Journal of Universal Computer Science, vol. 25, no. 8 (2019), 904-924
submitted: 26/12/18, accepted: 15/6/18, appeared: 28/8/19

Secrecy over Multiple-Access Channel: A Game of Competition and Cooperation

Yanling Chen
(University of Duisburg-Essen, Germany
yanling.chen@uni-due.de)

O. Ozan Koyluoglu
(University of California, Berkeley, USA
ozan.koyluoglu@berkeley.edu)

A. J. Han Vinck
(University of Duisburg-Essen, Germany
University of Johannesburg, South Africa
han.vinck@uni-due.de)

Abstract: Communication networks have had a transformative impact on our society as they have revolutionized almost all aspects of human interaction. The explosive growth of data traffic has led to an increased demand on improving the reliability, efficiency and security aspects of the systems. In this paper, we focus on the multiple access channel, a communication model where several transmitters communicate to a common receiver (e.g., a cellular telephone network) in the presence of an external eavesdropper. The goal is to explore the competitive yet cooperative relationship between the transmitters in order to obtain an efficient communication under a certain reliability and security guarantee. Moreover, we take a special look into the inner and outer bounds on the secrecy capacity regions over the 2-transmitter DM-MAC with a degraded eavesdropper (assuming that both transmitters are cooperative). We notice that the inner and outer bounds differentiate themselves in the permissible sets of input distributions and thus not tight in general. This leaves the problem of secrecy capacity regions still open.

Key Words: communication networks, multiple access channel, secrecy
Category: E.4

1 Introduction

1.1 Ubiquitous communication

Over the last decades, wireless communication has transformed from a niche technology into an indispensable part of life. The combination of ubiquitous cellular phone service and rapid growth of the Internet has created an environment where consumers desire seamless, high quality connectivity at all times and from virtually all locations. In fact, we are entering a new paradigm of information technology called Ambient Intelligence (AmI) that brings smartness to living and business environments to make them more sensitive, adaptive, autonomous and personalized to human needs. Towards AmI, ubiquitous communication severs as a key technology.

Most traditional wireless systems are based on the cellular methodology, where the area to be covered is broken into geographical cells. A base station (or access point) is placed in each cell, and the wireless users in each cell communicate exclusively with the corresponding base station, which acts as a gateway to the rest of the network. The single cell model shown in Fig. 1, in which there is a base station and multiple mobile devices. When the base station is transmitting messages to the mobiles, the channel is referred to as a downlink or broadcast channel (BC). Conversely, when the mobiles are transmitting messages to the base station, the channel is referred to as an uplink or multiple-access channel (MAC). Both BC and MAC are two important branches in the extensive field of the multiple-user communication. In this paper, we mainly focus on the MAC.

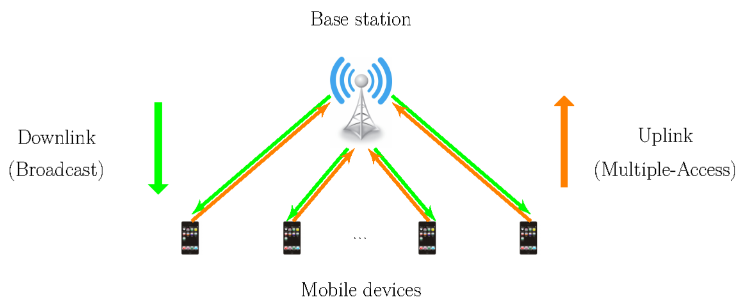

Figure 1: Cellular channel model.

1.2 Previous studies on MAC

The study of MAC can be traced back to the classic papers from the 70s. For the discrete memoryless MAC (DM-MAC) with independent messages, Ahlswede [Ahlswede 1973] first studied the 2-transmitter and 3-transmitter cases and determined the respective capacity regions; whilst Liao [Liao 1972] considered the general K-transmitter DM-MAC and fully characterized its capacity region. There are also many studies on different extensions of MAC, such as MAC with correlated sources [Slepian and Wolf 1973, Han 1979, Cover et al. 1980] and the Gaussian MAC [Cover 1975]. An extensive survey on the information-theoretic aspects of MAC was given in [Van der Meulen 1977].

Another remarkable result on MAC is that the capacity region of a memoryless MAC can be increased by feedback, unlike the capacity of a single user memoryless channel. Especially, Gaarder and Wolf [Gaarder and Wolf 1975], Cover and Leung-Yan-Cheong [Cover and Leung-Yan-Cheong 1976], by providing examples of the binary erasure MAC and the Gaussian MAC, respectively, showed that feedback will enlarge the capacity region of the 2-transmitter MAC. Several general achievable rate regions for the 2-transmitter MAC with noiseless feedback (MAC-FB) were established by Cover and Leung [Cover and Leung 1981], Carleial [Carleial 1982], Bross and Lapidoth [Bross and Lapidoth 2005], Venkataramanan and Pradhan [Venkataramanan and Pradhan 2011]; a dependence balance based outer bound was provided in [Hekstra and Willems 1989]; and constructive coding strategies that exploit feedback were discussed in [Vinck 1983, Vinck et al. 1985, Vinck 1985, Khachatrian and Martirossian 1998, Kramer 1999, Vinck 2007]. Nevertheless, the capacity region of the 2-transmitter MAC-FB remains unknown in general, except for a special class, in which at least one input is a function of the output and the other input [Willems 1982].

1.3 Secrecy over MAC: Transmitting confidential information

Nowadays, general awareness of user privacy in society has increased, leading to a greater focus on the protection of user metadata and communication. Inspired by the pioneering works of Wyner [Wyner 1975] and Csiszár and Körner [Csiszár and Körner 1978] that studied the information theoretic secrecy for a point-to-point communication in the presence of an external eavesdropper, MAC with an external eavesdropper was first introduced in [Tekin and Yener 2008a]. In particular, [Tekin and Yener 2008a] focused on a K-transmitter Gaussian MAC with a degraded external eavesdropper and established several achievable rate regions subject to pre-specified secrecy levels; while a later work [Tekin and Yener 2008b] extends the results of [Tekin and Yener 2008a] to the general Gaussian MAC and general Gaussian two-way channel (TWC).

For the discrete case, a 2-transmitter DM-MAC with an external eavesdropper was considered in [Tang et al. 2007]. Note that the model in [Tang et al. 2007] took into account the generalized feedback that may enable cooperation between transmitters; and, a *joint* secrecy constraint (i.e., information leakage rate from *both* messages to the eavesdropper is made vanishing) was imposed at the eavesdropper. Achievable secrecy rate regions were derived in [Tang et al. 2007]. Additional studies include [Yassaee and Aref 2010] and [Wiese and Boche 2013] that investigated MAC with a stronger secrecy criteria (i.e., the *amount* of information leakage from both messages to the eavesdropper is made vanishing). Nevertheless, for the general 2-transmitter DM-MAC (e.g., with an eavesdropper not necessarily degraded), the *joint* secrecy capacity region still remains open.

Besides, there is a relevant direction, i.e., the 2-transmitter MAC with confidential messages (without an external eavesdropper) [Liang and Poor 2008], worth mentioning. More specifically, the MAC with one (resp. two) confidential message (resp. messages) generalizes the classic 2-transmitter MAC in that one

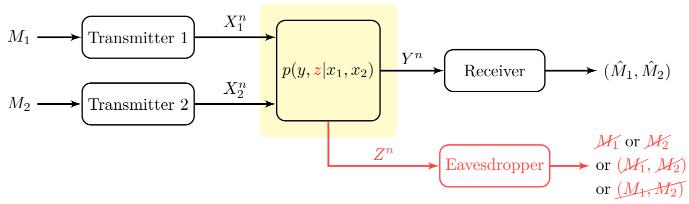

Figure 2: 2-transmitter DM-MAC with an external eavesdropper.

(resp. each) transmitter receives also channel output, and views the other as an eavesdropper. Note that both models were well studied in [Liang and Poor 2008].

2 Secure communication over 2-transmitter DM-MAC

In this paper, we denote random variables U, V, X, etc. by capital letters, their realizations by the corresponding lower case letters and their images (or ranges) by calligraphic letters. In addition, we use $X \sim p(x)$ to denote the fact that X has a probability mass function $p(x)$. This convention applies to a vector of random variables as well.

2.1 System model

In this paper, we focus on the 2-transmitter DM-MAC with an external eavesdropper, the model of which is shown in Fig. 2.

