# Multiple-Access Relay Wiretap Channel 

Bin Dai and Zheng Ma


#### Abstract

In this paper, we investigate the effects of an additional trusted relay node on the secrecy of multiple-access wiretap channel (MAC-WT) by considering the model of multiple-access relay wiretap channel (MARC-WT). More specifically, first, we investigate the discrete memoryless MARC-WT. Three inner bounds (with respect to decodeforward (DF), noise-forward (NF) and compress-forward (CF) strategies) on the secrecy capacity region are provided. Second, we investigate the degraded discrete memoryless MARC-WT, and present an outer bound on the secrecy capacity region of this degraded model. Finally, we investigate the Gaussian MARC-WT, and find that the NF and CF strategies help to enhance Tekin-Yener's achievable secrecy rate region of Gaussian MAC-WT. Moreover, we find that if the channel from the transmitters to the relay is less noisy than the channels from the transmitters to the legitimate receiver and the wiretapper, the achievable secrecy rate region of the DF strategy is even larger than the corresponding regions of the NF and CF strategies.


## Index Terms

Multiple-access wiretap channel, relay channel, secrecy capacity region.

## I. Introduction

Equivocation was first introduced into channel coding by Wyner in his study of wiretap channel [1]. It is a kind of discrete memoryless degraded broadcast channels. The objective is to transmit messages to the legitimate receiver, while keeping the wiretapper as ignorant of the messages as possible. Based on Wyners work, Leung-YanCheong and Hellman studied the Gaussian wiretap channel (GWC) [2], and showed that its secrecy capacity was the difference between the main channel capacity and the overall wiretap channel capacity (the cascade of main channel and wiretap channel).

After the publication of Wyner's work, Csiszár and Körner [3] investigated a more general situation: the 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 wiretapper, while the confidential message was only allowed to be obtained by the legitimate receiver. This model is also a generalization of [4], where no confidentiality condition is imposed. The capacity-equivocation region and the secrecy capacity region of BCC [3] were totally determined, and the results

[^0] e-mail: daibin@home.swjtu.edu.cn, zma@home.swjtu.edu.cn.
were also a generalization of those in [1]. Furthermore, the capacity-equivocation region of Gaussian BCC was determined in [22].

By using the approach of [1] and [3], the information-theoretic security for other multi-user communication systems has been widely studied, see the followings.

- For the broadcast channel, Liu et al. [5] studied the broadcast channel with two confidential messages (no common message), and provided an inner bound on the secrecy capacity region. Furthermore, Xu et al. [6] studied the broadcast channel with two confidential messages and one common message, and provided inner and outer bounds on the capacity-equivocation region.
- 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 [7]. An inner bound on the capacity-equivocation region is provided for the model with two confidential messages, and the capacityequivocation region is still not known. Furthermore, for the model of MAC with one confidential message [7], both inner and outer bounds on 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). The Gaussian MAC-WT was investigated in [8], [9]. An inner bound on the capacity-equivocation region is provided for the Gaussian MAC-WT. Other related works on MAC-WT can be found in [10], [11], [12], [13], [14], [15], [16].
- For the interference channel, Liu et al. [5] 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 capacityequivocation region was totally determined for this model.
- For the relay channel, Lai and Gamal [18] studied the relay-eavesdropper channel, where a source wishes to send messages to a destination while leveraging the help of a trusted relay node to hide those messages from the eavesdropper. Three inner bounds (with respect to decode-forward, noise-forward and compress-forward strategies) and one outer bound on the capacity-equivocation region were provided in [18]. Furthermore, Tang et. al. [27] introduced the noise-forward strategy of [18] into the wireless communication networks, and found that with the help of an independent interferer, the security of the wireless communication networks is enhanced. In addition, Oohama [19] 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 [19].

Recently, Ekrem and Ulukus [20] investigated the effects of user cooperation on the secrecy of broadcast channels by considering a cooperative relay broadcast channel. They showed that user cooperation can increase the achievable secrecy rate region of [5].

In this paper, we study the multiple-access relay wiretap channel (MARC-WT), see Figure 1. This model generalizes the MAC-WT by considering an additional trusted relay node. The motivation of this work is to investigate the effects of the trusted relay node on the secrecy of MAC-WT, and whether the achievable secrecy rate region of [9] can be enhanced by using an additional relay node.


Fig. 1: The multiple-access relay wiretap channel

First, we provide three inner bounds on the secrecy capacity region (achievable secrecy rate regions) of the discrete memoryless model of Figure 1 The decode-forward (DF), noise-forward (NF) and compress-forward (CF) relay strategies are used in the construction of the inner bounds. Second, we investigate the degraded discrete memoryless MARC-WT, and present an outer bound on the secrecy capacity region of this degraded case. Finally, the Gaussian model of Figure 1 is investigated, and we find that with the help of this additional trusted relay node, Tekin-Yeners achievable secrecy rate region of the Gaussian MAC-WT [9] is enhanced.

In this paper, random variables, 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 $\left(U_{1}, \ldots, U_{N}\right)$, and $u^{N}=\left(u_{1}, \ldots, u_{N}\right)$ 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 $\left(U_{i}, \ldots, U_{N}\right)$, and $u_{i}^{N}=\left(u_{i}, \ldots, u_{N}\right)$ is a specific vector value in $\mathcal{U}_{i}^{N}$. Let $P_{V}(v)$ denote the probability mass function $\operatorname{Pr}\{V=v\}$. Throughout the paper, the logarithmic function is to the base 2 .

The organization of this paper is as follows. Section $\Pi$ provides the achievable secrecy rate regions of the discrete memoryless model of Figure 1 The Gaussian model of Figure 1 is investigated in Section $I I I$ Final conclusions are provided in Section IV

## II. DISCRETE MEMORYLESS MULTIPLE-ACCESS RELAY WIRETAP CHANNEL

## A. Inner bounds on the secrecy capacity region of the discrete memoryless MARC-WT

The discrete memoryless model of Figure 1 is a five-terminal discrete channel consisting of finite sets $\mathcal{X}_{1}, \mathcal{X}_{2}$, $\mathcal{X}_{r}, \mathcal{Y}, \mathcal{Y}_{r}, \mathcal{Z}$ and a transition probability distribution $P_{Y, Y_{r}, Z \mid X_{1}, X_{2}, X_{r}}\left(y, y_{r}, z \mid x_{1}, x_{2}, x_{r}\right) . X_{1}^{N}, X_{2}^{N}$ and $X_{r}^{N}$ are the channel inputs from the transmitters and the relay respectively, while $Y^{N}, Y_{r}^{N}, Z^{N}$ are the channel outputs at the legitimate receiver, the relay and the wiretapper, respectively. The channel is discrete memoryless, i.e., the channel outputs $\left(y_{i}, y_{r, i}, z_{i}\right)$ at time $i$ only depend on the channel inputs $\left(x_{1, i}, x_{2, i}, x_{r, i}\right)$ at time $i$.

Definition 1: (Channel encoders) 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 channel encoders $f_{E 1}$ and $f_{E 2}$ are stochastic encoders that map the messages $w_{1}$ and $w_{2}$ into the codewords $x_{1}^{N} \in \mathcal{X}_{1}^{N}$ and $x_{2}^{N} \in \mathcal{X}_{2}^{N}$, respectively. The transmission rates of the confidential messages $W_{1}$ and $W_{2}$ are $\frac{\log \left\|\mathcal{W}_{1}\right\|}{N}$ and $\frac{\log \left\|\mathcal{W}_{2}\right\|}{N}$, respectively.

Definition 2: (Relay encoder) The relay encoder $\varphi_{i}$ is also a stochastic encoder that maps the signals $\left(y_{r, 1}, y_{r, 2}, \ldots, y_{r, i-1}\right)$ received before time $i$ to the channel input $x_{r, i}$.

Definition 3: (Decoder) The decoder for the legitimate receiver is a mapping $f_{D}: \mathcal{Y}^{N} \rightarrow \mathcal{W}_{1} \times \mathcal{W}_{2}$, with input $Y^{N}$ and outputs $\hat{W}_{1}, \hat{W}_{2}$. Let $P_{e}$ be the error probability of the legitimate receiver, and it is defined as $\operatorname{Pr}\left\{\left(W_{1}, W_{2}\right) \neq\left(\hat{W}_{1}, \hat{W}_{2}\right)\right\}$.

The equivocation rate at the wiretapper is defined as

$$
\begin{equation*}
\Delta=\frac{1}{N} H\left(W_{1}, W_{2} \mid Z^{N}\right) \tag{2.1}
\end{equation*}
$$

A rate pair $\left(R_{1}, R_{2}\right)$ (where $R_{1}, R_{2} \geq 0$ ) is called achievable with perfect secrecy if, for any $\epsilon>0$ (where $\epsilon$ is an arbitrary small positive real number), there exists a sequence of codes $\left(2^{N R_{1}}, 2^{N R_{2}}, N\right)$ such that

$$
\begin{align*}
& \frac{\log \left\|\mathcal{W}_{1}\right\|}{N}=R_{1}, \frac{\log \left\|\mathcal{W}_{2}\right\|}{N}=R_{2} \\
& \Delta \geq R_{1}+R_{2}-\epsilon, \quad P_{e} \leq \epsilon \tag{2.2}
\end{align*}
$$

Note that the above secrecy requirement on the full message set also ensures the secrecy of individual message, i.e., $\frac{1}{N} H\left(W_{1}, W_{2} \mid Z^{N}\right) \geq R_{1}+R_{2}-\epsilon$ implies that $\frac{1}{N} H\left(W_{t} \mid Z^{N}\right) \geq R_{t}-\epsilon$ for $t=1,2$, and the proof is as follows.

Proof: Since

$$
\begin{align*}
& 0 \geq R_{1}+R_{2}-\epsilon-\frac{1}{N} H\left(W_{1}, W_{2} \mid Z^{N}\right)=\frac{1}{N} H\left(W_{1}\right)+\frac{1}{N} H\left(W_{2}\right)-\frac{1}{N} H\left(W_{1}, W_{2} \mid Z^{N}\right)-\epsilon \\
& =\frac{1}{N} H\left(W_{1}\right)+\frac{1}{N} H\left(W_{2}\right)-\frac{1}{N} H\left(W_{1} \mid Z^{N}\right)-\frac{1}{N} H\left(W_{2} \mid W_{1}, Z^{N}\right)-\epsilon \\
& \geq \frac{1}{N} H\left(W_{1}\right)+\frac{1}{N} H\left(W_{2}\right)-\frac{1}{N} H\left(W_{1} \mid Z^{N}\right)-\frac{1}{N} H\left(W_{2} \mid Z^{N}\right)-\epsilon \\
& =\frac{1}{N} I\left(W_{1} ; Z^{N}\right)+\frac{1}{N} I\left(W_{2} ; Z^{N}\right)-\epsilon, \tag{2.3}
\end{align*}
$$

and $\frac{1}{N} I\left(W_{1} ; Z^{N}\right) \geq 0, \frac{1}{N} I\left(W_{2} ; Z^{N}\right) \geq 0$, it is easy to see that $\frac{1}{N} I\left(W_{1} ; Z^{N}\right) \leq \epsilon, \frac{1}{N} I\left(W_{2} ; Z^{N}\right) \leq \epsilon$, which implies that $\frac{1}{N} H\left(W_{t} \mid Z^{N}\right) \geq R_{t}-\epsilon$ for $t=1,2$. The proof is completed.

The secrecy capacity region $\mathcal{R}^{d}$ is a set composed of all achievable secrecy rate pairs $\left(R_{1}, R_{2}\right)$. Three inner bounds (with respect to DF, NF and CF strategies) on $\mathcal{R}^{d}$ are provided in the following Theorem 1, 2, 3,

Our first step is to characterize the inner bound on the secrecy capacity region $\mathcal{R}^{d}$ by using Cover-El Gamal's Decode and Forward (DF) Strategy [23]. In the DF Strategy, the relay node will first decode the confidential messages, and then re-encode them to cooperate with the transmitters. The superposition coding and random binning techniques will be combined with the classical DF strategy [23] to characterize the DF inner bound of the discrete memoryless MARC-WT. The following Theorem 1 shows the DF inner bound on $\mathcal{R}^{d}$.

Theorem 1: (Inner bound 1: DF strategy) A single-letter characterization of the region $\mathcal{R}^{d 1}\left(\mathcal{R}^{d 1} \subseteq \mathcal{R}^{d}\right)$ is as follows,

$$
\begin{aligned}
& \mathcal{R}^{d 1}=\left\{\left(R_{1}, R_{2}\right): R_{1}, R_{2} \geq 0\right. \\
& R_{1} \leq \min \left\{I\left(X_{1} ; Y_{r} \mid X_{r}, X_{2}, V_{1}, V_{2}\right), I\left(X_{1}, X_{r} ; Y \mid X_{2}, V_{2}\right)\right\}-I\left(X_{1} ; Z\right) \\
& R_{2} \leq \min \left\{I\left(X_{2} ; Y_{r} \mid X_{r}, X_{1}, V_{1}, V_{2}\right), I\left(X_{2}, X_{r} ; Y \mid X_{1}, V_{1}\right)\right\}-I\left(X_{2} ; Z\right) \\
& \left.R_{1}+R_{2} \leq \min \left\{I\left(X_{1}, X_{2} ; Y_{r} \mid X_{r}, V_{1}, V_{2}\right), I\left(X_{1}, X_{2}, X_{r} ; Y\right)\right\}-I\left(X_{1}, X_{2} ; Z\right)\right\}
\end{aligned}
$$

for some distribution

$$
\begin{aligned}
& P_{Y, Z, Y_{r}, X_{r}, X_{1}, X_{2}, V_{1}, V_{2}}\left(y, z, y_{r}, x_{r}, x_{1}, x_{2}, v_{1}, v_{2}\right)= \\
& P_{Y, Z, Y_{r} \mid X_{r}, X_{1}, X_{2}}\left(y, z, y_{r} \mid x_{r}, x_{1}, x_{2}\right) P_{X_{r} \mid V_{1}, V_{2}}\left(x_{r} \mid v_{1}, v_{2}\right) P_{X_{1} \mid V_{1}}\left(x_{1} \mid v_{1}\right) P_{X_{2} \mid V_{2}}\left(x_{2} \mid v_{2}\right) P_{V_{1}}\left(v_{1}\right) P_{V_{2}}\left(v_{2}\right)
\end{aligned}
$$

Proof:
The achievable coding scheme is a combination of [26], [21] and [9], and the details about the proof are provided in Appendix A

Remark 1: There are some notes on Theorem 1, see the following.

- If we let $Z=$ const (which implies that there is no wiretapper), the region $\mathcal{R}^{d 1}$ reduces to the following achievable region $\mathcal{R}^{\text {marc }}$, where

$$
\begin{align*}
& \mathcal{R}^{\text {marc }}=\left\{\left(R_{1}, R_{2}\right): R_{1}, R_{2} \geq 0\right. \\
& R_{1} \leq \min \left\{I\left(X_{1} ; Y_{r} \mid X_{r}, X_{2}, V_{1}, V_{2}\right), I\left(X_{1}, X_{r} ; Y \mid X_{2}, V_{2}\right)\right\} \\
& R_{2} \leq \min \left\{I\left(X_{2} ; Y_{r} \mid X_{r}, X_{1}, V_{1}, V_{2}\right), I\left(X_{2}, X_{r} ; Y \mid X_{1}, V_{1}\right)\right\} \\
& \left.R_{1}+R_{2} \leq \min \left\{I\left(X_{1}, X_{2} ; Y_{r} \mid X_{r}, V_{1}, V_{2}\right), I\left(X_{1}, X_{2}, X_{r} ; Y\right)\right\}\right\} \tag{2.4}
\end{align*}
$$

Here note that the achievable region $\mathcal{R}^{\text {marc }}$ is exactly the same as the achievable DF region (DF inner bound on the capacity region) of the discrete memoryless multiple-access relay channel [26], [21].

- If we let $Y_{r}=Y$ and $V_{1}=V_{2}=X_{r}=$ const (which implies that there is no relay), the region $\mathcal{R}^{d 1}$ reduces
to the region $\mathcal{R}^{m a c-w t}$, where

$$
\begin{align*}
& \mathcal{R}^{m a c-w t}=\left\{\left(R_{1}, R_{2}\right): R_{1}, R_{2} \geq 0\right. \\
& R_{1} \leq I\left(X_{1} ; Y \mid X_{2}\right)-I\left(X_{1} ; Z\right) \\
& R_{2} \leq I\left(X_{2} ; Y \mid X_{1}\right)-I\left(X_{2} ; Z\right) \\
& \left.R_{1}+R_{2} \leq I\left(X_{1}, X_{2} ; Y\right)-I\left(X_{1}, X_{2} ; Z\right)\right\} \tag{2.5}
\end{align*}
$$

Also note that the region $\mathcal{R}^{m a c-w t}$ is exactly the same as the achievable secrecy rate region of discrete memoryless multiple-access wiretap channel [9].

The second step is to characterize the inner bound on the secrecy capacity region $\mathcal{R}^{d}$ by using the noise and forward (NF) strategy. In the NF Strategy, the relay node does not attempt to decode the messages but sends sequences that are independent of the transmitters' messages, and these sequences aid in confusing the wiretapper.

More specifically, for a given input distribution of the relay, if the corresponding mutual information with the legitimate receiver's output is not less than that with the wiretapper's output, we allow the legitimate receiver to decode the sequence of the relay, and the wiretapper can not decode it. Therefore, in this case, the sequence of the relay can be viewed as a noise signal to confuse the wiretapper.

On the other hand, if the corresponding mutual information with the legitimate receiver's output is not more than that with the wiretapper's output, we allow both the receivers to decode the sequence of the relay. In this case, the sequence of the relay does not make any contribution to the security of the discrete memoryless MARC-WT.

The following Theorem 2 shows the NF inner bound on $\mathcal{R}^{d}$.
Theorem 2: (Inner bound 2: NF strategy) A single-letter characterization of the region $\mathcal{R}^{d 2}\left(\mathcal{R}^{d 2} \subseteq \mathcal{R}^{d}\right)$ is as follows,

$$
\mathcal{R}^{d 2}=\text { convex closure of } \quad\left(\mathcal{L}^{1} \bigcup \mathcal{L}^{2}\right)
$$

where $\mathcal{L}^{1}$ is given by

$$
\mathcal{L}^{1}=\bigcup_{\substack{P_{Y, Z, Y_{r}, X_{r}, X_{1}, X_{2}}^{I\left(X_{r} ; Y\right) \geq I\left(X_{r} ; Z\right)}}}\left\{\begin{array}{l}
\left(R_{1}, R_{2}\right): R_{1}, R_{2} \geq 0 \\
R_{1} \leq I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)-I\left(X_{1}, X_{r} ; Z\right)+R_{r} \\
R_{2} \leq I\left(X_{2} ; Y \mid X_{1}, X_{r}\right)-I\left(X_{2}, X_{r} ; Z\right)+R_{r} \\
R_{1}+R_{2} \leq I\left(X_{1}, X_{2} ; Y \mid X_{r}\right)-I\left(X_{1}, X_{2}, X_{r} ; Z\right)+R_{r}
\end{array}\right\}
$$

$R_{r}$ denotes

$$
R_{r}=\min \left\{I\left(X_{r} ; Y\right), I\left(X_{r} ; Z \mid X_{1}\right), I\left(X_{r} ; Z \mid X_{2}\right)\right\}
$$

and $\mathcal{L}^{2}$ is given by

$$
\mathcal{L}^{2}=\bigcup_{\substack{P_{Y, Z, Y_{r}, X_{r}, X_{1}, X_{2}}: \\
I\left(X_{r} ; Z\right) \geq I\left(X_{r} ; Y\right)}}\left\{\begin{array}{l}
\left(R_{1}, R_{2}\right): R_{1}, R_{2} \geq 0 \\
R_{1} \leq I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)-I\left(X_{1} ; Z \mid X_{r}\right) \\
R_{2} \leq I\left(X_{2} ; Y \mid X_{1}, X_{r}\right)-I\left(X_{2} ; Z \mid X_{r}\right) \\
R_{1}+R_{2} \leq I\left(X_{1}, X_{2} ; Y \mid X_{r}\right)-I\left(X_{1}, X_{2} ; Z \mid X_{r}\right)
\end{array}\right\}
$$

here the joint probability $P_{Y, Z, Y_{r}, X_{r}, X_{1}, X_{2}}\left(y, z, y_{r}, x_{r}, x_{1}, x_{2}, u\right)$ satisfies

$$
P_{Y, Z, Y_{r}, X_{r}, X_{1}, X_{2}}\left(y, z, y_{r}, x_{r}, x_{1}, x_{2}\right)=P_{Y, Z, Y_{r} \mid X_{r}, X_{1}, X_{2}}\left(y, z, y_{r} \mid x_{r}, x_{1}, x_{2}\right) P_{X_{r}}\left(x_{r}\right) P_{X_{1}}\left(x_{1}\right) P_{X_{2}}\left(x_{2}\right) .
$$

Proof:
The achievable coding scheme is a combination of [18, Theorem 3] and [9], and the details about the proof are provided in Appendix B.

