Relay Broadcast Channels with Confidential Messages

Bin Dai and Zheng Ma

Abstract

We investigate the effects of an additional relay node on the secrecy of broadcast channels by considering the model of relay broadcast channels with confidential messages. We show that this additional relay node can increase the achievable secrecy rate region of the broadcast channels with confidential messages. More specifically, first, we investigate the discrete memoryless relay broadcast channels with two confidential messages and one common message. Three inner bounds (with respect to decode-forward, generalized noise-forward and compress-forward strategies) and an outer bound on the capacity-equivocation region are provided. Removing the secrecy constraint, this outer bound can also be served as a new outer bound for the relay broadcast channel. Second, we investigate the discrete memoryless relay broadcast channels with two confidential messages (no common message). Inner and outer bounds on the capacity-equivocation region are provided. Then, we study the Gaussian case, and find that with the help of the relay node, the achievable secrecy rate region of the Gaussian broadcast channels with two confidential messages is enhanced. Finally, we investigate the discrete memoryless relay broadcast channels with one confidential message and one common message. This work generalizes Lai-Gamals work on the relay-eavesdropper channel by considering an additional common message for both the legitimate receiver and the eavesdropper. Inner and outer bounds on the capacity-equivocation region are provided, and the results are further explained via a Gaussian example. Compared with Csiszár-Körner’s work on broadcast channels with confidential messages (BCC), we find that with the help of the relay node, the secrecy capacity region of the Gaussian BCC is enhanced.

Index Terms

Capacity-equivocation region, confidential messages, relay broadcast channel, secrecy capacity region.

I. INTRODUCTION

The security of a communication system was first studied by Shannon [1] from a standpoint of information theory. He discussed a theoretical model of cryptosystems using the framework of classical one way noiseless channels and derived some conditions for secure communication. Subsequently, Wyner, in his paper on the discrete memoryless wiretap channel [2], studied the problem that how to transmit the confidential messages to the legitimate receiver via a discrete memoryless degraded broadcast channel, while keeping the wiretapper as ignorant of the messages.
as possible. Measuring the uncertainty of the wiretapper by equivocation, the capacity-equivocation region was established. Furthermore, the secrecy capacity was also established, which provided the maximum transmission rate with perfect secrecy. Based on Wyner’s work, Leung-Yan-Cheong and Hellman studied the Gaussian wiretap channel (GWC) [3], 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). Moreover, Merhav [4] studied a specified wiretap channel, and obtained the capacity-equivocation region, where both the legitimate receiver and the wiretapper have access to some leaked symbols from the source, but the channels for the wiretapper are more noisy than the legitimate receiver, which shares a secret key with the encoder.

Other related works on the wiretap channel are split into the following four directions.

- The first is the wiretap channel with feedback, and it was first investigated by Ahlswede and Cai [5]. In [5], the general wiretap channel (not physically or stochastically degraded) with noiseless feedback from the legitimate receiver to the channel encoder was studied, and both upper and lower bounds on the secrecy capacity were provided. Specifically, for the physically degraded case, they showed that the secrecy capacity is larger than that of Wyner’s wiretap channel (without feedback), i.e., the noiseless feedback helps to enhance the secrecy capacity of [2]. Besides Ahlswede and Cai’s work, the wiretap channel with noisy feedback was studied in [6], and the wiretap channel with secure rate-limited feedback was studied in [7], and both of them focused on bounds of the secrecy capacity.

- The second is the wiretap channel with channel state information (CSI). Mitrpant et al. [8] studied the Gaussian wiretap channel with CSI, and provided an inner bound on the capacity-equivocation region. Furthermore, Chen et al. [9] investigated the discrete memoryless wiretap channel with noncausal CSI (CSI is available to the channel encoder in a noncausal manner), and also provided an inner bound on the capacity-equivocation region.

- The third is the compound wiretap channel. The compound wiretap channel can be viewed as a wiretap channel with multiple legitimate receivers and multiple wiretappers, and the source message must be successfully transmitted to all receivers and must be kept secret from all wiretappers. The compound wiretap channel was studied in [10], [11], [12], [13], [14], [15], [16].

- The fourth is the MIMO compound wiretap channel, in which the transmitters, legitimate receivers and the wiretappers are equipped with several antennas. The MIMO compound wiretap channel was studied in [17], [18], [19].

After the publication of Wyner’s work, Csiszár and Körner [20] 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 [21], where no confidentiality condition is imposed. The capacity-equivocation region and the secrecy capacity region of BCC [20] were totally determined, and the results were also a generalization of those in [2]. Furthermore, the capacity-equivocation region of Gaussian BCC was
determined in [33].

By using the approach of [2] and [20], the information-theoretic security for other multi-user communication systems has been widely studied, see the followings.

- For the broadcast channel, Liu et al. [22] 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. [23] 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 [24]. An inner bound on the capacity-equivocation region is provided for the model with two confidential messages, and the capacity-equivocation region is still not known. Furthermore, for the model of MAC with one confidential message [24], 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 [25]. 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 [26], [27].

- For the interference channel, Liu et al. [22] studied the interference channel with two confidential messages, and provided inner and outer bounds on the secrecy capacity region. In addition, Liang et al. [28] studied the cognitive interference channel with one common message and one confidential message, and the capacity-equivocation region was totally determined for this model.

- For the relay channel, Lai and Gamal [29] studied the relay-eavesdropper channel, where a source wishes to send messages to a destination while leveraging the help of a relay node to hide those messages from the eavesdropper. 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 [29]. In addition, Oohama [30] 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 [30].
Recently, Ekrem and Ulukus [31] 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 [22].

In this paper, first, we study the relay broadcast channels with two confidential messages and one common message, see Figure 1. This model generalizes the broadcast channels with confidential messages [23] by considering an additional relay node. The motivation of this work is to investigate the effects of an additional relay node on the secrecy of broadcast channels, and whether the achievable rate-equivocation regions of [20], [22], [23] can be enhanced by using an additional relay node.

![Fig. 1: Relay broadcast channels with two confidential messages and one common message](image)

For the model of Figure 1, we provide inner and outer bounds on the capacity-equivocation region. The decode-forward (DF), generalized noise-forward (GNF) and compress-forward (CF) relay strategies are used in the construction of the inner bounds. Of particular interest is the generalized noise-forward relay strategy, which is an extension of Lai-Gamal’s noise-forward (NF) strategy [29]. The idea of this strategy is as follows.

The relay sends the codeword \( x_1^N \) to both receivers, and \( x_1^N \) is independent of the transmitter’s messages.

- If the channel from the relay to receiver 1 is less noisy than the channel from the relay to receiver 2, we allow receiver 1 to decode \( x_1^N \), and receiver 2 can not decode \( x_1^N \). Therefore, in this case, \( x_1^N \) can be viewed as a noise signal to confuse receiver 2.

- If the channel from the relay to receiver 1 is more noisy than the channel from the relay to receiver 2, we allow receiver 2 to decode \( x_1^N \), and receiver 1 can not decode \( x_1^N \). Therefore, in this case, \( x_1^N \) can be viewed as a noise signal to confuse receiver 1.

The outer bound on the capacity-equivocation region of the model of Figure 1 generalizes the outer bound in [23]. In addition, removing the secrecy constraint, this outer bound can also be served as a new bound for the relay broadcast channel.

Second, we study the relay broadcast channels with two confidential messages (no common message), see Figure 2. Inner and outer bounds on the capacity-equivocation region of Figure 2 are provided. The outer bound is directly obtained from that of Figure 1. The inner bounds are also constructed according to the three relay strategies (DF,
GNF, CF). In addition, we present a Gaussian example for the model of Figure 2 and find that with the help of the relay, the achievable secrecy rate region of the Gaussian broadcast channels with two confidential messages is enhanced.

![Fig. 2: Relay broadcast channels with two confidential messages](image)

Third, we study the relay broadcast channels with one confidential message and one common message, see Figure 3. This model generalizes Lai-Gamal’s work [29] by considering an additional common message. Inner and outer bounds on the capacity-equivocation region are also provided. The outer bound is also directly obtained from that of Figure 1. The inner bounds are constructed according to the DF, NF and CF strategies. Here note that the NF strategy of Figure 3 is slightly different from that of Figure 1 and it is considered into two cases, see the followsings.

- If the channel from the relay to receiver 1 is less noisy than the channel from the relay to receiver 2, we allow receiver 1 to decode $x_1^N$, and receiver 2 can not decode $x_1^N$. Therefore, in this case, $x_1^N$ can be viewed as a noise signal to confuse receiver 2.
- If the channel from the relay to receiver 1 is more noisy than the channel from the relay to receiver 2, we allow both the receivers to decode $x_1^N$, and therefore, in this case, the relay codeword $x_1^N$ can not make any contribution to the security of the model of Figure 3.

Moreover, a Gaussian example for the model of Figure 3 is provided, and we find that with the help of the relay, the secrecy capacity region of the Gaussian BCC [33] is enhanced.

![Fig. 3: Relay broadcast channels with one confidential message and one common message](image)
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 $(U_1, ..., U_N)$, and $u^N = (u_1, ..., u_N)$ is a specific vector value in $U^N$ that is the $N$th Cartesian power of $U$. $U_i^N$ denotes a random $N-i+1$-vector $(U_i, ..., U_N)$, and $u_i^N = (u_i, ..., u_N)$ is a specific vector value in $U_i^N$. Let $p_{V}(v)$ denote the probability mass function $Pr\{V = v\}$.

Throughout the paper, the logarithmic function is to the base 2.

The organization of this paper is as follows. Section II provides the inner and outer bounds on the capacity-equivocation region of the model of Figure 1. The model of Figure 2 and its Gaussian case are investigated in Section III. The model of Figure 3 and its Gaussian case are investigated in Section IV. Final conclusions are provided in Section V.

II. RELAY BROADCAST CHANNELS WITH TWO CONFIDENTIAL MESSAGES AND ONE COMMON MESSAGE

The model of Figure 1 is a four-terminal discrete channel consisting of finite sets $X$, $X_1$, $Y$, $Y_1$, $Z$ and a transition probability distribution $p_{Y,Y_1,Z|X,X_1,Y}(y,y_1,z|x,x_1)$. $X^N$ and $X^N_1$ are the channel inputs from the transmitter and the relay respectively, while $Y^N$, $Y^N_1$, $Z^N$ are the channel outputs at receiver 1, relay and receiver 2, respectively. The channel is discrete memoryless, i.e., the channel outputs $(y_i; y_{1,i}, z_i)$ at time $i$ only depend on the channel inputs $(x_i; x_{1,i})$ at time $i$.

**Definition 1:** (Channel encoder) The confidential messages $W_1$ and $W_2$ take values in $W_1$, $W_2$, respectively. The common message $W_0$ takes values in $W_0$. $W_1$, $W_2$ and $W_0$ are independent and uniformly distributed over their ranges. The channel encoder is a stochastic encoder $f_E$ that maps the messages $w_1$, $w_2$ and $w_0$ into a codeword $x^N \in \mathcal{X}^N$. The transmission rates of the confidential messages $(W_1, W_2)$ and the common message $(W_0)$ are $\frac{\log \|W_1\|}{N}$, $\frac{\log \|W_2\|}{N}$ and $\frac{\log \|W_0\|}{N}$, respectively.

**Definition 2:** (Relay encoder) The relay encoder is also a stochastic encoder $\varphi_1$ that maps the signals $(y_{1,1}, y_{1,2}, ..., y_{1,i-1})$ received before time $i$ to the channel input $x_{1,i}$.

**Definition 3:** (Decoder) The Decoder for receiver 1 is a mapping $f_{D1} : Y^N \rightarrow W_0 \times W_1$, with input $Y^N$ and outputs $\hat{W}_0$, $\hat{W}_1$. Let $P_{e1}$ be the error probability of receiver 1, and it is defined as $Pr\{(W_0, W_1) \neq (\hat{W}_0, \hat{W}_1)\}$.

The Decoder for receiver 2 is a mapping $f_{D2} : Z^N \rightarrow W_0 \times W_2$, with input $Z^N$ and outputs $\hat{W}_0$, $\hat{W}_2$. Let $P_{e2}$ be the error probability of receiver 1, and it is defined as $Pr\{(W_0, W_2) \neq (\hat{W}_0, \hat{W}_2)\}$.

The equivocation rate at receiver 2 is defined as

$$\Delta_1 = \frac{1}{N}H(W_1|Z^N). \quad (2.1)$$

Analogously, the equivocation rate at receiver 1 is defined as

$$\Delta_2 = \frac{1}{N}H(W_2|Y^N). \quad (2.2)$$

A rate quintuple $(R_0, R_1, R_2, R_{e1}, R_{e2})$ (where $R_0, R_1, R_2, R_{e1}, R_{e2} > 0$) is called achievable if, for any $\epsilon > 0$ (where $\epsilon$ is an arbitrary small positive real number and $\epsilon \rightarrow 0$), there exists a channel encoder-decoder
\((N, \Delta_1, \Delta_2, P_{e1}, P_{e2})\) such that
\[
\lim_{N \to \infty} \frac{\log \|W_0\|}{N} = R_0, \quad \lim_{N \to \infty} \frac{\log \|W_1\|}{N} = R_1, \quad \lim_{N \to \infty} \frac{\log \|W_2\|}{N} = R_2,
\]
\[
\lim_{N \to \infty} \Delta_1 \geq R_{e1}, \quad \lim_{N \to \infty} \Delta_2 \geq R_{e2}, \quad P_{e1} \leq \epsilon, \quad P_{e2} \leq \epsilon.
\]

(2.3)

The capacity-equivocation region \(\mathcal{R}^{(A)}\) is a set composed of all achievable \((R_0, R_1, R_2, R_{e1}, R_{e2})\) quintuples. The inner and outer bounds on the capacity-equivocation region \(\mathcal{R}^{(A)}\) are provided from Theorem 1 to Theorem 4 and they are proved in Appendix A, Appendix B, Appendix C, and Appendix D, respectively.