As its name suggests, it consists of 2 transmitters, one legitimate receiver, and one passive eavesdropper, which is defined by the transition probability $p(y, z|x_1, x_2)$. The transmitter i, aims to send message m_i, to the legitimate receiver, where $i \in \{1, 2\}$. Define rate R_i at transmitter i by

$$R_i = \frac{1}{n} H(M_i), \quad \text{for } i = 1, 2, \tag{1}$$

where $H(\cdot)$ is the entropy function [El Gamal and Kim 2012]. Suppose that x_i^n is the channel input at transmitter i, and the channel outputs at the legitimate receiver and eavesdropper are y^n and z^n, respectively. By the *discrete memoryless* nature of the channel (without any feedback), we have

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

Over such a channel model, the goal is to achieve a reliable and secure communication. To do it, we first define a secrecy code. More specifically, a $(2^{nR_1}, 2^{nR_2}, n)$ secrecy code $\mathcal{C}_n$ for the 2-transmitter DM-MAC consists of

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

2.2 System requirements

Reliability at the legitimate receiver:

Define the *average probability of decoding error* at the legitimate receiver by

$$P_e^n(\mathcal{C}_n) = \frac{1}{2^{n[R_1+R_2]}} \sum_{m_1 \in \mathcal{M}_1} \sum_{m_2 \in \mathcal{M}_2} \Pr\left\{ \bigcup_{i \in \{1,2\}} \{m_i \neq \hat{m}_i\} \mid \mathcal{C}_n \right\}. \tag{3}$$

Note that $P_e^n(\mathcal{C}_n) = \Pr\left\{\{M_1 \neq \hat{M}_1\} \bigcup \{M_2 \neq \hat{M}_2\} | \mathcal{C}_n\right\}$ if M_1, M_2 are uniformly distributed over their corresponding message sets.

Secrecy against the eavesdropper:

Suppose that the transmitters are aware of the presence of the passive eavesdropper. Briefly, we have the following scenarios:

- The secrecy of the messages is not of concern to both transmitters; or,
- The secrecy of the respective message is of concern only to one transmitter. In more details, we have the following possibilities:
  - Secrecy of M_1 is required, but not M_2. We define the *information leakage rate* of M_1 from transmitter 1 to the eavesdropper by

    $$R_{L,\{1\}}(\mathcal{C}_n) = \frac{1}{n} I(M_1; Z^n | \mathcal{C}_n), \tag{4}$$

    where $I(\cdot)$ is the mutual information function [El Gamal and Kim 2012].
  - Secrecy of M_2 is required, but not M_1. We define the *information leakage rate* of M_2 from transmitter 2 to the eavesdropper by

    $$R_{L,\{2\}}(\mathcal{C}_n) = \frac{1}{n} I(M_2; Z^n | \mathcal{C}_n). \tag{5}$$

- The secrecy of the messages is of concern to both transmitters. In this scenario, we have the following two cases:

- From end user point of view, each transmitter only cares about the secrecy of its own message. This is equivalent to limit

$$R_{L,\{1\},\{2\}}(\mathcal{C}_n) = R_{L,\{1\}}(\mathcal{C}_n) + R_{L,\{2\}}(\mathcal{C}_n). \tag{6}$$

  In this case, the correlation information between M_1 and M_2 may be leaked to the eavesdropper, say $M_1 \oplus M_2$ but not M_1, M_2 individually.

- From the system designer's perspective, the information leakage of M_1, M_2 is considered jointly by defining

$$R_{L,\{1,2\}}(\mathcal{C}_n) = \frac{1}{n} I(M_1, M_2; Z^n|\mathcal{C}_n). \tag{7}$$

  Note that $R_{L,\{1,2\}}(\mathcal{C}_n) \to 0$ implies that $R_{L,\{1\}}(\mathcal{C}_n) \to 0$ and $R_{L,\{2\}}(\mathcal{C}_n) \to 0$ and thus $R_{L,\{1\},\{2\}}(\mathcal{C}_n) \to 0$. This is due to the non-negativity of the mutual information and by definition, $R_{L,\{1,2\}} \geq R_{L,\{i\}}$ for $i = 1, 2$. That is, imposing a limit on (7) implies limits on (4), (5) and (6) as well. As the limit becomes arbitrarily small, the correlation information between M_1 and M_2 may not be leaked to the eavesdropper in this case.

Cooperative or competitive transmission strategy at the transmitters:

If there is no secrecy concern, the transmitters are competitive since they have to share the same channel resource. However, in case of a secure communication, the transmitters can be also cooperative since the transmission of one user essentially helps to hide the other user's message from the eavesdropper. Especially in case that only one message is required to be kept confidential from the eavesdropper, the other transmitter may

- use a deterministic encoder (which is conventionally used for DM-MAC without secrecy). The transmitter can compete in this case for the channel resource (i.e., being competitive); or,
- use a stochastic encoder (which is common in achieving information theoretic secrecy), helping to hide other transmitter' message from the eavesdropper (i.e., being cooperative).

Considering that secrecy does not come for free, we assume that the transmitter who demands secrecy for its message, will use the stochastic encoder. Thus,

- if there is no secrecy requirement from both transmitters, then both use deterministic encoders, i.e., being competitive;
- if only one transmitter demands secrecy for its message, then it uses the stochastic encoder, i.e., being cooperative; while, the other transmitter could be either cooperative or competitive;

– if both transmitters demand secrecy for their messages, (including both the individual or joint secrecy), then both use the stochastic encodes, i.e., being cooperative.

We remark here that the deterministic encoder can be considered as a special case of the stochastic encoder. Therefore, for the transmitter, being cooperative will be at least as good as being competitive in achieving the desired transmission rates. Recall the fact that being competitive is sufficient in achieving the capacity region in case of no secrecy constraints, i.e., being cooperative does not provide any gain in the reliable communication over MAC. However, the problem of our interest is, if there is any gain in secure communication over MAC for being cooperative; and if yes, how much is the gain?

2.3 System throughput

If there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes $\{\mathcal{C}_n\}$ such that

$$P_e^n(\mathcal{C}_n) \leq \epsilon_n \quad \text{and} \quad \lim_{n\to\infty} \epsilon_n = 0, \tag{8}$$

$$R_L(\mathcal{C}_n) \leq \tau_n \quad \text{and} \quad \lim_{n\to\infty} \tau_n = 0, \tag{9}$$

then the rate pair (R_1, R_2) is said to be *achievable under the secrecy constraint defined by (9)*. Note that (8) is the *reliability constraint*; and (9) is the *secrecy constraint*. In particular, if $R_L(\mathcal{C}_n)$ in (9) is defined by (4), or (5), or (7), it corresponds to the $\mathcal{S}$-collective secrecy that is introduced in [Chen et al. 2018], for $\mathcal{S}$ being $\{1\}, \{2\}$ or $\{1, 2\}$, respectively. More specifically, (R_1, R_2) is said to be

1) $\{1\}$-collective secrecy achievable, if $R_L(\mathcal{C}_n)$ is defined by (4);

2) $\{2\}$-collective secrecy achievable, if $R_L(\mathcal{C}_n)$ is defined by (5);

3) individual secrecy achievable, if $R_L(\mathcal{C}_n)$ is defined by (6);

4) $\{1, 2\}$-collective or joint secrecy achievable, if $R_L(\mathcal{C}_n)$ is defined by (7).

Clearly, for given reliability and secrecy constraints, the union of all the achievable rate pairs gives the respective achievable rate regions, providing fundamental limits on the system throughput.

3 Discussions

3.1 Impact of different secrecy requirements

Recall that $\mathcal{S}$-collective secrecy is studied in [Chen et al. 2018], which includes all the instances of the above discussed secrecy requirements except the individual

Table 1: 2-transmitter DM-MAC with an external eavesdropper: under different secrecy constraints with both transmitters being cooperative.

