Achievable Region of the K-User MAC Wiretap Channel Under Strong Secrecy

Hao Xu*, Kai-Kit Wong*, and Giuseppe Caire†
*Department of Electronic and Electrical Engineering, University College London, London WC1E7JE, U.K.
†Faculty of Electrical Engineering and Computer Science, Technical University of Berlin, 10587 Berlin, Germany
E-mail: hao.xu@ucl.ac.uk; kai-kit.wong@ucl.ac.uk; caire@tu-berlin.de

***Abstract*—This paper investigates the information-theoretic secrecy problem for a K-user discrete memoryless (DM) multiple-access wiretap (MAC-WT) channel. Instead of using the *weak secrecy* criterion characterized by *information leakage rate*, we adopt the *strong secrecy* metric defined by *information leakage* to better protect the confidential information. We provide an achievable rate region and prove its achievability by providing a coding scheme and analyzing the output statistics in terms of (average) variational distance. We show that the rate region obtained in previous works on the subject is a special case of ours. We also show that the achievability proof in such works is incomplete, because it is assumed that certain inequalities hold while they may not in some cases. We solve this problem by constructing an inequality structure for the rates of all users' secret and redundant messages, and analyzing the conditions required to maintain this structure.**

I. Introduction

Following the pioneering work of Wyner [1] and Csiszár and Körner [2], information-theoretic secrecy has been studied for many different channel models, including multiple access wiretap (MAC-WT) channels. In [3]–[5], two-user MAC-WT systems were studied, where [3] developed inner and outer bounds for a discrete memoryless (DM) MAC-WT channel with a weaker eavesdropper (Eve), and [4] and [5] studied a channel where two users communicate with a common receiver and see each other as an Eve. In [6]–[11], the more general scenario with an arbitrary number of users was investigated. Specifically, [6] and [7] developed achievable regions for DM MAC-WT channels. Reference [8] studied a Gaussian MAC-WT system with a weaker Eve seeing a degraded channel. The work was extended by [9] to a non-degraded Gaussian case where each user has, in addition to confidential information, also an open (non-confidential) message intended for the legitimate receiver (Bob). Then, in [10] and [11], the results of [9] were further improved.

The above mentioned literature considered the *weak secrecy* criterion characterized by *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. The notion of *strong secrecy* was introduced in [12], [13], 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. In particular, [14]–[16] have considered the MAC-WT under strong secrecy. In [14], by analyzing the output statistics in terms of (average) variational distance and applying random coding, an achievable region was provided for a DM MAC-WT channel. In [15], the MAC-WT system with a DM main channel and different wiretapping scenarios was studied. Both [14] and [15] considered only two-user case. Based on Rényi mutual information, [16] considered the general K-user DM MAC-WT channel and strengthened the results in [6] and [7] subject to the strong secrecy criterion. However, by checking the two-user case and comparing [16, (14)] with [14, Theorem 1], it can be easily found that the achievable region given in [16] includes only $\mathcal{R}_1$ in [14] 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.

In this paper, we continue the study of information-theoretic secrecy for a K-user DM MAC-WT channel under strong secrecy and contribute in three aspects. 1) In wiretap channels, typical achievability strategies are based on introducing redundant messages to protect the confidential information. When introducing such a message, one has to ensure that, on one hand, its rate is large enough for protecting the secret message, and on the other hand, the resulting sum rate (together with the secret message rate) does not exceed Bob's decoding capability. This creates the need for an inequality structure involving the rates of all users' secret and redundant messages. We explore and construct such a structure in Theorem 1, which has never been analyzed before. 2) Unlike [16], we prove the achievability based on the (average) variational distance as in [14]. To this end, we extend the results on the output statistics for a two-user MAC channel in [14] to the general K-user case. 3) We provide an achievable region for the considered channel and show that those given in [14] and [16] are special cases of ours. Most importantly, we show that to use Theorem 1 for the achievability proof, some conditions must be met such that the inequality structure built in Theorem 1 can be maintained. Therefore, in proving the achievability, we separately talk about cases where these conditions can and cannot be satisfied. As we explain in Remark 1, a similar problem also exists in [14] and [16], but it was not addressed.

Notations: We use upper and lower case letters to denote random variables and their realizations, e.g., X, x. $P_X(\cdot)$ represents the distribution of X and $P_X(x) = \Pr\{X = x\}$. For two different distributions, $P_X(\cdot)$ and $Q_X(\cdot)$, defined both on alphabet $\mathcal{X}$, their variational distance is $\|P_X(\cdot) - Q_X(\cdot)\|_1 =$

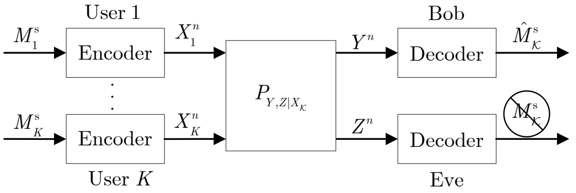

Fig. 1. Block diagram of a K-user DM MAC-WT channel.

$\sum_{x\in\mathcal{X}}|P_X(x)-Q_X(x)|$. We use calligraphic capital letters to denote sets, $|\cdot|$ to stand for the cardinality of a set, and " $\setminus$ " to represent the set subtraction operation. 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 calligraphic subscript to denote the set of elements whose indexes take values from the subscript set, e.g., $X_{\mathcal{K}}=\{X_k,\forall k\in\mathcal{K}\}$.