Remark 2: There are some notes on Theorem 2, see the following.

- Since the two regions $\mathcal{L}^{1}$ and $\mathcal{L}^{2}$ are not necessarily contained by one another, by using time-sharing arguments, it is easy to find a new achievable region which is the convex-closure of the union of the two regions.
- The region $\mathcal{L}^{1}$ is characterized under the condition that for a given input distribution of the relay, the corresponding mutual information with the legitimate receiver's output is not less than that with the wiretapper's output $\left(I\left(X_{r} ; Y\right) \geq I\left(X_{r} ; Z\right)\right)$. Then, in this case, the legitimate receiver is allowed to decode the sequence of the relay, and the wiretapper is not allowed to decode it. The rate of the sequence is defined as $R_{r}=\min \left\{I\left(X_{r} ; Y\right), I\left(X_{r} ; Z \mid X_{1}\right), I\left(X_{r} ; Z \mid X_{2}\right)\right\}$, and the sequence is viewed as pure noise for the wiretapper.
- The region $\mathcal{L}^{2}$ is characterized under the condition that for a given input distribution of the relay, the corresponding mutual information with the legitimate receiver's output is not more than that with the wiretapper's output $\left(I\left(X_{r} ; Y\right) \leq I\left(X_{r} ; Z\right)\right)$. Then, in this case, both the legitimate receiver and the wiretapper are allowed to decode the sequence of the relay. The rate of the sequence is defined as $R_{r}=I\left(X_{r} ; Y\right)$, and the sequence does not make any contribution to the security of the discrete memoryless MARC-WT.

The third step is to characterize the inner bound on the secrecy capacity region $\mathcal{R}^{d}$ by using a combination of Cover- El Gamals compress and forward (CF) strategy [23] and the NF strategy provided in Theorem 2, i.e., in addition to the independent codewords, the relay also sends a quantized version of its noisy observations to the legitimate receiver. This noisy version of the relay's observations helps the legitimate receiver in decoding the transmitters' messages, while the independent codewords help in confusing the wiretapper. The following Theorem 3 shows the CF inner bound on $\mathcal{R}^{d}$.

Theorem 3: (Inner bound 3: CF strategy) A single-letter characterization of the region $\mathcal{R}^{d 3}\left(\mathcal{R}^{d 3} \subseteq \mathcal{R}^{d}\right)$ is as follows,

$$
\mathcal{R}^{d 3}=\text { convex closure of } \quad\left(\mathcal{L}^{3} \bigcup \mathcal{L}^{4}\right)
$$

where $\mathcal{L}^{3}$ is given by

$$
\mathcal{L}^{3}=\underset{\substack{P_{Y, Z, Y_{r}, \hat{Y}_{r}, X_{r}, X_{1}, X_{2}}: I\left(X_{r} ; Y\right) \geq I\left(X_{r} ; Z\right) \\
R_{r 1}^{*}-R^{*} \geq I\left(Y_{r} ; \hat{Y}_{r} \mid X_{r}\right)}}{ }\left\{\begin{array}{l}
\left(R_{1}, R_{2}\right): R_{1}, R_{2} \geq 0, \\
R_{1} \leq I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-I\left(X_{1}, X_{r} ; Z\right)+R^{*}, \\
R_{2} \leq I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{1}, X_{r}\right)-I\left(X_{2}, X_{r} ; Z\right)+R^{*}, \\
R_{1}+R_{2} \leq I\left(X_{1}, X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)-I\left(X_{1}, X_{2}, X_{r} ; Z\right)+R^{*} .
\end{array}\right\}
$$

$R_{r 1}^{*}=\min \left\{I\left(X_{r} ; Z \mid X_{1}\right), I\left(X_{r} ; Z \mid X_{2}\right), I\left(X_{r} ; Y\right)\right\}, R^{*}$ is the rate of pure noise generated by the relay to confuse the wiretapper, $R_{r 1}^{*}-R^{*}$ is the part of the rate allocated to send the compressed signal $\hat{Y}_{r}$ to help the legitimate
receiver, and $\mathcal{L}^{4}$ is given by

$$
\mathcal{L}^{4}=\underset{\substack{P_{Y, Z, Y_{r}, \hat{Y}_{r}, X_{r}, X_{1}, X_{2}: I\left(X_{r} ; Z\right) \geq I\left(X_{r} ; Y\right)}^{I\left(X_{r} ; Y\right) \geq I\left(Y_{r} ; \hat{Y}_{r} \mid X_{r}\right)}}}{\mathcal{S}_{\substack{ }}}\left\{\begin{array}{l}
\left(R_{1}, R_{2}\right): R_{1}, R_{2} \geq 0, \\
R_{1} \leq I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-I\left(X_{1} ; Z \mid X_{r}\right), \\
R_{2} \leq I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{1}, X_{r}\right)-I\left(X_{2} ; Z \mid X_{r}\right), \\
R_{1}+R_{2} \leq I\left(X_{1}, X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)-I\left(X_{1}, X_{2} ; Z \mid X_{r}\right) .
\end{array}\right\} .
$$

The joint probability $P_{Y, Z, Y_{r}, \hat{Y}_{r}, X_{r}, X_{1}, X_{2}}\left(y, z, y_{r}, \hat{y}_{r}, x_{r}, x_{1}, x_{2}\right)$ satisfies

$$
\begin{aligned}
& P_{Y, Z, Y_{r}, \hat{Y}_{r}, X_{r}, X_{1}, X_{2}}\left(y, z, y_{r}, \hat{y}_{r}, x_{r}, x_{1}, x_{2}\right)= \\
& P_{\hat{Y}_{r} \mid Y_{r}, X_{r}}\left(\hat{y}_{r} \mid y_{r}, x_{r}\right) P_{Y, Z, Y_{r} \mid X_{r}, X_{1}, X_{2}}\left(y, z, y_{r} \mid x_{r}, x_{1}, x_{2}\right) P_{X_{r}}\left(x_{r}\right) P_{X_{1}}\left(x_{1}\right) P_{X_{2}}\left(x_{2}\right) .
\end{aligned}
$$

Proof:
The achievable coding scheme is a combination of [18, Theorem 4] and [9], and the details about the proof are provided in Appendix C

Remark 3: There are some notes on Theorem 3, see the following.

- Since the two regions $\mathcal{L}^{3}$ and $\mathcal{L}^{4}$ are not necessarily contained by one another, by using time-sharing arguments, it is easy to find a new achievable region which is the convex-closure of the union of the two regions.
- The region $\mathcal{L}^{3}$ is characterized under the condition that for a given input distribution of the relay, the corresponding mutual information with the legitimate receiver's output is not less than that with the wiretapper's output $\left(I\left(X_{r} ; Y\right) \geq I\left(X_{r} ; Z\right)\right)$. Then, in this case, the legitimate receiver is allowed to decode the sequence of the relay, and the wiretapper is not allowed to decode it. Here note that if $R^{*}=R_{r 1}^{*}$, this scheme is exactly the same as the NF scheme.
- The region $\mathcal{L}^{4}$ is characterized under the condition that for a given input distribution of the relay, the corresponding mutual information with the legitimate receiver's output is not more than that with the wiretapper's output $\left(I\left(X_{r} ; Y\right) \leq I\left(X_{r} ; Z\right)\right)$. Then, in this case, both the legitimate receiver and the wiretapper are allowed to decode the sequence of the relay. However, the relay can still help to enhance the security of the discrete memoryless MARC-WT by sending the compressed signal $\hat{Y}_{r}$ to the legitimate receiver.


## B. Outer bound on the secrecy capacity region of the degraded discrete memoryless MARC-WT

Compared with the discrete memoryless MARC-WT (see Figure 1), the degraded case implies the existence of a Markov chain $\left(X_{1}, X_{2}, X_{r}, Y_{r}\right) \rightarrow Y \rightarrow Z$. The secrecy capacity region $\mathcal{R}^{d d}$ of the degraded discrete memoryless MARC-WT is a set composed of all achievable secrecy rate pairs $\left(R_{1}, R_{2}\right)$. An outer bound on $\mathcal{R}^{d d}$ is provided in the following Theorem 4

Theorem 4: (Outer bound) A single-letter characterization of the region $\mathcal{R}^{d d o}$ ( $\mathcal{R}^{d d} \subseteq \mathcal{R}^{d d o}$ ) is as follows,

$$
\begin{aligned}
& \mathcal{R}^{d d o}=\left\{\left(R_{1}, R_{2}\right): R_{1}, R_{2} \geq 0\right. \\
& R_{1} \leq I\left(X_{1}, X_{r} ; Y \mid X_{2}, U\right)-I\left(X_{1} ; Z \mid U\right) \\
& R_{2} \leq I\left(X_{2}, X_{r} ; Y \mid X_{1}, U\right)-I\left(X_{2} ; Z \mid U\right) \\
& \left.R_{1}+R_{2} \leq I\left(X_{1}, X_{2}, X_{r} ; Y \mid U\right)-I\left(X_{1}, X_{2} ; Z \mid U\right)\right\}
\end{aligned}
$$

for some distribution

$$
\begin{aligned}
& P_{Z, Y, Y_{r}, X_{r}, X_{1}, X_{2}, U}\left(z, y, y_{r}, x_{r}, x_{1}, x_{2}, u\right)= \\
& P_{Z \mid Y}(z \mid y) P_{Y, Y_{r} \mid X_{1}, X_{2}, X_{r}}\left(y, y_{r} \mid x_{1}, x_{2}, x_{r}\right) P_{U, X_{1}, X_{2}, X_{r}}\left(u, x_{1}, x_{2}, x_{r}\right)
\end{aligned}
$$

Proof:
The details about the proof are provided in Appendix D
Remark 4: The outer bound on the secrecy capacity region of the degraded discrete memoryless MARC-WT is generally loose, but it is still useful for the analysis of the outer bound on the secrecy capacity region of the Gaussian MARC-WT, and this is because the scalar Gaussian MARC-WT is always degraded. The capacity results on the Gaussian MARC-WT will be given in the next section.

## III. Gaussian multiple-access relay wiretap channel

In this section, we investigate the Gaussian multiple-access relay wiretap channel (GMARC-WT). The signal received at each node is given by

$$
\begin{align*}
& Y_{r}=X_{1}+X_{2}+Z_{r} \\
& Y=X_{1}+X_{2}+X_{r}+Z_{1} \\
& Z=X_{1}+X_{2}+X_{r}+Z_{2} \tag{3.1}
\end{align*}
$$

where $Z_{r} \sim \mathcal{N}\left(0, N_{r}\right), Z_{1} \sim \mathcal{N}\left(0, N_{1}\right), Z_{2} \sim \mathcal{N}\left(0, N_{2}\right)$, and they are independent. The Gaussian noise vectors $Z_{r}^{N}, Z_{1}^{N}$ and $Z_{2}^{N}$ are composed of i.i.d. components with probability distributions $Z_{r} \sim \mathcal{N}\left(0, N_{r}\right), Z_{1} \sim \mathcal{N}\left(0, N_{1}\right)$ and $Z_{2} \sim \mathcal{N}\left(0, N_{2}\right)$, respectively. The average power constraints of $X_{1}^{N}, X_{2}^{N}$ and $X_{r}^{N}$ are $\frac{1}{N} \sum_{i=1}^{N} E\left[X_{1, i}^{2}\right] \leq P_{1}$, $\frac{1}{N} \sum_{i=1}^{N} E\left[X_{2, i}^{2}\right] \leq P_{2}$ and $\frac{1}{N} \sum_{i=1}^{N} E\left[X_{r, i}^{2}\right] \leq P_{r}$, respectively.

The remainder of this section is organized as follows. Subsection III-A shows the achievable secrecy rate regions of GMARC-WT, and the numerical examples and discussions are given in Subsection III-B.

## A. Capacity results on GMARC-WT

Theorem 5: The DF inner bound on the secrecy capacity region of the GMARC-WT is given by

$$
\mathcal{R}^{g 1}=\bigcup_{0 \leq \gamma \leq 1}\left\{\begin{array}{l}
\left(R_{1}, R_{2}\right): R_{1}, R_{2} \geq 0  \tag{3.2}\\
R_{1} \leq \min \left\{\frac{1}{2} \log \left(1+\frac{P_{1}}{N_{r}}\right), \frac{1}{2} \log \left(1+\frac{P_{1}+\gamma P_{r}}{N_{1}}\right)\right\}-\frac{1}{2} \log \frac{P_{1}+P_{2}+P_{r}+N_{2}}{P_{2}+P_{r}+N_{2}}, \\
R_{2} \leq \min \left\{\frac{1}{2} \log \left(1+\frac{P_{2}}{N_{r}}\right), \frac{1}{2} \log \left(1+\frac{P_{2}+(1-\gamma) P_{r}}{N_{1}}\right)\right\}-\frac{1}{2} \log \frac{P_{1}+P_{2}+P_{r}+N_{2}}{P_{1}+P_{r}+N_{2}} \\
R_{1}+R_{2} \leq \min \left\{\frac{1}{2} \log \left(1+\frac{P_{1}+P_{2}}{N_{r}}\right), \frac{1}{2} \log \left(1+\frac{P_{1}+P_{2}+P_{r}}{N_{1}}\right)\right\}-\frac{1}{2} \log \frac{P_{1}+P_{2}+P_{r}+N_{2}}{P_{r}+N_{2}}
\end{array}\right\}
$$

Proof:
First, let $X_{r}=V_{1}+V_{2}$, where $V_{1} \sim \mathcal{N}\left(0, \gamma P_{r}\right)$ and $V_{2} \sim \mathcal{N}\left(0,(1-\gamma) P_{r}\right)$.
Let $X_{1}=\sqrt{\frac{(1-\alpha) P_{1}}{\gamma P_{r}}} V_{1}+X_{10}$, where $0 \leq \alpha \leq 1$ and $X_{10} \sim \mathcal{N}\left(0, \alpha P_{1}\right)$.
Analogously, let $X_{2}=\sqrt{\frac{(1-\beta) P_{2}}{(1-\gamma) P_{r}}} V_{2}+X_{20}$, where $0 \leq \beta \leq 1$ and $X_{20} \sim \mathcal{N}\left(0, \beta P_{2}\right)$.
Here note that $V_{1}, V_{2}, X_{10}$ and $X_{20}$ are independent random variables.
The region $\mathcal{R}^{g 1}$ is obtained by substituting the above definitions into Theorem 1 , and maximizing $\alpha$ and $\beta$ (the maximum of $\mathcal{R}^{g 1}$ is achieved when $\alpha=\beta=1$ ). Thus, the proof of Theorem 5 is completed.

Theorem 6: The NF inner bound on the secrecy capacity region of the GMARC-WT is given by

$$
\mathcal{R}^{g 2}=\text { convex closure of } \quad\left(\mathcal{G}^{1} \bigcup \mathcal{G}^{2}\right)
$$

where $\mathcal{G}^{1}$ is given by

$$
\mathcal{G}^{1}=\bigcup_{N_{1} \leq N_{2}}\left\{\begin{array}{l}
\left(R_{1}, R_{2}\right): R_{1}, R_{2} \geq 0 \\
R_{1} \leq \frac{1}{2} \log \left(1+\frac{P_{1}}{N_{1}}\right)-\frac{1}{2} \log \left(1+\frac{P_{1}+P_{r}}{P_{2}+N_{2}}\right)+R_{r} \\
R_{2} \leq \frac{1}{2} \log \left(1+\frac{P_{2}}{N_{1}}\right)-\frac{1}{2} \log \left(1+\frac{P_{2}+P_{r}}{P_{1}+N_{2}}\right)+R_{r} \\
R_{1}+R_{2} \leq \frac{1}{2} \log \left(1+\frac{P_{1}+P_{2}}{N_{1}}\right)-\frac{1}{2} \log \left(1+\frac{P_{1}+P_{2}+P_{r}}{N_{2}}\right)+R_{r} .
\end{array}\right\}
$$

$R_{r}=\min \left\{\frac{1}{2} \log \left(1+\frac{P_{r}}{P_{1}+P_{2}+N_{1}}\right), \frac{1}{2} \log \left(1+\frac{P_{r}}{P_{2}+N_{2}}\right), \frac{1}{2} \log \left(1+\frac{P_{r}}{P_{1}+N_{2}}\right)\right\}$, and $\mathcal{G}^{2}$ is given by

$$
\mathcal{G}^{2}=\bigcup_{N_{1} \geq N_{2}}\left\{\begin{array}{l}
\left(R_{1}, R_{2}\right): R_{1}, R_{2} \geq 0 \\
R_{1} \leq \frac{1}{2} \log \left(1+\frac{P_{1}}{N_{1}}\right)-\frac{1}{2} \log \left(1+\frac{P_{1}}{P_{2}+N_{2}}\right) \\
R_{2} \leq \frac{1}{2} \log \left(1+\frac{P_{2}}{N_{1}}\right)-\frac{1}{2} \log \left(1+\frac{P_{2}}{P_{1}+N_{2}}\right), \\
R_{1}+R_{2} \leq \frac{1}{2} \log \left(1+\frac{P_{1}+P_{2}}{N_{1}}\right)-\frac{1}{2} \log \left(1+\frac{P_{1}+P_{2}}{N_{2}}\right) .
\end{array}\right\}
$$

Proof:
Here note that $N_{1} \leq N_{2}$ implies $I\left(X_{r} ; Y\right) \geq I\left(X_{r} ; Z\right)$. The region $\mathcal{G}^{1}$ is obtained by substituting $X_{1} \sim \mathcal{N}\left(0, P_{1}\right)$, $X_{2} \sim \mathcal{N}\left(0, P_{2}\right)$ and $X_{r} \sim \mathcal{N}\left(0, P_{r}\right)$ into the region $\mathcal{L}^{1}$ of Theorem 2 and using the fact that $X_{1}, X_{2}$ and $X_{r}$ are independent random variables.

Analogously, $N_{1} \geq N_{2}$ implies $I\left(X_{r} ; Y\right) \leq I\left(X_{r} ; Z\right)$. The region $\mathcal{G}^{2}$ is obtained by substituting $X_{1} \sim \mathcal{N}\left(0, P_{1}\right)$, $X_{2} \sim \mathcal{N}\left(0, P_{2}\right)$ and $X_{r} \sim \mathcal{N}\left(0, P_{r}\right)$ into the region $\mathcal{L}^{2}$ of Theorem 2, and using the fact that $X_{1}, X_{2}$ and $X_{r}$ are independent random variables. Thus, the proof of Theorem 6 is completed.