Our first result establishes an outer-bound on the capacity-equivocation region of the model of Figure 1.

**Theorem 1: (Outer bound)** A single-letter characterization of the region \(\mathcal{R}^{(Ao)}\) \((\mathcal{R}^{(A)} \subseteq \mathcal{R}^{(Ao)})\) is as follows,
\[
\mathcal{R}^{(Ao)} = \{(R_0, R_1, R_2, R_{e1}, R_{e2}) : R_{e1} \leq R_1, R_{e2} \leq R_2, R_0 \leq \min\{I(U, U_1; Y), I(U; Y, Y_1|U_1)\}, R_0 \leq \min\{I(U, U_2; Z), I(U; Z, Y_1|U_2)\}, R_0 + R_1 \leq \min\{I(U, U_1, V_1; Y), I(U, V_1; Y, Y_1|U_1)\}, R_0 + R_2 \leq \min\{I(U, U_2, V_2; Z), I(U, V_2; Z, Y_1|U_2)\}, R_0 + R_1 + R_2 \leq I(U, U_2, V_1; Y, Y_1|U_1) + I(V_2; Z, Y_1|U, U_1, U_2, V_1), R_0 + R_1 + R_2 \leq I(U, U_1, V_2; Z, Y_1|U_2) + I(V_1; Y, Y_1|U, U_1, U_2, V_2), R_{e1} \leq \min\{I(V_1; Y|U, V_2) - I(V_1; Z|U, V_2), I(V_1; Y|U) - I(V_1; Z|U)\}, R_{e2} \leq \min\{I(V_2; Z|U, V_1) - I(V_2; Y|U, V_1), I(V_2; Z|U) - I(V_2; Y|U)\}\}
\]

where \(U \to (U_1, U_2, V_1, V_2) \to (X, X_1) \to (Y, Y_1, Z)\).

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

- The relay \(X_1\) is represented by auxiliary random variables \(U_1\) and \(U_2\). The common message \(W_0\) is represented by \(U\), and the confidential messages \(W_1, W_2\) are represented by \(V_1\) and \(V_2\), respectively.
- Removing the relay node from the model of Figure 1, the model of Figure 1 reduces to the broadcast channels with two confidential messages and one common message [23].

Letting \(U_1 = U_2 = Y_1 = \text{const}\), the region \(\mathcal{R}^{(Ao)}\) reduces to \(\mathcal{R}^{(Ao1)}\), and it is given by
\[
\mathcal{R}^{(Ao1)} = \{(R_0, R_1, R_2, R_{e1}, R_{e2}) : R_{e1} \leq R_1, R_{e2} \leq R_2, R_0 \leq I(U; Y), R_0 \leq I(U; Z), R_0 + R_1 \leq I(U, V_1; Y), R_0 + R_2 \leq I(U, V_2; Z), R_0 + R_1 + R_2 \leq I(U, V_1; Y) + I(V_2; Z|U, V_1), \}
\]
\[ R_0 + R_1 + R_2 \leq I(U, V_2; Z) + I(V_1; Y|U, V_2), \]
\[ R_{e1} \leq \min\{I(V_1; Y|U, V_2) - I(V_1; Z|U, V_2), I(V_1; Y|U) - I(V_1; Z|U)\}, \]
\[ R_{e2} \leq \min\{I(V_2; Z|U, V_1) - I(V_2; Y|U, V_1), I(V_2; Z|U) - I(V_2; Y|U)\}. \]

This region \( \mathcal{R}^{(Ao)} \) is exactly the same as the outer bound in [23]. Note that removing the secrecy constraint, the above region is the same as the outer bound for the general broadcast channel provided by Nair and Gamal [34].

- Removing the secrecy constraint, the model of Figure 1 reduces to the general relay broadcast channel. Then, the following region \( \mathcal{R}^{(Co)} \) can be served as a new outer bound for the general relay broadcast channel.

\[ \mathcal{R}^{(Co)} = \{(R_0, R_1, R_2): \]
\[ R_0 \leq \min\{I(U, U_1; Y), I(U; Y, Y_1|U_1)\}, \]
\[ R_0 \leq \min\{I(U, U_2; Z), I(U; Z, Y_1|U_2)\}, \]
\[ R_0 + R_1 \leq \min\{I(U, U_1, V_1; Y), I(U, V_1; Y, Y_1|U_1)\}, \]
\[ R_0 + R_2 \leq \min\{I(U, U_2, V_2; Z), I(U, V_2; Z, Y_1|U_2)\}, \]
\[ R_0 + R_1 + R_2 \leq I(U, U_2, V_1; Y, Y_1|U_1) + I(V_2; Z, Y_1|U, U_1, U_2, V_1), \]
\[ R_0 + R_1 + R_2 \leq I(U, U_1, V_1; Z, Y_1|U_2) + I(V_1; Y, Y_1|U, U_1, U_2, V_2), \]

where \( U \rightarrow (U_1, U_2, V_1, V_2) \rightarrow (X, X_1) \rightarrow (Y, Y_1, Z). \)

- The outer bound on the secrecy capacity region is denoted as \( \mathcal{C}^{Ao}_a \), which is the set of triples \((R_0, R_1, R_2)\) such that \((R_0, R_1, R_2, R_{e1} = R_1, R_{e2} = R_2) \in \mathcal{R}^{(Ao)}\).

**Corollary 1:**

\[ \mathcal{C}^{Ao}_a = \{(R_0, R_1, R_2): \]
\[ R_0 \leq \min\{I(U, U_1; Y), I(U; Y, Y_1|U_1)\}, \]
\[ R_0 \leq \min\{I(U, U_2; Z), I(U; Z, Y_1|U_2)\}, \]
\[ R_0 + R_1 \leq \min\{I(U, U_1, V_1; Y), I(U, V_1; Y, Y_1|U_1)\}, \]
\[ R_0 + R_2 \leq \min\{I(U, U_2, V_2; Z), I(U, V_2; Z, Y_1|U_2)\}, \]
\[ R_0 + R_1 + R_2 \leq I(U, U_2, V_1; Y, Y_1|U_1) + I(V_2; Z, Y_1|U, U_1, U_2, V_1), \]
\[ R_0 + R_1 + R_2 \leq I(U, U_1, V_1; Z, Y_1|U_2) + I(V_1; Y, Y_1|U, U_1, U_2, V_2), \]
\[ R_1 \leq \min\{I(V_1; Y|U, V_2) - I(V_1; Z|U, V_2), I(V_1; Y|U) - I(V_1; Z|U)\}, \]
\[ R_2 \leq \min\{I(V_2; Z|U, V_1) - I(V_2; Y|U, V_1), I(V_2; Z|U) - I(V_2; Y|U)\}. \]

**Proof:** Substituting \( R_{e1} = R_1 \) and \( R_{e2} = R_2 \) into the region \( \mathcal{R}^{(Ao)} \), Corollary 1 is easily to be checked. ■
We now turn our attention to constructing cooperation strategies for the model of Figure 1. Our first step is to characterize the inner bound on the capacity-equivocation region by using Cover-Gamal’s Decode and Forward (DF) Strategy [35]. In the DF Strategy, the relay node will first decode the common message, and then re-encode the common message to cooperate with the transmitter. Then, the superposition coding and random binning techniques used in [23] will be combined with the DF cooperation strategy to characterize the inner bound.

**Theorem 2:** (*Inner bound 1: DF strategy*) A single-letter characterization of the region $R^{(A1)} (R^{(A1)} \subseteq R^{(A)})$ is as follows,

$$R^{(A1)} = \{(R_0, R_1, R_2, R_{e1}, R_{e2}) : R_{e1} \leq R_1, R_{e2} \leq R_2, \quad R_0 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\},$$

$$R_0 + R_1 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\} + I(V_1; Y|U, X_1),$$

$$R_0 + R_2 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\} + I(V_2; Z|U, X_1),$$

$$R_0 + R_1 + R_2 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\} + I(V_1; Y|U, X_1) + I(V_2; Z|U, X_1) - I(V_1; V_2|U, X_1),$$

$$R_{e1} \leq I(V_1; Y|U, X_1) - I(V_1; V_2|U, X_1) - I(V_1; Z|U, X_1, V_2),$$

$$R_{e2} \leq I(V_2; Z|U, X_1) - I(V_1; V_2|U, X_1) - I(V_2; Y|U, X_1, V_1),$$

for some distribution

$$P_{Y,Z,Y_1,X_1,V_1,V_2,U}(y, z, y_1, x_1, v_1, v_2, u) = P_{Y,Z,Y_1,X_1}(y, z, y_1|x_1)P_{X,X_1|U,V_1,V_2}(x, x_1|u, v_1, v_2)P_{U,V_1,V_2}(u, v_1, v_2).$$

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

- The common message $W_0$ is represented by $U$, and the confidential messages $W_1$, $W_2$ are represented by $V_1$ and $V_2$, respectively.
- The inequality $R_0 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\}$ of Theorem 2 implies that the relay node decode-and-forward the common message $W_0$. Other inequalities in Theorem 2 follow the ideas of [23], [36], [37].
- The first inner bound on the secrecy capacity region of Figure 1 is denoted as $C_s^{A1}$, which is the set of triples $(R_0, R_1, R_2)$ such that $(R_0, R_1, R_2, R_{e1} = R_1, R_{e2} = R_2) \in R^{(A1)}$.

**Corollary 2:**

$$C_s^{A1} = \{(R_0, R_1, R_2) : \quad R_0 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\},$$

$$R_1 \leq I(V_1; Y|U, X_1) - I(V_1; V_2|U, X_1) - I(V_1; Z|U, X_1, V_2),$$

$$R_2 \leq I(V_2; Z|U, X_1) - I(V_1; V_2|U, X_1) - I(V_2; Y|U, X_1, V_1)\}.$$

**Proof:** Substituting $R_{e1} = R_1$ and $R_{e2} = R_2$ into the region $R^{(A1)}$, Corollary 2 is easily to be checked.
The second step is to characterize the inner bound on the capacity-equivocation region by using the generalized noise and forward (GNF) strategy. In the GNF Strategy, the relay node does not attempt to decode the messages but sends codewords that are independent of the transmitters messages, and these codewords aid in confusing the receivers. Specifically, if the channel from the relay to receiver 1 is less noisy than the channel from the relay to receiver 2, we allow receiver 1 to decode the relay codeword, and receiver 2 can not decode it. Therefore, in this case, the relay codeword can be viewed as a noise signal to confuse receiver 2. Analogously, if the channel from the relay to receiver 1 is more noisy than the channel from the relay to receiver 2, we allow receiver 2 to decode the relay codeword, and receiver 1 can not decode it. Thus, in this case, the relay codeword is a noise signal to confuse receiver 1.

**Theorem 3: (Inner bound 2: GNF strategy)** A single-letter characterization of the region $\mathcal{R}^{(A/2)} (\mathcal{R}^{(A/2)} \subseteq \mathcal{R}^{(A)})$ is as follows,

\[
\mathcal{R}^{(A/2)} = \mathcal{L}^1 \cup \mathcal{L}^2,
\]

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

\[
\mathcal{L}^1 = \bigcup_{P_{Y,Z,Y_1,X,X_1,V_1,V_2,U,Y,1} \mid I(X_1;V) \geq I(X_1;Y|U,V_1)} \left\{ \begin{array}{l}
(R_0, R_1, R_2, R_{e1}, R_{e2}) : R_{e1} \leq R_1, R_{e2} \leq R_2, \\
R_0 \leq \min\{I(U;Y|X_1), I(U;Z)\}, \\
R_0 + R_1 \leq \min\{I(U;Y|X_1), I(U;Z)\} + I(V_1;Y|U,X_1), \\
R_0 + R_2 \leq \min\{I(U;Y|X_1), I(U;Z)\} + I(V_2;Z|U), \\
R_0 + R_1 + R_2 \leq \min\{I(U;Y|X_1), I(U;Z)\} + I(V_1;Y|U,X_1) \\
+ I(V_1;V_2|U) - I(X_1,V_1,Z|U,V_2), \\
R_{e1} \leq \min\{I(X_1;Z|U,V_1,V_2), I(X_1;Y)\} + I(V_1;Y|U,X_1) \\
R_{e2} \leq I(V_2;Z|U) - I(V_1;V_2|U) - I(V_2;Y|U,X_1,V_1). \end{array} \right. \]

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

\[
\mathcal{L}^2 = \bigcup_{P_{Y,Z,Y_1,X,X_1,V_1,V_2,U,Y,1} \mid I(X_1;V) \geq I(X_1;Y|U,V_1)} \left\{ \begin{array}{l}
(R_0, R_1, R_2, R_{e1}, R_{e2}) : R_{e1} \leq R_1, R_{e2} \leq R_2, \\
R_0 \leq \min\{I(U;Z|X_1), I(U;Y)\}, \\
R_0 + R_1 \leq \min\{I(U;Z|X_1), I(U;Y)\} + I(V_1;Y|U), \\
R_0 + R_2 \leq \min\{I(U;Z|X_1), I(U;Y)\} + I(V_2;Z|U,X_1), \\
R_0 + R_1 + R_2 \leq \min\{I(U;Z|X_1), I(U;Y)\} + I(V_1;Y|U,X_1) \\
+ I(V_1;V_2|U) - I(V_1;V_2|U) - I(V_1;Z|U,V_2,X_1), \\
R_{e1} \leq I(V_1;Y|U) - I(V_1;V_2|U) - I(V_1;Z|U,V_2,X_1), \\
R_{e2} \leq \min\{I(X_1;Y|U,V_1,V_2), I(X_1;Z)\} + I(V_2;Z|U,X_1) \\
- I(V_1;V_2|U) - I(X_1,V_1,V_2|U,V_1). \end{array} \right. \]

and $P_{Y,Z,Y_1,X,X_1,V_1,V_2,U}(y, z, y_1, x, x_1, v_1, v_2, u)$ satisfies

\[
P_{Y,Z,Y_1,X,X_1,V_1,V_2,U}(y, z, y_1, x, x_1, v_1, v_2, u) = P_{Y,Z,Y_1,X,X_1}(y, z, y_1|x, x_1)P_{X|U,V_1,V_2}(x|u, v_1, v_2)P_{U,V_1,V_2}(u, v_1, v_2)P_{X_1}(x_1). \]
Remark 3: There are some notes on Theorem 3, see the following.

