Hao Xu, *Member, IEEE*, Kai-Kit Wong, *Fellow, IEEE*, and Giuseppe Caire, *Fellow, IEEE*

Abstract

This paper investigates the achievable region of a K-user discrete memoryless (DM) multiple access wiretap (MAC-WT) channel, where each user transmits both secret and open (i.e., non-confidential) messages. All these messages are intended for the legitimate receiver (Bob), while the eavesdropper (Eve) is only interested in the secret messages. In the achievable coding strategy, the confidential information is protected by open messages and also by the introduction of auxiliary messages. When introducing an auxiliary message, one has to ensure that, on one hand, its rate is large enough for protecting the secret message from Eve and, on the other hand, the resulting sum rate (together with the secret and open message rate) does not exceed Bob's decoding capability. This yields an inequality structure involving the rates of all users' secret, open, and auxiliary messages. We provide such a structure and give the general proof. Note that for a case with a few users, the result can be proven by direct application of the Fourier-Motzkin elimination procedure. However, this direct approach becomes extremely intractable as the number of users increases and does not generalize to the model at hand with an arbitrary number of users. We prove the result in full generality through the combined use of Fourier-Motzkin elimination procedure and mathematical induction. This paper adopts the *strong secrecy* metric, characterized by *information leakage*. To prove the achievability under this criterion, we analyze the resolvability region

H. Xu and K.-K. Wong are with the Department of Electronic and Electrical Engineering, University College London, London WC1E 7JE, UK (e-mail: hao.xu@ucl.ac.uk; kai-kit.wong@ucl.ac.uk).

G. Caire is with the Faculty of Electrical Engineering and Computer Science at the Technical University of Berlin, 10587 Berlin, Germany (e-mail: caire@tu-berlin.de).

of a K-user DM-MAC channel (not necessarily a wiretap channel). In addition, we show that users with zero secrecy rate can play different roles and use different strategies in encoding their messages. These strategies yield non-redundant (i.e., not mutually dominating) rate inequalities. By considering all possible coding strategies, we provide a new achievable region for the considered channel, and show that it strictly improves those already known in the existing literature by considering a two-user binary adder channel.

Index Terms

Discrete memoryless (DM) multiple access wiretap (MAC-WT) channel, strong secrecy, secret and open messages, achievable rate region, binary adder channel.

I. INTRODUCTION

Information theoretic security, also known as *physical layer security*, is an alternative to cryptographic security that may be attractive in cases where generating, distributing, and managing cryptographic keys is difficult, or if advances in quantum computing will make systems based on classical computational cryptography intrinsically insecure. Physical layer security techniques exploit the randomness of the transmission channel and particular code constructions to prevent the eavesdroppers (Eves) from wiretapping, and do not rely on Eves' limited computational capability assumptions. After the first seminal works on the single-user wiretap channel [2]–[5], the research on physical layer security considered various network topologies such as multiple access (MAC) wiretap channels [6]–[18], broadcast channels [19]–[22], interference channels [23]–[26], and relay-aided channels [27]–[30].

This paper focuses on the MAC wiretap (MAC-WT) channel. To put our work in context, we review the main related literature below. In [6]–[8], two-user discrete memoryless (DM) MAC-WT systems were studied, where [6] developed inner and outer bounds for a channel with a weaker Eve, and [7] and [8] studied a channel where two users communicate with a common receiver and see each other as an Eve. In [10]–[15], the more general scenario with an arbitrary number K of users was investigated. Specifically, [10] and [11] developed achievable regions for DM MAC-WT channels, and [12] studied a Gaussian MAC-WT system with a weaker Eve seeing a degraded channel. Reference [13] extended the work of [12] to the non-degraded Gaussian MAC and Gaussian two-way wiretap channels, where each user has, in addition to confidential information, also an open (i.e., non-confidential) message for the legitimate receiver. Achievable regions were derived, the sum secrecy rate was maximized by power control, and cooperative

jamming was also proposed to enhance the secrecy. Note that in some papers, "open message" is also called "private message" [31]. In [14] and [15], the achievable regions of MAC-WT systems with open and secret messages were further studied, and it was shown that by introducing open messages to wiretap channels, the system spectral efficiency can be significantly increased while the secrecy performance remains unchanged.

The literature mentioned above considered the *weak secrecy* criterion, characterized by the *information leakage rate*. It should be noted that a vanishing information leakage rate does not imply that a vanishing number of information bits of the secret message are leaked, because the length of the message in bits grows linearly with the block length n. To address this issue, *strong secrecy* was introduced in [32], [33], by considering directly the *information leakage* in terms of the multi-letter mutual information between messages and Eve's received signal, without normalization by n. A comprehensive discussion on different secrecy metrics can be found in [34]. Under strong secrecy, [16]–[18] have studied the standard DM MAC-WT channel with only secret messages. Specifically, by analyzing the output statistics in terms of average variational distance and applying random coding, an achievable region was provided in [16]. In [17], the MAC-WT system with a DM main channel and different wiretapping scenarios was studied. Both [16] and [17] considered the two-user case. In [18], a K-user DM MAC-WT channel was investigated and the results in [10] and [11] were strengthened subject to the strong secrecy metric. However, by checking the two-user case and comparing [18, (14)] with [16, Theorem 1], it can be seen that the achievable region given in [18] includes only the region $\mathcal{R}_1$ in [16] but not $\mathcal{R}_2$ and $\mathcal{R}_3$, indicating that even for the MAC-WT channel with only secret messages, there is still space for improvement of the achievable region.

In this paper, we study the information-theoretic secrecy problem for a K-user DM MAC-WT channel where users have both secret and open messages for the intended receiver (Bob) while preserving the confidentiality of the secret messages with respect to Eve. Eve aims to wiretap the confidential information of all users and the users do not care if their open messages may be decoded by Eve. The main contributions of this work are summarized below.

- In wiretap channels, typical achievability strategies are based on introducing auxiliary messages to protect the confidential information. When introducing an auxiliary message, one has to ensure that, on one hand, its rate is large enough for protecting the secret message from Eve and, on the other hand, the resulting sum rate (together with the secret and open message rate) does not exceed Bob's decoding capability. This yields an inequality

structure involving the rates of all users' secret, open, and auxiliary messages. In Theorem 1 we provide such structure and also give the conditions under which this structure can be satisfied. An essential step in the proof of Theorem 1 is provided by Lemma 1. A two-user case of Lemma 1 was proven in [15, Lemma 7] by direct application of the Fourier-Motzkin elimination procedure [35, Appendix D]. However, as K grows, this direct proof becomes unmanageable due to the excessively large number of inequalities. To exemplify the complexity of the direct Fourier-Motzkin application, we provided the case $K = 3$ in the unpublished research note [36], from which we see that even in this relatively simple case, over 130 inequalities are generated in the direct elimination procedure. Besides the extremely high complexity, another disadvantage of the direct elimination strategy is that it can be applied in principle only if the number of users K is fixed so that all inequalities can be listed. This makes the direct proof approach inappropriate for Lemma 1, since it is stated for general K, which can take any value. In Appendix A, we circumvent this problem and provide a general proof of Lemma 1 through the combined use of Fourier-Motzkin elimination procedure and mathematical induction. Then, using this lemma, the general proof of Theorem 1 follows. We prove the achievability under the *strong secrecy* metric. To this end, we analyze the resolvability region for a K-user standard DM-MAC channel (not necessarily a wiretap channel) in Theorem 2.[1]

- In this paper, the confidential information is protected by open messages and also by the introduced auxiliary messages. In general, the sum rate of these messages should exceed a certain amount such that the confidential information can be perfectly protected. However, a novel observation and main contribution of this paper is that if a user has no secret message, this may no longer be necessary and may even limit the resulted achievable region. In this case, the user can play different roles and has two options: 1) introducing an additional auxiliary message such that the sum rate of its messages is beyond Eve's decoding capability; 2) simply encoding and transmitting its open message as in a standard MAC channel with no wiretapping. We show that both these two options can guarantee the secrecy, but yield non-redundant (i.e., not mutually dominating) rate inequalities. Therefore, by considering the union over all options, i.e., all coding strategies for the users with zero secret rates,

---

[1]One may refer to [34], [37], and [38] for the notion of resolvability and resolvability region, and their relationship with secrecy.

we obtain a larger achievable region (Theorem 3) than previously known. Interestingly, by simply letting the open message rate of all users be zero, we obtain an achievable region for the standard DM MAC-WT channel with only secret messages directly from Theorem 3. This region is strictly larger than that provided in [18], and generalizes the region for $K = 2$ provided in [16].

- To compare the proposed new achievable region with that provided in [15], we consider a two-user binary adder channel with Bernoulli-distributed noise. For such a channel, all bounds in the derived achievable region can be computed. Considering a given noise distribution and depicting the region given in [15] and also partial of the achievable region proposed in this paper over all input distributions, we obtain two convex hulls. For convenience, we call them old and new convex hulls, respectively. The numerical results show that there exist channels with given noise distribution such that the two convex hulls have non-overlapping areas. In addition, we can find points in the new convex hull that can be linearly separated from the old convex hull using a support vector machine (SVM). These points are thus not included in the old convex hull. These results indicate that the achievable region proposed in this paper can strictly improve that provided in [15].

The rest of this paper is organized as follows. In Section II we introduce the K-user DM MAC-WT channel model and give the definition of "achievability". In Section III we give the main results. The achievability proof of the new region is provided in Section IV. In Section V, the proposed new region is compared with the region in the existing literature in a two-user binary adder channel. Section VI points out some concluding remarks. Auxiliary technical results are given in the appendices.

Notations: We use upper and lower case letters to denote random variables and their realizations, e.g., X, x. $P_X(\cdot)$ denotes the probability mass function (pmf) [2] of X in the sense that $P_X(\cdot) \triangleq \{P_X(x) : x \in \mathcal{X}\}$ where $P_X(x) = \Pr\{X = x\}$. For two different distributions $\hat{P}_X(\cdot)$ and $\tilde{P}_X(\cdot)$ on the same alphabet $\mathcal{X}$, their total variational distance is defined as the ℓ_1 norm of the difference of the corresponding pmfs, i.e., $\left\| \hat{P}_X(\cdot) - \tilde{P}_X(\cdot) \right\|_1 = \sum_{x \in \mathcal{X}} \left| \hat{P}_X(x) - \tilde{P}_X(x) \right|$. We use calligraphic capital letters to denote sets, $|\mathcal{X}|$ indicates the cardinality of a set $\mathcal{X}$, and $\mathcal{X}_1 \setminus \mathcal{X}_2$ denotes set subtraction, and $\mathcal{X}_1 \times \mathcal{X}_2$ is the Cartesian product set. We use line over a calligraphic letter to indicate it is the complement of a set, e.g., $\overline{\mathcal{K}'} = \mathcal{K} \setminus \mathcal{K}'$ if $\mathcal{K}' \subseteq \mathcal{K}$, and

---

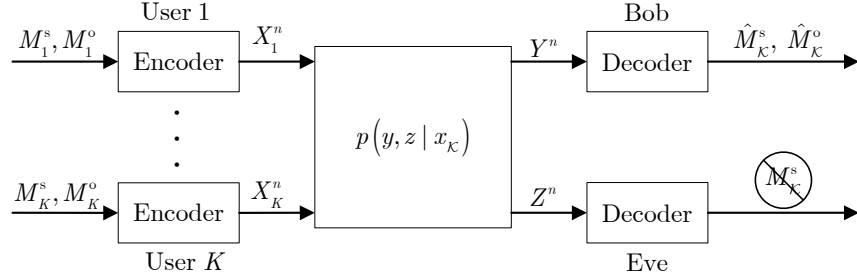[2]Loosely referred to as "distributions" in the following.

Fig. 1. Block diagram of a K-user DM MAC-WT channel with secret (i.e., confidential) and open (i.e., non-confidential) messages. Both secret and open messages are intended for Bob, while Eve is interested only in the secret messages.

calligraphic subscript to denote the set of elements whose indexes take values from the subscript set, e.g., $X_{\mathcal{K}} = \{X_k : k \in \mathcal{K}\}$. Finally, we use $[\cdot]^+ \triangleq \max(\cdot, 0)$.

II. CHANNEL MODEL AND PROBLEM DEFINITION

Fig. 1 shows the considered DM MAC-WT channel with K transmitters, a legitimate receiver (Bob), and an eavesdropper (Eve). Let $\mathcal{K} = \{1, \cdots, K\}$ denote the set of all users. The DM MAC-WT channel is defined by $(\mathcal{X}_{\mathcal{K}}, P_{Y,Z|X_{\mathcal{K}}}, \mathcal{Y}, \mathcal{Z})$ (in short $P_{Y,Z|X_{\mathcal{K}}}$), where $\mathcal{X}_k$, $\mathcal{Y}$, and $\mathcal{Z}$ are finite alphabets, $x_k \in \mathcal{X}_k$ is the channel input of user k, and $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$ are respectively channel outputs at Bob and Eve. Each user $k \in \mathcal{K}$ has a secret (i.e., confidential) message M_k^{s} and also an open (i.e., non-confidential) message M_k^{o} intended for Bob. Both messages carry useful information for Bob, and therefore must be reliably decoded by Bob. Eve attempts to overhear the secret messages and is not interested in the open messages, although it may decode (some of) them as part of an eavesdropping strategy. User k encodes its information into a codeword X_k^n and then transmits it over the channel. Upon receiving the sequence Y^n, Bob decodes the messages of all users. To avoid leakage of confidential information to Eve, the secret messages of all users, i.e., $M_{\mathcal{K}}^{\mathrm{s}}$, should be protected.

Let R_k^{s} and R_k^{o} denote the rate of user k's secret and open messages. Then, a secrecy code for the considered DM MAC-WT channel consists of

- Secret and open message sets: $\mathcal{M}_k^{\mathrm{s}} = [1 : 2^{nR_k^{\mathrm{s}}}]$ and $\mathcal{M}_k^{\mathrm{o}} = [1 : 2^{nR_k^{\mathrm{o}}}]$, $\forall k \in \mathcal{K}$. Messages M_k^{s} and M_k^{o} are uniformly distributed over the corresponding sets $\mathcal{M}_k^{\mathrm{s}}$ and $\mathcal{M}_k^{\mathrm{o}}$.
- K randomized encoders: the encoder of user k maps the message pair $(M_k^{\mathrm{s}}, M_k^{\mathrm{o}}) \in \mathcal{M}_k^{\mathrm{s}} \times \mathcal{M}_k^{\mathrm{o}}$ to a (possibly random) codeword X_k^n.

- A decoder at Bob which maps the received noisy sequence Y^n to the message estimate $\left(\hat{M}_k^s, \hat{M}_k^o \right) \in \mathcal{M}_k^s \times \mathcal{M}_k^o, \forall k \in \mathcal{K}$.

Next, we define the criteria for achievability. These criteria are defined in an *operational sense*, i.e., in terms of the behavior of the error probability at Bob and information leakage at Eve.

Definition 1. *A rate-tuple* $(R_1^s, R_1^o, \cdots, R_K^s, R_K^o)$ *is said to be achievable if there exists a sequence of* $\left(2^{nR_1^s}, 2^{nR_1^o}, \cdots, 2^{nR_K^s}, 2^{nR_K^o}, n \right)$ *codes such that*

$$\lim_{n \to \infty} Pr\left\{ \left(\hat{M}_{\mathcal{K}}^s, \hat{M}_{\mathcal{K}}^o \right) \neq (M_{\mathcal{K}}^s, M_{\mathcal{K}}^o) \right\} = 0, \tag{1}$$

$$\lim_{n \to \infty} I(M_{\mathcal{K}}^s; Z^n) = 0, \tag{2}$$

can be satisfied. ◇

Given an ensemble of coding strategies, the corresponding achievable region $\mathscr{R}$ for the DM MAC-WT is the convex closure of all rate-tuples $(R_1^s, R_1^o, \cdots, R_K^s, R_K^o) \in \mathbb{R}_+^{2K}$ satisfying Definition 1 under such coding strategies. The determination of the largest possible achievable region (i.e., the capacity region) requires also the proof of a converse result. Converses (i.e., matching outer bounds) for the DM MAC-WT are generally yet an open problem even in the case of zero open message rates, while of course they are well-known in the case of zero secret message rates [39]. Focusing on achievability, in the following we provide a new achievable region which is generally larger than what was known in the existing literature.

III. MAIN RESULTS

In this section, we provide an achievable region for the considered DM MAC-WT channel under strong secrecy and show that it improves the one in [15, Lemma 1]. Using the result, a new achievable secrecy rate region can be directly obtained for the standard DM MAC-WT channel with only secret messages. Before giving the regions, we first provide some auxiliary results that are important for the achievability proof.

A. Auxiliary Results

We shall consider achievability strategies where users may introduce auxiliary messages to protect the confidential information, and use superscript "a" to distinguish from the secret and open messages. Let M_k^a denote the auxiliary message introduced for user k and R_k^a denote its rate. Note that in this paper, there are three types of messages, i.e., secret, open, and auxiliary

messages. As we have explained at the beginning of Section II, both the secret and open messages are intended for Bob, while Eve is only interested in the secret messages. Note that the auxiliary messages are not intended for either Bob or Eve. They are introduced only to add dummy randomness to protect or "hide" the secret messages. As explained in the introduction, there should be a relationship or structure for R_k^s, R_k^o, and R_k^a, $\forall k \in \mathcal{K}$ such that the sum rate of the messages does not exceed Bob's decoding capability and the confidential information can be protected. In the following theorem, we construct such a structure (see (5)) and also give the conditions (see (3) and (4)) under which this structure can be satisfied.

Theorem 1. *Let* $(X_\mathcal{K}, Y, Z) \sim \prod_{k=1}^{K} P_{X_k} P_{Y,Z|X_\mathcal{K}}$. *For a given subset* $\mathcal{K}' \subseteq \mathcal{K}$, *if*

$$I(X_\mathcal{S}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) - I(X_\mathcal{S}; Z | X_{\overline{\mathcal{K}'}}) \geq 0, \forall \mathcal{S} \subseteq \mathcal{K}', \tag{3}$$

then, for any rate-tuple $(R_1^s, R_1^o, \cdots, R_K^s, R_K^o)$ *satisfying*

$$\begin{cases} R_k^s = 0, \forall k \in \overline{\mathcal{K}'}, \\ \sum_{k \in \mathcal{S}} R_k^s + \sum_{k \in \mathcal{S} \backslash \mathcal{S}'} R_k^o + \sum_{k \in \mathcal{T}} R_k^o \leq I(X_\mathcal{S}, X_\mathcal{T}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}) - I(X_{\mathcal{S}'}; Z | X_{\overline{\mathcal{K}'}}), \\ \qquad\qquad\qquad \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S}' \subseteq \mathcal{S}, \mathcal{T} \subseteq \overline{\mathcal{K}'}, \end{cases} \tag{4}$$

there exist R_k^a, $\forall k \in \mathcal{K}'$ *such that*

$$\begin{cases} R_k^a \geq 0, \forall k \in \mathcal{K}', \\ \sum_{k \in \mathcal{S}} (R_k^s + R_k^o + R_k^a) + \sum_{k \in \mathcal{T}} R_k^o \leq I(X_\mathcal{S}, X_\mathcal{T}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}), \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{T} \subseteq \overline{\mathcal{K}'}, \\ \sum_{k \in \mathcal{S}} (R_k^o + R_k^a) \geq I(X_\mathcal{S}; Z | X_{\overline{\mathcal{K}'}}), \forall \mathcal{S} \subseteq \mathcal{K}', \end{cases} \tag{5}$$

where $\overline{\mathcal{K}'} = \mathcal{K} \setminus \mathcal{K}'$, $\overline{\mathcal{S}} = \mathcal{K}' \setminus \mathcal{S}$, *and* $\overline{\mathcal{T}} = \overline{\mathcal{K}'} \setminus \mathcal{T}$.

Proof: In the following Lemma 1 and Appendix A, we give a special case of Theorem 1 with $\mathcal{K}' = \mathcal{K}$ and its proof. Then, we prove Theorem 1 in Appendix B by using Lemma 1. $\square$

For any $\mathcal{K}' \subseteq \mathcal{K}$, using the chain rule and non-negativity of mutual information, we have

$$I(X_\mathcal{S}, X_\mathcal{T}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}) = I(X_\mathcal{S}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) + I(X_\mathcal{T}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}})$$

$$\geq I(X_\mathcal{S}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}), \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{T} \subseteq \overline{\mathcal{K}'},$$

$$I(X_\mathcal{S}; Z | X_{\overline{\mathcal{K}'}}) = I(X_{\mathcal{S}'}, X_{\mathcal{S} \backslash \mathcal{S}'}; Z | X_{\overline{\mathcal{K}'}})$$

$$= I(X_{\mathcal{S}'}; Z | X_{\overline{\mathcal{K}'}}) + I(X_{\mathcal{S} \backslash \mathcal{S}'}; Z | X_{\mathcal{S}'}, X_{\overline{\mathcal{K}'}})$$

$$\geq I(X_{\mathcal{S}'}; Z | X_{\overline{\mathcal{K}'}}), \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S}' \subseteq \mathcal{S}. \tag{6}$$

If (3) holds, due to (6), we have

$$I(X_{\mathcal{S}}, X_{\mathcal{T}}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}) - I(X_{\mathcal{S}'}; Z | X_{\overline{\mathcal{K}'}}) \geq 0, \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S}' \subseteq \mathcal{S}, \mathcal{T} \subseteq \overline{\mathcal{K}'}, \tag{7}$$

i.e., each upper bound in (4) is non-negative. On the other hand, by setting $\mathcal{S}' = \mathcal{S}$ and $\mathcal{T} = \phi$ in (7), we can obtain (3) directly from (7). Hence, (3) and (7) are actually equivalent.

For each $\mathcal{K}' \subseteq \mathcal{K}$, Theorem 1 gives the existence conditions of $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}'$ in (3) and (4). To apply the coding scheme provided in the next section, it is also necessary to know how to obtain $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}'$. This can be done efficiently as follows. For a given rate point $(R_1^{\mathrm{s}}, R_1^{\mathrm{o}}, \cdots, R_K^{\mathrm{s}}, R_K^{\mathrm{o}})$, if (3) and (4) can be satisfied, the linear inequalities in (5) define a polytope as a feasible region of $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}'$. Then, we may apply Dantzig's simplex algorithm to obtain $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}'$ [40].

Now we consider the special case of Theorem 1 with $\mathcal{K}' = \mathcal{K}$. The basic result is collected in the following lemma.

Lemma 1. *Let* $(X_{\mathcal{K}}, Y, Z) \sim \prod_{k=1}^{K} P_{X_k} P_{Y,Z|X_{\mathcal{K}}}$. *If*

$$I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}) - I(X_{\mathcal{S}}; Z) \geq 0, \forall \mathcal{S} \subseteq \mathcal{K}, \tag{8}$$

then, for any rate-tuple $(R_1^{\mathrm{s}}, R_1^{\mathrm{o}}, \cdots, R_K^{\mathrm{s}}, R_K^{\mathrm{o}})$ *satisfying*

$$\sum_{k \in \mathcal{S}} R_k^{\mathrm{s}} + \sum_{k \in \mathcal{S} \setminus \mathcal{S}'} R_k^{\mathrm{o}} \leq I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}) - I(X_{\mathcal{S}'}; Z), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S}' \subseteq \mathcal{S}, \tag{9}$$

there exist $R_k^a, \forall k \in \mathcal{K}$ *such that*

$$\begin{cases} R_k^a \geq 0, \forall k \in \mathcal{K}, \\ \sum_{k \in \mathcal{S}} (R_k^{\mathrm{s}} + R_k^{\mathrm{o}} + R_k^a) \leq I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}), \forall \mathcal{S} \subseteq \mathcal{K}, \\ \sum_{k \in \mathcal{S}} (R_k^{\mathrm{o}} + R_k^a) \geq I(X_{\mathcal{S}}; Z), \forall \mathcal{S} \subseteq \mathcal{K}, \end{cases} \tag{10}$$

where $\overline{\mathcal{S}} = \mathcal{K} \setminus \mathcal{S}$.

Proof: See Appendix A. □

Remark 1. *Lemma 1 is a direct extension of [15, Lemma 7] from a two-user case to the general K-user case. For the simple system with a small K, e.g., $K = 1$ or $K = 2$, Lemma 1 can be proven by eliminating R_k^a in (10) using the Fourier-Motzkin procedure [35, Appendix D] and showing that (9) is the projection of (10) onto the hyperplane $\{R_k^a = 0, \forall k \in \mathcal{K}\}$. However, when K increases, the number of inequalities resulted in the elimination procedure grows very*

quickly (doubly exponentially), making it quite difficult or even impractical to prove this lemma by following this brute-force way. Besides the great complexity, another problem is that the direct elimination strategy works in principle only if K is fixed so that all inequalities can be listed. This makes the strategy inappropriate for the proof of Lemma 1, since it is stated for general K, which can take any value.

In the research note [36], we consider a system with $K = 3$ and prove Lemma 1 by eliminating R_1^a, R_2^a, and R_3^a one by one. From (10) we first get 4 upper bounds and 5 lower bounds on R_1^a. By pairing up these lower and upper bounds, we get 20 inequalities, based on which 8 upper bounds and 7 lower bounds on R_2^a are obtained. We then eliminate R_2^a and get 56 inequalities, most of which are redundant. Neglecting the redundant terms, we further get 9 upper bounds and 7 lower bounds on R_3^a, and 63 inequalities by pairing them up. Neglecting the redundant terms, we show that the remaining inequalities construct (9). This unpublished note is mentioned here and made public in [36] to illustrate how difficult the brute-force Fourier-Motzkin elimination is, even in the simple case of 3 users. ◇

This paper employs the strong secrecy metric and proves the achievability based on the resolvability theory of the MAC channel. The notion of channel resolvability was introduced in [41] to approximate the output distribution of single-user channels by simulating an input process. Then, in [42] and [43], it was further developed to study the randomness needed for approximating the output distribution and the identification capacity for two-user MAC channels, respectively. The resolvability theory has also been shown to be a powerful tool in proving strong secrecy in wiretap channels [16], [34], [37], [44]. Specifically, in [34] and [37], channel resolvability was leveraged to establish the secrecy-capacity region for single-user wiretap channels under the strong secrecy metric. In [16] and [44], achievable regions of two-user wiretap channels under different system settings and the strong secrecy metric were studied based on channel resolvability. In this paper, we show that the resolvability theory can also be applied to prove the strong secrecy for the considered system, where the users transmit both secret and open messages. To this end, we first extend the resolvability result in [16] from a two-user case to the K-user DM-MAC channel (not necessarily a wiretap channel) in Theorem 2.

In particular, we consider a DM-MAC channel (not necessarily a wiretap channel) with K users and a receiver. Each user k has a message M_k at rate Q_k, and M_k is uniformly distributed over

$\mathcal{M}_k = \left[1 : 2^{nQ_k}\right]$. User k generates a codebook $\mathbf{c}_k$ by randomly and independently generating 2^{nQ_k} sequences $x_k^n(m_k), \forall m_k \in \mathcal{M}_k$, each according to $\prod_{i=1}^n P_{X_k}(x_{ki})$. Then, for a given message $m_k \in \mathcal{M}_k$, user k transmits codeword $x_k^n(m_k)$ over the channel $P_{Z|X_{\mathcal{K}}}$.[3] The observation of the receiver is Z^n. Let $\mathcal{C}_k$ denote the random choice of codebook $\mathbf{c}_k$ and define the following conditional output distribution

$$P_{Z^n}(\cdot|\mathcal{C}_{\mathcal{K}}) = \sum_{m_{\mathcal{K}} \in \prod_{k \in \mathcal{K}} \mathcal{M}_k} P_{M_{\mathcal{K}}}(m_{\mathcal{K}}) P_{Z^n}(\cdot|\mathcal{C}_{\mathcal{K}}, m_{\mathcal{K}})$$

$$= 2^{-n\sum_{k \in \mathcal{K}} Q_k} \sum_{m_{\mathcal{K}} \in \prod_{k \in \mathcal{K}} \mathcal{M}_k} P_{Z^n}\left(\cdot \mid \{X_k^n(m_k)\}_{k \in \mathcal{K}}\right). \tag{11}$$

In addition, for a given $\mathcal{K}' \subseteq \mathcal{K}$, define

$$P_{Z^n}(\cdot|\mathcal{C}_{\overline{\mathcal{K}'}}) = 2^{-n\sum_{k \in \overline{\mathcal{K}'}} Q_k} \sum_{m_{\overline{\mathcal{K}'}} \in \prod_{k \in \overline{\mathcal{K}'}} \mathcal{M}_k} P_{Z^n}\left(\cdot \mid \{X_k^n(m_k)\}_{k \in \overline{\mathcal{K}'}}\right), \tag{12}$$

where

$$P_{Z^n}\left(\cdot \mid \{X_k^n(m_k)\}_{k \in \overline{\mathcal{K}'}}\right) = \sum_{x_{\mathcal{K}'}^n \in \prod_{k \in \mathcal{K}'} \mathcal{X}_k^n} P_{X_{\mathcal{K}'}^n}(x_{\mathcal{K}'}^n) P_{Z^n}\left(\cdot|x_{\mathcal{K}'}^n, \{X_k^n(m_k)\}_{k \in \overline{\mathcal{K}'}}\right). \tag{13}$$

In the following theorem we show that when certain conditions are satisfied, using the coding scheme provided above, the average variational distance between the output statistics $P_{Z^n}(\cdot|\mathcal{C}_{\mathcal{K}})$ and $P_{Z^n}(\cdot|\mathcal{C}_{\overline{\mathcal{K}'}})$ vanishes exponentially in n.

