Entropy **2014**, *16*, 4693-4712; doi:10.3390/e16084693

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Article

Some New Results on the Multiple-Access Wiretap Channel

Bin Dai * and Zheng Ma

School of Information Science and Technology, Southwest JiaoTong University, Northbound Section Second Ring Road 111, Chengdu 610031, China; E-Mail: zma@home.swjtu.edu.cn

* Author to whom correspondence should be addressed; E-Mail: daibinsjtu@gmail.com; Tel.:+86-028-87634758.

Received: 4 May 2014; in revised form: 18 July 2014 / Accepted: 15 August 2014 / Published: 21 August 2014

Abstract: In this paper, some new results on the multiple-access wiretap channel (MAC-WT) are provided. Specifically, first, we investigate the degraded MAC-WT, where two users transmit their corresponding confidential messages (no common message) to a legitimate receiver via a multiple-access channel (MAC), while a wiretapper wishes to obtain the messages via a physically degraded wiretap channel. The secrecy capacity region of this model is determined for both the discrete memoryless and Gaussian cases. For the Gaussian case, we find that this secrecy capacity region is exactly the same as the achievable secrecy rate region provided by Tekin and Yener, *i.e.*, Tekin–Yener's achievable region is exactly the secrecy capacity region of the degraded Gaussian MAC-WT. Second, we study a special Gaussian MAC-WT, and find the power control for two kinds of optimal points (max-min point and single user point) on the secrecy rate region of this special Gaussian model.

Keywords: multiple-access wiretap channel (MAC-WT); Gaussian multiple-access wiretap channel (GMAC-WT); secrecy capacity region; power control

1. Introduction

Transmission of confidential messages has been studied in the literature of several classes of channels. Wyner, in his well-known paper on the wiretap channel [1], studied the problem of how to transmit the confidential messages to a legitimate receiver via a degraded broadcast channel, while keeping the eavesdropper as ignorant of the messages as possible. Measuring the uncertainty of the eavesdropper by equivocation, the capacity-equivocation region was established. Furthermore, the secrecy capacity was also established, which provided the maximum transmission rate with perfect secrecy. After the publication of Wyner's work, Csiszár and Körner [2] investigated a more general situation: broadcast channels with confidential messages (BCC). In this model, a common message and a confidential message were sent through a general broadcast channel. The common message was assumed to be decoded correctly by the legitimate receiver and the eavesdropper, while the confidential message was only allowed to be obtained by the legitimate receiver. This model is also a generalization of the model in [3], where no confidentiality condition is imposed. The capacity-equivocation region and the secrecy capacity region of BCC [2] were totally determined, and the results were also a generalization of those in [1]. Based on Wyner's work, Leung- Yan-Cheong and Hellman studied the Gaussian wiretap channel (GWC) [4] and showed that its secrecy capacity was the difference between the main channel capacity and the overall wiretap channel capacity. Some other related works on the wiretap channel (including feedback, side information and secret key) can be found in [5–12].

Recently, by using the approach of [1,2], the information-theoretical security for other multi-user communication systems has been widely studied.

For the relay channel, Lai-Gamal [13] and Xu *et al.* [14] studied the relay-eavesdropper channel, where a source wishes to send messages to a destination while leveraging the help of a relay node to hide those messages from the eavesdropper. Inner and outer bounds on the capacity-equivocation region were provided in these papers. In addition, Oohama [15] studied the relay channel with confidential messages, where a relay helps the transmission of messages from one sender to one receiver. The relay is considered not only as a sender that helps the message transmission, but also as a wiretapper who can obtain some knowledge about the transmitted messages. Measuring the uncertainty of the relay by equivocation, the inner and outer bounds on the capacity-equivocation region were provided in [15].

For the interference channel, Liu *et al.* [16] studied the interference channel with two confidential messages and provided inner and outer bounds on the secrecy capacity region. In addition, Liang *et al.* [17] studied the cognitive interference channel with one common message and one confidential message, and the capacity-equivocation region was totally determined for this model.

For the multiple-access channel (MAC), the security problems are split into two directions.

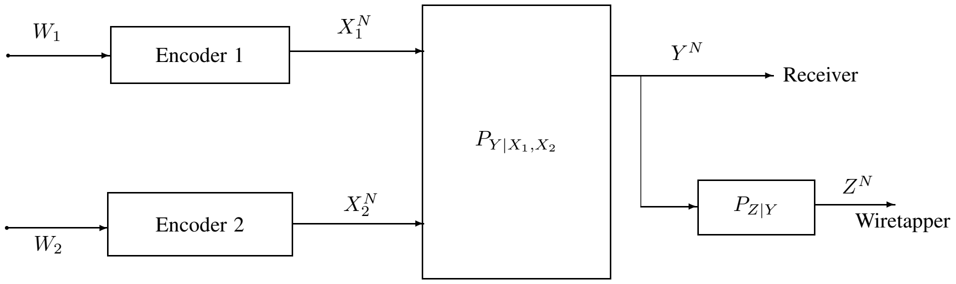
- The first is that two users wish to transmit their corresponding messages to a destination, and meanwhile, they also receive the channel output. Each user treats the other user as a wiretapper and wishes to keep its confidential message as secret as possible from the wiretapper. This model is usually called the MAC with confidential messages, and it was studied by Liang and Poor [18]. An inner bound on the capacity-equivocation region is provided for the model with two confidential messages, and the capacity-equivocation region is still not known. Furthermore, for the model of MAC with one confidential message [18], both inner and outer bounds on the capacity-equivocation region are derived. Moreover, for the degraded MAC with one confidential message, the capacity-equivocation region is totally determined.
- The second is that an additional wiretapper has access to the MAC output via a wiretap channel, and therefore, how to keep the confidential messages of the two users as secret as possible from the additional wiretapper is the main concern of the system designer. This model is usually called the multiple-access wiretap channel (MAC-WT). An inner bound on the secrecy capacity region of the degraded Gaussian MAC-WT was provided in [19], and a n-letter form

of the secrecy capacity region of the degraded Gaussian MAC-WT was shown in (Theorem 6 in [20]). Moreover, an inner bound on the secrecy capacity region of the general Gaussian MAC-WT was provided in [21]. In [22,23], the MAC-WT with partially cooperating encoders (one encoder is allowed to conference and the other does not transmit any message) was studied, and inner and outer bounds on the capacity-equivocation region of this model were provided. The MAC-WT with two conference links between the encoders was investigated in [24], and inner and outer bounds on the secrecy capacity region were established for this model. Besides these works on the discrete memoryless and Gaussian cases of MAC-WT, He *et al.* [25] studied the MIMO MAC-WT, where the channel matrices of the legitimate users are fixed and revealed to all of the terminals, whereas the channel matrices of the eavesdropper are arbitrarily varying and only known to the eavesdropper. Recently, Zaidi *et al.* ([26,27]) investigated the secrecy problem of MIMO x-channels with output feedback and delayed CSI (an extension of the model of MAC-WT). The optimal sum secure degrees of freedom (SDoF) region was characterized in [26,27], and the artificial noise technique was used to construct the corresponding encoding-decoding scheme.

In this paper, first, we study the degraded MAC-WT, see Figure 1. The motivation of this work is to find the secrecy capacity region of the general (not degraded) MAC-WT. However, it is difficult to find a tight outer bound on the secrecy capacity region of the general MAC-WT, and thus, in this paper, we focus on the secrecy capacity region of the degraded MAC-WT. Compared with the capacity result of (Theorem 6 in [20]) (n-letter form), the main contribution of this paper is the single-letter characterization of the secrecy capacity region of the degraded MAC-WT.

In Figure 1, two users transmit their corresponding confidential messages (no common message) to a legitimate receiver via a multiple-access channel (MAC), while an eavesdropper wishes to obtain the messages via a physically degraded wiretap channel. The secrecy capacity region of the model of Figure 1 is determined for both the discrete memoryless and Gaussian cases. Furthermore, for the Gaussian case, we find that the secrecy capacity region provided in this paper is exactly the same as the achievable secrecy rate region provided by Tekin and Yener [21]. Then, we study the power control for two kinds of optimal points (max-min point and single user point) on the secrecy rate region of a special Gaussian MAC-WT and find that these optimum points tend to be constants when the power tends to infinity.

Figure 1. The degraded multiple-access wiretap channel (MAC-WT).



In this paper, random variab1es, sample values and alphabets are denoted by capital letters, lower case letters and calligraphic letters, respectively. A similar convention is applied to the random vectors and their sample values. For example, U^N denotes a random N-vector $(U_1, ..., U_N)$, and $u^N = (u_1, ..., u_N)$ is a specific vector value in $\mathcal{U}^N$ that is the N-th Cartesian power of $\mathcal{U}$. U_i^N denotes a random $N-i+1$-vector $(U_i, ..., U_N)$, and $u_i^N = (u_i, ..., u_N)$ is a specific vector value in $\mathcal{U}_i^N$. Let $P_V(v)$ denote the probability mass function $Pr\{V = v\}$. Throughout the paper, the logarithmic function is to base two.

The organization of this paper is as follows. In Section 2, the secrecy capacity region of the degraded discrete memoryless MAC-WT is given by Theorem 1. In Section 3, the secrecy capacity region of the degraded Gaussian MAC-WT is given by Theorem 2. The power control for a special Gaussian MAC-WT is investigated in Section 4. Final conclusions are provided in Section 5.