		Rate region	Input distribution
$\mathcal{C}$:	No secrecy [El Gamal and Kim 2012, Theorem 4.3]	$R_1 \leq I(X_1;Y\|X_2,Q)$ $R_2 \leq I(X_2;Y\|X_1,Q)$ $R_1+R_2 \leq I(X_1,X_2;Y\|Q)$	$(Q,X_1,X_2) \sim p(q)p(x_1\|q)p(x_2\|q)$
$\mathcal{R}_{\{1\}}$:	$\{1\}$ − collective secrecy $\frac{1}{n}I(M_1;Z^n) \to 0$ [Chen et al. 2018, Theorem 1]	$R_2 \leq I(V_2;Y\|V_1,Q)$ $R_1 \leq \min\left\{\begin{array}{l} I(V_1;Y\|V_2,Q)-I(V_1;Z\|Q) \\ I(V_1,V_2;Y\|Q)-I(V_1,V_2;Z\|Q) \end{array}\right\}$ $R_1+R_2 \leq I(V_1,V_2;Y\|Q)-I(V_1;Z\|Q)$	$(Q,V_1,V_2,X_1,X_2) \sim p(q)\prod_{i=1}^{2} p(v_i\|q)p(x_i\|v_i)$ such that $I(V_2;Z\|Q) \leq I(V_2;Y\|V_1,Q)$
$\mathcal{R}_{\{2\}}$:	$\{2\}$ − collective secrecy $\frac{1}{n}I(M_2;Z^n) \to 0$ [Chen et al. 2018, Theorem 1]	$R_1 \leq I(V_1;Y\|V_2,Q)$ $R_2 \leq \min\left\{\begin{array}{l} I(V_2;Y\|V_1,Q)-I(V_2;Z\|Q) \\ I(V_1,V_2;Y\|Q)-I(V_1,V_2;Z\|Q) \end{array}\right\}$ $R_1+R_2 \leq I(V_1,V_2;Y\|Q)-I(V_2;Z\|Q)$	$(Q,V_1,V_2,X_1,X_2) \sim p(q)\prod_{i=1}^{2} p(v_i\|q)p(x_i\|v_i)$ such that $I(V_1;Z\|Q) \leq I(V_1;Y\|V_2,Q)$
$\mathcal{R}_{\{1\},\{2\}}$:	Individual secrecy [Chen et al. 2016, Theorem 1] $\frac{1}{n}I(M_1;Z^n) \to 0$ $\frac{1}{n}I(M_2;Z^n) \to 0$	$R_1 \leq I(V_1;Y\|V_2,Q)-I(V_1;Z\|Q)$ $R_2 \leq I(V_2;Y\|V_1,Q)-I(V_2;Z\|Q)$ $\max\{R_1,R_2\} \leq I(V_1,V_2;Y\|Q)-I(V_1,V_2;Z\|Q)$ $R_1+R_2 \leq I(V_1,V_2;Y\|Q)-I(V_1;Z\|Q)-I(V_2;Z\|Q)$	$(Q,V_1,V_2,X_1,X_2) \sim p(q)\prod_{i=1}^{2} p(v_i\|q)p(x_i\|v_i)$
$\mathcal{R}_{\{1,2\}}$:	$\{1,2\}$ − collective secrecy i.e., joint secrecy [Chen et al. 2016, Theorem 2] $\frac{1}{n}I(M_1,M_2;Z^n) \to 0$	$R_1 \leq I(V_1;Y\|V_2,Q)-I(V_1;Z\|Q)$ $R_2 \leq I(V_2;Y\|V_1,Q)-I(V_2;Z\|Q)$ $R_1+R_2 \leq I(V_1,V_2;Y\|Q)-I(V_1,V_2;Z\|Q)$	$(Q,V_1,V_2,X_1,X_2) \sim p(q)\prod_{i=1}^{2} p(v_i\|q)p(x_i\|v_i)$

secrecy. Nevertheless, the individual secrecy has been studied in [Chen et al. 2016] together with joint secrecy for the 2-transmitter DM-MAC with an external eavesdropper. In addition, the capacity region in case of no secrecy constraint has been characterized [Ahlswede 1973] (see also [El Gamal and Kim 2012, Theorem 4.3]). Therefore, we could give a rather complete review on the achievable rate regions under different secrecy constraints.

For a fair comparison, we consider the optimistic case that both transmitter are cooperative in all scenarios. In Table 1, we provide the respective regions corresponding to the 5 different secrecy strengths (in which 4 secrecy constraints are as discussed above and the additional one is no secrecy constraint). In particular, we denote the $\mathcal{S}$-collective secrecy region to be $\mathcal{R}_\mathcal{S}$ for $\mathcal{S} \in \{1,2\}$, $\mathcal{S} \neq \emptyset$, $\mathcal{C}$ for the case of no secrecy, and $\mathcal{R}_{\{1\},\{2\}}$ for the individual secrecy rate region.

We provide a numerical illustration in Fig. 3, where we plotted all these regions for a 2-transmitter DM-MAC with an external eavesdropper, where the channel from (X_1,X_2) to Y is a binary multiplier MAC (i.e., $Y = X_1 \cdot X_2$), and Z is a degraded version of Y through a binary symmetric channel (BSC) with crossover probability $p = 0.1$. Note that V_1, V_2 are taken as binary for the calculations. Not surprisingly, we observe that $\mathcal{R}_{\{1,2\}} \subseteq \mathcal{R}_{\{1\},\{2\}} \subseteq \mathcal{R}_{\{1\}}$ or $\mathcal{R}_{\{2\}} \subseteq \mathcal{C}$, where $\mathcal{R}_{\{1,2\}}$ is enclosed by (red) dashed lines; $\mathcal{R}_{\{1\},\{2\}}$ by (yellow) dotted lines; $\mathcal{R}_{\{1\}}$ and $\mathcal{R}_{\{2\}}$ by dash-dotted lines (blue for $\mathcal{R}_{\{1\}}$ and forest-green for $\mathcal{R}_{\{2\}}$, respectively); and $\mathcal{C}$ by (green) solid lines. Note that the inclusion relation of these regions is due to the correspondingly relaxed secrecy strengths. That is, more stringent is the secrecy requirement, smaller is the correspondingly achievable secrecy region. Another interesting observation is that $\mathcal{R}_{\{1\},\{2\}} \subset \mathcal{R}_{\{1\}} \cap \mathcal{R}_{\{2\}}$. In other words, $\mathcal{R}_{\{1\},\{2\}} = \mathcal{R}_{\{1\}} \cap \mathcal{R}_{\{2\}}$ does not hold. This implies that there are rate pairs achievable for either the secrecy of M_1 or the secrecy of M_2, but not the secrecy of M_1 and secrecy of M_2 simultaneously (i.e., individual secrecy).

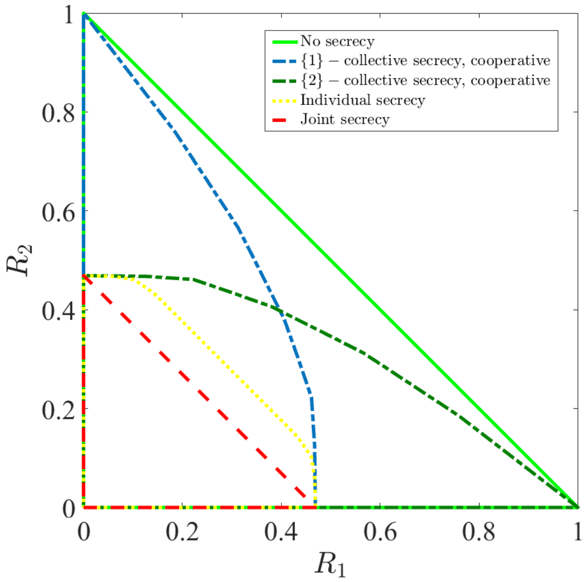

Figure 3: Achievable rate regions for a binary multiplier 2-transmitter MAC with a degraded eavesdropper, with different secrecy constraints but cooperative transmitters. See [Chen et al. 2018, Fig. 2(b)].

3.2 Impact of transmitters being cooperative or competitive

Recall the fact that being cooperative does not provide any gain in the reliable communication over MAC (i.e., no secrecy requirement). However, we wonder if it is still the case in the secure communication over MAC.

Table 2: 2-transmitter DM-MAC with an external eavesdropper: {1}-collective secrecy.

