On Secure Communication over the Multiple Access Channel

Yanling Chen*, O. Ozan Koyluoglu† and A. J. Han Vinck*
* Institute of Digital Signal Processing, University of Duisburg-Essen, Germany.
† Department of Electrical and Computer Engineering, The University of Arizona, USA.
Email: {yanling.chen, han.vinck}@uni-due.de, ozan@email.arizona.edu.

***Abstract*—This paper studies the problem of secure communication over a 2-transmitter multiple access channel (MAC) in the presence of an external eavesdropper. Two different secrecy constraints are considered: 1) individual secrecy (i.e., information leakage rate from each message to the eavesdropper is made vanishing) and 2) joint secrecy (i.e., information leakage rate from both messages to the eavesdropper is made vanishing). As a general result, the respective achievable secrecy rate regions are established. The single-letter characterizations of both regions involve three auxiliary random variables, one for time sharing and two for channel prefixing. Numerical results are presented to demonstrate the impact of different secrecy constraints and the advantage of channel prefixing in enlarging the achievable (individual/joint) secrecy rate regions.**

I. Introduction

Multiple access channel (MAC) is an important branch in the extensive field of the multiple-user communication. For MAC with independent sources, Ahlswede [1] first studied the 2-transmitter and 3-transmitter cases and determined the respective capacity regions; whilst Liao [2] considered the general K-transmitter MAC and fully characterized its capacity region.

Inspired by the pioneering works of Wyner [3] and Csiszár and Körner [4] 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 [5]. In particular, [5] focused on a degraded Gaussian MAC with K-transmitters and established several achievable rate regions subject to pre-specified secrecy levels; while a discrete memoryless 2-transmitter MAC with an external eavesdropper was considered in [6]. Note that the model in [6] takes into accounts 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) is imposed at the eavesdropper. Further works include [7], [8] that focus on the Gaussian scenario, and [9], [10] that investigate 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 case (e.g., with an eavesdropper not necessarily degraded), the *joint* secrecy capacity region still remains

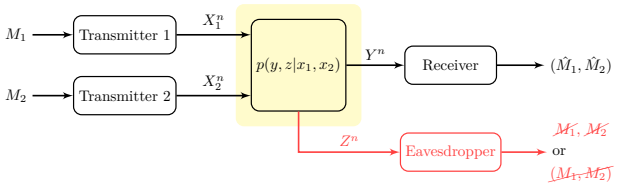


Fig. 1: DM-MAC with an external eavesdropper.

open in spite of all these efforts. And, a treatment subject to other secrecy criteria such as *individual* secrecy constraint (i.e., information leakage rate from *each* message to the eavesdropper is made vanishing), is missing. Note that individual secrecy has been well studied for the secure broadcasting problem [11]–[13].

In this paper, we focus on the problem of secure communication over a 2-transmitter MAC subject to two different secrecy constraints: 1) *individual* secrecy and 2) *joint* secrecy. The channel model is shown in Fig. 1. Note that the joint secrecy constraint offers a higher secrecy level from the system design perspective, while the individual secrecy constraint could provide an acceptable security strength from the end user's point of view with potential gains in increasing transmission rates. Therefore, our study provides insights for trading-off of the throughput and secrecy level. As a main result of the paper, we provide the respective achievable secrecy rate regions of the 2-transmitter MAC with an external eavesdropper subject to these two different secrecy constraints.

The rest of the paper is organized as follows. Section II introduces the system model; Section III gives the main result, i.e., the achievable individual/joint secrecy rate regions, which proofs are provided in Section IV. Section V provides some numerical results. Finally, Section VI concludes the paper. To enhance the flow, some details are relegated to the appendix.