2. Degraded Discrete Memoryless Multiple-Access Wiretap Channel

In this section, a description of the model of Figure 1 is given by Definition 1 to Definition 3. The secrecy capacity region $\mathcal{R}^D$ composed of all achievable secrecy pairs (R_1, R_2) in the model of Figure 1 is characterized in Theorem 1, where the achievable secrecy pair (R_1, R_2) is defined in Definition 4.

Definition 1. *(**Channel encoder**) The confidential messages W_1 and W_2 take values in $\mathcal{W}_1$, $\mathcal{W}_2$, respectively. W_1 and W_2 are independent and uniformly distributed over their ranges. The input of Encoder 1 (Encoder 2) is W_1 (W_2), while the output of Encoder 1 (Encoder 2) is X_1^N (X_2^N). We assume that the encoders are stochastic encoders, i.e., the encoder g_i^N ($i = 1, 2$) is a matrix of conditional probabilities $g_i^N(x_i^N|w_i)$, where $x_i^N \in \mathcal{X}_i^N$, $w_i \in \mathcal{W}_i$, and $g_i^N(x_i^N|w_i)$ is the probability that the message w_i is encoded as the channel input x_i^N. Note that X_1^N is independent of X_2^N. The transmission rates of the confidential messages are $\frac{\log\|\mathcal{W}_1\|}{N}$ and $\frac{\log\|\mathcal{W}_2\|}{N}$.*

Definition 2. *(**Channels**) The MAC is a discrete memoryless channel (DMC) with a finite input alphabet $\mathcal{X}_1 \times \mathcal{X}_2$, a finite output alphabet $\mathcal{Y}$ and transition probability $P_{Y|X_1,X_2}(y|x_1, x_2)$. Note that $P_{Y^N|X_1^N,X_2^N}(y^N|x_1^N, x_2^N) = \prod_{n=1}^N P_{Y_n|X_{1,n},X_{2,n}}(y_n|x_{1,n}, x_{2,n})$. The inputs of the MAC are X_1^N and X_2^N, while the output is Y^N.*

The wiretap channel is a DMC with finite input alphabet Y, finite output alphabet Z and transition probability $P_{Z|Y}(z|y)$. The wiretapper's equivocation to the confidential messages W_1 and W_2 is defined as:

$$\Delta = \frac{1}{N} H(W_1, W_2|Z^N). \tag{1}$$

Definition 3. *(**Decoder**) The decoder for the legitimate receiver is a mapping $f_D : \mathcal{Y}^N \to \mathcal{W}_1 \times \mathcal{W}_2$, with input Y^N and outputs $\breve{W}_1$, $\breve{W}_2$. Let P_e be the error probability of the receiver, and it is defined as $Pr\{(W_1, W_2) \neq (\breve{W}_1, \breve{W}_2)\}$.*

Definition 4. *(**Achievable secrecy pair (R_1, R_2) in the model of Figure 1**) A secrecy pair (R_1, R_2) (where $R_1, R_2 > 0$) is called achievable if, for any $\epsilon > 0$ (where ϵ is an arbitrary small positive real number and $\epsilon \to 0$), there exists a channel encoder-decoder (N, Δ, P_e), such that:*

$$\lim_{N\to\infty} \frac{\log \parallel \mathcal{W}_1 \parallel}{N} = R_1, \ \lim_{N\to\infty} \frac{\log \parallel \mathcal{W}_2 \parallel}{N} = R_2,$$
$$\lim_{N\to\infty} \Delta \geq R_1 + R_2, \ \ P_e \leq \epsilon. \tag{2}$$

Theorem 1 gives a single-letter characterization of the secrecy capacity region $\mathcal{R}^D$, which is composed of all achievable secrecy pairs (R_1, R_2) in the model of Figure 1.

Theorem 1. *A single-letter characterization of the secrecy capacity region $\mathcal{R}^D$ is as follows,*

$$\begin{aligned}
&\mathcal{R}^D = \{(R_1, R_2) : \\
&R_1 \leq I(X_1; Y|X_2, U) - I(X_1; Z|U) \\
&R_2 \leq I(X_2; Y|X_1, U) - I(X_2; Z|U) \\
&R_1 + R_2 \leq I(X_1, X_2; Y|U) - I(X_1, X_2; Z|U)\}
\end{aligned}$$

for some distribution:

$$P_{Z,Y,X_1,X_2,U}(z, y, x_1, x_2, u) = P_{Z|Y}(z|y)P_{Y|X_1,X_2}(y|x_1, x_2)P_{UX_1X_2}(u, x_1, x_2).$$

Proof. The converse proof of Theorem 1 is given in Section 7, and it is from the standard technique used in [1,2]. Now, we focus on the direct (achievability) proof of Theorem 1, and it is considered into two cases.

- Case 1: the pair $(R_1 = I(X_1; Y|U) - I(X_1; Z|U, X_2), R_2 = I(X_2; Y|X_1, U) - I(X_2; Z|U))$ is achievable.
- Case 2: the pair $(R_1 = I(X_1; Y|X_2, U) - I(X_1; Z|U), R_2 = I(X_2; Y|U) - I(X_2; Z|U, X_1))$ is achievable.

The encoding schemes for Case 1 and Case 2 are roughly illustrated in Figures 2 and 3, respectively. The proposed achievable encoding schemes combine the random binning, superposition coding and artificial noise techniques.

In Figure 2, the dummy message w^* is encoded as u^N, and the channel input x_1^N represents the superposition code in which the confidential message w_1 is superimposed on w^*. In addition, the channel input x_2^N represents the random binning codeword encoded by the confidential message w_2.

Analogously, in Figure 3, the dummy message w^* is encoded as u^N, and the channel input x_2^N represents the superposition code in which the confidential message w_2 is superimposed on w^*. In addition, the channel input x_1^N represents the random binning codeword encoded by the confidential message w_1.

The details of the complete proof will be provided in Section 6. □

Remark 1. *There are some notes on Theorem 1; see the following.*

- *The MAC-WT was first investigated by Tekin and Yener [19,21]. In [21], an achievable secrecy rate region (inner bound on the secrecy capacity region) is given by:*

$$\begin{aligned}
&\mathcal{R}^{Di} = \{(R_1, R_2) : \\
&R_1 \leq I(X_1; Y|X_2) - I(X_1; Z) \\
&R_2 \leq I(X_2; Y|X_1) - I(X_2; Z) \\
&R_1 + R_2 \leq I(X_1, X_2; Y) - I(X_1, X_2; Z)\}
\end{aligned}$$

Letting U be a constant, it is easy to see that the region $\mathcal{R}^D$ of Theorem 1 reduces to $\mathcal{R}^{Di}$, i.e., $\mathcal{R}^{Di} \subseteq \mathcal{R}^D$.

- *Note that the above $\mathcal{R}^{Di}$ is constructed according to the random binning technique. In this paper, we combine the artificial noise technique (the dummy message w^* can be also viewed as an artificial noise) with the classical random binning technique to construct the encoding scheme of the model of Figure 1. To be more specific, first, we randomly choose a dummy message (artificial noise) w^*. Second, the transmitted codeword is constructed by using the double binning technique, where the index of the bin is related to w^* and the index of the sub-bin is related to the transmitted message w_1 or w_2. Finally, we randomly choose a codeword in sub-bin w_1 or w_2 to transmit. By using this double binning technique, we prove that $\mathcal{R}^D$ is achievable. Here, note that the double binning technique (combination of artificial noise and binning) is also used in [22,23]. By using the Markov chain $(X_1, X_2) \rightarrow Y \rightarrow Z$ and letting $R_e = R_1$, $V = const$, $V_1 = X_1$, $V_2 = X_2$ and $C_{12} = 0$, it is easy to see that the third inequality of (Theorem 2 in [22]) reduces to $R_1 \leq I(X_1; Y|X_2, U) - I(X_1; Z|U)$, and it is coincident with the first inequality of $\mathcal{R}^D$.*
- *The region $\mathcal{R}^D$ is convex. The proof is directly obtained by introducing a time sharing random variable into Theorem 1, and thus, it is omitted here.*

Figure 2. The encoding scheme for Case 1.