Theorem 2. *For given distribution $\prod_{k=1}^K P_{X_k} P_{Z|X_{\mathcal{K}}}$ and subset $\mathcal{K}' \subseteq \mathcal{K}$, if*

$$Q_k = 0, \forall k \in \overline{\mathcal{K}'},$$

$$\sum_{k \in \mathcal{S}} Q_k > I(X_{\mathcal{S}}; Z|X_{\overline{\mathcal{K}'}}), \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S} \neq \phi, \tag{14}$$

using the above coding scheme, there exists $\varepsilon > 0$ such that

$$\mathbb{E} \left\| P_{Z^n}(\cdot|\mathcal{C}_{\mathcal{K}}) - P_{Z^n}(\cdot|\mathcal{C}_{\overline{\mathcal{K}'}}) \right\|_1 \leq e^{-n\varepsilon}, \tag{15}$$

where the expectation is taken over the random codebooks.

Proof: See Appendix C. $\qquad \square$

By a standard random coding argument, (15) implies that, if a rate-tuple $(Q_1, \cdots, Q_K)$ satisfies (14), there must exist codebooks $\mathbf{c}_{\mathcal{K}}$ such that

$$\left\| P_{Z^n}(\cdot|\mathbf{c}_{\mathcal{K}}) - P_{Z^n}(\cdot|\mathbf{c}_{\overline{\mathcal{K}'}}) \right\|_1 \leq e^{-n\varepsilon}. \tag{16}$$

---

[3]Note that the coding scheme considered here is instrumental to prove Theorem 2, and it is different from that in Section IV.

Therefore, the region defined by (14) is the resolvability region of the DM-MAC channel with input process $X_{\mathcal{K}} \sim \prod_k P_{X_k}$ [38]. Theorem 2 shows that if a rate point is in the resolvability region, as the block length n goes to infinity, the induced output distribution $P_{Z^n}(\cdot|\mathcal{C}_{\mathcal{K}})$ conditioned on the codebooks approaches $P_{Z^n}(\cdot|\mathcal{C}_{\overline{\mathcal{K}'}})$, which is induced by the knowledge of some codebooks and randomly guessing (with the given distribution $\prod_k P_{X_k}$) the other input $x_{\mathcal{K}'}^n$ over the whole alphabets $\prod_{k \in \mathcal{K}'} \mathcal{X}_k^n$. Our result in Theorem 2 for $K = 2$ and $\mathcal{K}' = \{1,2\}$ coincides with that given by [16, Theorem 2].

B. Achievable Regions

In the following theorem we provide the new achievable region for the considered DM MAC-WT channel with both secret and open messages.

Theorem 3. *For given distribution $\prod_{k=1}^K P_{X_k} P_{Z|X_{\mathcal{K}}}$ and subset $\mathcal{K}' \subseteq \mathcal{K}$, any rate-tuple $(R_1^s, R_1^o, \cdots, R_K^s, R_K^o)$ satisfying*

$$
\begin{cases}
R_k^s = 0, \forall k \in \overline{\mathcal{K}'}, \\
\sum_{k \in \mathcal{S}} R_k^s + \sum_{k \in \mathcal{S} \setminus \mathcal{S}'} R_k^o + \sum_{k \in \mathcal{T}} R_k^o \leq [I(X_{\mathcal{S}}, X_{\mathcal{T}}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}) - I(X_{\mathcal{S}'}; Z | X_{\overline{\mathcal{K}'}})]^+, \\
\qquad\qquad\qquad \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S}' \subseteq \mathcal{S}, \mathcal{T} \subseteq \overline{\mathcal{K}'},
\end{cases}
\tag{17}
$$

is achievable, where $\overline{\mathcal{S}}$, $\overline{\mathcal{T}}$, and $\overline{\mathcal{K}'}$ are defined in (5). Let $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ denote the set of rate tuples satisfying (17). Then, the convex hull of the union of $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ over all $\prod_{k=1}^K P_{X_k}$ and $\mathcal{K}' \subseteq \mathcal{K}$ is an achievable rate region of the DM MAC-WT channel.

Proof: The proof is provided in Section IV. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad \square$

It can be found that [15, Lemma 1] is a special case of Theorem 3 with $\mathcal{K}' = \mathcal{K}$. In the following remark, we explain why Theorem 3 can improve [15, Lemma 1].

Remark 2. *The partitioning of $\mathcal{K}$ into $\mathcal{K}'$ and $\overline{\mathcal{K}'}$ is very important in determining the achievable region, where users in $\mathcal{K}'$ have zero secrecy rate. We observe that if a user has no secret message, it can play different roles and has two options: 1) introducing an additional auxiliary message such that the sum rate of its messages is beyond Eve's decoding capability; 2) simply encoding and transmitting its open message as in a standard MAC channel with no wiretapping. The achievability proof in the next section shows that both these two options have advantages and disadvantages in determining the achievable regions. Using the first option, the signal of the*

user plays as noise to Eve and can thus weaken its wiretapping capability. However, more constraints are imposed on the message rate, which is detrimental to determining the achievable region. The advantage and disadvantage of the second option are exactly the opposite, i.e., fewer constraints are imposed, but Eve has a stronger wiretapping capability. Therefore, to obtain a larger achievable region, all 2^K possible partitions $\mathcal{K} = \mathcal{K}' \cup \overline{\mathcal{K}'}$ should be taken into account. In [15], only the $\mathcal{K}' = \mathcal{K}$ case was considered. Hence, Theorem 3 improves the region in [15, Lemma 1]. ◊

Now we consider two special cases of Theorem 3 with respectively $R_k^{\mathrm{s}} = 0, \forall k \in \mathcal{K}$ and $R_k^{\mathrm{o}} = 0, \forall k \in \mathcal{K}$. First, if $R_k^{\mathrm{s}} = 0, \forall k \in \mathcal{K}$, each user has only one open message, which does not interest Eve. The system can then be seen as a normal DM-MAC channel with no wiretapping. It can be proven that in this case, the region given in Theorem 3 becomes the capacity region of the standard K-user DM-MAC channel with no Eve [35, Chapter 4]. Since the proof is easy, for brevity, we do not provide the details here.

Next, we consider the case with $R_k^{\mathrm{o}} = 0, \forall k \in \mathcal{K}$. In this case, the system reduces to the conventional DM MAC-WT channel with only secret messages. The achievable regions of such a channel have been investigated in [10], [16], [18]. In particular, [16] studied the two-user case under strong secrecy, [10] considered the K-user case with weak secrecy, and [18] strengthened the result in [10] subject to the strong secrecy measure. Though both [16] and [18] considered strong secrecy, by checking the two-user case and comparing [18, (14)] with [16, Theorem 1], it can be found that the achievable region given in [18] includes only $\mathcal{R}_1$ in [16] but not $\mathcal{R}_2$ and $\mathcal{R}_3$, indicating that there is still space for improvement of the achievable region of the general K-user MAC-WT channel. We show later that our results improve those in [10], [16], [18]. If $R_k^{\mathrm{o}} = 0, \forall k \in \mathcal{K}$, (17) becomes

$$\begin{cases} R_k^{\mathrm{s}} = 0, \forall k \in \overline{\mathcal{K}'}, \\ \sum_{k \in \mathcal{S}} R_k^{\mathrm{s}} \le [I(X_{\mathcal{S}}, X_{\mathcal{T}}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}) - I(X_{\mathcal{S}'}; Z | X_{\overline{\mathcal{K}'}})]^+, \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S}' \subseteq \mathcal{S}, \mathcal{T} \subseteq \overline{\mathcal{K}'}, \end{cases} \quad (18)$$

which can be simplified as (19) due to (6). Then, we give the following lemma.

Lemma 2. *If $R_k^{o} = 0, \forall k \in \mathcal{K}$, for each given $\mathcal{K}' \subseteq \mathcal{K}$, any rate-tuple $(R_1^{\mathrm{s}}, \cdots, R_K^{\mathrm{s}})$ satisfying*

$$\begin{cases} R_k^{\mathrm{s}} = 0, \forall k \in \overline{\mathcal{K}'}, \\ \sum_{k \in \mathcal{S}} R_k^{\mathrm{s}} \le [I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{S}}; Z | X_{\overline{\mathcal{K}'}})]^+, \forall \mathcal{S} \subseteq \mathcal{K}', \end{cases} \quad (19)$$

is achievable. Let $\mathscr{R}^s(X_{\mathcal{K}}, \mathcal{K}')$ denote the set of rate tuples satisfying (19). Then, the convex hull of the union of $\mathscr{R}^s(X_{\mathcal{K}}, \mathcal{K}')$ over all $\prod_{k=1}^{K} P_{X_k}$ and $\mathcal{K}' \subseteq \mathcal{K}$ is an achievable secrecy rate region of the DM MAC-WT channel with only secret messages. $\square$

Remark 3. *It can be seen that [16, Theorem 1] and [18, Theorem 1] are special cases of Lemma 2 by respectively setting $K = 2$ and considering only $\mathcal{K}' = \mathcal{K}$. As shown in the next section, for a given $\mathcal{K}'$, we introduce auxiliary messages, whose rates satisfy (5), and then prove the achievability of $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ by providing a coding scheme. However, (5) can only be satisfied if (3) is true. If it is not, the proof is no longer valid. As a matter of fact, this problem also exists in [16] and [18] (by respectively checking [16, (7), (20)] and [18, (11), (13)]), but was not considered, making the proof incomplete. In the next section we prove that if (3) is not true, there always exists $\mathcal{K}'' \subsetneq \mathcal{K}'$ such that (3) becomes true for the reduced set $\mathcal{K}''$ and $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ is included in $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}'')$, which can then be proved to be achievable. Therefore, this paper not only generalizes the results given by [16] and [18], but also "completes" the proofs in these works.* $\diamondsuit$

This paper studies wiretap channels. Hence, we are especially concerned about the maximum achievable sum secrecy rate of the system. In addition, apart from the secret message, each user also has an open message intended for Bob. Then, an interesting question is if all users transmit their confidential information at the maximum sum secrecy rate, what is the maximum sum rate at which they could encode their open messages. We give the answer in the following Theorem.

Theorem 4. *For the considered DM MAC-WT channel and given $\prod_{k=1}^{K} P_{X_k} P_{Z|X_{\mathcal{K}}}$, the maximum achievable sum secrecy rate $\sum_{k \in \mathcal{K}} R_k^s$ is*

$$R^s(X_{\mathcal{K}}) = \max_{\mathcal{K}' \subseteq \mathcal{K}} \left\{ [I(X_{\mathcal{K}'}; Y | X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}'}; Z | X_{\overline{\mathcal{K}'}})]^+ \right\}. \tag{20}$$

Let $\mathcal{K}'^*$ denote the subset in $\mathcal{K}$ which achieves (20) and $\overline{\mathcal{K}'^*} = \mathcal{K} \setminus \mathcal{K}'^*$. If $R^s(X_{\mathcal{K}}) > 0$ and all users transmit their confidential messages at sum rate $R^s(X_{\mathcal{K}})$, the maximum achievable sum rate at which users in $\mathcal{K}$ could send their open messages is given by[4]

$$R^o(X_{\mathcal{K}}) = I(X_{\overline{\mathcal{K}'^*}}; Y) + I(X_{\mathcal{K}'^*}; Z | X_{\overline{\mathcal{K}'^*}}). \tag{21}$$

---

[4]Here we assume $R^s(X_{\mathcal{K}}) > 0$ since otherwise we have $R_k^s = 0, \forall k \in \mathcal{K}$, i.e., the system reduces to a standard DM-MAC channel with no wiretapping.

Proof: See Appendix D. □

Theorem 4 shows that the channel can support a non-trivial additional open sum rate even if the coding scheme is designed to maximize the sum secrecy rate.

IV. ACHIEVABILITY PROOF

In this section, we prove Theorem 3. We start from a special case with $\mathcal{K}' = \phi$ and $\overline{\mathcal{K}'} = \mathcal{K}$. In this case, (17) becomes

$$
\begin{cases}
R_k^{\mathrm{s}} = 0, \forall k \in \mathcal{K}, \\
\sum_{k \in \mathcal{T}} R_k^{\mathrm{o}} \leq I(X_{\mathcal{T}}; Y | X_{\overline{\mathcal{T}}}), \forall \mathcal{T} \subseteq \mathcal{K}.
\end{cases}
\tag{22}
$$

The region $\mathscr{R}(X_{\mathcal{K}}, \phi)$ defined above is included in the capacity region of a standard DM-MAC channel with no wiretapping and its achievability proof is well known. One may refer to [35, Chapter 4] for the detailed proof.

Next, we prove the achievability of $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ for any non-empty subset $\mathcal{K}' \subseteq \mathcal{K}$. Without loss of generality (w.l.o.g.), we always assume

$$
I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}) > 0, \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi,
\tag{23}
$$

since otherwise users in $\mathcal{S}$ cannot communicate with Bob. Moreover, we assume

$$
I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{S}}; Z | X_{\overline{\mathcal{K}'}}) > 0, \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S} \neq \phi,
\tag{24}
$$

which is (3) with strict ">". If (24) can be satisfied, Theorem 1 can be applied for the achievability proof. Otherwise, we show later that the achievability could be proven by modifying the proof steps.

A. Achievability Proof When (24) Holds

In this subsection, we show that with (24), any rate-tuple inside $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ is achievable. This, together with the standard time-sharing over coding strategies, suffices to prove the achievability of $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$. If (24) can be satisfied, due to (6), we have

$$
I(X_{\mathcal{S}}, X_{\mathcal{T}}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}) - I(X_{\mathcal{S}'}; Z | X_{\overline{\mathcal{K}'}}) > 0, \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S}' \subseteq \mathcal{S}, \mathcal{T} \subseteq \overline{\mathcal{K}'}, \mathcal{S} \neq \phi.
\tag{25}
$$

Then, the rate tuples inside region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ satisfy

$$
\begin{cases}
R_k^{\mathrm{s}} = 0, \forall k \in \overline{\mathcal{K}'}, \\
\sum_{k \in \mathcal{S}} R_k^{\mathrm{s}} + \sum_{k \in \mathcal{S} \setminus \mathcal{S}'} R_k^{\mathrm{o}} + \sum_{k \in \mathcal{T}} R_k^{\mathrm{o}} < I(X_{\mathcal{S}}, X_{\mathcal{T}}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}) - I(X_{\mathcal{S}'}; Z | X_{\overline{\mathcal{K}'}}) - \epsilon, \\
\qquad\qquad\qquad\qquad \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S}' \subseteq \mathcal{S}, \mathcal{T} \subseteq \overline{\mathcal{K}'}, \mathcal{S} \cup \mathcal{T} \neq \phi,
\end{cases}
\tag{26}
$$

where ϵ is an arbitrarily small positive number. For a given rate-tuple $(R_1^{\mathrm{s}}, R_1^{\mathrm{o}}, \cdots, R_K^{\mathrm{s}}, R_K^{\mathrm{o}})$ satisfying (26), it is known from Theorem 1 that there exist $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}'$ such that

$$
\begin{cases}
R_k^{\mathrm{a}} \geq 0, \forall k \in \mathcal{K}', \\
\sum_{k \in \mathcal{S}} (R_k^{\mathrm{s}} + R_k^{\mathrm{o}} + R_k^{\mathrm{a}}) + \sum_{k \in \mathcal{T}} R_k^{\mathrm{o}} < I(X_{\mathcal{S}}, X_{\mathcal{T}}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}) - \epsilon, \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{T} \subseteq \overline{\mathcal{K}'}, \mathcal{S} \cup \mathcal{T} \neq \phi, \\
\sum_{k \in \mathcal{S}} (R_k^{\mathrm{o}} + R_k^{\mathrm{a}}) > I(X_{\mathcal{S}}; Z | X_{\overline{\mathcal{K}'}}), \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S} \neq \phi,
\end{cases} \quad (27)
$$

and $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}'$ can be found by applying Dantzig's simplex algorithm [40]. Now we provide a coding scheme and show that the metrics in Definition 1 can be satisfied.

1) Coding Scheme: Assume w.l.o.g. that $2^{nR_k^{\mathrm{s}}}$, $2^{n(R_k^{\mathrm{o}} + R_k^{\mathrm{a}})}$, $2^{nR_k^{\mathrm{a}}}, \forall k \in \mathcal{K}'$, and $2^{nR_k^{\mathrm{o}}}, \forall k \in \overline{\mathcal{K}'}$, are integers.
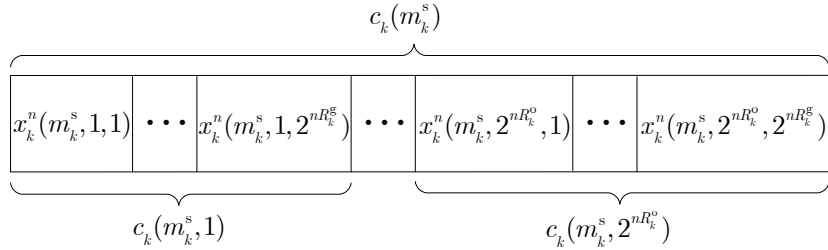

Fig. 2. A division of subcodebook $\mathcal{C}_k(m_k^{\mathrm{s}})$ of user $k \in \mathcal{K}'$.

Codebook generation. For each message pair $(m_k^{\mathrm{s}}, m_k^{\mathrm{o}}) \in \mathcal{M}_k^{\mathrm{s}} \times \mathcal{M}_k^{\mathrm{o}}$ of user $k \in \mathcal{K}'$, generate a sub-subcodebook $\mathcal{C}_k(m_k^{\mathrm{s}}, m_k^{\mathrm{o}})$ by randomly and independently generating $2^{nR_k^{\mathrm{a}}}$ sequences $x_k^n(m_k^{\mathrm{s}}, m_k^{\mathrm{o}}, m_k^{\mathrm{a}}), \forall m_k^{\mathrm{a}} \in \mathcal{M}_k^{\mathrm{a}}$, each according to $\prod_{i=1}^{n} P_{X_k}(x_{ki})$. For a given secret message m_k^{s}, the sub-subcodebooks for all open messages constitute subcodebook $\mathcal{C}_k(m_k^{\mathrm{s}})$, i.e., $\mathcal{C}_k(m_k^{\mathrm{s}}) = \bigcup_{m_k^{\mathrm{o}} \in \mathcal{M}_k^{\mathrm{o}}} \mathcal{C}_k(m_k^{\mathrm{s}}, m_k^{\mathrm{o}})$. Fig. 2 gives an example of subcodebook $\mathcal{C}_k(m_k^{\mathrm{s}})$. Then, as shown in Fig. 3, these subcodebooks constitute the codebook of user k, i.e., $\mathcal{C}_k = \bigcup_{m_k^{\mathrm{s}} \in \mathcal{M}_k^{\mathrm{s}}} \mathcal{C}_k(m_k^{\mathrm{s}})$. For each user k in $\overline{\mathcal{K}'}$, we apply the random coding scheme used in the standard MAC channel with no wiretapping. In particular, user $k \in \overline{\mathcal{K}'}$ generate its codebook $\mathcal{C}_k$ by randomly and independently generating $2^{nR_k^{\mathrm{o}}}$ sequences $x_k^n(m_k^{\mathrm{o}}), \forall m_k^{\mathrm{o}} \in \mathcal{M}_k^{\mathrm{o}}$, each according to $\prod_{i=1}^{n} P_{X_k}(x_{ki})$. The codebooks of all users are then revealed to all transmitters and receivers, including Eve.

Encoding. To send message pair $(m_k^{\mathrm{s}}, m_k^{\mathrm{o}}) \in \mathcal{M}_k^{\mathrm{s}} \times \mathcal{M}_k^{\mathrm{o}}$, encoder $k \in \mathcal{K}'$ uniformly chooses a codeword (with index m_k^{a}) from sub-subcodebook $\mathcal{C}_k(m_k^{\mathrm{s}}, m_k^{\mathrm{o}})$ and then transmits $x_k^n(m_k^{\mathrm{s}}, m_k^{\mathrm{o}}, m_k^{\mathrm{a}})$. To send message $m_k^{\mathrm{o}} \in \mathcal{M}_k^{\mathrm{o}}$, encoder $k \in \overline{\mathcal{K}'}$ transmits $x_k^n(m_k^{\mathrm{o}})$.

Fig. 3. Codebook $\mathcal{c}_k$ of user $k \in \mathcal{K}'$.

Decoding. The decoder at Bob uses joint typicality decoding to find an estimate of the messages and declares that $(\hat{m}^{\mathrm{s}}_{\mathcal{K}'}, \hat{m}^{\mathrm{o}}_{\mathcal{K}'}, \hat{m}^{\mathrm{o}}_{\overline{\mathcal{K}'}})$ is sent if there exists $\hat{m}^{\mathrm{a}}_{\mathcal{K}'} \in \prod_{k \in \mathcal{K}'} \mathcal{M}^{\mathrm{a}}_k$ such that $(\hat{m}^{\mathrm{s}}_{\mathcal{K}'}, \hat{m}^{\mathrm{o}}_{\mathcal{K}'}, \hat{m}^{\mathrm{a}}_{\mathcal{K}'}, \hat{m}^{\mathrm{o}}_{\overline{\mathcal{K}'}})$ is the unique message-tuple satisfying $(\{x^n_k(\hat{m}^{\mathrm{s}}_k, \hat{m}^{\mathrm{o}}_k, \hat{m}^{\mathrm{a}}_k)\}_{k \in \mathcal{K}'}, \{x^n_k(\hat{m}^{\mathrm{o}}_k)\}_{k \in \overline{\mathcal{K}'}}, y^n) \in \mathcal{T}^{(n)}_{\epsilon}(X_{\mathcal{K}}, Y)$.

2) Analysis of the Probability of Error: Since users in $\mathcal{K}'$ and $\overline{\mathcal{K}'}$ respectively transmit their messages at rate $R_k = R^{\mathrm{s}}_k + R^{\mathrm{o}}_k + R^{\mathrm{a}}_k$ and $R_k = R^{\mathrm{o}}_k$, and (see (27))

$$\sum_{k \in \mathcal{S}}(R^{\mathrm{s}}_k + R^{\mathrm{o}}_k + R^{\mathrm{a}}_k) + \sum_{k \in \mathcal{T}} R^{\mathrm{o}}_k < I(X_{\mathcal{S}}, X_{\mathcal{T}}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}) - \epsilon, \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{T} \subseteq \overline{\mathcal{K}'}, \mathcal{S} \cup \mathcal{T} \neq \phi, \quad (28)$$

the rate-tuple $(R_1, \cdots, R_K)$ is inside the capacity region of the MAC channel from all users to Bob. Then, it can be proven by using the law of large numbers (LLN) and the packing lemma that the average probability of error at Bob vanishes as n goes to infinity, i.e.,

$$\lim_{n \to \infty} \Pr\left\{\left(\hat{M}^{\mathrm{s}}_{\mathcal{K}}, \hat{M}^{\mathrm{o}}_{\mathcal{K}}, \hat{M}^{\mathrm{a}}_{\mathcal{K}}\right) \neq (M^{\mathrm{s}}_{\mathcal{K}}, M^{\mathrm{o}}_{\mathcal{K}}, M^{\mathrm{a}}_{\mathcal{K}})\right\} = 0, \quad (29)$$

Note that for notational convenience, in (29), every user has M^{s}_k, M^{o}_k, and M^{a}_k. For users in $\overline{\mathcal{K}'}$, which have only open messages, M^{s}_k and M^{a}_k are actually constants and do not affect the value of the probability term in (29). The proof of (29) follows exactly the same steps used in [35, Subsection 4.5.1] and is omitted here. Since

$$\Pr\left\{\left(\hat{M}^{\mathrm{s}}_{\mathcal{K}}, \hat{M}^{\mathrm{o}}_{\mathcal{K}}, \hat{M}^{\mathrm{a}}_{\mathcal{K}}\right) \neq (M^{\mathrm{s}}_{\mathcal{K}}, M^{\mathrm{o}}_{\mathcal{K}}, M^{\mathrm{a}}_{\mathcal{K}})\right\} = \Pr\left\{\left(\hat{M}^{\mathrm{s}}_{\mathcal{K}}, \hat{M}^{\mathrm{o}}_{\mathcal{K}}\right) \neq (M^{\mathrm{s}}_{\mathcal{K}}, M^{\mathrm{o}}_{\mathcal{K}}) \text{ or } \hat{M}^{\mathrm{a}}_{\mathcal{K}} \neq M^{\mathrm{a}}_{\mathcal{K}}\right\}$$

$$\geq \Pr\left\{\left(\hat{M}^{\mathrm{s}}_{\mathcal{K}}, \hat{M}^{\mathrm{o}}_{\mathcal{K}}\right) \neq (M^{\mathrm{s}}_{\mathcal{K}}, M^{\mathrm{o}}_{\mathcal{K}})\right\}, \quad (30)$$

we know that (1) is true.