Theorem 7: The CF inner bound on the secrecy capacity region of the GMARC-WT is given by

$$
\mathcal{R}^{g 3}=\text { convex closure of } \quad\left(\mathcal{G}^{3} \bigcup \mathcal{G}^{4}\right)
$$

where $\mathcal{G}^{3}$ is given by

$$
\mathcal{G}^{3}=\bigcup_{N_{1} \leq N_{2}}\left\{\begin{array}{l}
\left(R_{1}, R_{2}\right): R_{1}, R_{2} \geq 0 \\
R_{1} \leq \frac{1}{2} \log \left(1+\frac{P_{1}\left(Q+N_{1}+N_{r}\right)}{N_{1}\left(N_{r}+Q\right)}\right)-\frac{1}{2} \log \left(1+\frac{P_{1}+P_{r}}{P_{2}+N_{2}}\right)+R^{*} \\
R_{2} \leq \frac{1}{2} \log \left(1+\frac{P_{2}\left(Q+N_{1}+N_{r}\right)}{N_{1}\left(N_{r}+Q\right)}\right)-\frac{1}{2} \log \left(1+\frac{P_{2}+P_{r}}{P_{1}+N_{2}}\right)+R^{*} \\
R_{1}+R_{2} \leq \frac{1}{2} \log \left(1+\frac{\left(P_{1}+P_{2}\right)\left(Q+N_{1}+N_{r}\right)}{N_{1}\left(N_{r}+Q\right)}\right)-\frac{1}{2} \log \left(1+\frac{P_{1}+P_{2}+P_{r}}{N_{2}}\right)+R^{*} .
\end{array}\right\}
$$

$Q$ satisfies

$$
\frac{1}{2} \log \left(1+\frac{P_{1}+P_{2}+N_{r}}{Q}\right) \leq \min \left\{\frac{1}{2} \log \left(1+\frac{P_{r}}{P_{1}+P_{2}+N_{1}}\right), \frac{1}{2} \log \left(1+\frac{P_{r}}{P_{2}+N_{2}}\right), \frac{1}{2} \log \left(1+\frac{P_{r}}{P_{1}+N_{2}}\right)\right\}
$$

and $R^{*}$ satisfies

$$
\begin{aligned}
0 \leq R^{*} \leq & \min \left\{\frac{1}{2} \log \left(1+\frac{P_{r}}{P_{1}+P_{2}+N_{1}}\right), \frac{1}{2} \log \left(1+\frac{P_{r}}{P_{2}+N_{2}}\right), \frac{1}{2} \log \left(1+\frac{P_{r}}{P_{1}+N_{2}}\right)\right\} \\
& -\frac{1}{2} \log \left(1+\frac{P_{1}+P_{2}+N_{r}}{Q}\right)
\end{aligned}
$$

and $\mathcal{G}^{4}$ is given by

$$
\mathcal{G}^{4}=\bigcup_{N_{1} \geq N_{2}}\left\{\begin{array}{l}
\left(R_{1}, R_{2}\right): R_{1}, R_{2} \geq 0 \\
R_{1} \leq \frac{1}{2} \log \left(1+\frac{P_{1}\left(Q+N_{1}+N_{r}\right)}{N_{1}\left(N_{r}+Q\right)}\right)-\frac{1}{2} \log \left(1+\frac{P_{1}}{P_{2}+N_{2}}\right) \\
R_{2} \leq \frac{1}{2} \log \left(1+\frac{P_{2}\left(Q+N_{1}+N_{r}\right)}{N_{1}\left(N_{r}+Q\right)}\right)-\frac{1}{2} \log \left(1+\frac{P_{2}}{P_{1}+N_{2}}\right) \\
R_{1}+R_{2} \leq \frac{1}{2} \log \left(1+\frac{\left(P_{1}+P_{2}\right)\left(Q+N_{1}+N_{r}\right)}{N_{1}\left(N_{r}+Q\right)}\right)-\frac{1}{2} \log \left(1+\frac{P_{1}+P_{2}}{N_{2}}\right)
\end{array}\right\}
$$

here $Q$ satisfies $Q \geq \frac{\left(P_{1}+P_{2}\right)^{2}+\left(P_{1}+P_{2}\right)\left(N_{r}+N_{1}\right)+N_{r} N_{1}}{P_{r}}$.
Proof:
Here note that $N_{1} \leq N_{2}$ implies $I\left(X_{r} ; Y\right) \geq I\left(X_{r} ; Z\right)$. The region $\mathcal{G}^{3}$ is obtained by substituting $X_{1} \sim \mathcal{N}\left(0, P_{1}\right)$, $X_{2} \sim \mathcal{N}\left(0, P_{2}\right), X_{r} \sim \mathcal{N}\left(0, P_{r}\right), \hat{Y}_{r}=Y_{r}+Z_{Q}{ }^{1}$ and $Z_{Q} \sim \mathcal{N}(0, Q)$ into the region $\mathcal{L}^{3}$ of Theorem 3, and using the fact that $X_{1}, X_{2}$ and $X_{r}$ are independent random variables.

Analogously, $N_{1} \geq N_{2}$ implies $I\left(X_{r} ; Y\right) \leq I\left(X_{r} ; Z\right)$. The region $\mathcal{G}^{4}$ is obtained by substituting $X_{1} \sim \mathcal{N}\left(0, P_{1}\right)$, $X_{2} \sim \mathcal{N}\left(0, P_{2}\right), X_{r} \sim \mathcal{N}\left(0, P_{r}\right), \hat{Y}_{r}=Y_{r}+Z_{Q}$ and $Z_{Q} \sim \mathcal{N}(0, Q)$ into the region $\mathcal{L}^{4}$ of Theorem 3 and using the fact that $X_{1}, X_{2}$ and $X_{r}$ are independent random variables. Thus, the proof of Theorem 7 is completed.

By using Theorem 4, we provide an outer bound on the secrecy capacity region of the GMARC-WT under the condition that $N_{2} \geq N_{1}$, see the followings.
${ }^{1}$ Here note that $\hat{Y}_{r}=Y_{r}+Z_{Q}$ is from the similar argument for the CF strategy of the Gaussian relay channel [28] pp. 402-403].

Theorem 8: For the case that $N_{2} \geq N_{1}$, an outer bound $\mathcal{R}^{\text {gout }}$ on the secrecy capacity region of the GMARC-WT is given by

$$
\mathcal{R}^{\text {gout }}=\bigcup_{0 \leq \alpha, \beta_{1}, \beta_{2}, \gamma \leq 1}\left\{\begin{array}{l}
\left(R_{1}, R_{2}\right): R_{1} \geq 0, R_{2} \geq 0, \\
R_{1} \leq \frac{1}{2} \log \left(1+\frac{P_{r}\left(\alpha+\beta_{2}-\alpha \beta_{2}\right)+\beta_{2} P_{1}}{N_{1}}\right)-\frac{1}{2} \log \left(\frac{C+\gamma\left(P_{1}+P_{2}+P_{r}+N_{2}-C\right)}{N_{2}+P_{r}\left(\alpha+\beta_{1}-\alpha \beta_{1}\right)+\beta_{1} P_{2}}\right), \\
R_{2} \leq \frac{1}{2} \log \left(1+\frac{P_{r}\left(\alpha+\beta_{1}-\alpha \beta_{1}\right)+\beta_{1} P_{2}}{N_{1}}\right)-\frac{1}{2} \log \left(\frac{C+\gamma\left(P_{1}+P_{2}+P_{r}+N_{2}-C\right)}{N_{2}+P_{r}\left(\alpha+\beta_{2}-\alpha \beta_{2}\right)+\beta_{2} P_{1}}\right), \\
R_{1}+R_{2} \leq \frac{1}{2} \log \left(\frac{C+\gamma\left(P_{1}+P_{2}+P_{r}+N_{1}-C\right)}{N_{1}}\right)-\frac{1}{2} \log \left(\frac{C+\gamma\left(P_{1}+P_{2}+P_{r}+N_{2}-C\right)}{N_{2}+\alpha P_{r}}\right),
\end{array}\right\}
$$

where $C$ satisfies

$$
C=\max \left\{N_{2}+P_{r}\left(\alpha+\beta_{1}-\alpha \beta_{1}\right)+\beta_{1} P_{2}, N_{2}+P_{r}\left(\alpha+\beta_{2}-\alpha \beta_{2}\right)+\beta_{2} P_{1}\right\} .
$$

Proof:
See Appendix E

Theorem 9: Finally, remember that [9] provides an achievable secrecy rate region $\mathcal{R}^{G i}$ of the Gaussian multipleaccess wiretap channel (GMAC-WT), and it is given by

$$
\mathcal{R}^{G i}=\left\{\begin{array}{l}
\left(R_{1}, R_{2}\right): R_{1}, R_{2} \geq 0 \\
R_{1} \leq \frac{1}{2} \log \left(1+\frac{P_{1}}{N_{1}}\right)-\frac{1}{2} \log \left(1+\frac{P_{1}}{N_{2}+P_{2}}\right) \\
R_{2} \leq \frac{1}{2} \log \left(1+\frac{P_{2}}{N_{1}}\right)-\frac{1}{2} \log \left(1+\frac{P_{2}}{N_{2}+P_{1}}\right) \\
R_{1}+R_{2} \leq \frac{1}{2} \log \left(1+\frac{P_{1}+P_{2}}{N_{1}}\right)-\frac{1}{2} \log \left(1+\frac{P_{1}+P_{2}}{N_{2}}\right)
\end{array}\right\}
$$

Proof:
The proof is in [9], and it is omitted here.

## B. Numerical Examples and Discussions

Letting $P_{1}=5, P_{2}=6, P_{r}=20, N_{1}=2, N_{2}=14$ and $Q=200$, the following Figure 2, 3, 4 and 5 show the inner and outer bounds on the secrecy capacity region of the GMARC-WT for different values of $N_{r}$.

Compared with the achievable secrecy rate region $\mathcal{R}^{G i}$ of GMAC-WT, it is easy to see that the NF region ( $\mathcal{R}^{g 2}$ ) and the CF region $\left(\mathcal{R}^{g 3}\right)$ enhance the region $\mathcal{R}^{G i}$ (no relay). The CF region is always smaller than the NF region, and when $Q \rightarrow \infty$, the CF region tends to the NF region. For the DF region $\left(\mathcal{R}^{g 1}\right)$, we find that when $N_{r}$ is much larger than $N_{1}, \mathcal{R}^{g 1}$ is even smaller than $\mathcal{R}^{G i}$ (see Figure 2). When $N_{r}$ is close to $N_{1}$ (still larger than $N_{1}$ ), $\mathcal{R}^{g 1}$ is larger than $\mathcal{R}^{G i}$, but it is still smaller than the NF and CF regions (see Figure 3). When $N_{r}$ is smaller than $N_{1}$, as we can see in Figure 4 and 5, the DF region $\mathcal{R}^{g 1}$ is larger than the NF and CF regions.

Figure $2,3,4$ and 5 also show that there exists a gap between the inner and outer bounds, and the gap is reduced as $N_{r}$ decreases.


Fig. 2: The bounds on the secrecy capacity region of GMARC-WT for $N_{r}=5$


Fig. 3: The bounds on the secrecy capacity region of GMARC-WT for $N_{r}=2.3$

## IV. Conclusion

In this paper, first, we provide three inner bounds on the secrecy capacity region (achievable secrecy rate regions) of the discrete memoryless model of Figure 1. The decode-forward (DF), noise-forward (NF), and compress-forward $(\mathrm{CF})$ relay strategies are used in the construction of these inner bounds. Second, we investigate the degraded discrete memoryless MARC-WT, and present an outer bound on the secrecy capacity region of this degraded case. Finally,


Fig. 4: The bounds on the secrecy capacity region of GMARC-WT for $N_{r}=1.6$


Fig. 5: The bounds on the secrecy capacity region of GMARC-WT for $N_{r}=0$
we study the Gaussian MARC-WT, and find that the NF and CF strategies help to enhance Tekin-Yener's achievable secrecy rate region of Gaussian MAC-WT. Moreover, we find that if the channel from the transmitters to the relay is less noisy than the channels from the transmitters to the legitimate receiver and the wiretapper, the achievable secrecy rate region of the DF strategy is even larger than the corresponding regions of the NF and CF strategies.

## Acknowledgement

The authors would like to thank Professor Ning Cai for his valuable suggestions to improve this paper. This work was supported by a sub-project in National Basic Research Program of China under Grant 2012CB316100 on Broadband Mobile Communications at High Speeds, the National Natural Science Foundation of China under Grant 61301121, and the Fundamental Research Funds for the Central Universities under Grant 2682014CX099.

## Appendix A

## Proof of Theorem 1

In order to prove Theorem 1, we need to show that any pair $\left(R_{1}, R_{2}\right) \in \mathcal{R}^{d 1}$ is achievable, i.e., for any $\epsilon>0$, there exists a sequence of codes $\left(2^{N R_{1}}, 2^{N R_{2}}, N\right)$ such that $\frac{\log \left\|\mathcal{W}_{1}\right\|}{N}=R_{1}, \frac{\log \left\|\mathcal{W}_{2}\right\|}{N}=R_{2}, P_{e} \leq \epsilon$ and $\frac{1}{N} H\left(W_{1}, W_{2} \mid Z^{N}\right) \geq R_{1}+R_{2}-\epsilon$. The details are as follows.

The coding scheme combines the decode-and-forward (DF) strategy of MARC [21], random binning, superposition coding, and block Markov coding techniques, see the followings.

Fix the joint probability mass function $P_{Y, Z, Y_{r} \mid X_{r}, X_{1}, X_{2}}\left(y, z, y_{r} \mid x_{r}, x_{1}, x_{2}\right) P_{X_{r} \mid V_{1}, V_{2}}\left(x_{r} \mid v_{1}, v_{2}\right)$ $P_{X_{1} \mid V_{1}}\left(x_{1} \mid v_{1}\right) P_{X_{2} \mid V_{2}}\left(x_{2} \mid v_{2}\right) P_{V_{1}}\left(v_{1}\right) P_{V_{2}}\left(v_{2}\right)$. For a given $\left(R_{1}, R_{2}\right) \in \mathcal{R}^{d 1}$, define the messages $W_{1}$ and $W_{2}$ taking values in the alphabets $\mathcal{W}_{1}$ and $\mathcal{W}_{2}$, respectively, where

$$
\mathcal{W}_{1}=\left\{1,2, \ldots, 2^{N R_{1}}\right\}, \quad \mathcal{W}_{2}=\left\{1,2, \ldots, 2^{N R_{2}}\right\}
$$

## Relay Code-books Construction:

For a given $R_{1}^{*} \geq 0$, generate at random $2^{N\left(R_{1}+R_{1}^{*}\right)}$ i.i.d. sequences $v_{1}^{N}$ according to $P_{V_{1}^{N}}\left(v_{1}^{N}\right)=\prod_{i=1}^{N} P_{V_{1}}\left(v_{1, i}\right)$. Index them as $v_{1}^{N}\left(a_{1}, b_{1}\right)$, where $a_{1} \in\left\{1,2, \ldots, 2^{N R_{1}}\right\}$ and $b_{1} \in\left\{1,2, \ldots, 2^{N R_{1}^{*}}\right\}$. For convenience, define $s_{1}=$ $\left(a_{1}, b_{1}\right)$, where $s_{1} \in\left\{1,2, \ldots, 2^{N\left(R_{1}+R_{1}^{*}\right)}\right\}$.

Analogously, for a given $R_{2}^{*} \geq 0$, generate at random $2^{N\left(R_{2}+R_{2}^{*}\right)}$ i.i.d. sequences $v_{2}^{N}$ according to $P_{V_{2}^{N}}\left(v_{2}^{N}\right)=$ $\prod_{i=1}^{N} P_{V_{2}}\left(v_{2, i}\right)$. Index them as $v_{2}^{N}\left(a_{2}, b_{2}\right)$, where $a_{2} \in\left\{1,2, \ldots, 2^{N R_{2}}\right\}$ and $b_{2} \in\left\{1,2, \ldots, 2^{N R_{2}^{*}}\right\}$. For convenience, define $s_{2}=\left(a_{2}, b_{2}\right)$, where $s_{2} \in\left\{1,2, \ldots, 2^{N\left(R_{2}+R_{2}^{*}\right)}\right\}$.

Generate at random $2^{N\left(R_{1}+R_{1}^{*}+R_{2}+R_{2}^{*}\right)}$ i.i.d. sequences $x_{r}^{N}$ according to $P_{X_{r}^{N} \mid V_{1}^{N}, V_{2}^{N}}\left(x_{r}^{N} \mid v_{1}^{N}, v_{2}^{N}\right)=$ $\prod_{i=1}^{N} P_{X_{r, i} \mid V_{1, i}, V_{2, i}}\left(x_{r, i} \mid v_{1, i}, v_{2, i}\right)$. Index them as $x_{r}^{N}\left(s_{1}, s_{2}\right)$, where $s_{1} \in\left\{1,2, \ldots, 2^{N\left(R_{1}+R_{1}^{*}\right)}\right\}$ and $s_{2} \in\left\{1,2, \ldots, 2^{N\left(R_{2}+R_{2}^{*}\right)}\right\}$.

## Transmitters' Code-books Construction:

- For a given $v_{1}^{N}\left(s_{1}\right)$, generate at random $2^{N\left(R_{1}+R_{1}^{*}\right)}$ i.i.d. sequences $x_{1}^{N}\left(w_{1}, w_{1}^{*} \mid s_{1}\right)\left(w_{1} \in\left\{1,2, \ldots, 2^{N R_{1}}\right\}\right.$, $w_{1}^{*} \in$ $\left\{1,2, \ldots, 2^{N R_{1}^{*}}\right\}, s_{1} \in\left\{1,2, \ldots, 2^{N\left(R_{1}+R_{1}^{*}\right)}\right\}$ ) according to $\prod_{i=1}^{N} P_{X_{1} \mid V_{1}}\left(x_{1, i} \mid v_{1, i}\right)$.
- Analogously, for a given $v_{2}^{N}\left(s_{2}\right)$, generate at random $2^{N\left(R_{2}+R_{2}^{*}\right)}$ i.i.d. sequences $x_{2}^{N}\left(w_{2}, w_{2}^{*} \mid s_{2}\right)\left(w_{2} \in\right.$ $\left.\left\{1,2, \ldots, 2^{N R_{2}}\right\}, w_{2}^{*} \in\left\{1,2, \ldots, 2^{N R_{2}^{*}}\right\}, s_{2} \in\left\{1,2, \ldots, 2^{N\left(R_{2}+R_{2}^{*}\right)}\right\}\right)$ according to $\prod_{i=1}^{N} P_{X_{2} \mid V_{2}}\left(x_{2, i} \mid v_{2, i}\right)$.

Encoding: We exploit the block Markov coding scheme, because, as argued in [23], the loss induced by this scheme is negligible as the number of blocks $n \rightarrow \infty$. For block $i(1 \leq i \leq n)$, encoding proceeds as follows.

First, for convenience, the messages $w_{1}, w_{1}^{*}, w_{2}, w_{2}^{*}, s_{1}$ and $s_{2}$ transmitted in the $i$-th block are denoted by $w_{1, i}$, $w_{1, i}^{*}, w_{2, i}, w_{2, i}^{*}, s_{1, i}$ and $s_{2, i}$, respectively.

## - (Channel encoders)

1) The message $w_{1, i}^{*}(1 \leq i \leq n-1)$ is randomly chosen from the set $\left\{1,2, \ldots, 2^{N R_{1}^{*}}\right\}$. The transmitter 1 (encoder 1) sends $x_{1}^{N}\left(w_{1,1}, w_{1,1}^{*} \mid 1,1\right)$ at the first block, $x_{1}^{N}\left(w_{1, i}, w_{1, i}^{*} \mid w_{1, i-1}, w_{1, i-1}^{*}\right)$ (note that here $s_{1, i}=$ $\left(w_{1, i-1}, w_{1, i-1}^{*}\right)$ ) from block $2 \leq i \leq n-1$, and $x_{1}^{N}\left(1,1 \mid w_{1, n-1}, w_{1, n-1}^{*}\right)$ at block $n\left(s_{1, n}=\left(w_{1, n-1}, w_{1, n-1}^{*}\right)\right.$ ).
2) The message $w_{2, i}^{*}(1 \leq i \leq n-1)$ is randomly chosen from the set $\left\{1,2, \ldots, 2^{N R_{2}^{*}}\right\}$. The transmitter 2 (encoder 2) sends $x_{2}^{N}\left(w_{2,1}, w_{2,1}^{*} \mid 1,1\right)$ at the first block, $x_{2}^{N}\left(w_{2, i}, w_{2, i}^{*} \mid w_{2, i-1}, w_{2, i-1}^{*}\right)\left(s_{2, i}=\left(w_{2, i-1}, w_{2, i-1}^{*}\right)\right)$ from block $2 \leq i \leq n-1$, and $x_{2}^{N}\left(1,1 \mid w_{2, n-1}, w_{2, n-1}^{*}\right)$ at block $n\left(s_{2, n}=\left(w_{2, n-1}, w_{2, n-1}^{*}\right)\right.$ ).