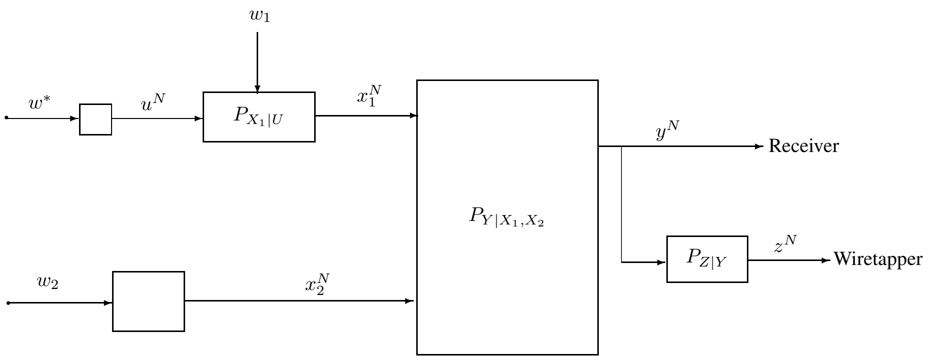
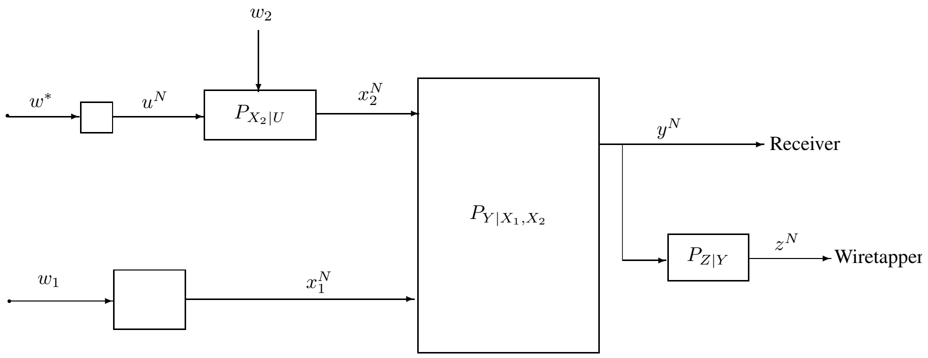


Figure 3. The encoding scheme for Case 2.



3. Degraded Gaussian Multiple-Access Wiretap Channel

3.1. Secrecy Capacity Region of the Degraded Gaussian Multiple-Access Wiretap Channel

In this subsection, we investigate the Gaussian case of the model of Figure 1, where the channel input-output relationships at each time instant i $(1 \leq i \leq N)$ are given by:

$$Y_i = X_{1,i} + X_{2,i} + \eta_{1,i}, \tag{1}$$

and:

$$Z_i = X_{1,i} + X_{2,i} + \eta_{1,i} + \eta_{2,i}, \tag{2}$$

where $\eta_{1,i} \sim \mathcal{N}(0, N_1)$ and $\eta_{2,i} \sim \mathcal{N}(0, N_2)$. The random vectors η_1^N and η_2^N are independent with i.i.d. components. The channel inputs X_1^N and X_2^N are subject to the average power constraints P_1 and P_2, respectively, *i.e.*,

$$\frac{1}{N}\sum_{i=1}^{N} E[X_{1,i}^2] = p_1 \le P_1, \quad \frac{1}{N}\sum_{i=1}^{N} E[X_{2,i}^2] = p_2 \le P_2. \tag{3}$$

Note that X_1^N is independent of X_2^N.

Theorem 2. *The secrecy capacity region $\mathcal{R}^G$ of the Gaussian model of Figure 1 is given by:*

$$\mathcal{R}^G = \mathcal{A}\bigcup\mathcal{B},$$

where:

$$\mathcal{A} = \bigcup_{\substack{0\le\alpha\le 1\\ 0\le p_1\le P_1\\ 0\le p_2\le P_2}} \left\{\begin{array}{l}(R_1,R_2):\\ R_1 \le \frac{1}{2}\log(1+\frac{(1-\alpha)p_1}{N_1}) - \frac{1}{2}\log(1+\frac{(1-\alpha)p_1}{N_1+N_2+p_2})\\ R_2 \le \frac{1}{2}\log(1+\frac{p_2}{N_1}) - \frac{1}{2}\log(1+\frac{p_2}{N_1+N_2+(1-\alpha)p_1})\\ R_1+R_2 \le \frac{1}{2}\log(1+\frac{(1-\alpha)p_1+p_2}{N_1}) - \frac{1}{2}\log(1+\frac{(1-\alpha)p_1+p_2}{N_1+N_2})\end{array}\right\},$$

and:

$$\mathcal{B} = \bigcup_{\substack{0\le\alpha\le 1\\ 0\le p_1\le P_1\\ 0\le p_2\le P_2}} \left\{\begin{array}{l}(R_1,R_2):\\ R_1 \le \frac{1}{2}\log(1+\frac{p_1}{N_1}) - \frac{1}{2}\log(1+\frac{p_1}{N_1+N_2+(1-\alpha)p_2})\\ R_2 \le \frac{1}{2}\log(1+\frac{(1-\alpha)p_2}{N_1}) - \frac{1}{2}\log(1+\frac{(1-\alpha)p_2}{N_1+N_2+p_1})\\ R_1+R_2 \le \frac{1}{2}\log(1+\frac{(1-\alpha)p_2+p_1}{N_1}) - \frac{1}{2}\log(1+\frac{(1-\alpha)p_2+p_1}{N_1+N_2})\end{array}\right\}.$$

Proof. The proof of Theorem 2 is considered in the following two parts:

- (Proof of $\mathcal{A}$): The direct proof follows by computing the mutual information terms in Theorem 1 with the following distributions: $X_1 = U + V$, $U \sim \mathcal{N}(0, \alpha p_1)$, $V \sim \mathcal{N}(0, (1-\alpha)p_1)$ and $X_2 \sim \mathcal{N}(0, p_2)$. U, V and X_2 are independent. The details are omitted here. The converse proof follows from Section 7, and it is omitted here, too. Thus, the proof of $\mathcal{A}$ is completed.
- (Proof of $\mathcal{B}$): The direct proof follows by computing the mutual information terms in Theorem 1 with the following distributions: $X_2 = U + V$, $U \sim \mathcal{N}(0, \alpha p_2)$, $V \sim \mathcal{N}(0, (1-\alpha)p_2)$ and $X_1 \sim \mathcal{N}(0, p_1)$. U, V and X_1 are independent. The details are omitted here. The converse proof follows from Section 7, and it is omitted here, too. Thus, the proof of $\mathcal{B}$ is completed.

The proof of Theorem 2 is completed. □

3.2. Discussions

First, note that an achievable secrecy rate region of the degraded Gaussian MAC-WT is provided in [21], and it is given by:

$$\mathcal{R}^{Gi} = \bigcup_{\substack{0 \leq p_1 \leq P_1 \\ 0 \leq p_2 \leq P_2}} \left\{ \begin{array}{l} (R_1, R_2): \\ R_1 \leq \frac{1}{2}\log(1+\frac{p_1}{N_1}) - \frac{1}{2}\log(1+\frac{p_1}{N_1+N_2+p_2}) \\ R_2 \leq \frac{1}{2}\log(1+\frac{p_2}{N_1}) - \frac{1}{2}\log(1+\frac{p_2}{N_1+N_2+p_1}) \\ R_1+R_2 \leq \frac{1}{2}\log(1+\frac{p_1+p_2}{N_1}) - \frac{1}{2}\log(1+\frac{p_1+p_2}{N_1+N_2}) \end{array} \right\}.$$

The secrecy capacity region $\mathcal{R}^G$ is achieved when $\alpha = 0$, and it coincides with Tekin–Yener's inner bound $\mathcal{R}^{Gi}$, *i.e.*, Tekin–Yener's inner bound $\mathcal{R}^{Gi}$ is, in fact, the secrecy capacity region of the degraded Gaussian MAC-WT. The rigorous proof is as follows.

Proof. Observing that the region $\mathcal{A}$ of Theorem 2 can be rewritten as:

$$\mathcal{A} = \bigcup_{\substack{0 \leq \alpha \leq 1 \\ 0 \leq p_1 \leq P_1 \\ 0 \leq p_2 \leq P_2}} \left\{ \begin{array}{l} (R_1, R_2): \\ R_1 \leq \frac{1}{2}\log(\frac{p_2+N_1+N_2}{N_1}(1-\frac{p_2+N_2}{p_2+N_2+N_1+(1-\alpha)p_1})) \\ R_2 \leq \frac{1}{2}\log(\frac{p_2+N_1}{N_1}(1-\frac{p_2}{p_2+N_2+N_1+(1-\alpha)p_1})) \\ R_1+R_2 \leq \frac{1}{2}\log(\frac{N_1+N_2}{N_1}(1-\frac{N_2}{p_2+N_2+N_1+(1-\alpha)p_1})) \end{array} \right\}.$$

It is easy to see that the region $\mathcal{A}$ achieves its maximum when $\alpha = 0$. Analogously, the region $\mathcal{B}$ achieves its maximum when $\alpha = 0$. Note that the regions $\mathcal{A}$ and $\mathcal{B}$ are exactly the same as the region $\mathcal{R}^{Gi}$ if $\alpha = 0$. Thus, the proof is completed.

□

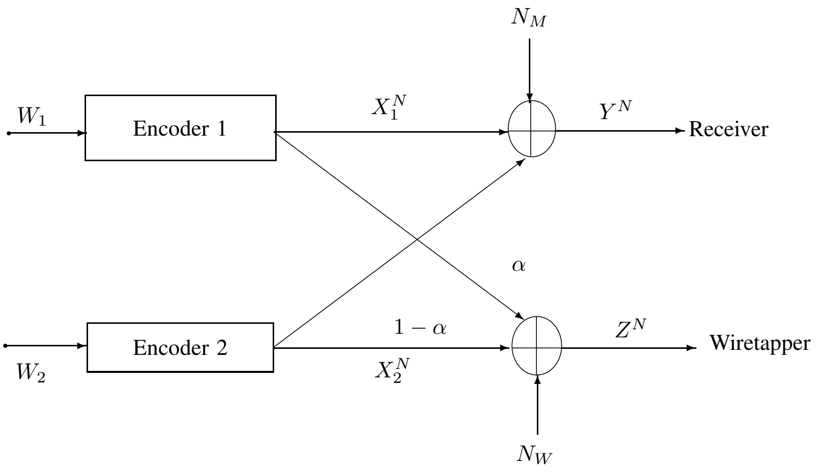
4. Power Control for Two Kinds of Optimal Points on the Secrecy Rate Region of a Special Gaussian Multiple-Access Wiretap Channel

In this section, we investigate a special Gaussian MAC-WT; see Figure 4. The model of Figure 4 is characterized by:

$$Y^N = X_1^N + X_2^N + N_M, \quad Z^N = \alpha X_1^N + (1-\alpha)X_2^N + N_W, \tag{1}$$

where $N_M, N_W \sim \mathcal{N}(0,1)$ and $0 < \alpha \leq \frac{1}{2}$.