3) Analysis of the Information Leakage: Define the following total variational distance

$$d(\mathcal{C}_{\mathcal{K}}, m^{\mathrm{s}}_{\mathcal{K}'}, m^{\mathrm{o}}_{\overline{\mathcal{K}'}}) = \left\| P_{Z^n}\left(\cdot | \mathcal{C}_{\mathcal{K}'}, \{\mathcal{C}_k(m^{\mathrm{o}}_k)\}_{k\in\overline{\mathcal{K}'}}\right) - P_{Z^n}\left(\cdot | \{\mathcal{C}_k(m^{\mathrm{s}}_k)\}_{k\in\mathcal{K}'}, \{\mathcal{C}_k(m^{\mathrm{o}}_k)\}_{k\in\overline{\mathcal{K}'}}\right) \right\|_1. \quad (31)$$

As shown below, we can get an upper bound on the expectation of $d(\mathcal{C}_{\mathcal{K}}, m^{\mathrm{s}}_{\mathcal{K}'}, m^{\mathrm{o}}_{\overline{\mathcal{K}'}})$

$$\mathbb{E}\left[d(\mathcal{C}_{\mathcal{K}}, m^{\mathrm{s}}_{\mathcal{K}'}, m^{\mathrm{o}}_{\overline{\mathcal{K}'}})\right] \leq \mathbb{E}\left\| P_{Z^n}\left(\cdot | \mathcal{C}_{\mathcal{K}'}, \{\mathcal{C}_k(m^{\mathrm{o}}_k)\}_{k\in\overline{\mathcal{K}'}}\right) - P_{Z^n}\left(\cdot | \{\mathcal{C}_k(m^{\mathrm{o}}_k)\}_{k\in\overline{\mathcal{K}'}}\right)\right\|_1$$

$$+ \mathbb{E}\left\| P_{Z^n}\left(\cdot | \{\mathcal{C}_k(m^{\mathrm{s}}_k)\}_{k\in\mathcal{K}'}, \{\mathcal{C}_k(m^{\mathrm{o}}_k)\}_{k\in\overline{\mathcal{K}'}}\right) - P_{Z^n}\left(\cdot | \{\mathcal{C}_k(m^{\mathrm{o}}_k)\}_{k\in\overline{\mathcal{K}'}}\right)\right\|_1$$

$$\leq 2^{-n\sum_{k\in\mathcal{K}'} R^{\mathrm{s}}_k} \sum_{m^{\mathrm{s}}_{\mathcal{K}'}\in\prod_{k\in\mathcal{K}'}\mathcal{M}^{\mathrm{s}}_k} \mathbb{E}\left\| P_{Z^n}\left(\cdot | \{\mathcal{C}_k(m^{\mathrm{s}}_k)\}_{k\in\mathcal{K}'}, \{\mathcal{C}_k(m^{\mathrm{o}}_k)\}_{k\in\overline{\mathcal{K}'}}\right) - P_{Z^n}\left(\cdot | \{\mathcal{C}_k(m^{\mathrm{o}}_k)\}_{k\in\overline{\mathcal{K}'}}\right)\right\|_1$$

$$+ \mathbb{E}\left\| P_{Z^n}\left(\cdot | \{\mathcal{C}_k(m^{\mathrm{s}}_k)\}_{k\in\mathcal{K}'}, \{\mathcal{C}_k(m^{\mathrm{o}}_k)\}_{k\in\overline{\mathcal{K}'}}\right) - P_{Z^n}\left(\cdot | \{\mathcal{C}_k(m^{\mathrm{o}}_k)\}_{k\in\overline{\mathcal{K}'}}\right)\right\|_1, \quad (32)$$

where the expectations are taken over the random codebooks, the first step follows from first introducing $P_{Z^n}\left(\cdot | \{\mathcal{C}_k(m^{\mathrm{o}}_k)\}_{k\in\overline{\mathcal{K}'}}\right)$ and then applying the triangular inequality, and the second step holds by computing $P_{Z^n}\left(\cdot | \mathcal{C}_{\mathcal{K}'}, \{\mathcal{C}_k(m^{\mathrm{o}}_k)\}_{k\in\overline{\mathcal{K}'}}\right)$ over all possible $m^{\mathrm{s}}_{\mathcal{K}'}$ and also applying the triangular inequality. In addition, it is known from the coding scheme provided above that there are respectively $2^{n(R^{\mathrm{a}}_k + R^{\mathrm{o}}_k)}$ codewords in $\mathcal{C}_k(m^{\mathrm{s}}_k), \forall k \in \mathcal{K}'$ and one codeword in $\mathcal{C}_k(m^{\mathrm{o}}_k), \forall k \in \overline{\mathcal{K}'}$. Letting $Q_k = \log|\mathcal{C}_k(m^{\mathrm{o}}_k)| = 0, \forall k \in \overline{\mathcal{K}'}$ and $Q_k = \log|\mathcal{C}_k(m^{\mathrm{s}}_k)| = R^{\mathrm{o}}_k + R^{\mathrm{a}}_k, \forall k \in \mathcal{K}'$, since $\sum_{k\in\mathcal{S}}(R^{\mathrm{o}}_k + R^{\mathrm{a}}_k) > I(X_{\mathcal{S}}; Z | X_{\overline{\mathcal{K}'}}), \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S} \neq \phi$ (see (27)), we know that (14) can be satisfied. Theorem 2 can then be applied and yields

$$\mathbb{E}\left\| P_{Z^n}\left(\cdot | \{\mathcal{C}_k(m^{\mathrm{s}}_k)\}_{k\in\mathcal{K}'}, \{\mathcal{C}_k(m^{\mathrm{o}}_k)\}_{k\in\overline{\mathcal{K}'}}\right) - P_{Z^n}\left(\cdot | \{\mathcal{C}_k(m^{\mathrm{o}}_k)\}_{k\in\overline{\mathcal{K}'}}\right)\right\|_1$$

$$\leq e^{-n\varepsilon}, \forall m^{\mathrm{s}}_{\mathcal{K}'} \in \prod_{k\in\mathcal{K}'} \mathcal{M}^{\mathrm{s}}_k. \quad (33)$$

Based on (33), (32) can be further upper bounded as follows

$$\mathbb{E}\left[d(\mathcal{C}_{\mathcal{K}}, m^{\mathrm{s}}_{\mathcal{K}'}, m^{\mathrm{o}}_{\overline{\mathcal{K}'}})\right] \leq 2e^{-n\varepsilon} \to 0. \quad (34)$$

Now we evaluate the information leakage over all codebooks as follows

$$I\left(M_{\mathcal{K}'}^{\mathrm{s}}; Z^n | M_{\overline{\mathcal{K}'}}^{\mathrm{o}}, \mathcal{C}_{\mathcal{K}}\right) = H\left(Z^n | M_{\overline{\mathcal{K}'}}^{\mathrm{o}}, \mathcal{C}_{\mathcal{K}}\right) - H\left(Z^n | M_{\mathcal{K}'}^{\mathrm{s}}, M_{\overline{\mathcal{K}'}}^{\mathrm{o}}, \mathcal{C}_{\mathcal{K}}\right)$$

$$= H\left(Z^n | \mathcal{C}_{\mathcal{K}'}, \{\mathcal{C}_k(M_k^{\mathrm{o}})\}_{k \in \overline{\mathcal{K}'}}\right) - H\left(Z^n | \{\mathcal{C}_k(M_k^{\mathrm{s}})\}_{k \in \mathcal{K}'}, \{\mathcal{C}_k(M_k^{\mathrm{o}})\}_{k \in \overline{\mathcal{K}'}}\right)$$

$$\overset{(a)}{\leq} 2^{-n\left(\sum_{k \in \mathcal{K}'} R_k^{\mathrm{s}} + \sum_{k \in \overline{\mathcal{K}'}} R_k^{\mathrm{o}}\right)} \sum_{\substack{m_{\mathcal{K}'}^{\mathrm{s}} \in \prod_{k \in \mathcal{K}'} \mathcal{M}_k^{\mathrm{s}}, \\ m_{\overline{\mathcal{K}'}}^{\mathrm{o}} \in \prod_{k \in \overline{\mathcal{K}'}} \mathcal{M}_k^{\mathrm{o}}}} \Big| H\left(Z^n | \mathcal{C}_{\mathcal{K}'}, \{\mathcal{C}_k(m_k^{\mathrm{o}})\}_{k \in \overline{\mathcal{K}'}}\right)$$

$$- H\left(Z^n | \{\mathcal{C}_k(m_k^{\mathrm{s}})\}_{k \in \mathcal{K}'}, \{\mathcal{C}_k(m_k^{\mathrm{o}})\}_{k \in \overline{\mathcal{K}'}}\right) \Big|$$

$$\overset{(b)}{\leq} 2^{-n\left(\sum_{k \in \mathcal{K}'} R_k^{\mathrm{s}} + \sum_{k \in \overline{\mathcal{K}'}} R_k^{\mathrm{o}}\right)} \sum_{\substack{m_{\mathcal{K}'}^{\mathrm{s}} \in \prod_{k \in \mathcal{K}'} \mathcal{M}_k^{\mathrm{s}}, \\ m_{\overline{\mathcal{K}'}}^{\mathrm{o}} \in \prod_{k \in \overline{\mathcal{K}'}} \mathcal{M}_k^{\mathrm{o}}}} \mathbb{E}\left[d(\mathcal{C}_{\mathcal{K}}, m_{\mathcal{K}'}^{\mathrm{s}}, m_{\overline{\mathcal{K}'}}^{\mathrm{o}}) \ln \frac{|\mathcal{Z}|^n}{d(\mathcal{C}_{\mathcal{K}}, m_{\mathcal{K}'}^{\mathrm{s}}, m_{\overline{\mathcal{K}'}}^{\mathrm{o}})}\right]$$

$$\overset{(c)}{\leq} 2^{-n\left(\sum_{k \in \mathcal{K}'} R_k^{\mathrm{s}} + \sum_{k \in \overline{\mathcal{K}'}} R_k^{\mathrm{o}}\right)} \sum_{\substack{m_{\mathcal{K}'}^{\mathrm{s}} \in \prod_{k \in \mathcal{K}'} \mathcal{M}_k^{\mathrm{s}}, \\ m_{\overline{\mathcal{K}'}}^{\mathrm{o}} \in \prod_{k \in \overline{\mathcal{K}'}} \mathcal{M}_k^{\mathrm{o}}}} \mathbb{E}\left[d(\mathcal{C}_{\mathcal{K}}, m_{\mathcal{K}'}^{\mathrm{s}}, m_{\overline{\mathcal{K}'}}^{\mathrm{o}})\right] \ln \frac{|\mathcal{Z}|^n}{\mathbb{E}\left[d(\mathcal{C}_{\mathcal{K}}, m_{\mathcal{K}'}^{\mathrm{s}}, m_{\overline{\mathcal{K}'}}^{\mathrm{o}})\right]}$$

$$\leq 2e^{-n\varepsilon}\left(n \ln |\mathcal{Z}| + n\varepsilon - \ln 2\right) \to 0, \tag{35}$$

where (35a), (35b), and (35c) follow by respectively applying the triangular inequality, [45, Lemma 2.7], and Jensen's inequality, and the last step is obtained by using (34) and the fact that $u \ln \frac{|\mathcal{Z}|^n}{u}$ is an increasing function of u in $(0, \frac{|\mathcal{Z}|^n}{e}]$ and $0 < 2e^{-n\varepsilon} < \frac{1}{e} \leq \frac{|\mathcal{Z}|^n}{e}$ (as n goes to infinity). Using the chain rule and non-negativity of mutual information,

$$I\left(M_{\mathcal{K}'}^{\mathrm{s}}; Z^n | M_{\overline{\mathcal{K}'}}^{\mathrm{o}}, \mathcal{C}_{\mathcal{K}}\right) = I\left(M_{\mathcal{K}'}^{\mathrm{s}}; Z^n, \mathcal{C}_{\mathcal{K}} | M_{\overline{\mathcal{K}'}}^{\mathrm{o}}\right) - I\left(M_{\mathcal{K}'}^{\mathrm{s}}; \mathcal{C}_{\mathcal{K}} | M_{\overline{\mathcal{K}'}}^{\mathrm{o}}\right)$$

$$\overset{(a)}{=} I\left(M_{\mathcal{K}'}^{\mathrm{s}}; Z^n, \mathcal{C}_{\mathcal{K}} | M_{\overline{\mathcal{K}'}}^{\mathrm{o}}\right)$$

$$= I\left(M_{\mathcal{K}'}^{\mathrm{s}}; Z^n | M_{\overline{\mathcal{K}'}}^{\mathrm{o}}\right) + I\left(M_{\mathcal{K}'}^{\mathrm{s}}; \mathcal{C}_{\mathcal{K}} | Z^n, M_{\overline{\mathcal{K}'}}^{\mathrm{o}}\right)$$

$$\geq I\left(M_{\mathcal{K}'}^{\mathrm{s}}; Z^n | M_{\overline{\mathcal{K}'}}^{\mathrm{o}}\right), \tag{36}$$

where (36a) holds since the choices of random messages at different users are independent of each other and also independent of the choices of random codebooks, resulting in $I\left(M_{\mathcal{K}'}^{\mathrm{s}}; \mathcal{C}_{\mathcal{K}} | M_{\overline{\mathcal{K}'}}^{\mathrm{o}}\right) = 0$. It is known from (35) and (36) that

$$\lim_{n \to \infty} I\left(M_{\mathcal{K}'}^{\mathrm{s}}; Z^n | M_{\overline{\mathcal{K}'}}^{\mathrm{o}}\right) = 0. \tag{37}$$

Since $R_k^{\mathrm{s}} = 0, \forall k \in \overline{\mathcal{K}'}$ and the messages of different users are independent, we have

$$I\left(M_{\mathcal{K}'}^{\mathrm{s}}; Z^n | M_{\overline{\mathcal{K}'}}^{\mathrm{o}}\right) \geq I\left(M_{\mathcal{K}'}^{\mathrm{s}}; Z^n\right)$$

$$= I\left(M_{\mathcal{K}}^{\mathrm{s}}; Z^n\right). \tag{38}$$

Then, it is known that (2) is true.

B. Achievability Proof When (24) does not Hold

For a given $\mathcal{K}' \subseteq \mathcal{K}$, if (24) cannot be satisfied, then, there exists at least one non-empty set $\mathcal{S} \subseteq \mathcal{K}'$ such that

$$I(X_\mathcal{S}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) - I(X_\mathcal{S}; Z | X_{\overline{\mathcal{K}'}}) \leq 0. \tag{39}$$

With (39), there are two possible cases, i.e.,

$$I(X_{\mathcal{K}'}; Y | X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}'}; Z | X_{\overline{\mathcal{K}'}}) \leq 0, \tag{40}$$

and

$$I(X_{\mathcal{K}'}; Y | X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}'}; Z | X_{\overline{\mathcal{K}'}}) > 0. \tag{41}$$

In the following, we prove the achievability of $\mathscr{R}(X_\mathcal{K}, \mathcal{K}')$ when either (40) or (41) holds.

In the first case, i.e., when (40) holds, by setting $\mathcal{S} = \mathcal{K}'$, $\mathcal{S}' = \mathcal{S} = \mathcal{K}'$ and $\mathcal{T} = \phi$ in (17), we get

$$\sum_{k \in \mathcal{K}'} R_k^{\mathrm{s}} \leq [I(X_{\mathcal{K}'}; Y | X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}'}; Z | X_{\overline{\mathcal{K}'}})]^+ = 0. \tag{42}$$

Hence, $R_k^{\mathrm{s}} = 0, \forall k \in \mathcal{K}'$. Considering that $R_k^{\mathrm{s}} = 0, \forall k \in \overline{\mathcal{K}'}$ in (17), we have $R_k^{\mathrm{s}} = 0, \forall k \in \mathcal{K}$. Then, in this case, (17) becomes

$$\begin{cases} R_k^{\mathrm{s}} = 0, \forall k \in \mathcal{K}, \\ \sum_{k \in \mathcal{S} \backslash \mathcal{S}'} R_k^{\mathrm{o}} + \sum_{k \in \mathcal{T}} R_k^{\mathrm{o}} \leq [I(X_\mathcal{S}, X_\mathcal{T}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}) - I(X_{\mathcal{S}'}; Z | X_{\overline{\mathcal{K}'}})]^+, \\ \qquad\qquad \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S}' \subseteq \mathcal{S}, \mathcal{T} \subseteq \overline{\mathcal{K}'}, \end{cases} \tag{43}$$

which is included in

$$\begin{cases} R_k^{\mathrm{s}} = 0, \forall k \in \mathcal{K}, \\ \sum_{k \in \mathcal{S}} R_k^{\mathrm{o}} + \sum_{k \in \mathcal{T}} R_k^{\mathrm{o}} \leq I(X_\mathcal{S}, X_\mathcal{T}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}), \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{T} \subseteq \overline{\mathcal{K}'}, \end{cases} \tag{44}$$

since (44) consists of only partial inequalities in (43) (those with $\mathcal{S}' = \phi$). Note that (44) can be seen as the capacity region of a standard DM-MAC channel $P_{Y|X_\mathcal{K}}$ with no wiretapping and K users, each transmitting at rate R_k^{o}. Hence, the achievability of (43) is obvious.

In the second case, i.e., when (41) holds, due to (39), there must exist at least one subset $\mathcal{K}_0 \subsetneq \mathcal{K}'$ such that

$$I(X_{\mathcal{K}_0}; Y | X_{\mathcal{K}' \backslash \mathcal{K}_0}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}_0}; Z | X_{\overline{\mathcal{K}'}}) \leq 0, \tag{45}$$

and

$$I(X_{\mathcal{K}_0 \cup \mathcal{V}}; Y | X_{\mathcal{K}' \setminus (\mathcal{K}_0 \cup \mathcal{V})}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}_0 \cup \mathcal{V}}; Z | X_{\overline{\mathcal{K}'}}) > 0, \forall \mathcal{V} \subseteq \mathcal{K}' \setminus \mathcal{K}_0, \mathcal{V} \neq \phi. \qquad (46)$$

The inequalities (45) and (46) indicate that $\mathcal{K}_0$ is the largest set in $\mathcal{K}'$ which includes all users in $\mathcal{K}_0$ and ensures (45). Adding any other users in $\mathcal{K}' \setminus \mathcal{K}_0$ to $\mathcal{K}_0$ results in (46). Note that if there are multiple subsets in $\mathcal{K}'$ making (45) and (46) hold, we let $\mathcal{K}_0$ be any of them. Let

$$\begin{aligned} \mathcal{K}'' &= \mathcal{K}' \setminus \mathcal{K}_0 \\ &= \mathcal{K} \setminus (\overline{\mathcal{K}'} \cup \mathcal{K}_0), \\ \overline{\mathcal{K}''} &= \mathcal{K} \setminus \mathcal{K}'' \\ &= \overline{\mathcal{K}'} \cup \mathcal{K}_0. \end{aligned} \qquad (47)$$

Then, we give the following theorem.

Theorem 5. *With $\mathcal{K}_0$, $\mathcal{K}''$, and $\overline{\mathcal{K}''}$ defined above, we have*

$$I(X_{\mathcal{V}}; Y | X_{\overline{\mathcal{V}}}, X_{\overline{\mathcal{K}''}}) - I(X_{\mathcal{V}}; Z | X_{\overline{\mathcal{K}''}}) > 0, \forall \mathcal{V} \subseteq \mathcal{K}'', \mathcal{V} \neq \phi, \qquad (48)$$

where $\overline{\mathcal{V}} = \mathcal{K}'' \setminus \mathcal{V}$. In addition, if a rate-tuple $(R_1^s, R_1^o, \cdots, R_K^s, R_K^o)$ is in region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ defined by Theorem 3 and has (45) as well as (46) met, then, it is also in region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}'')$, i.e., it satisfies

$$\begin{cases} R_k^s = 0, \forall k \in \overline{\mathcal{K}''}, \\ \sum_{k \in \mathcal{V}} R_k^s + \sum_{k \in \mathcal{V} \setminus \mathcal{V}'} R_k^o + \sum_{k \in \mathcal{W}} R_k^o \leq I(X_{\mathcal{V}}, X_{\mathcal{W}}; Y | X_{\overline{\mathcal{V}}}, X_{\overline{\mathcal{W}}}) - I(X_{\mathcal{V}'}; Z | X_{\overline{\mathcal{K}''}}), \\ \qquad\qquad\qquad \forall \mathcal{V} \subseteq \mathcal{K}'', \mathcal{V}' \subseteq \mathcal{V}, \mathcal{W} \subseteq \overline{\mathcal{K}''}, \end{cases} \qquad (49)$$

where $\overline{\mathcal{W}} = \overline{\mathcal{K}''} \setminus \mathcal{W}$.

    Proof: See Appendix E. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

It can be similarly proven as (7) that (48) is equivalent to

$$I(X_{\mathcal{V}}, X_{\mathcal{W}}; Y | X_{\overline{\mathcal{V}}}, X_{\overline{\mathcal{W}}}) - I(X_{\mathcal{V}'}; Z | X_{\overline{\mathcal{K}''}}) > 0, \forall \mathcal{V} \subseteq \mathcal{K}'', \mathcal{V}' \subseteq \mathcal{V}, \mathcal{W} \subseteq \overline{\mathcal{K}''}, \mathcal{V} \cup \mathcal{W} \neq \phi. \quad (50)$$

$[\cdot]^+$ in (49) can thus be omitted. Note that to make it easier to read and explain, instead of $\mathcal{S}$ and $\mathcal{T}$, we use new notations $\mathcal{V}$ and $\mathcal{W}$ in Theorem 5 and Appendix E to respectively denote subsets in $\mathcal{K}''$ and $\overline{\mathcal{K}''}$.

Theorem 5 shows that if a rate-tuple $(R_1^s, R_1^o, \cdots, R_K^s, R_K^o)$ is in region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ and has (45) as well as (46) met, it is also in region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}'')$ and satisfies (50). Then, its achievability

is immediately clear if we could prove that with (50), any rate-tuple in $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}'')$ is achievable. Interestingly, this can be realized by using similar techniques provided in the previous subsection.

V. TWO-USER BINARY ADDER CHANNEL

In this section, we consider a two-user binary adder channel and show that the achievable region proposed in Theorem 3 can strictly improve that provided in [15, Theorem 1].

A. Two-User DM MAC-WT Channel

When $K = 2$, by respectively letting $\mathcal{K}'$ in (17) be $\{1, 2\}$, $\{1\}$, $\{2\}$, and ϕ, we obtain the following four regions

$$
\mathscr{R}(X_{\mathcal{K}}, \{1, 2\})
\begin{cases}
R_1^{\mathrm{s}} + R_1^{\mathrm{o}} \leq I(X_1; Y | X_2) \\
R_2^{\mathrm{s}} + R_2^{\mathrm{o}} \leq I(X_2; Y | X_1) \\
R_1^{\mathrm{s}} + R_1^{\mathrm{o}} + R_2^{\mathrm{s}} + R_2^{\mathrm{o}} \leq I(X_1, X_2; Y) \\
R_1^{\mathrm{s}} \leq [I(X_1; Y | X_2) - I(X_1; Z)]^+ \\
R_2^{\mathrm{s}} \leq [I(X_2; Y | X_1) - I(X_2; Z)]^+ \\
R_1^{\mathrm{s}} + R_2^{\mathrm{s}} \leq [I(X_1, X_2; Y) - I(X_1, X_2; Z)]^+ \\
R_1^{\mathrm{s}} + R_1^{\mathrm{o}} + R_2^{\mathrm{s}} \leq [I(X_1, X_2; Y) - I(X_2; Z)]^+ \\
R_1^{\mathrm{s}} + R_2^{\mathrm{s}} + R_2^{\mathrm{o}} \leq [I(X_1, X_2; Y) - I(X_1; Z)]^+
\end{cases}
, \tag{51}
$$

$$
\mathscr{R}(X_{\mathcal{K}}, \{1\})
\begin{cases}
R_2^{\mathrm{s}} = 0 \\
R_1^{\mathrm{s}} + R_1^{\mathrm{o}} \leq I(X_1; Y | X_2) \\
R_2^{\mathrm{o}} \leq I(X_2; Y | X_1) \\
R_1^{\mathrm{s}} + R_1^{\mathrm{o}} + R_2^{\mathrm{o}} \leq I(X_1, X_2; Y) \\
R_1^{\mathrm{s}} \leq [I(X_1; Y | X_2) - I(X_1; Z | X_2)]^+ \\
R_1^{\mathrm{s}} + R_2^{\mathrm{o}} \leq [I(X_1, X_2; Y) - I(X_1; Z | X_2)]^+
\end{cases}
, \tag{52}
$$

$$
\mathscr{R}(X_{\mathcal{K}}, \{2\})
\begin{cases}
R_1^{\mathrm{s}} = 0 \\
R_1^{\mathrm{o}} \leq I(X_1; Y | X_2) \\
R_2^{\mathrm{s}} + R_2^{\mathrm{o}} \leq I(X_2; Y | X_1) \\
R_1^{\mathrm{o}} + R_2^{\mathrm{s}} + R_2^{\mathrm{o}} \leq I(X_1, X_2; Y) \\
R_2^{\mathrm{s}} \leq [I(X_2; Y | X_1) - I(X_2; Z | X_1)]^+ \\
R_1^{\mathrm{o}} + R_2^{\mathrm{s}} \leq [I(X_1, X_2; Y) - I(X_2; Z | X_1)]^+
\end{cases}
, \tag{53}
$$

$$\mathscr{R}(X_{\mathcal{K}}, \{\phi\}) \begin{cases} R_1^s = 0 \\ R_2^s = 0 \\ R_1^o \leq I(X_1; Y|X_2) \\ R_2^o \leq I(X_2; Y|X_1) \\ R_1^o + R_2^o \leq I(X_1, X_2; Y) \end{cases} . \tag{54}$$

For convenience, we denote the following convex hulls

$$\mathscr{R}_{\text{new}} = \text{Conv} \bigcup_{P_{X_1} P_{X_2}} \mathscr{R}(X_{\mathcal{K}}, \{1,2\}) \cup \mathscr{R}(X_{\mathcal{K}}, \{1\}) \cup \mathscr{R}(X_{\mathcal{K}}, \{2\}) \cup \mathscr{R}(X_{\mathcal{K}}, \phi),$$

$$\mathscr{R}_{\text{old}} = \mathscr{R}_{\text{new}}^{\{1,2\}} = \text{Conv} \bigcup_{P_{X_1} P_{X_2}} \mathscr{R}(X_{\mathcal{K}}, \{1,2\}),$$

$$\mathscr{R}_{\text{new}}^{\{1\}} = \text{Conv} \bigcup_{P_{X_1} P_{X_2}} \mathscr{R}(X_{\mathcal{K}}, \{1\}). \tag{55}$$

It has been proven in [15, Theorem 1] that $\mathscr{R}_{\text{old}}$ is an achievable rate region of the two-user DM MAC-WT channel. In Theorem 3 of this paper, we further propose a new achievable region $\mathscr{R}_{\text{new}}$. In the following we prove that $\mathscr{R}_{\text{new}}$ can strictly improve $\mathscr{R}_{\text{old}}$. Noticing that $\mathscr{R}_{\text{old}}$ and $\mathscr{R}_{\text{new}}^{\{1\}}$ are both partial of $\mathscr{R}_{\text{new}}$, it is sufficient to prove the improvement if we could show that $\mathscr{R}_{\text{new}}^{\{1\}}$ contains achievable points that are not contained in $\mathscr{R}_{\text{old}}$. We show below that this is possible.

Note that (51) and (52) respectively define a four-dimensional space for $(R_1^s, R_1^o, R_2^s, R_2^o)$ and a three-dimensional space for (R_1^s, R_1^o, R_2^o). For ease of explanation and to make the following results easier to plot and understand, we let $R_1^o = R_2^s = 0$ in (51) and $R_1^o = 0$ in (52), and obtain two two-dimensional spaces for (R_1^s, R_2^o). In particular, if $R_1^o = R_2^s = 0$, it can be easily checked that the 1st, 3rd, 5th, and 7th inequalities in (51) are redundant. By removing them, (51) reduces to

$$\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1,2\}) \begin{cases} R_1^s \leq \min\{[I(X_1; Y|X_2) - I(X_1; Z)]^+, [I(X_1, X_2; Y) - I(X_1, X_2; Z)]^+\} \\ R_2^o \leq I(X_2; Y|X_1) \\ R_1^s + R_2^o \leq [I(X_1, X_2; Y) - I(X_1; Z)]^+ \end{cases} . \tag{56}$$

If $R_1^o = 0$, by removing the redundant inequalities, (52) reduces to

$$\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1\}) \begin{cases} R_1^s \leq [I(X_1; Y|X_2) - I(X_1; Z|X_2)]^+ \\ R_2^o \leq I(X_2; Y|X_1) \\ R_1^s + R_2^o \leq [I(X_1, X_2; Y) - I(X_1; Z|X_2)]^+ \end{cases} . \tag{57}$$

Denote the convex hulls of the union of $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1,2\})$ and $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1\})$ over all $P_{X_1} P_{X_2}$ by

$$\hat{\mathscr{R}}_{\text{old}} = \hat{\mathscr{R}}_{\text{new}}^{\{1,2\}} = \text{Conv} \bigcup_{P_{X_1} P_{X_2}} \hat{\mathscr{R}}(X_{\mathcal{K}}, \{1,2\}),$$

$$\hat{\mathscr{R}}_{\text{new}}^{\{1\}} = \text{Conv} \bigcup_{P_{X_1} P_{X_2}} \hat{\mathscr{R}}(X_{\mathcal{K}}, \{1\}). \tag{58}$$

Note that $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1,2\})$ is the orthogonal projection of $\mathscr{R}(X_{\mathcal{K}}, \{1,2\})$ onto the hyperplane $R_1^{\text{o}} = R_2^{\text{s}} = 0$. The convex hulls of them over all $P_{X_1} P_{X_2}$, i.e., $\hat{\mathscr{R}}_{\text{old}}$ and $\mathscr{R}_{\text{old}}$, thus contain the same achievable set about $(R_1^{\text{s}}, R_2^{\text{o}})$. This ensures that if a rate tuple $(R_1^{\text{s}}, R_1^{\text{o}}, R_2^{\text{s}}, R_2^{\text{o}})$ is in $\mathscr{R}_{\text{old}}$, then, $(R_1^{\text{s}}, R_2^{\text{o}})$ is in $\hat{\mathscr{R}}_{\text{old}}$. Reversely, if $(R_1^{\text{s}}, R_2^{\text{o}})$ is in $\hat{\mathscr{R}}_{\text{old}}$, then, there must exist $(R_1^{\text{o}}, R_2^{\text{s}})$ such that $(R_1^{\text{s}}, R_1^{\text{o}}, R_2^{\text{s}}, R_2^{\text{o}})$ is in $\mathscr{R}_{\text{old}}$. Similarly, we know that $\hat{\mathscr{R}}_{\text{new}}^{\{1\}}$ and $\mathscr{R}_{\text{new}}^{\{1\}}$ contain the same achievable set about $(R_1^{\text{s}}, R_2^{\text{o}})$. It is thus sufficient to prove that $\mathscr{R}_{\text{new}}$ can strictly improve $\mathscr{R}_{\text{old}}$ by showing that $\hat{\mathscr{R}}_{\text{new}}^{\{1\}}$ contains achievable $(R_1^{\text{s}}, R_2^{\text{o}})$ that are not contained in $\hat{\mathscr{R}}_{\text{old}}$.

