# Multiple Access Wiretap Channel with Noiseless Feedback

Bin Dai and Zheng Ma

## Abstract

The physical layer security in the up-link of the wireless communication systems is often modeled as the multiple access wiretap channel (MAC-WT), and recently it has received a lot attention. In this paper, the MAC-WT has been re-visited by considering the situation that the legitimate receiver feeds his received channel output back to the transmitters via two noiseless channels, respectively. This model is called the MAC-WT with noiseless feedback. Inner and outer bounds on the secrecy capacity region of this feedback model are provided. To be specific, we first present a decode-and-forward (DF) inner bound on the secrecy capacity region of this feedback model, and this bound is constructed by allowing each transmitter to decode the other one's transmitted message from the feedback, and then each transmitter uses the decoded message to re-encode his own messages, i.e., this DF inner bound allows the independent transmitters to co-operate with each other. Then, we provide a hybrid inner bound which is strictly larger than the DF inner bound, and it is constructed by using the feedback as a tool not only to allow the independent transmitters to co-operate with each other, but also to generate two secret keys respectively shared between the legitimate receiver and the two transmitters. Finally, we give a sato-type outer bound on the secrecy capacity region of this feedback model. The results of this paper are further explained via a Gaussian example.

## Index Terms

Multiple-access wiretap channel, noiseless feedback, secrecy capacity region.

## I. INTRODUCTION

The physical layer security (PLS) was first investigated by Wyner in his landmark paper on the degraded wiretap channel [1]. Wyner's degraded wiretap channel model consists of one transmitter and two receivers (a legitimate receiver and an eavesdropper). The transmitter sends a private message to the legitimate receiver via a discrete memoryless main channel, and an eavesdropper eavesdrops the output of the main channel via another discrete memoryless wiretap channel. We say that the perfect secrecy is achieved if no information about the private

B. Dai is with the School of Information Science and Technology, Southwest JiaoTong University, Chengdu 610031, China, and with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi′an, Shaanxi 710071, China, e-mail: daibin@home.swjtu.edu.cn.

Z. Ma is with the School of Information Science and Technology, Southwest JiaoTong University, Chengdu 610031, China, e-mail: zma@home.swjtu.edu.cn.

message is leaked to the eavesdropper. The secrecy capacity $C_s$, which is the maximum reliable transmission rate with perfect secrecy constraint, was characterized by Wyner [1], and it is given by

$$C_s = \max_{p(x)} (I(X;Y) - I(X;Z)), \tag{1.1}$$

where $X$, $Y$ and $Z$ are the input of the main channel, output of the main channel and output of the wiretap channel, respectively, and they satisfy the Markov chain $X \to Y \to Z$. Here note that (1.1) holds under the degradedness assumption $X \to Y \to Z$, and the secrecy capacity of the general wiretap channel (the wiretap channel without the degradedness assumption) was determined by Csiszár and Körner [2]. The work of [1] and [2] lays a foundation for the PLS of the practical communication systems.

Since Wozencraft et al. [3] showed that the time-variant noisy two-way channels can be used to provide noiseless feedback, whether this noiseless feedback helps to enhance the capacities of various communication channels motivates the researchers to study the channels with noiseless feedback. Shannon first proved that the noiseless feedback does not increase the capacity of a point-to-point discrete memoryless channel (DMC) [4]. After that, Cover et al. [5], [6] and Bross et al. [7] showed that the capacity regions of several multi-user channels, such as multiple-access channel (MAC) and relay channel, can be enhanced by feeding back the receiver's channel output to the transmitter over a noiseless channel. Then, it is natural to ask: does the noiseless feedback from the legitimate receiver to the transmitter also help to enhance the secrecy capacity of the wiretap channel? Ahlswede and Cai [8] answered this question by considering the wiretap channel with noiseless feedback. Since the noiseless feedback is known by the legitimate receiver and the transmitter, and it is not available for the eavesdropper, Ahlswede and Cai pointed out that the noiseless feedback can be used to generate a secret key shared only between the transmitter and the legitimate receiver, and we can use this key to encrypt the transmitted messages. Combining the idea of generating a secret key from the noiseless feedback with Wyner's random binning technique used in the achievability proof of (1.1), Ahlswede and Cai showed that the secrecy capacity $C_{sf}$ of the degraded wiretap channel with noiseless feedback is given by

$$C_{sf} = \max_{p(x)} \min\{I(X;Y), I(X;Y) - I(X;Z) + H(Y|X,Z)\}, \tag{1.2}$$

where $X$, $Y$ and $Z$ are defined the same as those in (1.1), and $X \to Y \to Z$ forms a Markov chain. Comparing (1.2) with (1.1), it is easy to see that the noiseless feedback increases the secrecy capacity of the degraded wiretap channel. Other related works on the wiretap channel with noiseless feedback are in [9]-[11].

In recent years, the PLS in the up-link of wireless communication system receives a lot attention, see [12]-[16]. These work extends Wyner's wiretap channel to a multiple access situation: the multiple-access wiretap channel (MAC-WT). Bounds on the secrecy capacity region of MAC-WT are provided in [12]-[16]. In order to investigate whether the noiseless feedback from the legitimate receiver to the transmitters helps to enhance the secrecy capacity region of the MAC-WT, in this paper, we study the MAC-WT with noiseless feedback, see Figure 1. We first present a DF inner bound on the secrecy capacity region of the model of Figure 1, and this bound is constructed by using the DF strategy of the MAC-WT with noisy feedback [17], where each transmitter of the MAC decodes the other

one's transmitted message from the noisy feedback and then uses it to re-encode his own messages. Second, note that the noiseless feedback can not only be used to re-encode the messages of the transmitters, but also be used to generate secret keys to encrypt the transmitted messages, thus we present a hybrid inner bound on the secrecy capacity region of the model of Figure 1 by combining Ahlswede and Cai's idea of generating a secret key from the noiseless feedback [8] with the DF strategy used in [17], and we show that this hybrid inner bound is strictly larger than the DF inner bound. Third, we present a sato-type outer bound on the secrecy capacity region of the model of Figure 1. Finally, the results of this paper are further explained via a Gaussian example.

The rest of this paper is organized as follows. In Section II, we show the definitions, notations and the main results of the model of Figure 1. An Gaussian example of the model of Figure 1 is provided in Section III. Final conclusions are presented in Section IV.



Fig. 1: The multiple-access wiretap channel with noiseless feedback

## II. MODEL DESCRIPTION AND THE MAIN RESULT

*Basic notations:* We use the notation $p_V(v)$ to denote the probability mass function $Pr\{V = v\}$, where $V$ (capital letter) denotes the random variable, $v$ (lower case letter) denotes the real value of the random variable $V$. Denote the alphabet in which the random variable $V$ takes values by $\mathcal{V}$ (calligraphic letter). Similarly, let $U^N$ be a random vector $(U_1, ..., U_N)$, and $u^N$ be a vector value $(u_1, ..., u_N)$. In the rest of this paper, the log function is taken to the base 2.

*Definitions of the model of Figure 1:*

Let $W_1$, uniformly distributed over the finite alphabet $\mathcal{W}_1 = \{1, 2, ..., M_1\}$, be the message sent by the transmitter 1. Similarly, let $W_2$, uniformly distributed over the finite alphabet $\mathcal{W}_2 = \{1, 2, ..., M_2\}$, be the message sent by the transmitter 2.