Figure 4. A special Gaussian multiple-access wiretap channel.



An achievable secrecy rate region $\mathcal{R}$ of the model of Figure 4 is given by (2), where p_1 and p_2 are transmission powers for the codewords x_1^N and x_2^N, respectively, and $0 \le p_1, p_2 \le P$. Note that the region $\mathcal{R}$ is directly from [21].

$$\mathcal{R} = \bigcup_{\substack{0 \le p_1 \le P_1 \\ 0 \le p_2 \le P_2}} \left\{ \begin{array}{l} (R_1, R_2): \\ R_1 \le \frac{1}{2}\log(1+p_1) - \frac{1}{2}\log(1+\frac{\alpha p_1}{1+(1-\alpha)p_2}) \\ R_2 \le \frac{1}{2}\log(1+p_2) - \frac{1}{2}\log(1+\frac{(1-\alpha)p_2}{1+\alpha p_1}) \\ R_1 + R_2 \le \frac{1}{2}\log(1+p_1+p_2) - \frac{1}{2}\log(1+\alpha p_1 + (1-\alpha)p_2) \end{array} \right\}. \tag{2}$$

In addition, the optimum power control for the maximization of the total secrecy sum rate is given by:

$$(p_1^*, p_2^*) = \begin{cases} (P, P), & \text{if } 0 \le P \le \frac{\alpha}{1-2\alpha}, \\ (P, 0), & P > \frac{\alpha}{1-2\alpha}. \end{cases} \tag{3}$$

and the corresponding maximum secrecy sum rate R_{sum}^* is given by:

$$R_{sum}^* = \max(R_1 + R_2) = \begin{cases} \frac{1}{2}\log\frac{1+2P}{1+P}, & \text{if } 0 \le P \le \frac{\alpha}{1-2\alpha}, \\ \frac{1}{2}\log\frac{1+P}{1+\alpha P}, & P > \frac{\alpha}{1-2\alpha}. \end{cases} \tag{4}$$

In the remainder of this section, the power control for two kinds of optimum points (max-min point and single user point) on the secrecy rate region of Figure 4 is provided in Sections 4.1 and 4.2. Numerical examples and discussions are in Section 4.3.

4.1. Max-Min Point

We first define an optimal point in the following sense:

$$R_{min}^* \triangleq \max_{p_1, p_2} \min\{R_1, R_2\}. \tag{5}$$

Theorem 3. *For the model of Figure 4, the optimum point R_{min}^* satisfies:*

$$R_{min}^* = \begin{cases} \frac{1}{2}\log(1+\alpha P), & \textit{if } 0 \le P \le \frac{\sqrt{(\alpha-2)^2+4}-(\alpha+2)}{2\alpha}, \\ \frac{1}{2}\log\frac{1+2P}{1+P}, & P > \frac{\sqrt{(\alpha-2)^2+4}-(\alpha+2)}{2\alpha}. \end{cases}$$

R_{min}^* is achieved if $(p_1^*, p_2^*) = (P, P)$.

Proof. First, for convenience, define:

$$a = \frac{1}{2}\log\frac{(1+p_1)(1+(1-\alpha)p_2)}{1+(1-\alpha)p_2+\alpha p_1}, \tag{6}$$

$$b = \frac{1}{2}\log\frac{(1+p_2)(1+\alpha p_1)}{1+(1-\alpha)p_2+\alpha p_1}, \tag{7}$$

$$c = \frac{1}{2}\log\frac{1+p_1+p_2}{1+(1-\alpha)p_2+\alpha p_1}. \tag{8}$$

Then, (2) can be rewritten as:

$$\mathcal{R} = \bigcup_{\substack{0 \le p_1 \le P_1 \\ 0 \le p_2 \le P_2}} \left\{ \begin{array}{l} (R_1, R_2): \\ R_1 \le a \\ R_2 \le b \\ R_1 + R_2 \le c \end{array} \right\}. \tag{9}$$

The calculation of R^*_{min} depends on the following three cases; see Figure 5. The regions $\mathcal{A}$ and $\mathcal{B}$ of these three figures imply that $R_1 \le R_2$ and $R_1 \ge R_2$, respectively. In region $\mathcal{A}$, $R^*_{min} = \max\min\{R_1, R_2\} = \max R_1$, and in region $\mathcal{B}$, $R^*_{min} = \max\min\{R_1, R_2\} = \max R_2$.

Therefore, from Figure 5a, it is easy to see that:

$$R^*_{min} = \max_{p_1,p_2} b, \quad s.t.\ b \le \frac{1}{2}c \le a. \tag{10}$$

Similarly, from Figure 5b, we see that:

$$R^*_{min} = \max_{p_1,p_2} \frac{1}{2}c, \quad s.t.\ \frac{1}{2}c \le \min\{a, b\}. \tag{11}$$

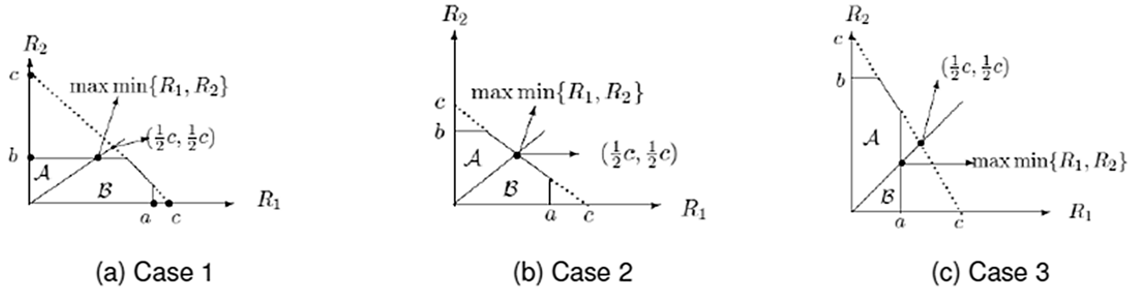
From Figure 5c, we see that:

$$R^*_{min} = \max_{p_1,p_2} a, \quad s.t.\ a \le \frac{1}{2}c \le b. \tag{12}$$

By using the well-known method of Lagrange multipliers on (10), (11) and (12), Theorem 3 is proven.

□

Figure 5. All cases for the calculation of R^*_{min}.



4.2. Single User Point

We now investigate another point, called the single user point, on which the legitimate receiver tries to maximize the secrecy rate R_1 (or R_2) with the help of the senders, *i.e.*, $R^*_{su,i} = \max R_i$ $(i = 1, 2)$.

Theorem 4. *For the model of Figure 4, the optimum point $R^*_{su,1}$ satisfies:*

$$R^*_{su,1} = \begin{cases} \frac{1}{2}\log(1 + (1-\alpha)P), & \text{if } 0 \le P \le \frac{\alpha}{1-\alpha}, \\ \frac{1}{2}\log\frac{1+2P}{1+P}, & \text{if } \frac{\alpha}{1-\alpha} \le P \le \frac{\alpha}{1-2\alpha}, \\ \frac{1}{2}\log\frac{1+P}{1+\alpha P}, & P > \frac{\alpha}{1-2\alpha}. \end{cases}$$

The optimum power control achieving $R^*_{su,1}$ is given by:

$$(p_1^*, p_2^*) = \begin{cases} (P, P), & \textit{if } 0 \le P \le \frac{\alpha}{1-\alpha}, \\ (P, P), & \textit{if } \frac{\alpha}{1-\alpha} \le P \le \frac{\alpha}{1-2\alpha}, \\ (P, 0), & P > \frac{\alpha}{1-2\alpha}. \end{cases}$$

The optimum point $R^*_{su,2}$ satisfies:

- *If* $0 \le \alpha \le \frac{3-\sqrt{5}}{2}$,

$$R^*_{su,2} = \begin{cases} \frac{1}{2}\log(1+\alpha P), & \textit{if } 0 \le P \le \frac{\alpha}{1-2\alpha}, \\ \frac{1}{2}\log(1+\alpha P), & \textit{if } \frac{\alpha}{1-2\alpha} \le P \le \frac{1-2\alpha}{\alpha^2}, \\ \frac{1}{2}\log\frac{1+P}{1+\alpha P}, & P > \frac{1-2\alpha}{\alpha^2}. \end{cases}$$