II. Channel Model

As shown in Fig. 1, we consider a DM MAC-WT channel with K users, a legitimate receiver (or Bob for brevity), and an Eve. Let $\mathcal{K}=\{1,\cdots,K\}$. The DM MAC-WT system can then be denoted by $\left(\mathcal{X}_{\mathcal{K}},P_{Y,Z|X_{\mathcal{K}}},\mathcal{Y},\mathcal{Z}\right)$ (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 inputs from user k, and $y\in\mathcal{Y}$ and $z\in\mathcal{Z}$ are respectively channel outputs at Bob and Eve. Each user $k\in\mathcal{K}$ transmits a secret message M_k^{s} to Bob. Specifically, user k encodes its information into a codeword X_k^n, and then transmits it over the channel with transition probability $P_{Y,Z|X_{\mathcal{K}}}$. Upon receiving the sequence Y^n, Bob decodes the messages of all users. Eve attempts to overhear the secret messages of all users. Let R_k^{s} denote the rate of user k's secret message. Then, a $\left(2^{nR_1^{\mathrm{s}}},\cdots,2^{nR_K^{\mathrm{s}}},n\right)$ secrecy code for the considered DM MAC-WT channel consists of

- Message sets: $\mathcal{M}_k^{\mathrm{s}}=\left[1:2^{nR_k^{\mathrm{s}}}\right],\forall k\in\mathcal{K}$. Each message M_k^{s} is uniformly distributed over $\mathcal{M}_k^{\mathrm{s}}$.
- Randomized encoders: the encoder of user k maps message $M_k^{\mathrm{s}}\in\mathcal{M}_k^{\mathrm{s}}$ to a n-length codeword X_k^n.
- A decoder at Bob which maps the received noisy sequence Y^n to the message estimate $\hat{M}_k^{\mathrm{s}}\in\mathcal{M}_k^{\mathrm{s}},\forall k\in\mathcal{K}$.

To evaluate the performance, we define two metrics, i.e., the average probability of error $\Pr\left\{\hat{M}_{\mathcal{K}}^{\mathrm{s}}\neq M_{\mathcal{K}}^{\mathrm{s}}\right\}$ for Bob, and the information leakage $I\left(M_{\mathcal{K}}^{\mathrm{s}};Z^n\right)$ for Eve. A rate tuple $(R_1^{\mathrm{s}},\cdots,R_K^{\mathrm{s}})$ is said to be achievable if there exists a sequence of $\left(2^{nR_1^{\mathrm{s}}},\cdots,2^{nR_K^{\mathrm{s}}},n\right)$ codes such that

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

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

III. Main Results

In this section, we provide an achievable region for the considered DM MAC-WT channel. Before that we first give two auxiliary theorems important for the achievability proof.

A. Auxiliary Results

We use m_k^{g} and R_k^{g} to denote the redundant message introduced for user k and its rate. Since Bob does not need this information, we call it "garbage" message and use superscript "g" to distinguish from the secret messages. As explained in Section I, there should exist a relationship or structure for $R_k^{\mathrm{s}},R_k^{\mathrm{g}},\forall k\in\mathcal{K}$ such that all messages could be perfectly decoded by Bob and the confidential information could be protected. The following theorem characterizes such structure.

Theorem 1. *For each given $\mathcal{K}'\subseteq\mathcal{K}$, if*

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

where $\overline{\mathcal{K}'}=\mathcal{K}\setminus\mathcal{K}'$ and $\overline{\mathcal{S}}=\mathcal{K}'\setminus\mathcal{S}$, then, for any rate tuple $(R_1^s,\cdots,R_K^s)$ satisfying $R_k^s=0,\forall k\in\overline{\mathcal{K}'}$ and

$$\sum_{k\in\mathcal{S}}R_k^s\leq I(X_{\mathcal{S}};Y|X_{\overline{\mathcal{S}}},X_{\overline{\mathcal{K}'}})-I(X_{\mathcal{S}};Z|X_{\overline{\mathcal{K}'}}),\forall\mathcal{S}\subseteq\mathcal{K}', \tag{4}$$

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

$$\begin{cases}\sum\limits_{k\in\mathcal{S}}(R_k^s+R_k^g)\leq I(X_{\mathcal{S}};Y|X_{\overline{\mathcal{S}}},X_{\overline{\mathcal{K}'}}),\forall\mathcal{S}\subseteq\mathcal{K}',\\ \sum\limits_{k\in\mathcal{S}}R_k^g\geq I(X_{\mathcal{S}};Z|X_{\overline{\mathcal{K}'}}),\forall\mathcal{S}\subseteq\mathcal{K}'.\end{cases} \tag{5}$$

Proof: See Appendix A. □

Next, we prove another auxiliary result that yields an exponential upper bound to the average total variational distance of the n-variate output distribution, subject to certain single-letter mutual information inequalities. Consider a DM MAC channel (not necessarily a wiretap channel) with K users and a receiver. Each user $k\in\mathcal{K}$ has a message set $\mathcal{M}_k=\left[1:2^{nR_k}\right]$ and its message M_k is uniformly distributed over $\mathcal{M}_k$. User k generates a codebook $\mathfrak{C}_k$ by randomly and independently generating 2^{nR_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 channel $P_{Z|X_{\mathcal{K}}}$. Let $\mathcal{C}_k$ denote the random choice of codebook $\mathfrak{C}_k$ and define the following conditional probability

$$\begin{aligned}&P_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}})\\ =&2^{-n\sum_{k\in\mathcal{K}}R_k}\sum_{m_{\mathcal{K}}\in\prod_{k\in\mathcal{K}}\mathcal{M}_k}P_{Z^n}\left(z^n|\left\{X_k^n(m_k)\right\}_{k\in\mathcal{K}}\right).\end{aligned} \tag{6}$$

Since $\mathcal{C}_k$ is a random variable, $P_{Z^n}\left(z^n|\left\{X_k^n(m_k)\right\}_{k\in\mathcal{K}}\right)$ and $P_{Z^n}(z^n|\mathcal{C}_{\mathcal{K}})$ in (6) are conditional distributions whose values depend on the specific realizations of $\mathcal{C}_k,\forall k\in\mathcal{K}$.