The inputs of the channel are $x_1^N$ and $x_2^N$, while the outputs are $y^N$ and $z^N$. The channel is discrete memoryless, i.e., at the $i$-th time, the channel outputs $Y_i$ and $Z_i$ depend only on $X_{1,i}$ and $X_{2,i}$, and thus we have

$$P_{Y^N, Z^N | X_1^N, X_2^N}(y^N, z^N | x_1^N, x_2^N)$$
$$= \prod_{i=1}^{N} P_{Y,Z|X_1,X_2}(y_i, z_i | x_{1,i}, x_{2,i}). \tag{2.1}$$

Since $y^N$ can be fed back to the transmitters via a noiseless feedback channel, at the $i$-th time, the channel input $X_{j,i}$ $(j = 1, 2)$ is given by

$$X_{j,i} = \begin{cases} f_{j,i}(W_j), & i = 1 \\ f_{j,i}(W_j, Y^{i-1}), & 2 \le i \le N. \end{cases} \quad (2.2)$$

Here note that the $i$-th time channel encoder $f_{j,i}$ $(j = 1, 2)$ is a stochastic encoder, and the transmission rates of the messages $W_1$ and $W_2$ are $\frac{\log M_1}{N}$ and $\frac{\log M_2}{N}$, respectively.

The decoder is a mapping $\psi: \mathcal{Y}^N \to \mathcal{W}_1 \times \mathcal{W}_2$, with input $Y^N$ and outputs $\hat{W}_1$, $\hat{W}_2$. The average probability of error $P_e$ is denoted by

$$P_e = \frac{1}{M_1 M_2} \sum_{i=1}^{M_1} \sum_{j=1}^{M_2} Pr\{\psi(y^N) \ne (i, j) | (i, j) \text{ sent}\}. \quad (2.3)$$

The eavesdropper's equivocation to the messages $W_1$ and $W_2$ is defined as

$$\Delta = \frac{1}{N} H(W_1, W_2 | Z^N). \quad (2.4)$$

A positive rate pair $(R_1, R_2)$ is called achievable with weak secrecy if, for any small positive $\epsilon$, there exists an $(M_1, M_2, N, P_e)$ code such that

$$\frac{\log M_1}{N} \ge R_1 - \epsilon, \frac{\log M_2}{N} \ge R_2 - \epsilon, \Delta \ge R_1 + R_2 - \epsilon, \quad P_e \le \epsilon. \quad (2.5)$$

Here we note that $\Delta \ge R_1 + R_2 - \epsilon$ also ensures $\frac{1}{N} H(W_t | Z^N) \ge R_t - \epsilon$ for $t = 1, 2$, and the proof is in [17, p. 609]. The secrecy capacity region $\mathcal{C}_s$ of the model of Figure 1 is a set composed of all rate pairs $(R_1, R_2)$ satisfying (2.5). The following Theorem 1 and Theorem 2 show two inner bounds on $\mathcal{C}_s$, and Theorem 3 shows an outer bound on $\mathcal{C}_s$.

*Theorem 1:* For the discrete memoryless MAC-WT with noiseless feedback, an inner bound $\mathcal{C}_s^{DF}$ on the secrecy capacity region $\mathcal{C}_s$ is given by

$$\mathcal{C}_s^{DF} = \{(R_1 \ge 0, R_2 \ge 0) : R_1 \le I(X_1; Y | X_2, U)$$

$$R_2 \le I(X_2; Y | X_1, U)$$

$$R_1 + R_2 \le \min\{I(X_1, X_2; Y), I(X_1; Y | X_2, U) + I(X_2; Y | X_1, U)\} - I(X_1, X_2; Z)\},$$

for some distribution

$$P_{Z,Y|X_1,X_2}(z, y | x_1, x_2) \cdot P_{X_1|U}(x_1 | u) \cdot P_{X_2|U}(x_2 | u) \cdot P_U(u). \quad (2.6)$$

*Proof:*

In the MAC-WT with noisy feedback [17], the legitimate receiver's channel output $Y$ is sent to the transmitters via two noisy feedback channels, and the outputs of the noisy feedback channel are $Y_1$ and $Y_2$. Substituting $Y_1 = Y_2 = Y$ (which implies the feedback channel is noiseless) into [17, Theorem 2], the DF inner bound $\mathcal{C}_s^{DF}$ for the model of Figure 1 is obtained, and the proof of $\mathcal{C}_s^{DF}$ is along the lines of that of [17, Theorem 2] (the full DF inner bound on the secrecy capacity region of the MAC-WT with noisy feedback), and thus we omit the proof here. ∎

*Remark 1:* In [17, Theorem 1], Tang et al. also provide a partial DF inner bound on the secrecy capacity region of the MAC-WT with noisy feedback. Substituting $Y_1 = Y_2 = Y$ into [17, Theorem 1], and using Fourier-Motzkin elimination (see, e.g., [18]) to eliminate $R_{10}$, $R_{12}$, $R_{20}$ and $R_{21}$, it is not difficult to show that the partial DF inner bound $\mathcal{C}_s^{PDF}$ of the model of Figure 1 is exactly the same as the DF inner bound $\mathcal{C}_s^{DF}$ shown in Theorem 1.

*Theorem 2:* For the discrete memoryless MAC-WT with noiseless feedback, an inner bound $\mathcal{C}_s^{in}$ on the secrecy capacity region $\mathcal{C}_s$ is given by

$$\mathcal{C}_s^{in} = \{(R_1 \geq 0, R_2 \geq 0) : R_1 \leq I(X_1; Y|X_2, U)$$

$$R_2 \leq I(X_2; Y|X_1, U)$$

$$R_1 + R_2 \leq \min\{I(X_1, X_2; Y), I(X_1; Y|X_2, U)$$

$$+I(X_2; Y|X_1, U)\} - I(X_1, X_2; Z)$$

$$+\min\{I(X_1, X_2; Z), H(Y|Z, X_1, X_2)\}\},$$

for some distribution satisfying (2.7).

*Proof:*

The hybrid inner bound $\mathcal{C}_s^{in}$ is constructed by combining Ahlswede and Cai's idea of generating a secret key from the noiseless feedback [8] with the DF strategy used in [17, Theorem 2], and it is achieved by the following key steps:

- For the transmitter 1, split the transmitted message $W_1$ into $W_{1,0}$ and $W_{1,1}$, and let $W_1^*$ be a dummy message randomly generated by the transmitter 1, and it is used to confuse the eavesdropper. Analogously, for the transmitter 2, split the transmitted message $W_2$ into $W_{2,0}$ and $W_{2,1}$, and let $W_2^*$ be a dummy message randomly generated by the transmitter 2, and it is used to confuse the eavesdropper.

- The messages $W_1$ and $W_2$ are transmitted through $n$ blocks, and in block $i$ ($2 \leq i \leq n$), when each transmitter receives the noiseless feedback, he tries to decode the other transmitter's message (including the transmitted message and the dummy message) and uses it to re-encode his own message. In addition, the noiseless feedback is used to generate a pair of secret keys $(K_1^*, K_2^*)$, and $K_j^*$ ($j = 1, 2$) is used to encrypt the sub-message $W_{j,1}$.

- Comparing the above code construction of $\mathcal{C}_s^{in}$ with that of $\mathcal{C}_s^{DF}$, the encoding and decoding schemes of these two bounds are almost the same, except that the sub-message $W_{j,1}$ ($j = 1, 2$) is encrypted by a secret key $K_j^*$. Thus the secrecy sum rate $R_1 + R_2$ is bounded by two part: the first part is the upper bound on the sum rate of $\mathcal{C}_s^{DF}$, and the second part is the upper bound on the rate of the secret keys $K_1^*$ and $K_2^*$. Using the balanced coloring lemma introduced by Ahlswede and Cai [8], we conclude that the rate of the secret keys $K_1^*$ and $K_2^*$ is bounded by $\min\{H(Y|X_1, X_2, Z), I(X_1, X_2; Z)\}$. Thus, the hybrid inner bound $\mathcal{C}_s^{in}$ is obtained.