- (Relay encoder)

The relay sends $\left(v_{1}^{N}(1,1), v_{2}^{N}(1,1), x_{r}^{N}(1,1,1,1)\right)$ at the first block, and $\left(v_{1}^{N}\left(\hat{s}_{1, i}\right), v_{2}^{N}\left(\hat{s}_{2, i}\right), x_{r}^{N}\left(\hat{s}_{1, i}, \hat{s}_{2, i}\right)\right)$ from block $2 \leq i \leq n$, where $\hat{s}_{1, i}=\left(\hat{w}_{1, i-1}, \hat{w}_{1, i-1}^{*}\right)$ and $\hat{s}_{2, i}=\left(\hat{w}_{2, i-1}, \hat{w}_{2, i-1}^{*}\right)$.

Decoding: Decoding proceeds as follows.

1) (At the relay) At the end of block $i(1 \leq i \leq n)$, the relay already has an estimation of the $s_{1, i}$ and $s_{2, i}$ (denoted by $\hat{s}_{1, i}$ and $\hat{s}_{2, i}$, respectively), and will declare that it receives $\hat{w}_{1, i}, \hat{w}_{1, i}^{*}, \hat{w}_{2, i}$ and $\hat{w}_{2, i}^{*}$ if this is the only quadruple such that $\left(x_{1}^{N}\left(\hat{w}_{1, i}, \hat{w}_{1, i}^{*} \mid \hat{s}_{1, i}\right), x_{2}^{N}\left(\hat{w}_{2, i}, \hat{w}_{2, i}^{*} \mid \hat{s}_{2, i}\right), x_{r}^{N}\left(\hat{s}_{1, i}, \hat{s}_{2, i}\right), v_{1}\left(\hat{s}_{1, i}\right), v_{2}\left(\hat{s}_{2, i}\right), y_{r}^{N}(i)\right)$ are jointly typical. Here note that $y_{r}^{N}(i)$ indicates the output sequence $y_{r}^{N}$ in block $i, \hat{s}_{1, i+1}=\left(\hat{w}_{1, i}, \hat{w}_{1, i}^{*}\right)$ and $\hat{s}_{2, i+1}=\left(\hat{w}_{2, i}, \hat{w}_{2, i}^{*}\right)$. The indexes $\hat{s}_{1, i+1}$ and $\hat{s}_{2, i+1}$ will be used in the $i+1$-th block.

Based on the AEP, the error probability $\operatorname{Pr}\left\{\left(\hat{s}_{1, i+1}, \hat{s}_{2, i+1}\right) \neq\left(s_{1, i+1}, s_{2, i+1}\right)\right\}$ goes to 0 if

$$
\begin{gather*}
R_{1}+R_{1}^{*} \leq I\left(X_{1} ; Y_{r} \mid X_{r}, V_{1}, V_{2}, X_{2}\right)  \tag{A1}\\
R_{2}+R_{2}^{*} \leq I\left(X_{2} ; Y_{r} \mid X_{r}, V_{1}, V_{2}, X_{1}\right)  \tag{A2}\\
R_{1}+R_{1}^{*}+R_{2}+R_{2}^{*} \leq I\left(X_{1}, X_{2} ; Y_{r} \mid X_{r}, V_{1}, V_{2}\right) . \tag{A3}
\end{gather*}
$$

2) (At the legitimate receiver) The legitimate receiver decodes from the last block, i.e., block $n$. At the end of block $i+1$, the legitimate receiver already has an estimation of the $\breve{w}_{1, i+1}, \check{w}_{1, i+1}^{*}, \check{w}_{2, i+1}$ and $\check{w}_{2, i+1}^{*}$, and will declare that it receives $\check{s}_{1, i+1}$ and $\check{s}_{2, i+1}$ if this is the only pair such that $\left(x_{1}^{N}\left(\check{w}_{1, i+1}, \breve{w}_{1, i+1}^{*} \mid \check{s}_{1, i+1}\right), x_{2}^{N}\left(\check{w}_{2, i+1}\right.\right.$, $\left.\left.\check{w}_{2, i+1}^{*} \mid \check{s}_{2, i+1}\right), x_{r}^{N}\left(\check{s}_{1, i+1}, \check{s}_{2, i+1}\right), v_{1}\left(\check{s}_{1, i+1}\right), v_{2}\left(\check{s}_{2, i+1}\right), y^{N}(i+1)\right)$ are jointly typical. Here note that $y^{N}(i+1)$ indicates the output sequence $y^{N}$ in block $i+1, \check{s}_{1, i+1}=\left(\check{w}_{1, i}, \check{w}_{1, i}^{*}\right)$ and $\check{s}_{2, i+1}=\left(\check{w}_{2, i}, \check{w}_{2, i}^{*}\right)$.

Based on the AEP, the error probability $\operatorname{Pr}\left\{\left(\check{s}_{1, i+1}, \check{s}_{2, i+1}\right) \neq\left(s_{1, i+1}, s_{2, i+1}\right)\right\}$ goes to 0 if

$$
\begin{gather*}
R_{1}+R_{1}^{*} \leq I\left(V_{1}, X_{r}, X_{1} ; Y \mid V_{2}, X_{2}\right) \stackrel{(a)}{=} I\left(X_{r}, X_{1} ; Y \mid X_{2}, V_{2}\right),  \tag{A4}\\
R_{2}+R_{2}^{*} \leq I\left(V_{2}, X_{r}, X_{2} ; Y \mid V_{1}, X_{1}\right) \stackrel{(b)}{=} I\left(X_{r}, X_{2} ; Y \mid X_{1}, V_{1}\right),  \tag{A5}\\
R_{1}+R_{1}^{*}+R_{2}+R_{2}^{*} \leq I\left(V_{1}, V_{2}, X_{r}, X_{1}, X_{2} ; Y\right) \stackrel{(c)}{=} I\left(X_{r}, X_{1}, X_{2} ; Y\right), \tag{A6}
\end{gather*}
$$

where (a) is from the Markov chain $V_{1} \rightarrow\left(X_{r}, X_{1}, X_{2}, V_{2}\right) \rightarrow Y$, (b) is from the Markov chain $V_{2} \rightarrow\left(X_{r}, X_{1}, X_{2}, V_{1}\right) \rightarrow$ $Y$, and (c) is from the Markov chain $\left(V_{1}, V_{2}\right) \rightarrow\left(X_{r}, X_{1}, X_{2}\right) \rightarrow Y$.

By using A1, A2, A3, A4, A5 and A6, it is easy to check that $P_{e} \leq \epsilon$. It remains to show that $\Delta \geq R_{1}+R_{2}-\epsilon$, see the followings.

## Equivocation Analysis:

Similar to the equivocation analysis of [18, proof of Theorem 2], for simplicity, we only focus on the equivocation of one block, see the followings.

$$
\begin{align*}
\frac{1}{N} H\left(W_{1}, W_{2} \mid Z^{N}\right) & =\frac{1}{N}\left(H\left(W_{1}, W_{2}, Z^{N}\right)-H\left(Z^{N}\right)\right) \\
& =\frac{1}{N}\left(H\left(W_{1}, W_{2}, Z^{N}, X_{1}^{N}, X_{2}^{N}\right)-H\left(X_{1}^{N}, X_{2}^{N} \mid W_{1}, W_{2}, Z^{N}\right)-H\left(Z^{N}\right)\right) \\
& \stackrel{(a)}{=} \frac{1}{N}\left(H\left(Z^{N} \mid X_{1}^{N}, X_{2}^{N}\right)+H\left(X_{1}^{N}\right)+H\left(X_{2}^{N}\right)-H\left(X_{1}^{N}, X_{2}^{N} \mid W_{1}, W_{2}, Z^{N}\right)-H\left(Z^{N}\right)\right) \\
& =\frac{1}{N}\left(H\left(X_{1}^{N}\right)+H\left(X_{2}^{N}\right)-I\left(X_{1}^{N}, X_{2}^{N} ; Z^{N}\right)-H\left(X_{1}^{N}, X_{2}^{N} \mid W_{1}, W_{2}, Z^{N}\right)\right) \tag{A7}
\end{align*}
$$

where (a) follows from $\left(W_{1}, W_{2}\right) \rightarrow\left(X_{1}^{N}, X_{2}^{N}\right) \rightarrow Z^{N}, H\left(W_{1} \mid X_{1}^{N}\right)=0, H\left(W_{2} \mid X_{2}^{N}\right)=0$, and $X_{1}^{N}$ is independent of $X_{2}^{N}$.

Consider the first term of A7), the code-book generation of $x_{1}^{N}$ shows that the total number of $x_{1}^{N}$ is $2^{N\left(R_{1}+R_{1}^{*}\right)}$. Thus, using the same approach as that in [7, Lemma 3], we have

$$
\begin{equation*}
\frac{1}{N} H\left(X_{1}^{N}\right) \geq R_{1}+R_{1}^{*}-\epsilon_{1, N} \tag{A8}
\end{equation*}
$$

where $\epsilon_{1, N} \rightarrow 0$ as $N \rightarrow \infty$.
Analogously, the second term of A7 is bounded by

$$
\begin{equation*}
\frac{1}{N} H\left(X_{2}^{N}\right) \geq R_{2}+R_{2}^{*}-\epsilon_{2, N} \tag{A9}
\end{equation*}
$$

where $\epsilon_{2, N} \rightarrow 0$ as $N \rightarrow \infty$.
For the third term of A7, since the channel is memoryless, and $X_{1}^{N}, X_{2}^{N}, X_{r}^{N}$ are i.i.d. generated, we get

$$
\begin{equation*}
\frac{1}{N} I\left(X_{1}^{N}, X_{2}^{N} ; Z^{N}\right)=I\left(X_{1}, X_{2} ; Z\right) \tag{A10}
\end{equation*}
$$

Now, we consider the last term of A7. Given $W_{1}$ and $W_{2}$, the wiretapper does joint decoding at each block. At the end of block 1, the wiretapper tries to find a unique pair $\left(\tilde{w}_{1,1}^{*}, \tilde{w}_{2,1}^{*}\right)$ such that $\left(x_{1}^{N}\left(w_{1,1}, \tilde{w}_{1,1}^{*} \mid 1,1\right), x_{2}^{N}\left(w_{2,1}, \tilde{w}_{2,1}^{*} \mid 1,1\right), z^{N}(1)\right)$ are jointly typical. At the end of block $i(2 \leq i \leq n-1)$, the wiretapper already has an estimation of the $\tilde{w}_{1, i-1}^{*}$ and $\tilde{w}_{2, i-1}^{*}$, and thus he also get $\tilde{s}_{1, i}=\left(w_{1, i-1}, \tilde{w}_{1, i-1}^{*}\right)$ and $\tilde{s}_{2, i}=$ $\left(w_{2, i-1}, \tilde{w}_{2, i-1}^{*}\right)$. Then he tries to find a unique pair $\left(\tilde{w}_{1, i}^{*}, \tilde{w}_{2, i}^{*}\right)$ such that $\left(x_{1}^{N}\left(w_{1, i}, \tilde{w}_{1, i}^{*} \mid \tilde{s}_{1, i}\right), x_{2}^{N}\left(w_{2, i}, \tilde{w}_{2, i}^{*} \mid \tilde{s}_{2, i}\right), z^{N}(i)\right)$ are jointly typical. Based on the AEP, the error probability $\operatorname{Pr}\left\{\left(\tilde{w}_{1, i}^{*}, \tilde{w}_{2, i}^{*}\right) \neq\left(w_{1, i}^{*}, w_{2, i}^{*}\right)\right\}$ goes to 0 if

$$
\begin{gather*}
R_{1}^{*} \leq I\left(X_{1} ; Z \mid X_{2}\right)  \tag{A11}\\
R_{2}^{*} \leq I\left(X_{2} ; Z \mid X_{1}\right)  \tag{A12}\\
R_{1}^{*}+R_{2}^{*} \leq I\left(X_{1}, X_{2} ; Z\right) \tag{A13}
\end{gather*}
$$

Then based on Fanos inequality, we have

$$
\begin{equation*}
\frac{1}{N} H\left(X_{1}^{N}, X_{2}^{N} \mid W_{1}, W_{2}, Z^{N}\right) \leq \epsilon_{3, N} \tag{A14}
\end{equation*}
$$

where $\epsilon_{3, N} \rightarrow 0$ as $N \rightarrow \infty$.
Substituting (A8, (A9, A10) and A14) into A7), we have

$$
\begin{equation*}
\frac{1}{N} H\left(W_{1}, W_{2} \mid Z^{N}\right) \geq R_{1}+R_{1}^{*}+R_{2}+R_{2}^{*}-I\left(X_{1}, X_{2} ; Z\right)-\epsilon_{1, N}-\epsilon_{2, N}-\epsilon_{3, N} . \tag{A15}
\end{equation*}
$$

It is easy to see that if we let

$$
\begin{equation*}
R_{1}^{*}+R_{2}^{*}=I\left(X_{1}, X_{2} ; Z\right) \tag{A16}
\end{equation*}
$$

and choose sufficiently large $N$ such that $\epsilon_{1, N}+\epsilon_{2, N}+\epsilon_{3, N} \leq \epsilon, \Delta=\frac{1}{N} H\left(W_{1}, W_{2} \mid Z^{N}\right) \geq R_{1}+R_{2}-\epsilon$ is guaranteed.

Based on A1, A2, A3, A4, A5, A6, A11, A12, and A16, the achievable region $\mathcal{R}^{d 1}$ is obtained. The proof of Theorem 1 is completed.

## Appendix B

## Proof of Theorem 2

For Theorem 2, we only need to prove that the corner points of $\mathcal{L}^{1}$ and $\mathcal{L}^{2}$ are achievable, see the followings.

- (Case 1) If $I\left(X_{r} ; Y\right) \geq I\left(X_{r} ; Z\right)$, we allow the legitimate receiver to decode $x_{r}^{N}$, and the wiretapper can not decode it. For case 1 , it is sufficient to show that the pair $\left(R_{1}, R_{2}\right) \in \mathcal{L}^{1}$ with the condition

$$
\begin{equation*}
R_{1}=I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)-I\left(X_{1}, X_{r} ; Z\right)+R_{r}, \quad R_{2}=I\left(X_{2} ; Y \mid X_{r}\right)-I\left(X_{2} ; Z \mid X_{1}, X_{r}\right) \tag{A17}
\end{equation*}
$$

is achievable. The achievability proof of the other corner point $\left(R_{1}=I\left(X_{1} ; Y \mid X_{r}\right)-I\left(X_{1} ; Z \mid X_{2}, X_{r}\right), R_{2}=\right.$ $\left.I\left(X_{2} ; Y \mid X_{1}, X_{r}\right)-I\left(X_{2}, X_{r} ; Z\right)+R_{r}\right)$ follows by symmetry.

- (Case 2) If $I\left(X_{r} ; Y\right) \leq I\left(X_{r} ; Z\right)$, we allow both the receivers to decode $x_{r}^{N}$. For case 2, it is sufficient to show that the pair $\left(R_{1}, R_{2}\right) \in \mathcal{L}^{2}$ with the condition

$$
\begin{equation*}
R_{1}=I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)-I\left(X_{1} ; Z \mid X_{r}\right), \quad R_{2}=I\left(X_{2} ; Y \mid X_{r}\right)-I\left(X_{2} ; Z \mid X_{1}, X_{r}\right) \tag{A18}
\end{equation*}
$$

is achievable. The achievability proof of the other corner point $\left(R_{1}=I\left(X_{1} ; Y \mid X_{r}\right)-I\left(X_{1} ; Z \mid X_{2}, X_{r}\right), R_{2}=\right.$ $\left.I\left(X_{2} ; Y \mid X_{1}, X_{r}\right)-I\left(X_{2} ; Z \mid X_{r}\right)\right)$ follows by symmetry.

Fix the joint probability mass function $P_{Y, Z, Y_{r} \mid X_{r}, X_{1}, X_{2}}\left(y, z, y_{r} \mid x_{r}, x_{1}, x_{2}\right) P_{X_{r}}\left(x_{r}\right) P_{X_{1}}\left(x_{1}\right) P_{X_{2}}\left(x_{2}\right)$. Define the messages $W_{1}, W_{2}$ taking values in the alphabets $\mathcal{W}_{1}, \mathcal{W}_{2}$, respectively, where

$$
\mathcal{W}_{1}=\left\{1,2, \ldots, 2^{N R_{1}}\right\}, \quad \mathcal{W}_{2}=\left\{1,2, \ldots, 2^{N R_{2}}\right\}
$$

## Code-book Construction for the Two Cases:

## - Code-book construction for case 1 :

- First, generate at random $2^{N\left(R_{r}-\epsilon^{\prime}\right)}$ (where $\epsilon^{\prime}$ is a small positive number) i.i.d. sequences at the relay node each drawn according to $P_{X_{r}^{N}}\left(x_{r}^{N}\right)=\prod_{i=1}^{N} P_{X_{r}}\left(x_{r, i}\right)$, index them as $x_{r}^{N}(a), a \in\left[1,2^{N\left(R_{r}-\epsilon^{\prime}\right)}\right]$, where

$$
\begin{equation*}
R_{r}=\min \left\{I\left(X_{r} ; Z \mid X_{1}\right), I\left(X_{r} ; Z \mid X_{2}\right), I\left(X_{r} ; Y\right)\right\} \tag{A19}
\end{equation*}
$$

Here note that

$$
\begin{equation*}
R_{r} \geq I\left(X_{r} ; Z\right) \tag{A20}
\end{equation*}
$$

- Second, generate $2^{N\left(I\left(X_{2} ; Y \mid X_{r}\right)-\epsilon^{\prime}\right)}$ i.i.d. codewords $x_{2}^{N}$ according to $P_{X_{2}}\left(x_{2}\right)$, and divide them into $2^{N R_{2}}$ bins. Each bin contains $2^{N\left(I\left(X_{2} ; Y \mid X_{r}\right)-\epsilon^{\prime}-R_{2}\right)}$ codewords, where

$$
\begin{equation*}
I\left(X_{2} ; Y \mid X_{r}\right)-\epsilon^{\prime}-R_{2}=I\left(X_{2} ; Z \mid X_{1}, X_{r}\right)-\epsilon^{\prime} \tag{A21}
\end{equation*}
$$

- Third, generate $2^{N\left(I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)-\epsilon^{\prime}\right)}$ i.i.d. codewords $x_{1}^{N}$ according to $P_{X_{1}}\left(x_{1}\right)$, and divide them into $2^{N R_{1}}$ bins. Each bin contains $2^{N\left(I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)-\epsilon^{\prime}-R_{1}\right)}$ codewords.


## - Code-book Construction for case 2:

- Generate at random $2^{N\left(R_{r}-\epsilon^{\prime}\right)}$ i.i.d. sequences at the relay node each drawn according to $P_{X_{r}^{N}}\left(x_{r}^{N}\right)=$ $\prod_{i=1}^{N} P_{X_{r}}\left(x_{r, i}\right)$, index them as $x_{r}^{N}(a), a \in\left[1,2^{N\left(R_{r}-\epsilon^{\prime}\right)}\right]$, where

$$
\begin{equation*}
R_{r}=I\left(X_{r} ; Y\right) \leq I\left(X_{r} ; Z\right) \tag{A22}
\end{equation*}
$$

- Second, generate $2^{N\left(I\left(X_{2} ; Y \mid X_{r}\right)-\epsilon^{\prime}\right)}$ i.i.d. codewords $x_{2}^{N}$ according to $P_{X_{2}}\left(x_{2}\right)$, and divide them into $2^{N R_{2}}$ bins. Each bin contains $2^{N\left(I\left(X_{2} ; Y \mid X_{r}\right)-\epsilon^{\prime}-R_{2}\right)}$ codewords, where

$$
\begin{equation*}
I\left(X_{2} ; Y \mid X_{r}\right)-\epsilon^{\prime}-R_{2}=I\left(X_{2} ; Z \mid X_{1}, X_{r}\right)-\epsilon^{\prime} \tag{A23}
\end{equation*}
$$

- Third, generate $2^{N\left(I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)-\epsilon^{\prime}\right)}$ i.i.d. codewords $x_{1}^{N}$ according to $P_{X_{1}}\left(x_{1}\right)$, and divide them into $2^{N R_{1}}$ bins. Each bin contains $2^{N\left(I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)-\epsilon^{\prime}-R_{1}\right)}$ codewords, where

$$
\begin{equation*}
I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)-\epsilon^{\prime}-R_{1}=I\left(X_{1} ; Z \mid X_{r}\right)-\epsilon^{\prime} \tag{A24}
\end{equation*}
$$

## Encoding for both cases:

The relay uniformly picks a codeword $x_{r}^{N}(a)$ from $\left[1,2^{N\left(R_{r}-\epsilon^{\prime}\right)}\right]$, and sends $x_{r}^{N}(a)$.
For a given confidential message $w_{2}$, randomly choose a codeword $x_{2}^{N}$ in bin $w_{2}$ to transmit. Similarly, for a given confidential message $w_{1}$, randomly choose a codeword $x_{1}^{N}$ in bin $w_{1}$ to transmit.