Theorem 2. *Let $(X_{\mathcal{K}},Z)\sim\prod_{k=1}^K P_{X_k}P_{Z|X_{\mathcal{K}}}$. For any given $\mathcal{K}'\subseteq\mathcal{K}$, if*

$$\begin{aligned}&R_k=0,\forall k\in\overline{\mathcal{K}'},\\ &\sum_{k\in\mathcal{S}}R_k>I(X_{\mathcal{S}};Z|X_{\overline{\mathcal{K}'}}),\forall\mathcal{S}\subseteq\mathcal{K}',\mathcal{S}\neq\phi,\end{aligned} \tag{7}$$

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

$$\mathbb{E}\left\|P_{Z^n}(\cdot|\mathcal{C}_{\mathcal{K}})-P_{Z^n}(\cdot|\mathcal{C}_{\overline{\mathcal{K}'}})\right\|_1\leq e^{-n\varepsilon}, \tag{8}$$

where $P_{Z^n}(\cdot|\mathcal{C}_{\overline{\mathcal{K}'}})$ is similarly defined as $P_{Z^n}(\cdot|\mathcal{C}_{\mathcal{K}})$ in (6), and the expectation is taken over the random codebooks. □

The detailed proof of Theorem 2 will be provided in [17]. Theorem 2 shows that with (7), the coding scheme provided above ensures that the variational distance between output statistics $P_{Z^n}(\cdot|\mathcal{C}_{\mathcal{K}})$ and $P_{Z^n}(\cdot|\mathcal{C}_{\overline{\mathcal{K}'}})$ vanishes exponentially in n. Note that the above coding scheme is provided mainly for reaching Theorem 2 and is different from that in Section IV.

B. Achievable Region

In the following theorem, we give an achievable region for the considered DM MAC-WT channel.

Theorem 3. *Let* $(X_{\mathcal{K}}, Y, Z) \sim \prod_{k=1}^{K} P_{X_k} P_{Y,Z|X_{\mathcal{K}}}$*. Then, for each given* $\mathcal{K}' \subseteq \mathcal{K}$*, any rate tuple* $(R_1^s, \cdots, R_K^s)$ *in region*

$$\begin{cases} R_k^s = 0, \forall k \in \overline{\mathcal{K}'}, \\ \sum\limits_{k\in\mathcal{S}} R_k^s \leq [I(X_{\mathcal{S}}; Y|X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{S}}; Z|X_{\overline{\mathcal{K}'}})]^+, \forall \mathcal{S} \subseteq \mathcal{K}', \end{cases} \tag{9}$$

is achievable. Let $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ *denote the set of rate tuples satisfying (9). 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.*

The proof of Theorem 3 is provided in the next section.

Remark 1. *It is easy to see that [14, Theorem 1] and [16, Theorem 1] are special cases of Theorem 3 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 "garbage" 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 [14] and [16] (by respectively checking [14, (7), (20)] and [16, (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* $\mathcal{K}'' \subsetneqq \mathcal{K}'$ *such that (3) becomes true for the reduced set* $\mathcal{K}''$ *and* $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ *is in* $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}'')$*, which can then be proved to be achievable. Therefore, this paper not only extends the achievable region given by [14] and [16], but also "completes" the proofs in these works.*

IV. Achievability Proof

It can be easily checked that if $\mathcal{K}' = \phi$, $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ contains only rate tuple $(R_1^{\mathrm{s}} = 0, \cdots, R_K^{\mathrm{s}} = 0)$, whose achievability is obvious. Now we prove the achievability of $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ for any $\mathcal{K}' \subseteq \mathcal{K}$ and $\mathcal{K}' \neq \phi$. Without loss of generality (w.l.o.g.), we always assume

$$I(X_{\mathcal{S}_0}; Y|X_{\overline{\mathcal{S}_0}}) > 0, \forall \mathcal{S}_0 \subseteq \mathcal{K}, \mathcal{S}_0 \neq \phi, \tag{10}$$

where $\overline{\mathcal{S}_0} = \mathcal{K} \setminus \mathcal{S}_0$ since otherwise users in $\mathcal{S}_0$ cannot communicate with Bob. Moreover, we assume

$$I(X_{\mathcal{S}}; Y|X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{S}}; Z|X_{\overline{\mathcal{K}'}}) > 0, \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S} \neq \phi, \tag{11}$$

which is (3) with strict $>$. If (11) cannot not be satisfied, we show later that the achievability could be proven by modifying the proof steps.

A. Achievability Proof When (11) Holds

In this subsection, we show that with (11), 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 assumption (11) can be met, a rate tuple $(R_1^{\mathrm{s}}, \cdots, R_K^{\mathrm{s}})$ inside $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ satisfies

$$\begin{cases} R_k^{\mathrm{s}} = 0, \forall k \in \overline{\mathcal{K}'}, \\ \sum\limits_{k\in\mathcal{S}} R_k^{\mathrm{s}} < I(X_{\mathcal{S}}; Y|X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{S}}; Z|X_{\overline{\mathcal{K}'}}) - \epsilon, \\ \qquad \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S} \neq \phi, \end{cases} \tag{12}$$

where ϵ is an arbitrarily small positive number. Then, according to Theorem 1, there exist $R_k^{\mathrm{g}}, \forall k \in \mathcal{K}'$ such that

$$\begin{cases} \sum\limits_{k\in\mathcal{S}} (R_k^{\mathrm{s}} + R_k^{\mathrm{g}}) < I(X_{\mathcal{S}}; Y|X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) - \epsilon, \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S} \neq \phi, \\ \sum\limits_{k\in\mathcal{S}} R_k^{\mathrm{g}} > I(X_{\mathcal{S}}; Z|X_{\overline{\mathcal{K}'}}), \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S} \neq \phi. \end{cases} \tag{13}$$

Now we provide a coding scheme and show that the rate tuples inside $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ are achievable. Note that for each user $k \in \overline{\mathcal{K}'}$, since $R_k^{\mathrm{s}} = 0$, we have $\mathcal{M}_k^{\mathrm{s}} = \{1\}$ and $|\mathcal{M}_k^{\mathrm{s}}| = 1$. Hence, each user $k \in \overline{\mathcal{K}'}$ transmits a fixed message.