	Competitive Transmitter 2, [Chen et al. 2018, (10) in Theorem 1]	Cooperative Transmitter 2, [Chen et al. 2018, (11) in Theorem 1]
Rate region	$R_2 \geq I(V_2;Z\|Q)$ $R_2 \leq I(V_2;Y\|V_1,Q)$ $R_1 \leq \min \begin{Bmatrix} I(V_1;Y\|V_2,Q) - I(V_1;Z\|Q) \\ I(V_1,V_2;Y\|Q) - I(V_1,V_2;Z\|Q) \end{Bmatrix}$ $R_1 - R_2 \leq I(V_1;Y\|V_2,Q) - I(V_1,V_2;Z\|Q)$ $R_1 + R_2 \leq I(V_1,V_2;Y\|Q) - I(V_1;Z\|Q)$	$R_2 \leq I(V_2;Y\|V_1,Q)$ $R_1 \leq \min \begin{Bmatrix} I(V_1;Y\|V_2,Q) - I(V_1;Z\|Q) \\ I(V_1,V_2;Y\|Q) - I(V_1,V_2;Z\|Q) \end{Bmatrix}$ $R_1 + R_2 \leq I(V_1,V_2;Y\|Q) - I(V_1;Z\|Q)$
Input distribution	$(Q,V_1,V_2,X_1,X_2) \sim p(q) \prod_{i=1}^{2} p(v_i\|q)p(x_i\|v_i)$ such that $I(V_2;Z\|Q) \leq I(V_2;Y\|V_1,Q)$	

Consider the specific case that transmitter 1 would like to keep its message secret from the eavesdropper; while transmitter 2 not. That is, transmitter 1 uses a stochastic encoder for the purpose of secrecy of M_1; while transmitter

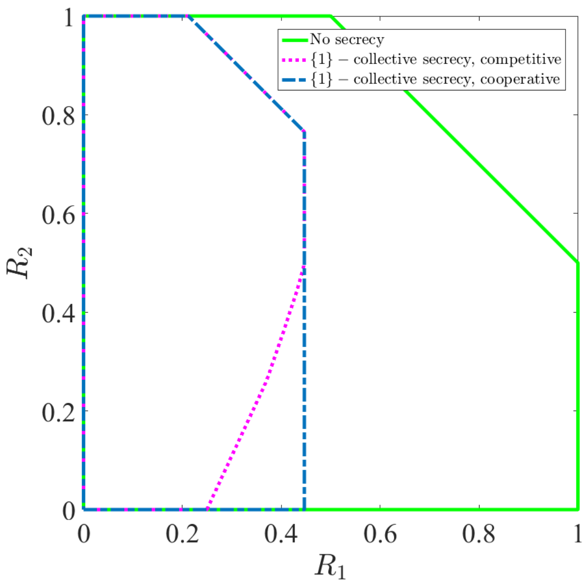

Figure 4: Achievable rate regions for a binary input adder 2-transmitter MAC with a degraded eavesdropper, where transmitter 1 demands the secrecy but not transmitter 2. See [Chen et al. 2018, Fig. 2(a)].

2 may take a conventional deterministic encoder for being competitive for the same channel resource; or take a stochastic encoder for being cooperative to help to hide M_1 from the eavesdropper. According to [Chen et al. 2018, Theorem 1], we have two achievable regions corresponding to these two different transmission strategies at transmitter 2, and we provide them in Table 2.

Moreover, a numerical illustration is provided in Fig. 4, where we show the advantage of transmitter 2 being cooperative (in obtaining a larger secrecy rate region) by a concrete example. Consider the 2-transmitter DM-MAC with an external eavesdropper, where the channel from (X_1, X_2) to Y is a binary input adder MAC (i.e., $Y = X_1 + X_2$), and Z is a degraded version of Y with $p(z|y) = 1-p$ for $z = y$ and $p(z|y) = p$ for $z = y+1 \pmod 3$, where $p = 0.1$. In Fig. 4, we depict the respective achievable regions (with binary V_1, V_2 for the calculations), where the one enclosed by (magenta) dotted lines is for the case of transmitter 2 being competitive; and the one enclosed by (blue) dash-dotted lines is for the case of transmitter 2 being cooperative. The capacity region (without secrecy constraint) is also plotted for reference purpose, which is enclosed by the (green) solid lines.

As one can see in Fig. 4, in case of transmitter 2 being cooperative, the region is strictly larger than the case of transmitter 2 being competitive. In particular, a big gap in the achievable secret rate R_1 can be observed at $R_2 = 0$. The gap indicates that transmitter 2 can indeed help the secret transmission of transmitter 1 by sending random signals to jam the eavesdropper. (This is similar to the cooperative jamming observed in the Gaussian scenario [Tekin and Yener 2008b], but as its counterpart in the discrete setting. More specifically, in this case, transmitter 2 have two ways of cooperation, one is to utilize codewords that carry randomization (bogus) messages and the other is to utilize additional noise in mapping codewords to channel inputs (channel prefixing)). Even in case that transmitter 2 uses a deterministic encoder, its transmission at low rates to some extent, could help transmitter 1 to achieve a larger secrecy rate. However, the advantage of using cooperative transmission strategy at transmitter 2, diminishes or even vanishes especially when R_2 is at high rates. This is because of the bounded sum rate capacity, due to the fact that the same channel resource is shared by both transmitters. This observation provides interesting insights into the competitive yet cooperative relationship between the transmitters in a secure communication, unlike their simple competitive relationship in a reliable communication.

4 Fundamental limits on the system performance

For simplicity, we only consider the special case that the channel to the eavesdropper is *degraded* to the one to the legitimate receiver, referred to as 2-transmitter DM-MAC with a degraded eavesdropper. In this section, we provide inner bounds and outer bounds on the secrecy capacity regions in Table 3 and Table 4, respectively, while assuming that both transmitters are cooperative.

4.1 Inner bounds on the secrecy capacity regions

The inner bounds are given in Table 3, which can be obtained by taking $V_1 = X_1$ and $V_2 = X_2$ in the achievable rate regions in Table 1. Remarkably, here the input variables (Q, X_1, X_2) have a distribution in form of $p(q)p(x_1|q)p(x_2|q)$.

4.2 Outer bounds on the secrecy capacity regions

The outer bounds are given in Table 4. As one may notice, they enjoy the same expressions as those for the corresponding inner bounds in Table 3; but differentiate themselves in the allowable input distribution for (Q, X_1, X_2), here in form of $p(q)p(x_1, x_2|q)$.

To establish the outer bounds, we need the following lemma, which proof is provided in Appendix A.

Table 3: 2-transmitter DM-MAC with an external eavesdropper: inner bounds on rate region under different secrecy constraints.

		Rate region	Input distribution
$\underline{\mathcal{R}}_{\{1\}}$:	$\{1\}$ – collective secrecy $\frac{1}{n}I(M_1;Z^n) \to 0$ [Chen et al. 2018, Theorem 1]	$R_2 \leq I(X_2;Y\|X_1,Q)$ $R_1 \leq \min \left\{ \begin{array}{l} I(X_1;Y\|X_2,Q) - I(X_1;Z\|Q) \\ I(X_1,X_2;Y\|Q) - I(X_1,X_2;Z\|Q) \end{array} \right\}$ $R_1 + R_2 \leq I(X_1,X_2;Y\|Q) - I(X_1;Z\|Q)$	$(Q,X_1,X_2) \sim p(q)p(x_1\|q)p(x_2\|q)$
$\underline{\mathcal{R}}_{\{2\}}$:	$\{2\}$ – collective secrecy $\frac{1}{n}I(M_2;Z^n) \to 0$ [Chen et al. 2018, Theorem 1]	$R_1 \leq I(X_1;Y\|X_2,Q)$ $R_2 \leq \min \left\{ \begin{array}{l} I(X_2;Y\|X_1,Q) - I(X_2;Z\|Q) \\ I(X_1,X_2;Y\|Q) - I(X_1,X_2;Z\|Q) \end{array} \right\}$ $R_1 + R_2 \leq I(X_1,X_2;Y\|Q) - I(X_2;Z\|Q)$	
$\underline{\mathcal{R}}_{\{1\},\{2\}}$:	Individual secrecy [Chen et al. 2016, Theorem 1] $\frac{1}{n}I(M_1;Z^n) \to 0$ $\frac{1}{n}I(M_2;Z^n) \to 0$	$R_1 \leq I(X_1;Y\|X_2,Q) - I(X_1;Z\|Q)$ $R_2 \leq I(X_2;Y\|X_1,Q) - I(X_2;Z\|Q)$ $\max\{R_1,R_2\} \leq I(X_1,X_2;Y\|Q) - I(X_1,X_2;Z\|Q)$ $R_1 + R_2 \leq I(X_1,X_2;Y\|Q) - I(X_1;Z\|Q) - I(X_2;Z\|Q)$	
$\underline{\mathcal{R}}_{\{1,2\}}$:	$\{1,2\}$ – collective secrecy i.e., joint secrecy [Chen et al. 2016, Theorem 2] $\frac{1}{n}I(M_1,M_2;Z^n) \to 0$	$R_1 \leq I(X_1;Y\|X_2,Q) - I(X_1;Z\|Q)$ $R_2 \leq I(X_2;Y\|X_1,Q) - I(X_2;Z\|Q)$ $R_1 + R_2 \leq I(X_1,X_2;Y\|Q) - I(X_1,X_2;Z\|Q)$	

Table 4: 2-transmitter DM-MAC with an external eavesdropper: outer bounds on rate region under different secrecy constraints.