The optimum power control achieving $R^*_{su,2}$ is given by:

$$(p_1^*, p_2^*) = \begin{cases} (P, P), & \textit{if } 0 \le P \le \frac{\alpha}{1-2\alpha}, \\ (P, 0), & \textit{if } \frac{\alpha}{1-2\alpha} \le P \le \frac{1-2\alpha}{\alpha^2}, \\ (P, 0), & P > \frac{1-2\alpha}{\alpha^2}. \end{cases}$$

- *If* $\frac{3-\sqrt{5}}{2} \le \alpha \le \frac{1}{2}$,

$$R^*_{su,2} = \begin{cases} \frac{1}{2}\log(1+\alpha P), & \textit{if } 0 \le P \le \frac{1-\alpha}{\alpha}, \\ \frac{1}{2}\log\frac{1+2P}{1+P}, & \textit{if } \frac{1-\alpha}{\alpha} \le P \le \frac{\alpha}{1-2\alpha}, \\ \frac{1}{2}\log\frac{1+P}{1+\alpha P}, & P > \frac{\alpha}{1-2\alpha}. \end{cases}$$

The optimum power control achieving $R^*_{su,2}$ is given by:

$$(p_1^*, p_2^*) = \begin{cases} (P, P), & \textit{if } 0 \le P \le \frac{1-\alpha}{\alpha}, \\ (P, P), & \textit{if } \frac{1-\alpha}{\alpha} \le P \le \frac{\alpha}{1-2\alpha}, \\ (P, 0), & P > \frac{\alpha}{1-2\alpha}. \end{cases}$$

Proof. By using (2), $R^*_{su,1}$ and $R^*_{su,2}$ can be rewritten as $R^*_{su,1} = \max R_1 = \max\{a, c\}$ and $R^*_{su,2} = \max R_2 = \max\{b, c\}$, respectively. Here, a, b and c are defined in (6), (7) and (8), respectively.

By using the method of Lagrange multipliers, Theorem 4 is proven.

□

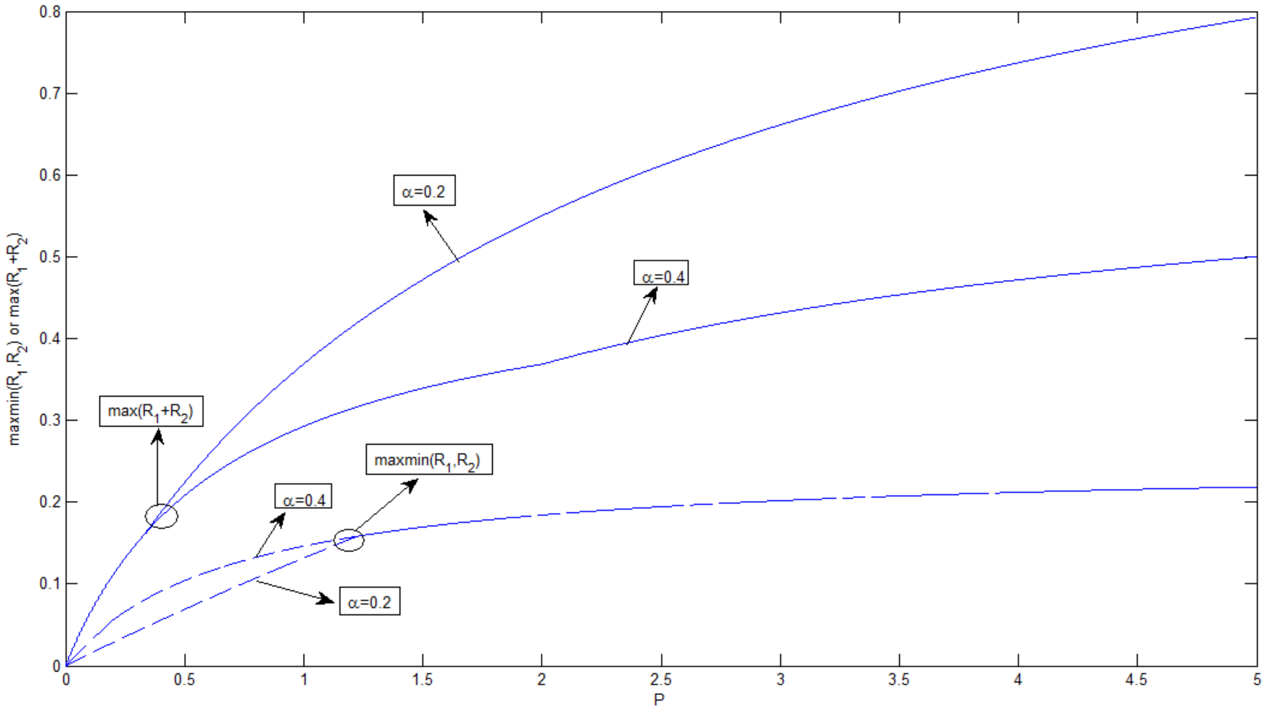
4.3. Numerical Examples and Discussions

Figure 6 shows the max-min point R^*_{min} and the maximum secrecy sum rate R^*_{sum} for $\alpha = 0.2$ and $\alpha = 0.4$. It is easy to see that R^*_{sum} increases while α decreases and that R^*_{min} increases while α increases. Furthermore, R^*_{min} tends to be a constant (0.5) while P tends to infinity. R^*_{sum} tends to be $\frac{1}{2}\log\frac{1}{\alpha}$ while P tends to infinity.

Figure 7 shows the single user points $R^*_{su,1}$ and $R^*_{su,2}$ for $\alpha = 0.2$ and $\alpha = 0.4$. It is easy to see that the curve for $R^*_{su,1}$ is always better than that for $R^*_{su,2}$. Furthermore, $R^*_{su,1}$ and $R^*_{su,2}$ tend to be the same constant $\frac{1}{2}\log\frac{1}{\alpha}$, while P tends to infinity. In addition, for a fixed α, when P tends to infinity, R^*_{sum}, $R^*_{su,1}$ and $R^*_{su,2}$ are the same.

The above results show that the secrecy rate region of Gaussian MAC-WT behaves significantly different from the classical capacity of Gaussian MAC. When classical capacity is concerned, the max-min point is always attained when the sum rate $R_1 + R_2$ is also maximized. However, for secrecy capacity, the point $\max(R_1 + R_2)$ does not necessarily coincide with R^*_{min} all the time.

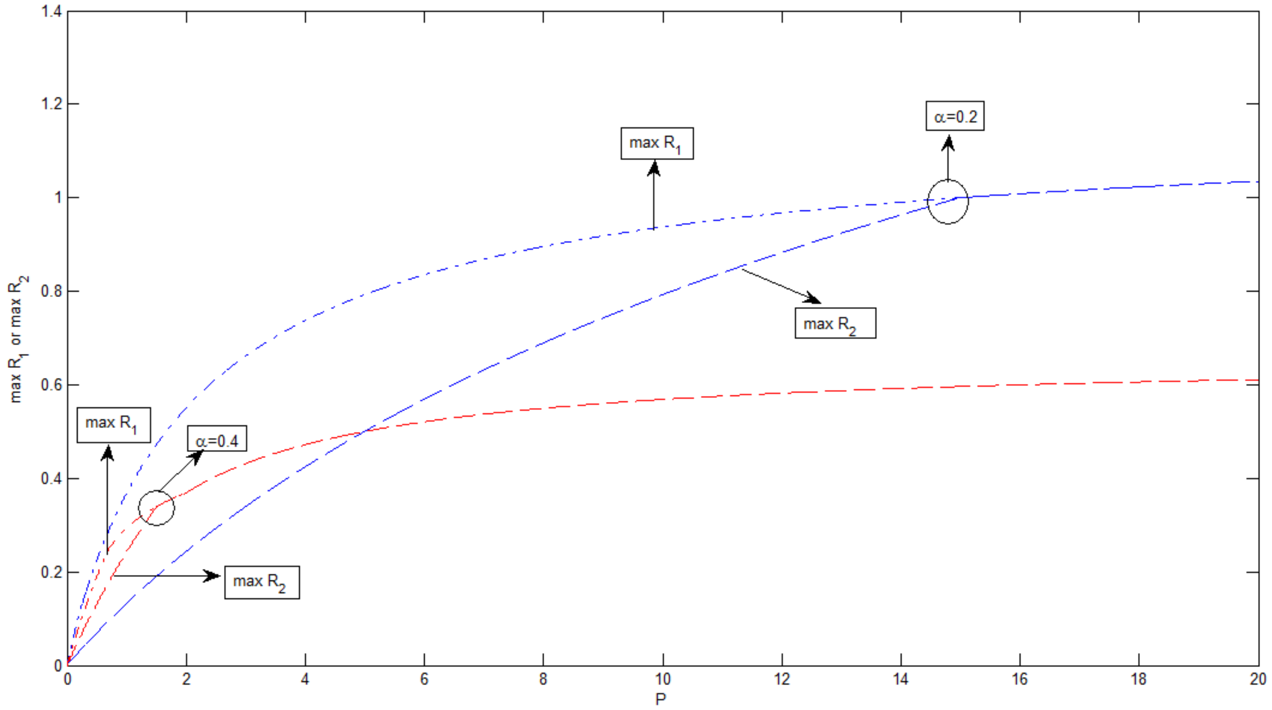
Figure 6. The R^*_{min} and R^*_{sum} for $\alpha = 0.2$ and $\alpha = 0.4$.