## Decoding for both cases:

For a given $y^{N}$, try to find a sequence $x_{r}^{N}(\hat{a})$ such that $\left(x_{r}^{N}(\hat{a}), y^{N}\right)$ are jointly typical. If there exists a unique sequence with the index $\hat{a}$, put out the corresponding $\hat{a}$, else declare a decoding error. Based on the AEP and A19) (or A22), the probability $\operatorname{Pr}\{\hat{a}=a\}$ goes to 1 .

After decoding $\hat{a}$, the legitimate receiver tries to find a sequence $x_{2}^{N}\left(\hat{w}_{2}\right)$ such that $\left(x_{2}^{N}\left(\hat{w}_{2}\right), x_{r}^{N}(\hat{a}), y^{N}\right)$ 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 and the construction of $x_{2}^{N}$ for both cases, the probability $\operatorname{Pr}\left\{\hat{w}_{2}=w_{2}\right\}$ goes to 1 .

Finally, after decoding $\hat{a}$ and $\hat{w}_{2}$, the legitimate receiver tries to find a sequence $x_{1}^{N}\left(\hat{w}_{1}\right)$ such that $\left(x_{1}^{N}\left(\hat{w}_{1}\right), x_{2}^{N}\left(\hat{w}_{2}\right), x_{r}^{N}(\hat{a}), y^{N}\right)$ are jointly typical. If 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 and the construction of $x_{1}^{N}$ for both cases, the probability $\operatorname{Pr}\left\{\hat{w}_{1}=w_{1}\right\}$ goes to 1 .
$P_{e} \leq \epsilon$ is easy to be checked by using the above encoding-decoding schemes. Now, it remains to prove $\Delta \geq$ $R_{1}+R_{2}-\epsilon$ for both cases, see the followings.

## Equivocation Analysis:

Proof of $\Delta \geq R_{1}+R_{2}-\epsilon$ for case 1:

$$
\begin{align*}
\Delta & =\frac{1}{N} H\left(W_{1}, W_{2} \mid Z^{N}\right) \\
& =\frac{1}{N}\left(H\left(W_{1} \mid Z^{N}\right)+H\left(W_{2} \mid W_{1}, Z^{N}\right)\right) \tag{A25}
\end{align*}
$$

The first term in A25 is bounded as follows.

$$
\begin{align*}
\frac{1}{N} H\left(W_{1} \mid Z^{N}\right) & =\frac{1}{N}\left(H\left(W_{1}, Z^{N}\right)-H\left(Z^{N}\right)\right) \\
& =\frac{1}{N}\left(H\left(W_{1}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right)-H\left(X_{1}^{N}, X_{r}^{N} \mid W_{1}, Z^{N}\right)-H\left(Z^{N}\right)\right) \\
& \stackrel{(a)}{=} \frac{1}{N}\left(H\left(Z^{N} \mid X_{1}^{N}, X_{r}^{N}\right)+H\left(X_{1}^{N}\right)+H\left(X_{r}^{N}\right)-H\left(X_{1}^{N}, X_{r}^{N} \mid W_{1}, Z^{N}\right)-H\left(Z^{N}\right)\right) \\
& =\frac{1}{N}\left(H\left(X_{1}^{N}\right)+H\left(X_{r}^{N}\right)-I\left(X_{1}^{N}, X_{r}^{N} ; Z^{N}\right)-H\left(X_{1}^{N}, X_{r}^{N} \mid W_{1}, Z^{N}\right)\right) \tag{A26}
\end{align*}
$$

where (a) follows from $W_{1} \rightarrow\left(X_{1}^{N}, X_{r}^{N}\right) \rightarrow Z^{N}, H\left(W_{1} \mid X_{1}^{N}\right)=0$ and the fact that $X_{1}^{N}$ is independent of $X_{r}^{N}$.
Consider the first term in A26, the code-book generation of $x_{1}^{N}$ shows that the total number of $x_{1}^{N}$ is $2^{N\left(I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)-\epsilon^{\prime}\right)}$. Thus, using the same approach as that in [7] Lemma 3], we have

$$
\begin{equation*}
\frac{1}{N} H\left(X_{1}^{N}\right) \geq I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)-\epsilon^{\prime}-\epsilon_{1, N} \tag{A27}
\end{equation*}
$$

where $\epsilon_{1, N} \rightarrow 0$ as $N \rightarrow \infty$.
For the second term in A26, the code-book generation of $x_{r}^{N}$ guarantees that

$$
\begin{equation*}
\frac{1}{N} H\left(X_{r}^{N}\right) \geq R_{r}-\epsilon^{\prime}-\epsilon_{2, N} \tag{A28}
\end{equation*}
$$

where $\epsilon_{2, N} \rightarrow 0$ as $N \rightarrow \infty$.
For the third term in A26, since the channel is memoryless, and $X_{1}^{N}, X_{2}^{N}, X_{r}^{N}$ are i.i.d. generated, we get

$$
\begin{equation*}
\frac{1}{N} I\left(X_{1}^{N}, X_{r}^{N} ; Z^{N}\right)=I\left(X_{1}, X_{r} ; Z\right) \tag{A29}
\end{equation*}
$$

Now, we consider the last term of A26. Given $w_{1}$, the wiretapper can do joint decoding. Specifically, given $z^{N}$ and $w_{1}$,

$$
\begin{equation*}
\frac{1}{N} H\left(X_{1}^{N}, X_{r}^{N} \mid W_{1}, Z^{N}\right) \leq \epsilon_{3, N} \tag{A30}
\end{equation*}
$$

$\left(\epsilon_{3, N} \rightarrow 0\right.$ as $\left.N \rightarrow \infty\right)$ is guaranteed if $R_{r} \leq I\left(X_{r} ; Z \mid X_{1}\right)$ and $R_{r} \geq I\left(X_{r} ; Z\right)$, and this is from the properties of AEP (similar argument is used in the proof of [18, Theorem 3]). By checking A19] and A20, A30, is obtained.

Substituting (A27), A28, (A29) and A30 into A26, we have

$$
\begin{equation*}
\frac{1}{N} H\left(W_{1} \mid Z^{N}\right) \geq I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)+R_{r}-I\left(X_{1}, X_{r} ; Z\right)-2 \epsilon^{\prime}-\epsilon_{1, N}-\epsilon_{2, N}-\epsilon_{3, N} \tag{A31}
\end{equation*}
$$

The second term in A25 is bounded as follows.

$$
\begin{align*}
& \frac{1}{N} H\left(W_{2} \mid W_{1}, Z^{N}\right) \geq \frac{1}{N} H\left(W_{2} \mid W_{1}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right) \\
& \stackrel{(1)}{=} \frac{1}{N} H\left(W_{2} \mid Z^{N}, X_{1}^{N}, X_{r}^{N}\right) \\
&= \frac{1}{N}\left(H\left(W_{2}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right)-H\left(Z^{N}, X_{1}^{N}, X_{r}^{N}\right)\right) \\
&= \frac{1}{N}\left(H\left(W_{2}, Z^{N}, X_{1}^{N}, X_{r}^{N}, X_{2}^{N}\right)-H\left(X_{2}^{N} \mid W_{2}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right)-H\left(Z^{N}, X_{1}^{N}, X_{r}^{N}\right)\right) \\
& \stackrel{(2)}{=} \frac{1}{N}\left(H\left(Z^{N} \mid X_{1}^{N}, X_{2}^{N}, X_{r}^{N}\right)+H\left(X_{r}^{N}\right)+H\left(X_{1}^{N}\right)+H\left(X_{2}^{N}\right)\right. \\
&\left.-H\left(X_{2}^{N} \mid W_{2}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right)-H\left(Z^{N} \mid X_{1}^{N}, X_{r}^{N}\right)-H\left(X_{1}^{N}\right)-H\left(X_{r}^{N}\right)\right) \\
&= \frac{1}{N}\left(H\left(X_{2}^{N}\right)-I\left(X_{2}^{N} ; Z^{N} \mid X_{1}^{N}, X_{r}^{N}\right)-H\left(X_{2}^{N} \mid W_{2}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right)\right) \tag{A32}
\end{align*}
$$

where (1) is from the Markov chain $W_{1} \rightarrow\left(Z^{N}, X_{1}^{N}, X_{r}^{N}\right) \rightarrow W_{2}$, and (2) is from the Markov chain $W_{2} \rightarrow$ $\left(X_{1}^{N}, X_{2}^{N}, X_{r}^{N}\right) \rightarrow Z^{N}, H\left(W_{2} \mid X_{2}^{N}\right)=0$, and the fact that $X_{1}^{N}, X_{2}^{N}$ and $X_{r}^{N}$ are independent.

Consider the first term in A32, the code-book generation of $x_{2}^{N}$ shows that the total number of $x_{2}^{N}$ is $2^{N\left(I\left(X_{2} ; Y \mid X_{r}\right)-\epsilon^{\prime}\right)}$. Thus, using the same approach as that in [7, Lemma 3], we have

$$
\begin{equation*}
\frac{1}{N} H\left(X_{2}^{N}\right) \geq I\left(X_{2} ; Y \mid X_{r}\right)-\epsilon^{\prime}-\epsilon_{4, N} \tag{A33}
\end{equation*}
$$

where $\epsilon_{4, N} \rightarrow 0$ as $N \rightarrow \infty$.
For the second term in A32, since the channel is memoryless, and $X_{1}^{N}, X_{2}^{N}, X_{r}^{N}$ are i.i.d. generated, we get

$$
\begin{equation*}
\frac{1}{N} I\left(X_{2}^{N} ; Z^{N} \mid X_{1}^{N}, X_{r}^{N}\right)=I\left(X_{2} ; Z \mid X_{1}, X_{r}\right) \tag{A34}
\end{equation*}
$$

Now, we consider the last term of A32. Given $Z^{N}, X_{1}^{N}, X_{r}^{N}$ and $W_{2}$, the total number of possible codewords of $x_{2}^{N}$ is $2^{N\left(I\left(X_{2} ; Y \mid X_{r}\right)-\epsilon^{\prime}-R_{2}\right)}$. By using the Fano's inequality and A21, we have

$$
\begin{equation*}
\frac{1}{N} H\left(X_{2}^{N} \mid W_{2}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right) \leq \epsilon_{5, N} \tag{A35}
\end{equation*}
$$

where $\epsilon_{5, N} \rightarrow 0$ as $N \rightarrow \infty$.
Substituting A33, A34 and A35 into A32, we have

$$
\begin{equation*}
\frac{1}{N} H\left(W_{2} \mid W_{1}, Z^{N}\right) \geq I\left(X_{2} ; Y \mid X_{r}\right)-I\left(X_{2} ; Z \mid X_{1}, X_{r}\right)-\epsilon^{\prime}-\epsilon_{4, N}-\epsilon_{5, N} \tag{A36}
\end{equation*}
$$

Substituting A31 and A36 into A25, and choosing $\epsilon^{\prime}$ and sufficiently large $N$ such that $3 \epsilon^{\prime}+\epsilon_{1, N}+\epsilon_{2, N}+$ $\epsilon_{3, N}+\epsilon_{4, N}+\epsilon_{5, N} \leq \epsilon, \Delta \geq R_{1}+R_{2}-\epsilon$ for case 1 is proved.

Proof of $\Delta \geq R_{1}+R_{2}-\epsilon$ for case 2:

$$
\begin{align*}
\Delta & =\frac{1}{N} H\left(W_{1}, W_{2} \mid Z^{N}\right) \\
& =\frac{1}{N}\left(H\left(W_{1} \mid Z^{N}\right)+H\left(W_{2} \mid W_{1}, Z^{N}\right)\right) \tag{A37}
\end{align*}
$$

The first term in A37 is bounded as follows.

$$
\begin{align*}
& \frac{1}{N} H\left(W_{1} \mid Z^{N}\right) \geq \frac{1}{N} H\left(W_{1} \mid Z^{N}, X_{r}^{N}\right) \\
&= \frac{1}{N}\left(H\left(W_{1}, Z^{N}, X_{r}^{N}\right)-H\left(Z^{N}, X_{r}^{N}\right)\right) \\
&= \frac{1}{N}\left(H\left(W_{1}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right)-H\left(X_{1}^{N} \mid W_{1}, Z^{N}, X_{r}^{N}\right)-H\left(Z^{N}, X_{r}^{N}\right)\right) \\
& \stackrel{(a)}{=} \frac{1}{N}\left(H\left(Z^{N} \mid X_{1}^{N}, X_{r}^{N}\right)+H\left(X_{1}^{N}\right)+H\left(X_{r}^{N}\right)-H\left(X_{1}^{N} \mid W_{1}, Z^{N}, X_{r}^{N}\right)\right. \\
&\left.-H\left(Z^{N} \mid X_{r}^{N}\right)-H\left(X_{r}^{N}\right)\right) \\
&= \frac{1}{N}\left(H\left(X_{1}^{N}\right)-I\left(X_{1}^{N} ; Z^{N} \mid X_{r}^{N}\right)-H\left(X_{1}^{N} \mid W_{1}, Z^{N}, X_{r}^{N}\right)\right) \tag{A38}
\end{align*}
$$

where (a) follows from $W_{1} \rightarrow\left(X_{1}^{N}, X_{r}^{N}\right) \rightarrow Z^{N}, H\left(W_{1} \mid X_{1}^{N}\right)=0$ and the fact that $X_{1}^{N}$ is independent of $X_{r}^{N}$.
Consider the first term in A38, the code-book generation of $x_{1}^{N}$ shows that the total number of $x_{1}^{N}$ is $2^{N\left(I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)-\epsilon^{\prime}\right)}$. Thus, using the same approach as that in [7] Lemma 3], we have

$$
\begin{equation*}
\frac{1}{N} H\left(X_{1}^{N}\right) \geq I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)-\epsilon^{\prime}-\epsilon_{1, N} \tag{A39}
\end{equation*}
$$

where $\epsilon_{1, N} \rightarrow 0$ as $N \rightarrow \infty$.
For the second term in A38, since the channel is memoryless, and $X_{1}^{N}, X_{2}^{N}, X_{r}^{N}$ are i.i.d. generated, we get

$$
\begin{equation*}
\frac{1}{N} I\left(X_{1}^{N} ; Z^{N} \mid X_{r}^{N}\right)=I\left(X_{1} ; Z \mid X_{r}\right) \tag{A40}
\end{equation*}
$$

Now, we consider the last term of A38. Given $Z^{N}, X_{r}^{N}$ and $W_{1}$, the total number of possible codewords of $x_{1}^{N}$ is $2^{N\left(I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)-\epsilon^{\prime}-R_{1}\right)}$. By using the Fano's inequality and A24, we have

$$
\begin{equation*}
\frac{1}{N} H\left(X_{1}^{N} \mid W_{1}, Z^{N}, X_{r}^{N}\right) \leq \epsilon_{2, N} \tag{A41}
\end{equation*}
$$

where $\epsilon_{2, N} \rightarrow 0$ as $N \rightarrow \infty$.
Substituting A39, A40 and A41 into A38), we have

$$
\begin{equation*}
\frac{1}{N} H\left(W_{1} \mid Z^{N}\right) \geq I\left(X_{1} ; Y \mid X_{2}, X_{r}\right)-I\left(X_{1} ; Z \mid X_{r}\right)-\epsilon^{\prime}-\epsilon_{1, N}-\epsilon_{2, N} \tag{A42}
\end{equation*}
$$

The second term in A37 is bounded the same as that for case 1 , and thus, we have

$$
\begin{equation*}
\frac{1}{N} H\left(W_{2} \mid W_{1}, Z^{N}\right) \geq I\left(X_{2} ; Y \mid X_{r}\right)-I\left(X_{2} ; Z \mid X_{1}, X_{r}\right)-\epsilon^{\prime}-\epsilon_{3, N}-\epsilon_{4, N} \tag{A43}
\end{equation*}
$$

where $\epsilon_{3, N}, \epsilon_{4, N} \rightarrow 0$ as $N \rightarrow \infty$. The proof is omitted here.
Substituting A42, and A43 into A37, and choosing $\epsilon^{\prime}$ and sufficiently large $N$ such that $2 \epsilon^{\prime}+\epsilon_{1, N}+\epsilon_{2, N}+$ $\epsilon_{3, N}+\epsilon_{4, N} \leq \epsilon, \Delta \geq R_{1}+R_{2}-\epsilon$ for case 2 is proved.

The proof of Theorem 2 is completed.

## Appendix C

## Proof of Theorem 3

For Theorem 3, we only need to prove that the corner points of $\mathcal{L}^{3}$ and $\mathcal{L}^{4}$ are achievable, see the followings.

- (Case 1) If $I\left(X_{r} ; Y\right) \geq I\left(X_{r} ; Z\right)$, we allow the legitimate receiver to decode $x_{r}^{N}$, and the wiretapper can not decode it. For case 1 , it is sufficient to show that the pair $\left(R_{1}, R_{2}\right) \in \mathcal{L}^{3}$ with the condition

$$
\begin{equation*}
R_{1}=I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-I\left(X_{1}, X_{r} ; Z\right)+R^{*}, \quad R_{2}=I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)-I\left(X_{2} ; Z \mid X_{1}, X_{r}\right) \tag{A44}
\end{equation*}
$$

is achievable. The achievability proof of the other corner point $\left(R_{1}=I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{r}\right)-I\left(X_{1} ; Z \mid X_{2}, X_{r}\right), R_{2}=\right.$ $\left.I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{1}, X_{r}\right)-I\left(X_{2}, X_{r} ; Z\right)+R^{*}\right)$ follows by symmetry. Here note that $R^{*}$ satisfies

$$
\begin{equation*}
\min \left\{I\left(X_{r} ; Z \mid X_{1}\right), I\left(X_{r} ; Z \mid X_{2}\right), I\left(X_{r} ; Y\right)\right\}-R^{*} \geq I\left(Y_{r} ; \hat{Y}_{r} \mid X_{r}\right) \tag{A45}
\end{equation*}
$$

- (Case 2) If $I\left(Y_{r} ; \hat{Y}_{r} \mid X_{r}\right) \leq I\left(X_{r} ; Y\right) \leq I\left(X_{r} ; Z\right)$, we allow both the receivers to decode $x_{r}^{N}$. For case 2, it is sufficient to show that the pair $\left(R_{1}, R_{2}\right) \in \mathcal{L}^{4}$ with the condition

$$
\begin{equation*}
R_{1}=I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-I\left(X_{1} ; Z \mid X_{r}\right), \quad R_{2}=I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)-I\left(X_{2} ; Z \mid X_{1}, X_{r}\right) \tag{A46}
\end{equation*}
$$

is achievable. The achievability proof of the other corner point $\left(R_{1}=I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{r}\right)-I\left(X_{1} ; Z \mid X_{2}, X_{r}\right), R_{2}=\right.$ $\left.I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{1}, X_{r}\right)-I\left(X_{2} ; Z \mid X_{r}\right)\right)$ follows by symmetry.