Codebook generation. For each secret message $m_k^{\mathrm{s}} \in \mathcal{M}_k^{\mathrm{s}}$ of user $k \in \mathcal{K}'$, generate a subcodebook $\mathcal{C}_k(m_k^{\mathrm{s}})$ by randomly and independently generating $2^{nR_k^{\mathrm{g}}}$ sequences $x_k^n(m_k^{\mathrm{s}}, m_k^{\mathrm{g}}), \forall m_k^{\mathrm{g}} \in \mathcal{M}_k^{\mathrm{g}}$, each according to $\prod_{i=1}^{n} P_{X_k}(x_{ki})$. All these subcodebooks constitute the codebook of user $k \in \mathcal{K}'$, i.e., $\mathcal{C}_k = \{\mathcal{C}_k(m_k^{\mathrm{s}}), \forall m_k^{\mathrm{s}} \in \mathcal{M}_k^{\mathrm{s}}\}$. For each user $k \in \overline{\mathcal{K}'}$, randomly generate a sequence $x_k^n(1)$ with index "1" and this unique codeword constructs its codebook, i.e., $\mathcal{C}_k = \{x_k^n(1)\}$. The codebooks of all users are then revealed to all transmitters and receivers, including Eve.

Encoding. To send message $m_k^{\mathrm{s}} \in \mathcal{M}_k^{\mathrm{s}}$, user $k \in \mathcal{K}'$ uniformly chooses a codeword (with index m_k^{g}) from subcodebook $\mathcal{C}_k(m_k^{\mathrm{s}})$ and then transmits $x_k^n(m_k^{\mathrm{s}}, m_k^{\mathrm{g}})$. In contrast, user $k \in \overline{\mathcal{K}'}$ has only one message and transmits $x_k^n(1)$.

Decoding. The decoder at Bob declares that $\hat{m}_{\mathcal{K}'}^{\mathrm{s}}$ is sent if there exists $\hat{m}_{\mathcal{K}'}^{\mathrm{g}} \in \prod_{k\in\mathcal{K}'} \mathcal{M}_k^{\mathrm{g}}$ such that $(\hat{m}_{\mathcal{K}'}^{\mathrm{s}}, \hat{m}_{\mathcal{K}'}^{\mathrm{g}})$ is the unique message tuple satisfying $\big(\{x_k^n(\hat{m}_k^{\mathrm{s}}, \hat{m}_k^{\mathrm{g}})\}_{k\in\mathcal{K}'}, \{x_k^n(1)\}_{k\in\overline{\mathcal{K}'}}, y^n\big) \in \mathcal{T}_\epsilon^{(n)}(X_{\mathcal{K}}, Y)$.

Now we show that using the coding scheme provided above, both (1) and (2) can be satisfied. Since users in $\mathcal{K}'$ and $\overline{\mathcal{K}'}$ respectively transmit messages at rate $R_k^{\mathrm{s}} + R_k^{\mathrm{g}}$ and $R_k^{\mathrm{s}} = 0$, and (see (13))

$$\sum_{k\in\mathcal{S}} (R_k^{\mathrm{s}} + R_k^{\mathrm{g}}) < I(X_{\mathcal{S}}; Y|X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) - \epsilon, \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S} \neq \phi, \tag{14}$$

the rate tuple $\big(\{R_k^{\mathrm{s}} + R_k^{\mathrm{g}}\}_{k\in\mathcal{K}'}, \{R_k^{\mathrm{s}} = 0\}_{k\in\overline{\mathcal{K}'}}\big)$ is thus inside the capacity region of the MAC channel from all users to Bob. Hence, Bob can perfectly decode all messages and (1) can be satisfied.

We now verify (2). Define the following variational distance

$$\begin{aligned} d\left(\mathcal{C}_{\mathcal{K}}, m_{\mathcal{K}}^{\mathrm{s}}\right) &= \left\| P_{Z^n}\left(\cdot|\mathcal{C}_{\mathcal{K}}\right) - P_{Z^n}\left(\cdot|\left\{\mathcal{C}_k(m_k^{\mathrm{s}})\right\}_{k\in\mathcal{K}}\right)\right\|_1 \\ &= \left\| P_{Z^n}\left(\cdot|\mathcal{C}_{\mathcal{K}'}, \{\mathcal{C}_k(1)\}_{k\in\overline{\mathcal{K}'}}\right)\right. \\ &\quad \left. - P_{Z^n}\left(\cdot|\left\{\mathcal{C}_k(m_k^{\mathrm{s}})\right\}_{k\in\mathcal{K}'}, \{\mathcal{C}_k(1)\}_{k\in\overline{\mathcal{K}'}}\right)\right\|_1. \end{aligned} \tag{15}$$

As shown in (16) at the bottom of the next page, we can get an upper bound on the expectation of $d\left(\mathcal{C}_{\mathcal{K}}, m_{\mathcal{K}}^{\mathrm{s}}\right)$, where the expectation is taken over $\mathcal{C}_{\mathcal{K}}$. In (16), (16a) follows from first introducing $P_{Z^n}\left(\cdot|\left\{\mathcal{C}_k(1)\right\}_{k\in\overline{\mathcal{K}'}}\right)$ and then applying the triangular inequality, and (16b) holds by computing $P_{Z^n}\left(\cdot|\mathcal{C}_{\mathcal{K}'}, \{\mathcal{C}_k(1)\}_{k\in\overline{\mathcal{K}'}}\right)$ over all possible $m_{\mathcal{K}'}$ and also applying the triangular inequality. In addition, it is known from the coding scheme provided above that there are respectively $2^{nR_k^{\mathrm{g}}}$ codewords in $\mathcal{C}_k(m_k^{\mathrm{s}}), \forall k \in \mathcal{K}'$ and one codeword in $\mathcal{C}_k(1), \forall k \in \overline{\mathcal{K}'}$. Since $R_k^{\mathrm{s}} = 0, \forall k \in \overline{\mathcal{K}'}$ and (see (13))

$$\sum_{k\in\mathcal{S}} R_k^{\mathrm{g}} > I(X_{\mathcal{S}}; Z|X_{\overline{\mathcal{K}'}}), \forall \mathcal{S} \subseteq \mathcal{K}', \mathcal{S} \neq \phi, \tag{17}$$