		Rate region	Input distribution
$\overline{\mathcal{R}}_{\{1\}}$:	$\{1\}$ – collective secrecy $\frac{1}{n}I(M_1;Z^n) \to 0$	$R_2 \leq I(X_2;Y\|X_1,Q)$ $R_1 \leq \min \left\{ \begin{array}{l} I(X_1;Y\|X_2,Q) - I(X_1;Z\|Q) \\ I(X_1,X_2;Y\|Q) - I(X_1,X_2;Z\|Q) \end{array} \right\}$ $R_1 + R_2 \leq I(X_1,X_2;Y\|Q) - I(X_1;Z\|Q)$	$(Q,X_1,X_2) \sim p(q)p(x_1,x_2\|q)$
$\overline{\mathcal{R}}_{\{2\}}$:	$\{2\}$ – collective secrecy $\frac{1}{n}I(M_2;Z^n) \to 0$	$R_1 \leq I(X_1;Y\|X_2,Q)$ $R_2 \leq \min \left\{ \begin{array}{l} I(X_2;Y\|X_1,Q) - I(X_2;Z\|Q) \\ I(X_1,X_2;Y\|Q) - I(X_1,X_2;Z\|Q) \end{array} \right\}$ $R_1 + R_2 \leq I(X_1,X_2;Y\|Q) - I(X_2;Z\|Q)$	
$\overline{\mathcal{R}}_{\{1\},\{2\}}$:	Individual secrecy $\frac{1}{n}I(M_1;Z^n) \to 0$ $\frac{1}{n}I(M_2;Z^n) \to 0$	$R_1 \leq I(X_1;Y\|X_2,Q) - I(X_1;Z\|Q)$ $R_2 \leq I(X_2;Y\|X_1,Q) - I(X_2;Z\|Q)$ $\max\{R_1,R_2\} \leq I(X_1,X_2;Y\|Q) - I(X_1,X_2;Z\|Q)$ $R_1 + R_2 \leq I(X_1,X_2;Y\|Q) - I(X_1;Z\|Q) - I(X_2;Z\|Q)$	
$\overline{\mathcal{R}}_{\{1,2\}}$:	$\{1,2\}$ – collective secrecy i.e., joint secrecy $\frac{1}{n}I(M_1,M_2;Z^n) \to 0$	$R_1 \leq I(X_1;Y\|X_2,Q) - I(X_1;Z\|Q)$ $R_2 \leq I(X_2;Y\|X_1,Q) - I(X_2;Z\|Q)$ $R_1 + R_2 \leq I(X_1,X_2;Y\|Q) - I(X_1,X_2;Z\|Q)$	

Lemma 1. *Consider a discrete memoryless channel defined by $p(y,z|x_1,x_2)$ and assume that Z is a degraded version of Y. We have*

$$
\begin{aligned}
I(X_1^n, X_2^n; Y^n) &\leq nI(X_1, X_2; Y|Q); && (10)\\
I(X_1^n; Y^n|X_2^n) &\leq nI(X_1; Y|X_2, Q); && (11)\\
I(X_2^n; Y^n|X_1^n) &\leq nI(X_2; Y|X_1, Q); && (12)\\
I(X_1^n, X_2^n; Z^n) &= nI(X_1, X_2; Z|Q); && (13)\\
I(X_1^n; Z^n) &\geq nI(X_1; Z|Q); && (14)\\
I(X_2^n; Z^n) &\geq nI(X_2; Z|Q), && (15)
\end{aligned}
$$

where $Q = (Z^{T-1}, T)$, $X_1 = X_{1,T}$, $X_2 = X_{2,T}$, $Z = Z_T$, and T is a random variable that is uniformly distributed over $[1:n]$.

4.2.1 Without secrecy constraint

First we consider the general outer bounds on R_1, R_2 and $R_1 + R_2$, for the 2-transmitter MAC with a degraded eavesdropper (without secrecy constraint). We have the followings:

$$\begin{aligned} nR_1 =& H(M_1) \\ &\overset{(a)}{\leq} H(M_1) - H(M_1|Y^n, X_2^n) + n\lambda_1(\epsilon_n) \\ &= I(M_1; Y^n, X_2^n) + n\lambda_1(\epsilon_n) \\ &\overset{(b)}{\leq} I(X_1^n; Y^n|X_2^n) + n\lambda_1(\epsilon_n) \qquad (16) \\ &\overset{(c)}{\leq} nI(X_1; Y|X_2, Q) + n\lambda_1(\epsilon_n), \qquad (17) \end{aligned}$$

where (a) is due to reliability constraint (8), Fano's inequality and taking $\lambda_1(\epsilon_n) = 1/n + \epsilon_n R_1$; (b) is due to the Markov chain $M_1 \rightarrow X_1^n \rightarrow (X_2^n, Y^n)$ and the fact that X_1^n and X_2^n are independent; and (c) is by applying (11) in Lemma 1.

A similar proof applies to bound R_2. We have

$$\begin{aligned} nR_2 \leq& I(X_2^n; Y^n|X_1^n) + n\lambda_2(\epsilon_n) \qquad (18) \\ \leq& nI(X_2; Y|X_1, Q) + n\lambda_2(\epsilon_n), \qquad (19) \end{aligned}$$

where $\lambda_2(\epsilon_n) = 1/n + \epsilon_n R_2$.

An outer bound on $R_1 + R_2$ could be obtained as follows:

$$\begin{aligned} n(R_1 + R_2) =& H(M_1, M_2) \\ &\overset{(d)}{\leq} H(M_1, M_2) - H(M_1, M_2|Y^n) + n\lambda(\epsilon_n) \\ &= I(M_1, M_2; Y^n) + n\lambda(\epsilon_n) \\ &\overset{(e)}{\leq} I(X_1^n, X_2^n; Y^n) + n\lambda(\epsilon_n) \\ &\overset{(f)}{\leq} nI(X_1, X_2; Y|Q) + n\lambda(\epsilon_n), \qquad (20) \end{aligned}$$

where (d) is due to reliability constraint (8), Fano's inequality and taking $\lambda(\epsilon_n) = 1/n + \epsilon_n(R_1 + R_2)$; (e) is due to the Markov chain $(M_1, M_2) \rightarrow (X_1^n, X_2^n) \rightarrow Y^n$; and (f) is by applying (10) in Lemma 1.

4.2.2 Under secrecy constraint $\frac{1}{n}I(M_1; Z^n) \rightarrow 0$

Under secrecy constraint $\frac{1}{n}I(M_1; Z^n) \rightarrow 0$, we could bound R_1 as follows:

$$nR_1 = H(M_1)$$

$$
\begin{aligned}
&\overset{(g)}{\leq} H(M_1|Z^n) - H(M_1|M_2, Y^n, Z^n) + n\lambda(\epsilon_n, \tau_n) \\
&\overset{(h)}{\leq} H(M_1|Z^n) - H(M_1|M_2, X_2^n, Y^n, Z^n) + n\lambda(\epsilon_n, \tau_n) \\
&\overset{(i)}{=} H(M_1|Z^n) - H(M_1|X_2^n, Y^n, Z^n) + n\lambda(\epsilon_n, \tau_n) \\
&= I(M_1; X_2^n, Y^n|Z^n) + 2n\lambda(\epsilon_n, \tau_n) \\
&= H(X_2^n, Y^n|Z^n) - H(X_2^n, Y^n|M_1, Z^n) + n\lambda(\epsilon_n, \tau_n) \\
&\overset{(h)}{\leq} H(X_2^n, Y^n|Z^n) - H(X_2^n, Y^n|M_1, X_1^n, Z^n) + n\lambda(\epsilon_n, \tau_n) \\
&\overset{(i)}{=} H(X_2^n, Y^n|Z^n) - H(X_2^n, Y^n|X_1^n, Z^n) + n\lambda(\epsilon_n, \tau_n) \\
&= I(X_1^n; X_2^n, Y^n|Z^n) + n\lambda(\epsilon_n, \tau_n) \\
&= H(X_1^n|Z^n) - H(X_1^n|X_2^n, Y^n, Z^n) + n\lambda(\epsilon_n, \tau_n) \\
&\overset{(j)}{=} H(X_1^n|Z^n) - H(X_1^n|X_2^n, Y^n) - H(X_1^n) + H(X_1^n|X_2^n) + n\lambda(\epsilon_n, \tau_n) \\
&= I(X_1^n; Y^n|X_2^n) - I(X_1^n; Z^n) + n\lambda(\epsilon_n, \tau_n) \qquad (21) \\
&\overset{(k)}{\leq} n\left[I(X_1; Y|X_2, Q) - I(X_1; Z|Q)\right] + n\lambda(\epsilon_n, \tau_n) \qquad (22)
\end{aligned}
$$

where (g) is due to reliability constraint (8), Fano's inequality, the secrecy constraint (9) (i.e., $\frac{1}{n}I(M_1; Z^n) \leq \tau_n$) and taking $\lambda(\tau_n, \epsilon_n) = \tau_n + 1/n + \epsilon_n(R_1 + R_2)$; (h) is by the fact that conditioning does not increase entropy; (i) is due to the Markov chain $M_2 \to X_2^n \to (M_1, Y^n, Z^n)$ and $M_1 \to X_1^n \to (M_2, Y^n, Z^n)$; (j) is due to the fact that Z^n is a degraded version of Y^n; and X_1^n and X_2^n are independent; and (k) is by applying (11) and (14) in Lemma 1.