The details of the proof are in Appendix A. ■

*Remark 2:* Comparing the DF inner bound $\mathcal{C}_s^{DF}$ and the partial DF inner bound $\mathcal{C}_s^{PDF}$ with our hybrid new inner bound $\mathcal{C}_s^{in}$, it is easy to see that our new inner bound $\mathcal{C}_s^{in}$ is strictly larger than $\mathcal{C}_s^{DF}$ and $\mathcal{C}_s^{PDF}$.

*Theorem 3:* For the discrete memoryless MAC-WT with noiseless feedback, an outer bound $\mathcal{C}_s^{out}$ on the secrecy capacity region $\mathcal{C}_s$ is given by

$$\mathcal{C}_s^{out} = \{(R_1 \geq 0, R_2 \geq 0) : R_1 + R_2 \leq H(Y|Z)\},$$

for some distribution

$$P_{Z,Y|X_1,X_2}(z,y|x_1,x_2) \cdot P_{X_1 X_2}(x_1,x_2). \tag{2.7}$$

*Proof:* The outer bound $\mathcal{C}_s^{out}$ is a simple sato-type outer bound, and the proof is in Appendix B. ∎

## III. GAUSSIAN EXAMPLE

*A. Capacity Results on the Gaussian MAC-WT with Noiseless Feedback*

For the Gaussian case of the model of Figure 1, the channel inputs and outputs satisfy

$$Y = X_1 + X_2 + N_1 \quad Z = X_1 + X_2 + N_2, \tag{3.1}$$

where the channel noises $N_1$ and $N_2$ are independent and Gaussian distributed, i.e., $N_1 \sim \mathcal{N}(0,\sigma_1^2)$, and $N_2 \sim \mathcal{N}(0,\sigma_2^2)$. The average power constraint of the transmitted signal $X_j$ $(j = 1,2)$ is given by

$$\frac{1}{N}\sum_{i=1}^{N} E[X_{ji}^2] \leq P_j, \; j = 1,2. \tag{3.2}$$

***The DF and partial DF inner bounds on the secrecy capacity region for the Gaussian case of the model of Figure 1:***

*Theorem 4:* The DF inner bound $C_s^{gdf}$ and the partial DF inner bound $C_s^{gpdf}$ for the Gaussian case of the model of Figure 1 are given by

$$C_s^{gdf} = C_s^{gpdf} = \{(R_1 \geq 0, R_2 \geq 0) : R_1 \leq \frac{1}{2}\log(1 + \frac{P_1}{\sigma_1^2}),$$

$$R_2 \leq \frac{1}{2}\log(1 + \frac{P_2}{\sigma_1^2}),$$

$$R_1 + R_2 \leq \frac{1}{2}\log(1 + \frac{P_1 + P_2}{\sigma_1^2}) - \frac{1}{2}\log(1 + \frac{P_1 + P_2}{\sigma_2^2})\}. \tag{3.3}$$

*Proof:* In Remark 1, we have shown that for the model of Figure 1, the DF inner bound is the same as the partial DF inner bound. Along the lines of [17, pp. 610-611], we have

$$C_s^{gdf} = C_s^{gpdf} = \{(R_1 \geq 0, R_2 \geq 0) : R_1 \leq \frac{1}{2}\log(1 + \frac{P_1}{\sigma_1^2}),$$

$$R_2 \leq \frac{1}{2}\log(1 + \frac{P_2}{\sigma_1^2}),$$

$$R_1 + R_2 \leq \min\{\frac{1}{2}\log(1 + \frac{P_1 + P_2}{\sigma_1^2}), \frac{1}{2}\log(1 + \frac{P_1}{\sigma_1^2}) + \frac{1}{2}\log(1 + \frac{P_2}{\sigma_1^2})\}$$

$$-\frac{1}{2}\log(1 + \frac{P_1 + P_2}{\sigma_2^2})\}. \tag{3.4}$$

Note that in (3.4), $\frac{1}{2}\log(1 + \frac{P_1 + P_2}{\sigma_1^2}) \leq \frac{1}{2}\log(1 + \frac{P_1}{\sigma_1^2}) + \frac{1}{2}\log(1 + \frac{P_2}{\sigma_1^2})$, and thus (3.3) is obtained. The proof is completed. ∎

*The hybrid inner bound on the secrecy capacity region for the Gaussian case of the model of Figure 1:*

*Theorem 5:* The hybrid inner bound $C_s^{gi}$ for the Gaussian case of the model of Figure 1 is given by

$$C_s^{gi} = \{(R_1 \geq 0, R_2 \geq 0) : R_1 \leq \frac{1}{2}\log(1 + \frac{P_1}{\sigma_1^2}),$$

$$R_2 \leq \frac{1}{2}\log(1 + \frac{P_2}{\sigma_1^2}),$$

$$R_1 + R_2 \leq \frac{1}{2}\log(1 + \frac{P_1 + P_2}{\sigma_1^2}) - \frac{1}{2}\log(1 + \frac{P_1 + P_2}{\sigma_2^2})$$

$$+ \min\{\frac{1}{2}\log(2\pi e\sigma_1^2), \frac{1}{2}\log(1 + \frac{P_1 + P_2}{\sigma_2^2})\}\}. \tag{3.5}$$

*Proof:* Similar to the corresponding proof in [17, pp. 610-611], substituting $X_1 = \sqrt{(1-\alpha)P_1}U + \sqrt{\alpha P_1}U_1$ ($0 \leq \alpha \leq 1$) and $X_2 = \sqrt{(1-\beta)P_2}U + \sqrt{\beta P_2}U_2$ ($0 \leq \beta \leq 1$) into (3.1), and using the fact that $U$, $U_1$ and $U_2$ are independent and Gaussian distributed with zero mean and unit variance, and $\frac{1}{2}\log(1 + \frac{P_1+P_2}{\sigma_1^2}) \leq \frac{1}{2}\log(1 + \frac{P_1}{\sigma_1^2}) + \frac{1}{2}\log(1 + \frac{P_2}{\sigma_1^2})$, (3.5) is directly obtained. Here note that (3.5) is achieved when $\alpha = 1$ and $\beta = 1$. The proof is completed. ∎

*The outer bound on the secrecy capacity region for the Gaussian case of the model of Figure 1:*

*Theorem 6:* For the case that $\sigma_1^2 \geq \sigma_2^2$, the outer bound $C_s^{go}$ for the Gaussian case of the model of Figure 1 is given by

$$C_s^{go} = \{(R_1 \geq 0, R_2 \geq 0) : R_1 + R_2 \leq \frac{1}{2}\log(2\pi e(\sigma_1^2 - \sigma_2^2))\}. \tag{3.6}$$

For the case that $\sigma_1^2 \leq \sigma_2^2$, the outer bound $C_s^{go}$ is given by

$$C_s^{go} = \{(R_1 \geq 0, R_2 \geq 0) : R_1 + R_2 \leq \frac{1}{2}\log(2\pi e(\sigma_2^2 - \sigma_1^2)) + \frac{1}{2}\log\frac{P_1 + P_2 + \sigma_1^2}{P_1 + P_2 + \sigma_2^2}\}. \tag{3.7}$$

*Proof:*

- For the case that $\sigma_1^2 \geq \sigma_2^2$, (3.1) can be re-written as

$$Y = X_1 + X_2 + N_2 + N_1 - N_2 \quad Z = X_1 + X_2 + N_2. \tag{3.8}$$

Substituting (3.8) into Theorem 3, we have

$$R_1 + R_2 \leq h(Y|Z) = h(X_1 + X_2 + N_2 + N_1 - N_2|X_1 + X_2 + N_2)$$

$$= h(N_1 - N_2|X_1 + X_2 + N_2) \leq h(N_1 - N_2) = \frac{1}{2}\log(2\pi e(\sigma_1^2 - \sigma_2^2)). \tag{3.9}$$