(16c) is obtained by using Theorem 2. Now we evaluate the information leakage over all codebooks in (18) at the bottom of this page, where (18a), (18b), and (18c) follow by respectively applying the triangular inequality, [18, Lemma 2.7], and Jensen's inequality, and the last step holds since $u \ln \frac{|\mathcal{Z}|^n}{u}$ 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 definition of mutual information,

$$\begin{aligned} I\left(M_{\mathcal{K}}^{\mathrm{s}}; Z^n|\mathcal{C}_{\mathcal{K}}\right) &= I\left(M_{\mathcal{K}}^{\mathrm{s}}; Z^n, \mathcal{C}_{\mathcal{K}}\right) - I\left(M_{\mathcal{K}}^{\mathrm{s}}; \mathcal{C}_{\mathcal{K}}\right) \\ &\overset{\text{(a)}}{=} I\left(M_{\mathcal{K}}^{\mathrm{s}}; Z^n, \mathcal{C}_{\mathcal{K}}\right) \\ &= I\left(M_{\mathcal{K}}^{\mathrm{s}}; Z^n\right) + I\left(M_{\mathcal{K}}^{\mathrm{s}}; \mathcal{C}_{\mathcal{K}}|Z^n\right) \\ &\geq I\left(M_{\mathcal{K}}^{\mathrm{s}}; Z^n\right), \end{aligned} \tag{19}$$

where (19a) holds since the choices of random messages and codebooks are independent, resulting in $I\left(M_{\mathcal{K}}^{\mathrm{s}}; \mathcal{C}_{\mathcal{K}}\right) = 0$. Combining (18) and (19), we know that (2) is true. Hence, if (11) is true, any rate tuple in $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ is achievable.

B. Achievability Proof When (11) does not Hold

Now we prove the achievability for the case where (11) does not hold. Beforehand, we first assume

$$I(X_{\mathcal{K}'}; Y|X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}'}; Z|X_{\overline{\mathcal{K}'}}) > 0, \tag{20}$$

which is one of the inequations in (11) with $\mathcal{S} = \mathcal{K}'$, since otherwise it is known from (9) that $R_k^{\mathrm{s}} = 0, \forall k \in \mathcal{K}$, and it is no longer necessary to prove the achievability. Then, if (11) does not hold, there must exist $\mathcal{S} \subsetneqq \mathcal{K}'$ and $\mathcal{S} \neq \phi$ such that

$$I(X_{\mathcal{S}}; Y|X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{S}}; Z|X_{\overline{\mathcal{K}'}}) \leq 0. \tag{21}$$

In this case, there must exist at least one subset $\mathcal{K}_0 \subsetneqq \mathcal{K}'$ and $\mathcal{K}_0 \neq \phi$ such that

$$I(X_{\mathcal{K}_0}; Y|X_{\mathcal{K}'\setminus\mathcal{K}_0}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}_0}; Z|X_{\overline{\mathcal{K}'}}) \leq 0, \tag{22}$$

and

$$\begin{aligned} &I(X_{\mathcal{K}_0\cup\mathcal{V}}; Y|X_{\mathcal{K}'\setminus(\mathcal{K}_0\cup\mathcal{V})}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}_0\cup\mathcal{V}}; Z|X_{\overline{\mathcal{K}'}}) > 0, \\ &\quad \forall \mathcal{V} \subseteq \mathcal{K}' \setminus \mathcal{K}_0,\ \mathcal{V} \neq \phi. \end{aligned} \tag{23}$$

The inequations (22) and (23) indicate that $\mathcal{K}_0$ is the largest set in $\mathcal{K}'$ which includes all users in $\mathcal{K}_0$ and ensures (22). Adding any other users in $\mathcal{K}' \setminus \mathcal{K}_0$ to $\mathcal{K}_0$ results in (23). Note that if there are multiple subsets in $\mathcal{K}'$ making (22) and (23) hold, we let $\mathcal{K}_0$ be any of them. Let

$$\begin{aligned} \mathcal{K}'' &= \mathcal{K}' \setminus \mathcal{K}_0 \\ &= \mathcal{K} \setminus (\overline{\mathcal{K}'} \cup \mathcal{K}_0), \\ \overline{\mathcal{K}''} &= \mathcal{K} \setminus \mathcal{K}'' \\ &= \overline{\mathcal{K}'} \cup \mathcal{K}_0. \end{aligned} \tag{24}$$

Then, we give the following theorem.