II. System model

Consider a discrete memoryless MAC (DM-MAC) with two transmitters, one legitimate receiver, and one passive eavesdropper, as shown in Fig. 1. The transmitter i, aims to send message m_i to the legitimate receiver, where $i = 1, 2$. 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, we have

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

A $(2^{nR_1}, 2^{nR_2}, n)$ secrecy code for the DM-MAC consists of

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

Assume that the messages are uniformly distributed over their corresponding message sets. We have

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

Denote the *average probability of decoding error* at the legitimate receiver as $P_e^n = \Pr\{\{M_1 \neq \hat{M}_1\} \cup \{M_2 \neq \hat{M}_2\}\}$. At the eavesdropper, denote $R_{L,i} = I(M_i; Z^n)/n$ to be the (individual) leakage rate of M_i for $i = 1, 2$, and $R_L = I(M_1, M_2; Z^n)/n$ to be the (joint) leakage rate of (M_1, M_2), respectively. The rate pair (R_1, R_2) is said to be *achievable under individual secrecy constraint*, if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes such that

$$P_e^n \leq \epsilon_n, \tag{2}$$

$$R_{L,i} \leq \tau_n, \quad \text{for } i = 1, 2 \tag{3}$$

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

Note that, (3) corresponds to the *individual* secrecy constraints. If the coding scheme fulfills (2), (4) and

$$R_L \leq \tau_n, \tag{5}$$

then the rate pair (R_1, R_2) is said to be *achievable under joint secrecy constraint*. Clearly, the joint secrecy (5) implies the individual secrecy (3) as $I(M_1, M_2; Z^n)/n = R_L \geq R_{L,1} + R_{L,2} = I(M_1; Z^n)/n + I(M_2; Z^n)/n$. Therefore, the jointly secret achievable rate pairs are by definition achievable as individually secret.

III. Main result

In this section, we present the main results of the paper.

Theorem 1. *An achievable individual secrecy rate region of the 2-transmitter DM-MAC with an external eavesdropper is given by the union of non-negative rate pairs (R_1, R_2) satisfying*

$$\begin{aligned} R_1 &\leq I(V_1; Y|V_2, Q) - I(V_1; Z|Q), \\ R_2 &\leq I(V_2; Y|V_1, Q) - I(V_2; Z|Q), \\ \max\{R_1, R_2\} &\leq I(V_1, V_2; Y|Q) - I(V_1, V_2; Z|Q), \\ R_1 + R_2 &\leq I(V_1, V_2; Y|Q) - I(V_1; Z|Q) - I(V_2; Z|Q), \end{aligned}$$

where the union is over all input probability distributions of the form $p(q)p(v_1|q)p(v_2|q)p(x_1|v_1)p(x_2|v_2)$.

Proof: See the achivability proof in Section IV-A. ■

Theorem 2. *An achievable joint secrecy rate region of the 2-transmitter DM-MAC with an external eavesdropper is given by the union of non-negative rate pairs (R_1, R_2) satisfying*

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

where the union is over all input probability distributions of the form $p(q)p(v_1|q)p(v_2|q)p(x_1|v_1)p(x_2|v_2)$.

Proof: See the achivability proof in Section IV-B. ■

Remark: Taking $V_1 = X_1, V_2 = X_2$, Theorem 2 recovers the achievable joint secrecy rate region given in [6, (8)], which does not involve the channel prefixing parameters (V_1, V_2); While, Theorem 2 (with channel prefixing) indeed improves [6, (8)] (without channel prefixing), as we demonstrate by the numerical results in Section V.

IV. Achievability proof

A. Achievability proof of Theorem 1

Fix $p(q), p(v_1|q), p(v_2|q), p(x_1|v_1), p(x_2|v_2)$. Generate a random sequence q^n, where $p(q^n) = \prod_{t=1}^{n} p(q(t))$ with each entry chosen as i.i.d. $p(q)$. The sequence q^n is given to every node in the system.

Codebook generation: To construct codebook i for $i = 1, 2$, randomly generate $2^{n(R_i + R_{i,r})}$ sequences $v_i^n(m_i, m_{i,r})$, with $(m_i, m_{i,r}) \in [1 : 2^{nR_i}] \times [1 : 2^{nR_{i,r}}]$, each with probability $p(v_i^n|q^n) = \prod_{t=1}^{n} p(v_i(t)|q(t))$, where $p(v_i(t)|q(t)) = p(v_1|q)$ for each t. Every node in the network knows these codebooks.