B. Two-User Binary Adder Channel
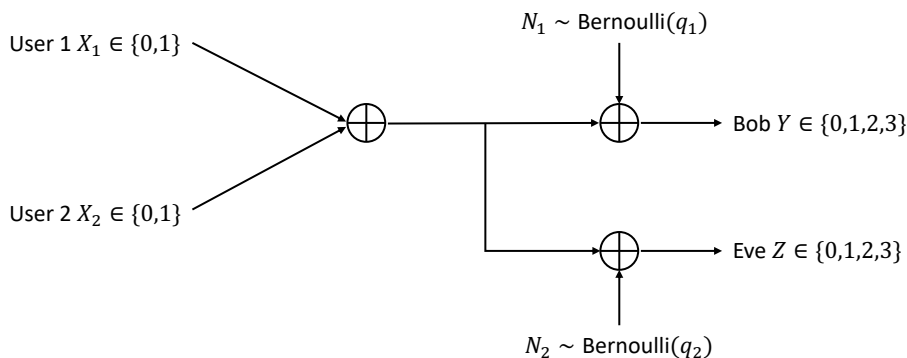
Fig. 4. Illustration of a two-user binary adder channel.

To make the upper bounds in (56) and (57) computable and comparable, as shown in Fig. 4, we consider a two-user binary adder channel in this subsection. The channel has binary inputs $X_1 \sim \{0,1\}$ and $X_2 \sim \{0,1\}$, and binary additive noise $N_1 \sim \text{Bernoulli}(q_1)$ and $N_2 \sim \text{Bernoulli}(q_2)$. X_1 and X_2 take the value 1 with probabilities α and β, respectively, and the value 0 with probabilities $1 - \alpha$ and $1 - \beta$. The received signals at Bob and Eve are given by

$$Y = X_1 + X_2 + N_1,$$

$$Z = X_1 + X_2 + N_2, \tag{59}$$

where Y and Z are both quaternary outputs that take values in the alphabet $\{0, 1, 2, 3\}$.

Now we compute the upper bounds in (56) and (57). First, based on (59), the mutual information terms in (56) can be expressed as

$$I(X_2; Y|X_1) = H(Y|X_1) - H(Y|X_1, X_2)$$

$$= H(Y|X_1) - H(N_1),$$

$$I(X_1; Y|X_2) - I(X_1; Z) = H(Y|X_2) - H(Y|X_1, X_2) - H(Z) + H(Z|X_1)$$

$$= H(Y|X_2) - H(N_1) - H(Z) + H(Z|X_1),$$

$$I(X_1, X_2; Y) - I(X_1, X_2; Z) = H(Y) - H(Y|X_1, X_2) - H(Z) + H(Z|X_1, X_2)$$

$$= H(Y) - H(N_1) - H(Z) + H(N_2),$$

$$I(X_1, X_2; Y) - I(X_1; Z) = H(Y) - H(Y|X_1, X_2) - H(Z) + H(Z|X_1)$$

$$= H(Y) - H(N_1) - H(Z) + H(Z|X_1), \tag{60}$$

and the mutual information differences in (57) can be expressed as

$$I(X_1; Y|X_2) - I(X_1; Z|X_2) = H(Y|X_2) - H(Y|X_1, X_2) - H(Z|X_2) + H(Z|X_1, X_2)$$

$$= H(Y|X_2) - H(N_1) - H(Z|X_2) + H(N_2),$$

$$I(X_1, X_2; Y) - I(X_1; Z|X_2) = H(Y) - H(Y|X_1, X_2) - H(Z|X_2) + H(Z|X_1, X_2)$$

$$= H(Y) - H(N_1) - H(Z|X_2) + H(N_2). \tag{61}$$

From (60) and (61) we know that to compute the upper bounds in (56) and (57), we need to compute the entropies $H(N_1)$, $H(N_2)$, $H(Y)$, $H(Y|X_1)$, $H(Y|X_2)$, $H(Z)$, $H(Z|X_1)$, and $H(Z|X_2)$.

Since both N_1 and N_2 follow Bernoulli distribution with parameters q_1 and q_2, we have

$$H(N_1) = -q_1 \log q_1 - (1 - q_1) \log(1 - q_1),$$

$$H(N_2) = -q_2 \log q_2 - (1 - q_2) \log(1 - q_2). \tag{62}$$

Based on the distributions of X_1, X_2, and N_1, we list the values of $P_{X_1, X_2, N_1}(x_1, x_2, n_1)$ and Y

TABLE I

$P_{X_1,X_2,N_1}(x_1, x_2, n_1)$ AND Y OVER DIFFERENT REALIZATIONS OF (X_1, X_2, N_1).

		$P_{X_1,X_2,N_1}(x_1, x_2, n_1)$	Y
	$(0,0,0)$	$(1-\alpha)(1-\beta)(1-q_1)$	0
	$(0,0,1)$	$(1-\alpha)(1-\beta)q_1$	1
	$(0,1,0)$	$(1-\alpha)\beta(1-q_1)$	1
(X_1, X_2, N_1)	$(0,1,1)$	$(1-\alpha)\beta q_1$	2
	$(1,0,0)$	$\alpha(1-\beta)(1-q_1)$	1
	$(1,0,1)$	$\alpha(1-\beta)q_1$	2
	$(1,1,0)$	$\alpha\beta(1-q_1)$	2
	$(1,1,1)$	$\alpha\beta q_1$	3

over different realizations of (X_1, X_2, N_1) in Table I, from which we have

$$P_Y(0) = (1-\alpha)(1-\beta)(1-q_1),$$

$$P_Y(1) = (1-\alpha)(1-\beta)q_1 + (1-\alpha)\beta(1-q_1) + \alpha(1-\beta)(1-q_1),$$

$$P_Y(2) = (1-\alpha)\beta q_1 + \alpha(1-\beta)q_1 + \alpha\beta(1-q_1),$$

$$P_Y(3) = \alpha\beta q_1. \tag{63}$$

Accordingly, the entropy of Y can be computed as

$$
\begin{aligned}
H(Y) = & -\sum_{y\in\{0,1,2,3\}} P_Y(y)\log P_Y(y) \\
= & -(1-\alpha)(1-\beta)(1-q_1)\log[(1-\alpha)(1-\beta)(1-q_1)] \\
& -[(1-\alpha)(1-\beta)q_1 + (1-\alpha)\beta(1-q_1) + \alpha(1-\beta)(1-q_1)] \\
& \times \log[(1-\alpha)(1-\beta)q_1 + (1-\alpha)\beta(1-q_1) + \alpha(1-\beta)(1-q_1)] \\
& -[(1-\alpha)\beta q_1 + \alpha(1-\beta)q_1 + \alpha\beta(1-q_1)]\log[(1-\alpha)\beta q_1 + \alpha(1-\beta)q_1 + \alpha\beta(1-q_1)] \\
& -\alpha\beta q_1\log(\alpha\beta q_1). \tag{64}
\end{aligned}
$$

In Table II, we list the values of $P_{X_1,Y}(x_1, y)$ and $P_{Y|X_1}(y|x_1)$ over different realizations of

(X_1, Y), from which the conditional entropy $H(Y|X_1)$ can be computed as follows

$$H(Y|X_1) = - \sum_{x_1 \in \{0,1\}} \sum_{y \in \{0,1,2,3\}} P_{X_1,Y}(x_1, y) \log P_{Y|X_1}(y|x_1)$$

$$= - (1-\beta)(1-q_1) \log[(1-\beta)(1-q_1)]$$

$$- [(1-\beta)q_1 + \beta(1-q_1)] \log[(1-\beta)q_1 + \beta(1-q_1)] - \beta q_1 \log(\beta q_1). \quad (65)$$

TABLE II

$P_{X_1,Y}(x_1, y)$ AND $P_{Y|X_1}(y|x_1)$ OVER DIFFERENT REALIZATIONS OF (X_1, Y).

		$P_{X_1,Y}(x_1, y)$	$P_{Y|X_1}(y|x_1)$
(X_1, Y)	$(0,0)$	$(1-\alpha)(1-\beta)(1-q_1)$	$(1-\beta)(1-q_1)$
	$(0,1)$	$(1-\alpha)(1-\beta)q_1 + (1-\alpha)\beta(1-q_1)$	$(1-\beta)q_1 + \beta(1-q_1)$
	$(0,2)$	$(1-\alpha)\beta q_1$	βq_1
	$(0,3)$	0	0
	$(1,0)$	0	0
	$(1,1)$	$\alpha(1-\beta)(1-q_1)$	$(1-\beta)(1-q_1)$
	$(1,2)$	$\alpha(1-\beta)q_1 + \alpha\beta(1-q_1)$	$(1-\beta)q_1 + \beta(1-q_1)$
	$(1,3)$	$\alpha\beta q_1$	αq_1

TABLE III

$P_{X_2,Y}(x_2, y)$ AND $P_{Y|X_2}(y|x_2)$ OVER DIFFERENT REALIZATIONS OF (X_2, Y).

		$P_{X_2,Y}(x_2, y)$	$P_{Y|X_2}(y|x_2)$
(X_2, Y)	$(0,0)$	$(1-\alpha)(1-\beta)(1-q_1)$	$(1-\alpha)(1-q_1)$
	$(0,1)$	$(1-\alpha)(1-\beta)q_1 + \alpha(1-\beta)(1-q_1)$	$(1-\alpha)q_1 + \alpha(1-q_1)$
	$(0,2)$	$\alpha(1-\beta)q_1$	αq_1
	$(0,3)$	0	0
	$(1,0)$	0	0
	$(1,1)$	$(1-\alpha)\beta(1-q_1)$	$(1-\alpha)(1-q_1)$
	$(1,2)$	$(1-\alpha)\beta q_1 + \alpha\beta(1-q_1)$	$(1-\alpha)q_1 + \alpha(1-q_1)$
	$(1,3)$	$\alpha\beta q_1$	αq_1

Similarly, $H(Y|X_2)$ can be calculated based on Table III as

$$
\begin{aligned}
H(Y|X_2) = & -\sum_{x_2 \in \{0,1\}} \sum_{y \in \{0,1,2,3\}} P_{X_2,Y}(x_2, y) \log P_{Y|X_2}(y|x_2) \\
= & -(1-\alpha)(1-q_1) \log[(1-\alpha)(1-q_1)] \\
& - [(1-\alpha)q_1 + \alpha(1-q_1)] \log[(1-\alpha)q_1 + \alpha(1-q_1)] - \alpha q_1 \log(\alpha q_1).
\end{aligned}
\tag{66}
$$

Analogously, the entropies $H(Z)$, $H(Z|X_1)$, and $H(Z|X_2)$ can be computed as follows

$$
\begin{aligned}
H(Z) = & -\sum_{z \in \{0,1,2,3\}} P_Z(z) \log P_Z(z) \\
= & -(1-\alpha)(1-\beta)(1-q_2) \log[(1-\alpha)(1-\beta)(1-q_2)] \\
& - [(1-\alpha)(1-\beta)q_2 + (1-\alpha)\beta(1-q_2) + \alpha(1-\beta)(1-q_2)] \\
& \times \log[(1-\alpha)(1-\beta)q_2 + (1-\alpha)\beta(1-q_2) + \alpha(1-\beta)(1-q_2)] \\
& - [(1-\alpha)\beta q_2 + \alpha(1-\beta)q_2 + \alpha\beta(1-q_2)] \log[(1-\alpha)\beta q_2 + \alpha(1-\beta)q_2 + \alpha\beta(1-q_2)] \\
& - \alpha\beta q_2 \log(\alpha\beta q_2).
\end{aligned}
\tag{67}
$$

$$
\begin{aligned}
H(Z|X_1) = & -\sum_{x_1 \in \{0,1\}} \sum_{z \in \{0,1,2,3\}} P_{X_1,Z}(x_1, z) \log P_{Z|X_1}(z|x_1) \\
= & -(1-\beta)(1-q_2) \log[(1-\beta)(1-q_2)] \\
& - [(1-\beta)q_2 + \beta(1-q_2)] \log[(1-\beta)q_2 + \beta(1-q_2)] - \beta q_2 \log(\beta q_2).
\end{aligned}
\tag{68}
$$

$$
\begin{aligned}
H(Z|X_2) = & -\sum_{x_2 \in \{0,1\}} \sum_{z \in \{0,1,2,3\}} P_{X_2,Z}(x_2, z) \log P_{Z|X_2}(z|x_2) \\
= & -(1-\alpha)(1-q_2) \log[(1-\alpha)(1-q_2)] \\
& - [(1-\alpha)q_2 + \alpha(1-q_2)] \log[(1-\alpha)q_2 + \alpha(1-q_2)] - \alpha q_2 \log(\alpha q_2).
\end{aligned}
\tag{69}
$$

By substituting (62) and (64) $\sim$ (69) to (60) and (61), the upper bounds in (56) and (57) can be computed.

C. Numerical Results

In this subsection, we depict the convex hulls $\hat{\mathscr{R}}_{\text{old}}$ and $\hat{\mathscr{R}}_{\text{new}}^{\{1\}}$ in (58) for the binary adder channel with $(q_1, q_2) = (0.5, 0.75)$, and show that $\hat{\mathscr{R}}_{\text{new}}^{\{1\}}$ contains points that are not in $\hat{\mathscr{R}}_{\text{old}}$. The Matlab code is provided in .... We first depict $\hat{\mathscr{R}}_{\text{old}}$. For convenience, denote

$$a_1 = \min\{[I(X_1; Y|X_2) - I(X_1; Z)]^+, [I(X_1, X_2; Y) - I(X_1, X_2; Z)]^+\},$$

$$b = I(X_2; Y|X_1),$$

$$c_1 = [I(X_1, X_2; Y) - I(X_1; Z)]^+, \tag{70}$$

based on which $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1, 2\})$ in (56) can be rewritten as

$$\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1, 2\}) \begin{cases} R_1^{\text{s}} \leq a_1 \\ R_2^{\text{o}} \leq b \\ R_1^{\text{s}} + R_2^{\text{o}} \leq c_1 \end{cases}. \tag{71}$$

Note that in the binary adder channel, the distributions of X_1 and X_2 are respectively determined by $\alpha \in [0, 1]$ and $\beta \in [0, 1]$. Then, $\hat{\mathscr{R}}_{\text{old}}$ in (58) can be rewritten as

$$\hat{\mathscr{R}}_{\text{old}} = \text{Conv} \bigcup_{\alpha \in [0,1], \beta \in [0,1]} \hat{\mathscr{R}}(X_{\mathcal{K}}, \{1, 2\}). \tag{72}$$

Using the definition and non-negativity of mutual information, we have

$$I(X_1, X_2; Y) - I(X_1; Z) = I(X_1; Y|X_2) + I(X_2; Y) - I(X_1; Z)$$

$$\geq I(X_1; Y|X_2) - I(X_1; Z),$$

$$I(X_1, X_2; Y) - I(X_1; Z) \geq I(X_1, X_2; Y) - I(X_1; Z) - I(X_2; Z|X_1)$$

$$= I(X_1, X_2; Y) - I(X_1, X_2; Z). \tag{73}$$

Combining (70) and (73), we know that $c_1 \geq a_1$. Since $(q_1, q_2) = (0.5, 0.75)$, if (α, β) is known, the values of a_1, b, and c_1 can be computed based on the analysis given in the previous subsection. As discussed below, $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1, 2\})$ has five possible shapes, depending on the values of a_1, b, and c_1.

- Case 1: $c_1 = 0$.

  In this case, both R_1^{s} and R_1^{s} are 0. $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1, 2\})$ thus contains only one point $(0, 0)$.

- Case 2: $a_1 = 0$.

  In this case, $R_1^{\text{s}} = 0$ and $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1, 2\})$ is a line segment between $(0, 0)$ and $(0, \min\{b, c_1\})$.
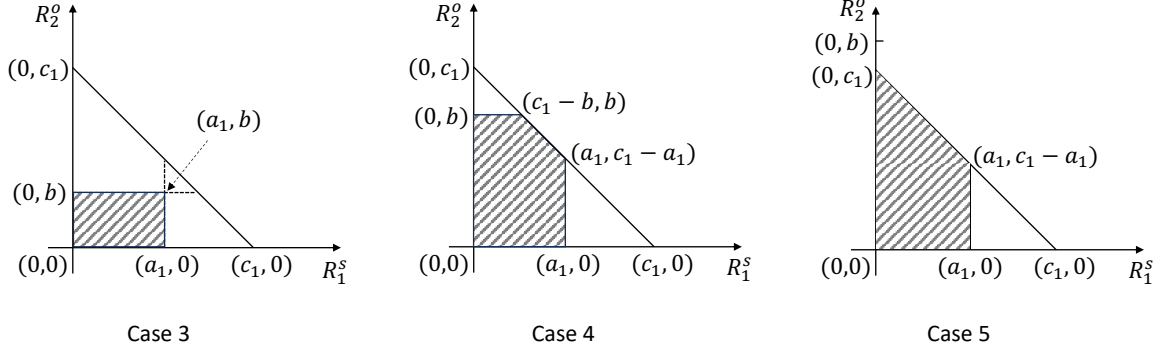
Fig. 5. Achievable region $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1,2\})$ in different cases.

- Case 3: $a_1 > 0$ and $b \leq c_1 - a_1$.

  As shown in Fig. 5, $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1,2\})$ in this case is a rectangular region with four vertices $(0,0)$, $(a_1, 0)$, (a_1, b), and $(0, b)$.

- Case 4: $a_1 > 0$ and $c_1 - a_1 < b \leq c_1$.

  As shown in Fig. 5, $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1,2\})$ in this case is a pentagon region with five vertices $(0,0)$, $(a_1, 0)$, $(a_1, c_1 - a_1)$, $(c_1 - b, b)$, and $(0, b)$.

- Case 5: $a_1 > 0$ and $b > c_1$.

  As shown in Fig. 5, $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1,2\})$ in this case is a trapezoidal region with four vertices $(0,0)$, $(a_1, 0)$, $(a_1, c_1 - a_1)$, and $(0, c_1)$.

To depict $\hat{\mathscr{R}}_{\text{old}}$, we sample α and β in the range [0,1] with step $\delta = 0.01$, record the corner points of $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1,2\})$ for each given (α, β), and then depict the convex hull consisting of all these corner points using Matlab. In Fig. 6, the area encircled by the red line is $\hat{\mathscr{R}}_{\text{old}}$.

Now we depict $\hat{\mathscr{R}}_{\text{new}}^{\{1\}}$. For convenience, denote

$$a_2 = [I(X_1; Y|X_2) - I(X_1; Z|X_2)]^+ ,$$

$$c_2 = [I(X_1, X_2; Y) - I(X_1; Z|X_2)]^+ , \tag{74}$$

based on which $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1\})$ in (57) and $\hat{\mathscr{R}}_{\text{old}}$ in (58) can be respectively rewritten as

$$\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1\}) \begin{cases} R_1^s \leq a_2 \\ R_2^o \leq b \\ R_1^s + R_2^o \leq c_2 \end{cases} , \tag{75}$$

$$\hat{\mathscr{R}}_{\text{new}}^{\{1\}} = \text{Conv} \bigcup_{\alpha \in [0,1], \beta \in [0,1]} \hat{\mathscr{R}}(X_{\mathcal{K}}, \{1\}). \tag{76}$$
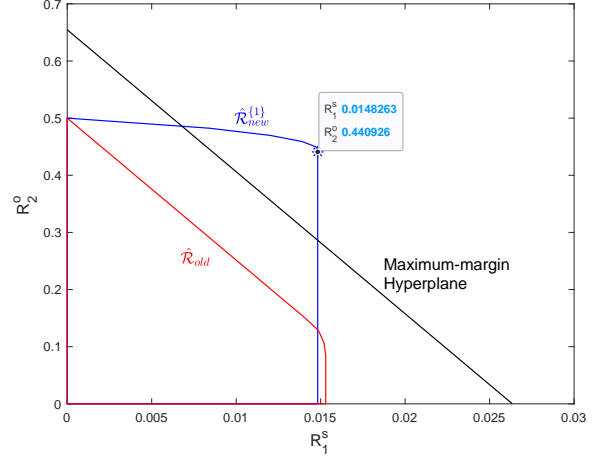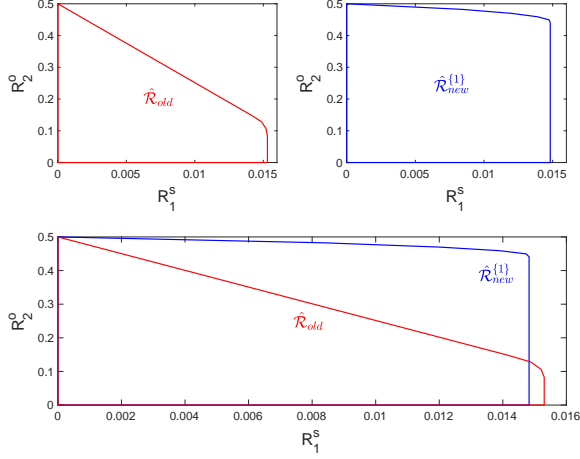
Fig. 6. Convex hulls $\hat{\hat{\mathscr{R}}}_{\text{old}}$ and $\hat{\hat{\mathscr{R}}}_{\text{new}}^{\{1\}}$ with $(q_1, q_2) = (0.5, 0.75)$. Fig. 7. SVM-based separation of an extreme point in $\hat{\hat{\mathscr{R}}}_{\text{new}}^{\{1\}}$ and $\hat{\hat{\mathscr{R}}}_{\text{old}}$.

Since

$$I(X_1, X_2; Y) - I(X_1; Z|X_2) = I(X_1; Y|X_2) + I(X_2; Y) - I(X_1; Z|X_2)$$

$$\geq I(X_1; Y|X_2) - I(X_1; Z|X_2), \tag{77}$$

we have $c_2 \geq a_2$. Then, $\hat{\hat{\mathscr{R}}}_{\text{new}}^{\{1\}}$ can be depicted similarly as $\hat{\hat{\mathscr{R}}}_{\text{old}}$. We omit the details for brevity. In Fig. 6, the area encircled by the blue line is $\hat{\hat{\mathscr{R}}}_{\text{new}}^{\{1\}}$.

From Fig. 6 we see that $\hat{\hat{\mathscr{R}}}_{\text{old}}$ and $\hat{\hat{\mathscr{R}}}_{\text{new}}^{\{1\}}$ have non-overlapping areas. In the following, we choose a point in $\hat{\hat{\mathscr{R}}}_{\text{new}}^{\{1\}}$, and show that it is linearly separable from those in $\hat{\hat{\mathscr{R}}}_{\text{old}}$ using a support vector machine (SVM). This point is thus not included in $\hat{\hat{\mathscr{R}}}_{\text{old}}$. In particular, let $\mathcal{J}$ denote the convex set of all corner points of $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1, 2\})$ collected in depicting $\hat{\hat{\mathscr{R}}}_{\text{old}}$ for all (α, β), and $\mathcal{J}_0$ denote the set of all extreme points of $\mathcal{J}$. Note that an extreme point of a convex set is a point in the set that does not lie on any open line segment between any other two points of the same set. Therefore, $\mathcal{J}_0$ is the minimal convex subset in $\mathcal{J}$ that has the same convex hull as $\mathcal{J}$. Denote the j-th extreme point in $\mathcal{J}_0$ by $\boldsymbol{v}_j = [R_1^s(j), R_2^o(j)]^T$. Similarly, we let $\mathcal{L}$ denote the convex set of all corner points of $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1\})$ collected in depicting $\hat{\hat{\mathscr{R}}}_{\text{new}}^{\{1\}}$ for all (α, β), and $\mathcal{L}_0$ denote the set of all extreme points of $\mathcal{L}$. We choose an extreme point $\boldsymbol{v}_0 = [0.0148263, 0.440926]^T$ in $\mathcal{L}_0$. Now we show that $\boldsymbol{v}_0$ and the points in $\mathcal{J}_0$ are linearly separable, i.e., there exists a hyperplane such that $\boldsymbol{v}_0$ and all points in $\mathcal{J}_0$ lie on different sides of the hyperplane. The hyperplane can
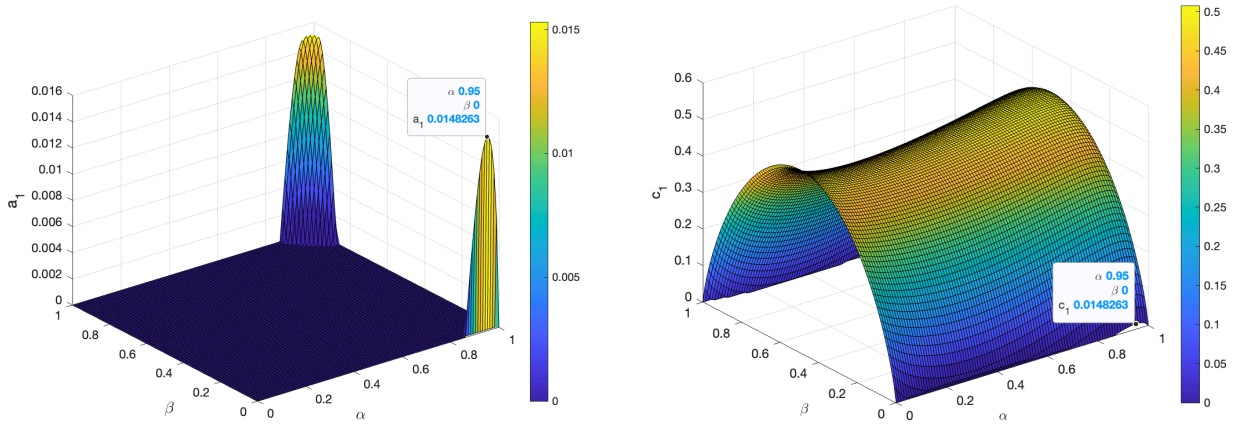
Fig. 8. a_1 versus α and β with $\hat{\hat{\mathscr{R}}}_{\text{new}}^{\{1\}}$ with $(q_1, q_2) = (0.5, 0.75)$ and sampling size $\delta = 0.01$.

Fig. 9. c_1 versus α and β with $\hat{\hat{\mathscr{R}}}_{\text{new}}^{\{1\}}$ with $(q_1, q_2) = (0.5, 0.75)$ and sampling size $\delta = 0.01$.

be found by considering the following optimization problem

$$\min_{\boldsymbol{w}, t} \quad ||\boldsymbol{w}||_2^2$$

$$\text{s.t.} \quad \boldsymbol{w}^T \boldsymbol{v}_0 - t \geq 1,$$

$$\boldsymbol{w}^T \boldsymbol{v}_j - t \leq -1, \forall j = 1, \cdots, |\mathcal{J}_0|, \tag{78}$$

where $\boldsymbol{w} \in \mathbb{R}^{2 \times 1}$ and $t \in \mathbb{R}$ are the optimization variables. Problem (78) is a linear SVM and $\boldsymbol{w}^T \boldsymbol{v} - t = 0$ is known as the maximum-margin hyperplane. Since (78) is a convex problem, we solve it by CVX in matlab, and depict $\hat{\hat{\mathscr{R}}}_{\text{old}}$, $\hat{\hat{\mathscr{R}}}_{\text{new}}^{\{1\}}$, $\boldsymbol{v}_0$, and the maximum-margin hyperplane $\boldsymbol{w}^T \boldsymbol{v} - t = 0$ in Fig. 7. As we can see from this figure, $\boldsymbol{v}_0$ and all points in $\mathcal{J}_0$ can be separated by the maximum-margin hyperplane. Since $\mathcal{J}_0$ consists of all the extreme points in $\mathcal{J}$, we know that all points in $\mathcal{J}$ can be separated from $\boldsymbol{v}_0$. Therefore, $\boldsymbol{v}_0$ is not in $\hat{\hat{\mathscr{R}}}_{\text{old}}$. Since it is in $\hat{\hat{\mathscr{R}}}_{\text{new}}^{\{1\}}$, the proposed region $\mathscr{R}_{\text{new}}$ can strictly improve $\mathscr{R}_{\text{old}}$ given in [15, Theorem 1].