- The region $\mathcal{L}^1$ is characterized under the condition that the channel from the relay to receiver 1 is less noisy than the channel from the relay to receiver 2 ($I(X_1; Y) \geq I(X_1; Z|U, V_2)$ and $X_1$ is independent of $U, V_2$ imply that $I(X_1; Y) \geq I(X_1; Z)$). Then, in this case, receiver 1 is allowed to decode the relay codeword, and receiver 2 is not allowed to decode it. The rate of the relay is defined as $\min\{I(X_1; Z|U, V_1, V_2), I(X_1; Y)\}$, and the relay codeword is viewed as pure noise for receiver 2. Analogously, the region $\mathcal{L}^2$ is characterized under the condition that the channel from the relay to receiver 2 is less noisy than the channel from the relay to receiver 1. Then, in this case, receiver 2 is allowed to decode the relay codeword, and receiver 1 is not allowed to decode it.

- The second inner bound on the secrecy capacity region of Figure 1 is denoted as $\mathcal{C}_s^{\text{Ai2}}$, which is the set of triples $(R_0, R_1, R_2)$ such that $(R_0, R_1, R_2, R_{e_1} = R_1, R_{e_2} = R_2) \in \mathcal{R}^{(\text{Ai2})}$.

Corollary 3:

$$\mathcal{C}_s^{\text{Ai2}} = \mathcal{L}^a \cup \mathcal{L}^b,$$

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

$$\mathcal{L}^1 = \bigcup_{P_{Y,Z,Y_1,X_1,V_1,Y_2,U: I(X_1,Y) \geq I(X_1; Z|U, V_2)} \{ (R_0, R_1, R_2) : \\
R_0 \leq \min\{I(U; Y|X_1), I(U; Z)\}, \\
R_0 + R_1 \leq \min\{I(U; Y|X_1), I(U; Z)\} + I(V_1; Y|U, X_1), \\
R_1 \leq \min\{I(X_1; Z|U, V_1, V_2), I(X_1; Y)\} + I(V_1; Y|U, X_1) \\
- I(V_1; V_2|U) - I(X_1, V_1; Z|U, V_2), \\
R_2 \leq I(V_2; Z|U) - I(V_1; V_2|U) - I(V_2; Y|U, X_1, V_1). \} ,$$

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

$$\mathcal{L}^2 = \bigcup_{P_{Y,Z,Y_1,X_1,V_1,Y_2,U: I(X_1,Z) \geq I(X_1; Y|U, V_1)} \{ (R_0, R_1, R_2) : \\
R_0 \leq \min\{I(U; Z|X_1), I(U; Y)\}, \\
R_0 + R_2 \leq \min\{I(U; Z|X_1), I(U; Y)\} + I(V_2; Z|U, X_1), \\
R_1 \leq I(V_1; Y|U) - I(V_1; V_2|U) - I(V_1; Z|U, V_2, X_1), \\
R_2 \leq \min\{I(X_1; Y|U, V_1, V_2), I(X_1; Z)\} + I(V_2; Z|U, X_1) \\
- I(V_1; V_2|U) - I(X_1, V_2; Y|U, V_1). \} .$$

Proof: Substituting $R_{e_1} = R_1$ and $R_{e_2} = R_2$ into the region $\mathcal{R}^{(\text{Ai2})}$, Corollary 3 is easily to be checked.

The third step is to characterize the inner bound on the capacity-equivocation region by using a combination of Cover- Gamal’s compress and forward (CF) strategy and the GNF strategy, i.e., in addition to the independent codewords, the relay also sends a quantized version of its noisy observations to the receivers. This noisy version of the relay’s observations helps the receivers in decoding the transmitter’s messages, while the independent codewords help in confusing the receivers. Similar to Theorem 3, if the channel from the relay to receiver 1 is less noisy than...
the channel from the relay to receiver 2, we allow receiver 1 to decode the relay codeword, and receiver 2 can not decode it. Analogously, if the channel from the relay to receiver 1 is more noisy than the channel from the relay to receiver 2, we allow receiver 2 to decode the relay codeword, and receiver 1 can not decode it.

**Theorem 4:** (Inner bound 3: CF strategy) A single-letter characterization of the region $\mathcal{R}^{(Av3)} (\mathcal{R}^{(Av3)} \subseteq \mathcal{R}^{(A)})$ is as follows,

$$\mathcal{R}^{(Av3)} = \mathcal{L}^3 \bigcup \mathcal{L}^4,$$

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

$$\mathcal{L}^3 = \bigcup_{P_{Y,Z,Y_1,Y_2,X,V_1,V_2,U} : I(X_1; Y) \geq I(X_1; Z(U, V_2))} \{ (R_0, R_1, R_2, R_{e1}, R_{e2}) : R_{e1} \leq R_1, R_{e2} \leq R_2, \}
\begin{align*}
R_0 &\leq \min\{I(U; Y, \hat{Y}_1|X_1), I(U; Z)\}, \\
R_0 + R_1 &\leq \min\{I(U; Y, \hat{Y}_1|X_1), I(U; Z)\} + I(V_1; Y|U, X_1), \\
R_0 + R_2 &\leq \min\{I(U; Y, \hat{Y}_1|X_1), I(U; Z)\} + I(V_2; Z|U), \\
R_0 + R_1 + R_2 &\leq \min\{I(U; Y, \hat{Y}_1|X_1), I(U; Z)\} + I(V_1; V_2|U), \\
R_{e1} &\leq R^* + I(V_1; Y, \hat{Y}_1|U, X_1) - I(V_1; V_2|U), \\
R_{e2} &\leq I(V_2; Z|U) - I(V_1; V_2|U) - I(V_2; Y|U, X_1, V_1). \\
\end{align*}$$

$$R_{r1}^* = \min\{I(X_1; Z(U, V_1, V_2), I(X_1; Y))\},$$

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

$$\mathcal{L}^4 = \bigcup_{P_{Y,Z,Y_1,Y_2,X,V_1,V_2,U} : I(X_1; Z) \geq I(X_1; Y(U, V_1))} \{ (R_0, R_1, R_2, R_{e1}, R_{e2}) : R_{e1} \leq R_1, R_{e2} \leq R_2, \}
\begin{align*}
R_0 &\leq \min\{I(U; Z, \hat{Y}_1|X_1), I(U; Y)\}, \\
R_0 + R_1 &\leq \min\{I(U; Z, \hat{Y}_1|X_1), I(U; Y)\} + I(V_1; Y|U), \\
R_0 + R_2 &\leq \min\{I(U; Z, \hat{Y}_1|X_1), I(U; Y)\} + I(V_2; Z|U, X_1), \\
R_0 + R_1 + R_2 &\leq \min\{I(U; Z, \hat{Y}_1|X_1), I(U; Y)\} + I(V_1; V_2|U), \\
R_{e1} &\leq I(V_1; Y|U) - I(V_1; V_2|U) - I(V_1; Z(U, V_2, X_1), \\
R_{e2} &\leq R^* + I(V_2; Z, \hat{Y}_1|U, X_1) - I(V_1; V_2|U) \\
R_{r2}^* &\leq \min\{I(X_1; Y(U, V_1, V_2), I(X_1; Z))\}. \\
\end{align*}$$

The joint probability $P_{Y,Z,Y_1,Y_2,X,V_1,V_2,U}(y, z, y_1, \hat{y}_1, x, x_1, v_1, v_2, u)$ satisfies

$$P_{Y,Z,Y_1,X,V_1,V_2,U}(y, z, y_1, \hat{y}_1, x, x_1, v_1, v_2, u) = P_{Y,Z,Y_1,X}(y, z, y_1|x_1)P_{X|U,V_1,V_2}(x|u, v_1, v_2)P_{U,V_1,V_2}(u, v_1, v_2)P_{Y_1|Y_1,X_1}(\hat{y}_1|y_1, x_1)P_{X_1}(x_1).$$

**Remark 4:** There are some notes on Theorem 4, see the following.
In Theorem 4, \( R^* \) is the rate of pure noise generated by the relay to confuse the receivers, while \( R^*_{r1} - R^*_{r2} \) \( (R^*_{r2} - R^*) \) is the part of the rate allocated to send the compressed signal \( \hat{Y}_1 \) to help the receivers. If \( R^* = R^*_{r1} \) \( (R^* = R^*_{r2}) \), this scheme is exactly the same as the GNF scheme used in Theorem 5.

The third inner bound on the secrecy capacity region of Figure 1 is denoted as \( C_{s}^{Ai3} \), which is the set of triples \( (R_0, R_1, R_2) \) such that \( (R_0, R_1, R_2, R_{e1} = R_1, R_{e2} = R_2) \in \mathcal{R}^{(Ai3)} \).

**Corollary 4:**

\[
C_{s}^{Ai3} = \mathcal{L}^e \cup \mathcal{L}^d,
\]

where \( \mathcal{L}^e \) is given by

\[
\mathcal{L}^e = \bigcup_{P_{Y,Z,V_1,V_2,U} \mid I(X_1; Y) \geq I(X_1; Z|U,V_2)} \{ (R_0, R_1, R_2) : 
\begin{align*}
R_0 &\leq \min\{I(U; Y, \hat{Y}_1|X_1), I(U; Z)\}, \\
R_0 + R_1 &\leq \min\{I(U; Y, \hat{Y}_1|X_1), I(U; Z)\} \\
&\quad + I(V_1; Y, \hat{Y}_1|U, X_1), \\
R_1 \leq R^* + I(V_1; Y, \hat{Y}_1|U, X_1) - I(V_1; V_2|U) \\
&\quad - I(X_1, V_1; Z|U, V_2), \\
R_2 \leq I(V_2; Z|U) - I(V_1; V_2|U) - I(V_2; Y|U, X_1, V_1).
\end{align*}
\}
\]

\( R^*_{r1} = \min\{I(X_1; Z|U, V_1, V_2), I(X_1; Y)\} \), and \( \mathcal{L}^d \) is given by

\[
\mathcal{L}^d = \bigcup_{P_{Y,Z,V_1,V_2,U} \mid I(X_1; Z) \geq I(X_1; Y|U,V_1)} \{ (R_0, R_1, R_2) : 
\begin{align*}
R_0 &\leq \min\{I(U; Z, \hat{Y}_1|X_1), I(U; Y)\}, \\
R_0 + R_2 &\leq \min\{I(U; Z, \hat{Y}_1|X_1), I(U; Y)\} \\
&\quad + I(V_2; Z, \hat{Y}_1|U, X_1), \\
R_1 \leq I(V_1; Y|U) - I(V_1; V_2|U) - I(V_1; Z|U, V_2, X_1), \\
R_2 \leq R^* + I(V_2; Z, \hat{Y}_1|U, X_1) - I(V_1; V_2|U) \\
&\quad - I(X_1, V_2; Y|U, V_1).
\end{align*}
\}
\]

\( R^*_{r2} = \min\{I(X_1; Y|U, V_1, V_2), I(X_1; Z)\} \).

**Proof:** Substituting \( R_{e1} = R_1 \) and \( R_{e2} = R_2 \) into the region \( \mathcal{R}^{(Ai3)} \), Corollary 4 is easily to be checked.

### III. Relay Broadcast Channels with Two Confidential Messages

In this section, the main results on the model of Figure 2 are provided in Subsection III-A and the results are further explained via a Gaussian example, see Subsection III-B.