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

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

Analysis of the error probability of decoding: From the decoding analysis for the multiple access channel, see, e.g., [14], P_e can be made approximately zero as $n \to \infty$ if

$$\begin{aligned} R_1 + R_{1,r} &\leq I(V_1; Y|V_2, Q), \\ R_2 + R_{2,r} &\leq I(V_2; Y|V_1, Q), \\ R_1 + R_{1,r} + R_2 + R_{2,r} &\leq I(V_1, V_2; Y|Q). \end{aligned} \tag{6}$$

Analysis of individual secrecy: For the individual secrecy (3), i.e., $R_{L,i} \leq \tau_n$, for $i = 1, 2$, we show in the following its equivalent form that $H(M_i|Z^n, Q^n) \geq nR_i - n\tau_n$, as this implies $nR_{L,i} = I(M_i; Z^n) \leq I(M_i; Z^n, Q^n) \leq n\tau_n$.

The following lemma is used for the secrecy analysis.

Lemma 3. *$H(V_1^n, V_2^n|M_1, Z^n, Q^n) \le n[R_{1,r}+R_2+R_{2,r}-I(V_1,V_2;Z|Q)]+n\varepsilon_n$ if*

$$R_{1,r} \ge I(V_1;Z|Q), \tag{7}$$
$$R_2 + R_{2,r} \ge I(V_2;Z|Q), \tag{8}$$
$$R_{1,r} + R_2 + R_{2,r} \ge I(V_1,V_2;Z|Q). \tag{9}$$

Proof: See a detailed proof in Appendix A. ∎

First, we consider $H(M_1|Z^n,Q^n)$.

$$\begin{aligned}
&H(M_1|Z^n,Q^n) = H(M_1,Z^n|Q^n) - H(Z^n|Q^n)\\
=&H(M_1,M_{1,r},M_2,M_{2,r},Z^n|Q^n)\\
&- H(M_{1,r},M_2,M_{2,r}|M_1,Z^n,Q^n) - H(Z^n|Q^n)\\
\overset{(a)}{=}&H(M_1,M_{1,r},M_2,M_{2,r}|Q^n) + H(Z^n|V_1^n,V_2^n,Q^n)\\
&- H(M_{1,r},M_2,M_{2,r},V_1^n,V_2^n|M_1,Z^n,Q^n) - H(Z^n|Q^n)\\
\overset{(b)}{\ge}&n[R_1+R_{1,r}+R_2+R_{2,r}] - I(V_1^n,V_2^n;Z^n|Q^n)\\
&- H(V_1^n,V_2^n|M_1,Z^n,Q^n) - n\varepsilon_n\\
\overset{(c)}{\ge}&n[R_1+R_{1,r}+R_2+R_{2,r}] - nI(V_1,V_2;Z|Q\\
&- H(V_1^n,V_2^n|M_1,Z^n,Q^n) - 2n\varepsilon_n\\
\overset{(d)}{\ge}&nR_1 - n\tau_n,
\end{aligned}$$

where (a) follows from the fact that V_1^n and V_2^n are functions of $(M_1,M_{1,r})$ and $(M_2,M_{2,r})$, respectively, and the Markov chain $(M_1,M_{1,r},M_2,M_{2,r}) \to (V_1^n,V_2^n,Q^n) \to Z^n$; (b) follows from the fact that $H(M_1,M_{1,r},M_2,M_{2,r}|Q^n) = n[R_1+R_{1,r}+R_2+R_{2,r}]$; and $H(M_{1,r},M_2,M_{2,r}|M_1,V_1^n,V_2^n,Z^n,Q^n) \le n\varepsilon_n$ by date processing inequality and Fano's inequality (if (6) is fulfilled):

$$\begin{aligned}
&H(M_{1,r},M_2,M_{2,r}|M_1,V_1^n,V_2^n,Z^n,Q^n)\\
\le&H(M_1,M_{1,r},M_2,M_{2,r}|V_1^n,V_2^n,Q^n)\\
\le&H(M_1,M_{1,r},M_2,M_{2,r}|Y^n,Q^n) \le n\varepsilon_n;
\end{aligned}$$