Besides, we note that

$$nR_1 \leq nR_1 + [nR_2 + n\tau_n - I(M_1, M_2; Z^n)]$$

holds since

$$I(M_1, M_2; Z^n) = I(M_1; Z^n) + I(M_2; Z^n|M_1) \leq nR_2 + n\tau_n;$$

where the inequality is due to the secrecy constrain (9) (i.e., $\frac{1}{n}I(M_1; Z^n) \leq \tau_n$). Therefore, we have

$$
\begin{aligned}
nR_1 &\leq n[R_1 + R_2] - I(M_1, M_2; Z^n) + n\tau_n \\
&\overset{(l)}{\leq} I(M_1, M_2; Y^n) - I(M_1, M_2; Z^n) + n\lambda(\tau_n, \epsilon_n) \\
&\overset{(m)}{\leq} I(X_1^n, X_2^n; Y^n) - I(X_1^n, X_2^n; Z^n) + n\lambda(\tau_n, \epsilon_n) \\
&\overset{(n)}{\leq} n\left[I(X_1, X_2; Y|Q) - I(X_1, X_2; Z|Q)\right] + n\lambda(\tau_n, \epsilon_n), \qquad (23)
\end{aligned}
$$

where (l) is due to reliability constraint (8), Fano's inequality and taking $\lambda(\tau_n, \epsilon_n) = \tau_n + 1/n + \epsilon_n(R_1 + R_2)$; (m) is due to the Markov chain $(M_1, M_2) \to$

$(X_1^n, X_2^n) \to (Y^n, Z^n)$ and the fact that Z^n is a degraded version of Y^n; and (n) is by applying (10) and (13) in Lemma 1.

Moreover, we have

$$\begin{aligned} nR_1 =& H(M_1) \\ \overset{(o)}{\leq}& H(M_1|Z^n) - H(M_1|Y^n, Z^n) + n\lambda(\epsilon_n, \tau_n) \\ =& I(M_1; Y^n|Z^n) + n\lambda(\epsilon_n, \tau_n) \\ \overset{(p)}{\leq}& I(X_1^n; Y^n|Z^n) + n\lambda(\epsilon_n, \tau_n) \\ =& I(X_1^n; Y^n) - I(X_1^n; Z^n) + n\lambda(\epsilon_n, \tau_n), \end{aligned} \tag{24}$$

where (o) is due to reliability constraint (8), Fano's inequality, the secrecy constraint (9) (i.e., $\frac{1}{n}I(M_1; Z^n) \leq \tau_n$) and taking $\lambda(\tau_n, \epsilon_n) = \tau_n + 1/n + \epsilon_n(R_1 + R_2)$; (p) is by the Markov chain $M_2 \to X_2^n \to (Y^n, Z^n)$ and the fact that Z^n is a degraded version of Y^n.

Combining (24) (that is obtained under secrecy constraint $\frac{1}{n}I(M_1; Z^n) \to 0$) and (18) (that is obtained only under reliability constraint) and taking $\lambda_2(\epsilon_n, \tau_n) = \lambda(\epsilon_n, \tau_n) + \lambda_2(\epsilon_n)$, we have

$$\begin{aligned} n(R_1 + R_2) \leq& I(X_1^n; Y^n) - I(X_1^n; Z^n) + I(X_2^n; Y^n|X_1^n) + n\lambda_2(\epsilon_n, \tau_n) \\ =& I(X_1^n, X_2^n; Y^n) - I(X_1^n; Z^n) + n\lambda_2(\epsilon_n, \tau_n) \\ \overset{(q)}{=}& n\left[I(X_1, X_2; Y|Q) - I(X_1; Z|Q)\right] + n\lambda_2(\tau_n, \epsilon_n). \end{aligned} \tag{25}$$

where (q) is by applying (10) and (14) in Lemma 1.

In summary, for $\overline{\mathcal{R}}_{\{1\}}$, we have the general bounds (17), (19), (20) (obtained under the reliability constraint only), and the bounds (22), (23) and (25) (obtained under the additional secrecy constraint $\frac{1}{n}I(M_1; Z^n) \to 0$). We note that (17) and (20) are redundant due to (22) and (25), respectively. Thus taking the limit as $n \to \infty$ such that $\lambda_2(\epsilon_n), \lambda(\epsilon_n, \tau_n), \lambda_2(\epsilon_n, \tau_n) \to 0$ in (19), (22), (23) and (25), we establish the outer bound $\overline{\mathcal{R}}_{\{1\}}$ as given in Table 4.

4.2.3 Under secrecy constraint $\frac{1}{n}I(M_2; Z^n) \to 0$:

A similar approach applies to establish the bound $\overline{\mathcal{R}}_{\{2\}}$. In particular, we have

$$nR_2 \leq I(X_2^n; Y^n|X_1^n) - I(X_2^n; Z^n) + n\lambda(\epsilon_n, \tau_n) \tag{26}$$

$$\leq n\left[I(X_2; Y|X_1, Q) - I(X_2; Z|Q)\right] + n\lambda(\epsilon_n, \tau_n); \tag{27}$$

$$nR_2 \leq n\left[I(X_1, X_2; Y|Q) - I(X_1, X_2; Z|Q)\right] + n\lambda(\tau_n, \epsilon_n) \tag{28}$$

$$n(R_1 + R_2) \leq n\left[I(X_1, X_2; Y|Q) - I(X_2; Z|Q)\right] + n\lambda_1(\tau_n, \epsilon_n), \tag{29}$$

where $\lambda_1(\epsilon_n, \tau_n) = \lambda(\epsilon_n, \tau_n) + \lambda_1(\epsilon_n)$.

4.2.4 Under secrecy constraint $\frac{1}{n}I(M_1; Z^n) + \frac{1}{n}I(M_2; Z^n) \to 0$:

Combining (24) (that is obtained under secrecy constraint $\frac{1}{n}I(M_1; Z^n) \to 0$) and (26) (that is obtained under secrecy constraint $\frac{1}{n}I(M_2; Z^n) \to 0$), we have

$$\begin{aligned} n(R_1 + R_2) \leq & I(X_1^n; Y^n) - I(X_1^n; Z^n) + I(X_2^n; Y^n|X_1^n) \\ & - I(X_2^n; Z^n) + 2n\lambda(\epsilon_n, \tau_n) \\ =& I(X_1^n, X_2^n; Y^n) - I(X_1^n; Z^n) - I(X_2^n; Z^n) + 2n\lambda(\epsilon_n, \tau_n) \\ \overset{(r)}{\leq}& n\left[I(X_1, X_2; Y|Q) - I(X_1; Z|Q) - I(X_2; Z|Q)\right] + 2n\lambda(\tau_n, \epsilon_n). \end{aligned} \quad (30)$$

where (r) is by applying (10), (14) and (15) in Lemma 1.

Note that for $\overline{\mathcal{R}}_{\{1\},\{2\}}$, we have not only the bound (30), but also the bounds (19), (22), (23), (25) (those are valid under secrecy constraint $\frac{1}{n}I(M_1; Z^n) \to 0$), and the bounds (17), (27), (28), (29) (those are valid under secrecy constraint $\frac{1}{n}I(M_2; Z^n) \to 0$). We note that (17) and (19) are redundant due to (22) and (27), respectively; (25) and (29) are redundant due to (30). Thus taking the limit as $n \to \infty$ such that $\lambda(\epsilon_n, \tau_n) \to 0$ in (22), (23),(27), (28) and (30), we establish the outer bound $\overline{\mathcal{R}}_{\{1\},\{2\}}$ as given in Table 4.

4.2.5 Under secrecy constraint $\frac{1}{n}I(M_1, M_2; Z^n) \to 0$:

$$\begin{aligned} n(R_1 + R_2) =& H(M_1, M_2) \\ =& H(M_1, M_2|Y^n) + I(M_1, M_2; Y^n) \\ \overset{(s)}{\leq}& I(M_1, M_2; Y^n) - I(M_1, M_2; Z^n) + n\lambda(\epsilon_n, \tau_n) \\ \overset{(t)}{\leq}& n\left[I(X_1, X_2; Y|Q) - I(X_1, X_2; Z|Q)\right] + n\lambda(\tau_n, \epsilon_n), \end{aligned} \quad (31)$$

where (s) is due to reliability constraint (8), Fano's inequality, the secrecy constraint (9) (i.e., $\frac{1}{n}I(M_1, M_2; Z^n) \leq \tau_n$) and taking $\lambda(\tau_n, \epsilon_n) = \tau_n + 1/n + \epsilon_n(R_1 + R_2)$; and (t) follows the same arguments as for step (r).