#### A. Problem formulation and the main results

The model of Figure 2 is similar to the model of Figure 1 except that there is no common message \( W_0 \). The channel encoder is a stochastic encoder that maps the messages \( W_1 \) and \( W_2 \) into a codeword \( x^N \in \mathcal{X}^N \).
The decoder for receiver 1 is a mapping $f_{D1} : \mathcal{Y}^N \rightarrow \mathcal{W}_1$, with input $Y^N$ and output $\hat{W}_1$. Let $P_{e1}$ be the error probability of receiver 1, and it is defined as $Pr\{\hat{W}_1 \neq W_1\}$.

Analogously, the decoder for receiver 2 is a mapping $f_{D2} : \mathcal{Z}^N \rightarrow \mathcal{W}_2$, with input $Z^N$ and output $\hat{W}_2$. Let $P_{e2}$ be the error probability of receiver 2, and it is defined as $Pr\{\hat{W}_2 \neq W_2\}$.

A rate quadruple $(R_1, R_2, R_{e1}, R_{e2})$ (where $R_1, R_2, R_{e1}, R_{e2} > 0$) is called achievable if, for any $\epsilon > 0$ (where $\epsilon$ is an arbitrary small positive real number and $\epsilon \rightarrow 0$), there exists a channel encoder-decoder $(N, \Delta_1, \Delta_2, P_{e1}, P_{e2})$ such that

$$\lim_{N \rightarrow \infty} \frac{\log \|W_1\|}{N} = R_1, \quad \lim_{N \rightarrow \infty} \frac{\log \|W_2\|}{N} = R_2,$$

$$\lim_{N \rightarrow \infty} \Delta_1 \geq R_{e1}, \quad \lim_{N \rightarrow \infty} \Delta_2 \geq R_{e2}, \quad P_{e1} \leq \epsilon, \quad P_{e2} \leq \epsilon.$$  

(3.4)

The capacity-equivocation region $\mathcal{R}^{(B)}$ is a set composed of all achievable $(R_1, R_2, R_{e1}, R_{e2})$ quadruples. The inner and outer bounds on the capacity-equivocation region $\mathcal{R}^{(B)}$ are provided from Theorem 5 to Theorem 8, see the remaining of this subsection.

The first result is an outer-bound on the capacity-equivocation region of the model of Figure 2.

**Theorem 5: (Outer bound)** A single-letter characterization of the region $\mathcal{R}^{(Bo)}$ ($\mathcal{R}^{(B)} \subseteq \mathcal{R}^{(Bo)}$) is as follows,

$$\mathcal{R}^{(Bo)} = \{(R_1, R_2, R_{e1}, R_{e2}) : R_{e1} \leq R_1, \quad R_{e2} \leq R_2, \quad R_1 \leq \min\{I(U_1, V_1; Y), I(V_1; Y|U_1)\}, \quad R_2 \leq \min\{I(U_2, V_2; Z), I(V_2; Z|U_2)\}, \quad R_1 + R_2 \leq I(U_2, V_1; Y, Y_1|U_1) + I(V_2; Z, Y_1|U_1, U_2, Y_1), \quad R_1 + R_2 \leq I(U_1, V_2; Z, Y_1|U_2) + I(V_1; Y, Y_1|U_1, U_2, V_2), \quad R_{e1} \leq \min\{I(V_1; Y|V_2) - I(V_1; Z|V_2), I(V_1; Y|U) - I(V_1; Z|U)\}, \quad R_{e2} \leq \min\{I(V_2; Z|V_1) - I(V_2; Y|V_1), I(V_2; Z|U) - I(V_2; Y|U)\}, \quad$$

where $U \rightarrow (U_1, U_2, V_1, V_2) \rightarrow (X, X_1) \rightarrow (Y, Y_1, Z)$.

**Remark 5:** There are some notes on Theorem 5, see the following.

- **Theorem 5** is directly obtained from Theorem 1 by letting $R_0 = 0$, and therefore, we omit the proof here.
- Removing the relay node from the model of Figure 1 the model reduces to the broadcast channels with two confidential messages [22]. Letting $U_1 = U_2 = Y_1 = const$, the region $\mathcal{R}^{(Bo)}$ is exactly the same as the outer bound in [22].
- The outer bound on the secrecy capacity region of Figure 2 is denoted as $\mathcal{C}_s^{Bo}$, which is the set of pairs $(R_1, R_2)$ such that $(R_1, R_2, R_{e1} = R_1, R_{e2} = R_2) \in \mathcal{R}^{(Bo)}$. 
Superposition coding and random binning techniques used in [22] are combined with the DF cooperation strategy. Theorem 6, Theorem 7 and Theorem 8 are omitted here.

Remark 6: We now turn our attention to constructing the achievable rate-equivocation regions of the model of Figure 2. We first decode the messages of Figure 2. Then, replacing the common messages (intended to be decoded by both receivers, i.e., $W_0$ into $W_{10}$ and $W_{11}$, and $W_2$ into $W_{20}$ and $W_{22}$). The messages $W_{10}$ and $W_{20}$ are intended to be decoded by both receivers, i.e., $W_{10}$ and $W_{20}$ can be viewed as the common messages for the model of Figure 2. Then, replacing the common messages $(W_0, W_{10}, W_{20})$ of the model of Figure 2 by $(W_{10}, W_{20})$, the achievable regions of the model of Figure 2 are along the lines of those in Figure 1 and therefore, the proofs of Theorem 6, Theorem 7 and Theorem 8 are omitted here.

We now turn our attention to constructing the achievable rate-equivocation regions of the model of Figure 2. We split the confidential message $W_1$ into $W_{10}$ and $W_{11}$, and $W_2$ into $W_{20}$ and $W_{22}$. The messages $W_{10}$ and $W_{20}$ are intended to be decoded by both receivers, i.e., $W_{10}$ and $W_{20}$ can be viewed as the common messages for the model of Figure 2. Then, replacing the common messages $(W_0, W_{10}, W_{20})$ of the model of Figure 2 by $(W_{10}, W_{20})$, the achievable regions of the model of Figure 2 are along the lines of those in Figure 1 and therefore, the proofs of Theorem 6, Theorem 7 and Theorem 8 are omitted here.

The first inner bound on $\mathcal{R}^{(B)}$ is characterized by using DF Strategy. In this DF Strategy, the relay node will first decode the messages $W_{10}$ and $W_{20}$, and then re-encode these messages to cooperate with the transmitter. The superposition coding and random binning techniques used in [22] are combined with the DF cooperation strategy to characterize the inner bound.

**Theorem 6:** (Inner bound 1: DF strategy) A single-letter characterization of the region $\mathcal{R}^{(B_1)}$ ($\mathcal{R}^{(B_1)} \subseteq \mathcal{R}^{(B)}$) is as follows,

$$\mathcal{R}^{(A_1)} = \{(R_1, R_2, R_{e1}, R_{e2}) : R_{e1} \leq R_1, R_{e2} \leq R_2, R_1 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\} + I(V_1; Y|U, X_1), R_2 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\} + I(V_2; Z|U, X_1), R_1 + R_2 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\} + I(V_1; Y|U, X_1) + I(V_2; Z|U, X_1) - I(V_1; V_2|U, X_1), R_{e1} \leq I(V_1; Y|U, X_1) - I(V_1; V_2|U, X_1) - I(V_1; Z|U, X_1), R_{e2} \leq I(V_2; Z|U, X_1) - I(V_1; V_2|U, X_1) - I(V_2; Y|U, X_1, V_1)\},$$

for some distribution

$$P_{Y,Z,Y_1,X,X_1,V_1,V_2,U}(y, z, y_1, x, x_1, v_1, v_2, u) = P_{Y,Z,Y_1,X,X_1}(y, z, y_1|x, x_1)P_{X,X_1|U,V_1,V_2}(x, x_1|u, v_1, v_2)P_{U,V_1,V_2}(u, v_1, v_2).$$

**Remark 6:** There are some notes on Theorem 6 see the following.
• Theorem 6 is directly obtained from Theorem 2 by letting $R_0 = 0$.

• The first inner bound on the secrecy capacity region of Figure 2 is denoted as $\mathcal{C}^{B1}_{s}$, which is the set of pairs $(R_1, R_2)$ such that $(R_1, R_2, R_{e1} = R_1, R_{e2} = R_2) \in \mathcal{R}^{(B1)}$.

Corollary 6:

$$\mathcal{C}^{B1}_{s} = \{(R_1, R_2) : R_1 \leq I(V_1; Y|U, X_1) - I(V_1; V_2|U, X_1) - I(V_1; Z|U, X_1, V_2),$$

$$R_2 \leq I(V_2; Z|U, X_1) - I(V_1; V_2|U, X_1) - I(V_2; Y|U, X_1, V_1)\}.$$  

Proof: Substituting $R_{e1} = R_1$ and $R_{e2} = R_2$ into the region $\mathcal{R}^{(B1)}$, Corollary 6 is easily to be checked.

The second inner bound on $\mathcal{R}^{(B)}$ is characterized by using the noise and forward (NF) strategy. In this NF Strategy, the relay node sends codewords that are independent of the transmitters messages, and these codewords aid in confusing the receivers.

Theorem 7: (Inner bound 2: NF strategy) A single-letter characterization of the region $\mathcal{R}^{(B2)}$ ($\mathcal{R}^{(B2)} \subseteq \mathcal{R}^{(B)}$) is as follows,

$$\mathcal{R}^{(B2)} = \mathcal{L}^5 \cup \mathcal{L}^6,$$

where $\mathcal{L}^5$ is given by

$$\mathcal{L}^5 = \bigcup_{P_{Y, Z, Y_1, X_1, V_1, V_2, U} : I(X_1, Y) \geq I(X_1, Z|U, V_2)}
\begin{cases}
(R_1, R_2, R_{e1}, R_{e2}) : R_{e1} \leq R_1, R_{e2} \leq R_2, \\
R_1 \leq \min\{I(U; Y|X_1), I(U; Z)\} + I(V_1; Y|U, X_1), \\
R_2 \leq \min\{I(U; Y|X_1), I(U; Z)\} + I(V_2; Z|U), \\
R_1 + R_2 \leq \min\{I(U; Y|X_1), I(U; Z)\} + I(V_1; Y|U, X_1) + I(V_2; Z|U, V_2), \\
+ I(V_1; Y|U, X_1) + I(V_2; Z|U) - I(V_1; V_2|U), \\
R_{e1} \leq \min\{I(X_1; Z|U, V_1, V_2), I(X_1; Y)\} + I(V_1; Y|U, X_1) \\
- I(V_1; V_2|U) - I(X_1, V_1; Z|U, V_2), \\
R_{e2} \leq I(V_2; Z|U) - I(V_1; V_2|U) - I(V_2; Y|U, X_1, V_1). \\
\end{cases}$$

$\mathcal{L}^6$ is given by

$$\mathcal{L}^6 = \bigcup_{P_{Y, Z, Y_1, X_1, V_1, V_2, U} : I(X_1, Z) \geq I(X_1, Y|U, V_2)}
\begin{cases}
(R_1, R_2, R_{e1}, R_{e2}) : R_{e1} \leq R_1, R_{e2} \leq R_2, \\
R_1 \leq \min\{I(U; Z|X_1), I(U; Y)\} + I(V_1; Y|U), \\
R_2 \leq \min\{I(U; Z|X_1), I(U; Y)\} + I(V_2; Z|U, X_1), \\
R_1 + R_2 \leq \min\{I(U; Z|X_1), I(U; Y)\} + I(V_1; Y|U) + I(V_2; Z|U, X_1) - I(V_1; V_2|U), \\
R_{e1} \leq I(V_1; Y|U) - I(V_1; V_2|U) - I(V_1; Z|U, V_2, X_1), \\
R_{e2} \leq \min\{I(X_1; Y|U, V_1, V_2), I(X_1; Z)\} + I(V_2; Z|U, X_1) + I(V_1; Y|U, X_1) \\
- I(V_1; V_2|U) - I(X_1, V_2; Y|U, V_1). \\
\end{cases}$$
and $P_{Y,Z,Y_1,X_1,V_1,V_2,U}(y, z, y_1, x, x_1, v_1, v_2, u)$ satisfies

$$P_{Y,Z,Y_1,X_1,V_1,V_2,U}(y, z, y_1, x, x_1, v_1, v_2, u) = P_{Y,Z,Y_1,X_1}(y, z, y_1 | x, x_1) P_{X|U,V_1,V_2}(x | u, v_1, v_2) P_{U,V_1,V_2}(u, v_1, v_2) P_{X_1}(x_1).$$

**Remark 7:** There are some notes on Theorem 7, see the following.

- Theorem 7 is directly obtained from Theorem 3 by letting $R_0 = 0$.
- The second inner bound on the secrecy capacity region of Figure 2 is denoted as $\mathcal{C}_s^{Bi2}$, which is the set of pairs $(R_1, R_2)$ such that $(R_1, R_2, R_{e1} = R_1, R_{e2} = R_2) \in \mathcal{R}^{(Bi2)}$.