(c) follows from the fact that $I(V_1^n,V_2^n;Z^n|Q^n) \le nI(V_1,V_2;Z|Q)+n\varepsilon_n$ (the proof of which follows similarly to the proof of [15, Lemma 3]); and (d) is due to Lemma 3 by requiring (7), (8) and (9) and by taking $\tau_n = 3\varepsilon_n$.

A similar proof applies to $H(M_2|Z^n,Q^n)$. That is, for the secrecy of M_2 at the eavesdropper, the following additional conditions have to be fulfilled (as required in step (d) for the secrecy of M_1 at the eavesdropper):

$$R_{2,r} \ge I(V_2;Z|Q), \tag{10}$$
$$R_1 + R_{1,r} \ge I(V_1;Z|Q), \tag{11}$$
$$R_{2,r} + R_1 + R_{1,r} \ge I(V_1,V_2;Z|Q). \tag{12}$$

Note that (8), (11) are fulfilled if (7), (10) are satisfied (due to the non-negativity of the rates).

Individual secrecy achievable rate region: We summarize the requirements in order to guarantee a reliable communication under the individual secrecy constraint as follows:

- the non-negativity for rates;
- the conditions for a reliable communication to the legitimate receiver, i.e., (6); and
- the conditions for individual secrecy of the messages at the eavesdropper, i.e., (7), (9), (10) and (12).

Eliminating $R_{1,r}, R_{2,r}$ by applying Fourier-Motzkin procedure [14], we get the desired rate region in Theorem 1.

B. Achievability proof of Theorem 2

For the achievability of the joint secrecy rate region in Theorem 2, we utilize the same encoding and decoding scheme (at the transmitters and legitimate receiver) as described in Section IV-A. As a direct consequence, the reliability proof (i.e., analysis of the error probability of decoding) remains the same. Therefore, we only need to revise the secrecy analysis under the joint secrecy constraint. Following a similar proof for Lemma 3, we have the following lemma for the joint secrecy analysis.

Lemma 4. *$H(V_1^n, V_2^n|M_1, M_2, Z^n, Q^n) \le n[R_{1,r}+R_{2,r}-I(V_1,V_2;Z|Q)]+n\varepsilon_n$ if*

$$R_{1,r} \ge I(V_1;Z|Q), \tag{13}$$
$$R_{2,r} \ge I(V_2;Z|Q), \tag{14}$$
$$R_{1,r} + R_{2,r} \ge I(V_1,V_2;Z|Q). \tag{15}$$

Analysis of joint secrecy: For the joint secrecy (5), i.e., $R_L \le \tau_n$, we show in the following its equivalent form that $H(M_1,M_2|Z^n,Q^n) \ge n[R_1+R_2]-n\tau_n$, as this implies $nR_L = I(M_1,M_2;Z^n) \le I(M_1,M_2;Z^n,Q^n) \le n\tau_n$.