Now we explain why for the considered binary adder channel with $(q_1, q_2) = (0.5, 0.75)$, $\hat{\hat{\mathscr{R}}}_{\text{old}}$ and $\hat{\hat{\mathscr{R}}}_{\text{new}}^{\{1\}}$ have non-overlapping areas, by depicting a_1, c_1, a_2, c_2, and b over α and β. In Fig. 8 and Fig. 9, we depict a_1 and c_1 versus α and β with sampling size $\delta = 0.01$. It can be seen from Fig. 8 that for most values of α and β, $a_1 = 0$. Since a_1 is the upper bound to R_1^{s} in $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1, 2\})$, we have is $R_1^{\text{s}} = 0$ in these cases. Only when α is around 0.95 and β is close to 0 or 1, will R_1^{s} take on a relatively large value. However, in these cases, we see from Fig. 9 that c_1 is small. Since c_1 is the upper bound to $R_1^{\text{s}} + R_2^{\text{o}}$ in $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1, 2\})$, it is impossible for
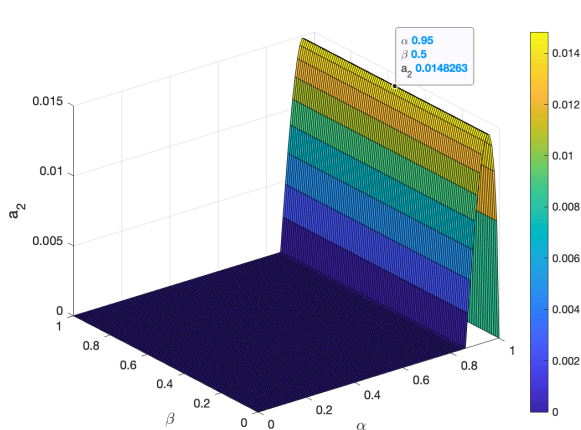
Fig. 10. a_2 versus α and β with $\hat{\mathscr{R}}_{\text{new}}^{\{1\}}$ with $(q_1, q_2) = (0.5, 0.75)$ and sampling size $\delta = 0.01$.
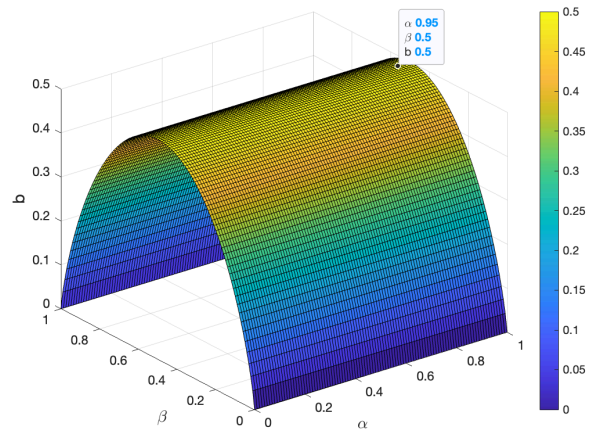
Fig. 11. b versus α and β with $\hat{\mathscr{R}}_{\text{new}}^{\{1\}}$ with $(q_1, q_2) = (0.5, 0.75)$ and sampling size $\delta = 0.01$.
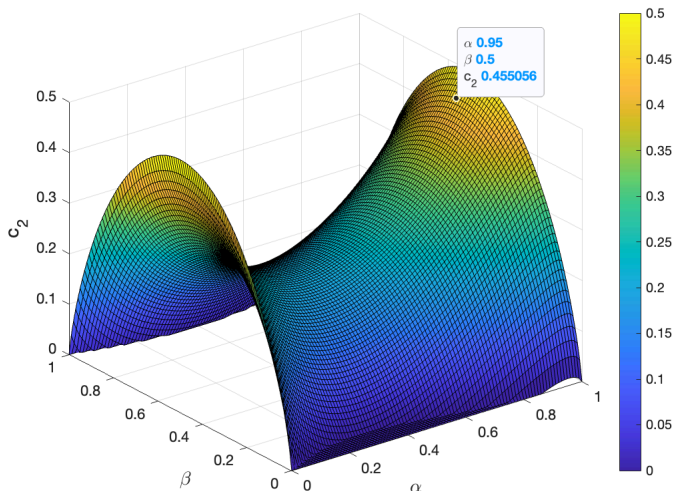

Fig. 12. c_2 versus α and β with $\hat{\mathscr{R}}_{\text{new}}^{\{1\}}$ with $(q_1, q_2) = (0.5, 0.75)$ and sampling size $\delta = 0.01$.

R_2^{o} to take a large value in these cases. This explains why when R_1^{s} is large, R_2^{o} is small in $\hat{\mathscr{R}}_{\text{old}}$ (see Fig. 6).

In Fig. 10, Fig. 11, and Fig. 12, we depict a_2, b, and c_2 versus α and β, respectively. Different from a_1, Fig. 10 shows that whatever the value of β, as long as α is around 0.95, a_2 takes on a relatively large value. When α and β are respectively 0.5 and 0.95, a_2, b, and c_2 are all relatively large. Since a_2, b, and c_2 are respectively upper bounds to R_1^{s}, R_2^{o}, and $R_1^{\text{s}} + R_2^{\text{o}}$, it is possible for a point $(R_1^{\text{s}}, R_2^{\text{o}})$ in the region $\hat{\mathscr{R}}(X_{\mathcal{K}}, \{1\})$ to have both large R_1^{s} and R_2^{o}. This explains why $\hat{\mathscr{R}}_{\text{new}}^{\{1\}}$ has a non-overlapping area on the upper-right side of $\hat{\mathscr{R}}_{\text{old}}$ in Fig. 6.

VI. Conclusions

In this paper, we studied the information-theoretic secrecy for a K-user DM MAC-WT channel, where each user has both secret and open messages for the intended receiver. Auxiliary messages were introduced to protect the confidential information. To ensure that the rate of auxiliary messages is large enough for protecting the secret message from Eve and the resulting sum rate (together with the secret and open message rate) does not exceed Bob's decoding capability, we developed an inequality structure involving the rates of all users' secret, open, and auxiliary messages, and also gave the general proof. We adopted strong secrecy, defined by the mutual information between all confidential messages and the received signal at Eve, as the secrecy metric. To prove the achievability under this criterion, we analyzed the output statistics in terms of variational distance for the K-user standard DM-MAC channel. In addition, we showed that users with zero secrecy rate may have different options in choosing their coding schemes. By considering all possible options, we obtained a new achievable region for the considered channel that enlarges previously known results, and the improvement has been verified by a two-user binary adder channel. Considering the fact that even for the classical two-user DM MAC-WT channel with only secret messages, the tight converse is still an open problem, this paper focused on studying the achievable region for the K-user DM MAC-WT channel, and did not derive a converse. We plan to study the converse from the two-user DM MAC-WT channel with only secret messages in the future.

Appendix A

Proof of Lemma 1

In this appendix, we prove Lemma 1 by showing that (9) is the projection of (10) onto the hyperplane $\{R_k^{\mathrm{a}} = 0, \forall k \in \mathcal{K}\}$. Note that due to (8), the polytope defined by (9) is non-empty. Since as shown below we can successfully prove that (9) is the projection of (10), we know from [35, Appendix D] that the polytope defined by (10) must be non-empty. As stated in Remark 1, it is impossible to prove Lemma 1 by directly using the Fourier-Motzkin procedure to eliminate all R_k^{a} in (10), not only because of its huge complexity but also due to the fact that the elimination strategy works only if K is given. Hence, we adopt mathematical induction in the following to prove Lemma 1.

We first consider the base case with $K = 1$. By eliminating R_1^a in (10) using the Fourier-Motzkin procedure [35, Appendix D], it can be easily proven that (9) is the projection of (10) onto the hyperplane $\{R_1^a = 0\}$. Lemma 1 can thus be proven for this simple case.

Next, we consider the induction step. Assume that for any given positive integer K, (9) is the projection of (10) onto the hyperplane $\{R_k^a = 0, \forall k \in \mathcal{K}\}$. Then, by this assumption, it is possible to obtain (9) by eliminating the variables $R_k^a, \forall k \in \mathcal{K}$ using the Fourier-Motzkin procedure. For convenience, in the following we refer to this assumption as the *induction assumption*. Under the induction assumption, we shall prove that the statement of Lemma 1 holds for $K + 1$ users. With $K + 1$ users, (9) and (10) become

$$\sum_{k \in \mathcal{S}} R_k^s + \sum_{k \in \mathcal{S} \setminus \mathcal{S}'} R_k^o \leq I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}) - I(X_{\mathcal{S}'}; Z), \forall \mathcal{S} \subseteq \mathcal{K} \cup \{K + 1\}, \mathcal{S}' \subseteq \mathcal{S}, \quad (79)$$

and

$$\begin{cases} R_k^a \geq 0, \forall k \in \mathcal{K} \cup \{K + 1\}, \\ \sum_{k \in \mathcal{S}} (R_k^s + R_k^o + R_k^a) \leq I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}), \forall \mathcal{S} \subseteq \mathcal{K} \cup \{K + 1\}, \\ \sum_{k \in \mathcal{S}} (R_k^o + R_k^a) \geq I(X_{\mathcal{S}}; Z), \forall \mathcal{S} \subseteq \mathcal{K} \cup \{K + 1\}. \end{cases} \quad (80)$$

We need to show that (79) is the projection of (80) onto the hyperplane $\{R_k^a = 0, \forall k \in \mathcal{K} \cup \{K + 1\}\}$, i.e., (79) can be obtained by eliminating $R_k^a, \forall k \in \mathcal{K}$ as well as R_{K+1}^a in (80). For this purpose, by separating user $K + 1$ from users in set $\mathcal{K}$, we rewrite (79) equivalently as

$$\sum_{k \in \mathcal{S}} R_k^s + \sum_{k \in \mathcal{S} \setminus \mathcal{S}'} R_k^o \leq I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}, X_{K+1}) - I(X_{\mathcal{S}'}; Z), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S}' \subseteq \mathcal{S}, \quad (81a)$$

$$\sum_{k \in \mathcal{S}} R_k^s + R_{K+1}^s + \sum_{k \in \mathcal{S} \setminus \mathcal{S}'} R_k^o + R_{K+1}^o \leq I(X_{\mathcal{S}}, X_{K+1}; Y | X_{\overline{\mathcal{S}}}) - I(X_{\mathcal{S}'}; Z), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S}' \subseteq \mathcal{S}, \quad (81b)$$

$$\sum_{k \in \mathcal{S}} R_k^s + R_{K+1}^s + \sum_{k \in \mathcal{S} \setminus \mathcal{S}'} R_k^o \leq I(X_{\mathcal{S}}, X_{K+1}; Y | X_{\overline{\mathcal{S}}}) - I(X_{\mathcal{S}'}, X_{K+1}; Z), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S}' \subseteq \mathcal{S}, \quad (81c)$$

and (80) as

$$R_k^{\mathrm{a}} \geq 0, \forall k \in \mathcal{K}, \tag{82a}$$

$$\sum_{k \in \mathcal{S}} (R_k^{\mathrm{s}} + R_k^{\mathrm{o}} + R_k^{\mathrm{a}}) \leq I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}, X_{K+1}), \forall \mathcal{S} \subseteq \mathcal{K}, \tag{82b}$$

$$\sum_{k \in \mathcal{S}} (R_k^{\mathrm{o}} + R_k^{\mathrm{a}}) \geq I(X_{\mathcal{S}}; Z), \forall \mathcal{S} \subseteq \mathcal{K}, \tag{82c}$$

$$\sum_{k \in \mathcal{S}} (R_k^{\mathrm{s}} + R_k^{\mathrm{o}} + R_k^{\mathrm{a}}) \leq I(X_{\mathcal{S}}, X_{K+1}; Y | X_{\overline{\mathcal{S}}}) - (R_{K+1}^{\mathrm{s}} + R_{K+1}^{\mathrm{o}} + R_{K+1}^{\mathrm{a}}), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi, \tag{82d}$$

$$\sum_{k \in \mathcal{S}} (R_k^{\mathrm{o}} + R_k^{\mathrm{a}}) \geq I(X_{\mathcal{S}}, X_{K+1}; Z) - (R_{K+1}^{\mathrm{o}} + R_{K+1}^{\mathrm{a}}), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi, \tag{82e}$$

$$R_{K+1}^{\mathrm{a}} \geq 0, \tag{82f}$$

$$R_{K+1}^{\mathrm{s}} + R_{K+1}^{\mathrm{o}} + R_{K+1}^{\mathrm{a}} \leq I(X_{K+1}; Y | X_{\mathcal{K}}), \tag{82g}$$

$$R_{K+1}^{\mathrm{o}} + R_{K+1}^{\mathrm{a}} \geq I(X_{K+1}; Z). \tag{82h}$$

Note that in (82d) and (82e) we let $\mathcal{S} \neq \phi$ since otherwise they reduce to (82g) and (82h), which do not contain $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}$. In the following, we eliminate first $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}$ and then R_{K+1}^{a}.

A. Elimination of $R_k^{a}, \forall k \in \mathcal{K}$

To eliminate $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}$ in (82), we focus on (82a) $\sim$ (82e) since only these inequalities contain $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}$ while (82f) $\sim$ (82h) do not. Since there are K different R_k^{a}, as stated above, it is impractical to eliminate R_k^{a} one by one. Hence, instead of eliminating $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}$ directly from (82a) $\sim$ (82e), we divide these inequalities into 4 categories (see Fig. 13), which together consider all possible upper and lower bound pairs on $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}$, and eliminate $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}$ in each category using the induction assumption.

For convenience, we call the inequality system (IES) consisting of (82a) $\sim$ (82e) IES 1. As we can see from (82), in IES 1, there are three lower bounds on $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}$, i.e., (82a), (82c), and (82e), which are marked in blue color in Fig. 13, and two upper bounds on $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}$, i.e., (82b) and (82d), which are marked in red color. To eliminate $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}$ in IES 1 based on the induction assumption, as shown in Fig. 13, we first repeat the inequalities in IES 1 and obtain IES 2. Since the repeated inequalities can neither expand nor shrink the region of IES 1, IES 1 and IES 2 are equivalent. Then, we change the order of the inequalities in IES 2 and obtain IES 3. Obviously, IES 3 is equivalent to IES 2, and is thus also equivalent IES 1. Therefore,

eliminating $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}$ in IES 1 is equivalent to eliminating those in IES 3, which as we will show below, can be realized by separately eliminating $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}$ in each category using the induction assumption.
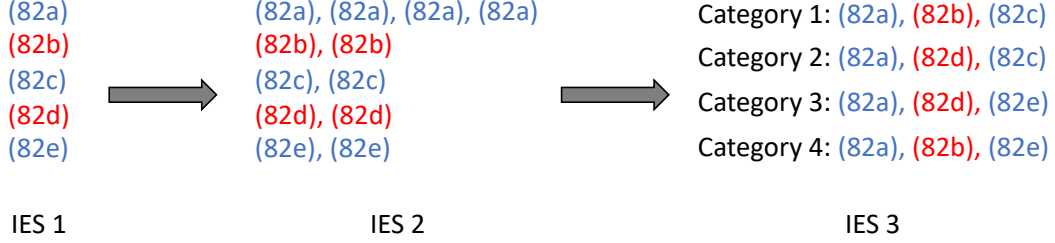
(82a)	(82a), (82a), (82a), (82a)	Category 1: (82a), (82b), (82c)
(82b)	(82b), (82b)	Category 2: (82a), (82d), (82c)
(82c)	(82c), (82c)	Category 3: (82a), (82d), (82e)
(82d)	(82d), (82d)	Category 4: (82a), (82b), (82e)
(82e)	(82e), (82e)	
IES 1	IES 2	IES 3

Fig. 13. Division of ISE 1.

1) Category 1: We include inequalities (82a), (82b), and (82c) in Category 1, and rewrite them as follows for clarity

$$
\begin{cases}
R_k^{\mathrm{a}} \geq 0, \forall k \in \mathcal{K}, \\
\sum_{k \in \mathcal{S}} (R_k^{\mathrm{s}} + R_k^{\mathrm{o}} + R_k^{\mathrm{a}}) \leq I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}, X_{K+1}), \forall \mathcal{S} \subseteq \mathcal{K}, \\
\sum_{k \in \mathcal{S}} (R_k^{\mathrm{o}} + R_k^{\mathrm{a}}) \geq I(X_{\mathcal{S}}; Z), \forall \mathcal{S} \subseteq \mathcal{K}.
\end{cases}
\tag{83}
$$

Note that (83) has a similar formulation as (10). Then, from the induction assumption it is known that the projection of (83) onto the hyperplane $\{R_k^{\mathrm{a}} = 0, \forall k \in \mathcal{K}\}$ is

$$
\sum_{k \in \mathcal{S}} R_k^{\mathrm{s}} + \sum_{k \in \mathcal{S} \setminus \mathcal{S}'} R_k^{\mathrm{o}} \leq I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}, X_{K+1}) - I(X_{\mathcal{S}'}; Z), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S}' \subseteq \mathcal{S},
\tag{84}
$$

which is the same as (81a).

2) Category 2: In this category we include (82a), (82d), and (82c), and rewrite them as

$$
\begin{cases}
R_k^{\mathrm{a}} \geq 0, \forall k \in \mathcal{K}, \\
\sum_{k \in \mathcal{S}} (R_k^{\mathrm{s}} + R_k^{\mathrm{o}} + R_k^{\mathrm{a}}) \leq I(X_{\mathcal{S}}, X_{K+1}; Y | X_{\overline{\mathcal{S}}}) - (R_{K+1}^{\mathrm{s}} + R_{K+1}^{\mathrm{o}} + R_{K+1}^{\mathrm{a}}), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi, \\
\sum_{k \in \mathcal{S}} (R_k^{\mathrm{o}} + R_k^{\mathrm{a}}) \geq I(X_{\mathcal{S}}; Z), \forall \mathcal{S} \subseteq \mathcal{K}.
\end{cases}
\tag{85}
$$

Note that though we let $\mathcal{S} \neq \phi$ in (82d), (85) still has a similar expression as (10). It can be checked that if $\mathcal{S} = \phi$, the second inequality of (10) gives $0 \leq 0$, which can be omitted. Hence,

we may also let $\mathcal{S} \neq \phi$ in (10) without changing its formulation. The induction assumption can thus be used to eliminate $R_k^a, \forall k \in \mathcal{K}$ in (85) and obtain

$$\sum_{k \in \mathcal{S}} R_k^s + \sum_{k \in \mathcal{S} \backslash \mathcal{S}'} R_k^o \leq I(X_{\mathcal{S}}, X_{K+1}; Y | X_{\overline{\mathcal{S}}}) - (R_{K+1}^s + R_{K+1}^o + R_{K+1}^a) - I(X_{\mathcal{S}'}; Z),$$

$$\forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi, \mathcal{S}' \subseteq \mathcal{S}, \tag{86}$$

which contains R_{K+1}^a and thus has to be considered in the next step when eliminating R_{K+1}^a.

3) Category 3*:* In Category 3 we include (82a), (82d), and (82e), and rewrite them as follows

$$\begin{cases} R_k^a \geq 0, \forall k \in \mathcal{K}, \\ \sum_{k \in \mathcal{S}} (R_k^s + R_k^o + R_k^a) \leq I(X_{\mathcal{S}}, X_{K+1}; Y | X_{\overline{\mathcal{S}}}) - (R_{K+1}^s + R_{K+1}^o + R_{K+1}^a), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi, \\ \sum_{k \in \mathcal{S}} (R_k^o + R_k^a) \geq I(X_{\mathcal{S}}, X_{K+1}; Z) - (R_{K+1}^o + R_{K+1}^a), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi. \end{cases} \tag{87}$$

Using the induction assumption to eliminate $R_k^a, \forall k \in \mathcal{K}$, we have

$$\sum_{k \in \mathcal{S}} R_k^s + \sum_{k \in \mathcal{S} \backslash \mathcal{S}'} R_k^o$$

$$\leq I(X_{\mathcal{S}}, X_{K+1}; Y | X_{\overline{\mathcal{S}}}) - (R_{K+1}^s + R_{K+1}^o + R_{K+1}^a) - \left[I(X_{\mathcal{S}'}, X_{K+1}; Z) - (R_{K+1}^o + R_{K+1}^a) \right],$$

$$= I(X_{\mathcal{S}}, X_{K+1}; Y | X_{\overline{\mathcal{S}}}) - I(X_{\mathcal{S}'}, X_{K+1}; Z) - R_{K+1}^s, \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi, \mathcal{S}' \subseteq \mathcal{S}, \mathcal{S}' \neq \phi. \tag{88}$$

By comparing (88) with (81c), it is known that (88) consists of partial inequalities in (81c) with $\mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi, \mathcal{S}' \subseteq \mathcal{S}, \mathcal{S}' \neq \phi$.

4) Category 4*:* We include inequalities (82a), (82b), and (82e) in Category 4, and rewrite them as follows

$$\begin{cases} R_k^a \geq 0, \forall k \in \mathcal{K}, \\ \sum_{k \in \mathcal{S}} (R_k^s + R_k^o + R_k^a) \leq I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}, X_{K+1}), \forall \mathcal{S} \subseteq \mathcal{K}, \\ \sum_{k \in \mathcal{S}} (R_k^o + R_k^a) \geq I(X_{\mathcal{S}}, X_{K+1}; Z) - (R_{K+1}^o + R_{K+1}^a), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi. \end{cases} \tag{89}$$

The following projection of (89) can then be obtained from the induction assumption

$$\sum_{k \in \mathcal{S}} R_k^s + \sum_{k \in \mathcal{S} \backslash \mathcal{S}'} R_k^o \leq I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}, X_{K+1}) - I(X_{\mathcal{S}'}, X_{K+1}; Z) + R_{K+1}^o + R_{K+1}^a,$$

$$\forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi, \mathcal{S}' \subseteq \mathcal{S}, \mathcal{S}' \neq \phi, \tag{90}$$

which also contains R_{K+1}^a and has to be considered in the next step when eliminating R_{K+1}^a.

Combining (82f) $\sim$ (82h), (84), (86), (88), and (90), we get a projection of (82) onto the hyperplane $\{R_k^a = 0, \forall k \in \mathcal{K}\}$. To further get a projection of (82) onto the hyperplane $\{R_k^a = 0, \forall k \in \mathcal{K} \cup \{K + 1\}\}$, we have to eliminate R_{K+1}^a.

B. Elimination of R^a_{K+1}

In this subsection, we eliminate R^a_{K+1} in (82). Note that in the previous step, we have eliminated $R^a_k, \forall k \in \mathcal{K}$ in (82a) $\sim$ (82e), and obtained (84), (86), (88), and (90), in which (86) and (90) contain R^a_{K+1}. Therefore, when eliminating R^a_{K+1}, we should not consider all the inequalities (82a) $\sim$ (82h) in (82). Instead, we consider part of them, i.e., (82f) $\sim$ (82h), and also (86) and (90). From (82g) and (86), we get the following upper bounds on R^a_{K+1}

$$R^a_{K+1} \le I(X_{K+1}; Y | X_\mathcal{K}) - (R^s_{K+1} + R^o_{K+1}), \tag{91a}$$

$$R^a_{K+1} \le I(X_\mathcal{S}, X_{K+1}; Y | X_{\overline{\mathcal{S}}}) - I(X_{\mathcal{S}'}; Z) - \left(\sum_{k \in \mathcal{S}} R^s_k + \sum_{k \in \mathcal{S} \backslash \mathcal{S}'} R^o_k + R^s_{K+1} + R^o_{K+1} \right),$$

$$\forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \ne \phi, \mathcal{S}' \subseteq \mathcal{S}. \tag{91b}$$

Moreover, the following lower bounds on R^a_{K+1} can be obtained from (82f), (82h), and (90)

$$R^a_{K+1} \ge 0, \tag{92a}$$

$$R^a_{K+1} \ge I(X_{K+1}; Z) - R^o_{K+1}, \tag{92b}$$

$$R^a_{K+1} \ge -I(X_\mathcal{S}; Y | X_{\overline{\mathcal{S}}}, X_{K+1}) + I(X_{\mathcal{S}'}, X_{K+1}; Z) + \sum_{k \in \mathcal{S}} R^s_k + \sum_{k \in \mathcal{S} \backslash \mathcal{S}'} R^o_k - R^o_{K+1},$$

$$\forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \ne \phi, \mathcal{S}' \subseteq \mathcal{S}, \mathcal{S}' \ne \phi. \tag{92c}$$

Comparing these upper and lower bounds, we can eliminate R^a_{K+1}.

Firstly, we compare (91) with (92a), and get

$$R^s_{K+1} + R^o_{K+1} \le I(X_{K+1}; Y | X_\mathcal{K}), \tag{93a}$$

$$\sum_{k \in \mathcal{S}} R^s_k + \sum_{k \in \mathcal{S} \backslash \mathcal{S}'} R^o_k + R^s_{K+1} + R^o_{K+1} \le I(X_\mathcal{S}, X_{K+1}; Y | X_{\overline{\mathcal{S}}}) - I(X_{\mathcal{S}'}; Z),$$

$$\forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \ne \phi, \mathcal{S}' \subseteq \mathcal{S}. \tag{93b}$$

The inequalities (93a) and (93b) can be integrated into one formula as follows

$$\sum_{k \in \mathcal{S}} R^s_k + \sum_{k \in \mathcal{S} \backslash \mathcal{S}'} R^o_k + R^s_{K+1} + R^o_{K+1} \le I(X_\mathcal{S}, X_{K+1}; Y | X_{\overline{\mathcal{S}}}) - I(X_{\mathcal{S}'}; Z), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S}' \subseteq \mathcal{S}, \tag{94}$$

which is the same as (81b).

Secondly, we compare (91) with (92b), and get

$$R^{\text{s}}_{K+1} \leq I(X_{K+1}; Y|X_{\mathcal{K}}) - I(X_{K+1}; Z), \tag{95a}$$

$$\sum_{k \in \mathcal{S}} R^{\text{s}}_k + \sum_{k \in \mathcal{S} \backslash \mathcal{S}'} R^{\text{o}}_k + R^{\text{s}}_{K+1} \leq I(X_{\mathcal{S}}, X_{K+1}; Y|X_{\overline{\mathcal{S}}}) - I(X_{\mathcal{S}'}; Z) - I(X_{K+1}; Z),$$

$$\forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi, \mathcal{S}' \subseteq \mathcal{S}. \tag{95b}$$

By separately considering $\mathcal{S}' = \phi$ and $\mathcal{S}' \neq \phi$, we may divide (95b) into two formulas as below

$$\sum_{k \in \mathcal{S}} (R^{\text{s}}_k + R^{\text{o}}_k) + R^{\text{s}}_{K+1} \leq I(X_{\mathcal{S}}, X_{K+1}; Y|X_{\overline{\mathcal{S}}}) - I(X_{K+1}; Z), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi, \mathcal{S}' = \phi, \tag{96a}$$

$$\sum_{k \in \mathcal{S}} R^{\text{s}}_k + \sum_{k \in \mathcal{S} \backslash \mathcal{S}'} R^{\text{o}}_k + R^{\text{s}}_{K+1} \leq I(X_{\mathcal{S}}, X_{K+1}; Y|X_{\overline{\mathcal{S}}}) - I(X_{\mathcal{S}'}; Z) - I(X_{K+1}; Z),$$

$$\forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi, \mathcal{S}' \subseteq \mathcal{S}, \mathcal{S}' \neq \phi. \tag{96b}$$

From (88), (95a), and (96a), it can be found that these inequalities can be integrated into one formula as follows

$$\sum_{k \in \mathcal{S}} R^{\text{s}}_k + \sum_{k \in \mathcal{S} \backslash \mathcal{S}'} R^{\text{o}}_k + R^{\text{s}}_{K+1} \leq I(X_{\mathcal{S}}, X_{K+1}; Y|X_{\overline{\mathcal{S}}}) - I(X_{\mathcal{S}'}, X_{K+1}; Z), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S}' \subseteq \mathcal{S}, \tag{97}$$

which is the same as (81c). Combining (84), (94), and (97), it is known that (81) or (79) has already been obtained. All the other inequalities resulted from the elimination procedure should be redundant if Lemma 1 is true. Hence, we have to prove that (96b) is redundant. Since X_{K+1} is independent of $X_{\mathcal{S}'}$, (88) can be rewritten and relaxed as follows

$$\sum_{k \in \mathcal{S}} R^{\text{s}}_k + \sum_{k \in \mathcal{S} \backslash \mathcal{S}'} R^{\text{o}}_k + R^{\text{s}}_{K+1}$$

$$\leq I(X_{\mathcal{S}}, X_{K+1}; Y|X_{\overline{\mathcal{S}}}) - I(X_{\mathcal{S}'}, X_{K+1}; Z)$$

$$\leq I(X_{\mathcal{S}}, X_{K+1}; Y|X_{\overline{\mathcal{S}}}) - I(X_{\mathcal{S}'}; Z) - I(X_{K+1}; Z), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi, \mathcal{S}' \subseteq \mathcal{S}, \mathcal{S}' \neq \phi, \tag{98}$$

where the second inequality is the upper bound in (96b). This indicates that (88) sets a tighter upper bond on $\sum_{k \in \mathcal{S}} R^{\text{s}}_k + \sum_{k \in \mathcal{S} \backslash \mathcal{S}'} R^{\text{o}}_k + R^{\text{s}}_{K+1}$ than (96b). Since (88) is included in (97) or (81c), (96b) is thus redundant.