Corollary 7:

$$\mathcal{C}_s^{Bi2} = \mathcal{L}^e \bigcup \mathcal{L}^f,$$

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

$$\mathcal{L}^e = \bigcup_{P_{Y,Z,Y_1,X_1,V_1,V_2,U}: I(X_1; Y) \geq I(X_1; Z|U, V_2)} \{ (R_0, R_1, R_2) : \begin{align*}
R_1 &\leq \min\{I(U; Y|X_1), I(U; Z)\} + I(V_1; Y|U, X_1), \\
R_1 &\leq \min\{I(X_1; Z|U, V_2), I(X_1; Y)\} + I(V_1; Y|U, X_1) \\
&\quad - I(V_1; V_2|U) - I(X_1, V_1; Z|U, V_2), \\
R_2 &\leq I(V_2; Z|U) - I(V_1; V_2|U) - I(V_2; Y|U, X_1, V_1). 
\end{align*} \}.$$

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

$$\mathcal{L}^f = \bigcup_{P_{Y,Z,Y_1,X_1,V_1,V_2,U}: I(X_1; Z) \geq I(X_1; Y|U, V_2)} \{ (R_1, R_2) : \begin{align*}
R_2 &\leq \min\{I(U; Z|X_1), I(U; Y)\} + I(V_2; Z|U, X_1), \\
R_1 &\leq I(V_1; Y|U) - I(V_1; V_2|U) - I(V_1; Z|U, V_2, X_1), \\
R_2 &\leq \min\{I(X_1; Y|U, V_1, V_2), I(X_1; Z)\} + I(V_2; Z|U, X_1) \\
&\quad - I(V_1; V_2|U) - I(X_1, V_2; Y|U, V_1). 
\end{align*} \}.$$

**Proof:** Substituting $R_{e1} = R_1$ and $R_{e2} = R_2$ into the region $\mathcal{R}^{(Bi2)}$, Corollary 7 is easily to be checked.

The third inner bound on $\mathcal{R}^{(B)}$ is characterized by using a combination of compress and forward (CF) strategy and the GNF strategy, and this inner bound is similar to Theorem 4.

**Theorem 8:** (Inner bound 3: CF strategy) A single-letter characterization of the region $\mathcal{R}^{(Bi3)}$ ($\mathcal{R}^{(Bi3)} \subseteq \mathcal{R}^{(B)}$) is as follows,

$$\mathcal{R}^{(Bi3)} = \mathcal{L}^7 \bigcup \mathcal{L}^8,$$
where $\mathbb{L}^7$ is given by

$$
\mathbb{L}^7 = \bigcup_{P_{Y,Z,Y_1,X,X_1,V_1,V_2,U} : I(X_1; Y) \geq I(X_1; Z | U, V_2), R^*_{r_2} - R^* \geq I(V_1; Y_1 | X_1)} \{(R_1, R_2, R_{e_1}, R_{e_2}) : R_{e_1} \leq R_1, R_{e_2} \leq R_2, R_1 \leq \min\{I(U; Y, 1 X_1), I(U; Z)\} + I(V_1; Y_1 | U, X_1), R_2 \leq \min\{I(U; Y, 1 X_1), I(U; Z)\} + I(V_2; Z | U), R_1 + R_2 \leq \min\{I(U; Y, 1 X_1), I(U; Z)\} + I(V_1; V_2 | U), R_{e_1} \leq R^* + I(V_1; Y, 1 X_1) - I(V_1; V_2 | U) - I(X_1, V_1; Z | U, V_2), R_{e_2} \leq I(V_2; Z | U) - I(V_1; V_2 | U) - I(V_2; Y | U, X_1, V_1).\}
$$

$R^*_{r_1} = \min\{I(X_1; Z | U, V_1, V_2), I(X_1; Y)\}$, and $\mathbb{L}^8$ is given by

$$
\mathbb{L}^8 = \bigcup_{P_{Y,Z,Y_1,X,X_1,V_1,V_2,U} : I(X_1; Z | U, V_2), R^*_{r_2} - R^* \geq I(V_1; Y_1 | X_1)} \{(R_1, R_2, R_{e_1}, R_{e_2}) : R_{e_1} \leq R_1, R_{e_2} \leq R_2, R_1 \leq \min\{I(U; Z, 1 X_1), I(U; Y)\} + I(V_1; Y | U), R_2 \leq \min\{I(U; Z, 1 X_1), I(U; Y)\} + I(V_2; Z, Y_1 | U, X_1) - I(V_1; V_2 | U), R_1 + R_2 \leq \min\{I(U; Z, 1 X_1), I(U; Y)\} + I(V_1; Y | U) + I(V_2; Z, Y_1 | U, X_1) - I(V_1; V_2 | U), R_{e_1} \leq I(V_1; Y | U) - I(V_1; V_2 | U) - I(V_1; Z | U, V_2, X_1), R_{e_2} \leq R^* + I(V_2; Z, Y_1 | U, X_1) - I(V_1; V_2 | U) - I(X_1, V_1; Y | U, V_1).\}
$$

$R^*_{r_2} = \min\{I(X_1; Y | U, V_1, V_2), I(X_1; Z)\}$.

The joint probability $P_{Y,Z,Y_1,X,X_1,V_1,V_2,U}(y, z, y_1, \tilde{y}_1, x, x_1, v_1, v_2, u)$ satisfies

$$
P_{Y,Z,Y_1,X,X_1,V_1,V_2,U}(y, z, y_1, \tilde{y}_1, x, x_1, v_1, v_2, u) = P_{Y,Z,Y_1,X,X_1}(y, z, y_1 | x, x_1) P_{X|U,V_1,V_2}(x | v_1, v_2) P_{U,V_1,V_2}(u, v_1, v_2) P_{Y_1,Y_1}(y_1 | y_1, x_1) P_{X_1}(x_1).
$$

Remark 8: There are some notes on Theorem 8, see the following.

- Theorem 8 is directly obtained from Theorem 4 by letting $R_0 = 0$.
- The third inner bound on the secrecy capacity region of Figure 2 is denoted as $\mathcal{C}_s^{B_3}$, which is the set of pairs $(R_1, R_2)$ such that $(R_1, R_2, R_{e_1} = R_1, R_{e_2} = R_2) \in \mathcal{R}^{(B_3)}$.

Corollary 8:

$$
\mathcal{C}_s^{B_3} = \mathcal{L}^8 \bigcup \mathcal{L}^h,
$$

B. Gaussian relay broadcast channels with two confidential messages

In this subsection, we investigate the Gaussian case of the model of Figure 2. The signal received at each node is given by

\[ Y_1 = X + Z_r, \]
\[ Y = X + X_1 + Z_1, \]
\[ Z = X + X_1 + Z_2, \]  \hspace{1cm} (3.5)\]

where \( Z_r \sim \mathcal{N}(0, N_r) \), \( Z_1 \sim \mathcal{N}(0, N_1) \), \( Z_2 \sim \mathcal{N}(0, N_2) \), and they are independent, \( E[X^2] \leq P_1 \), \( E[X_1^2] \leq P_2 \). In this subsection, we assume that \( N_1 + P_1 \leq N_2 \), which implies that the channel for receiver 1 is less noisy than the channel for receiver 2.

The inner bound on the secrecy capacity region of Figure 2 by using the DF strategy is given by

\[
C_s^{Bi1} = \bigcup_{0 \leq \alpha \leq 1, 0 \leq \beta \leq 1} \left\{ \begin{array}{c}
(R_1, R_2) : \\
R_1 \leq \frac{1}{2} \log \frac{(1-\beta)P_1+N_1}{(1-\beta)(1-\alpha)P_1+N_1} - \frac{1}{2} \log \frac{(1-\beta)P_1+N_2}{N_2}, \\
R_2 \leq \frac{1}{2} \log \frac{(1-\beta)P_1+N_2}{(1-\beta)(1-\alpha)P_1+N_1} - \frac{1}{2} \log \frac{(1-\beta)P_1+N_2}{N_1}.
\end{array} \right\}
\]  \hspace{1cm} (3.6)\]

Here \( C_s^{Bi1} \) is obtained by letting \( X = U + V_1 + V_2 \) and \( U = c_1 X_1 + X_{10} \), where \( U \sim \mathcal{N}(0, \beta P_1) \), \( V_1 \sim \mathcal{N}(0, (1-\beta)P_1(1-\alpha)) \), \( V_2 \sim \mathcal{N}(0, (1-\beta)P_1(1-\alpha)) \), \( X_{10} \sim \mathcal{N}(0, \beta \gamma P_1) \) (0 \( \leq \gamma \leq 1 \)), and \( c_1 = \sqrt{\frac{P_1(1-\gamma)}{P_2}} \). \( X_{10}, X_1, V_1, \) and \( V_2 \) are independent random variables.
Then, the inner bound on the secrecy capacity region by using the NF strategy is given by
\[
C_{s}^{Bi2} = \bigcup_{0 \leq 0 < 1 \leq 1}
\begin{cases}
(R_1, R_2) : \\
R_1 \leq \min \left\{ \frac{1}{2} \log \frac{P_1 + N_1}{(1 - \beta)P_1 + N_1}, \frac{1}{2} \log \frac{P_1 + P_2 + N_2}{(1 - \beta)P_1 + P_2 + N_2} \right\} + \frac{1}{2} \log \frac{(1 - \beta)P_1 + N_1}{(1 - \beta)P_1(1 - \alpha) + N_1}, \\
R_1 \leq \min \left\{ \frac{1}{2} \log \frac{P_1 + N_1}{P_1 + N_1}, \frac{1}{2} \log \frac{P_1 + P_2 + N_2}{P_1 + N_1} \right\} + \frac{1}{2} \log \frac{(1 - \beta)P_1 + P_2 + N_2}{P_1 + N_1} - \frac{1}{2} \log \frac{(1 - \alpha)(1 - \beta)P_1 + N_1}{N_1}, \end{cases}
\]
(3.7)

Here note that if \( N_1 + P_1 \leq N_2 \) implies that \( I(X_1; Y) \geq I(X_1; Z|U, V_2) \), and \( C_{s}^{Bi2} \) is obtained by letting \( X = U + V_1 + V_2 \), where \( V_1 \sim \mathcal{N}(0, (1 - \beta)P_1 \alpha), V_2 \sim \mathcal{N}(0, (1 - \beta)P_1 (1 - \alpha)) \), \( U \sim \mathcal{N}(0, \beta P_1) \). \( X_1, U, V_1 \) and \( V_2 \) are independent random variables.

Next, the inner bound on the secrecy capacity region by using the CF strategy is given by
\[
C_{s}^{Bi3} = \bigcup_{0 \leq 0 \leq 1 \leq 1}
\begin{cases}
(R_1, R_2) : \\
R_1 \leq \min \left\{ \frac{1}{2} \log \frac{P_1(N_1 + P_2 + N_1 + N_1 + Q)}{(1 - \beta)P_1(N_1 + P_2 + N_1 + N_1 + Q)}, \frac{1}{2} \log \frac{P_1 + P_2 + N_2}{P_1 + P_2 + N_2} \right\} + \frac{1}{2} \log \frac{(1 - \beta)P_1(N_1 + P_2 + N_1 + N_1 + Q)}{(1 - \beta)P_1(1 - \alpha)(N_1 + P_2 + N_1 + N_1 + Q)}, \\
R_1 \leq R^* + \frac{1}{2} \log \frac{(1 - \beta)P_1(N_1 + P_2 + N_1 + N_1 + Q)}{(1 - \beta)P_1(1 - \alpha)(N_1 + P_2 + N_1 + N_1 + Q)} - \frac{1}{2} \log \frac{(1 - \beta)P_2 + N_2}{P_1 + N_1}, \\
R_2 \leq \frac{1}{2} \log \frac{(1 - \beta)P_2 + P_2 + N_2}{(1 - \beta)P_1 + P_2 + N_2} - \frac{1}{2} \log \frac{(1 - \alpha)(1 - \beta)P_2 + N_1}{N_1}.
\end{cases}
\]
(3.8)

subject to
\[
0 \leq R^* \leq \min \left\{ \frac{1}{2} \log \frac{P_2 + N_2}{N_2}, \frac{1}{2} \log \frac{P_1 + P_2 + N_1}{P_1 + N_1} \right\} - \frac{1}{2} \log \frac{P_1 + Q + N_r}{Q}.
\]
(3.9)

Here note that if \( N_1 + P_1 \leq N_2 \) implies that \( I(X_1; Y) \geq I(X_1; Z|U, V_2) \), and \( C_{s}^{Bi3} \) is obtained by letting \( X = U + V_1 + V_2, \hat{Y}_1 = Y_1 + ZQ \), where \( ZQ \sim \mathcal{N}(0, Q), V_1 \sim \mathcal{N}(0, (1 - \beta)P_1 \alpha), V_2 \sim \mathcal{N}(0, (1 - \beta)P_1 (1 - \alpha)) \), \( U \sim \mathcal{N}(0, \beta P_1) \). \( X_1, U, V_1 \) and \( V_2 \) are independent random variables.

Finally, remember that [22] provides an inner bound on the secrecy capacity region of the broadcast channels with two confidential messages, and it is given by
\[
C_{s}^{(Bi)} = \{(R_1, R_2) : \\
R_1 \leq I(V_1; Y|U) - I(V_1; V_2|U) - I(V_1; Z|V_2, U), \\
R_2 \leq I(V_2; Z|U) - I(V_1; V_2|U) - I(V_2; Y|V_1, U)\}
\]

Letting \( X = U + V_1 + V_2, V_1 \sim \mathcal{N}(0, (1 - \beta)P_1 \alpha), V_2 \sim \mathcal{N}(0, (1 - \beta)P_1 (1 - \alpha)) \), \( U \sim \mathcal{N}(0, \beta P_1) \), \( Y = X + Z_1, Z = X + Z_2, Z_1 \sim \mathcal{N}(0, N_1), Z_2 \sim \mathcal{N}(0, N_2) \), and \( E[X^2] \leq P_1 \), we find that the secrecy rate region of the Gaussian case of [22] is exactly the same as (3.6), i.e., the DF strategy can not enhance the secrecy rate region of the broadcast channels with two confidential messages [22].