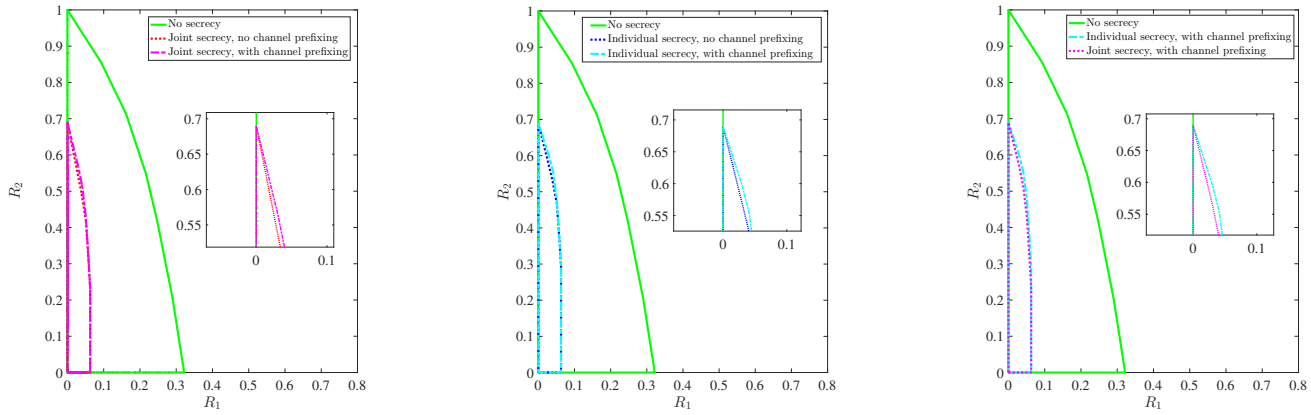
$$\begin{aligned}
&H(M_1,M_2|Z^n,Q^n) = H(M_1,M_2,Z^n|Q^n) - H(Z^n|Q^n)\\
=&H(M_1,M_{1,r},M_2,M_{2,r},Z^n|Q^n)\\
&- H(M_{1,r},M_{2,r}|M_1,M_2,Z^n,Q^n) - H(Z^n|Q^n)\\
\overset{(e)}{=}&H(M_1,M_{1,r},M_2,M_{2,r}|Q^n) + H(Z^n|V_1^n,V_2^n,Q^n)\\
&- H(M_{1,r},M_{2,r},V_1^n,V_2^n|M_1,M_2,Z^n,Q^n) - H(Z^n|Q^n)\\
\overset{(f)}{\ge}&n[R_1+R_{1,r}+R_2+R_{2,r}] - I(V_1^n,V_2^n;Z^n|Q^n)\\
&- H(V_1^n,V_2^n|M_1,M_2,Z^n,Q^n) - n\varepsilon_n\\
\overset{(g)}{\ge}&n[R_1+R_{1,r}+R_2+R_{2,r}] - nI(V_1,V_2;Z|Q)\\
&- H(V_1^n,V_2^n|M_1,M_2,Z^n,Q^n) - 2n\varepsilon_n\\
\overset{(h)}{\ge}&n[R_1+R_2] - n\tau_n,
\end{aligned}$$

where (e), (f), (g) follows the similar argument as for the steps (a), (b), (c) in Section IV-A, respectively; and (h) follows from Lemma 4 by requiring (13), (14) and (15).

Joint secrecy achievable rate region: We summarize the requirements in order to guarantee a reliable communication under the joint secrecy constraint as follows:

- the non-negativity for rates;
- the conditions for a reliable communication to the legitimate receiver, i.e., (6); and
- the conditions for the joint secrecy of the messages at the eavesdropper, i.e., (13), (14) and (15).

Eliminating $R_{1,r}, R_{2,r}$ by applying Fourier-Motzkin procedure [14], we get the desired rate region in Theorem 2.



(a) Joint/No secrecy (b) Individual/No secrecy (c) Joint/Individual/No secrecy

Fig. 2: Impacts of channel prefixing on achievable rate regions under different secrecy constraints.

V. Numerical results

In this section, we provide numerical results to illustrate the impact of channel prefixing and different secrecy constraints on the respective achievable rate regions.