Finally, we compare (91) with (92c), which results in

$$\sum_{k \in \mathcal{S}} R_k^{\text{s}} + \sum_{k \in \mathcal{S} \setminus \mathcal{S}'} R_k^{\text{o}} + R_{K+1}^{\text{s}} \leq I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}, X_{K+1}) + I(X_{K+1}; Y | X_{\mathcal{K}}) - I(X_{\mathcal{S}'}, X_{K+1}; Z),$$

$$\forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi, \mathcal{S}' \subseteq \mathcal{S}, \mathcal{S}' \neq \phi, \tag{99a}$$

$$\sum_{k \in \mathcal{S}} R_k^{\text{s}} + \sum_{k \in \mathcal{S} \setminus \mathcal{S}'} R_k^{\text{o}} + \sum_{k \in \mathcal{S}_1} R_k^{\text{s}} + \sum_{k \in \mathcal{S}_1 \setminus \mathcal{S}_1'} R_k^{\text{o}} + R_{K+1}^{\text{s}} \leq I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}, X_{K+1}) - I(X_{\mathcal{S}'}, X_{K+1}; Z)$$

$$+ I(X_{\mathcal{S}_1}, X_{K+1}; Y | X_{\overline{\mathcal{S}_1}}) - I(X_{\mathcal{S}_1'}; Z), \forall \mathcal{S}, \mathcal{S}_1 \subseteq \mathcal{K}, \mathcal{S}, \mathcal{S}_1 \neq \phi, \mathcal{S}' \subseteq \mathcal{S}, \mathcal{S}' \neq \phi, \mathcal{S}_1' \subseteq \mathcal{S}_1. \tag{99b}$$

Note that when comparing (91b) with (92c), which gives (99b), we replace notations $\mathcal{S}$ and $\mathcal{S}'$ in (91b) with $\mathcal{S}_1$ and $\mathcal{S}_1'$, respectively, to avoid ambiguity. As stated after after (97), (99a) and (99b) should be redundant if Lemma 1 is true. We prove the redundancy in the following.

We first prove that (99a) is redundant. Since $X_k, \forall k \in \mathcal{K} \cup \{K+1\}$ are independent of each other and $\overline{\mathcal{S}} \subseteq \mathcal{K}$, we have

$$I(X_{\mathcal{S}}, X_{K+1}; Y | X_{\overline{\mathcal{S}}}) - I(X_{\mathcal{S}'}, X_{K+1}; Z)$$

$$= I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}) + I(X_{K+1}; Y | X_{\mathcal{K}}) - I(X_{\mathcal{S}'}, X_{K+1}; Z)$$

$$\leq I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}, X_{K+1}) + I(X_{K+1}; Y | X_{\mathcal{K}}) - I(X_{\mathcal{S}'}, X_{K+1}; Z), \forall \mathcal{S} \subseteq \mathcal{K}, \mathcal{S} \neq \phi, \mathcal{S}' \subseteq \mathcal{S}, \mathcal{S}' \neq \phi. \tag{100}$$

By replacing the corresponding terms in (98) with (100), the redundancy of (99a) can be similarly proven as that of (96b). Since the redundancy proof of (99b) is much more complicated than that of (96b) and (99a), for the sake of clarity, we give the proof in the following separate subsection.

C. Redundancy Proof of (99b)

Note that the redundancy of an inequality can be proven by showing that this inequality or a tighter bound can be obtained by linearly combining other inequalities. The most important step in the proof is to know how to divide the sum rate, which in our case is the left-hand-side term of (99b), into several terms such that combining upper bounds on these terms, we can get either (99b) or a tighter bound. Now we show how to do this. We first rewrite the left-hand-side term of (99b) as follows

$$\underbrace{\sum_{k \in \mathcal{S}} R_k^{\text{s}} + \sum_{k \in \mathcal{S} \setminus \mathcal{S}'} R_k^{\text{o}}}_{\text{Term } a} + \underbrace{\sum_{k \in \mathcal{S}_1} R_k^{\text{s}} + \sum_{k \in \mathcal{S}_1 \setminus \mathcal{S}_1'} R_k^{\text{o}} + R_{K+1}^{\text{s}}}_{\text{Term } b}, \tag{101}$$

which contains Term a and Term b. Note that adding the upper bounds on Term a and Term b cannot prove the redundancy. Therefore, we have to divide (101) into several other terms. We
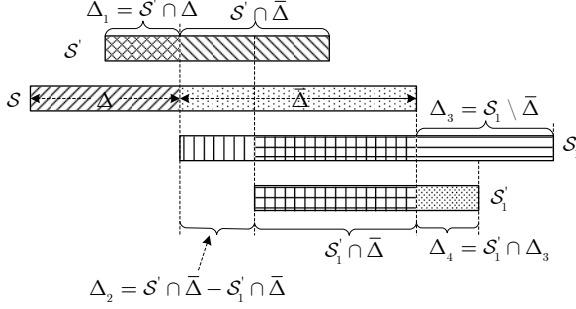
Fig. 14. Sets $\mathcal{S}$, $\mathcal{S}'$, $\mathcal{S}_1$, $\mathcal{S}'_1$, and their divisions.
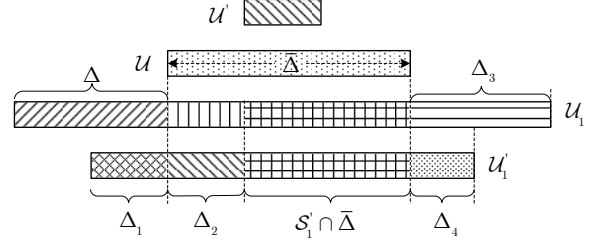
Fig. 15. Sets $\mathcal{U}, \mathcal{U}', \mathcal{U}_1, \mathcal{U}'_1$ obtained from $\mathcal{S}, \mathcal{S}', \mathcal{S}_1, \mathcal{S}'_1$ based on Criteria $1 \sim 5$.

show that it is enough for the proof to divide (101) into two terms. In particular, we exchange the message rates R^{s}_k and R^{o}_k in Term a and Term b, and obtain two new terms, i.e., Term a' and Term b', whose upper bounds then help prove the redundancy. We set the following criteria for the exchange process.

- Criterion 1. Term b' contains as many secret message rates R^{s}_k as possible;
- Criterion 2. Term a' contains as many open message rates R^{o}_k as possible;
- Criterion 3. Criterion 1 has a higher priority than Criterion 2;
- Criterion 4. For any k, there could be only one R^{s}_k or R^{o}_k in Term a' or Term b';
- Criterion 5. For any k, if R^{s}_k is not in Term a' or Term b', R^{o}_k cannot be in this term.

For ease of understanding, we give an example system with $\mathcal{K} = \{1, 2, 3, 4\}$, $\mathcal{S} = \{1, 3, 4\}$, $\mathcal{S}' = \{4\}$, $\mathcal{S}_1 = \{1, 2, 4\}$, and $\mathcal{S}'_1 = \phi$. In this case, (101) takes on form

$$\underbrace{R^{\mathrm{s}}_1 + R^{\mathrm{o}}_1 + R^{\mathrm{s}}_3 + R^{\mathrm{o}}_3 + R^{\mathrm{s}}_4}_{\text{Term } a} + \underbrace{R^{\mathrm{s}}_1 + R^{\mathrm{o}}_1 + R^{\mathrm{s}}_2 + R^{\mathrm{o}}_2 + R^{\mathrm{s}}_4 + R^{\mathrm{o}}_4 + R^{\mathrm{s}}_5}_{\text{Term } b}. \tag{102}$$

Since R^{s}_3 is not included in Term b, according to Criterion 1 and Criterion 3, R^{s}_3 should be moved into Term b. Note that R^{o}_3 has also to be moved into Term b since otherwise Criterion 5 is violated. Since both Term a and Term b contain R^{s}_4, while only Term b contains R^{o}_4, according to Criterion 2, R^{o}_4 should be moved into Term a. Note that we may not move R^{o}_1 in Term b into Term a since otherwise Criterion 4 is violated, and may not move R^{o}_2 into Term a since otherwise Criterion 5 is violated. With these operations, (102) becomes

$$\underbrace{R^{\mathrm{s}}_1 + R^{\mathrm{o}}_1 + R^{\mathrm{s}}_4 + R^{\mathrm{o}}_4}_{\text{Term } a'} + \underbrace{R^{\mathrm{s}}_1 + R^{\mathrm{o}}_1 + R^{\mathrm{s}}_2 + R^{\mathrm{o}}_2 + R^{\mathrm{s}}_3 + R^{\mathrm{o}}_3 + R^{\mathrm{s}}_4 + R^{\mathrm{s}}_5}_{\text{Term } b'}. \tag{103}$$

In the following, we first describe these operations mathematically and then prove the redundancy of (99b). For convenience, we give an example of sets $\mathcal{S}$, $\mathcal{S}'$, $\mathcal{S}_1$, $\mathcal{S}'_1$, and their divisions

in Fig. 14. Let $\overline{\Delta}$ denote the set of user indexes which are in both $\mathcal{S}$ and $\mathcal{S}_1$, and Δ denote the set of indexes which are in $\mathcal{S}$ but not in $\mathcal{S}_1$, i.e.,

$$\overline{\Delta} = \mathcal{S} \cap \mathcal{S}_1,$$

$$\Delta = \mathcal{S} - \mathcal{S}_1. \tag{104}$$

Let Δ_1 denote the intersection of $\mathcal{S}'$ and Δ, and Δ_2 denote the set of user indexes which are in $\mathcal{S}' \cap \overline{\Delta}$ but not in $\mathcal{S}_1' \cap \overline{\Delta}$, i.e.,

$$\Delta_1 = \mathcal{S}' \cap \Delta,$$

$$\Delta_2 = \mathcal{S}' \cap \overline{\Delta} - \mathcal{S}_1' \cap \overline{\Delta}. \tag{105}$$

With the operations described above, let $\mathcal{U}$, $\mathcal{U}'$, $\mathcal{U}_1$, and $\mathcal{U}_1'$, which respectively correspond to $\mathcal{S}$, $\mathcal{S}'$, $\mathcal{S}_1$, and $\mathcal{S}_1'$ in (101), denote the user indexes in Term a' and Term b'. Then, according to Criterion 1,

$$\mathcal{U} = \mathcal{S} \setminus \Delta,$$

$$\mathcal{U}_1 = \mathcal{S}_1 \cup \Delta. \tag{106}$$

The complementary sets of $\mathcal{U}$ and $\mathcal{U}_1$ are

$$\overline{\mathcal{U}} = \mathcal{K} \setminus (\mathcal{S} \setminus \Delta)$$

$$= \overline{\mathcal{S}} \cup \Delta,$$

$$\overline{\mathcal{U}_1} = \mathcal{K} \setminus (\mathcal{S}_1 \cup \Delta)$$

$$= \overline{\mathcal{S}_1} \setminus \Delta, \tag{107}$$

where $\overline{\mathcal{S}} = \mathcal{K} \setminus \mathcal{S}$ and $\overline{\mathcal{S}_1} = \mathcal{K} \setminus \mathcal{S}_1$. Moreover, according to Criterion 2, Criterion 4, and Criterion 5, we have

$$\mathcal{U}' = \mathcal{S}' \setminus (\Delta_1 \cup \Delta_2),$$

$$\mathcal{U}_1' = \mathcal{S}_1' \cup (\Delta_1 \cup \Delta_2). \tag{108}$$

Fig. 15 depicts the sets $\mathcal{U}, \mathcal{U}', \mathcal{U}_1, \mathcal{U}_1'$ obtained from $\mathcal{S}, \mathcal{S}', \mathcal{S}_1, \mathcal{S}_1'$ in Fig. 14. We thus have

$$
\underbrace{\sum_{k \in \mathcal{S}} R_k^{\mathrm{s}} + \sum_{k \in \mathcal{S} \setminus \mathcal{S}'} R_k^{\mathrm{o}}}_{\text{Term } a} + \underbrace{\sum_{k \in \mathcal{S}_1} R_k^{\mathrm{s}} + \sum_{k \in \mathcal{S}_1 \setminus \mathcal{S}_1'} R_k^{\mathrm{o}} + R_{K+1}^{\mathrm{s}}}_{\text{Term } b}
$$

$$
= \underbrace{\sum_{k \in \mathcal{U}} R_k^{\mathrm{s}} + \sum_{k \in \mathcal{U} \setminus \mathcal{U}'} R_k^{\mathrm{o}}}_{\text{Term } a'} + \underbrace{\sum_{k \in \mathcal{U}_1} R_k^{\mathrm{s}} + \sum_{k \in \mathcal{U}_1 \setminus \mathcal{U}_1'} R_k^{\mathrm{o}} + R_{K+1}^{\mathrm{s}}}_{\text{Term } b'}
$$

$$
\leq I(X_{\mathcal{U}}; Y | X_{\overline{\mathcal{U}}}, X_{K+1}) - I(X_{\mathcal{U}'}; Z) + I(X_{\mathcal{U}_1}, X_{K+1}; Y | X_{\overline{\mathcal{U}_1}}) - I(X_{\mathcal{U}_1'}, X_{K+1}; Z)
$$

$$
= I(X_{\mathcal{S}} \setminus X_{\Delta}; Y | X_{\overline{\mathcal{S}}}, X_{\Delta}, X_{K+1}) - I(X_{\mathcal{S}'} \setminus X_{\Delta_1 \cup \Delta_2}; Z)
$$

$$
+ I(X_{\mathcal{S}_1}, X_{\Delta}, X_{K+1}; Y | X_{\overline{\mathcal{S}_1}} \setminus X_{\Delta}) - I(X_{\mathcal{S}_1'}, X_{\Delta_1}, X_{\Delta_2}, X_{K+1}; Z),
$$

$$
\forall \mathcal{S}, \mathcal{S}_1 \subseteq \mathcal{K}, \mathcal{S}, \mathcal{S}_1 \neq \phi, \mathcal{S}' \subseteq \mathcal{S}, \mathcal{S}' \neq \phi, \mathcal{S}_1' \subseteq \mathcal{S}_1, \tag{109}
$$

where the inequality results from (84) and (97). On the other hand, based on the definitions of Δ, Δ_1, and Δ_2, and the chain rule of mutual information, (99b) can be rewritten as follows

$$
\sum_{k \in \mathcal{S}} R_k^{\mathrm{s}} + \sum_{k \in \mathcal{S} \setminus \mathcal{S}'} R_k^{\mathrm{o}} + \sum_{k \in \mathcal{S}_1} R_k^{\mathrm{s}} + \sum_{k \in \mathcal{S}_1 \setminus \mathcal{S}_1'} R_k^{\mathrm{o}} + R_{K+1}^{\mathrm{s}}
$$

$$
\leq I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}, X_{K+1}) - I(X_{\mathcal{S}'}, X_{K+1}; Z) + I(X_{\mathcal{S}_1}, X_{K+1}; Y | X_{\overline{\mathcal{S}_1}}) - I(X_{\mathcal{S}_1'}; Z)
$$

$$
= I(X_{\mathcal{S}} \setminus X_{\Delta}, X_{\Delta}; Y | X_{\overline{\mathcal{S}}}, X_{K+1}) - I(X_{\mathcal{S}'} \setminus X_{\Delta_1 \cup \Delta_2}, X_{\Delta_1 \cup \Delta_2}, X_{K+1}; Z)
$$

$$
+ I(X_{\mathcal{S}_1}, X_{K+1}; Y | X_{\overline{\mathcal{S}_1}}) - I(X_{\mathcal{S}_1'}; Z)
$$

$$
= I(X_{\mathcal{S}} \setminus X_{\Delta}; Y | X_{\overline{\mathcal{S}}}, X_{\Delta}, X_{K+1}) + I(X_{\Delta}; Y | X_{\overline{\mathcal{S}}}, X_{K+1}) - I(X_{\mathcal{S}'} \setminus X_{\Delta_1 \cup \Delta_2}; Z)
$$

$$
- I(X_{\Delta_1}, X_{\Delta_2}, X_{K+1}; Z | X_{\mathcal{S}'} \setminus X_{\Delta_1 \cup \Delta_2}) + I(X_{\mathcal{S}_1}, X_{K+1}; Y | X_{\overline{\mathcal{S}_1}}) - I(X_{\mathcal{S}_1'}; Z),
$$

$$
\forall \mathcal{S}, \mathcal{S}_1 \subseteq \mathcal{K}, \mathcal{S}, \mathcal{S}_1 \neq \phi, \mathcal{S}' \subseteq \mathcal{S}, \mathcal{S}' \neq \phi, \mathcal{S}_1' \subseteq \mathcal{S}_1. \tag{110}
$$

In the following, we show that the upper bound in (109) is no larger and is thus tighter than that in (110). Then, (110) is redundant. Neglecting the common terms $I(X_{\mathcal{S}} \setminus X_{\Delta}; Y | X_{\overline{\mathcal{S}}}, X_{\Delta}, X_{K+1})$ and $I(X_{\mathcal{S}'} \setminus X_{\Delta_1 \cup \Delta_2}; Z)$ in (109) and (110), we prove

$$
I(X_{\mathcal{S}_1}, X_{\Delta}, X_{K+1}; Y | X_{\overline{\mathcal{S}_1}} \setminus X_{\Delta}) \leq I(X_{\Delta}; Y | X_{\overline{\mathcal{S}}}, X_{K+1}) + I(X_{\mathcal{S}_1}, X_{K+1}; Y | X_{\overline{\mathcal{S}_1}}), \tag{111}
$$

and

$$
I(X_{\mathcal{S}_1'}, X_{\Delta_1}, X_{\Delta_2}, X_{K+1}; Z) \geq I(X_{\Delta_1}, X_{\Delta_2}, X_{K+1}; Z | X_{\mathcal{S}'} \setminus X_{\Delta_1 \cup \Delta_2}) + I(X_{\mathcal{S}_1'}; Z). \tag{112}
$$

From the definitions of $\overline{\Delta}$ and Δ in (104), it is known that $\Delta \cap \overline{\Delta} = \phi$ and $\mathcal{S} = \Delta \cup \overline{\Delta}$. Hence,

$$\overline{\mathcal{S}} = \mathcal{K} \setminus \mathcal{S}$$
$$= (\mathcal{K} \setminus \overline{\Delta}) \setminus \Delta. \tag{113}$$

Moreover, since $\overline{\Delta} \subseteq \mathcal{S}_1$,

$$\overline{\mathcal{S}_1} = \mathcal{K} \setminus \mathcal{S}_1$$
$$\subseteq \mathcal{K} \setminus \overline{\Delta}. \tag{114}$$

Based on (113) and (114), we have

$$\overline{\mathcal{S}_1} \setminus \Delta \subseteq (\mathcal{K} \setminus \overline{\Delta}) \setminus \Delta$$
$$= \overline{\mathcal{S}}. \tag{115}$$

Using the chain rule of mutual information, (115), and the fact that $X_k, \forall k \in \mathcal{K} \cup \{K+1\}$ are independent of each other, we have

$$I(X_{\mathcal{S}_1}, X_\Delta, X_{K+1}; Y | X_{\overline{\mathcal{S}_1}} \setminus X_\Delta) = I(X_\Delta; Y | X_{\overline{\mathcal{S}_1}} \setminus X_\Delta) + I(X_{\mathcal{S}_1}, X_{K+1}; Y | X_{\overline{\mathcal{S}_1}})$$
$$\leq I(X_\Delta; Y | X_{\overline{\mathcal{S}}}, X_{K+1}) + I(X_{\mathcal{S}_1}, X_{K+1}; Y | X_{\overline{\mathcal{S}_1}}). \tag{116}$$

The inequation (111) is thus true. On the other hand, since $\mathcal{S} = \Delta \cup \overline{\Delta}$, $\Delta \cap \overline{\Delta} = \phi$, and $\mathcal{S}' \subseteq \mathcal{S}$, as shown in Fig. 14, $\mathcal{S}'$ can be divided into two disjoint parts as follows

$$\mathcal{S}' = (\mathcal{S}' \cap \Delta) \cup (\mathcal{S}' \cap \overline{\Delta})$$
$$= \Delta_1 \cup (\mathcal{S}' \cap \overline{\Delta}), \tag{117}$$

where we used the definition of Δ_1 in (105). Hence,

$$\mathcal{S}' \cap \overline{\Delta} = \mathcal{S}' \setminus \Delta_1. \tag{118}$$

Let Δ_3 denote the set of user indexes which are in $\mathcal{S}_1$ but not in $\mathcal{S}$, and Δ_4 denote the intersection of $\mathcal{S}'_1$ and Δ_3, i.e.,

$$\Delta_3 = \mathcal{S}_1 - \mathcal{S}$$
$$= \mathcal{S}_1 \setminus \overline{\Delta},$$
$$\Delta_4 = \mathcal{S}'_1 \cap \Delta_3. \tag{119}$$

It can then be similarly proven as (118) that

$$\mathcal{S}_1' \cap \overline{\Delta} = \mathcal{S}_1' \setminus \Delta_4, \tag{120}$$

which can also be found from Fig. 14. From (118), (120), and the definition of Δ_2 in (105), $\mathcal{S}'$ in (117) can be further divided into three disjoint parts as follows

$$\begin{aligned}
\mathcal{S}' &= \Delta_1 \cup (\mathcal{S}' \cap \overline{\Delta}) \\
&= \Delta_1 \cup \Delta_2 \cup \left[(\mathcal{S}' \cap \overline{\Delta}) \cap (\mathcal{S}_1' \cap \overline{\Delta}) \right] \\
&= \Delta_1 \cup \Delta_2 \cup \left[(\mathcal{S}' \setminus \Delta_1) \cap (\mathcal{S}_1' \setminus \Delta_4) \right] \\
&= \Delta_1 \cup \Delta_2 \cup (\mathcal{S}' \cap \mathcal{S}_1'),
\end{aligned} \tag{121}$$

where the last step holds since $\Delta_1 \cap \Delta_4 = \phi$. Accordingly, we have

$$\begin{aligned}
\mathcal{S}' \setminus (\Delta_1 \cup \Delta_2) &= \mathcal{S}' \cap \mathcal{S}_1' \\
&\subseteq \mathcal{S}_1'.
\end{aligned} \tag{122}$$

Then, using the chain rule of mutual information, (122), and the fact that $X_k, \forall k \in \mathcal{K} \cup \{K+1\}$ are independent of each other, we have

$$\begin{aligned}
I(X_{\mathcal{S}_1'}, X_{\Delta_1}, X_{\Delta_2}, X_{K+1}; Z) &= I(X_{\Delta_1}, X_{\Delta_2}, X_{K+1}; Z | X_{\mathcal{S}_1'}) + I(X_{\mathcal{S}_1'}; Z) \\
&\geq I(X_{\Delta_1}, X_{\Delta_2}, X_{K+1}; Z | X_{\mathcal{S}'} \setminus X_{\Delta_1 \cup \Delta_2}) + I(X_{\mathcal{S}_1'}; Z),
\end{aligned} \tag{123}$$

i.e., (112) is true. Combining (109), (110), (116), and (123), it is known that (99b) is redundant.

So far we have shown that (79) (or (81)) can be obtained by eliminating $R_k^{\mathrm{a}}, \forall k \in \mathcal{K} \cup \{K+1\}$ in (80) (or (82)), and all the other inequalities resulted from the elimination procedure, i.e., (96b), (99a), and (99b), are redundant. As a result, (79) is the projection of (80) onto the hyperplane $\{R_k^{\mathrm{a}} = 0, \forall k \in \mathcal{K} \cup \{K+1\}\}$. Lemma 1 is thus proven.

APPENDIX B

PROOF OF THEOREM 1

Since $\overline{\mathcal{K}'}$ has $2^{|\overline{\mathcal{K}'}|}$ subsets, we may divide the inequality system (5) into $2^{|\overline{\mathcal{K}'}|}$ subsystems with each one corresponding to a subset $\mathcal{T} \subseteq \overline{\mathcal{K}'}$. For any $\mathcal{T} \subseteq \overline{\mathcal{K}'}$, the inequality subsystem is

$$\begin{cases}
R_k^{\mathrm{a}} \geq 0, \forall k \in \mathcal{K}', \\
\sum_{k \in \mathcal{S}} (R_k^{\mathrm{s}} + R_k^{\mathrm{o}} + R_k^{\mathrm{a}}) + \sum_{k \in \mathcal{T}} R_k^{\mathrm{o}} \leq I(X_{\mathcal{S}}, X_{\mathcal{T}}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}), \forall \mathcal{S} \subseteq \mathcal{K}', \\
\sum_{k \in \mathcal{S}} (R_k^{\mathrm{o}} + R_k^{\mathrm{a}}) \geq I(X_{\mathcal{S}}; Z | X_{\overline{\mathcal{K}'}}), \forall \mathcal{S} \subseteq \mathcal{K}'.
\end{cases} \tag{124}$$

It is obvious that eliminating $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}'$ in (5) is equivalent to eliminating $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}'$ in (124) for all $\mathcal{T} \subseteq \overline{\mathcal{K}'}$. Due to the assumption $I(X_{\mathcal{S}}; Y|X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) \geq I(X_{\mathcal{S}}; Z|X_{\overline{\mathcal{K}'}}), \forall \mathcal{S} \subseteq \mathcal{K}'$ made in Theorem 1, for a given $\mathcal{T} \subseteq \overline{\mathcal{K}'}$, we have

$$I(X_{\mathcal{S}}, X_{\mathcal{T}}; Y|X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}) \geq I(X_{\mathcal{S}}; Y|X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}})$$

$$\geq I(X_{\mathcal{S}}; Z|X_{\overline{\mathcal{K}'}}), \forall \mathcal{S} \subseteq \mathcal{K}'. \tag{125}$$

Then, by replacing $I(X_{\mathcal{S}}; Y|X_{\overline{\mathcal{S}}})$ in (10) with $I(X_{\mathcal{S}}, X_{\mathcal{T}}; Y|X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}) - \sum_{k \in \mathcal{T}} R_k^{\mathrm{o}}$ and $I(X_{\mathcal{S}}; Z)$ with $I(X_{\mathcal{S}}; Z|X_{\overline{\mathcal{K}'}})$, we can eliminate $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}'$ in (124) based on Lemma 1 and get

$$\sum_{k \in \mathcal{S}} R_k^{\mathrm{s}} + \sum_{k \in \mathcal{S} \setminus \mathcal{S}'} R_k^{\mathrm{o}} \leq I(X_{\mathcal{S}}, X_{\mathcal{T}}; Y|X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}) - \sum_{k \in \mathcal{T}} R_k^{\mathrm{o}} - I(X_{\mathcal{S}'}; Z|X_{\overline{\mathcal{K}'}}), \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S}' \subseteq \mathcal{S}. \tag{126}$$

Combining the inequalities (126) for all $\mathcal{T} \subseteq \overline{\mathcal{K}'}$, (4) can be obtained, and Theorem 1 is thus proven.