For $\overline{\mathcal{R}}_{\{1,2\}}$, we have not only the bounds for individual rates in (22), (23), (27) and (28) (those are valid under secrecy constraint $\frac{1}{n}I(M_1; Z^n) + \frac{1}{n}I(M_2; Z^n) \to 0$), but also the bound on the sum-rate in (31). We note that (23) and (28) are redundant due to (31). Thus taking the limit as $n \to \infty$ such that $\lambda(\epsilon_n, \tau_n) \to 0$ in (22), (23) and (31), we establish the outer bound $\overline{\mathcal{R}}_{\{1,2\}}$ as given in Table 4.

4.3 Discussion on the tightness on the inner and outer bounds

Unfortunately, the bounds are not tight in general. For simplicity, we denote

$$\mathcal{P}_1 = \{(Q, X_1, X_2)|p(u, x_1, x_2) = p(q)p(x_1|q)p(x_2|q)\},$$

$$\mathcal{P}_2 = \{(Q, X_1, X_2)|p(u, x_1, x_2) = p(q)p(x_1, x_2|q)\}.$$

Consider the extreme case with $Z = \emptyset$ under the joint secrecy constraint. Then $\underline{\mathcal{R}}_{\{1,2\}}$ and $\overline{\mathcal{R}}_{\{1,2\}}$ reduce to $\bigcup_{\mathcal{P}_1} \mathcal{R}_{\{1,2\}}(Z = \emptyset)$ and $\bigcup_{\mathcal{P}_2} \mathcal{R}_{\{1,2\}}(Z = \emptyset)$, respectively, where

$$\mathcal{R}_{\{1,2\}}(Z = \emptyset) = \left\{ (R_1, R_2) \left| \begin{array}{r} R_1 \leq I(X_1; Y|X_2, Q) \\ R_2 \leq I(X_2; Y|X_1, Q) \\ R_1 + R_2 \leq I(X_1, X_2; Y|Q) \end{array} \right. \right\}. \tag{32}$$

Interestingly, we see that

- $\bigcup_{\mathcal{P}_1} \mathcal{R}_{\{1,2\}}(Z = \emptyset)$ is included by the Cover-Leung region for MAC-FB [Cover and Leung 1981].
- $\bigcup_{\mathcal{P}_2} \mathcal{R}_{\{1,2\}}(Z = \emptyset)$ is larger than the dependence balance based outer bound [Hekstra and Willems 1989] on the capacity region for MAC-FB.

Remarkably, the Cover-Leung region is not tight in general. An improvement was proposed by Bross and Lapidoth [Bross and Lapidoth 2005] with an example demonstrating the strict inclusion. Clearly, the same example also exhibits a distinct gap between $\bigcup_{\mathcal{P}_1} \mathcal{R}_{\{1,2\}}(Z = \emptyset)$ and $\bigcup_{\mathcal{P}_2} \mathcal{R}_{\{1,2\}}(Z = \emptyset)$, as a special instance of $\underline{\mathcal{R}}_{\{1,2\}}$ and $\overline{\mathcal{R}}_{\{1,2\}}$. As a conclusion, for the 2-transmitter DM-MAC with an external eavesdropper, the respective secrecy capacity regions still remain unknown, even for the degraded case.

5 Concluding remarks

In this paper, we review the secrecy results obtained for the 2-transmitter multiple access channel with an external eavesdropper. In particular, we discuss 5 secrecy strengths, from both end user's perspective and system designer's perspective. Both theoretical and numerical results are presented to show the impact of different secrecy requirements on the respective achievable rate regions (or in other words, the price paid for the required secrecy). Moreover, we look into the case where either competitive or cooperative transmission strategies can be employed at the transmitter who does not demand secrecy for its message. Unlike the reliable communication scenario where secrecy is not concerned, and it does not make any difference for the transmitters for being either cooperative or competitive, we show that in a secure communication over MAC, being cooperative can significantly enlarge the corresponding achievable secrecy region.

Besides, assuming that both transmitters are cooperative, we take a special look into the inner and outer bounds on the secrecy capacity regions over the

2-transmitter DM-MAC with a degraded eavesdropper. We notice that the inner and outer bounds differentiate themselves in the permissible sets of input distributions. Especially, we give an example to show that the bounds are not tight in general. To close the gap, we need to either improve the achievable regions or tighten the outer bounds. 2-transmitter multiple access channel is a rather simple model, which has been extensively investigated and which results provide insights into the open problems in multi-use communications. One can refer to [Chen et al. 2018] for extended results on the secrecy rate regions for a multiple access channel with arbitrarily many transmitters, where a class of collective secrecy was introduced and studied therein.

Acknowledgements

This work is supported in part by the German Research Foundation (DFG) KA 1154/37-1 and National Science Foundation (NSF) grants CCF-1748585 and CNS-1748692. The support of DFG and NSF is greatly appreciated.

References

[Ahlswede 1973] R. Ahlswede: Multi-way communication channels. *Akadémiai Kiadó*, (1973).

[Bross and Lapidoth 2005] S. I. Bross and A. Lapidoth: An improved achievable region for the discrete memoryless two-user multiple-access channel with noiseless feedback. *IEEE Trans. Inf. Theory*, **51**(3), 811–833 (2005).

[Carleial 1982] A. Carleial: Multiple-access channels with different generalized feedback signals. *IEEE Trans. Inf. Theory*, **28**(6), 841–850 (1982).

[Chen et al. 2016] Y. Chen, O. O. Koyluoglu and A. J. Han Vinck: On secure communication over the multiple access channel, In *Proc. 2016 IEEE International Symposium on Information Theory and Its Applications (ISITA)*, 355–359 (2016).

[Chen et al. 2018] Y. Chen, O. O. Koyluoglu and A. J. Han Vinck: Collective secrecy over the K-transmitter multiple access channel. *IEEE Transactions on Information Forensics and Security*, **13** (9), 2279–2293 (2018).

[Cover 1975] T. M. Cover: Some advances in broadcast channels. *Advances in Communication Systems*, **4**, 229 – 260 (1975).

[Cover and Leung 1981] T. Cover and C. Leung: An achievable rate region for the multiple-access channel with feedback. *IEEE Trans. Inf. Theory*, **27**(3), 292–298 (1981).

[Cover and Leung-Yan-Cheong 1976] T. M. Cover and S. K. Leung-Yan-Cheong: A scheme for enlarging the capacity region of multiple-access channels using feedback. Dept. of Stat., Stanford Univ., Stanford, CA, *Tech. Rep. 17*, (1976).

[Cover et al. 1980] T. Cover, A. Gamal, and M. Salehi: Multiple access channels with arbitrarily correlated sources. *IEEE Trans. Inf. Theory*, **26**(6), 648–657 (1980).

[Csiszár and Körner 1978] I. Csiszár and J. Körner: Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, **24**(3), 339–348 (1978).

[El Gamal and Kim 2012] A. El Gamal and Y.-H. Kim: *Network Information Theory.* New York, NY, USA: Cambridge University Press, (2012).

[Gaarder and Wolf 1975] N. Gaarder and J. Wolf: The capacity region of a multiple-access discrete memoryless channel can increase with feedback. *IEEE Trans. Inf. Theory*, **21**(1), 100–102 (1975).

[Han 1979] Te Sun Han: The capacity region of general multiple-access channel with certain correlated sources. *Information and Control*, **40**(1), 37-60 (1979).

[Hekstra and Willems 1989] A. P. Hekstra and F. M. J. Willems: Dependence balance bounds for single-output two-way channels. *IEEE Trans. Info. Theory*, **35**(1), 44–53 (1989).

[Khachatrian and Martirossian 1998] G. H. Khachatrian and S. S. Martirossian: Code construction for the T-user noiseless adder channel. *IEEE Trans. Inf. Theory*, **44** (5), 1953–1957 (1998).

[Kramer 1999] G. Kramer: Feedback strategies for a class of two-user multiple-access channels. *IEEE Trans. Inf. Theory*, **45** (6), 2054–2059 (1999).

[Liang and Poor 2008] Y. Liang and H. V. Poor: Multiple-access channels with confidential messages. *IEEE Trans. Inf. Theory*, vol. **54** (3), 976–1002 (2008).