Consider a binary-input binary-output MAC with an external eavesdropper. The channel to the legitimate receiver $(X_1, X_2) \to Y$ is defined by the transition matrix

$$p(y|x_1,x_2): \quad \begin{matrix} \\ (x_1,x_2)=00 \\ (x_1,x_2)=01 \\ (x_1,x_2)=10 \\ (x_1,x_2)=11 \end{matrix} \quad \begin{matrix} y=0 & y=1 \\ \end{matrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1/2 & 1/2 \\ 0 & 1 \end{bmatrix}; \tag{16}$$

while the channel to the eavesdropper $(X_1, X_2) \to Z$ is defined by the transition matrix

$$p(z|x_1,x_2): \quad \begin{matrix} \\ (x_1,x_2)=00 \\ (x_1,x_2)=01 \\ (x_1,x_2)=10 \\ (x_1,x_2)=11 \end{matrix} \quad \begin{matrix} z=0 & z=1 \\ \end{matrix} \quad \begin{bmatrix} 1 & 0 \\ 1/2 & 1/2 \\ 1/2 & 1/2 \\ 0 & 1 \end{bmatrix}. \tag{17}$$

For this specific MAC with an external eavesdropper, its achievable rate regions under different secrecy constraints are depicted in Fig. 2. The capacity region (without any secrecy constraint) is enclosed by (green) solid lines. It is known that channel prefixing is not necessary in this case [14]. However, for the secrecy rate regions, channel prefixing demonstrates its advantage as can be seen in Fig. 2a (under joint secrecy) and Fig. 2b (under individual secrecy). The achievable individual and joint secrecy regions (according to Theorem 1 and Theorem 2, respectively) are shown in Fig. 2c (with binary V_1, V_2). Not surprisingly, there is a price for the secrecy. As one can see, the joint secrecy rate region is smaller than the individual one; and both secrecy rate regions are smaller than the capacity region with no secrecy constraint. Interestingly, in both secrecy scenarios, the maximum marginal transmission rates (i.e., only one active transmitter), remain the same.

VI. Conclusion

In this paper, we studied the problem of secure communication over a 2-transmitter MAC subject to the individual/joint secrecy constraint. As a result, we provided the respective achievable secrecy rate regions. Moreover, we showed that channel prefixing is advantageous in enlarging the achievable rate region under both secrecy constraints.

Appendix A
Proof of Lemma 3

To prove Lemma 3, we need to show that the inequality $H(V_1^n, V_2^n|M_1, Z^n, Q^n) \le n[R_{1,r} + R_2 + R_{2,r} - I(V_1, V_2; Z|Q)] + n\varepsilon_n$ holds if the rates fulfill (7), (8) and (9). This can be done by showing that if taking (7), (8) and (9), $H(V_1^n, V_2^n|m_1^*, Z^n, Q^n) \le n[R_{1,r} + R_2 + R_{2,r} - I(V_1, V_2; Z|Q)] + n\varepsilon_n$ holds for each fixed $M_1 = m_1^*$, and then averaging over M_1. The proof is given as follows.

For a given $M_1 = m_1^*$, consider the corresponding subcodebook of codebook 1 (which construction is described in Section IV-A), i.e., the set of codewords $v_1^n(m_1^*, m_{1,r})$ with $m_{1,r} \in [1 : 2^{nR_{1,r}}]$. Randomly and equally partition the $2^{nR_{1,r}}$ codewords into 2^{nI_1} sets such that each set consists of $2^{n\min\{R_{1,r}, I(V_1;Z|V_2,Q)-\varepsilon_n/2\}}$ codewords, where

$$I_1 = \max\{0, R_{1,r} - I(V_1; Z|V_2, Q) + \varepsilon_n/2\}. \tag{18}$$

We use W_1 to denote the index of the sets that takes value from $[1 : 2^{nI_1}]$, and $C_1(W_1)$ for the corresponding set.

Secondly consider the codebook 2 (as described in Section IV-A), i.e., the set of codewords $v_2^n(m_2, m_{2,r})$ with $(m_2, m_{2,r}) \in [1 : 2^{nR_2}] \times [1 : 2^{nR_{2,r}}]$. Randomly and equally partition the $2^{n[R_2+R_{2,r}]}$ codewords into 2^{nI_2} sets such that each set consists of $2^{n\min\{R_2+R_{2,r}, I(V_2;Z|V_1,Q)-\varepsilon_n/2\}}$ codewords, where

$$I_2 = \max\{0, R_2 + R_{2,r} - I(V_2; Z|V_1, Q) + \varepsilon_n/2\}. \tag{19}$$

We use W_2 to denote the index of the sets that takes value from $[1 : 2^{nI_2}]$, and $C_2(W_2)$ for the corresponding set.