- For the case that $\sigma_1^2 \leq \sigma_2^2$, (3.1) can be re-written as

$$Y = X_1 + X_2 + N_1 \quad Z = X_1 + X_2 + N_1 + N_2 - N_1. \tag{3.10}$$

Substituting (3.10) into Theorem 3, we have

$$R_1 + R_2 \leq h(Y|Z) = h(Y, Z) - h(Z) = h(Z|Y) + h(Y) - h(Z)$$

$$= h(X_1 + X_2 + N_1 + N_2 - N_1 | X_1 + X_2 + N_1) + h(Y) - h(Y + N_2 - N_1)$$

$$= h(N_2 - N_1 | X_1 + X_2 + N_1) + h(Y) - h(Y + N_2 - N_1)$$

$$\leq h(N_2 - N_1) + h(Y) - h(Y + N_2 - N_1)$$

$$\overset{(a)}{\leq} h(N_2 - N_1) + h(Y) - \frac{1}{2} \log(2^{2h(Y)} + 2^{2h(N_2 - N_1)})$$

$$\overset{(b)}{\leq} h(N_2 - N_1) + \frac{1}{2} \log(2\pi e(P_1 + P_2 + \sigma_1^2)) - \frac{1}{2} \log(2\pi e(P_1 + P_2 + \sigma_1^2) + 2\pi e(\sigma_2^2 - \sigma_1^2))$$

$$= \frac{1}{2} \log(2\pi e(\sigma_2^2 - \sigma_1^2)) + \frac{1}{2} \log(2\pi e(P_1 + P_2 + \sigma_1^2)) - \frac{1}{2} \log(2\pi e(P_1 + P_2 + \sigma_1^2) + 2\pi e(\sigma_2^2 - \sigma_1^2))$$

$$= \frac{1}{2} \log(2\pi e(\sigma_2^2 - \sigma_1^2)) + \frac{1}{2} \log \frac{P_1 + P_2 + \sigma_1^2}{P_1 + P_2 + \sigma_2^2}, \tag{3.11}$$

where (a) is from the entropy power inequality, i.e., $2^{2h(Y+N_2-N_1)} \geq 2^{2h(Y)} + 2^{2h(N_2-N_1)}$, and (b) is from the fact that $h(Y) - \frac{1}{2} \log(2^{2h(Y)} + 2^{2h(N_2-N_1)})$ is increasing while $h(Y)$ is increasing, $h(Y) = h(X_1 + X_2 + N_1) \leq \frac{1}{2} \log(2\pi e(P_1 + P_2 + \sigma_1^2))$ and $h(N_2 - N_1) = \frac{1}{2} \log(2\pi e(\sigma_2^2 - \sigma_1^2))$.

The proof is completed. ∎

Finally, recall that Tekin and Yener [12] have shown that for the Gaussian MAC-WT without feedback, an inner bound $C_s^{gmac-wt}$ is given by

$$C_s^{gmac-wt} = \{(R_1 \geq 0, R_2 \geq 0) : R_1 \leq \frac{1}{2} \log(1 + \frac{P_1}{\sigma_1^2}) - \frac{1}{2} \log(1 + \frac{P_1}{\sigma_2^2 + P_2}),$$

$$R_2 \leq \frac{1}{2} \log(1 + \frac{P_2}{\sigma_1^2}) - \frac{1}{2} \log(1 + \frac{P_2}{\sigma_2^2 + P_1}),$$

$$R_1 + R_2 \leq \frac{1}{2} \log(1 + \frac{P_1 + P_2}{\sigma_1^2}) - \frac{1}{2} \log(1 + \frac{P_1 + P_2}{\sigma_2^2})\}. \tag{3.12}$$

For the case that $\sigma_1^2 \leq \sigma_2^2$, the following Figure 2 shows the inner bound $C_s^{gi}$, the partial ($C_s^{gpdf}$) and full ($C_s^{gdf}$) DF inner bounds for the Gaussian case of Figure 1, the outer bound $C_s^{go}$ and Tekin-Yener's inner bound $C_s^{gmac-wt}$ of the Gaussian MAC-WT [12] for $P_1 = P_2 = 1$, $\sigma_1^2 = 1$ and $\sigma_2^2 = 10$. From Figure 2, it is easy to see that our new inner bound $C_s^{gi}$ is larger than the DF inner bounds $C_s^{gpdf}$ and $C_s^{gdf}$, and the noiseless feedback helps to enhance the secrecy rate region $C_s^{gmac-wt}$ of the Gaussian MAC-WT.

For the case that $\sigma_1^2 \geq \sigma_2^2$, the DF bounds $C_s^{gpdf}$, $C_s^{gdf}$ and Tekin-Yener's inner bound $C_s^{gmac-wt}$ reduce to the point ($R_1 = 0, R_2 = 0$). The following Figure 3 shows the inner bound $C_s^{gi}$ and the outer bound $C_s^{go}$ for $P_1 = P_2 = 10$, $\sigma_1^2 = 5$, $\sigma_2^2 = 2$. It is easy to see that when $\sigma_1^2 \geq \sigma_2^2$, our hybrid inner bound still provides positive secrecy rates, while there is no positive secrecy rate in the partial and full DF inner bounds.

### B. Power Control for the Maximum Secrecy Sum Rate of $C_s^{gi}$

In this subsection, we assume that the average power constraints of the transmitters satisfy

$$0 \leq P_1, P_2 \leq P, \tag{3.13}$$

Fig. 2: The bounds $C_s^{gi}$, $C_s^{gpdf}$, $C_s^{gdf}$, $C_s^{go}$, and $C_s^{gmac-wt}$ for $P_1 = P_2 = 1$, $\sigma_1^2 = 1$, $\sigma_2^2 = 10$

and define the maximum secrecy sum rate $R_{sum}^*$ of $C_s^{gi}$ as

$$R_{sum}^* = \max_{P_1, P_2} \frac{1}{2} \log(1 + \frac{P_1 + P_2}{\sigma_1^2}) - \frac{1}{2} \log(1 + \frac{P_1 + P_2}{\sigma_2^2})$$
$$+ \min\{\frac{1}{2} \log(2\pi e \sigma_1^2), \frac{1}{2} \log(1 + \frac{P_1 + P_2}{\sigma_2^2})\}. \tag{3.14}$$

In the remainder of this subsection, we calculate the maximum secrecy sum rate $R_{sum}^*$ of $C_s^{gi}$, and show the optimum power control (the optimum of $P_1$ and $P_2$ is denoted by $P_1^*$ and $P_2^*$, respectively) for $R_{sum}^*$.

*Theorem 7:* If $\sigma_1^2 > \sigma_2^2$, the maximum secrecy sum rate $R_{sum}^*$ of $C_s^{gi}$ is given by

$$R_{sum}^* = \begin{cases} \frac{1}{2} \log(1 + \frac{2P}{\sigma_1^2}), & 0 \le P \le \frac{(2\pi e \sigma_1^2 - 1)\sigma_2^2}{2} \\ \frac{1}{2} \log(1 + \frac{(2\pi e \sigma_1^2 - 1)\sigma_2^2}{\sigma_1^2}), & P \ge \frac{(2\pi e \sigma_1^2 - 1)\sigma_2^2}{2}, \end{cases} \tag{3.15}$$

and the optimum power control is given by

$$(P_1^*, P_2^*) = \begin{cases} (P, P), & 0 \le P \le \frac{(2\pi e \sigma_1^2 - 1)\sigma_2^2}{2} \\ (\frac{(2\pi e \sigma_1^2 - 1)\sigma_2^2}{2}, \frac{(2\pi e \sigma_1^2 - 1)\sigma_2^2}{2}), & P \ge \frac{(2\pi e \sigma_1^2 - 1)\sigma_2^2}{2}. \end{cases} \tag{3.16}$$