Fix the joint probability mass function $P_{\hat{Y}_{r} \mid Y_{r}, X_{r}}\left(\hat{y}_{r} \mid y_{r}, x_{r}\right) P_{Y, Z, Y_{r} \mid X_{r}, X_{1}, X_{2}}\left(y, z, y_{r} \mid x_{r}, x_{1}, x_{2}\right) P_{X_{r}}\left(x_{r}\right) P_{X_{1}}\left(x_{1}\right) P_{X_{2}}\left(x_{2}\right)$. Define the messages $W_{1}, W_{2}$ taking values in the alphabets $\mathcal{W}_{1}, \mathcal{W}_{2}$, respectively, where

$$
\mathcal{W}_{1}=\left\{1,2, \ldots, 2^{N R_{1}}\right\}, \quad \mathcal{W}_{2}=\left\{1,2, \ldots, 2^{N R_{2}}\right\}
$$

## Code-book Construction for the Two Cases:

- Code-book construction for case 1 :
- First, generate at random $2^{N\left(R_{r 1}^{*}-\epsilon^{\prime}\right)}\left(\epsilon^{\prime}\right.$ is a small positive number) i.i.d. sequences $x_{r}^{N}$ at the relay node each drawn according to $P_{X_{r}^{N}}\left(x_{r}^{N}\right)=\prod_{i=1}^{N} P_{X_{r}}\left(x_{r, i}\right)$, index them as $x_{r}^{N}(a), a \in\left[1,2^{N\left(R_{r 1}^{*}-\epsilon^{\prime}\right)}\right]$, where

$$
\begin{equation*}
R_{r 1}^{*}=\min \left\{I\left(X_{r} ; Z \mid X_{1}\right), I\left(X_{r} ; Z \mid X_{2}\right), I\left(X_{r} ; Y\right)\right\} \tag{A47}
\end{equation*}
$$

Here note that

$$
\begin{equation*}
R_{r 1}^{*} \geq I\left(X_{r} ; Z\right) \tag{A48}
\end{equation*}
$$

For each $x_{r}^{N}(a)\left(a \in\left[1,2^{N\left(R_{r 1}^{*}-\epsilon^{\prime}\right)}\right]\right)$, generate at random $2^{N\left(R_{r 1}^{*}-\epsilon^{\prime}-R^{*}\right)}$ i.i.d. $\hat{y}_{r}^{N}$ according to $P_{\hat{Y}_{r}^{N} \mid X_{r}^{N}}\left(\hat{y}_{r}^{N} \mid x_{r}^{N}\right)=$ $\prod_{i=1}^{N} P_{\hat{Y}_{r} \mid X_{r}}\left(\hat{y}_{r, i} \mid x_{r, i}\right)$. Label these $\hat{y}_{r}^{N}$ as $\hat{y}_{r}^{N}(m, a), m \in\left[1,2^{N\left(R_{r 1}^{*}-\epsilon^{\prime}-R^{*}\right)}\right], a \in\left[1,2^{N\left(R_{r 1}^{*}-\epsilon^{\prime}\right)}\right]$. Equally divide $2^{N\left(R_{r 1}^{*}-\epsilon^{\prime}\right)}$ sequences of $x_{r}^{N}$ into $2^{N\left(R_{r 1}^{*}-\epsilon^{\prime}-R^{*}\right)}$ bins, hence there are $2^{N R^{*}}$ sequences of $x_{r}^{N}$ at each bin.

- Second, generate $2^{N\left(I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)-\epsilon^{\prime}\right)}$ i.i.d. codewords $x_{2}^{N}$ according to $P_{X_{2}}\left(x_{2}\right)$, and divide them into $2^{N R_{2}}$ bins. Each bin contains $2^{N\left(I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)-\epsilon^{\prime}-R_{2}\right)}$ codewords, where

$$
\begin{equation*}
I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)-\epsilon^{\prime}-R_{2}=I\left(X_{2} ; Z \mid X_{1}, X_{r}\right)-\epsilon^{\prime} \tag{A49}
\end{equation*}
$$

- Third, generate $2^{N\left(I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-\epsilon^{\prime}+R^{*}-R_{r 1}^{*}\right)}$ i.i.d. codewords $x_{1}^{N}$ according to $P_{X_{1}}\left(x_{1}\right)$, and divide them into $2^{N R_{1}}$ bins. Each bin contains $2^{N\left(I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-\epsilon^{\prime}+R^{*}-R_{r 1}^{*}-R_{1}\right)}$ codewords. Here note that from A45 and A47, we know that $R^{*} \leq R_{r 1}^{*}$, and thus, we have

$$
\begin{equation*}
I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-\epsilon^{\prime}+R^{*}-R_{r 1}^{*} \leq I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-\epsilon^{\prime} \tag{A50}
\end{equation*}
$$

In addition, by using $R_{1}=I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-I\left(X_{1}, X_{r} ; Z\right)+R^{*}$, the codewords $x_{1}^{N}$ in each bin is upper bounded by

$$
\begin{align*}
& I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-\epsilon^{\prime}+R^{*}-R_{r 1}^{*}-R_{1} \\
= & I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-\epsilon^{\prime}+R^{*}-R_{r 1}^{*} \\
& -\left(I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-I\left(X_{1}, X_{r} ; Z\right)+R^{*}\right) \\
= & I\left(X_{1}, X_{r} ; Z\right)-R_{r 1}^{*}-\epsilon^{\prime} \\
\stackrel{(a)}{\leq} & I\left(X_{1}, X_{r} ; Z\right)-I\left(X_{r} ; Z\right)-\epsilon^{\prime} \\
= & I\left(X_{1} ; Z \mid X_{r}\right)-\epsilon^{\prime} \tag{A51}
\end{align*}
$$

where (a) is from A48.

- Code-book Construction for case 2 :
- First, generate at random $2^{N\left(R_{r 2}^{*}-\epsilon^{\prime}\right)}$ i.i.d. sequences $x_{r}^{N}$ at the relay node each drawn according to $P_{X_{r}^{N}}\left(x_{r}^{N}\right)=\prod_{i=1}^{N} P_{X_{r}}\left(x_{r, i}\right)$, index them as $x_{r}^{N}(a), a \in\left[1,2^{N\left(R_{r 2}^{*}-\epsilon^{\prime}\right)}\right]$, where

$$
\begin{equation*}
R_{r 2}^{*}=I\left(X_{r} ; Y\right) \leq I\left(X_{r} ; Z\right) \tag{A52}
\end{equation*}
$$

For each $x_{r}^{N}(a)\left(a \in\left[1,2^{N\left(R_{r 2}^{*}-\epsilon^{\prime}\right)}\right]\right)$, generate at random $2^{N\left(R_{r 2}^{*}-\epsilon^{\prime}\right)}$ i.i.d. $\hat{y}_{r}^{N}$ according to $P_{\hat{Y}_{r}^{N} \mid X_{r}^{N}}\left(\hat{y}_{r}^{N} \mid x_{r}^{N}\right)=$ $\prod_{i=1}^{N} P_{\hat{Y}_{r} \mid X_{r}}\left(\hat{y}_{r, i} \mid x_{r, i}\right)$. Label these $\hat{y}_{r}^{N}$ as $\hat{y}_{r}^{N}(a), a \in\left[1,2^{N\left(R_{r 2}^{*}-\epsilon^{\prime}\right)}\right]$.

- Second, generate $2^{N\left(I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)-\epsilon^{\prime}\right)}$ i.i.d. codewords $x_{2}^{N}$ according to $P_{X_{2}}\left(x_{2}\right)$, and divide them into $2^{N R_{2}}$ bins. Each bin contains $2^{N\left(I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)-\epsilon^{\prime}-R_{2}\right)}$ codewords, where

$$
\begin{equation*}
I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)-\epsilon^{\prime}-R_{2}=I\left(X_{2} ; Z \mid X_{1}, X_{r}\right)-\epsilon^{\prime} \tag{A53}
\end{equation*}
$$

- Third, generate $2^{N\left(I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-\epsilon^{\prime}\right)}$ i.i.d. codewords $x_{1}^{N}$ according to $P_{X_{1}}\left(x_{1}\right)$, and divide them into $2^{N R_{1}}$ bins. Each bin contains $2^{N\left(I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-\epsilon^{\prime}-R_{1}\right)}$ codewords, where

$$
\begin{equation*}
I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-\epsilon^{\prime}-R_{1}=I\left(X_{1} ; Z \mid X_{r}\right)-\epsilon^{\prime} \tag{A54}
\end{equation*}
$$

## Encoding:

Encoding involves the mapping of message indices to channel inputs, which are facilitated by the sequences generated above. We exploit the block Markov coding scheme, as argued in [23], the loss induced by this scheme is negligible as the number of blocks $n \rightarrow \infty$. For block $i(1 \leq i \leq n)$, encoding proceeds as follows.

First, for convenience, the messages $w_{1}$ and $w_{2}$ transmitted in the $i$-th block are denoted by $w_{1, i}$ and $w_{2, i}$, respectively. $y_{r}^{N}(i)$ and $\hat{y}_{r}^{N}(i)$ are the $y_{r}^{N}$ and $\hat{y}_{r}^{N}$ for the $i$-th block, respectively.

## - Encoding for case 1:

At the end of block $i(2 \leq i \leq n)$, assume that $\left(x_{r}^{N}\left(a_{i}\right), y_{r}^{N}(i), \hat{y}_{r}^{N}\left(m_{i}, a_{i}\right)\right)$ are jointly typical, then we choose $a_{i+1}$ uniformly from bin $m_{i}$, and the relay sends $x_{r}^{N}\left(a_{i+1}\right)$ at block $i+1$. In the first block, the relay sends $x_{r}^{N}(1)$.
For a given confidential message $w_{2}$, randomly choose a codeword $x_{2}^{N}$ in bin $w_{2}$ to transmit. Similarly, for a given confidential message $w_{1}$, randomly choose a codeword $x_{1}^{N}$ in bin $w_{1}$ to transmit.

## - Encoding for case 2:

In block $i(1 \leq i \leq n)$, the relay randomly choose an index $a_{i}$ from $\left[1,2^{N\left(R_{r 2}^{*}-\epsilon^{\prime}\right)}\right]$, and sends $x_{r}^{N}\left(a_{i}\right)$ and $\hat{y}_{r}^{N}\left(a_{i}\right)$.
For a given confidential message $w_{2}$, randomly choose a codeword $x_{2}^{N}$ in bin $w_{2}$ to transmit. Similarly, for a given confidential message $w_{1}$, randomly choose a codeword $x_{1}^{N}$ in bin $w_{1}$ to transmit.

## Decoding:

## - Decoding for case 1:

(At the relay) At the end of block $i$, the relay already has $a_{i}$, it then decides $m_{i}$ by choosing $m_{i}$ such that $\left(x_{r}^{N}\left(a_{i}\right), y_{r}^{N}(i), \hat{y}_{r}^{N}\left(m_{i}, a_{i}\right)\right)$ are jointly typical. There exists such $m_{i}$, if

$$
\begin{equation*}
R_{r 1}^{*}-R^{*} \geq I\left(Y_{r} ; \hat{Y}_{r} \mid X_{r}\right) \tag{A55}
\end{equation*}
$$

and $N$ is sufficiently large. Choose $a_{i+1}$ uniformly from bin $m_{i}$.
(At the legitimate receiver) The legitimate receiver does backward decoding. The decoding process starts at the last block $n$, the legitimate receiver decodes $a_{n}$ by choosing unique $\check{a}_{n}$ such that $\left(x_{r}^{N}\left(\check{a}_{n}\right), y^{N}(n)\right)$ are jointly typical. Since $R_{r 1}^{*}$ satisfies A47, the probability $\operatorname{Pr}\left\{\check{a}_{n}=a_{n}\right\}$ goes to 1 for sufficiently large $N$.
Next, the legitimate receiver moves to the block $n-1$. Now it already has $\check{a}_{n}$, hence we also have $\check{m}_{n-1}=f\left(\check{a}_{n}\right)$ (here $f$ is a deterministic function, which means that $\check{m}_{n-1}$ can be determined by $\check{a}_{n}$ ). It first declares that $\check{a}_{n-1}$ is received, if $\check{a}_{n-1}$ is the unique one such that $\left(x_{r}^{N}\left(\check{a}_{n-1}\right), y^{N}(n-1)\right)$ are joint typical. If A47) is satisfied, $\check{a}_{n-1}=a_{n-1}$ with high probability. After knowing $\check{a}_{n-1}$, the destination gets an estimation of $w_{2, n-1}$ by picking the unique $\check{w}_{2, n-1}$ such that $\left(x_{2}^{N}\left(\check{w}_{2, n-1}\right), \hat{y}_{r}^{N}\left(\check{m}_{n-1}, \check{a}_{n-1}\right), y^{N}(n-1), x_{r}^{N}\left(\check{a}_{n-1}\right)\right)$ are jointly typical. We will have $\check{w}_{2, n-1}=w_{2, n-1}$ with high probability, if the codewords of $x_{2}^{N}$ is upper bounded by $2^{N I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)}$ and $N$ is sufficiently large.
After decoding $\check{w}_{2, n-1}$, the legitimate receiver tries to find a quintuple such that
$\left(x_{1}^{N}\left(\check{w}_{1, n-1}\right), x_{2}^{N}\left(\check{w}_{2, n-1}\right), \hat{y}_{r}^{N}\left(\check{m}_{n-1}, \check{a}_{n-1}\right), y^{N}(n-1), x_{r}^{N}\left(\check{a}_{n-1}\right)\right)$ are jointly typical. Based on the AEP, the probability $\operatorname{Pr}\left\{\check{w}_{1, n-1}=w_{1, n-1}\right\}$ goes to 1 if the codewords of $x_{1}^{N}$ is upper bounded by $2^{N I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)}$ and $N$ is sufficiently large.
The decoding scheme of the legitimate receiver in block $i(1 \leq i \leq n-2)$ is similar to that in block $n-1$, and we omit it here.

- Decoding for case 2:
(At the relay) The relay does not need to decode any codeword.
(At the legitimate receiver) In block $i(1 \leq i \leq n)$, the legitimate receiver decodes $a_{i}$ by choosing unique $\check{a}_{i}$ such that $\left(x_{r}^{N}\left(\check{a}_{i}\right), y^{N}(i)\right)$ are jointly typical. Since $R_{r 2}^{*}$ satisfies A52, the probability $\operatorname{Pr}\left\{\check{a}_{i}=a_{i}\right\}$ goes to 1 for sufficiently large $N$.
Now since the legitimate receiver has $\check{a}_{i}$, he also knows $\hat{y}_{r}^{N}\left(\check{a}_{i}\right)$. Then he gets an estimation of $w_{2, i}$ by picking the unique $\check{w}_{2, i}$ such that $\left(x_{2}^{N}\left(\check{w}_{2, i}\right), \hat{y}_{r}^{N}\left(\check{a}_{i}\right), y^{N}(i), x_{r}^{N}\left(\check{a}_{i}\right)\right)$ are jointly typical. We will have $\check{w}_{2, i}=w_{2, i}$ with high probability, if the codewords of $x_{2}^{N}$ is upper bounded by $2^{N I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)}$ and $N$ is sufficiently large.
After decoding $\check{w}_{2, i}$, the legitimate receiver tries to find a quintuple such that
$\left(x_{1}^{N}\left(\check{w}_{1, i}\right), x_{2}^{N}\left(\check{w}_{2, i}\right), \hat{y}_{r}^{N}\left(\check{a}_{i}\right), y^{N}(i), x_{r}^{N}\left(\check{a}_{i}\right)\right)$ are jointly typical. Based on the AEP, the probability $\operatorname{Pr}\left\{\check{w}_{1, i}=\right.$ $\left.w_{1, i}\right\}$ goes to 1 if the codewords of $x_{1}^{N}$ is upper bounded by $2^{N I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)}$ and $N$ is sufficiently large.
$P_{e} \leq \epsilon$ is easy to be checked by using the above encoding-decoding schemes. Now, it remains to prove $\Delta \geq$ $R_{1}+R_{2}-\epsilon$ for both cases, see the followings.


## Equivocation Analysis:

Proof of $\Delta \geq R_{1}+R_{2}-\epsilon$ for case 1 :

$$
\begin{align*}
\Delta & =\frac{1}{N} H\left(W_{1}, W_{2} \mid Z^{N}\right) \\
& =\frac{1}{N}\left(H\left(W_{1} \mid Z^{N}\right)+H\left(W_{2} \mid W_{1}, Z^{N}\right)\right) \tag{A56}
\end{align*}
$$

The first term in A56 is bounded as follows.

$$
\begin{align*}
\frac{1}{N} H\left(W_{1} \mid Z^{N}\right) & =\frac{1}{N}\left(H\left(W_{1}, Z^{N}\right)-H\left(Z^{N}\right)\right) \\
& =\frac{1}{N}\left(H\left(W_{1}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right)-H\left(X_{1}^{N}, X_{r}^{N} \mid W_{1}, Z^{N}\right)-H\left(Z^{N}\right)\right) \\
& \stackrel{(a)}{=} \frac{1}{N}\left(H\left(Z^{N} \mid X_{1}^{N}, X_{r}^{N}\right)+H\left(X_{1}^{N}\right)+H\left(X_{r}^{N}\right)-H\left(X_{1}^{N}, X_{r}^{N} \mid W_{1}, Z^{N}\right)-H\left(Z^{N}\right)\right) \\
& =\frac{1}{N}\left(H\left(X_{1}^{N}\right)+H\left(X_{r}^{N}\right)-I\left(X_{1}^{N}, X_{r}^{N} ; Z^{N}\right)-H\left(X_{1}^{N}, X_{r}^{N} \mid W_{1}, Z^{N}\right)\right) \tag{A57}
\end{align*}
$$

where (a) follows from $W_{1} \rightarrow\left(X_{1}^{N}, X_{r}^{N}\right) \rightarrow Z^{N}, H\left(W_{1} \mid X_{1}^{N}\right)=0$ and the fact that $X_{1}^{N}$ is independent of $X_{r}^{N}$.
Consider the first term in A57, the code-book generation of $x_{1}^{N}$ shows that the total number of $x_{1}^{N}$ is upper bounded by A51). Thus, using the same approach as that in [7, Lemma 3], we have

$$
\begin{equation*}
\frac{1}{N} H\left(X_{1}^{N}\right) \geq I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)+R^{*}-R_{r 1}^{*}-\epsilon^{\prime}-\epsilon_{1, N} \tag{A58}
\end{equation*}
$$

where $\epsilon_{1, N} \rightarrow 0$ as $N \rightarrow \infty$.
For the second term in A57, the code-book generation of $x_{r}^{N}$ and [7, Lemma 3] guarantee that

$$
\begin{equation*}
\frac{1}{N} H\left(X_{r}^{N}\right) \geq R_{r 1}^{*}-\epsilon^{\prime}-\epsilon_{2, N} \tag{A59}
\end{equation*}
$$

where $\epsilon_{2, N} \rightarrow 0$ as $N \rightarrow \infty$.

For the third term in A57, since the channel is memoryless, and $X_{1}^{N}, X_{2}^{N}, X_{r}^{N}$ are i.i.d. generated, we get

$$
\begin{equation*}
\frac{1}{N} I\left(X_{1}^{N}, X_{r}^{N} ; Z^{N}\right)=I\left(X_{1}, X_{r} ; Z\right) \tag{A60}
\end{equation*}
$$

Now, we consider the last term of A57. Given $w_{1}$, the wiretapper can do joint decoding. Specifically, given $z^{N}$ and $w_{1}$,

$$
\begin{equation*}
\frac{1}{N} H\left(X_{1}^{N}, X_{r}^{N} \mid W_{1}, Z^{N}\right) \leq \epsilon_{3, N} \tag{A61}
\end{equation*}
$$

$\left(\epsilon_{3, N} \rightarrow 0\right.$ as $\left.N \rightarrow \infty\right)$ is guaranteed if $R_{r} \leq I\left(X_{r} ; Z \mid X_{1}\right)$ and $I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-\epsilon^{\prime}+R^{*}-R_{r 1}^{*}-R_{1} \leq$ $I\left(X_{1} ; Z \mid X_{r}\right)$, and this is from the properties of AEP (similar argument is used in the proof of [18, Theorem 3]). By checking A47, and A51, A61 is obtained.