Theorem 4. *With $\mathcal{K}_0$, $\mathcal{K}''$, and $\overline{\mathcal{K}''}$ defined above, we have*

$$I(X_{\mathcal{V}}; Y|X_{\overline{\mathcal{V}}}, X_{\overline{\mathcal{K}''}}) - I(X_{\mathcal{V}}; Z|X_{\overline{\mathcal{K}''}}) > 0, \forall \mathcal{V} \subseteq \mathcal{K}'', \mathcal{V} \neq \phi, \tag{25}$$

where $\overline{\mathcal{V}} = \mathcal{K}'' \setminus \mathcal{V}$. In addition, if a rate tuple $(R_1^{\mathrm{s}}, \cdots, R_K^{\mathrm{s}})$ is in region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ defined by (9) and has (22) and (23) met, it is also in region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}'')$, i.e., it satisfies

$$\begin{cases} R_k^{\mathrm{s}} = 0, \forall k \in \overline{\mathcal{K}''}, \\ \sum\limits_{k\in\mathcal{V}} R_k^{\mathrm{s}} \leq I(X_{\mathcal{V}}; Y|X_{\overline{\mathcal{V}}}, X_{\overline{\mathcal{K}''}}) - I(X_{\mathcal{V}}; Z|X_{\overline{\mathcal{K}''}}), \forall \mathcal{V} \subseteq \mathcal{K}'', \end{cases} \tag{26}$$

in which $[\cdot]^+$ is omitted due to (25).

Proof: See Appendix B. □

It is known from Theorem 4 that if a rate tuple $(R_1^{\mathrm{s}}, \cdots, R_K^{\mathrm{s}})$ in $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ satisfies (22) as well as (23), it also satisfies (25) and (26). Then, its achievability is immediately clear if we could prove that with (25), 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.

$$\begin{aligned} \mathbb{E}\left[d\left(\mathcal{C}_{\mathcal{K}}, m_{\mathcal{K}}^{\mathrm{s}}\right)\right] &\overset{\text{(a)}}{\leq} \mathbb{E}\left\|P_{Z^n}\left(\cdot|\mathcal{C}_{\mathcal{K}'}, \{\mathcal{C}_k(1)\}_{k\in\overline{\mathcal{K}'}}\right) - P_{Z^n}\left(\cdot|\{\mathcal{C}_k(1)\}_{k\in\overline{\mathcal{K}'}}\right)\right\|_1 \\ &\quad + \mathbb{E}\left\|P_{Z^n}\left(\cdot|\{\mathcal{C}_k(m_k^{\mathrm{s}})\}_{k\in\mathcal{K}'}, \{\mathcal{C}_k(1)\}_{k\in\overline{\mathcal{K}'}}\right) - P_{Z^n}\left(\cdot|\{\mathcal{C}_k(1)\}_{k\in\overline{\mathcal{K}'}}\right)\right\|_1 \\ &\overset{\text{(b)}}{\leq} 2^{-n\sum_{k\in\mathcal{K}'} R_k^{\mathrm{s}}} \sum_{m_{\mathcal{K}'}^{\mathrm{s}} \in \prod_{k\in\mathcal{K}'} \mathcal{M}_k^{\mathrm{s}}} \mathbb{E}\left\|P_{Z^n}\left(\cdot|\{\mathcal{C}_k(m_k^{\mathrm{s}})\}_{k\in\mathcal{K}'}, \{\mathcal{C}_k(1)\}_{k\in\overline{\mathcal{K}'}}\right) - P_{Z^n}\left(\cdot|\{\mathcal{C}_k(1)\}_{k\in\overline{\mathcal{K}'}}\right)\right\|_1 \\ &\quad + \mathbb{E}\left\|P_{Z^n}\left(\cdot|\{\mathcal{C}_k(m_k^{\mathrm{s}})\}_{k\in\mathcal{K}'}, \{\mathcal{C}_k(1)\}_{k\in\overline{\mathcal{K}'}}\right) - P_{Z^n}\left(\cdot|\{\mathcal{C}_k(1)\}_{k\in\overline{\mathcal{K}'}}\right)\right\|_1 \\ &\overset{\text{(c)}}{\leq} 2e^{-n\varepsilon} \to 0. \end{aligned} \tag{16}$$

$$\begin{aligned} I\left(M_{\mathcal{K}}^{\mathrm{s}}; Z^n|\mathcal{C}_{\mathcal{K}}\right) &= H\left(Z^n|\mathcal{C}_{\mathcal{K}}\right) - H\left(Z^n|\mathcal{C}_{\mathcal{K}}, M_{\mathcal{K}}^{\mathrm{s}}\right) \\ &= H\left(Z^n|\mathcal{C}_{\mathcal{K}'}, \{\mathcal{C}_k(1)\}_{k\in\overline{\mathcal{K}'}}\right) - H\left(Z^n|\{\mathcal{C}_k(M_k^{\mathrm{s}})\}_{k\in\mathcal{K}'}, \{\mathcal{C}_k(1)\}_{k\in\overline{\mathcal{K}'}}\right) \\ &\overset{\text{(a)}}{\leq} 2^{-n\sum_{k\in\mathcal{K}'} R_k^{\mathrm{s}}} \sum_{m_{\mathcal{K}'}^{\mathrm{s}} \in \prod_{k\in\mathcal{K}'} \mathcal{M}_k^{\mathrm{s}}} \left|H\left(Z^n|\mathcal{C}_{\mathcal{K}'}, \{\mathcal{C}_k(1)\}_{k\in\overline{\mathcal{K}'}}\right) - H\left(Z^n|\{\mathcal{C}_k(m_k^{\mathrm{s}})\}_{k\in\mathcal{K}'}, \{\mathcal{C}_k(1)\}_{k\in\overline{\mathcal{K}'}}\right)\right| \\ &\overset{\text{(b)}}{\leq} 2^{-n\sum_{k\in\mathcal{K}'} R_k^{\mathrm{s}}} \sum_{m_{\mathcal{K}'}^{\mathrm{s}} \in \prod_{k\in\mathcal{K}'} \mathcal{M}_k^{\mathrm{s}}} \mathbb{E}\left[d\left(\mathcal{C}_{\mathcal{K}}, m_{\mathcal{K}}^{\mathrm{s}}\right) \ln \frac{|\mathcal{Z}|^n}{d\left(\mathcal{C}_{\mathcal{K}}, m_{\mathcal{K}}^{\mathrm{s}}\right)}\right] \\ &\overset{\text{(c)}}{\leq} 2^{-n\sum_{k\in\mathcal{K}'} R_k^{\mathrm{s}}} \sum_{m_{\mathcal{K}'}^{\mathrm{s}} \in \prod_{k\in\mathcal{K}'} \mathcal{M}_k^{\mathrm{s}}} \mathbb{E}\left[d\left(\mathcal{C}_{\mathcal{K}}, m_{\mathcal{K}}^{\mathrm{s}}\right)\right] \ln \frac{|\mathcal{Z}|^n}{\mathbb{E}\left[d\left(\mathcal{C}_{\mathcal{K}}, m_{\mathcal{K}}^{\mathrm{s}}\right)\right]} \\ &\leq 2e^{-n\varepsilon}\left(n \ln |\mathcal{Z}| + n\varepsilon - \ln 2\right) \to 0. \end{aligned} \tag{18}$$