5. Conclusions

In this paper, first, we study the degraded multiple-access wiretap channel (MAC-WT). The secrecy capacity region is determined for both the discrete memoryless and Gaussian cases. Furthermore, for the Gaussian case, we find that the secrecy capacity region provided in this paper is exactly the same as the achievable secrecy rate region provided by Tekin and Yener. Then, we study the power control for two kinds of optimal points (max-min point and single user point) on the secrecy rate region of a special Gaussian MAC-WT and find that these optimum points tend to be constants when the power tends to infinity.

Figure 7. The $R^*_{su,1}$ and $R^*_{su,2}$ for $\alpha = 0.2$ and $\alpha = 0.4$.



6. Direct Proof of Theorem 1

We consider the achievability proof of Theorem 1 for the case that the pair $(R_1 = I(X_1;Y|X_2,U) - I(X_1;Z|U), R_2 = I(X_2;Y|U) - I(X_2;Z|U,X_1))$ is achievable, and the achievability proof for the pair $(R_1 = I(X_1;Y|U) - I(X_1;Z|U,X_2), R_2 = I(X_2;Y|X_1,U) - I(X_2;Z|U))$ follows by symmetry.

The coding scheme combines the random binning, superposition coding and artificial noise techniques; see Figure 3. Define the messages W_1, W_2 and W^* (dummy message) taking values in the alphabets $\mathcal{W}_1$, $\mathcal{W}_2$ and $\mathcal{W}^*$, respectively, where:

$$\mathcal{W}_1 = \{1,2,...,2^{NR_1}\},\ \mathcal{W}_2 = \{1,2,...,2^{NR_2}\},\ \mathcal{W}^* = \{1,2,...,2^{NR^*}\}.$$

Fix the joint probability mass function $P_{Z,Y,X_1,X_2,U}(z,y,x_1,x_2,u)$. For arbitrary $\epsilon > 0$, define:

$$R_1 = I(X_1;Y|X_2,U) - I(X_1;Z|U), \tag{1}$$

$$R_2 = I(X_2;Y|U) - I(X_2;Z|U,X_1), \tag{2}$$

$$R^* = \min\{I(U;Y), I(U;Z)\} - \epsilon_1 \overset{(a)}{=} I(U;Z) - \epsilon_1, \tag{3}$$

$$R^{**} = I(X_2;Z|U,X_1) - \epsilon_1, \tag{4}$$

where (a) is from the Markov chain $U \rightarrow Y \rightarrow Z$ and $\epsilon_1 \rightarrow 0$ as $N \rightarrow \infty$.

Here, note that:

$$R_2 + R^* + R^{**} = I(X_2;Y|U) + I(U;Z) - 2\epsilon_1 \leq I(X_2;Y|U) + I(U;Y) - 2\epsilon_1 \overset{(b)}{=} I(X_2;Y) - 2\epsilon_1, \tag{5}$$

where (b) is from the Markov chain $U \rightarrow X_2 \rightarrow Y$.

Now, the remainder of this section is organized as follows. The code construction is introduced in Section 6.1. For any $\epsilon > 0$, the proofs of $\lim_{N\to\infty} \frac{\log\|\mathcal{W}_1\|}{N} = R_1$, $\lim_{N\to\infty} \frac{\log\|\mathcal{W}_2\|}{N} = R_2$, $\lim_{N\to\infty} \Delta \geq R_1 + R_2$ and $P_e \leq \epsilon$ are given in Section 6.2.

6.1. Coding Construction

Construction of X_1^N: Generate $2^{N(I(X_1;Y|X_2,U)-\epsilon_2)}$ i.i.d. codewords x_1^N ($\epsilon_2 \to 0$ as $N \to \infty$) according to $\prod_{i=1}^{N} P_{X_1}(x_{1,i})$, and divide them into 2^{NR_1} bins. Each bin contains $2^{N(I(X_1;Y|X_2,U)-\epsilon_2-R_1)}$ codewords. Here, note that:

$$I(X_1;Y|X_2,U) - \epsilon_2 - R_1 \overset{(c)}{=} I(X_1;Z|U) - \epsilon_2, \tag{6}$$

where (c) is from (1). For a given confidential message w_1, randomly choose a codeword in bin w_1 to transmit.

Construction of U^N (dummy message): Generate 2^{NR^*} i.i.d. codewords u^N according to $\prod_{i=1}^{N} P_U(u_i)$. Randomly choose a $u^N(w^*)$ to transmit. Note that here, U^N is independent of X_1^N.

Construction of X_2^N: Generate $2^{N(R_2+R^*+R^{**})}$ i.i.d. codewords x_2^N according to $\prod_{i=1}^{N} P_{X_2|U}(x_{2,i}|u_i)$, and divide them into 2^{NR^*} bins. Each bin contains $2^{N(R_2+R^{**})}$ codewords. Divide the codewords in each bin into 2^{NR_2} sub-bins, and each sub-bin contains $2^{NR^{**}}$ codewords.

For a transmitted dummy message w^* and a given message w_2, first choose the index of the bin according to w^*, and then, choose the index of the sub-bin in bin w^* according to w_2. Finally, randomly choose a codeword in sub-bin w_2 to transmit.

Decoding scheme for the legitimate receiver: for a given y^N, try to find a sequence $u^N(\hat{w}^*)$, such that $(u^N(\hat{w}^*), y^N)$ are jointly typical. If there exists a unique sequence with the index $\hat{w}^*$, put out the corresponding $\hat{w}^*$, else declare a decoding error. Based on the AEPand (3), the probability $Pr\{\hat{w}^* = w^*\}$ goes to one.

After decoding $\hat{w}^*$, the legitimate receiver tries to find a sequence $x_2^N(\hat{w}_2, \hat{w}^*)$, such that $(u^N(\hat{w}^*), x_2^N(\hat{w}_2, \hat{w}^*), y^N)$ are jointly typical. If there exists a unique sequence with the index $\hat{w}_2$, put out the corresponding $\hat{w}_2$; else declare a decoding error. Based on the AEP, (2), (3), (4), (5) and the construction of x_2^N, the probability $Pr\{\hat{w}_2 = w_2\}$ goes to one.

Finally, after decoding $\hat{w}_2$ and $\hat{w}^*$, the legitimate receiver tries to find a sequence $x_1^N(\hat{w}_1)$, such that $(u^N(\hat{w}^*), x_1^N(\hat{w}_1), x_2^N(\hat{w}_2, \hat{w}^*), y^N)$ are jointly typical. There exists a unique sequence with the index $\hat{w}_1$; put out the corresponding $\hat{w}_1$; else declare a decoding error. Based on the AEP, (1) and the construction of x_1^N, the probability $Pr\{\hat{w}_1 = w_1\}$ goes to one.

6.2. Proof of the Achievability

By using the above definitions, it is easy to verify that $\lim_{N\to\infty} \frac{\log\|\mathcal{W}_1\|}{N} = R_1$ and $\lim_{N\to\infty} \frac{\log\|\mathcal{W}_2\|}{N} = R_2$. Then, by using the above encoding-decoding scheme, $P_e \leq \epsilon$ is easy to be checked. It remains to be shown that $\lim_{N\to\infty} \Delta \geq R_1 + R_2$; see the following.

$$\begin{aligned} \lim_{N\to\infty} \Delta &= \lim_{N\to\infty} \frac{1}{N} H(W_1, W_2|Z^N) \\ &= \lim_{N\to\infty} \frac{1}{N} (H(W_1|Z^N) + H(W_2|W_1, Z^N)). \end{aligned} \tag{7}$$

The first term in (7) is bounded as follows.

$$\begin{aligned}
&\lim_{N\to\infty}\frac{1}{N}H(W_1|Z^N) \geq \lim_{N\to\infty}\frac{1}{N}H(W_1|Z^N,U^N)\\
=\;&\lim_{N\to\infty}\frac{1}{N}(H(W_1,Z^N,U^N)-H(Z^N,U^N))\\
=\;&\lim_{N\to\infty}\frac{1}{N}(H(W_1,Z^N,U^N,X_1^N)-H(X_1^N|W_1,Z^N,U^N)-H(Z^N,U^N))\\
\overset{(a)}{=}\;&\lim_{N\to\infty}\frac{1}{N}(H(Z^N|U^N,X_1^N)+H(U^N)+H(X_1^N)-H(X_1^N|W_1,Z^N,U^N)\\
&-H(Z^N,U^N))\\
=\;&\lim_{N\to\infty}\frac{1}{N}(H(X_1^N)-I(X_1^N;Z^N|U^N)-H(X_1^N|W_1,Z^N,U^N)),
\end{aligned}\tag{8}$$

where (a) is from $H(W_1|X_1^N)=0$ and U^N is independent of X_1^N.