If $\sigma_1^2 \le \sigma_2^2$, the maximum secrecy sum rate $R_{sum}^*$ of $C_s^{gi}$ is given by

$$R_{sum}^* = \begin{cases} \frac{1}{2} \log(1 + \frac{2P}{\sigma_1^2}), & 0 \le P \le \frac{(2\pi e \sigma_1^2 - 1)\sigma_2^2}{2} \\ \frac{1}{2} \log(2\pi e \sigma_1^2) + \frac{1}{2} \log(1 + \frac{2P}{\sigma_1^2}) - \frac{1}{2} \log(1 + \frac{2P}{\sigma_2^2}), & P \ge \frac{(2\pi e \sigma_1^2 - 1)\sigma_2^2}{2}, \end{cases} \tag{3.17}$$

and the optimum power control is given by

$$(P_1^*, P_2^*) = \begin{cases} (P, P), & 0 \le P \le \frac{(2\pi e \sigma_1^2 - 1)\sigma_2^2}{2} \\ (P, P), & P \ge \frac{(2\pi e \sigma_1^2 - 1)\sigma_2^2}{2}. \end{cases} \tag{3.18}$$

Fig. 3: The bounds $C_s^{gi}$ and $C_s^{go}$ for $P_1 = P_2 = 10$, $\sigma_1^2 = 5$, $\sigma_2^2 = 2$

*Proof:* From Theorem 5, it is easy to see that the secrecy sum rate $R_{sum}$ of $C_s^{gi}$ is given by

$$R_{sum} = \frac{1}{2}\log(1 + \frac{P_1 + P_2}{\sigma_1^2}) - \frac{1}{2}\log(1 + \frac{P_1 + P_2}{\sigma_2^2}) + \min\{\frac{1}{2}\log(2\pi e\sigma_1^2), \frac{1}{2}\log(1 + \frac{P_1 + P_2}{\sigma_2^2})\}, (3.19)$$

and (3.19) can be re-written as

$$R_{sum} = \begin{cases} \frac{1}{2}\log(1 + \frac{P_1+P_2}{\sigma_1^2}), & 0 \leq P_1 + P_2 \leq (2\pi e\sigma_1^2 - 1)\sigma_2^2 \\ \frac{1}{2}\log(1 + \frac{P_1+P_2}{\sigma_1^2}) - \frac{1}{2}\log(1 + \frac{P_1+P_2}{\sigma_2^2}) + \frac{1}{2}\log(2\pi e\sigma_1^2), & P_1 + P_2 > (2\pi e\sigma_1^2 - 1)\sigma_2^2. \end{cases} \quad (3.20)$$

Since $0 \leq P_1 + P_2 \leq 2P$, the secrecy sum rate $R_{sum}$ in (3.20) can be considered into the following three cases:

- (Case 1:) If $0 \leq P \leq \frac{(2\pi e\sigma_1^2 - 1)\sigma_2^2}{2}$, it is easy to see that $R_{sum}$ is increasing while $P_1$ and $P_2$ are increasing, and thus we have $R_{sum}^* = \frac{1}{2}\log(1 + \frac{2P}{\sigma_1^2})$, and the corresponding optimum $P_1^*$ and $P_2^*$ equal to $P$.

- (Case 2:) If $P > \frac{(2\pi e\sigma_1^2 - 1)\sigma_2^2}{2}$ and $\sigma_1^2 \leq \sigma_2^2$, (3.20) is re-written as

$$R_{sum} = \begin{cases} \frac{1}{2}\log(1 + \frac{P_1+P_2}{\sigma_1^2}), & 0 \leq P_1 + P_2 \leq (2\pi e\sigma_1^2 - 1)\sigma_2^2 \\ \frac{1}{2}\log(1 + \frac{P_1+P_2}{\sigma_1^2}) - \frac{1}{2}\log(1 + \frac{P_1+P_2}{\sigma_2^2}) + \frac{1}{2}\log(2\pi e\sigma_1^2), & (2\pi e\sigma_1^2 - 1)\sigma_2^2 < P_1 + P_2 \leq 2P. \end{cases}$$
$$(3.21)$$

  It is not difficult to show that for this case, $R_{sum}^* = \frac{1}{2}\log(1 + \frac{2P}{\sigma_1^2}) - \frac{1}{2}\log(1 + \frac{2P}{\sigma_2^2}) + \frac{1}{2}\log(2\pi e\sigma_1^2)$, and the corresponding optimum $P_1^*$ and $P_2^*$ equal to $P$.

- (Case 3:) If $P > \frac{(2\pi e\sigma_1^2 - 1)\sigma_2^2}{2}$ and $\sigma_1^2 > \sigma_2^2$, it is not difficult to show that for this case, $R_{sum}^* = \frac{1}{2}\log(1 + \frac{(2\pi e\sigma_1^2 - 1)\sigma_2^2}{\sigma_1^2})$, and the corresponding optimum $P_1^*$ and $P_2^*$ equal to $\frac{(2\pi e\sigma_1^2 - 1)\sigma_2^2}{2}$.

Combining the above three cases, Theorem 7 is obtained, and the proof is completed. ∎

The following Figure 4 and Figure 5 show the maximum secrecy sum rate $R^*_{sum}$ and the corresponding optimum power control for $\sigma_1^2 > \sigma_2^2$ and $\sigma_1^2 \le \sigma_2^2$, respectively. It is easy to see that for both cases, $R^*_{sum}$ tends to a constant while $P$ tends to infinity.



Fig. 4: The maximum secrecy sum rate $R^*_{sum}$ and the corresponding optimum power control for $\sigma_1^2 = 5$ and $\sigma_2^2 = 2$

## IV. Conclusions

In this paper, we present two inner bounds and one outer bound on the secrecy capacity region of the MAC-WT with noiseless feedback. To be specific, the first inner bound is constructed by using the DF strategy, where each transmitter decodes the other one's transmitted message from the noiseless feedback and then uses the decoded message to re-encode his own messages. The second inner bound is constructed by combining Ahlswede and Cai's idea of generating a secret key from the noiseless feedback [8] with the DF strategy used in the first inner bound. The outer bound is a simple sato-type bound. We show that the second inner bound is strictly larger than the first one, and the capacity results are further explained via a Gaussian example.

## Acknowledgement

Fig. 5: The maximum secrecy sum rate $R^*_{sum}$ and the corresponding optimum power control for $\sigma_1^2 = 1$ and $\sigma_2^2 = 10$

## APPENDIX A

### PROOF OF THEOREM 2

The messages $W_1 = (W_{1,1}, ..., W_{1,n})$ and $W_2 = (W_{2,1}, ..., W_{2,n})$ are transmitted through $n$ blocks. In block $i$ ($1 \leq i \leq n$), the transmitted message $w_{j,i}$ ($j = 1, 2$) is denoted by $w_{j,i} = (w_{j,i,0}, w_{j,i,1})$, where $w_{j,i,0} \in \{1, 2, ..., 2^{NR_{j0}}\}$, $w_{j,i,1} \in \{1, 2, ..., 2^{NR_{j1}}\}$, $w_{j,i} \in \{1, 2, ..., 2^{NR_j}\}$ and $R_j = R_{j0} + R_{j1}$. Here note that in block 1, the transmitted message $w_{j,1} = (w_{j,1,0}, const)$ ($j = 1, 2$), which implies that the sub-message $w_{j,1,1}$ is a constant. For block $i$ ($1 \leq i \leq n$), let $w^*_{1,i}$ and $w^*_{2,i}$ be the randomly generated dummy messages for transmitters 1 and 2, respectively. Here $w^*_{j,i} \in \{1, 2, ..., 2^{NR^*_j}\}$ ($j = 1, 2$).