Note that if \( N_1 + P_1 \leq N_2 \) implies that \( N_1 \leq N_2, C_{s}^{Bi1}, C_{s}^{Bi2}, C_{s}^{Bi3} \) and \( C_{s}^{Bi} \) satisfy \( R_2 = 0 \). Letting \( P_1 = 5, P_2 = 3, N_1 = 2, N_2 = 8, N_r = 2 \) and \( Q = 300 \), and maximizing the secrecy rates \( R_1 \) of \( C_{s}^{Bi1}, C_{s}^{Bi2}, C_{s}^{Bi3} \) and \( C_{s}^{Bi} \), the following Figure 4 shows the relationship between \( R_1 \) and \( \alpha \) for different cooperation strategies. It is easy
to see that the NF strategy and the CF strategy help to obtain larger achievable secrecy rates. The DF strategy obtains the same secrecy rate as that of the Gaussian case of [22]. In addition, when $Q \to \infty$, the inner bound for the CF strategy is exactly the same as that for the NF strategy.

Fig. 4: The achievable secrecy rate $R_1$ of the model of Figure 2.

IV. RELAY BROADCAST CHANNELS WITH ONE CONFIDENTIAL MESSAGE AND ONE COMMON MESSAGE

In this section, the main results on the model of Figure 3 are provided in Subsection IV-A, and the results are further explained via a Gaussian example, see Subsection IV-B.

A. Problem formulation and the main results

The model of Figure 3 is similar to the model of Figure 1 except that there is no confidential message $W_2$. The channel encoder is a stochastic encoder that maps the messages $W_0$ and $W_1$ into a codeword $x^N \in \mathcal{X}^N$.

The decoder for receiver 1 is a mapping $f_{D1} : Y^N \to W_0 \times W_1$, with input $Y^N$ and outputs $\hat{W}_0$ and $\hat{W}_1$. Let $P_{e1}$ be the error probability of receiver 1, and it is defined as $Pr\{ (\hat{W}_0, \hat{W}_1) \neq (W_0, W_1) \}$.

Analogously, the decoder for receiver 2 is a mapping $f_{D2} : Z^N \to W_0$, with input $Z^N$ and output $\hat{W}_0$. Let $P_{e2}$ be the error probability of receiver 2, and it is defined as $Pr\{ \hat{W}_0 \neq W_0 \}$.

A rate triple $(R_0, R_1, R_e)$ (where $R_0, R_1, R_e > 0$) is called achievable if, for any $\epsilon > 0$ (where $\epsilon$ is an arbitrary small positive real number and $\epsilon \to 0$), there exists a channel encoder-decoder $(N, \Delta, P_{e1}, P_{e2})$ such that

$$\lim_{N \to \infty} \frac{\log \| W_0 \|}{N} = R_0, \quad \lim_{N \to \infty} \frac{\log \| W_1 \|}{N} = R_1, \quad \lim_{N \to \infty} \Delta \geq R_e, \quad P_{e1} \leq \epsilon, \quad P_{e2} \leq \epsilon.$$  \hspace{1cm} (4.10)
The capacity-equivocation region $\mathcal{R}^{(C)}$ is a set composed of all achievable $(R_0, R_1, R_e)$ triples. The inner and outer bounds on the capacity-equivocation region $\mathcal{R}^{(C)}$ are provided from Theorem 9 to Theorem 12; see the remainder of this subsection.

The first result is an outer-bound on the capacity-equivocation region of the model of Figure 3.

**Theorem 9: (Outer bound)** A single-letter characterization of the region $\mathcal{R}^{(Co)}$ ($\mathcal{R}^{(C)} \subseteq \mathcal{R}^{(Co)}$) is as follows,

$$
\mathcal{R}^{(Co)} = \{(R_0, R_1, R_e) : R_e \leq R_1, \quad
R_0 \leq \min\{I(U; U_1), I(U; Y_1|U_1)\}, \quad
R_0 \leq \min\{I(U; U_2; Z), I(U; Z, Y_1|U_2)\}, \quad
R_0 + R_1 \leq \min\{I(U; U_1, V; Y), I(U; V; Y, Y_1|U_1)\}, \quad
R_0 + R_1 \leq I(U; U_1; Z, Y_1|U_2) + I(V; Y, Y_1|U_1, U_2), \quad
R_e \leq I(V; Y|U) - I(V; Z|U),
$$

where $U \rightarrow (U_1, U_2, V) \rightarrow (X, X_1) \rightarrow (Y, Y_1, Z)$.

**Remark 9:** There are some notes on Theorem 9; see the following.

- **Theorem 9** is directly obtained from Theorem 1 by letting $R_2 = 0$, $R_{e2} = 0$ and $V_2 = \text{const}$, and therefore, the proof of Theorem 9 is omitted here.

- Removing the relay node from the model of Figure 3, the model reduces to the broadcast channels with one confidential message and one common message [20]. Letting $U_1 = U_2 = Y_1 = \text{const}$, the region $\mathcal{R}^{(Co)}$ is exactly the same as the capacity-equivocation region in [20].

- The outer bound on the secrecy capacity region of Figure 3 is denoted as $\mathcal{C}_s^{Co}$, which is the set of pairs $(R_0, R_1)$ such that $(R_0, R_1, R_e = R_1) \in \mathcal{R}^{(Co)}$.

**Corollary 9:**

$$
\mathcal{C}_s^{Co} = \{(R_0, R_1) : \quad
R_0 \leq \min\{I(U; U_1), I(U; Y_1|U_1)\}, \quad
R_0 \leq \min\{I(U; U_2; Z), I(U; Z, Y_1|U_2)\}, \quad
R_0 + R_1 \leq \min\{I(U; U_1, V; Y), I(U; V; Y, Y_1|U_1)\}, \quad
R_0 + R_1 \leq I(U; U_1; Z, Y_1|U_2) + I(V; Y, Y_1|U_1, U_2), \quad
R_1 \leq I(V; Y|U) - I(V; Z|U).
$$

**Proof:** Substituting $R_e = R_1$ into the region $\mathcal{R}^{(Co)}$, Corollary 9 is easily to be checked.

We now turn our attention to constructing cooperation strategies for the model of Figure 3. Our first step is to characterize the inner bound on the capacity-equivocation region by using DF Strategy. In the DF Strategy, the relay node will first decode the common message, and then re-encode the common message to cooperate with the
transmitter. Then, the superposition coding and random binning techniques used in [20] will be combined with the DF cooperation strategy to characterize the inner bound.

**Theorem 10:** (Inner bound 1: DF strategy) A single-letter characterization of the region \( R^{(C_{11})} \) \((R^{(C_{11})} \subseteq R^{(C)})\) is as follows,

\[
R^{(C_{11})} = \{(R_0, R_1, R_e) : R_e \leq R_1, \\
R_0 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\}, \\
R_0 + R_1 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\} + I(V; Y|U, X_1), \\
R_e \leq I(V; Y|U, X_1) - I(V; Z|U, X_1),
\]

for some distribution

\[
P_{Y,Z,Y_1,X_1,V,U}(y, z, y_1, x, x_1, v, u) = P_{Y,Z,Y_1,X_1}(y, z, y_1|x, x_1)P_{X_1|U,V}(x_1|u,v)P_{U,V}(u,v).
\]

**Remark 10:** There are some notes on Theorem 10, see the following.

- The inequality \( R_0 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\} \) follows from the fact that the relay node decode-and-forward the common message \( W_0 \). The inequalities \( R_0 + R_1 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\} \) + \( I(V; Y|U, X_1) \) and \( R_e \leq I(V; Y|U, X_1) - I(V; Z|U, X_1) \) follow from the fact that the relay codeword \( x_1^N \) can be decoded by both receivers, and from Csiszár-Körner’s techniques on broadcast channels with confidential messages [20]. Since the proof is obvious, we omit the details about the proof of Theorem 10.

- The first inner bound on the secrecy capacity region of Figure 3 is denoted as \( C_{s_{11}}^{C_{11}} \), which is the set of pairs \((R_0, R_1)\) such that \((R_0, R_1, R_e = R_1) \in R^{(C_{11})}\).

**Corollary 10:**

\[
C_{s_{11}}^{C_{11}} = \{(R_0, R_1) : \\
R_0 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\}, \\
R_1 \leq I(V; Y|U, X_1) - I(V; Z|U, X_1)\}.
\]

**Proof:** Substituting \( R_e = R_1 \) into the region \( R^{(C_{11})} \), Corollary 10 is easily to be checked.

The second step is to characterize the inner bound on the capacity-equivocation region by using the NF strategy. In the NF Strategy, the relay node does not attempt to decode the messages but sends codewords that are independent of the transmitters messages, and these codewords aid in confusing the receivers. Different from the NF strategies for the models with two confidential messages, the NF strategy for the model with one confidential message is considered into the following two cases.

- **(Case 1)** If the channel from the relay to receiver 1 is less noisy than the channel from the relay to receiver 2 \( I(X_1; Y) \geq I(X_1; Z|U) \), we allow receiver 1 to decode \( x_1^N \), and receiver 2 can not decode it. Therefore, in this case, \( x_1^N \) can be viewed as a noise signal to confuse receiver 2.
• (Case 2) If the channel from the relay to receiver 1 is more noisy than the channel from the relay to receiver 2, we allow both the receivers to decode $x_1^N$, and therefore, in this case, the relay codeword $x_1^N$ cannot make any contribution to the security of the model of Figure 3.

Theorem 11: (Inner bound 2: NF strategy) A single-letter characterization of the region $R^{(C/2)}$ ($R^{(C/2)} \subseteq R^{(C)}$) is as follows,

$$R^{(C/2)} = \mathcal{L}^9 \cup \mathcal{L}^{10},$$

where $\mathcal{L}^9$ is given by

$$\mathcal{L}^9 = \bigcup_{P_{Y,Z,Y_1,X,X_1,V,U}: I(X_1; Y) \geq I(X_1; Z|U)} \left\{ (R_0, R_1, R_v) : R_v \leq R_1, \\
R_0 \leq \min\{I(U; Y|X_1), I(U; Z)\}, \\
R_0 + R_1 \leq \min\{I(U; Y|X_1), I(U; Z)\} + I(V; Y|U, X_1), \\
R_v \leq \min\{I(X_1; Z|U, V), I(X_1; Y)\} + I(V; Y|U, X_1) - I(X_1, V; Z|U). \right\},$$

$\mathcal{L}^{10}$ is given by

$$\mathcal{L}^{10} = \bigcup_{P_{Y,Z,Y_1,X,X_1,V,U}: I(X_1; Z) \geq I(X_1; Y)} \left\{ (R_0, R_1, R_v) : R_v \leq R_1, \\
R_0 \leq \min\{I(U; Y|X_1), I(U; Z|X_1)\}, \\
R_0 + R_1 \leq \min\{I(U; Y|X_1), I(U; Z|X_1)\} + I(V; Y|U, X_1), \\
R_v \leq I(V; Y|U, X_1) - I(V; Z|U, X_1). \right\},$$

and $P_{Y,Z,Y_1,X,X_1,V,U}(y, z, y_1, x, x_1, v, u)$ satisfies

$$P_{Y,Z,Y_1,X,X_1,V,U}(y, z, y_1, x, x_1, v, u) = P_{Y,Z,Y_1,X,X_1}(y, z, y_1|x, x_1)P_{X,V|U}(x|u, v)P_{U,V}(u, v)P_{X_1}(x_1).$$

The proof of Theorem 11 is in Appendix E.

Remark 11: There are some notes on Theorem 11. See the following.

• The regions $\mathcal{L}^9$ and $\mathcal{L}^{10}$ are characterized according to case 1 and case 2, respectively.

• The second inner bound on the secrecy capacity region of Figure 3 is denoted as $C_s^{C/2}$, which is the set of pairs $(R_0, R_1)$ such that $(R_0, R_1, R_v = R_1) \in R^{(C/2)}$.

Corollary 11:

$$C_s^{C/2} = \mathcal{L}^i \cup \mathcal{L}^i,$$

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

$$\mathcal{L}^i = \bigcup_{P_{Y,Z,Y_1,X,X_1,V,U}: I(X_1; Y) \geq I(X_1; Z|U)} \left\{ (R_0, R_1) : \right.$$

$$R_0 \leq \min\{I(U; Y|X_1), I(U; Z)\}, \\
R_0 + R_1 \leq \min\{I(U; Y|X_1), I(U; Z)\} + I(V; Y|U, X_1), \\
R_1 \leq \min\{I(X_1; Z|U, V), I(X_1; Y)\} + I(V; Y|U, X_1) - I(X_1, V; Z|U). \right\},$$

$$\left. \right\}$$
and $\mathcal{L}^j$ is given by

$$
\mathcal{L}^j = \bigcup_{P_{Y,Z,Y_1,X_1,Y_2,V,U} : I(X_1,Y) \geq I(X_1,Z)} \left\{ (R_1, R_2) : \begin{array}{l}
R_0 \leq \min \{ I(U;Y|X_1), I(U;Z|X_1) \}, \\
R_1 \leq I(V;Y|U,X_1) - I(V;Z|U,X_1).
\end{array} \right\}.
$$

Proof: Substituting $R_e = R_1$ into the region $\mathcal{R}^{(C_{i3})}$, Corollary 11 is easily to be checked.