APPENDIX C

PROOF OF THEOREM 2

For notational convenience, in this appendix, we use $p(\cdot)$ to denote the probability of a variable's realization. For example, in the following formulas (129) and (130),

$$p(x_{\overline{\mathcal{K}'}}^n) = \Pr\left\{X_{\overline{\mathcal{K}'}}^n = x_{\overline{\mathcal{K}'}}^n\right\},$$

$$p(c_{\mathcal{K}'}) = \Pr\left\{\mathcal{C}_{\mathcal{K}'} = c_{\mathcal{K}'}\right\}. \tag{127}$$

In addition, if not specified, the realization of a variable in a $\sum$ or $\prod$ operator takes values from the set consisting of all possible values. For example, in (129c),

$$x_{\overline{\mathcal{K}'}}^n \in \prod_{k \in \overline{\mathcal{K}'}} \mathcal{X}_k^n \text{ and } z^n \in \mathcal{Z}^n. \tag{128}$$

Now we prove Theorem 2. First, the left-hand-side term of (15) can be rewritten as

$$\mathbb{E}\left\|P_{Z^n}(\cdot|\mathcal{C}_{\mathcal{K}}) - P_{Z^n}(\cdot|\mathcal{C}_{\overline{\mathcal{K}'}})\right\|_1 \overset{(a)}{=} \mathbb{E}\left\|P_{Z^n}(\cdot|\mathcal{C}_{\mathcal{K}'}, X_{\overline{\mathcal{K}'}}^n) - P_{Z^n}(\cdot|X_{\overline{\mathcal{K}'}}^n)\right\|_1$$

$$= \sum_{x_{\overline{\mathcal{K}'}}^n} p(x_{\overline{\mathcal{K}'}}^n) \mathbb{E}\left\|P_{Z^n}(\cdot|\mathcal{C}_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n) - P_{Z^n}(\cdot|x_{\overline{\mathcal{K}'}}^n)\right\|_1$$

$$\overset{(b)}{=} \sum_{x_{\overline{\mathcal{K}'}}^n} p(x_{\overline{\mathcal{K}'}}^n) \mathbb{E}\left\|P_{Z^n}(\cdot|\mathcal{C}_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n) - \mathbb{E}\left[P_{Z^n}(\cdot|\mathcal{C}_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)\right]\right\|_1$$

$$\overset{(c)}{=} \sum_{x_{\overline{\mathcal{K}'}}^n, z^n} p(x_{\overline{\mathcal{K}'}}^n) \mathbb{E}\left|P_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n) - \mathbb{E}\left[P_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)\right]\right|, \tag{129}$$

where (129a) holds since $Q_k = 0, \forall k \in \overline{\mathcal{K}'}$ and each codebook $\mathcal{C}_k, \forall k \in \overline{\mathcal{K}'}$ thus has only one codeword X_k^n, (129b) holds since

$$\mathbb{E}\left[P_{Z^n}(\cdot|\mathcal{C}_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)\right] = \sum_{c_{\mathcal{K}'}} p(c_{\mathcal{K}'}) P_{Z^n}(\cdot|c_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)$$

$$= \sum_{c_{\mathcal{K}'}} P_{Z^n}(\cdot, c_{\mathcal{K}'}|x_{\overline{\mathcal{K}'}}^n)$$

$$= P_{Z^n}(\cdot|x_{\overline{\mathcal{K}'}}^n), \tag{130}$$

and (129c) uses the definition of total variational distance. Since (see the definition in (11))

$$P_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n) = 2^{-n\sum_{k\in\mathcal{K}'} Q_k} \sum_{m_{\mathcal{K}'}\in\prod_{k\in\mathcal{K}'} \mathcal{M}_k} P_{Z^n}(z^n|\{X_k^n(m_k)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n), \tag{131}$$

we divide it into two parts as follows based on whether $\{X_k^n(m_k)\}_{k\in\mathcal{K}'}$, $x_{\overline{\mathcal{K}'}}^n$, and z^n are jointly typical or not

$$\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n) = 2^{-n\sum_{k\in\mathcal{K}'} Q_k} \sum_{m_{\mathcal{K}'}\in\prod_{k\in\mathcal{K}'} \mathcal{M}_k} \left\{ P_{Z^n}(z^n|\{X_k^n(m_k)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n) \right.$$

$$\left. \times O(\{X_k^n(m_k)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n) \right\},$$

$$\tilde{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n) = 2^{-n\sum_{k\in\mathcal{K}'} Q_k} \sum_{m_{\mathcal{K}'}\in\prod_{k\in\mathcal{K}'} \mathcal{M}_k} \left\{ P_{Z^n}(z^n|\{X_k^n(m_k)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n) \right.$$

$$\left. \times \tilde{O}(\{X_k^n(m_k)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n) \right\}, \tag{132}$$

where

$$O(\{X_k^n(m_k)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n) = \begin{cases} 1, & \text{if } (\{X_k^n(m_k)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n) \in \mathcal{T}_\epsilon^{(n)}, \\ 0, & \text{otherwise}, \end{cases} \tag{133}$$

$$\tilde{O}(\{X_k^n(m_k)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n) = \begin{cases} 1, & \text{if } (\{X_k^n(m_k)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n) \notin \mathcal{T}_\epsilon^{(n)}, \\ 0, & \text{otherwise}. \end{cases} \tag{134}$$

Using (132) and the triangular inequality, (129) can be upper bounded as follows

$$\mathbb{E}\|P_{Z^n}(\cdot|\mathcal{C}_{\mathcal{K}}) - P_{Z^n}(\cdot|\mathcal{C}_{\overline{\mathcal{K}'}})\|_1 \leq \sum_{x_{\overline{\mathcal{K}'}}^n, z^n} p(x_{\overline{\mathcal{K}'}}^n) \mathbb{E}\left|\tilde{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n) - \mathbb{E}\left[\tilde{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)\right]\right|$$

$$+ \sum_{(x_{\overline{\mathcal{K}'}}^n, z^n)\in\mathcal{T}_\epsilon^{(n)}} p(x_{\overline{\mathcal{K}'}}^n) \mathbb{E}\left|\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n) - \mathbb{E}\left[\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)\right]\right|. \tag{135}$$

Now we further upper bound (135) by separately evaluating its two summation terms. First,

$$\sum_{x^n_{\overline{\mathcal{K}'}}, z^n} p(x^n_{\overline{\mathcal{K}'}}) \mathbb{E}\left|\tilde{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}) - \mathbb{E}\left[\tilde{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})\right]\right|$$

$$\leq 2\sum_{x^n_{\overline{\mathcal{K}'}}, z^n} p(x^n_{\overline{\mathcal{K}'}})\mathbb{E}\left[\tilde{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})\right]$$

$$= 2\sum_{x^n_{\overline{\mathcal{K}'}}, z^n} p(x^n_{\overline{\mathcal{K}'}}) 2^{-n\sum_{k\in\mathcal{K}'} Q_k} \sum_{m_{\mathcal{K}'}\in\prod_{k\in\mathcal{K}'}\mathcal{M}_k} \mathbb{E}\left[P_{Z^n}(z^n|\{X^n_k(m_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})\tilde{O}(\{X^n_k(m_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}, z^n)\right]$$

$$\overset{(a)}{=} 2\sum_{x^n_{\overline{\mathcal{K}'}}, z^n} p(x^n_{\overline{\mathcal{K}'}})\mathbb{E}\left[P_{Z^n}(z^n|X^n_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})\tilde{O}(X^n_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}, z^n)\right]$$

$$\overset{(b)}{=} 2\sum_{(x^n_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}, z^n)\notin\mathcal{T}^{(n)}_\epsilon} p(x^n_{\mathcal{K}'})p(x^n_{\overline{\mathcal{K}'}})p(z^n|x^n_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})$$

$$= 2\sum_{(x^n_{\mathcal{K}}, z^n)\notin\mathcal{T}^{(n)}_\epsilon} p(x^n_{\mathcal{K}}, z^n)$$

$$= 2(1 - \Pr\{(x^n_{\mathcal{K}}, z^n)\in\mathcal{T}^{(n)}_\epsilon\})$$

$$\overset{(c)}{\leq} 4\prod_{k=1}^{K} |\mathcal{X}_k||\mathcal{Z}|e^{-n\epsilon^2\mu}, \tag{136}$$

where (136a) follows from the symmetry in codebook generation, (136b) holds due to (134), (136c) is obtained by using [46, Theorem 1.1], and μ is the smallest value of $p(x_{\mathcal{K}}, z)$. Note that in this appendix, we choose a sufficiently small ϵ such that $0 < \epsilon < \mu$.

Next, we evaluate the second summation term of (135). To this end, we first bound each expectation in the term. Specifically, for a given $(x^n_{\overline{\mathcal{K}'}}, z^n) \in \mathcal{T}^{(n)}_\epsilon$,

$$\mathbb{E}\left|\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}) - \mathbb{E}\left[\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})\right]\right| \leq \sqrt{\mathbb{E}\left[\left(\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}) - \mathbb{E}\left[\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})\right]\right)^2\right]}$$

$$= \sqrt{\mathrm{Var}\left(\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})\right)}, \tag{137}$$

where the first step holds since for a convex function $f(u) = u^2$, using Jensen's inequality, $(\mathbb{E}[u])^2 \leq \mathbb{E}[u^2]$. Using the definition of $\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})$, its variance in (137) can be computed

as (138) given below

$$\text{Var}\left(\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})\right)$$

$$=\mathbb{E}\left[\left(\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})\right)^2\right] - \left(\mathbb{E}\left[\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})\right]\right)^2$$

$$=2^{-2n\sum_{k\in\mathcal{K}'} Q_k}\left\{\mathbb{E}\left[\left(\sum_{m_{\mathcal{K}'}\in\prod_{k\in\mathcal{K}'}\mathcal{M}_k} P_{Z^n}(z^n|\{X^n_k(m_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})O(\{X^n_k(m_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}, z^n)\right)\right.\right.$$

$$\left.\times\left(\sum_{\hat{m}_{\mathcal{K}'}\in\prod_{k\in\mathcal{K}'}\mathcal{M}_k} P_{Z^n}(z^n|\{X^n_k(\hat{m}_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})O(\{X^n_k(\hat{m}_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}, z^n)\right)\right]$$

$$-\mathbb{E}\left[\sum_{m_{\mathcal{K}'}\in\prod_{k\in\mathcal{K}'}\mathcal{M}_k} P_{Z^n}(z^n|\{X^n_k(m_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})O(\{X^n_k(m_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}, z^n)\right]$$

$$\left.\times\mathbb{E}\left[\sum_{\hat{m}_{\mathcal{K}'}\in\prod_{k\in\mathcal{K}'}\mathcal{M}_k} P_{Z^n}(z^n|\{X^n_k(\hat{m}_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})O(\{X^n_k(\hat{m}_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}, z^n)\right]\right\}$$

$$=2^{-2n\sum_{k\in\mathcal{K}'} Q_k}\sum_{m_{\mathcal{K}'}}\sum_{\hat{m}_{\mathcal{K}'}}\left\{\mathbb{E}\left[P_{Z^n}(z^n|\{X^n_k(m_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})O(\{X^n_k(m_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}, z^n)\right.\right.$$

$$\left.\times\, P_{Z^n}(z^n|\{X^n_k(\hat{m}_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})O(\{X^n_k(\hat{m}_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}, z^n)\right]$$

$$-\mathbb{E}\left[P_{Z^n}(z^n|\{X^n_k(m_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})O(\{X^n_k(m_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}, z^n)\right]$$

$$\left.\times\mathbb{E}\left[P_{Z^n}(z^n|\{X^n_k(\hat{m}_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})O(\{X^n_k(\hat{m}_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}, z^n)\right]\right\}$$

$$=2^{-n\sum_{k\in\mathcal{K}'} Q_k}\sum_{\hat{m}_{\mathcal{K}'}}\left\{\mathbb{E}\left[P_{Z^n}(z^n|\{X^n_k(1)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})O(\{X^n_k(1)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}, z^n)\right.\right.$$

$$\left.\times\, P_{Z^n}(z^n|\{X^n_k(\hat{m}_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})O(\{X^n_k(\hat{m}_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}, z^n)\right]$$

$$-\mathbb{E}\left[P_{Z^n}(z^n|\{X^n_k(1)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})O(\{X^n_k(1)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}, z^n)\right]$$

$$\left.\times\mathbb{E}\left[P_{Z^n}(z^n|\{X^n_k(\hat{m}_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})O(\{X^n_k(\hat{m}_k)\}_{k\in\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}}, z^n)\right]\right\}, \tag{138}$$

in which the last step follows from the symmetry in codebook generation. Note that if none of $\hat{m}_k, \forall k \in \mathcal{K}'$ in (138) is 1, i.e.,

$$\hat{m}_k \neq 1, \forall k \in \mathcal{K}', \tag{139}$$

$\{X^n_k(\hat{m}_k)\}_{k\in\mathcal{K}'}$ is independent of $\{X^n_k(1)\}_{k\in\mathcal{K}'}$. In this case, the expectation difference in the

last step of (138) is 0, i.e.,

$$\mathbb{E}\left[P_{Z^n}(z^n|\{X_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)O(\{X_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n)\right.$$

$$\times \left. P_{Z^n}(z^n|\{X_k^n(\hat{m}_k)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)O(\{X_k^n(\hat{m}_k)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n)\right]$$

$$-\mathbb{E}\left[P_{Z^n}(z^n|\{X_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)O(\{X_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n)\right]$$

$$\times \mathbb{E}\left[P_{Z^n}(z^n|\{X_k^n(\hat{m}_k)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)O(\{X_k^n(\hat{m}_k)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n)\right] = 0. \qquad (140)$$

As a result, to evaluate (138), we only need to consider those $\hat{m}_{\mathcal{K}'} \in \prod_{k\in\mathcal{K}'}\mathcal{M}_k$ in which at least one $\hat{m}_k$ is 1, i.e., at least one user in $\mathcal{K}'$ transmits the first codeword. Let $\mathcal{A} \subsetneq \mathcal{K}'$ and $\overline{\mathcal{A}} = \mathcal{K}' \setminus \mathcal{A}$ denote sets of users which respectively satisfy

$$\hat{m}_k \neq 1, \forall k \in \mathcal{A},$$

$$\hat{m}_k = 1, \forall k \in \overline{\mathcal{A}}. \qquad (141)$$

Using (140) and (141), $\mathrm{Var}\left(\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)\right)$ in (138) can be upper bounded as

$$\mathrm{Var}\left(\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)\right)$$

$$=2^{-n\sum_{k\in\mathcal{K}'}Q_k}\sum_{\mathcal{A}\subsetneq\mathcal{K}'}\sum_{m_\mathcal{A}\in\prod_{k\in\mathcal{A}}\mathcal{M}_k\setminus\{1\}}\left\{\mathbb{E}\left[P_{Z^n}(z^n|\{X_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)O(\{X_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n)\right.\right.$$

$$\times \left. P_{Z^n}(z^n|\{X_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}, \{X_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n)O(\{X_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}, \{X_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n, z^n)\right]$$

$$- \mathbb{E}\left[P_{Z^n}(z^n|\{X_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)O(\{X_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n)\right]$$

$$\times \mathbb{E}\left.\left[P_{Z^n}(z^n|\{X_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}, \{X_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n)O(\{X_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}, \{X_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n, z^n)\right]\right\}$$

$$\leq 2^{-n\sum_{k\in\mathcal{K}'}Q_k}\sum_{\mathcal{A}\subsetneq\mathcal{K}'}\sum_{m_\mathcal{A}\in\prod_{k\in\mathcal{A}}\mathcal{M}_k\setminus\{1\}}\mathbb{E}\left[P_{Z^n}(z^n|\{X_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)O(\{X_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n)\right.$$

$$\times \left. P_{Z^n}(z^n|\{X_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}, \{X_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n)O(\{X_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}, \{X_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n, z^n)\right], \quad (142)$$

in which the last step holds since all non-negative subtrahends are omitted. We further bound

each expectation term in the last step of (142) as follows

$$\mathbb{E}\Big[P_{Z^n}(z^n|\{X_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)O(\{X_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n)$$

$$\times P_{Z^n}(z^n|\{X_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}, \{X_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n)O(\{X_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}, \{X_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n, z^n)\Big]$$

$$= \sum_{\substack{\{x_k^n(1)\}_{k\in\mathcal{K}'},\{x_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}:\\ (\{x_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n)\in\mathcal{T}_\epsilon^{(n)},\\ (\{x_k^n(\hat{m}_k)\}_{k\in\mathcal{A}},\{x_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n, z^n)\in\mathcal{T}_\epsilon^{(n)}}} \Big[p(\{x_k^n(1)\}_{k\in\mathcal{K}'})p(\{x_k^n(\hat{m}_k)\}_{k\in\mathcal{A}})p(z^n|\{x_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n)$$

$$\times p(z^n|\{x_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}, \{x_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n)\Big]$$

$$= \sum_{\substack{\{x_k^n(1)\}_{k\in\mathcal{K}'},\{x_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}:\\ (\{x_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n)\in\mathcal{T}_\epsilon^{(n)},\\ (\{x_k^n(\hat{m}_k)\}_{k\in\mathcal{A}},\{x_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n, z^n)\in\mathcal{T}_\epsilon^{(n)}}} p(\{x_k^n(1)\}_{k\in\mathcal{K}'}, z^n|x_{\overline{\mathcal{K}'}}^n)p(\{x_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}, z^n|\{x_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n)$$

$$\overset{(a)}{\leq} \sum_{\substack{\{x_k^n(1)\}_{k\in\mathcal{K}'}:\\ (\{x_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n)\in\mathcal{T}_\epsilon^{(n)}}} p(\{x_k^n(1)\}_{k\in\mathcal{K}'}, z^n|x_{\overline{\mathcal{K}'}}^n)\Bigg[\sum_{\{x_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}} p(\{x_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}, z^n|\{x_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n)\Bigg]$$

$$= \sum_{\substack{\{x_k^n(1)\}_{k\in\mathcal{K}'}:\\ (\{x_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n)\in\mathcal{T}_\epsilon^{(n)}}} p(\{x_k^n(1)\}_{k\in\mathcal{K}'}, z^n|x_{\overline{\mathcal{K}'}}^n)p(z^n|\{x_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n)$$

$$\overset{(b)}{\leq} 2^{-nH(Z|X_{\overline{\mathcal{A}}},X_{\overline{\mathcal{K}'}})(1-\epsilon)} \sum_{\{x_k^n(1)\}_{k\in\mathcal{K}'}} p(\{x_k^n(1)\}_{k\in\mathcal{K}'}, z^n|x_{\overline{\mathcal{K}'}}^n)$$

$$= 2^{-nH(Z|X_{\overline{\mathcal{A}}},X_{\overline{\mathcal{K}'}})(1-\epsilon)}p(z^n|x_{\overline{\mathcal{K}'}}^n)$$

$$\leq 2^{-n\big[H(Z|X_{\overline{\mathcal{K}'}})+H(Z|X_{\overline{\mathcal{A}}},X_{\overline{\mathcal{K}'}})\big](1-\epsilon)}, \tag{143}$$

where (143a) holds since in contrast to the previous step, $\{x_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}$ no longer has to satisfy $(\{x_k^n(\hat{m}_k)\}_{k\in\mathcal{A}}, \{x_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n, z^n) \in \mathcal{T}_\epsilon^{(n)}$, and (143b) holds since, on one hand, for any $(\{x_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n, z^n) \in \mathcal{T}_\epsilon^{(n)}$,

$$p(z^n|\{x_k^n(1)\}_{k\in\overline{\mathcal{A}}}, x_{\overline{\mathcal{K}'}}^n) \leq 2^{-nH(Z|X_{\overline{\mathcal{A}}},X_{\overline{\mathcal{K}'}})(1-\epsilon)}, \tag{144}$$

and on the other hand, $\{x_k^n(1)\}_{k\in\mathcal{K}'}$ no longer has to satisfy $(\{x_k^n(1)\}_{k\in\mathcal{K}'}, x_{\overline{\mathcal{K}'}}^n, z^n) \in \mathcal{T}_\epsilon^{(n)}$ as in

the previous step. Substituting (143) into (142), we have

$$\text{Var}\left(\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})\right) \le 2^{-n\sum_{k\in\mathcal{K}'}Q_k}\sum_{\substack{\mathcal{A}\subsetneq\mathcal{K}'}}\sum_{m_\mathcal{A}\in\prod_{k\in\mathcal{A}}\mathcal{M}_k\backslash\{1\}}2^{-n\left[H(Z|X_{\overline{\mathcal{K}'}})+H(Z|X_{\overline{\mathcal{A}}},X_{\overline{\mathcal{K}'}})\right](1-\epsilon)}$$

$$\overset{(a)}{=}\sum_{\substack{\mathcal{A}\subsetneq\mathcal{K}'}}\prod_{k\in\mathcal{A}}\left(2^{nQ_k}-1\right)2^{-n\left[\sum_{k\in\mathcal{K}'}Q_k+H(Z|X_{\overline{\mathcal{K}'}})+H(Z|X_{\overline{\mathcal{A}}},X_{\overline{\mathcal{K}'}})\right](1-\epsilon)}$$

$$\le\sum_{\substack{\mathcal{A}\subsetneq\mathcal{K}'}}2^{n\sum_{k\in\mathcal{A}}Q_k}2^{-n\left[\sum_{k\in\mathcal{K}'}Q_k+H(Z|X_{\overline{\mathcal{K}'}})+H(Z|X_{\overline{\mathcal{A}}},X_{\overline{\mathcal{K}'}})\right](1-\epsilon)}$$

$$=\sum_{\substack{\mathcal{A}\subsetneq\mathcal{K}'}}2^{-n\left[\sum_{k\in\overline{\mathcal{A}}}Q_k+H(Z|X_{\overline{\mathcal{K}'}})+H(Z|X_{\overline{\mathcal{A}}},X_{\overline{\mathcal{K}'}})\right](1-\epsilon)}, \tag{145}$$

where (145a) holds since for any $k\in\mathcal{A}$, $\hat{m}_k$ has $2^{nQ_k}-1$ possible values. Combining (137) and (145), we have

$$\mathbb{E}\left|\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})-\mathbb{E}\left[\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})\right]\right|\le\sqrt{\sum_{\substack{\mathcal{A}\subsetneq\mathcal{K}'}}2^{-n\left[\sum_{k\in\overline{\mathcal{A}}}Q_k+H(Z|X_{\overline{\mathcal{K}'}})+H(Z|X_{\overline{\mathcal{A}}},X_{\overline{\mathcal{K}'}})\right](1-\epsilon)}}$$

$$\le\sum_{\substack{\mathcal{A}\subsetneq\mathcal{K}'}}2^{-\frac{n}{2}\left[\sum_{k\in\overline{\mathcal{A}}}Q_k+H(Z|X_{\overline{\mathcal{K}'}})+H(Z|X_{\overline{\mathcal{A}}},X_{\overline{\mathcal{K}'}})\right](1-\epsilon)}. \tag{146}$$

Accordingly, the second summation term of (135) can be upper bounded as follows

$$\sum_{(x^n_{\overline{\mathcal{K}'}},z^n)\in\mathcal{T}_\epsilon^{(n)}}p(x^n_{\overline{\mathcal{K}'}})\mathbb{E}\left|\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})-\mathbb{E}\left[\hat{P}_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}'}, x^n_{\overline{\mathcal{K}'}})\right]\right|$$

$$\le 2^{nH(X_{\overline{\mathcal{K}'}},Z)(1+\epsilon)}2^{-nH(X_{\overline{\mathcal{K}'}})(1-\epsilon)}\sum_{\substack{\mathcal{A}\subsetneq\mathcal{K}'}}2^{-\frac{n}{2}\left[\sum_{k\in\overline{\mathcal{A}}}Q_k+H(Z|X_{\overline{\mathcal{K}'}})+H(Z|X_{\overline{\mathcal{A}}},X_{\overline{\mathcal{K}'}})\right](1-\epsilon)}$$

$$=\sum_{\substack{\mathcal{A}\subsetneq\mathcal{K}'}}2^{-\frac{n}{2}\left[\left(\sum_{k\in\overline{\mathcal{A}}}Q_k-I(X_{\overline{\mathcal{A}}};Z|X_{\overline{\mathcal{K}'}})\right)(1-\epsilon)-3\epsilon H(X_{\overline{\mathcal{K}'}},Z)\right]}. \tag{147}$$

For any $\mathcal{A}\subsetneq\mathcal{K}'$, we know that $\overline{\mathcal{A}}\subseteq\mathcal{K}'$ and $\overline{\mathcal{A}}\ne\phi$. Then, it is known from (14) that

$$\sum_{k\in\overline{\mathcal{A}}}Q_k-I(X_{\overline{\mathcal{A}}};Z|X_{\overline{\mathcal{K}'}})>0. \tag{148}$$

Since ϵ is an arbitrarily small positive number, we have

$$\left[\sum_{k\in\overline{\mathcal{A}}}Q_k-I(X_{\overline{\mathcal{A}}};Z|X_{\overline{\mathcal{K}'}})\right](1-\epsilon)-3\epsilon H(X_{\overline{\mathcal{K}'}},Z)>0. \tag{149}$$

Then, the upper bound (147) vanishes exponentially in n. Substituting (136) and (147) into (135), Theorem 2 can be proven.

APPENDIX D

PROOF OF THEOREM 4

We first prove (20). As we have shown in Lemma 2, if $R_k^o = 0, \forall k \in \mathcal{K}$, (17) becomes (19), which can be divided into

$$
\begin{cases}
R_k^s = 0, \forall k \in \overline{\mathcal{K}'}, \\
\sum_{k \in \mathcal{S}} R_k^s \leq [I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{S}}; Z | X_{\overline{\mathcal{K}'}})]^+, \forall \mathcal{S} \subsetneq \mathcal{K}',
\end{cases}
\tag{150}
$$

and

$$
\sum_{k \in \mathcal{K}'} R_k^s \leq [I(X_{\mathcal{K}'}; Y | X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}'}; Z | X_{\overline{\mathcal{K}'}})]^+.
\tag{151}
$$

(151) shows that for any rate-tuple in $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$, the sum secrecy rate $\sum_{k \in \mathcal{K}'} R_k^s$ is no larger than $[I(X_{\mathcal{K}'}; Y | X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}'}; Z | X_{\overline{\mathcal{K}'}})]^+$. We now show that this upper bound is achievable. To this end, we only need to prove that the inequality (151) is not redundant, i.e., any linear combination of inequalities in (150) does not generate (151) or a tighter upper bound to $\sum_{k \in \mathcal{K}'} R_k^s$. In [15, Appendix E], we have provided the proof for the case with $\mathcal{K}' = \mathcal{K}$. When $\mathcal{K}' \subsetneq \mathcal{K}$, we could complete the proof by following similar steps. We omit the details here for brevity. Note that for a given $\mathcal{K}' \subseteq \mathcal{K}$, $R_k^s = 0, \forall k \in \overline{\mathcal{K}'}$. Hence, the achievable upper bound on $\sum_{k \in \mathcal{K}} R_k^s$ given by (150) and (151) is $[I(X_{\mathcal{K}'}; Y | X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}'}; Z | X_{\overline{\mathcal{K}'}})]^+$. Then, considering all possible $\mathcal{K}' \subseteq \mathcal{K}$, the maximum achievable sum secrecy rate $\sum_{k \in \mathcal{K}} R_k^s$ is

$$
R^s(X_{\mathcal{K}}) = \max_{\mathcal{K}' \subseteq \mathcal{K}} \left\{ [I(X_{\mathcal{K}'}; Y | X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}'}; Z | X_{\overline{\mathcal{K}'}})]^+ \right\}.
\tag{152}
$$

(20) is thus true.

Let $\mathcal{K}'^*$ denote the subset in $\mathcal{K}$ which achieves (152) and assume

$$
I(X_{\mathcal{K}'^*}; Y | X_{\overline{\mathcal{K}'^*}}) - I(X_{\mathcal{K}'^*}; Z | X_{\overline{\mathcal{K}'^*}}) > 0,
\tag{153}
$$

since otherwise we have $R_k^s = 0, \forall k \in \mathcal{K}$, i.e., the system reduces to a standard DM-MAC channel with only open messages. Before proving the second part of Theorem 4, i.e., (21), we first show that with $\mathcal{K}'^*$ defined above, we have

$$
I(X_{\mathcal{S}}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'^*}}) - I(X_{\mathcal{S}}; Z | X_{\overline{\mathcal{K}'^*}}) \geq 0, \forall \mathcal{S} \subsetneq \mathcal{K}'^*.
\tag{154}
$$

(154) can be proven by reductio ad absurdum. If (154) is not true, then there exist subsets in $\mathcal{K}'^*$ such that the corresponding inequalities in (154) do not hold. W.l.o.g., we assume that there exists only one subset $\mathcal{S}_0$ in $\mathcal{K}'^*$ such that

$$
I(X_{\mathcal{S}_0}; Y | X_{\overline{\mathcal{S}_0}}, X_{\overline{\mathcal{K}'^*}}) - I(X_{\mathcal{S}_0}; Z | X_{\overline{\mathcal{K}'^*}}) < 0.
\tag{155}
$$

Using the chain rule of mutual information and the fact that $X_k, \forall k \in \mathcal{K}$ are independent of each other, the left-hand side term of (153) is upper bounded by

$$I(X_{\mathcal{K}'^*}; Y | X_{\overline{\mathcal{K}'^*}}) - I(X_{\mathcal{K}'^*}; Z | X_{\overline{\mathcal{K}'^*}})$$

$$=I(X_{\mathcal{K}'^* \setminus \mathcal{S}_0}, X_{\mathcal{S}_0}; Y | X_{\overline{\mathcal{K}'^*}}) - I(X_{\mathcal{K}'^* \setminus \mathcal{S}_0}, X_{\mathcal{S}_0}; Z | X_{\overline{\mathcal{K}'^*}})$$

$$=I(X_{\mathcal{K}'^* \setminus \mathcal{S}_0}; Y | X_{\mathcal{S}_0}, X_{\overline{\mathcal{K}'^*}}) - I(X_{\mathcal{K}'^* \setminus \mathcal{S}_0}; Z | X_{\overline{\mathcal{K}'^*}}) + I(X_{\mathcal{S}_0}; Y | X_{\overline{\mathcal{K}'^*}}) - I(X_{\mathcal{S}_0}; Z | X_{\mathcal{K}'^* \setminus \mathcal{S}_0}, X_{\overline{\mathcal{K}'^*}})$$

$$\leq I(X_{\mathcal{K}'^* \setminus \mathcal{S}_0}; Y | X_{\mathcal{S}_0}, X_{\overline{\mathcal{K}'^*}}) - I(X_{\mathcal{K}'^* \setminus \mathcal{S}_0}; Z | X_{\overline{\mathcal{K}'^*}}) + I(X_{\mathcal{S}_0}; Y | X_{\overline{\mathcal{S}_0}}, X_{\overline{\mathcal{K}'^*}}) - I(X_{\mathcal{S}_0}; Z | X_{\overline{\mathcal{K}'^*}})$$

$$<I(X_{\mathcal{K}'^* \setminus \mathcal{S}_0}; Y | X_{\mathcal{S}_0}, X_{\overline{\mathcal{K}'^*}}) - I(X_{\mathcal{K}'^* \setminus \mathcal{S}_0}; Z | X_{\overline{\mathcal{K}'^*}}), \tag{156}$$

where the last step holds due to (155). Then, $\mathcal{K}' = \mathcal{K}'^* \setminus \mathcal{S}_0$ and $\overline{\mathcal{K}'} = \overline{\mathcal{K}'^*} \cup \mathcal{S}_0$ result in a larger value in (152) than $\mathcal{K}'^*$, i.e., $R^{\mathrm{s}}(X_{\mathcal{K}})$ can be increased. This is contradicted to the assumption that $\mathcal{K}'^*$ achieves (152). When there are more subsets in $\mathcal{K}'^*$ such that the inequalities in (154) do not hold, we may prove by following similar steps that $R^{\mathrm{s}}(X_{\mathcal{K}})$ can be further increased. As a result, if $\mathcal{K}'^* \subseteq \mathcal{K}$ achieves (152) and (153) is true, we have (154).