For $1 \leq i \leq n$, let $\widetilde{X}_{j,i}$ ($j = 1, 2$), $\widetilde{U}_i$, $\widetilde{Y}_i$ and $\widetilde{Z}_i$ be the random vectors with length $N$ for block $i$. The specific values of the above random vectors are denoted by lower case letters. Moreover, let $X^n_j = (\widetilde{X}_{j,1}, ..., \widetilde{X}_{j,n})$, $U^n = (\widetilde{U}_1, ..., \widetilde{U}_n)$, $Y^n = (\widetilde{Y}_1, ..., \widetilde{Y}_n)$ and $Z^n = (\widetilde{Z}_1, ..., \widetilde{Z}_n)$.

*Construction of the code-books*: In each block $i$ ($1 \leq i \leq n$), for a fixed joint probability $P_{Z,Y|X_1,X_2}(z, y|x_1, x_2)$ $P_{X_1|U}(x_1|u) P_{X_2|U}(x_2|u) P_U(u)$, randomly generate $2^{N(R_{10}+R_{11}+R^*_1+R_{20}+R_{21}+R^*_2)}$ i.i.d. sequences $\widetilde{u}_i$ according to $P_U(u)$, and index these sequences as $\widetilde{u}_i(w'_{0,i})$, where $1 \leq w'_{0,i} \leq 2^{N(R_{10}+R_{11}+R^*_1+R_{20}+R_{21}+R^*_2)}$.

For each $w'_{0,i}$, randomly generate $2^{N(R_{j0}+R_{j1}+R^*_j)}$ ($j = 1, 2$) i.i.d. sequences $\widetilde{x}_{j,i}$ according to $P_{X_j|U}(x_j|u)$, and index these sequences as $\widetilde{x}_{j,i}(w'_{j,i})$, where $1 \leq w'_{j,i} \leq 2^{N(R_{j0}+R_{j1}+R^*_j)}$.

*Encoding scheme*: In block 1, both the transmitters choose $w'_{0,1} = 1$ as the index of the transmitted $\widetilde{u}_1$, and send $\widetilde{u}_1(1)$. Furthermore, the transmitter $j$ ($j = 1, 2$) chooses $w'_{j,1} = (w_{j,1,0}, w_{j,1,1} = const, w^*_{j,1})$ as the index of the

transmitted codeword $\widetilde{x}_{j,1}$.

In block $i$ ($2 \leq i \leq n$), suppose that transmitter 1 has already obtained $w'_{0,i-1}$ and $w'_{1,i-1} = (w_{1,i-1,0}, w_{1,i-1,1}, w^*_{1,i-1})$. Since the transmitter 1 receives the feedback $\widetilde{y}_{i-1}$, he tries to find a unique sequence $\widetilde{x}_{2,i-1}(\widecheck{w}'_{2,i-1}, w'_{0,i-1})$ such that $(\widetilde{x}_{2,i-1}(\widecheck{w}'_{2,i-1}, w'_{0,i-1}), \widetilde{x}_{1,i-1}(w'_{1,i-1}, w'_{0,i-1}), \widetilde{u}_{i-1}(w'_{0,i-1}),$

$\widetilde{y}_{i-1})$ are jointly typical sequences. From AEP, it is easy to see that the error probability $Pr\{\widecheck{w}'_{2,i-1} \neq w'_{2,i-1}\}$ goes to 0 if

$$R_{20} + R_{21} + R^*_2 \leq I(X_2; Y | X_1, U). \tag{A1}$$

Thus in block $i$, the transmitter 1 sends $\widetilde{u}_i$ with the index $w'_{0,i} = (w'_{1,i-1}, \widecheck{w}'_{2,i-1})$.

Analogously, since the transmitter 2 receives the feedback $\widetilde{y}_{i-1}$, he tries to find a unique sequence $\widetilde{x}_{1,i-1}(\widecheck{w}'_{1,i-1}, w'_{0,i-1})$ such that $(\widetilde{x}_{1,i-1}(\widecheck{w}'_{1,i-1}, w'_{0,i-1}), \widetilde{x}_{2,i-1}(w'_{2,i-1}, w'_{0,i-1}), \widetilde{u}_{i-1}(w'_{0,i-1}),$

$\widetilde{y}_{i-1})$ are jointly typical sequences. From AEP, it is easy to see that the error probability $Pr\{\widecheck{w}'_{1,i-1} \neq w'_{1,i-1}\}$ goes to 0 if

$$R_{10} + R_{11} + R^*_1 \leq I(X_1; Y | X_2, U). \tag{A2}$$

Thus in block $i$, the transmitter 2 sends $\widetilde{u}_i$ with the index $w'_{0,i} = (\widecheck{w}'_{1,i-1}, w'_{2,i-1})$.

In block $i$ ($2 \leq i \leq n$), before choosing the transmitted codewords $\widetilde{x}_{1,i}$ and $\widetilde{x}_{2,i}$, we generate a mapping $g_i : \widetilde{y}_{i-1} \rightarrow \{1, 2, ..., 2^{N(R_{11}+R_{21})}\}$. Furthermore, we define $K^*_i = (K^*_{i,1}, K^*_{i,2}) = g_i(\widetilde{Y}_{i-1})$ as a random variable uniformly distributed over $\{1, 2, ..., 2^{N(R_{11}+R_{21})}\}$, and it is independent of $\widetilde{X}_{1,i}$, $\widetilde{X}_{2,i}$, $\widetilde{Y}_i$, $\widetilde{Z}_i$, $W_{1,i}$, $W_{2,i}$, $W^*_{1,i}$ and $W^*_{2,i}$. Here note that $K^*_{i,j}$ ($j = 1, 2$) is used as a secret key shared by the transmitter $j$ and the receiver, and $k^*_{i,j} \in \{1, 2, ..., 2^{NR_{j1}}\}$ is a specific value of $K^*_{i,j}$. Reveal the mapping $g_i$ to the transmitters, receiver and the eavesdropper. After the generation of the secret key, the transmitter $j$ ($j = 1, 2$) sends $\widetilde{x}_{j,i}$ with the index $w'_{j,i} = (w_{j,i,0}, w_{j,i,1} \oplus k^*_{i,j}, w^*_{j,i})$.

*Decoding scheme for the receiver*: The intended receiver does backward decoding after the transmission of all $n$ blocks is completed, and the receiver's decoding scheme is exactly the same as that of the classical MAC with feedback [5, pp. 295-296]. Following similar steps of error probability analysis for MAC with feedback [5, pp. 295-296], we have

$$R_{10} + R_{11} + R^*_1 + R_{20} + R_{21} + R^*_2 \leq I(X_1, X_2; Y). \tag{A3}$$

*Equivocation analysis (1): For block $2 \leq i \leq n$, a lower bound on $H(K^*_i | \widetilde{X}_{1,i-1}, \widetilde{X}_{2,i-1}, \widetilde{Z}_{i-1})$: Given $\widetilde{X}_{1,i-1}$, $\widetilde{X}_{2,i-1}$ and $\widetilde{Z}_{i-1}$, the eavesdropper's equivocation about the secret key $k^*_i$ can be bounded by Ahlswede and Cai's balanced coloring lemma [8, p. 260], see the followings.*

*Lemma 1:* (**Balanced coloring lemma**) For arbitrary $\epsilon, \delta > 0$, sufficiently large $N$, all $N$-type $P_{X_1 X_2 Y}(x_1, x_2, y)$ and all $\widetilde{x}_{1,i-1}, \widetilde{x}_{2,i-1} \in T^N_{X_1 X_2}$ ($2 \leq i \leq n$), there exists a $\gamma$- coloring $c : T^N_{Y|X_1, X_2}(\widetilde{x}_{1,i-1}, \widetilde{x}_{2,i-1}) \rightarrow \{1, 2, .., \gamma\}$ of $T^N_{Y|X_1, X_2}(\widetilde{x}_{1,i-1}, \widetilde{x}_{2,i-1})$ such that for all joint $N$-type $P_{X_1 X_2 Y Z}(x_1, x_2, y, z)$ with marginal distribution

$P_{X_1X_2Z}(x_1, x_2, z)$ and $\dfrac{|T^N_{Y|X_1,X_2,Z}(\widetilde{x}_{1,i-1}, \widetilde{x}_{2,i-1}, \widetilde{z}_{i-1})|}{\gamma} \geq 2^{N\epsilon}$, $\widetilde{x}_{1,i-1}, \widetilde{x}_{2,i-1}, \widetilde{z}_{i-1} \in T_{X_1X_2Z}$,

$$|c^{-1}(k)| \leq \frac{|T^N_{Y|X_1,X_2,Z}(\widetilde{x}_{1,i-1}, \widetilde{x}_{2,i-1}, \widetilde{z}_{i-1})|(1+\delta)}{\gamma}, \tag{A4}$$

for $k = 1, 2, ..., \gamma$, where $c^{-1}$ is the inverse image of $c$.