Substituting A58, A59, A60 and A61 into A57, we have

$$
\begin{equation*}
\frac{1}{N} H\left(W_{1} \mid Z^{N}\right) \geq I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)+R^{*}-I\left(X_{1}, X_{r} ; Z\right)-2 \epsilon^{\prime}-\epsilon_{1, N}-\epsilon_{2, N}-\epsilon_{3, N} \tag{A62}
\end{equation*}
$$

The second term in A56 is bounded as follows.

$$
\begin{align*}
& \frac{1}{N} H\left(W_{2} \mid W_{1}, Z^{N}\right) \geq \frac{1}{N} H\left(W_{2} \mid W_{1}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right) \\
& \stackrel{(1)}{=} \frac{1}{N} H\left(W_{2} \mid Z^{N}, X_{1}^{N}, X_{r}^{N}\right) \\
&= \frac{1}{N}\left(H\left(W_{2}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right)-H\left(Z^{N}, X_{1}^{N}, X_{r}^{N}\right)\right) \\
&= \frac{1}{N}\left(H\left(W_{2}, Z^{N}, X_{1}^{N}, X_{r}^{N}, X_{2}^{N}\right)-H\left(X_{2}^{N} \mid W_{2}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right)-H\left(Z^{N}, X_{1}^{N}, X_{r}^{N}\right)\right) \\
& \stackrel{(2)}{=} \frac{1}{N}\left(H\left(Z^{N} \mid X_{1}^{N}, X_{2}^{N}, X_{r}^{N}\right)+H\left(X_{r}^{N}\right)+H\left(X_{1}^{N}\right)+H\left(X_{2}^{N}\right)\right. \\
&\left.-H\left(X_{2}^{N} \mid W_{2}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right)-H\left(Z^{N} \mid X_{1}^{N}, X_{r}^{N}\right)-H\left(X_{1}^{N}\right)-H\left(X_{r}^{N}\right)\right) \\
&= \frac{1}{N}\left(H\left(X_{2}^{N}\right)-I\left(X_{2}^{N} ; Z^{N} \mid X_{1}^{N}, X_{r}^{N}\right)-H\left(X_{2}^{N} \mid W_{2}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right)\right) \tag{A63}
\end{align*}
$$

where (1) is from the Markov chain $W_{1} \rightarrow\left(Z^{N}, X_{1}^{N}, X_{r}^{N}\right) \rightarrow W_{2}$, and (2) is from the Markov chain $W_{2} \rightarrow$ $\left(X_{1}^{N}, X_{2}^{N}, X_{r}^{N}\right) \rightarrow Z^{N}, H\left(W_{2} \mid X_{2}^{N}\right)=0$, and the fact that $X_{1}^{N}, X_{2}^{N}$ and $X_{r}^{N}$ are independent.

Consider the first term in A63, using the same approach as that in [7, Lemma 3], we have

$$
\begin{equation*}
\frac{1}{N} H\left(X_{2}^{N}\right) \geq I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)-\epsilon^{\prime}-\epsilon_{4, N} \tag{A64}
\end{equation*}
$$

where $\epsilon_{4, N} \rightarrow 0$ as $N \rightarrow \infty$.
For the second term in A63, since the channel is memoryless, and $X_{1}^{N}, X_{2}^{N}, X_{r}^{N}$ are i.i.d. generated, we get

$$
\begin{equation*}
\frac{1}{N} I\left(X_{2}^{N} ; Z^{N} \mid X_{1}^{N}, X_{r}^{N}\right)=I\left(X_{2} ; Z \mid X_{1}, X_{r}\right) \tag{A65}
\end{equation*}
$$

Now, we consider the last term of A63. Given $Z^{N}, X_{1}^{N}, X_{r}^{N}$ and $W_{2}$, the total number of possible codewords of $x_{2}^{N}$ is $2^{N\left(I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)-\epsilon^{\prime}-R_{2}\right)}$. By using the Fano's inequality and A49, we have

$$
\begin{equation*}
\frac{1}{N} H\left(X_{2}^{N} \mid W_{2}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right) \leq \epsilon_{5, N} \tag{A66}
\end{equation*}
$$

Substituting A64, A65 and A66 into A63, we have

$$
\begin{equation*}
\frac{1}{N} H\left(W_{2} \mid W_{1}, Z^{N}\right) \geq I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)-I\left(X_{2} ; Z \mid X_{1}, X_{r}\right)-\epsilon^{\prime}-\epsilon_{4, N}-\epsilon_{5, N} \tag{A67}
\end{equation*}
$$

Substituting A62 and A67 into A56, and choosing $\epsilon^{\prime}$ and sufficiently large $N$ such that $3 \epsilon^{\prime}+\epsilon_{1, N}+\epsilon_{2, N}+$ $\epsilon_{3, N}+\epsilon_{4, N}+\epsilon_{5, N} \leq \epsilon, \Delta \geq R_{1}+R_{2}-\epsilon$ for case 1 is proved.

Proof of $\Delta \geq R_{1}+R_{2}-\epsilon$ for case 2:

$$
\begin{align*}
\Delta & =\frac{1}{N} H\left(W_{1}, W_{2} \mid Z^{N}\right) \\
& =\frac{1}{N}\left(H\left(W_{1} \mid Z^{N}\right)+H\left(W_{2} \mid W_{1}, Z^{N}\right)\right) \tag{A68}
\end{align*}
$$

The first term in A68 is bounded as follows.

$$
\begin{align*}
\frac{1}{N} H\left(W_{1} \mid Z^{N}\right) \geq & \frac{1}{N} H\left(W_{1} \mid Z^{N}, X_{r}^{N}\right) \\
= & \frac{1}{N}\left(H\left(W_{1}, Z^{N}, X_{r}^{N}\right)-H\left(Z^{N}, X_{r}^{N}\right)\right) \\
= & \frac{1}{N}\left(H\left(W_{1}, Z^{N}, X_{1}^{N}, X_{r}^{N}\right)-H\left(X_{1}^{N} \mid W_{1}, Z^{N}, X_{r}^{N}\right)-H\left(Z^{N}, X_{r}^{N}\right)\right) \\
\stackrel{(a)}{=} & \frac{1}{N}\left(H\left(Z^{N} \mid X_{1}^{N}, X_{r}^{N}\right)+H\left(X_{1}^{N}\right)+H\left(X_{r}^{N}\right)-H\left(X_{1}^{N} \mid W_{1}, Z^{N}, X_{r}^{N}\right)\right. \\
& \left.-H\left(Z^{N} \mid X_{r}^{N}\right)-H\left(X_{r}^{N}\right)\right) \\
= & \frac{1}{N}\left(H\left(X_{1}^{N}\right)-I\left(X_{1}^{N} ; Z^{N} \mid X_{r}^{N}\right)-H\left(X_{1}^{N} \mid W_{1}, Z^{N}, X_{r}^{N}\right)\right) \tag{A69}
\end{align*}
$$

where (a) follows from $W_{1} \rightarrow\left(X_{1}^{N}, X_{r}^{N}\right) \rightarrow Z^{N}, H\left(W_{1} \mid X_{1}^{N}\right)=0$ and the fact that $X_{1}^{N}$ is independent of $X_{r}^{N}$.
Consider the first term in A69, the code-book generation of $x_{1}^{N}$ shows that the total number of $x_{1}^{N}$ is $2^{N\left(I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-\epsilon^{\prime}\right)}$. Thus, using the same approach as that in [7, Lemma 3], we have

$$
\begin{equation*}
\frac{1}{N} H\left(X_{1}^{N}\right) \geq I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-\epsilon^{\prime}-\epsilon_{1, N} \tag{A70}
\end{equation*}
$$

where $\epsilon_{1, N} \rightarrow 0$ as $N \rightarrow \infty$.
For the second term in A69, since the channel is memoryless, and $X_{1}^{N}, X_{2}^{N}, X_{r}^{N}$ are i.i.d. generated, we get

$$
\begin{equation*}
\frac{1}{N} I\left(X_{1}^{N} ; Z^{N} \mid X_{r}^{N}\right)=I\left(X_{1} ; Z \mid X_{r}\right) \tag{A71}
\end{equation*}
$$

Now, we consider the last term of A69. Given $Z^{N}, X_{r}^{N}$ and $W_{1}$, the total number of possible codewords of $x_{1}^{N}$ is $2^{N\left(I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-\epsilon^{\prime}-R_{1}\right)}$. By using the Fano's inequality and A54, we have

$$
\begin{equation*}
\frac{1}{N} H\left(X_{1}^{N} \mid W_{1}, Z^{N}, X_{r}^{N}\right) \leq \epsilon_{2, N} \tag{A72}
\end{equation*}
$$

where $\epsilon_{2, N} \rightarrow 0$ as $N \rightarrow \infty$.
Substituting A70, A71 and A72 into A69, we have

$$
\begin{equation*}
\frac{1}{N} H\left(W_{1} \mid Z^{N}\right) \geq I\left(X_{1} ; Y, \hat{Y}_{r} \mid X_{2}, X_{r}\right)-I\left(X_{1} ; Z \mid X_{r}\right)-\epsilon^{\prime}-\epsilon_{1, N}-\epsilon_{2, N} \tag{A73}
\end{equation*}
$$

The second term in A68) is bounded the same as that for case 1 , and thus, we have

$$
\begin{equation*}
\lim _{N \rightarrow \infty} \frac{1}{N} H\left(W_{2} \mid W_{1}, Z^{N}\right) \geq I\left(X_{2} ; Y, \hat{Y}_{r} \mid X_{r}\right)-I\left(X_{2} ; Z \mid X_{1}, X_{r}\right)-\epsilon^{\prime}-\epsilon_{3, N}-\epsilon_{4, N} \tag{A74}
\end{equation*}
$$

The proof is omitted here.
Substituting A73 and A74 into A68, and choosing $\epsilon^{\prime}$ and sufficiently large $N$ such that $2 \epsilon^{\prime}+\epsilon_{1, N}+\epsilon_{2, N}+$ $\epsilon_{3, N}+\epsilon_{4, N} \leq \epsilon, \Delta \geq R_{1}+R_{2}-\epsilon$ for case 2 is proved.

The proof of Theorem 3 is completed.

## Appendix D

## Proof of Theorem 4

In this section, we prove Theorem 4. all the achievable secrecy pairs $\left(R_{1}, R_{2}\right)$ of the degraded discrete memoryless MARC-WT are contained in the set $\mathcal{R}^{d d o}$. We will prove the inequalities of Theorem 4 in the remainder of this section.
(Proof of $R_{1} \leq I\left(X_{1}, X_{r} ; Y \mid X_{2}, U\right)-I\left(X_{1} ; Z \mid U\right)$ ):

$$
\begin{aligned}
R_{1}-\epsilon & =\frac{1}{N} H\left(W_{1}\right)-\epsilon \stackrel{(1)}{\leq} \frac{1}{N} H\left(W_{1} \mid Z^{N}\right) \\
& \stackrel{(2)}{\leq} \frac{1}{N}\left(H\left(W_{1} \mid Z^{N}\right)-H\left(W_{1} \mid Z^{N}, W_{2}, Y^{N}, X_{2}^{N}\right)+\delta\left(P_{e}\right)\right) \\
& \stackrel{(3)}{=} \frac{1}{N}\left(H\left(W_{1} \mid Z^{N}\right)-H\left(W_{1} \mid Z^{N}, Y^{N}, X_{2}^{N}\right)+\delta\left(P_{e}\right)\right) \\
& =\frac{1}{N}\left(I\left(W_{1} ; Y^{N}, X_{2}^{N} \mid Z^{N}\right)+\delta\left(P_{e}\right)\right) \\
& \leq \frac{1}{N}\left(H\left(Y^{N}, X_{2}^{N} \mid Z^{N}\right)-H\left(Y^{N}, X_{2}^{N} \mid Z^{N}, W_{1}, X_{1}^{N}\right)+\delta\left(P_{e}\right)\right) \\
& \stackrel{(4)}{=} \frac{1}{N}\left(H\left(Y^{N}, X_{2}^{N} \mid Z^{N}\right)-H\left(Y^{N}, X_{2}^{N} \mid Z^{N}, X_{1}^{N}\right)+\delta\left(P_{e}\right)\right) \\
& =\frac{1}{N}\left(I\left(Y^{N}, X_{2}^{N} ; X_{1}^{N} \mid Z^{N}\right)+\delta\left(P_{e}\right)\right) \\
& \stackrel{(5)}{=} \frac{1}{N}\left(H\left(X_{1}^{N} \mid Z^{N}\right)-H\left(X_{1}^{N} \mid Z^{N}, Y^{N}, X_{2}^{N}\right)-H\left(X_{1}^{N}\right)+H\left(X_{1}^{N} \mid X_{2}^{N}\right)+\delta\left(P_{e}\right)\right) \\
& \stackrel{(6)}{=} \frac{1}{N}\left(I\left(X_{1}^{N} ; Y^{N} \mid X_{2}^{N}\right)-I\left(X_{1}^{N} ; Z^{N}\right)+\delta\left(P_{e}\right)\right) \\
& \leq \frac{1}{N}\left(I\left(X_{1}^{N}, X_{r}^{N} ; Y^{N} \mid X_{2}^{N}\right)-I\left(X_{1}^{N} ; Z^{N}\right)+\delta\left(P_{e}\right)\right) \\
& =\frac{1}{N} \sum_{i=1}^{N}\left(H\left(Y_{i} \mid Y^{i-1}, X_{2}^{N}\right)-H\left(Y_{i} \mid X_{1, i}, X_{2, i}, X_{r, i}\right)-H\left(Z_{i} \mid Z^{i-1}\right)+H\left(Z_{i} \mid Z^{i-1}, X_{1}^{N}\right)\right)+\frac{\delta\left(P_{e}\right)}{N} \\
& \stackrel{(7)}{=} \frac{1}{N} \sum_{i=1}^{N}\left(H\left(Y_{i} \mid Y^{i-1}, X_{2}^{N}, Z^{i-1}\right)-H\left(Y_{i} \mid X_{1, i}, X_{2, i}, X_{r, i}, Z^{i-1}\right)-H\left(Z_{i} \mid Z^{i-1}\right)+H\left(Z_{i} \mid Z^{i-1}, X_{1}^{N}\right)\right)+\frac{\delta\left(P_{e}\right)}{N} \\
& \frac{1}{N} \sum_{i=1}^{N}\left(H\left(Y_{i} \mid X_{2, i}, Z^{i-1}\right)-H\left(Y_{i} \mid X_{1, i}, X_{2, i}, X_{r, i}, Z^{i-1}\right)-H\left(Z_{i} \mid Z^{i-1}\right)+H\left(Z_{i} \mid Z^{i-1}, X_{1, i}\right)\right)+\frac{\delta\left(P_{e}\right)}{N} \\
& \stackrel{(8)}{=} \frac{1}{N} \sum_{i=1}^{N}\left(H\left(Y_{i} \mid X_{2, i}, Z^{i-1}, J=i\right)-H\left(Y_{i} \mid X_{1, i}, X_{2, i}, X_{r, i}, Z^{i-1}, J=i\right)-H\left(Z_{i} \mid Z^{i-1}, J=i\right)\right. \\
&
\end{aligned}
$$

$$
\begin{array}{ll} 
& \left.+H\left(Z_{i} \mid Z^{i-1}, X_{1, i}, J=i\right)\right)+\frac{\delta\left(P_{e}\right)}{N} \\
\stackrel{(9)}{=} & H\left(Y_{J} \mid X_{2, J}, Z^{J-1}, J\right)-H\left(Y_{J} \mid X_{1, J}, X_{2, J}, X_{r, J}, Z^{J-1}, J\right)-H\left(Z_{J} \mid Z^{J-1}, J\right)+H\left(Z_{J} \mid Z^{J-1}, X_{1, J}, J\right)+\frac{\delta\left(P_{e}\right)}{N} \\
\stackrel{(10)}{=} & I\left(X_{1}, X_{r} ; Y \mid X_{2}, U\right)-I\left(X_{1} ; Z \mid U\right)+\frac{\delta\left(P_{e}\right)}{N}, \tag{A75}
\end{array}
$$

where (1) is from the fact that the secrecy requirement on the full message set also ensures the secrecy of individual message (see 2.3), (2) is from the Fanos inequality, (3) is from $H\left(W_{2} \mid X_{2}^{N}\right)=0$, (4) is from $H\left(W_{1} \mid X_{1}^{N}\right)=0$, (5) and (6) are from the fact that the wiretap channel is degraded, which implies the Markov chain $X_{1}^{N} \rightarrow\left(X_{2}^{N}, Y^{N}\right) \rightarrow$ $Z^{N}$, and from the fact that $X_{1}^{N}$ is independent of $X_{2}^{N}$, (7) is from the Markov chains $Y_{i} \rightarrow\left(Y^{i-1}, X_{2}^{N}\right) \rightarrow Z^{i-1}$ and $Y_{i} \rightarrow\left(X_{1, i}, X_{2, i}, X_{r, i}\right) \rightarrow Z^{i-1}$ (these Markov chains are also from the fact that the wiretap channel is degraded), (8) is from $J$ is a random variable (uniformly distributed over $\{1,2, \ldots, N\}$ ), and it is independent of $X_{1}^{N}, X_{2}^{N}, X_{r}^{N}, Y^{N}$ and $Z^{N}$, (9) is from $J$ is uniformly distributed over $\{1,2, \ldots, N\}$, and (10) is from the definitions that $X_{1} \triangleq X_{1, J}, X_{2} \triangleq X_{2, J}, X_{r} \triangleq X_{r, J}, Y \triangleq Y_{J}, Z \triangleq Z_{J}$ and $U \triangleq\left(Z^{J-1}, J\right)$.

By using $P_{e} \leq \epsilon$ and letting $\epsilon \rightarrow 0, R_{1} \leq I\left(X_{1}, X_{r} ; Y \mid X_{2}, U\right)-I\left(X_{1} ; Z \mid U\right)$ is proved.
(Proof of $R_{2} \leq I\left(X_{2}, X_{r} ; Y \mid X_{1}, U\right)-I\left(X_{2} ; Z \mid U\right)$ ):
The proof is analogous to the proof of $R_{1} \leq I\left(X_{1}, X_{r} ; Y \mid X_{2}, U\right)-I\left(X_{1} ; Z \mid U\right)$, and it is omitted here.
Proof of $R_{1}+R_{2} \leq I\left(X_{1}, X_{2}, X_{r} ; Y \mid U\right)-I\left(X_{1}, X_{2} ; Z \mid U\right)$ :

$$
\begin{aligned}
& R_{1}+R_{2}-\epsilon \stackrel{(1)}{\leq} \Delta=\frac{1}{N} H\left(W_{1}, W_{2} \mid Z^{N}\right) \\
& \stackrel{(2)}{\leq} \frac{1}{N}\left(H\left(W_{1}, W_{2} \mid Z^{N}\right)+\delta\left(P_{e}\right)-H\left(W_{1}, W_{2} \mid Y^{N}, Z^{N}\right)\right) \\
& \leq \frac{1}{N}\left(H\left(Y^{N} \mid Z^{N}\right)-H\left(Y^{N} \mid Z^{N}, W_{1}, W_{2}, X_{1}^{N}, X_{2}^{N}\right)+\delta\left(P_{e}\right)\right) \\
& \stackrel{(3)}{=} \frac{1}{N}\left(H\left(Y^{N} \mid Z^{N}\right)-H\left(Y^{N} \mid Z^{N}, X_{1}^{N}, X_{2}^{N}\right)+\delta\left(P_{e}\right)\right) \\
&= \frac{1}{N}\left(I\left(X_{1}^{N}, X_{2}^{N} ; Y^{N}\right)-I\left(X_{1}^{N}, X_{2}^{N} ; Z^{N}\right)+\delta\left(P_{e}\right)\right) \\
& \leq \frac{1}{N}\left(I\left(X_{1}^{N}, X_{2}^{N}, X_{r}^{N} ; Y^{N}\right)-I\left(X_{1}^{N}, X_{2}^{N} ; Z^{N}\right)+\delta\left(P_{e}\right)\right) \\
& \stackrel{(4)}{=} \frac{1}{N} \sum_{i=1}^{N}\left(H\left(Y_{i} \mid Y^{i-1}\right)-H\left(Y_{i} \mid X_{1, i}, X_{2, i}, X_{r, i}, Z^{i-1}\right)-H\left(Z_{i} \mid Z^{i-1}\right)+H\left(Z_{i} \mid X_{1, i}, X_{2, i}, Z^{i-1}\right)\right)+\frac{\delta\left(P_{e}\right)}{N} \\
& \stackrel{(5)}{\leq} \frac{1}{N} \sum_{i=1}^{N}\left(H\left(Y_{i} \mid Z^{i-1}\right)-H\left(Y_{i} \mid X_{1, i}, X_{2, i}, X_{r, i}, Z^{i-1}\right)-H\left(Z_{i} \mid Z^{i-1}\right)+H\left(Z_{i} \mid X_{1, i}, X_{2, i}, Z^{i-1}\right)\right)+\frac{\delta\left(P_{e}\right)}{N} \\
& \stackrel{(6)}{=} \frac{1}{N} \sum_{i=1}^{N}\left(H\left(Y_{i} \mid Z^{i-1}, J=i\right)-H\left(Y_{i} \mid X_{1, i}, X_{2, i}, X_{r, i}, Z^{i-1}, J=i\right)\right. \\
&\left.-H\left(Z_{i} \mid Z^{i-1}, J=i\right)+H\left(Z_{i} \mid X_{1, i}, X_{2, i}, Z^{i-1}, J=i\right)\right)+\frac{\delta\left(P_{e}\right)}{N} \\
& \stackrel{(7)}{=} H\left(Y_{J} \mid Z^{J-1}, J\right)-H\left(Y_{J} \mid X_{1, J}, X_{2, J}, X_{r, J}, Z^{J-1}, J\right) \\
&-H\left(Z_{J} \mid Z^{J-1}, J\right)+H\left(Z_{J} \mid X_{1, J}, X_{2, J}, Z^{J-1}, J\right)+\frac{\delta\left(P_{e}\right)}{N}
\end{aligned}
$$

$$
\begin{equation*}
\stackrel{(8)}{\leq} I\left(X_{1}, X_{2}, X_{r} ; Y \mid U\right)-I\left(X_{1}, X_{2} ; Z \mid U\right)+\frac{\delta(\epsilon)}{N} \tag{A76}
\end{equation*}
$$

where (1) is from 2.2, (2) is from the Fanos inequality, (3) is from $\left(W_{1}, W_{2}\right) \rightarrow\left(X_{1}^{N}, X_{2}^{N}, Z^{N}\right) \rightarrow Y^{N}$, (4) is from $Y_{i} \rightarrow\left(X_{1, i}, X_{2, i}, X_{r, i}\right) \rightarrow Z^{i-1}$, (5) is from $Y_{i} \rightarrow Y^{i-1} \rightarrow Z^{i-1}$, (6) is from $J$ is a random variable (uniformly distributed over $\{1,2, \ldots, N\}$ ), and it is independent of $X_{1}^{N}, X_{2}^{N}, X_{r}^{N}, Y^{N}$ and $Z^{N}$, (7) is from $J$ is uniformly distributed over $\{1,2, \ldots, N\}$, and (8) is from the definitions that $X_{1} \triangleq X_{1, J}, X_{2} \triangleq X_{2, J}, X_{r} \triangleq X_{r, J}$, $Y \triangleq Y_{J}, Z \triangleq Z_{J}$ and $U \triangleq\left(Z^{J-1}, J\right)$, and the fact that $P_{e} \leq \epsilon$.