Now, consider the product codebook for each fixed (W_1, W_2), i.e., $C_1(W_1) \times C_2(W_2)$, which consists of 2^{nJ} codewords with

$$\begin{aligned} J =& \min\{R_{1,r}, I(V_1; Z|V_2, Q) - \varepsilon_n/2\} \\ &+ \min\{R_2 + R_{2,r}, I(V_2; Z|V_1, Q) - \varepsilon_n/2\}. \end{aligned} \tag{20}$$

Randomly and equally partition them into 2^{nI_0} sets such that each set consists of $2^{n \min\{J, I(V_1,V_2;Z|Q) - \varepsilon_n/2\}}$ codewords, where

$$I_0 = \max\{0, J - I(V_1, V_2; Z|Q) + \varepsilon_n/2\}. \tag{21}$$

We use W_0 to denote the index of the sets that takes value from $[1 : 2^{nI_0}]$, and $C(W_0, W_1, W_2)$ for the corresponding set.

Let $W = (W_0, W_1, W_2)$ that takes value from $[1 : 2^{n(I_0+I_1+I_2)}]$. Note that if the eavesdropper is given the index information W, then the corresponding set $C(W_0, W_1, W_2)$ will be taken as a codebook to decode. With the observation Z^n, the eavesdropper could decode (V_1^n, V_2^n) correctly with an arbitrary small decoding error probability by using simultaneous jointly typical decoding. This follows from the standard decoding analysis for MAC and the construction of $C(W_0, W_1, W_2)$. That is, we have

$$H(V_1^n, V_2^n | m_1^*, W, Z^n, Q^n) \le n\varepsilon_n/2. \tag{22}$$

Note that

$$\begin{aligned} &H(V_1^n, V_2^n | m_1^*, Z^n, Q^n) = H(V_1^n, V_2^n, W | m_1^*, Z^n, Q^n) \\ =&H(W | m_1^*, Z^n, Q^n) + H(V_1^n, V_2^n | m_1^*, W, Z^n, Q^n) \\ \overset{(a)}{\le}& H(W) + n\varepsilon_n/2 \overset{(b)}{\le} n[I_0 + I_1 + I_2] + n\varepsilon_n/2 \\ \overset{(c)}{\le}& n[R_{1,r} + R_2 + R_{2,r} - I(V_1, V_2; Z|Q)] + n\varepsilon_n \end{aligned}$$

where (a) is due to (22); (b) is by the fact that $H(W) \le n[I_0 + I_1 + I_2]$; and (c) is by the fact that

$$I_0 + I_1 + I_2 \le R_{1,r} + R_2 + R_{2,r} - I(V_1, V_2; Z|Q) + \varepsilon_n/2, \tag{23}$$

if (7), (8) and (9) are fulfilled, i.e.,

$$\begin{aligned} R_{1,r} &\ge I(V_1; Z|Q), \\ R_2 + R_{2,r} &\ge I(V_2; Z|Q), \\ R_{1,r} + R_2 + R_{2,r} &\ge I(V_1, V_2; Z|Q). \end{aligned} \tag{24}$$

To prove (23), we consider the following 4 cases of (24):

- In addition to (24), in case of $R_{1,r} \le I(V_1; Z|V_2, Q) - \varepsilon_n/2$ and $R_2 + R_{2,r} \le I(V_2; Z|V_1, Q) - \varepsilon_n/2$, we have

$$\begin{aligned} J =& R_{1,r} + R_2 + R_{2,r}; \quad I_1 = I_2 = 0; \\ I_0 =& R_{1,r} + R_2 + R_{2,r} - I(V_1, V_2; Z|Q) + \varepsilon_n/2. \end{aligned}$$