The third step is to characterize the inner bound on the capacity-equivocation region by using a combination of CF strategy and NF strategy, i.e., in addition to the independent codewords, the relay also sends a quantized version of its noisy observations to the receivers. This noisy version of the relay’s observations helps the receivers in decoding the transmitter’s messages, while the independent codewords help in confusing the receivers. Similar to Theorem 11, we consider the CF strategy into two cases.

**Theorem 12:** (Inner bound 3: CF strategy) A single-letter characterization of the region $\mathcal{R}^{(C_{i3})}$ ($\mathcal{R}^{(C_{i3})} \subseteq \mathcal{R}^{(C)}$) is as follows,

$$
\mathcal{R}^{(C_{i3})} = \mathcal{L}^{11} \cup \mathcal{L}^{12},
$$

where $\mathcal{L}^{11}$ is given by

$$
\mathcal{L}^{11} = \bigcup_{P_{Y,Z,Y_1,X_1,Y_2,V,U} : I(X_1,Y) \geq I(X_1,Z)} \left\{ (R_0, R_1, R_e) : \begin{array}{l}
R_0 \leq \min \{ I(U;Y,Y_1|X_1), I(U;Z|X_1) \}, \\
R_0 + R_1 \leq \min \{ I(U;Y,Y_1|X_1), I(U;Z|X_1) \} + I(V;Y,Y_1|U,X_1), \\
R_e \leq R^* + I(V;Y,Y_1|U,X_1) - I(X_1,V;Z|U).
\end{array} \right\},
$$

and $P_{Y,Z,Y_1,X_1,X_1,Y_2,V,U}(y,z,y_1,\hat{y}_1, x_1, v, u)$ satisfies

$$
P_{Y,Z,Y_1,Y_1,X_1}(y,z,y_1|x_1)P_{X|V,U}(x|u,v)P_{U,V}(u,v)P_{Y_1|Y_1,x_1}(\hat{y}_1|y_1,x_1)P_{X_1}(x_1).
$$

The proof of Theorem 12 is in Appendix F.

**Remark 12:** There are some notes on Theorem 12, see the following.

- In $\mathcal{L}^{11}$, $R^*$ is the rate of pure noise generated by the relay to confuse the receivers, while $R^*_{r_1} - R^*$ is the part of the rate allocated to send the compressed signal $\hat{Y}_1$ to help the receivers. If $R^* = R^*_{r_1}$, this scheme is exactly the same as the NF scheme.

- The third inner bound on the secrecy capacity region of Figure 3 is denoted as $\mathcal{C}_s^{C_{i3}}$, which is the set of pairs $(R_0, R_1)$ such that $(R_0, R_1, R_e = R_1) \in \mathcal{R}^{(C_{i3})}$. 
Corollary 12:

\[ C_s^{C_{13}} = \mathcal{L}^k \bigcup \mathcal{L}^l, \]

where \( \mathcal{L}^k \) is given by

\[
\mathcal{L}^k = \bigcup_{P_{Y,Z,Y_1,X_1,V,X_1,U} : I(X_1;Y) \geq I(X_1;Z|U)} \{ (R_0, R_1) : \\
R_0 \leq \min\{I(U;Y,Y_1|X_1), I(U;Z)\} \\
R_0 + R_1 \leq \min\{I(U;Y,Y_1|X_1), I(U;Z) + I(V;Y,Y_1|U,X_1)\} \\
R_1 \leq R^* + I(V;Y,Y_1|U,X_1) - I(X_1,V;Z|U). \}
\]

\( R^*_{c1} = \min\{I(X_1;Z|U,V), I(X_1;Y)\} \), and \( \mathcal{L}^l \) is given by

\[
\mathcal{L}^l = \bigcup_{P_{Y,Z,Y_1,X_1,V,X_1,U} : I(X_1;Y) \geq I(X_1;Z|U)} \{ (R_0, R_1) : \\
R_0 \leq \min\{I(U;Y,Y_1|X_1), I(U;Z,Y_1|X_1)\} \\
R_1 \leq I(V;Y,Y_1|U,X_1) - I(V;Z|U,X_1). \}
\]

Proof: Substituting \( R_{c1} = R_1 \) into the region \( \mathcal{R}(C_{13}) \), Corollary 12 is easily to be checked.

B. Gaussian relay broadcast channels with one confidential message and one common message

In this subsection, we investigate the Gaussian case of the model of Figure 3. The signal received at each node is given by

\[
Y_1 = X + Z_r, \\
Y = X + X_1 + Z_1, \\
Z = X + X_1 + Z_2,
\]

(4.11)

where \( Z_r \sim \mathcal{N}(0, N_r) \), \( Z_1 \sim \mathcal{N}(0, N_1) \), \( Z_2 \sim \mathcal{N}(0, N_2) \), and they are independent, \( E[X^2] \leq P_1 \), \( E[X^2] \leq P_2 \). In this subsection, we assume that \( P_1 + N_1 \leq N_2 \), which implies that the channel for receiver 1 is less noisy than the channel for receiver 2.

The inner bound on the secrecy capacity region of Figure 3 by using the DF strategy is given by

\[
C_s^{C_{11}} = \bigcup_{0 \leq \alpha \leq 1} \{ (R_0, R_1) : \\
R_0 \leq \min\{\frac{1}{2} \log \frac{P_1 + N_1}{\alpha P_1 + N_1}, \frac{1}{2} \log \frac{P_1 + P_2 + N_1}{\alpha P_1 + N_1}, \frac{1}{2} \log \frac{P_1 + P_2 + N_2}{\alpha (P_1 + N_2)}\} \\
R_1 \leq \frac{1}{2} \log \frac{\alpha P_1 + N_1}{N_1} - \frac{1}{2} \log \frac{\alpha (P_1 + N_2)}{N_2}, \}
\]

(4.12)

Here \( C_s^{C_{11}} \) is obtained by letting \( X = U + V \) and \( U = c_1 X_1 + X_{10} \), where \( U \sim \mathcal{N}(0,(1-\alpha)P_1) \), \( V \sim \mathcal{N}(0,\alpha P_1) \), \( X_{10} \sim \mathcal{N}(0,(1-\alpha)\beta P_1) \) (0 \( \leq \beta \leq 1 \)), and \( c_1 = \sqrt{\frac{P_1(1-\alpha)[1-\beta]}{P_2}} \). \( X_{10}, X_1, V \) and \( U \) are independent random variables.

Then, the inner bound on the secrecy capacity region by using the NF strategy is given by

\[
C_s^{C_{12}} = \bigcup_{0 \leq \alpha \leq 1} \{ (R_0, R_1) : \\
R_0 \leq \min\{\frac{1}{2} \log \frac{P_3 + N_1}{\alpha P_3 + N_1}, \frac{1}{2} \log \frac{P_3 + P_2 + N_1}{\alpha P_3 + N_1}, \frac{1}{2} \log \frac{P_3 + P_2 + N_2}{\alpha (P_3 + N_2)}\} \\
R_1 \leq \frac{1}{2} \log \frac{\alpha (P_3 + N_1)}{N_1} - \frac{1}{2} \log \frac{\alpha (P_3 + P_2 + N_2)}{N_2}, \}
\]

(4.13)
Here note that \( P_1 + N_1 \leq N_2 \) implies \( I(X_1; Y) \geq I(X_1; Z|U) \), and \( C^C_{s12} \) is obtained by letting \( X = U + V \), where \( V \sim \mathcal{N}(0, (1-\alpha)P_1) \), \( U \sim \mathcal{N}(0, \alpha P_1) \). \( X_1 \), \( U \) and \( V \) are independent random variables.

Next, the inner bound on the secrecy capacity region by using the CF strategy is given by

\[
C^C_{s} = \bigcup_{0 \leq \alpha \leq 1} \left\{ (R_0, R_1) : \begin{array}{l}
R_0 \leq \min\left\{ \frac{1}{2} \log \frac{P_1(N_r+Q)+N_1}{N_1(N_r+Q)}, \frac{1}{2} \log \frac{P_1 + P_2 + N_2}{N_1(N_r+Q)} \right\} \\
R_1 \leq R^* + \frac{1}{2} \log \frac{P_1(N_r+Q)+N_1}{N_1(N_r+Q)} - \frac{1}{2} \log \frac{P_1 + P_2 + N_2}{N_1(N_r+Q)} \end{array} \right\},
\]

subject to

\[
0 \leq R^* \leq \min\left\{ \frac{1}{2} \log \frac{P_2 + N_2}{N_2}, \frac{1}{2} \log \frac{P_1 + P_2 + N_1}{P_1 + N_1} \right\} - \frac{1}{2} \log \frac{P_1 + Q + N_r}{Q}.
\]

Here note that \( P_1 + N_1 \leq N_2 \) implies \( I(X_1; Y) \geq I(X_1; Z|U) \), and \( C^C_{s13} \) is obtained by letting \( X = U + V \), \( \hat{Y}_1 = Y_1 + Z_Q \), where \( Z_Q \sim \mathcal{N}(0, Q) \), \( V \sim \mathcal{N}(0, (1-\alpha)P_1) \), \( U \sim \mathcal{N}(0, \alpha P_1) \). \( X_1 \), \( U \) and \( V \) are independent random variables.

Finally, remember that [33] provides the secrecy capacity region of the broadcast channels with one confidential message and one common message, and it is given by

\[
C^C_s = \bigcup_{0 \leq \alpha \leq 1} \left\{ (R_0, R_1) : \begin{array}{l}
R_0 \leq \min\left\{ \frac{1}{2} \log \frac{P_1(N_r+Q)+N_1}{N_1(N_r+Q)}, \frac{1}{2} \log \frac{P_1 + N_2}{N_1(N_r+Q)} \right\} \\
R_1 \leq \frac{1}{2} \log \frac{P_1(N_r+Q)+N_1}{N_1(N_r+Q)} - \frac{1}{2} \log \frac{P_1 + N_2}{N_1(N_r+Q)} \end{array} \right\}.
\]

Letting \( P_1 = 5 \), \( P_2 = 3 \), \( N_1 = 2 \), \( N_2 = 8 \), \( N_r = 2 \) and \( Q = 300 \), the following Figure 5 shows the achievable secrecy rate regions of the model of Figure 3 without the relay, it is easy to see that the maximum achievable secrecy rate \( R_1 \) is enhanced by using the NF and the CF strategies. For the DF strategy, though it can not increase the maximum achievable secrecy rate \( R_1 \), the maximum achievable common rate \( R_0 \) is enhanced. In addition, when \( Q \rightarrow \infty \), the inner bound for the CF strategy is exactly the same as that for the NF strategy.

V. CONCLUSION

In this paper, we generalize the previous works on the broadcast channels with confidential messages, the relay broadcast channel and the relay-eavesdropper channel. Several cooperative strategies are constructed to enhance the security of the broadcast channels with confidential messages. The details are as follows.

- First, we investigate the relay broadcast channels with two confidential messages and one common message.
  Three inner bounds (with respect to decode-forward, generalized noise-forward and compress-forward strategies) and an outer bound on the capacity-equivocation region are provided. Removing the secrecy constraint, this outer bound can also be served as a new outer bound for the general relay broadcast channel.

- Second, we investigate the relay broadcast channels with two confidential messages (no common message).
  Inner and outer bounds on the capacity-equivocation region are provided. Then, we study the Gaussian case, and find that with the help of the relay node, the achievable secrecy rate region of the broadcast channels with two confidential messages is enhanced.
• Third, we investigate the relay broadcast channels with one confidential message and one common message. This work generalizes Lai-Gamal’s work on the relay-eavesdropper channel by considering an additional common message for both the legitimate receiver and the eavesdropper. Inner and outer bounds on the capacity-equivocation region are provided, and the results are further explained via a Gaussian example. Compared with Csiszár-Körner’s work on broadcast channels with confidential messages (BCC), we find that with the help of the relay node, the secrecy capacity region of the Gaussian BCC is enhanced.

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, and the National Natural Science Foundation of China under Grant 61301121.

APPENDIX A

PROOF OF THEOREM

In this section, we will prove Theorem all the achievable \((R_0, R_1, R_2, R_{e1}, R_{e2})\) quintuples are contained in the set \(R_{Ao}\). The inequalities of Theorem are proved in the remainder of this section.

First, define the following auxiliary random variables,

\[
U_1 \triangleq Y_1^{J-1}, U_2 \triangleq Y_{1,J+1}^N, U \triangleq (Y^{J-1}, W_0, Z_{J+1}^N, J) \\
V_1 \triangleq (U, W_1), V_2 \triangleq (U, W_2) \\
Y \triangleq Y_J, Y_1 \triangleq Y_{1,J}, Z \triangleq Z_J,
\]

(A1)
where $J$ is a random variable (uniformly distributed over $\{1, 2, \ldots, N\}$), and it is independent of $Y^N$, $Y_1^N$, $Z^N$, $W_0$, $W_1$ and $W_2$.