From Lemma 1, we see that the typical set $T^N_{Y|X_1,X_2,Z}(\widetilde{x}_{1,i-1}, \widetilde{x}_{2,i-1}, \widetilde{z}_{i-1})$ maps into at least

$$\frac{|T^N_{Y|X_1,X_2,Z}(\widetilde{x}_{1,i-1}, \widetilde{x}_{2,i-1}, \widetilde{z}_{i-1}))|}{\frac{|T^N_{Y|X_1,X_2,Z}(\widetilde{x}_{1,i-1}, \widetilde{x}_{2,i-1}, \widetilde{z}_{i-1})|(1+\delta)}{\gamma}} = \frac{\gamma}{1+\delta} \tag{A5}$$

colors. On the other hand, the typical set $T^N_{Y|X_1,X_2,Z}(\widetilde{x}_{1,i-1}, \widetilde{x}_{2,i-1}, \widetilde{z}_{i-1})$ maps into at most $\gamma$ colors. From (A5), we can conclude that

$$H(K^*_i | \widetilde{X}_{1,i-1}, \widetilde{X}_{2,i-1}, \widetilde{Z}_{i-1}) \geq \log \frac{\gamma}{1+\delta}. \tag{A6}$$

Here note that $\dfrac{|T^N_{Y|X_1,X_2,Z}(\widetilde{x}_{1,i-1}, \widetilde{x}_{2,i-1}, \widetilde{z}_{i-1})|}{\gamma} \geq 2^{N\epsilon}$ implies that $\gamma \leq |T^N_{Y|X_1,X_2,Z}(\widetilde{x}_{1,i-1}, \widetilde{x}_{2,i-1}, \widetilde{z}_{i-1})|$. Choosing $\gamma = |T^N_{Y|X_1,X_2,Z}(\widetilde{x}_{1,i-1}, \widetilde{x}_{2,i-1}, \widetilde{z}_{i-1})|$ and noticing that

$$|T^N_{Y|X_1,X_2,Z}(\widetilde{x}_{1,i-1}, \widetilde{x}_{2,i-1}, \widetilde{z}_{i-1})| \geq (1 - \epsilon_1)2^{N(1-\epsilon_2)H(Y|X_1,X_2,Z)}, \tag{A7}$$

where $\epsilon_1$ and $\epsilon_2$ tend to $0$ as $N$ tends to infinity, (A6) can be further bounded by

$$H(K^*_i | \widetilde{X}_{1,i-1}, \widetilde{X}_{2,i-1}, \widetilde{Z}_{i-1}) \geq \log \frac{1-\epsilon_1}{1+\delta} + N(1-\epsilon_1)H(Y|X_1,X_2,Z). \tag{A8}$$

*Equivocation analysis (2): Bound on eavesdropper's equivocation* $\Delta$: For all blocks, the equivocation $\Delta$ is bounded by

$$\Delta = \frac{1}{nN}H(W_1, W_2|Z^n) \overset{(a)}{=} \frac{1}{nN}(H(W'_{1,0}, W'_{2,0}|Z^n)$$
$$+ H(W'_{1,1}, W'_{2,1}|Z^n, W'_{1,0}, W'_{2,0})), \tag{A9}$$

where (a) is from the definitions $W'_{j,0} = (W_{j,1,0}, ..., W_{j,n,0})$ and $W'_{j,1} = (W_{j,2,1}, ..., W_{j,n,1})$ for $j = 1, 2$. The conditional entropy $H(W'_{1,0}, W'_{2,0}|Z^n)$ of (A9) is bounded by

$$H(W'_{1,0}, W'_{2,0}|Z^n) = H(W'_{1,0}, W'_{2,0}, Z^n) - H(Z^n)$$
$$= H(W'_{1,0}, W'_{2,0}, Z^n, X^n_1, X^n_2) - H(X^n_1, X^n_2|W'_{1,0}, W'_{2,0}, Z^n) - H(Z^n)$$
$$\overset{(b)}{=} H(Z^n|X^n_1, X^n_2) + H(X^n_1, X^n_2) - H(X^n_1, X^n_2|W'_{1,0}, W'_{2,0}, Z^n) - H(Z^n)$$
$$\overset{(c)}{=} nN(R_{10} + R_{11} + R^*_1 + R_{20} + R_{21} + R^*_2) - nNI(X_1, X_2; Z) - H(X^n_1, X^n_2|W'_{1,0}, W'_{2,0}, Z^n)$$
$$\overset{(d)}{\geq} nN(R_{10} + R_{11} + R^*_1 + R_{20} + R_{21} + R^*_2) - nNI(X_1, X_2; Z) - nN\epsilon_3, \tag{A10}$$

where (b) is from $H(W'_{1,0}|X^n_1) = 0$ and $H(W'_{2,0}|X^n_2) = 0$, (c) is from the code constructions of $X^n_1$, $X^n_2$ and the fact that the channel is memoryless, and (d) is from the fact that given $w'_{1,0}$, $w'_{2,0}$ and $z^n$, the eavesdropper tries to find unique $w'_{1,1}$, $w'_{2,1}$, $w^*_1 = (w^*_{1,1}, ..., w^*_{1,n})$ and $w^*_2 = (w^*_{2,1}, ..., w^*_{2,n})$ such that $(x^n_1, x^n_2, z^n)$ are jointly typical, and from the properties of AEP, we see that the eavesdropper's decoding error probability tends to $0$ if

$$R_{1,1} + R_{2,1} + R^*_1 + R^*_2 \leq I(X_1, X_2; Z), \tag{A11}$$

then by using Fano's inequality, we have $\frac{1}{nN} H(X_1^n, X_2^n | W_{1,0}', W_{2,0}', Z^n) \leq \epsilon_3$, where $\epsilon_3 \to 0$ as $n, N \to \infty$. Moreover, the conditional entropy $H(W_{1,1}', W_{2,1}' | Z^n, W_{1,0}', W_{2,0}')$ of (A9) is bounded by

$$
\begin{aligned}
&H(W_{1,1}', W_{2,1}' | Z^n, W_{1,0}', W_{2,0}') \\
&\geq \sum_{i=2}^{n} H(W_{1,i,1}, W_{2,i,1} | Z^n, W_{1,0}', W_{2,0}', W_{1,1,1}, W_{2,1,1}, \\
&\quad ..., W_{1,i-1,1}, W_{2,i-1,1}, W_{1,i,1} \oplus K_{i,1}^*, W_{2,i,1} \oplus K_{i,2}^*) \\
&\overset{(e)}{=} \sum_{i=2}^{n} H(W_{1,i,1}, W_{2,i,1} | \widetilde{Z}_{i-1}, W_{1,i,1} \oplus K_{i,1}^*, W_{2,i,1} \oplus K_{i,2}^*) \\
&\geq \sum_{i=2}^{n} H(W_{1,i,1}, W_{2,i,1} | \widetilde{Z}_{i-1}, \widetilde{X}_{1,i-1}, \widetilde{X}_{2,i-1}, W_{1,i,1} \oplus K_{i,1}^*, W_{2,i,1} \oplus K_{i,2}^*) \\
&= \sum_{i=2}^{n} H(K_{i,1}^*, K_{i,2}^* | \widetilde{Z}_{i-1}, \widetilde{X}_{1,i-1}, \widetilde{X}_{2,i-1}, W_{1,i,1} \oplus K_{i,1}^*, W_{2,i,1} \oplus K_{i,2}^*) \\
&\overset{(f)}{=} \sum_{i=2}^{n} H(K_i^* | \widetilde{Z}_{i-1}, \widetilde{X}_{1,i-1}, \widetilde{X}_{2,i-1}) \\
&\overset{(g)}{\geq} (n-1)(\log \frac{1-\epsilon_1}{1+\delta} + N(1-\epsilon_1) H(Y | X_1, X_2, Z)),
\end{aligned}
$$