Now we show that if users in $\mathcal{K}'^*$ transmit their confidential messages at sum rate $R^{\mathrm{s}}(X_{\mathcal{K}})$, the maximum achievable sum rate at which users in $\mathcal{K}$ could send their open messages is given by (21). We divide the users in $\mathcal{K}$ into two classes, i.e., $\mathcal{K}'^*$ and $\overline{\mathcal{K}'^*}$, and separately consider their maximum sum open message rate.

First, if $(\{R_k^{\mathrm{s}}, R_k^{\mathrm{o}}\}_{k \in \mathcal{K}'^*}, \{R_k^{\mathrm{s}} = 0, R_k^{\mathrm{o}}\}_{k \in \overline{\mathcal{K}'^*}})$ is a rate-tuple in region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}'^*)$ defined by Theorem 3 and $\sum_{k \in \mathcal{K}'^*} R_k^{\mathrm{s}} = R^{\mathrm{s}}(X_{\mathcal{K}})$, which is assumed to be positive, by setting $\mathcal{S} = \mathcal{K}'^*$, $\mathcal{S}' = \phi$, and $\mathcal{T} = \phi$ in (17), we get

$$\sum_{k \in \mathcal{K}'^*} R_k^{\mathrm{o}} \leq I(X_{\mathcal{K}'^*}; Y | X_{\overline{\mathcal{K}'^*}}) - R^{\mathrm{s}}(X_{\mathcal{K}}) = I(X_{\mathcal{K}'^*}; Z | X_{\overline{\mathcal{K}'^*}}), \tag{157}$$

indicating that the sum rate at which users in $\mathcal{K}'^*$ can encode their open messages is no larger than $I(X_{\mathcal{K}'^*}; Z | X_{\overline{\mathcal{K}'^*}})$. Then, we prove that this rate is achievable. Since the rate-tuple is in region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}'^*)$, with inequalities (153) and (154), we could use Theorem 1 and find $R_k^{\mathrm{a}}, \forall k \in \mathcal{K}'^*$ such that

$$\begin{cases} R_k^{\mathrm{a}} \geq 0, \forall k \in \mathcal{K}'^*, \\ \sum_{k \in \mathcal{S}} (R_k^{\mathrm{s}} + R_k^{\mathrm{o}} + R_k^{\mathrm{a}}) + \sum_{k \in \mathcal{T}} R_k^{\mathrm{o}} \leq I(X_{\mathcal{S}}, X_{\mathcal{T}}; Y | X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{T}}}), \forall \mathcal{S} \subseteq \mathcal{K}'^*, \mathcal{T} \subseteq \overline{\mathcal{K}'^*}, \\ \sum_{k \in \mathcal{S}} (R_k^{\mathrm{o}} + R_k^{\mathrm{a}}) \geq I(X_{\mathcal{S}}; Z | X_{\overline{\mathcal{K}'^*}}), \forall \mathcal{S} \subseteq \mathcal{K}'^*. \end{cases} \tag{158}$$

From (158) it is known that if $\sum_{k \in \mathcal{K}'^*} R_k^{\mathrm{o}} < I(X_{\mathcal{K}'^*}; Z | X_{\overline{\mathcal{K}'^*}})$, we can always split partial rate in R_k^{a} to R_k^{o}, and get $\hat{R}_k^{\mathrm{a}}$ as well as $\hat{R}_k^{\mathrm{o}}$, such that

$$\hat{R}_k^{\mathrm{a}} \geq 0, \forall k \in \mathcal{K}'^*,$$

$$\hat{R}_k^{\mathrm{o}} + \hat{R}_k^{\mathrm{a}} = R_k^{\mathrm{o}} + R_k^{\mathrm{a}}, \forall k \in \mathcal{K}'^*, \tag{159}$$

and

$$\sum_{k \in \mathcal{K}'^*} \hat{R}_k^{\mathrm{o}} = I(X_{\mathcal{K}'^*}; Z | X_{\overline{\mathcal{K}'^*}}). \tag{160}$$

With (159), it can be verified that the new rate-tuple $(\{R_k^{\mathrm{s}}, \hat{R}_k^{\mathrm{o}}, \hat{R}_k^{\mathrm{a}}\}_{k \in \mathcal{K}'^*}, \{R_k^{\mathrm{s}} = 0, R_k^{\mathrm{o}}\}_{k \in \overline{\mathcal{K}'^*}})$ is in the region defined by (158), i.e., it satisfies all inequalities in (158). Since $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}'^*)$ can be obtained by projecting (158) onto hyperplane $\{R_k^{\mathrm{a}} = 0, \forall k \in \mathcal{K}'^*\}$, then, according to the property of Fourier-Motzkin elimination [35, Appendix D], we know that rate-tuple $(\{R_k^{\mathrm{s}}, \hat{R}_k^{\mathrm{o}}\}_{k \in \mathcal{K}'^*}, \{R_k^{\mathrm{s}} = 0, R_k^{\mathrm{o}}\}_{k \in \overline{\mathcal{K}'^*}})$ is in region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}'^*)$. Due to (160), with this rate-tuple, users in $\mathcal{K}'^*$ could send their open messages at sum rate $I(X_{\mathcal{K}'^*}; Z | X_{\overline{\mathcal{K}'^*}})$.

So far we have shown that the maximum achievable sum secrecy rate is $R^{\mathrm{s}}(X_{\mathcal{K}})$, and if $\sum_{k \in \mathcal{K}'^*} R_k^{\mathrm{s}} = R^{\mathrm{s}}(X_{\mathcal{K}})$, the maximum achievable sum rate $\sum_{k \in \mathcal{K}'^*} R_k^{\mathrm{o}}$ is $I(X_{\mathcal{K}'^*}; Z | X_{\overline{\mathcal{K}'^*}})$. Now we show that if

$$\sum_{k \in \mathcal{K}'^*} R_k^{\mathrm{s}} = R^{\mathrm{s}}(X_{\mathcal{K}}),$$

$$\sum_{k \in \mathcal{K}'^*} R_k^{\mathrm{o}} = I(X_{\mathcal{K}'^*}; Z | X_{\overline{\mathcal{K}'^*}}), \tag{161}$$

the maximum achievable sum rate $\sum_{k \in \overline{\mathcal{K}'^*}} R_k^{\mathrm{o}}$ is $I(X_{\overline{\mathcal{K}'^*}}; Y)$. Setting $\mathcal{S} = \mathcal{K}'^*$, $\mathcal{S}' = \phi$, and $\mathcal{T} = \overline{\mathcal{K}'^*}$ in (17), we have

$$\sum_{k \in \overline{\mathcal{K}'^*}} R_k^{\mathrm{o}} \leq I(X_{\mathcal{K}'^*}, X_{\overline{\mathcal{K}'^*}}; Y) - \sum_{k \in \mathcal{K}'^*} (R_k^{\mathrm{s}} + R_k^{\mathrm{o}})$$

$$= I(X_{\mathcal{K}'^*}, X_{\overline{\mathcal{K}'^*}}; Y) - R^{\mathrm{s}}(X_{\mathcal{K}}) - I(X_{\mathcal{K}'^*}; Z | X_{\overline{\mathcal{K}'^*}})$$

$$= I(X_{\overline{\mathcal{K}'^*}}; Y). \tag{162}$$

Note that from the perspective of Bob, we are considering a DM-MAC channel with K users. Then, it is known from [35, Chapter 4] that (162) can hold with equality. This can be realized by letting Bob treat the signal of users in $\mathcal{K}'^*$ as noise and decode the information of users in $\overline{\mathcal{K}'^*}$. Hence, the maximum achievable sum rate at which users in $\overline{\mathcal{K}'^*}$ could send their open messages is $I(X_{\overline{\mathcal{K}'^*}}; Y)$. Combining (161) and (162) (with equality), it is known that (21) is true. Theorem 4 is thus proven.

APPENDIX E

PROOF OF THEOREM 5

We first prove (48). Using the chain rule of mutual information, the left-hand-side term of (46) is upper bounded by

$$I(X_{\mathcal{K}_0 \cup \mathcal{V}}; Y | X_{\mathcal{K}' \setminus (\mathcal{K}_0 \cup \mathcal{V})}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}_0 \cup \mathcal{V}}; Z | X_{\overline{\mathcal{K}'}})$$

$$=I(X_{\mathcal{K}_0}, X_{\mathcal{V}}; Y | X_{\mathcal{K}' \setminus (\mathcal{K}_0 \cup \mathcal{V})}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}_0}, X_{\mathcal{V}}; Z | X_{\overline{\mathcal{K}'}}) \tag{163a}$$

$$=I(X_{\mathcal{K}_0}; Y | X_{\mathcal{K}' \setminus \mathcal{K}_0}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}_0}; Z | X_{\overline{\mathcal{K}'}}) + I(X_{\mathcal{V}}; Y | X_{\mathcal{K}' \setminus (\mathcal{K}_0 \cup \mathcal{V})}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{V}}; Z | X_{\overline{\mathcal{K}'} \cup \mathcal{K}_0}) \tag{163b}$$

$$\leq I(X_{\mathcal{V}}; Y | X_{\mathcal{K}' \setminus (\mathcal{K}_0 \cup \mathcal{V})}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{V}}; Z | X_{\overline{\mathcal{K}'} \cup \mathcal{K}_0}) \tag{163c}$$

$$\leq I(X_{\mathcal{V}}; Y | X_{\mathcal{K}' \setminus (\mathcal{K}_0 \cup \mathcal{V})}, X_{\overline{\mathcal{K}'} \cup \mathcal{K}_0}) - I(X_{\mathcal{V}}; Z | X_{\overline{\mathcal{K}'} \cup \mathcal{K}_0}) \tag{163d}$$

$$=I(X_{\mathcal{V}}; Y | X_{\overline{\mathcal{V}}}, X_{\overline{\mathcal{K}''}}) - I(X_{\mathcal{V}}; Z | X_{\overline{\mathcal{K}''}}), \forall \mathcal{V} \subseteq \mathcal{K}'', \mathcal{V} \neq \phi, \tag{163e}$$

where (163c) follows by using (45), (163d) holds by adding $X_{\mathcal{K}_0}$ and using the fact that $X_k, \forall k \in \mathcal{K}$ are independent of each other, and the last step follows by using the definitions of $\overline{\mathcal{K}''}$ and $\overline{\mathcal{V}}$ in (47) and (48). Combining (46) and (163), we know that (48) is true.

Next, we show that for any rate-tuple in region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ defined by Theorem 3, if (45) and (46) can be satisfied, it is also in region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}'')$. If $(R_1^s, R_1^o, \cdots, R_K^s, R_K^o)$ is in region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ and satisfies (45), by setting $\mathcal{S} = \mathcal{K}_0$, $\mathcal{S}' = \mathcal{S} = \mathcal{K}_0$ and $\mathcal{T} = \phi$ in (17), we get

$$\sum_{k \in \mathcal{K}_0} R_k^s \leq \left[I(X_{\mathcal{K}_0}; Y | X_{\mathcal{K}' \setminus \mathcal{K}_0}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}_0}; Z | X_{\overline{\mathcal{K}'}}) \right]^+ = 0. \tag{164}$$

Hence, $R_k^s = 0, \forall k \in \mathcal{K}_0$. Considering that $R_k^s = 0, \forall k \in \overline{\mathcal{K}'}$ in (17), we have

$$R_k^s = 0, \forall k \in \overline{\mathcal{K}''}, \tag{165}$$

which is required by (49). To prove that $(R_1^s, R_1^o, \cdots, R_K^s, R_K^o)$ is also in region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}'')$, we need to further verify the upper bounds on $\sum_{k \in \mathcal{V}} R_k^s + \sum_{k \in \mathcal{V} \setminus \mathcal{V}'} R_k^o + \sum_{k \in \mathcal{W}} R_k^o$ for all possible set choices given in (49). To this end, we separately prove

$$\sum_{k \in \mathcal{V}} R_k^s + \sum_{k \in \mathcal{V} \setminus \mathcal{V}'} R_k^o + \sum_{k \in \mathcal{W}} R_k^o \leq I(X_{\mathcal{V}}, X_{\mathcal{W}}; Y | X_{\overline{\mathcal{V}}}, X_{\overline{\mathcal{K}''} \setminus \mathcal{W}}) - I(X_{\mathcal{V}'}; Z | X_{\overline{\mathcal{K}''}}),$$

$$\forall \mathcal{V} \subseteq \mathcal{K}'', \mathcal{V}' \subseteq \mathcal{V}, \mathcal{W} \subseteq \overline{\mathcal{K}'}, \tag{166}$$

and

$$\sum_{k\in\mathcal{V}}R_k^{\text{s}} + \sum_{k\in\mathcal{V}\backslash\mathcal{V}'}R_k^{\text{o}} + \sum_{k\in\mathcal{W}}R_k^{\text{o}} \leq I(X_{\mathcal{V}},X_{\mathcal{W}};Y|X_{\overline{\mathcal{V}}},X_{\overline{\mathcal{K}''}\backslash\mathcal{W}}) - I(X_{\mathcal{V}'};Z|X_{\overline{\mathcal{K}''}}),$$

$$\forall\mathcal{V}\subseteq\mathcal{K}'',\mathcal{V}'\subseteq\mathcal{V},\mathcal{W}\subseteq\overline{\mathcal{K}''},\mathcal{W}\cap\mathcal{K}_0\neq\phi. \tag{167}$$

Since in (49), $\mathcal{W}\subseteq\overline{\mathcal{K}''}\triangleq\overline{\mathcal{K}'}\cup\mathcal{K}_0$, (166) together with (167) takes into account all possible choices of $\mathcal{W}$ in (49).

We first prove (166). Since $R_k^{\text{s}}=0,\forall k\in\mathcal{K}_0$,

$$\sum_{k\in\mathcal{V}}R_k^{\text{s}} + \sum_{k\in\mathcal{V}\backslash\mathcal{V}'}R_k^{\text{o}} + \sum_{k\in\mathcal{W}}R_k^{\text{o}}$$

$$= \sum_{k\in\mathcal{V}\cup\mathcal{K}_0}R_k^{\text{s}} + \sum_{k\in\mathcal{V}\cup\mathcal{K}_0\backslash(\mathcal{V}'\cup\mathcal{K}_0)}R_k^{\text{o}} + \sum_{k\in\mathcal{W}}R_k^{\text{o}} \tag{168a}$$

$$\leq I(X_{\mathcal{V}\cup\mathcal{K}_0},X_{\mathcal{W}};Y|X_{\mathcal{K}'\backslash(\mathcal{V}\cup\mathcal{K}_0)},X_{\overline{\mathcal{K}'}\backslash\mathcal{W}}) - I(X_{\mathcal{V}'\cup\mathcal{K}_0};Z|X_{\overline{\mathcal{K}'}}) \tag{168b}$$

$$= I(X_{\mathcal{K}_0};Y|X_{\mathcal{K}'\backslash\mathcal{K}_0},X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}_0};Z|X_{\overline{\mathcal{K}'}}) \tag{168c}$$

$$+ I(X_{\mathcal{V}},X_{\mathcal{W}};Y|X_{\mathcal{K}'\backslash(\mathcal{V}\cup\mathcal{K}_0)},X_{\overline{\mathcal{K}'}\backslash\mathcal{W}}) - I(X_{\mathcal{V}'};Z|X_{\overline{\mathcal{K}'}\cup\mathcal{K}_0}) \tag{168d}$$

$$\leq I(X_{\mathcal{V}},X_{\mathcal{W}};Y|X_{\mathcal{K}'\backslash(\mathcal{V}\cup\mathcal{K}_0)},X_{\overline{\mathcal{K}'}\backslash\mathcal{W}}) - I(X_{\mathcal{V}'};Z|X_{\overline{\mathcal{K}'}\cup\mathcal{K}_0}) \tag{168e}$$

$$= I(X_{\mathcal{V}},X_{\mathcal{W}};Y|X_{\overline{\mathcal{V}}},X_{\overline{\mathcal{K}'}\backslash\mathcal{W}}) - I(X_{\mathcal{V}'};Z|X_{\overline{\mathcal{K}''}}) \tag{168f}$$

$$\leq I(X_{\mathcal{V}},X_{\mathcal{W}};Y|X_{\overline{\mathcal{V}}},X_{\overline{\mathcal{K}'}\backslash\mathcal{W}},X_{\mathcal{K}_0}) - I(X_{\mathcal{V}'};Z|X_{\overline{\mathcal{K}''}}), \tag{168g}$$

$$= I(X_{\mathcal{V}},X_{\mathcal{W}};Y|X_{\overline{\mathcal{V}}},X_{\overline{\mathcal{K}''}\backslash\mathcal{W}}) - I(X_{\mathcal{V}'};Z|X_{\overline{\mathcal{K}''}}),\forall\mathcal{V}\subseteq\mathcal{K}'',\mathcal{V}'\subseteq\mathcal{V},\mathcal{W}\subseteq\overline{\mathcal{K}'}, \tag{168h}$$

where (168b) is obtained by using the fact that $(\mathcal{V}\cup\mathcal{K}_0)\subseteq\mathcal{K}'$, $\mathcal{W}\subseteq\overline{\mathcal{K}'}$, $(R_1^{\text{s}},R_1^{\text{o}},\cdots,R_K^{\text{s}},R_K^{\text{o}})$ is in region $\mathscr{R}(X_{\mathcal{K}},\mathcal{K}')$, and setting $\mathcal{S}=\mathcal{V}\cup\mathcal{K}_0$, $\mathcal{S}'=\mathcal{V}'\cup\mathcal{K}_0$, and $\mathcal{T}=\mathcal{W}$ in (17). In addition, (168e) follows from using (45), (168f) is true since $\overline{\mathcal{V}}=\mathcal{K}''\backslash\mathcal{V}=\mathcal{K}'\backslash(\mathcal{V}\cup\mathcal{K}_0)$ and $\overline{\mathcal{K}''}=\overline{\mathcal{K}'}\cup\mathcal{K}_0$, and (168g) is obtained by adding $X_{\mathcal{K}_0}$ and using the fact that $X_k,\forall k\in\mathcal{K}$ are independent of each other. (166) is thus proven.

Next we prove (167), in which $\mathcal{W}\subseteq\overline{\mathcal{K}''}\triangleq\overline{\mathcal{K}'}\cup\mathcal{K}_0$ and $\mathcal{W}\cap\mathcal{K}_0\neq\phi$. Obviously, $\mathcal{W}$ can be divided into two disjoint subsets, $\mathcal{W}_1$ and $\mathcal{W}_2$, with $\mathcal{W}_1\subseteq\overline{\mathcal{K}'}$ and $\mathcal{W}_2\subseteq\mathcal{K}_0$. Then,

$$\sum_{k\in\mathcal{W}_2}R_k^{\text{o}} = \sum_{k\in\mathcal{W}_2}R_k^{\text{s}} + \sum_{k\in\mathcal{W}_2}R_k^{\text{o}} \tag{169a}$$

$$\leq I(X_{\mathcal{W}_2};Y|X_{\mathcal{K}'\backslash\mathcal{W}_2},X_{\overline{\mathcal{K}'}}) \tag{169b}$$

$$= I(X_{\mathcal{W}_2};Y|X_{\mathcal{K}''},X_{\overline{\mathcal{K}'}},X_{\mathcal{K}_0\backslash\mathcal{W}_2}), \tag{169c}$$

where (169a) holds since $\mathcal{W}_2 \subseteq \mathcal{K}_0$ and $R_k^{\mathrm{s}} = 0, \forall k \in \mathcal{K}_0$ (see (165)), and (169c) is true since $\mathcal{K}' = \mathcal{K}'' \cup \mathcal{K}_0$. Note that as defined in (45), $\mathcal{K}_0 \subsetneq \mathcal{K}'$, making $\mathcal{W}_2 \subseteq \mathcal{K}'$. In addition, $(R_1^{\mathrm{s}}, R_1^{\mathrm{o}}, \cdots, R_K^{\mathrm{s}}, R_K^{\mathrm{o}})$ is in region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ and thus satisfies (17). Hence, (169b) is obtained by setting $\mathcal{S} = \mathcal{W}_2$, $\mathcal{S}' = \phi$, and $\mathcal{T} = \phi$ in (17). Then,

$$\sum_{k \in \mathcal{V}} R_k^{\mathrm{s}} + \sum_{k \in \mathcal{V} \setminus \mathcal{V}'} R_k^{\mathrm{o}} + \sum_{k \in \mathcal{W}} R_k^{\mathrm{o}}$$

$$= \sum_{k \in \mathcal{V}} R_k^{\mathrm{s}} + \sum_{k \in \mathcal{V} \setminus \mathcal{V}'} R_k^{\mathrm{o}} + \sum_{k \in \mathcal{W}_1} R_k^{\mathrm{o}} + \sum_{k \in \mathcal{W}_2} R_k^{\mathrm{o}} \tag{170a}$$

$$\leq I(X_{\mathcal{V}}, X_{\mathcal{W}_1}; Y | X_{\overline{\mathcal{V}}}, X_{\overline{\mathcal{K}'} \setminus \mathcal{W}_1}) - I(X_{\mathcal{V}'}; Z | X_{\overline{\mathcal{K}''}}) + I(X_{\mathcal{W}_2}; Y | X_{\mathcal{K}''}, X_{\overline{\mathcal{K}'}}, X_{\mathcal{K}_0 \setminus \mathcal{W}_2}) \tag{170b}$$

$$\leq I(X_{\mathcal{V}}, X_{\mathcal{W}_1}; Y | X_{\overline{\mathcal{V}}}, X_{\overline{\mathcal{K}'} \setminus \mathcal{W}_1}, X_{\mathcal{K}_0 \setminus \mathcal{W}_2}) - I(X_{\mathcal{V}'}; Z | X_{\overline{\mathcal{K}''}}) + I(X_{\mathcal{W}_2}; Y | X_{\mathcal{K}''}, X_{\overline{\mathcal{K}'}}, X_{\mathcal{K}_0 \setminus \mathcal{W}_2}) \tag{170c}$$

$$= I(X_{\mathcal{V}}, X_{\mathcal{W}_1}, X_{\mathcal{W}_2}; Y | X_{\overline{\mathcal{V}}}, X_{\overline{\mathcal{K}'} \setminus \mathcal{W}_1}, X_{\mathcal{K}_0 \setminus \mathcal{W}_2}) - I(X_{\mathcal{V}'}; Z | X_{\overline{\mathcal{K}''}}) \tag{170d}$$

$$= I(X_{\mathcal{V}}, X_{\mathcal{W}}; Y | X_{\overline{\mathcal{V}}}, X_{\overline{\mathcal{K}''} \setminus \mathcal{W}}) - I(X_{\mathcal{V}'}; Z | X_{\overline{\mathcal{K}''}}), \forall \mathcal{V} \subseteq \mathcal{K}'', \mathcal{V}' \subseteq \mathcal{V}, \mathcal{W} \subseteq \overline{\mathcal{K}''}, \mathcal{W} \cap \mathcal{K}_0 \neq \phi, \tag{170e}$$

where (170b) follows from using (168f) (since $\mathcal{W}_1 \subseteq \overline{\mathcal{K}'}$) and (169), and (170c) is obtained by adding $X_{\mathcal{K}_0 \setminus \mathcal{W}_2}$ and using the fact that $X_k, \forall k \in \mathcal{K}$ are independent of each other. Combining (165), (166), and (167), it is known that $(R_1^{\mathrm{s}}, R_1^{\mathrm{o}}, \cdots, R_K^{\mathrm{s}}, R_K^{\mathrm{o}})$ satisfies (49) and is thus also in $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}'')$. Theorem 5 is then proven.

REFERENCES

[1] H. Xu, K.-K. Wong, and G. Caire, "Achievable region of the K-user MAC wiretap channel under strong secrecy," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Taipei, Taiwan, Jun. 2023, pp. 2750–2755.

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

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

[4] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

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

[7] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seattle, WA, USA, July 2006, pp. 957–961.

[8] 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.

[9] R. Liu, Y. Liang, and H. V. Poor, "Fading cognitive multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4992–5005, Aug. 2011.

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

[11] ——, "Collective secrecy over the K-transmitter multiple access channel," *IEEE Trans. Information Forensics Security*, vol. 13, no. 9, pp. 2279–2293, Mar. 2018.

[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] ——, "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, June 2008.

[14] H. Xu, G. Caire, and C. Pan, "An achievable region for the multiple access wiretap channels with confidential and open messages," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Los Angeles, CA, USA, Jun. 2020, pp. 949–954.

[15] H. Xu, T. Yang, K.-K. Wong, and G. Caire, "Achievable regions and precoder designs for the multiple access wiretap channels with confidential and open messages," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 5, pp. 1407–1427, May 2022.

[16] M. H. Yassaee and M. R. Aref, "Multiple access wiretap channels with strong secrecy," in *Proc. IEEE Inf. Theory Workshop*, Dublin, Ireland, Aug./Sep. 2010, pp. 1–5.

[17] M. Nafea and A. Yener, "Generalizing multiple access wiretap and wiretap II channel models: Achievable rates and cost of strong secrecy," *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 5125–5143, Aug. 2019.

[18] M. Hayashi and Y. Chen, "Secrecy and error exponents of K-transmitter multiple access wiretap channel," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Visby, Sweden, Aug. 2019, pp. 1–5.

[19] E. Ekrem and S. Ulukus, "The secrecy capacity region of the gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[20] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output gaussian broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5477–5487, Nov. 2010.

[21] S. A. A. Fakoorian and A. L. Swindlehurst, "On the optimality of linear precoding for secrecy in the MIMO broadcast channel," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1701–1713, Sep. 2013.

[22] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2637–2652, Nov. 2020.

[23] 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, May 2008.

[24] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[25] 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.

[26] D. Park, "Weighted sum rate maximization of MIMO broadcast and interference channels with confidential messages," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 1742–1753, Mar. 2016.

[27] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[28] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Sig. Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[29] B. Dai and Z. Ma, "Multiple-access relay wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1835–1849, May 2015.

[30] C. Liu, N. Yang, R. Malaney, and J. Yuan, "Artificial-noise-aided transmission in multi-antenna relay wiretap channels with spatially random eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7444–7456, Nov. 2016.

[31] S. Watanabe and Y. Oohama, "The optimal use of rate-limited randomness in broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 61, no. 2, pp. 983–995, Feb. 2015.

[32] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology-Eurocrypt 2000 (Lecture Notes in Computer Science)*. Springer, Bruges, Belgium, May, 2000, pp. 351–368.

[33] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[34] 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.

[35] A. El Gamal and Y.-H. Kim, *Network information theory*. Cambridge University Press, 2011.

[36] H. Xu, K.-K. Wong, and G. Caire, "A note on Fourier-Motzkin elimination with three eliminating variables," *arXiv preprint arXiv:2210.07924*, pp. 1–26, 2022.

[37] M. R. Bloch, "Achieving secrecy: Capacity vs. resolvability," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, St. Petersburg, Russia, Aug. 2011, pp. 633–637.

[38] M. Frey, I. Bjelakovic, and S. Stanczak, "The MAC resolvability region, semantic security and its operational implications," *arXiv preprint arXiv:1710.02342*, 2018.

[39] T. M. Cover, *Elements of information theory*. John Wiley & Sons, 1999.

[40] S. I. Gass, *Linear programming: methods and applications*. Courier Corporation, 2003.

[41] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 752–772, May 1993.

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

[43] Y. Oohama, "Converse coding theorems for identification via multiple access channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Istanbul, Turkey, 2013, pp. 1650–1654.

[44] N. Helal, *Resolvability and Strong Secrecy for the Multiple Access Channel with Cooperation*. The University of Texas at Dallas, 2020.

[45] I. Csiszár and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.

[46] G. Kramer *et al.*, "Topics in multi-user information theory," *Foundations and Trends® in Communications and Information Theory*, vol. 4, no. 4–5, pp. 265–444, 2008.