V. Conclusions

In this paper, we studied information-theoretic secrecy for a K-user DM MAC-WT channel under strong secrecy. We developed an inequality structure for the rates of all users' secret and redundant messages, and analyzed the output statistics in terms of variational distance for the general K-user MAC channel. Based on these results, we provided and proved a new achievable region that enlarges previously known results.

Acknowledgments

This work was supported by the European Union's Horizon 2020 Research and Innovation Programme under Marie Skodowska-Curie Grant No. 101024636 and the Alexander von Humboldt Foundation.

Appendix A
Proof of Theorem 1

We prove Theorem 1 by eliminating R_k^{g} in (5) using the Fourier-Motzkin procedure [19, Appendix D] and showing that (4) is the projection of (5) onto the hyperplane $\{R_k^{\mathrm{g}} = 0, \forall k \in \mathcal{K}'\}$. To that end, we first obtain upper and lower bounds on sums of R_k^{g} from (5) as follows

$$\sum_{k\in\mathcal{S}} R_k^{\mathrm{g}} \le I(X_{\mathcal{S}}; Y|X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) - \sum_{k\in\mathcal{S}} R_k^{\mathrm{s}}, \forall \mathcal{S} \subseteq \mathcal{K}', \tag{27}$$

$$\sum_{k\in\mathcal{S}'} R_k^{\mathrm{g}} \ge I(X_{\mathcal{S}'}; Z|X_{\overline{\mathcal{K}'}}), \forall \mathcal{S}' \subseteq \mathcal{K}'. \tag{28}$$

Note that we use $\mathcal{S}'$ in (28) to distinguish from $\mathcal{S}$ in (27). By comparing the upper bounds in (27) with the lower bounds in (28), and eliminating $R_k^{\mathrm{g}}, \forall k \in \mathcal{K}'$ one by one, we finally get

$$\sum_{k\in\mathcal{S}} R_k^{\mathrm{s}} \le I(X_{\mathcal{S}}; Y|X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) - \sum_{\mathcal{S}_j\in\psi} I(X_{\mathcal{S}_j}; Z|X_{\overline{\mathcal{K}'}}),$$
$$\forall \mathcal{S} \subseteq \mathcal{K}', \psi \in \Psi_{\mathcal{S}}, \tag{29}$$

where $\Psi_{\mathcal{S}}$ is defined as

$$\Psi_{\mathcal{S}} = \Big\{\psi = \{\mathcal{S}_1, \cdots, \mathcal{S}_J\} | 1 \le J \le |\mathcal{S}|, \mathcal{S}_j, \mathcal{S}_{j'} \subseteq \mathcal{S},$$
$$\mathcal{S}_j \cap \mathcal{S}_{j'} = \phi, \forall j, j' \in \mathcal{J}, j \ne j', \mathcal{S}_1 \cup \cdots \cup \mathcal{S}_J = \mathcal{S}\Big\}, \tag{30}$$

and $\mathcal{J} = \{1, \cdots, J\}$. It is obvious that $\Psi_{\mathcal{S}}$ gives all possible divisions of $\mathcal{S}$.

The inequation system defined by (29) is the projection of (5) onto the hyperplane $\{R_k^{\mathrm{g}} = 0, \forall k \in \mathcal{K}'\}$. Now we show that it is equivalent to (4). For each given $\mathcal{S} \subseteq \mathcal{K}'$, (29) gives $|\Psi_{\mathcal{S}}|$ upper bounds on $\sum_{k\in\mathcal{S}} R_k^{\mathrm{s}}$, while (4) provides only one. When $J = 1$, i.e., $\psi = \{\mathcal{S}\}$, we get from (29)

$$\sum_{k\in\mathcal{S}} R_k^{\mathrm{s}} \le I(X_{\mathcal{S}}; Y|X_{\overline{\mathcal{S}}}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{S}}; Z|X_{\overline{\mathcal{K}'}}), \tag{31}$$

which is exactly (4). Hence, we only need to show that for a given $\mathcal{S}$, all uppers bounds on $\sum_{k\in\mathcal{S}} R_k^{\mathrm{s}}$ with $\psi \in \Psi_{\mathcal{S}} \setminus \{\mathcal{S}\}$ given in (29) is no tighter than that with $\psi = \{\mathcal{S}\}$, i.e., proving

$$I(X_{\mathcal{S}}; Z|X_{\overline{\mathcal{K}'}}) \ge \sum_{\mathcal{S}_j\in\psi} I(X_{\mathcal{S}_j}; Z|X_{\overline{\mathcal{K}'}}), \forall \psi \in \Psi_{\mathcal{S}} \backslash \{\mathcal{S}\}. \tag{32}$$

Since the sets in any ψ is a division of $\mathcal{S}$, using the chain rule of mutual information, we have

$$\begin{aligned}
&I(X_{\mathcal{S}}; Z|X_{\overline{\mathcal{K}'}})\\
=&I(X_{\mathcal{S}_1}, \cdots, X_{\mathcal{S}_J}; Z|X_{\overline{\mathcal{K}'}})\\
=&I(X_{\mathcal{S}_1}; Z|X_{\overline{\mathcal{K}'}}) + \cdots + I(X_{\mathcal{S}_J}; Z|X_{\mathcal{S}_1}, \cdots, X_{\mathcal{S}_{J-1}}, X_{\overline{\mathcal{K}'}})\\
\ge& \sum_{\mathcal{S}_j\in\psi} I(X_{\mathcal{S}_j}; Z|X_{\overline{\mathcal{K}'}}), \forall \psi \in \Psi_{\mathcal{S}} \setminus \{\mathcal{S}\},
\end{aligned} \tag{33}$$

where the last step holds since $X_k, \forall k \in \mathcal{K}$ are independent of each other. (32) is thus true and this completes the proof.