Consider the first term in (8); the codeword generation and [18, Lemma 3] ensure that:

$$\lim_{N\to\infty}\frac{1}{N}H(X_1^N) \geq I(X_1;Y|X_2,U). \tag{9}$$

For the second term in (8), using the same approach as that in [2, Lemma 3], we get:

$$\lim_{N\to\infty}\frac{1}{N}I(X_1^N;Z^N|U^N) \geq I(X_1;Z|U). \tag{10}$$

Now, we consider the last term of (8). From (6), given U^N, Z^N and W_1, the total number of possible codewords of X_1^N is $2^{N(I(X_1;Z|U)-\epsilon_2)}$. By using Fano's inequality and the fact that $\epsilon_2\to 0$ as $N\to\infty$, we have:

$$\lim_{N\to\infty}\frac{1}{N}H(X_1^N|W_1,Z^N,U^N)=0. \tag{11}$$

Substituting (9), (10) and (11) into (8), we have:

$$\lim_{N\to\infty}\frac{1}{N}H(W_1|Z^N) \geq I(X_1;Y|X_2,U)-I(X_1;Z|U)=R_1. \tag{12}$$

The second term in (7) is bounded as follows.

$$\begin{aligned}
&\lim_{N\to\infty}\frac{1}{N}H(W_2|W_1,Z^N) \geq \lim_{N\to\infty}\frac{1}{N}H(W_2|W_1,Z^N,U^N)\\
\geq\;&\lim_{N\to\infty}\frac{1}{N}H(W_2|W_1,Z^N,U^N,X_1^N)\\
\overset{(1)}{=}\;&\lim_{N\to\infty}\frac{1}{N}H(W_2|Z^N,U^N,X_1^N)\\
=\;&\lim_{N\to\infty}\frac{1}{N}(H(W_2,Z^N,U^N,X_1^N)-H(Z^N,U^N,X_1^N))\\
=\;&\lim_{N\to\infty}\frac{1}{N}(H(W_2,Z^N,U^N,X_1^N,X_2^N)-H(X_2^N|W_2,Z^N,U^N,X_1^N)\\
&-H(Z^N,U^N,X_1^N))\\
\overset{(2)}{=}\;&\lim_{N\to\infty}\frac{1}{N}(H(Z^N|U^N,X_1^N,X_2^N)+H(X_1^N)+H(U^N,X_2^N)\\
&-H(X_2^N|W_2,Z^N,U^N,X_1^N)-H(Z^N|U^N,X_1^N)-H(U^N)-H(X_1^N))\\
=\;&\lim_{N\to\infty}\frac{1}{N}(H(X_2^N|U^N)-I(X_2^N;Z^N|U^N,X_1^N)-H(X_2^N|W_2,Z^N,U^N,X_1^N)),
\end{aligned}\tag{13}$$

where (1) is from $H(W_1|X_1^N) = 0$ and (2) is from X_1^N independent of U^N and X_2^N.

Consider the first term in (13); the codeword generation and ([18] Lemma 3) LP1 ensure that:

$$\lim_{N\to\infty} \frac{1}{N} H(X_2^N|U^N) \geq I(X_2;Y|U). \tag{14}$$

For the second term in (13), using the same approach as that in ([2] Lemma 3), we get:

$$\lim_{N\to\infty} \frac{1}{N} I(X_2^N;Z^N|U^N,X_1^N) \geq I(X_2;Z|U,X_1). \tag{15}$$

Now, we consider the last term of (13). Given U^N, Z^N, X_1^N and W_2, the total number of possible codewords of X_1^N is $2^{NR^{**}}$. By using Fano's inequality and (4), we have:

$$\lim_{N\to\infty} \frac{1}{N} H(X_2^N|W_2,Z^N,U^N,X_1^N) = 0. \tag{16}$$

Substituting (14), (15) and (16) into (13), we have:

$$\lim_{N\to\infty} \frac{1}{N} H(W_2|W_1,Z^N) \geq I(X_2;Y|U) - I(X_2;Z|U,X_1) = R_2. \tag{17}$$

Substituting (12) and (17) into (7), $\lim_{N\to\infty} \Delta \geq R_1 + R_2$ is proven.

The achievability proof of Theorem 1 is completed.

7. Converse Proof of Theorem 1

In this section, we prove the converse part of Theorem 1: all the achievable secrecy pairs (R_1, R_2) are contained in the set $\mathcal{R}^D$. We will prove the inequalities of Theorem 1 in the remainder of this section.

(Proof of $R_1 \leq I(X_1;Y|X_2,U) - I(X_1;Z|U)$):

$$\begin{aligned}
&\frac{1}{N}H(W_1) \overset{(1)}{=} \frac{1}{N}H(W_1|Z^N)\\
=\ & \frac{1}{N}(H(W_1|Z^N) - H(W_1|Z^N,W_2,Y^N) + H(W_1|Z^N,W_2,Y^N))\\
\overset{(2)}{\leq}\ & \frac{1}{N}(I(W_1;W_2,Y^N|Z^N) + \delta(P_e))\\
\leq\ & \frac{1}{N}(H(W_1|Z^N) - H(W_1|Z^N,W_2,Y^N,X_2^N) + \delta(P_e))\\
\overset{(3)}{=}\ & \frac{1}{N}(H(W_1|Z^N) - H(W_1|Z^N,Y^N,X_2^N) + \delta(P_e))\\
=\ & \frac{1}{N}(I(W_1;Y^N,X_2^N|Z^N) + \delta(P_e))\\
\leq\ & \frac{1}{N}(H(Y^N,X_2^N|Z^N) - H(Y^N,X_2^N|Z^N,W_1,X_1^N) + \delta(P_e))\\
\overset{(4)}{=}\ & \frac{1}{N}(H(Y^N,X_2^N|Z^N) - H(Y^N,X_2^N|Z^N,X_1^N) + \delta(P_e))\\
=\ & \frac{1}{N}(I(Y^N,X_2^N;X_1^N|Z^N) + \delta(P_e))\\
\overset{(5)}{=}\ & \frac{1}{N}(H(X_1^N|Z^N) - H(X_1^N|Z^N,Y^N,X_2^N) - H(X_1^N) + H(X_1^N|X_2^N) + \delta(P_e))\\
=\ & \frac{1}{N}(I(X_1^N;Y^N|X_2^N) - I(X_1^N;Z^N) + \delta(P_e))
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{N}\sum_{i=1}^{N}(H(Y_i|Y^{i-1},X_2^N) - H(Y_i|X_{1,i},X_{2,i}) - H(Z_i|Z^{i-1}) + H(Z_i|Z^{i-1},X_1^N)) + \frac{\delta(P_e)}{N}\\
&\overset{(6)}{=} \frac{1}{N}\sum_{i=1}^{N}(H(Y_i|Y^{i-1},X_2^N,Z^{i-1}) - H(Y_i|X_{1,i},X_{2,i},Z^{i-1}) - H(Z_i|Z^{i-1}) + H(Z_i|Z^{i-1},X_1^N)) + \frac{\delta(P_e)}{N}\\
&\leq \frac{1}{N}\sum_{i=1}^{N}(H(Y_i|X_{2,i},Z^{i-1}) - H(Y_i|X_{1,i},X_{2,i},Z^{i-1}) - H(Z_i|Z^{i-1}) + H(Z_i|Z^{i-1},X_{1,i})) + \frac{\delta(P_e)}{N}\\
&\overset{(7)}{=} \frac{1}{N}\sum_{i=1}^{N}(H(Y_i|X_{2,i},Z^{i-1},J=i) - H(Y_i|X_{1,i},X_{2,i},Z^{i-1},J=i) - H(Z_i|Z^{i-1},J=i)\\
&\quad +H(Z_i|Z^{i-1},X_{1,i},J=i)) + \frac{\delta(P_e)}{N}\\
&\overset{(8)}{=} H(Y_J|X_{2,J},Z^{J-1},J) - H(Y_J|X_{1,J},X_{2,J},Z^{J-1},J) - H(Z_J|Z^{J-1},J) + H(Z_J|Z^{J-1},X_{1,J},J) + \frac{\delta(P_e)}{N}\\
&\overset{(9)}{=} I(X_1;Y|X_2,U) - I(X_1;Z|U) + \frac{\delta(P_e)}{N}, \qquad (1)
\end{aligned}
$$

where (1) is from the definition of the perfect secrecy; (2) is from Fano's inequality; (3) is from $H(W_2|X_2^N)=0$; (4) is from $H(W_1|X_1^N)=0$; (5) is from the Markov chain $X_1^N \rightarrow (X_2^N, Y^N) \rightarrow Z^N$ and the fact that X_1^N is independent of X_2^N; (6) is from the Markov chains $Y_i \rightarrow (Y^{i-1}, X_2^N) \rightarrow Z^{i-1}$ and $Y_i \rightarrow (X_{1,i}, X_{2,i}) \rightarrow Z^{i-1}$; (7) is from J is a random variable (uniformly distributed over $\{1,2,...,N\}$), and it is independent of X_1^N, X_2^N, Y^N and Z^N; (8) is from J is uniformly distributed over $\{1,2,...,N\}$; and (9) is from the definitions that $X_1 \triangleq X_{1,J}$, $X_2 \triangleq X_{2,J}$, $Y \triangleq Y_J$, $Z \triangleq Z_J$ and $U \triangleq (Z^{J-1}, J)$.

By using $P_e \leq \epsilon$, $\epsilon \rightarrow 0$ as $N \rightarrow \infty$, $\lim_{N\rightarrow\infty}\frac{H(W_1)}{N} = R_1$ and (1), it is easy to see that $R_1 \leq I(X_1;Y|X_2,U) - I(X_1;Z|U)$.