- In addition to (24), in case of $R_{1,r} \ge I(V_1; Z|V_2, Q) - \varepsilon_n/2$ and $R_2 + R_{2,r} \le I(V_2; Z|V_1, Q) - \varepsilon_n/2$, we have

$$\begin{aligned} J =& R_2 + R_{2,r} + I(V_1; Z|V_2, Q) - \varepsilon_n/2; \\ I_0 =& R_2 + R_{2,r} - I(V_2; Z|Q); \quad \text{(by (21) and (8))} \\ I_1 =& R_{1,r} - I(V_1; Z|V_2, Q) + \varepsilon_n/2; \quad I_2 = 0. \end{aligned}$$

- In addition to (24), in case of $R_{1,r} \le I(V_1; Z|V_2, Q) - \varepsilon_n/2$ and $R_2 + R_{2,r} \ge I(V_2; Z|V_1, Q) - \varepsilon_n/2$, we have

$$\begin{aligned} J =& R_{1,r} + I(V_2; Z|V_1, Q) - \varepsilon_n/2; \quad I_1 = 0; \\ I_0 =& R_{1,r} - I(V_1; Z|Q); \quad \text{(by (21) and (7))} \\ I_2 =& R_2 + R_{2,r} - I(V_2; Z|V_1, Q) + \varepsilon_n/2. \end{aligned}$$

- In addition to (24), in case of $R_{1,r} \ge I(V_1; Z|V_2, Q) - \varepsilon_n/2$ and $R_2 + R_{2,r} \ge I(V_2; Z|V_1, Q) - \varepsilon_n/2$, we have

$$\begin{aligned} J =& I(V_1; Z|V_2, Q) + I(V_2; Z|V_1, Q) - \varepsilon_n; \\ I_0 =& I(V_1; Z|V_2, Q) + I(V_2; Z|V_1, Q) \\ &- I(V_1, V_2; Z|Q) - \varepsilon_n/2; \\ I_1 =& R_{1,r} - I(V_1; Z|V_2, Q) + \varepsilon_n/2; \\ I_2 =& R_2 + R_{2,r} - I(V_2; Z|V_1, Q) + \varepsilon_n/2. \end{aligned}$$

It is easy to verify that (23) holds in all cases, i.e., if (24) (i.e., (7), (8) and (9)) is fulfilled. This concludes the proof.

References

[1] R. Ahlswede, *Multi-way communication channels.* Akadémiai Kiadó, 1973.

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

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

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

[5] 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.

[6] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "Multiple access channels with generalized feedback and confidential messages," in *Proc. 2007 IEEE Information Theory Workshop (ITW 2007)*, Sept 2007, pp. 608–613.

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

[8] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *2008 46th Annual Allerton Conference on Communication, Control, and Computing*, Sept 2008, pp. 1014–1021.

[9] M. Yassaee and M. Aref, "Multiple access wiretap channels with strong secrecy," in *2010 IEEE Information Theory Workshop (ITW 2010)*, Aug 2010, pp. 1–5.

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

[11] Y. Chen, O. O. Koyluoglu, and A. Sezgin, "Individual secrecy for broadcast channels with receiver side information," *CoRR*, vol. abs/1501.07547, Jan. 2015. [Online]. Available: http://arxiv.org/abs/1501.07547

[12] A. S. Mansour, R. F. Schaefer, and H. Boche, "Capacity regions for broadcast channels with degraded message sets and message cognition under different secrecy constraints," *CoRR*, vol. abs/1501.04490, Jan. 2015. [Online]. Available: http://arxiv.org/abs/1501.04490

[13] Y. Chen, O. O. Koyluoglu, and A. Sezgin, "Individual secrecy for the broadcast channel," *CoRR*, vol. abs/1511.09070, Nov. 2015. [Online]. Available: http://arxiv.org/abs/1511.09070

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

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