[Liao 1972] H. H.-J. Liao: Multiple Access Channels. Honolulu: *Ph.D. Dissertation*, University of Hawaii, (1972).

[Slepian and Wolf 1973] D. Slepian and J. K. Wolf: A coding theorem for multiple access channels with correlated sources. *Bell Syst. Tech. J.*, **52**(7), 1037–1076 (1973).

[Tang et al. 2007] X. Tang, R. Liu, P. Spasojevic, and H. Poor: Multiple access channels with generalized feedback and confidential messages. In: *Proc. ITW 2007*, (2007).

[Tekin and Yener 2008a] E. Tekin and A. Yener: The Gaussian multiple access wire-tap channel. *IEEE Trans. Inf. Theory*, **54**(12), 5747–5755 (2008).

[Tekin and Yener 2008b] E. Tekin and A. Yener: The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory*, **54**(6), 2735–2751 (2008).

[Van der Meulen 1977] E. van der Meulen: A survey of multi-way channels in information theory: 1961-1976. *IEEE Trans. Inf. Theory*, **23**(1), 1–37 (1977).

[Venkataramanan and Pradhan 2011] R. Venkataramanan and S. S. Pradhan: A new achievable rate region for the multiple-access channel with noiseless feedback. *IEEE Trans. Inf. Theory*, **57** (12), 8038–8054 (2011).

[Vinck 1983] A. J. Vinck: Constructive superposition coding for the binary erasure multiple access channel. *Proc. 4th Symp. Information Theory in Benelux*, 179-188 (1983).

[Vinck 1985] A. J. Han Vinck: On the multiple access channel. *Proc. of the 2nd Joint Swedish-Soviet Int. Workshop on Info. Theory*, **54** (1), 24-29 (1985).

[Vinck 2007] A. J. Han Vinck: Coding techniques and the two-access channel. In *NATO Security through Science Series - D: Information and Communication Security, Vol. 10: Multiple Access Channels,* 273–286 (2007).

[Vinck et al. 1985] A.J. Vinck, W.L.M. Hoeks and K.A. Post: On the capacity of the two-user M-ary multiple-access channel with feedback. *IEEE Trans. Info. Theory*, **31** (4), 540-543 (1985).

[Wiese and Boche 2013] M. Wiese and H. Boche: Strong secrecy for multiple access channels. In *Information Theory, Combinatorics, and Search Theory*, LNCS. Springer Berlin Heidelberg, **7777**, 71–122 (2013).

[Willems 1982] F. Willems: The feedback capacity region of a class of discrete memoryless multiple access channels. *IEEE Trans. Inf. Theory*, **28** (1), 93–95 (1982).

[Wyner 1975] A. D. Wyner: The wire-tap channel. *Bell Syst. Tech. J.*, **54**(8), 1355–1387 (1975).

[Yassaee and Aref 2010] M. Yassaee and M. Aref: Multiple access wiretap channels with strong secrecy. In: *Proc. ITW 2010*, Dublin, (2010).

A Proof of Lemma 1

Proof. First we prove (10), i.e., $I(X_1^n, X_2^n; Y^n) \leq nI(X_1, X_2; Y|Q)$ as follows:

$$\begin{aligned}
I(X_1^n, X_2^n; Y^n) =& H(Y^n) - H(Y^n|X_1^n, X_2^n) \\
\stackrel{(a)}{=}& \sum_{i=1}^{n} \left[H(Y_i|Y^{i-1}) - H(Y_i|X_{1,i}, X_{2,i})\right] \\
\stackrel{(b)}{=}& \sum_{i=1}^{n} \left[H(Y_i|Y^{i-1}, Z^{i-1}) - H(Y_i|X_{1,i}, X_{2,i}, Z^{i-1})\right] \\
\stackrel{(c)}{\leq}& \sum_{i=1}^{n} \left[H(Y_i|Z^{i-1}) - H(Y_i|X_{1,i}, X_{2,i}, Z^{i-1})\right] \\
\stackrel{(d)}{=}& \sum_{i=1}^{n} I(X_{1,i}, X_{2,i}; Y_i|U_i) \\
\stackrel{(e)}{=}& nI(X_1, X_2; Y|U, T) \\
\stackrel{(f)}{=}& nI(X_1, X_2; Y|Q),
\end{aligned}$$

where (a) is by the chain rule of the entropy and the discrete memoryless of the channel; (b) is by the Markov chain $Z^{i-1} \rightarrow (X_{1,i}, X_{2,i}) \rightarrow Y_i$ and the degradedness of the channel; (c) is by the fact that conditioning does not increase entropy; and (d) is by the definition of $U_i = Z^{i-1}$; (e) follows by standard techniques of using a time sharing variable T, and redefining variables for single-letter expressions. More specifically, we define $U = Z^{T-1}$, $X_1 = X_{1,T}$, $X_2 = X_{2,T}$ and $Z = Z_T$, where T is a random variable that is uniformly distributed over $[1 : n]$; and (f) is by defining $Q = (U, T)$.

To prove (11), i.e., $I(X_1^n; Y^n|X_2^n) \leq nI(X_1; Y|X_2, Q)$ we have the following.

$$\begin{aligned}
I(X_1^n; Y^n|X_2^n) =& H(Y^n|X_2^n) - H(Y^n|X_1^n, X_2^n) \\
\stackrel{(a)}{=}& \sum_{i=1}^{n} \left[H(Y_i|Y^{i-1}, X_2^n) - H(Y_i|X_{1,i}, X_{2,i})\right] \\
\stackrel{(b)}{=}& \sum_{i=1}^{n} \left[H(Y_i|Y^{i-1}, Z^{i-1}, X_2^n) - H(Y_i|X_{1,i}, X_{2,i}, Z^{i-1})\right] \\
\stackrel{(c)}{\leq}& \sum_{i=1}^{n} \left[H(Y_i|X_{2,i}, Z^{i-1}) - H(Y_i|X_{1,i}, X_{2,i}, Z^{i-1})\right] \\
\stackrel{(d)}{=}& \sum_{i=1}^{n} I(X_{1,i}; Y_i|X_{2,i}, U_i) \\
\stackrel{(g)}{=}& nI(X_1; Y|X_2, Q),
\end{aligned}$$

where (g) is by definitions of X_1, X_2, Y and Q in steps (e) and (f), respectively.

Note that similar steps can be applied to prove (12), i.e., $I(X_2^n; Y^n|X_1^n) \leq nI(X_2; Y|X_1, Q)$.

Now we proceed to prove (13), i.e., $I(X_1^n, X_2^n; Z^n) = nI(X_1, X_2; Y|Q)$.

$$\begin{aligned}
I(X_1^n, X_2^n; Z^n) =& H(Z^n) - H(Z^n|X_1^n, X_2^n) \\
\overset{(a)}{=}& \sum_{i=1}^{n} \left[H(Z_i|Z^{i-1}) - H(Z_i|X_{1,i}, X_{2,i})\right] \\
\overset{(h)}{=}& \sum_{i=1}^{n} \left[H(Z_i|Z^{i-1}) - H(Z_i|X_{1,i}, X_{2,i}, Z^{i-1})\right] \\
\overset{(d)}{=}& \sum_{i=1}^{n} I(X_{1,i}, X_{2,i}; Z_i|U_i) \\
\overset{(i)}{=}& nI(X_1, X_2; Y|Q),
\end{aligned}$$

where (h) is by the Markov chain $Z^{i-1} \to (X_{1,i}, X_{2,i}) \to Z_i$, and (i) follows by definitions of X_1, X_2, Y and Q in steps (e) and (f), respectively.

To prove (14), i.e., $I(X_1^n; Z^n) \geq nI(X_1; Z|Q)$, we have the following.

$$\begin{aligned}
I(X_1^n; Z^n) =& H(Z^n) - H(Z^n|X_1^n) \\
\overset{(a)}{=}& \sum_{i=1}^{n} \left[H(Z_i|Z^{i-1}) - H(Z_i|Z^{i-1}, X_1^n)\right] \\
\overset{(c)}{\geq}& \sum_{i=1}^{n} \left[H(Z_i|Z^{i-1}) - H(Z_i|Z^{i-1}, X_{1,i})\right] \\
\overset{(d)}{=}& \sum_{i=1}^{n} I(X_{1,i}; Z_i|U_i) \\
\overset{(j)}{=}& nI(X_1; Z|Q),
\end{aligned}$$

where (j) follows by definitions of X_1, Z and Q in steps (e) and (f), respectively.

Similar steps can be applied to prove (15), i.e., $I(X_2^n; Z^n) \geq nI(X_2; Z|Q)$.