Appendix B
Proof of Theorem 4

We first prove (25). Using the chain rule of mutual information, the left-hand-side term of (23) is upper bounded by

$$\begin{aligned}
&I(X_{\mathcal{K}_0\cup\mathcal{V}}; Y|X_{\mathcal{K}'\backslash(\mathcal{K}_0\cup\mathcal{V})}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}_0\cup\mathcal{V}}; Z|X_{\overline{\mathcal{K}'}})\\
=&I(X_{\mathcal{K}_0}, X_{\mathcal{V}}; Y|X_{\mathcal{K}'\backslash(\mathcal{K}_0\cup\mathcal{V})}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}_0}, X_{\mathcal{V}}; Z|X_{\overline{\mathcal{K}'}})\\
=&I(X_{\mathcal{K}_0}; Y|X_{\mathcal{K}'\backslash\mathcal{K}_0}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}_0}; Z|X_{\overline{\mathcal{K}'}})\\
&+I(X_{\mathcal{V}}; Y|X_{\mathcal{K}'\backslash(\mathcal{K}_0\cup\mathcal{V})}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{V}}; Z|X_{\overline{\mathcal{K}'}\cup\mathcal{K}_0})\\
\overset{\text{(a)}}{\le}&I(X_{\mathcal{V}}; Y|X_{\mathcal{K}'\backslash(\mathcal{K}_0\cup\mathcal{V})}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{V}}; Z|X_{\overline{\mathcal{K}'}\cup\mathcal{K}_0})\\
\overset{\text{(b)}}{\le}&I(X_{\mathcal{V}}; Y|X_{\mathcal{K}'\backslash(\mathcal{K}_0\cup\mathcal{V})}, X_{\overline{\mathcal{K}'}\cup\mathcal{K}_0}) - I(X_{\mathcal{V}}; Z|X_{\overline{\mathcal{K}'}\cup\mathcal{K}_0})\\
=&I(X_{\mathcal{V}}; Y|X_{\overline{\mathcal{V}}}, X_{\overline{\mathcal{K}''}}) - I(X_{\mathcal{V}}; Z|X_{\overline{\mathcal{K}''}}), \forall \mathcal{V} \subseteq \mathcal{K}'', \mathcal{V} \ne \phi,
\end{aligned} \tag{34}$$

where (34a) follows by using (22), (34b) holds by introducing $X_{\mathcal{K}_0}$ 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 $\mathcal{K}''$ as well as $\overline{\mathcal{K}''}$ in (24). Combining (23) and (34), we know that (25) is true.

Now we prove the second part of Theorem 4, i.e., if a rate tuple $(R_1^{\mathrm{s}}, \cdots, R_K^{\mathrm{s}})$ is in region $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ and has (22) as well as (23) met, it is also in $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}'')$. If (22) is satisfied, it is known from (9) that $R_k^{\mathrm{s}} = 0, \forall k \in \mathcal{K}_0$. Hence,

$$R_k^{\mathrm{s}} = 0, \forall k \in \overline{\mathcal{K}''}. \tag{35}$$

Since $(R_1^{\mathrm{s}}, \cdots, R_K^{\mathrm{s}})$ is in $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}')$ and $R_k^{\mathrm{s}} = 0, \forall k \in \mathcal{K}_0$, it satisfies

$$\begin{aligned}
\sum_{k\in\mathcal{V}} R_k^{\mathrm{s}} =& \sum_{k\in\mathcal{K}_0\cup\mathcal{V}} R_k^{\mathrm{s}}\\
\le& I(X_{\mathcal{K}_0\cup\mathcal{V}}; Y|X_{\mathcal{K}'\backslash(\mathcal{K}_0\cup\mathcal{V})}, X_{\overline{\mathcal{K}'}}) - I(X_{\mathcal{K}_0\cup\mathcal{V}}; Z|X_{\overline{\mathcal{K}'}})\\
\le& I(X_{\mathcal{V}}; Y|X_{\overline{\mathcal{V}}}, X_{\overline{\mathcal{K}''}}) - I(X_{\mathcal{V}}; Z|X_{\overline{\mathcal{K}''}}), \forall \mathcal{V} \subseteq \mathcal{K}'',
\end{aligned} \tag{36}$$

where the first inequation is obtained directly from (9) by replacing $\mathcal{S}$ in (9) with $\mathcal{K}_0 \cup \mathcal{V}$, and the last step follows by using (34). Note that due to (23), the $[\cdot]^+$ operation in the first inequation in (36) can be omitted. (35) together with (36) shows that the rate tuple $(R_1^{\mathrm{s}}, \cdots, R_K^{\mathrm{s}})$ can have (26) satisfied and is thus also in $\mathscr{R}(X_{\mathcal{K}}, \mathcal{K}'')$. Theorem 4 is then proven.

References

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

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

[3] 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.

[4] 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, Jul. 2006, pp. 957–961.

[5] 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.

[6] 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.

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

[8] 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.

[9] ——, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] H. Xu, , K.-K. Wong, and G. Caire, "A new achievable region of the K-user MAC wiretap channel with confidential and open messages under strong secrecy," *In preparation*.

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

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