(Proof of $R_2 \leq I(X_2;Y|X_1,U) - I(X_2;Z|U)$**)**:

The proof is analogous to the proof of $R_1 \leq I(X_1;Y|X_2,U) - I(X_1;Z|U)$, and it is omitted here.

Proof of $R_1 + R_2 \leq I(X_1,X_2;Y|U) - I(X_1,X_2;Z|U)$:

$$
\begin{aligned}
&\lim_{N\rightarrow\infty}\Delta = \lim_{N\rightarrow\infty}\frac{1}{N}H(W_1,W_2|Z^N)\\
&\overset{(1)}{\leq} \lim_{N\rightarrow\infty}\frac{1}{N}(H(W_1,W_2|Z^N) + \delta(P_e) - H(W_1,W_2|Y^N,Z^N))\\
&\leq \lim_{N\rightarrow\infty}\frac{1}{N}(H(Y^N|Z^N) - H(Y^N|Z^N,W_1,W_2,X_1^N,X_2^N) + \delta(P_e))\\
&\overset{(2)}{=} \lim_{N\rightarrow\infty}\frac{1}{N}(H(Y^N|Z^N) - H(Y^N|Z^N,X_1^N,X_2^N) + \delta(P_e))\\
&= \lim_{N\rightarrow\infty}\frac{1}{N}(I(X_1^N,X_2^N;Y^N) - I(X_1^N,X_2^N;Z^N) + \delta(P_e))\\
&\overset{(3)}{=} \lim_{N\rightarrow\infty}(\frac{1}{N}\sum_{i=1}^{N}(H(Y_i|Y^{i-1}) - H(Y_i|X_{1,i},X_{2,i},Z^{i-1}) - H(Z_i|Z^{i-1}) + H(Z_i|X_{1,i},X_{2,i},Z^{i-1})) + \frac{\delta(P_e)}{N})\\
&\overset{(4)}{\leq} \lim_{N\rightarrow\infty}(\frac{1}{N}\sum_{i=1}^{N}(H(Y_i|Z^{i-1}) - H(Y_i|X_{1,i},X_{2,i},Z^{i-1}) - H(Z_i|Z^{i-1}) + H(Z_i|X_{1,i},X_{2,i},Z^{i-1})) + \frac{\delta(P_e)}{N})
\end{aligned}
$$

$$
\begin{aligned}
&\overset{(5)}{=} \lim_{N\to\infty}\Big(\frac{1}{N}\sum_{i=1}^{N}(H(Y_i|Z^{i-1},J=i)-H(Y_i|X_{1,i},X_{2,i},Z^{i-1},J=i)\\
&\quad -H(Z_i|Z^{i-1},J=i)+H(Z_i|X_{1,i},X_{2,i},Z^{i-1},J=i))+\frac{\delta(P_e)}{N}\Big)\\
&\overset{(6)}{=} \lim_{N\to\infty}(H(Y_J|Z^{J-1},J)-H(Y_J|X_{1,J},X_{2,J},Z^{J-1},J)\\
&\quad -H(Z_J|Z^{J-1},J)+H(Z_J|X_{1,J},X_{2,J},Z^{J-1},J)+\frac{\delta(P_e)}{N})\\
&\overset{(7)}{=} I(X_1,X_2;Y|U)-I(X_1,X_2;Z|U), \qquad (2)
\end{aligned}
$$

where (1) is from Fano's inequality; (2) is from $(W_1, W_2) \rightarrow (X_1^N, X_2^N, Z^N) \rightarrow Y^N$; (3) is from $Y_i \rightarrow (X_{1,i}, X_{2,i}) \rightarrow Z^{i-1}$ and $Z_i \rightarrow (X_{1,i}, X_{2,i}) \rightarrow Z^{i-1}$; (4) is from $Y_i \rightarrow Y^{i-1} \rightarrow Z^{i-1}$; (5) is from J is a random variable (uniformly distributed over $\{1, 2, ..., N\}$), and it is independent of X_1^N, X_2^N, Y^N and Z^N; (6) is from J is uniformly distributed over $\{1, 2, ..., N\}$; and (7) is from the definitions that $X_1 \triangleq X_{1,J}$, $X_2 \triangleq X_{2,J}$, $Y \triangleq Y_J$, $Z \triangleq Z_J$ and $U \triangleq (Z^{J-1}, J)$ and the fact that $P_e \rightarrow 0$ as $N \rightarrow \infty$.

By using $\lim_{N\to\infty}\Delta \geq R_1 + R_2$ and (2), it is easy to see that $R_1 + R_2 \leq I(X_1, X_2; Y|U) - I(X_1, X_2; Z|U)$.

The converse proof of Theorem 1 is completed.

Acknowledgment

This work was supported by a sub-project of the National Basic Research Program of China under Grant 2012CB316100 on Broadband Mobile Communications at High Speeds and the National Natural Science Foundation of China under Grant 61301121.

Author Contributions

Bin Dai and Zheng Ma did the theoretical work and wrote this paper. All authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387.
2. Csiszár, I.; Körner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348.
3. Körner, J.; Marton, K. General broadcast channels with degraded message sets. *IEEE Trans Inf. Theory* **1977**, *23*, 60–64.
4. Leung-Yan-Cheong, S.K.; Hellman, M.E. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **1978**, *24*, 451–456.
5. Mitrpant, C.; Han Vinck, A.J.; Luo, Y. An achievable region for the Gaussian wiretap channel with side information. *IEEE Trans. Inf. Theory* **2006**, *52*, 2181–2190.

6. Chen, Y.; Han Vinck, A.J. Wiretap channel with side information. *IEEE Trans. Inf. Theory* **2008**, *54*, 395–402.
7. Dai, B.; Luo, Y. Some new results on wiretap channel with side information. *Entropy* **2012**, *14*, 1671–1702.
8. Ahlswede, R.; Cai, N. Transmission, identification and common randomness capacities for wire-tap channels with secure feedback from the decoder. In *General Theory of Information Transfer and Combinatorics*; Springer-Verlag: Berlin/Heidelberg, Germany, 2006; pp. 258–275.
9. Lai, L.; el Gamal, H.; Poor, V. The wiretap channel with feedback: Encryption over the channel. *IEEE Trans. Inf. Theory* **2008**, *54*, 5059–5067.
10. Ardestanizadeh, E.; Franceschetti, M.; Javidi, T.; Kim, Y. Wiretap channel with secure rate-limited feedback. *IEEE Trans. Inf. Theory* **2009**, *55*, 5353–5361.
11. Merhav, N. Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels. *IEEE Trans. Inf. Theory Special Issue Inf.-Secur.* **2008**, *54*, 2723–2734.
12. Xu, P.; Ding, Z.; Dai, X. A general framework of wiretap channel with helping interference and state information. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 182–195.
13. Lai, L.; el Gamal, H. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inf. Theory* **2008**, *54*, 4005–4019.
14. Xu, P.; Ding, Z.; Dai, X. A Hybrid cooperative coding scheme for the relay-ravesdropper rhannel. *Entropy* **2014**, *16*, 1819–1841.
15. Oohama, Y. Relay channels with confidential messages. **2007**, arXiv:cs/0611125 [cs.IT].
16. Liu, R.; Maric, I.; Spasojevic, P.; Yates, R. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Inf. Theory* **2008**, *54*, 2493–2507.
17. Liang, Y.; Somekh-Baruch, A.; Poor, H.V.; Shamai, S.; Verdu, S. Capacity of cognitive interference channels with and without secrecy. *IEEE Trans. Inf. Theory* **2009**, *55*, 604–619.
18. Liang, Y.; Poor, H. Multiple-access channels with confidential messages. *IEEE Trans. Inf. Theory* **2008**, *54*, 976–1002.
19. Tekin, E.; Yener, A. The Gaussian multiple access wire-tap channel. *IEEE Trans. Inf. Theory* **2008**, *54*, 5747–5755.
20. Ekrem, E.; Ulukus, S. On the secrecy of multiple access wiretap channel. In Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing, Urbana-Champaign, IL, USA, 23–26 September 2008.
21. Tekin, E.; Yener, A. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory* **2008**, *54*, 2735–2751.
22. Awan, Z. H.; Zaidi, A.; Vandendorpe, L. Multiaccess channel with partially cooperating encoders and security constraints. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1243–1254.
23. Awan, Z.H.; Zaidi, A.; Vandendorpe, L. On multiaccess channel with unidirectional cooperation and security constraints. In Proceedings of the 50th Annual Allerton Conference on Communication, Control, and Computing, Urbana-Champaign, IL, USA, 1–5 October 2012.

24. Xu, P.; Ding, Z.; Dai, X. Rate regions for multiple access channel with conference and secrecy constraints. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1961–1974.
25. He, X.; Khisti, A.; Yener, A. MIMO multiple access channel with an arbitrarily varying eavesdropper: Secrecy degrees of freedom. *IEEE Trans. Inf. Theory* **2013**, *59*, 4733–4745.
26. Zaidi, A.; Awan, Z.H.; Shamai, S.; Vandendorpe, L. Secure degrees of freedom of MIMO X-channels with output feedback and delayed CSI. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1760–1774.
27. Zaidi, A.; Awan, Z. H.; Shamai, S.; Vandendorpe, L. Secure degrees of freedom of X-channel with output feedback and delayed CSIT. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1760–1774.