$$(A12)$$

where (e) is from the Markov chain $(W_{1,i,1}, W_{2,i,1}) \to (\widetilde{Z}_{i-1}, W_{1,i,1} \oplus K_{i,1}^*, W_{2,i,1} \oplus K_{i,2}^*)$ $\to (W_{1,0}', W_{2,0}', W_{1,1,1}, W_{2,1,1}, ..., W_{1,i-1,1}, W_{2,i-1,1}, \widetilde{Z}_1, ..., \widetilde{Z}_{i-2},$ $\widetilde{Z}_i, ..., \widetilde{Z}_n)$, (f) is from the definition $K_i^* = (K_{i,1}^*, K_{i,2}^*)$ and the Markov chain $K_i^* \to (\widetilde{Z}_{i-1}, \widetilde{X}_{1,i-1}, \widetilde{X}_{2,i-1}) \to$ $(W_{1,i,1} \oplus K_{i,1}^*, W_{2,i,1} \oplus K_{i,2}^*)$, and (g) is from (A8).

Substituting (A10) and (A12) into (A9), we have

$$
\begin{aligned}
\Delta \geq R_{10} + R_{11} + R_1^* + R_{20} + R_{21} + R_2^* - I(X_1, X_2; Z) - \epsilon_3 + \frac{n-1}{nN} \log \frac{1-\epsilon_1}{1+\delta} \\
+ \frac{n-1}{n}(1-\epsilon_1) H(Y | X_1, X_2, Z).
\end{aligned}
$$

$$(A13)$$

The bound (A13) implies that if

$$
R_1^* + R_2^* \geq I(X_1, X_2; Z) - H(Y | X_1, X_2, Z)
$$

$$(A14)$$

we can prove that $\Delta \geq R_{10} + R_{11} + R_{20} + R_{21} - \epsilon$ by choosing sufficiently large $n$ and $N$.

Finally, applying Fourier-Motzkin elimination (see, e.g., [18]) on (A1), (A2), (A3), (A11) and (A14), Theorem 2 is obtained. The proof of Theorem 2 is completed.

## APPENDIX B
### PROOF OF THEOREM 3

Note that

$$
R_1 + R_2 - \epsilon \overset{(1)}{\leq} \frac{H(W_1, W_2 | Z^N)}{N}
$$

$$
\begin{aligned}
&= \frac{1}{N}(H(W_1, W_2|Z^N) - H(W_1, W_2|Z^N, Y^N) + H(W_1, W_2|Z^N, Y^N)) \\
&\overset{(2)}{\leq} \frac{1}{N}(I(W_1, W_2; Y^N|Z^N) + \delta(P_e)) \\
&\leq \frac{1}{N}(H(Y^N|Z^N) + \delta(P_e)) \\
&= \frac{1}{N}\sum_{i=1}^{N} H(Y_i|Y^{i-1}, Z^N) + \frac{\delta(P_e)}{N} \\
&\leq \frac{1}{N}\sum_{i=1}^{N} H(Y_i|Z_i) + \frac{\delta(P_e)}{N} \\
&\overset{(3)}{=} \frac{1}{N}\sum_{i=1}^{N} H(Y_i|Z_i, J = i) + \frac{\delta(P_e)}{N} \\
&\overset{(4)}{=} H(Y_J|Z_J, J) + \frac{\delta(P_e)}{N} \\
&\overset{(5)}{\leq} H(Y_J|Z_J) + \frac{\delta(\epsilon)}{N} \\
&\overset{(6)}{=} H(Y|Z) + \frac{\delta(\epsilon)}{N},
\end{aligned}
\tag{A15}
$$

where (1) is from (2.5), (2) is from Fano's inequality, (3) and (4) are from the fact that $J$ is a random variable (uniformly distributed over $\{1, 2, ..., N\}$), and it is independent of $Y^N$, $Z^N$, $W_1$ and $W_2$, (5) is from $P_e \leq \epsilon$ and $\delta(P_e)$ is increasing while $P_e$ is increasing, and (6) is from the definitions $Y \triangleq Y_J$ and $Z \triangleq Z_J$. Letting $\epsilon \to 0$, $R_1 + R_2 \leq H(Y|Z)$ is proved. The proof of Theorem 3 is completed.

## REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

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

[3] J. M. Wozencraft, M. Horstein, "Coding for two-way channels," *MASSACHUSETTS INST OF TECH CAMBRIDGE RESEARCH LAB OF ELECTRONICS*, 1961.

[4] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY: Wiley-Interscience, 1991.

[5] T. M. Cover and C. S. K. Leung, "An achievable rate region for the multiple-access channel with feedback," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 3, pp. 292-298, 1981.

[6] T. M. Cover and A. El Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inf. Theory*, vol. IT-25, pp. 572-584, 1979.

[7] I. S. Bross and A. Lapidoth, "An improved achievable region for the discrete memoryless two-user multiple-access channel with noiseless feedback," *IEEE Trans. Inf. Theory*, vol. IT-51, no. 3, pp. 811-833, 2005.

[8] R. Ahlswede and N. Cai, "Transmission, Identification and Common Randomness Capacities for Wire-Tap Channels with Secure Feedback from the Decoder," book chapter in *General Theory of Information Transfer and Combinatorics*, LNCS 4123, pp. 258-275, Berlin: Springer-Verlag, 2006.

[9] E. Ardestanizadeh, M. Franceschetti, T.Javidi and Y.Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Trans. Inf. Theory*, vol. IT-55, no. 12, pp. 5353-5361, December 2009.

[10] B. Dai, A. J. Han vinck, Y. Luo and Z. Zhuang, "Capacity region of non-degraded wiretap channel with noiseless feedback," *Proceedings of 2012 IEEE International Symposium on Information Theory*, USA, 2012.

[11] B. Dai, Z. Ma and X. Fang, "Feedback Enhances the Security of State-Dependent Degraded Broadcast Channels With Confidential Messages," *IEEE Trans. Inf. Forensics and Security*, Vol. 10, No. 7, pp. 1529-1542, 2015.

[12] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-54, no. 12, pp. 5747-5755, Dec. 2008.

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

[14] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *Proc. Annual Allerton Conf. on Communications, Control and Computing*, Monticello, IL, Sept. 2008.

[15] M. H. Yassaee and M. R. Aref, "Multiple access wiretap channels with strong secrecy," *Proceedings of 2010 IEEE Information Theory Workshop*, pp. 1-5, 2010.

[16] M. Wiese and H. Boche, "An Achievable Region for the Wiretap Multiple-Access Channel with Common Message," *Proceedings of 2012 IEEE International Symposium on Information Theory*, 2012.

[17] X. Tang, R. Liu, P. Spasojević and H. V. Poor, "Multiple access channels with generalized feedback and confidential messages," *Proceedings of 2007 IEEE Information Theory Workshop*, pp. 608-613, 2007.

[18] S. Lall, "Advanced topics in computation for control," Lecture notes for Engr210b, Stanford University, Fall, 2004.