Letting $\epsilon \rightarrow 0, R_{1}+R_{2} \leq I\left(X_{1}, X_{2}, X_{r} ; Y \mid U\right)-I\left(X_{1}, X_{2} ; Z \mid U\right)$ is proved.
The proof of Theorem 4 is completed.

## Appendix E

## Proof of Theorem 8

Since $N_{2} \geq N_{1}$, the GMARC-WT reduces to a kind of degraded MARC-WT with the Markov chain $\left(X_{1}, X_{2}, X_{r}, Y_{r}\right) \rightarrow$ $Y \rightarrow Z$, and thus the outer bound $\mathcal{R}^{\text {gout }}$ can be obtained from Theorem 4 . The details are as follows.

From A75, we know that

$$
\begin{align*}
R_{1} \leq & \frac{1}{N} \sum_{i=1}^{N}\left(h\left(Y_{i} \mid X_{2, i}, Z^{i-1}\right)-h\left(Y_{i} \mid X_{1, i}, X_{2, i}, X_{r, i}, Z^{i-1}\right)\right. \\
& \left.-h\left(Z_{i} \mid Z^{i-1}\right)+h\left(Z_{i} \mid Z^{i-1}, X_{1, i}\right)\right)+\frac{\delta\left(P_{e}\right)}{N} \tag{A77}
\end{align*}
$$

Analogously,

$$
\begin{align*}
R_{2} \leq & \frac{1}{N} \sum_{i=1}^{N}\left(h\left(Y_{i} \mid X_{1, i}, Z^{i-1}\right)-h\left(Y_{i} \mid X_{1, i}, X_{2, i}, X_{r, i}, Z^{i-1}\right)-h\left(Z_{i} \mid Z^{i-1}\right)\right. \\
& \left.+h\left(Z_{i} \mid Z^{i-1}, X_{2, i}\right)\right)+\frac{\delta\left(P_{e}\right)}{N} \tag{A78}
\end{align*}
$$

From A76, we have

$$
\begin{align*}
R_{1}+R_{2} \leq & \frac{1}{N} \sum_{i=1}^{N}\left(h\left(Y_{i} \mid Z^{i-1}\right)-h\left(Y_{i} \mid X_{1, i}, X_{2, i}, X_{r, i}, Z^{i-1}\right)-h\left(Z_{i} \mid Z^{i-1}\right)\right. \\
& \left.\left.+h\left(Z_{i} \mid X_{1, i}, X_{2, i}, Z^{i-1}\right)\right)+\frac{\delta\left(P_{e}\right)}{N}\right) \tag{A79}
\end{align*}
$$

It remains to bound the conditional entropies in A77, A78 and A79, see the followings.
First note that

$$
\begin{aligned}
\frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid X_{1, i}, X_{2, i}, Z^{i-1}\right) & \leq \frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid X_{1, i}, X_{2, i}\right) \\
& \stackrel{(1)}{\leq} \frac{1}{N} \sum_{i=1}^{N} h\left(Z_{2, i}+X_{r, i}\right) \\
& \leq \frac{1}{N} \sum_{i=1}^{N} \frac{1}{2} \log 2 \pi e\left(E\left[X_{r, i}^{2}\right]+N_{2}\right)
\end{aligned}
$$

$$
\begin{align*}
& \stackrel{(2)}{\leq} \frac{1}{2} \log 2 \pi e\left(\frac{1}{N} \sum_{i=1}^{N} E\left[X_{r, i}^{2}\right]+N_{2}\right) \\
& \leq \frac{1}{2} \log 2 \pi e\left(P_{r}+N_{2}\right) \tag{A80}
\end{align*}
$$

where (1) is from $Z_{i}=X_{1, i}+X_{2, i}+X_{r, i}+Z_{2, i}$, and (2) is from Jensen's inequality.
On the other hand,

$$
\begin{align*}
\frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid X_{1, i}, X_{2, i}, Z^{i-1}\right) & \geq \frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid X_{1, i}, X_{2, i}, X_{r, i}, Z^{i-1}\right) \\
& \stackrel{(a)}{=} \frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid X_{1, i}, X_{2, i}, X_{r, i}\right) \\
& =\frac{1}{N} \sum_{i=1}^{N} h\left(Z_{2, i}\right) \\
& =\frac{1}{N} \sum_{i=1}^{N} \frac{1}{2} \log 2 \pi e N_{2}=\frac{1}{2} \log 2 \pi e N_{2} \tag{A81}
\end{align*}
$$

where (a) is from the Markov chain $Z^{i-1} \rightarrow\left(X_{1, i}, X_{2, i}, X_{r, i}\right) \rightarrow Z_{i}$.
Combining A80 and A81, we establish that there exists some $\alpha \in[0,1]$ such that

$$
\begin{equation*}
\frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid X_{1, i}, X_{2, i}, Z^{i-1}\right)=\frac{1}{2} \log 2 \pi e\left(\alpha P_{r}+N_{2}\right) \tag{A82}
\end{equation*}
$$

Second, since

$$
\begin{align*}
\frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid X_{1, i}, Z^{i-1}\right) & \geq \frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid X_{1, i}, X_{2, i}, Z^{i-1}\right) \\
& =\frac{1}{2} \log 2 \pi e\left(\alpha P_{r}+N_{2}\right) \tag{A83}
\end{align*}
$$

and

$$
\begin{align*}
\frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid X_{1, i}, Z^{i-1}\right) & \leq \frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid X_{1, i}\right) \\
& \leq \frac{1}{N} \sum_{i=1}^{N} h\left(Z_{2, i}+X_{2, i}+X_{r, i}\right) \\
& \leq \frac{1}{N} \sum_{i=1}^{N} \frac{1}{2} \log 2 \pi e\left(E\left[X_{r, i}^{2}\right]+E\left[X_{2, i}^{2}\right]+N_{2}\right) \\
& \leq \frac{1}{2} \log 2 \pi e\left(\frac{1}{N} \sum_{i=1}^{N} E\left[X_{r, i}^{2}\right]+\frac{1}{N} \sum_{i=1}^{N} E\left[X_{2, i}^{2}\right]+N_{2}\right) \\
& \leq \frac{1}{2} \log 2 \pi e\left(P_{r}+P_{2}+N_{2}\right) \tag{A84}
\end{align*}
$$

we establish that there exists some $\beta_{1} \in[0,1]$ such that

$$
\begin{align*}
& \frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid X_{1, i}, Z^{i-1}\right)=\frac{1}{2} \log 2 \pi e\left(\alpha P_{r}+N_{2}+\beta_{1}\left(P_{r}+P_{2}+N_{2}-\alpha P_{r}-N_{2}\right)\right) \\
& =\frac{1}{2} \log 2 \pi e\left(N_{2}+P_{r}\left(\alpha+\beta_{1}-\alpha \beta_{1}\right)+\beta_{1} P_{2}\right) \tag{A85}
\end{align*}
$$

Third, analogously, there exists some $\beta_{2} \in[0,1]$ such that

$$
\begin{equation*}
\frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid X_{2, i}, Z^{i-1}\right)=\frac{1}{2} \log 2 \pi e\left(N_{2}+P_{r}\left(\alpha+\beta_{2}-\alpha \beta_{2}\right)+\beta_{2} P_{1}\right) \tag{A86}
\end{equation*}
$$

Fourth, since

$$
\begin{align*}
\frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid Z^{i-1}\right) & \geq \frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid X_{1, i}, Z^{i-1}\right) \\
& =\frac{1}{2} \log 2 \pi e\left(N_{2}+P_{r}\left(\alpha+\beta_{1}-\alpha \beta_{1}\right)+\beta_{1} P_{2}\right)  \tag{A87}\\
\frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid Z^{i-1}\right) & \geq \frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid X_{2, i}, Z^{i-1}\right) \\
& =\frac{1}{2} \log 2 \pi e\left(N_{2}+P_{r}\left(\alpha+\beta_{2}-\alpha \beta_{2}\right)+\beta_{2} P_{1}\right) \tag{A88}
\end{align*}
$$

and

$$
\begin{align*}
\frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid Z^{i-1}\right) & \leq \frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i}\right) \\
& =\frac{1}{N} \sum_{i=1}^{N} h\left(Z_{2, i}+X_{1, i}+X_{2, i}+X_{r, i}\right) \\
& \leq \frac{1}{N} \sum_{i=1}^{N} \frac{1}{2} \log 2 \pi e\left(E\left[X_{r, i}^{2}\right]+E\left[X_{1, i}^{2}\right]+E\left[X_{2, i}^{2}\right]+N_{2}\right) \\
& \leq \frac{1}{2} \log 2 \pi e\left(\frac{1}{N} \sum_{i=1}^{N} E\left[X_{r, i}^{2}\right]+\frac{1}{N} \sum_{i=1}^{N} E\left[X_{1, i}^{2}\right]+\frac{1}{N} \sum_{i=1}^{N} E\left[X_{2, i}^{2}\right]+N_{2}\right) \\
& \leq \frac{1}{2} \log 2 \pi e\left(P_{r}+P_{1}+P_{2}+N_{2}\right) \tag{A89}
\end{align*}
$$

there exists some $\gamma \in[0,1]$ such that

$$
\begin{equation*}
\frac{1}{N} \sum_{i=1}^{N} h\left(Z_{i} \mid Z^{i-1}\right)=\frac{1}{2} \log 2 \pi e\left(C+\gamma\left(P_{r}+P_{1}+P_{2}+N_{2}-C\right)\right) \tag{A90}
\end{equation*}
$$

where $C$ is given by

$$
\begin{equation*}
C=\max \left\{N_{2}+P_{r}\left(\alpha+\beta_{1}-\alpha \beta_{1}\right)+\beta_{1} P_{2}, N_{2}+P_{r}\left(\alpha+\beta_{2}-\alpha \beta_{2}\right)+\beta_{2} P_{1}\right\} \tag{A91}
\end{equation*}
$$

Fifth, by using the entropy power inequality, we have

$$
\begin{align*}
2^{2 h\left(Z_{i} \mid X_{1, i}, Z^{i-1}\right)} & \stackrel{(1)}{=} 2^{2 h\left(Y_{i}+Z_{2, i}^{\prime} \mid X_{1, i}, Z^{i-1}\right)} \\
& \stackrel{(2)}{\geq} 2^{2 h\left(Y_{i} \mid X_{1, i}, Z^{i-1}\right)}+2^{2 h\left(Z_{2, i}^{\prime} \mid X_{1, i}, Z^{i-1}\right)} \\
& \stackrel{(3)}{=} 2^{2 h\left(Y_{i} \mid X_{1, i}, Z^{i-1}\right)}+2^{2 h\left(Z_{2, i}^{\prime}\right)} \tag{A92}
\end{align*}
$$

where (1) is from the definition that $Z_{2, i}^{\prime}=Z_{2, i}-Z_{1, i}$, (2) is from the entropy power inequality, and (3) is from $Z_{2, i}^{\prime}$ is independent of $X_{1, i}$ and $Z^{i-1}$.

Substituting $h\left(Z_{2, i}^{\prime}\right)=\frac{1}{2} \log 2 \pi e\left(N_{2}-N_{1}\right)$ and A85 into A92, and using Jensen's inequality, we have

$$
\begin{equation*}
\frac{1}{N} \sum_{i=1}^{N} h\left(Y_{i} \mid X_{1, i}, Z^{i-1}\right) \leq \frac{1}{2} \log 2 \pi e\left(P_{r}\left(\alpha+\beta_{1}-\alpha \beta_{1}\right)+\beta_{1} P_{2}+N_{1}\right) \tag{A93}
\end{equation*}
$$

Analogously, we have

$$
\begin{equation*}
\frac{1}{N} \sum_{i=1}^{N} h\left(Y_{i} \mid X_{2, i}, Z^{i-1}\right) \leq \frac{1}{2} \log 2 \pi e\left(P_{r}\left(\alpha+\beta_{2}-\alpha \beta_{2}\right)+\beta_{2} P_{1}+N_{1}\right) \tag{A94}
\end{equation*}
$$

and

$$
\begin{equation*}
\frac{1}{N} \sum_{i=1}^{N} h\left(Y_{i} \mid Z^{i-1}\right) \leq \frac{1}{2} \log 2 \pi e\left(C+\gamma\left(P_{r}+P_{1}+P_{2}+N_{1}-C\right)\right) \tag{A95}
\end{equation*}
$$

Finally, note that

$$
\begin{align*}
h\left(Y_{i} \mid X_{1, i}, X_{2, i}, X_{r, i}, Z^{i-1}\right) & =h\left(Z_{1, i} \mid X_{1, i}, X_{2, i}, X_{r, i}, Z^{i-1}\right) \\
& \stackrel{(1)}{=} h\left(Z_{1, i}\right)=\frac{1}{2} \log 2 \pi e N_{1} \tag{A96}
\end{align*}
$$

where (1) is from $Z_{1, i}$ is independent of $X_{1, i}, X_{2, i}, X_{r, i}$ and $Z^{i-1}$.
Substituting A82, A85, A86, A90, A93, A94, A95 and A96, into A77, A78 and A79, using the fact that $P_{e} \leq \epsilon$ and letting $\epsilon \rightarrow 0$, Theorem 8 is proved.

## REFERENCES

[1] A. D. Wyner, "The wire-tap channel," The Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, 1975.
[2] S. K. Leung-Yan-Cheong, M. E. Hellman, "The Gaussian wire-tap channel," IEEE Trans Inf Theory, vol. IT-24, no. 4, pp. 451-456, July 1978.
[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Trans Inf Theory, vol. IT-24, no. 3, pp. 339-348, May 1978.
[4] J. Körner and K. Marton, "General broadcast channels with degraded message sets," IEEE Trans Inf Theory, vol. IT-23, no. 1, pp. 60-64, January 1977.
[5] R. Liu, I. Maric, P. Spasojevic and R.D Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," IEEE Trans Inf Theory, vol. IT-54, no. 6, pp. 2493-2507, Jun. 2008.
[6] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," IEEE Trans Inf Theory, vol. IT-55, no. 6, pp. 4529-4542. 2009.
[7] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," IEEE Trans Inf Theory, vol. IT-54, no. 3, pp. 976-1002, Mar. 2008.
[8] 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.
[9] 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.
[10] 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.
[11] R. Bassily and S. Ulukus, "A New Achievable Ergodic Secrecy Rate Region for the Fading Multiple Access Wiretap Channel," in Proc. Annual Allerton Conf. on Communications, Control and Computing, Monticello, IL, Sept. 2009.
[12] 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.
[13] M. Wiese and H. Boche, "Strong secrecy for multiple access channels," Information Theory, Combinatorics, and Search Theory, Springer Berlin Heidelberg, pp. 71-122, 2013.
[14] M. H. Yassaee and M. R. Aref, "Multiple access wiretap channels with strong secrecy," Proceedings of IEEE Information Theory Workshop, 2010.
[15] X. He, A. Khisti, and A. Yener, "MIMO Multiple Access Channel With an Arbitrarily Varying Eavesdropper: Secrecy Degrees of Freedom," IEEE Trans Inf Theory, vol. IT-59, no. 8, pp. 4733-4745, 2013.
[16] P. Xu, Z. Ding, and X. Dai, "Rate Regions for Multiple Access Channel With Conference and Secrecy Constraints," IEEE Trans. Inf. Forensics and Security, vol. 8, no. 12, pp. 1961-1974, 2013.
[17] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," IEEE Trans. Inf. Theory, vol. IT-55, pp. 604-619, 2009.
[18] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," IEEE Trans Inf Theory, vol. IT-54, no. 9, pp. 4005C4019, Sep. 2008.
[19] Y. Oohama, "Coding for relay channels with confidential messages," in Proceedings of IEEE Information Theory Workshop, Australia, 2001.
[20] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," IEEE Trans Inf Theory, vol. IT-57, pp. 137-155, 2011.
[21] G. Kramer, M. Gastpar and P. Gupta, "Cooperative strategies and capacity theorems for relay networks," IEEE Trans Inf Theory, vol. IT-51, pp. 3037-3063, 2005.
[22] Y. Liang, H. V. Poor and S. Shamai, "Secure communication over fading channels," IEEE Trans Inf Theory, vol. IT-54, pp. 2470-2492, 2008.
[23] T. M. Cover and A. El Gamal, "Capacity theorems for the relay channel," IEEE Trans Inf Theory, vol. IT-25, pp. 572-584, 1979.
[24] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," IEEE Trans Inf Theory, vol. IT-25, pp. 306-311, 1979.
[25] A. A. El Gamal and E. C. van der Meulen, "A proof of Martons coding theorems for the discrete memoryless broadcast channel," IEEE Trans Inf Theory, vol. IT-27, pp. 120-122, 1981.
[26] L. Sankaranarayanan , G. Kramer and N. B. Mandayam, "Capacity theorems for the multiple-access relay channel," Proceedings of Allerton Conference on Communications, Control and Computing, 2004.
[27] X. Tang, R. Liu, P. P. Spasojevic and H. V. Poor, "Interference assisted secret communication," IEEE Trans Inf Theory, vol. IT-57, pp. 3153-3167, 2011.
[28] A. El Gamal and Y. H. Kim, Network information theory. Cambridge University Press, 2011.


[^0]:    B. Dai and Z. Ma are with the School of Information Science and Technology, Southwest JiaoTong University, Chengdu 610031, China