**(Proof of $R_0 \leq \min\{I(U, U_1; Y), I(U; Y, Y_1|U_1)\}**

The inequality $R_0 \leq I(U, U_1; Y)$ is proved as follows.

$$
\frac{1}{N} H(W_0) \leq \frac{1}{N} (I(W_0; Y^N) + H(W_0|Y^N))
$$

$$
\leq (a) \frac{1}{N} (I(W_0; Y^N) + \delta(P_{\epsilon}))
$$

$$
= \frac{1}{N} \left( \sum_{i=1}^{N} I(W_0; Y_i|Y^{i-1}) + \delta(P_{\epsilon}) \right)
$$

$$
= \frac{1}{N} \left( \sum_{i=1}^{N} (H(Y_i|Y^{i-1}) - H(Y_i|Y^{i-1}, W_0)) + \frac{\delta(P_{\epsilon})}{N} \right)
$$

$$
\leq \frac{1}{N} \left( \sum_{i=1}^{N} (H(Y_i) - H(Y_i|Y^{i-1}, W_0, Y_1^{i-1}, Z_i^{N+1}, J = i)) + \frac{\delta(P_{\epsilon})}{N} \right)
$$

$$
= b) \frac{1}{N} \sum_{i=1}^{N} (H(Y_i|J = i) - H(Y_i|Y^{i-1}, W_0, Y_1^{i-1}, Z_i^{N+1}, J = i)) + \frac{\delta(P_{\epsilon})}{N}
$$

$$
= c) H(Y_J) - H(Y_J|Y^{J-1}, W_0, Y_1^{J-1}, Z_{J+1}^{N}, J) + \frac{\delta(P_{\epsilon})}{N}
$$

$$
= d) H(Y) - H(Y|U_1, U) + \frac{\delta(P_{\epsilon})}{N}
$$

$$
= e) I(U_1, U; Y) + \frac{\delta(\epsilon)}{N}, \quad (A2)
$$

where (a) is from the Fano’s inequality, (b) is from the fact that $J$ is a random variable (uniformly distributed over $\{1, 2, \ldots, N\}$), and it is independent of $Y^N$, $Y_1^N$, $Z^N$, $W_0$, $W_1$ and $W_2$, (c) is from $J$ is uniformly distributed over $\{1, 2, \ldots, N\}$, (d) is from the definitions of the auxiliary random variables (see (A1)), and (e) is from $P_{\epsilon} \leq \epsilon$.

By using $\epsilon \to 0$, $R_0 = \lim_{N \to \infty} \frac{H(W_0)}{N}$ and (A2), $R_0 \leq I(U, U_1; Y)$ is obtained.

The inequality $R_0 \leq I(U; Y, Y_1|U_1)$ is proved as follows.

$$
\frac{1}{N} H(W_0) \leq \frac{1}{N} (I(W_0; Y_1^N, Y^N) + H(W_0|Y_1^N, Y^N))
$$

$$
\leq \frac{1}{N} (I(W_0; Y_1^N, Y^N) + \delta(P_{\epsilon}))
$$

$$
= \frac{1}{N} \left( \sum_{i=1}^{N} I(W_0; Y_1^{i}, Y_i|Y^{i-1}) + \delta(P_{\epsilon}) \right)
$$

$$
= \frac{1}{N} \left( \sum_{i=1}^{N} (H(Y_1^{i}, Y_i|Y^{i-1}) - H(Y_1^{i}, Y_i|Y^{i-1}, Y_1^{i-1}, Y^{i-1}, W_0)) + \frac{\delta(P_{\epsilon})}{N} \right)
$$

$$
\leq \frac{1}{N} \left( \sum_{i=1}^{N} (H(Y_1^{i}, Y_i|Y^{i-1}) - H(Y_1^{i}, Y_i|Y^{i-1}, W_0, Y_1^{i-1}, Z_i^{N+1})) + \frac{\delta(P_{\epsilon})}{N} \right)
$$

$$
= \frac{1}{N} \left( \sum_{i=1}^{N} (H(Y_1^{i}, Y_i|Y^{i-1}, J = i) - H(Y_1^{i}, Y_i|Y^{i-1}, W_0, Y_1^{i-1}, Z_i^{N+1}, J = i)) + \frac{\delta(P_{\epsilon})}{N} \right)
$$
\[
\begin{aligned}
& \leq H(Y_J, Y_{1,J}|Y_1^{J-1}) - H(Y_J, Y_{1,J}|Y_1^{J-1}, Y_0, Y_1^{J-1}, Z_{J+1}^N, J) + \frac{\delta(P_{c1})}{N} \\
& \overset{(a)}{=} H(Y, Y_1|U_1) - H(Y, Y_1|U_1, U) + \frac{\delta(P_{c1})}{N} \\
& \leq I(U; Y, Y_1|U_1) + \frac{\delta(\epsilon)}{N},
\end{aligned}
\]

where (a) is from (A1). By using $\epsilon \to 0$, $R_0 = \lim_{N \to \infty} \frac{H(W_0)}{N}$ and (A3), $R_0 \leq I(U; Y, Y_1|U_1)$ is obtained.

Therefore, $R_0 \leq \min\{I(U, U_2; Z), I(U; Z, Y_1|U_2)\}$ is proved.

**Proof of** $R_0 \leq \min\{I(U, U_2; Z), I(U; Z, Y_1|U_2)\}$

The inequality $R_0 \leq I(U, U_2; Z)$ is proved as follows.

\[
\begin{aligned}
\frac{1}{N} H(W_0) & \leq \frac{1}{N} (I(W_0; Z^N) + H(W_0|Z^N)) \\
& \leq \frac{1}{N} (I(W_0; Z^N) + \delta(P_{c2})) \\
& = \frac{1}{N} \sum_{i=1}^N I(W_0; Z_i|Z_i^{N+1}) + \delta(P_{c2})) \\
& = \frac{1}{N} \sum_{i=1}^N (H(Z_i|Z_i^{N+1}) - H(Z_i|Z_i^{N+1}, W_0)) + \frac{\delta(P_{c2})}{N} \\
& \leq \frac{1}{N} \sum_{i=1}^N (H(Z_i) - H(Z_i|Y_i^{i-1}, W_0, Y_i^{N+1}, Z_i^{N+1}, J = i)) + \frac{\delta(P_{c2})}{N} \\
& = H(Z) - H(Z|Y_{1,i+1}, Z_{i+1}^N, J) + \frac{\delta(P_{c2})}{N} \\
& \leq I(U_2; U; Z) + \frac{\delta(\epsilon)}{N}.
\end{aligned}
\]

By using $\epsilon \to 0$, $R_0 = \lim_{N \to \infty} \frac{H(W_0)}{N}$ and (A4), $R_0 \leq I(U_2, U; Z)$ is obtained.

The inequality $R_0 \leq I(U; Z, Y_1|U_2)$ is proved as follows.

\[
\begin{aligned}
\frac{1}{N} H(W_0) & \leq \frac{1}{N} (I(W_0; Y_1^N, Z^N) + H(W_0|Y_1^N, Z^N)) \\
& \leq \frac{1}{N} (I(W_0; Y_1^N, Z^N) + \delta(P_{c2})) \\
& = \frac{1}{N} \sum_{i=1}^N I(W_0; Y_{1,i}, Z_i|Y_{1,i}^{N+1}, Z_i^{N+1}, Z_i^{N+1}) + \delta(P_{c2})) \\
& = \frac{1}{N} \sum_{i=1}^N (H(Y_{1,i}, Z_i|Y_{1,i}^{N+1}, Z_i^{N+1}) - H(Y_{1,i}, Z_i|Y_{1,i}^{N+1}, Z_i^{N+1}, W_0)) + \frac{\delta(P_{c2})}{N} \\
& \leq \frac{1}{N} \sum_{i=1}^N (H(Y_{1,i}, Z_i|Y_{1,i}^{N+1}) - H(Y_{1,i}, Z_i|Y_{1,i}^{N+1}, W_0, Y_{1,i}^{N+1}, Z_{i+1}^N)) + \frac{\delta(P_{c2})}{N} \\
& = \frac{1}{N} \sum_{i=1}^N (H(Y_{1,i}, Z_i|Y_{1,i}^{N+1}, J = i) - H(Y_{1,i}, Z_i|Y_{1,i}^{N+1}, W_0, Y_{1,i}^{N+1}, Z_{i+1}^N)) + \frac{\delta(P_{c2})}{N}
\end{aligned}
\]
\begin{align*}
  &\leq H(Z_J,Y_{1,J}|Y_{1,J+1}^{N}) - H(Z_J,Y_{1,J}|Y^{J-1},W_0,Y_{1,J+1}^{N},Z_{J+1}^{N},J) + \frac{\delta(P_{e1})}{N} \\
  &= H(Z,Y_{1}|U_2) - H(Z,Y_{1}|U_2,U) + \frac{\delta(P_{e2})}{N} \\
  &\leq I(U;Z,Y_{1}|U_2) + \frac{\delta(\epsilon)}{N}. \quad \text{(A5)}
\end{align*}

By using $\epsilon \to 0$, $R_0 = \lim_{N \to \infty} \frac{H(W_0)}{N}$ and (A5), $R_0 \leq I(U;Z,Y_{1}|U_2)$ is obtained.

Therefore, $R_0 \leq \min\{I(U,U_2;Z),I(U;Z,Y_{1}|U_2)\}$ is proved.

**Proof of** $R_0 + R_1 \leq \min\{I(U,U_1,V_1;Y),I(U,V_1;Y,Y_{1}|U_1)\}$

The inequality $R_0 + R_1 \leq I(U,U_1,V_1;Y)$ is proved as follows.

\begin{align*}
  \frac{1}{N}H(W_0,W_1) &\leq \frac{1}{N}(I(W_0,W_1;Y^N) + H(W_0,W_1|Y^N)) \\
  &\leq \frac{1}{N}(I(W_0,W_1;Y^N) + \delta(P_{e1})) \\
  &= \frac{1}{N}\left(\sum_{i=1}^{N} I(W_0,W_1;Y_i|Y^{i-1}) + \delta(P_{e1})\right) \\
  &= \frac{1}{N}\left(\sum_{i=1}^{N} (H(Y_i|Y^{i-1}) - H(Y_i|Y^{i-1},W_0,W_1)) + \frac{\delta(P_{e1})}{N}\right) \\
  &\leq \frac{1}{N}\left(\sum_{i=1}^{N} (H(Y_i) - H(Y_i|Y^{i-1},W_0,W_1,Y_{1,i-1},Z_{1,i+1}^{N})) + \frac{\delta(P_{e1})}{N}\right) \\
  &= \frac{1}{N}\left(\sum_{i=1}^{N} (H(Y_{J}) - H(Y_{J}|Y^{J-1},W_0,W_1,Y_{1,i-1},Z_{1,i+1}^{N},J) + \frac{\delta(P_{e1})}{N}\right) \\
  &\leq H(Y_{J}) - H(Y_{J}|Y^{J-1},W_0,W_1,Y_{1,i-1},Z_{1,i+1}^{N},J) + \frac{\delta(P_{e1})}{N} \\
  &= I(U_1,U,V_1;Y) + \frac{\delta(\epsilon)}{N}. \quad \text{(A6)}
\end{align*}

By using $\epsilon \to 0$, $R_0 + R_1 = \lim_{N \to \infty} \frac{H(W_0,W_1)}{N}$ and (A6), $R_0 + R_1 \leq I(U,U_1,V_1;Y)$ is obtained.

The inequality $R_0 + R_1 \leq I(U,V_1;Y,Y_{1}|U_1)$ is proved as follows.

\begin{align*}
  \frac{1}{N}H(W_0,W_1) &\leq \frac{1}{N}(I(W_0,W_1;Y^N,Y^N) + H(W_0,W_1|Y^N,Y^N)) \\
  &\leq \frac{1}{N}(I(W_0,W_1;Y^N,Y^N) + \delta(P_{e1})) \\
  &= \frac{1}{N}\left(\sum_{i=1}^{N} I(W_0,W_1;Y_{1,i},Y_{1,i-1},Y^{i-1}) + \delta(P_{e1})\right) \\
  &= \frac{1}{N}\left(\sum_{i=1}^{N} (H(Y_{1,i},Y_{1,i-1},Y^{i-1}) - H(Y_{1,i},Y_{1,i-1},Y^{i-1},W_0,W_1)) + \frac{\delta(P_{e1})}{N}\right) \\
  &\leq \frac{1}{N}\left(\sum_{i=1}^{N} (H(Y_{1,i},Y_{1,i-1}) - H(Y_{1,i},Y_{1,i-1},W_0,W_1,Y_{1,i-1},Z_{1,i+1}^{N})) + \frac{\delta(P_{e1})}{N}\right) \\
  &= \frac{1}{N}\left(\sum_{i=1}^{N} (H(Y_{1,i},Y_{1,i-1},J = i) - H(Y_{1,i},Y_{1,i-1},W_0,W_1,Y_{1,i-1},Z_{1,i+1}^{N},J = i)) + \frac{\delta(P_{e1})}{N}\right)
\end{align*}
\[ H(Y_j, Y_1, j|Y_1^{j-1}) - H(Y_j, Y_1, j|Y_1^{j-1}, W_0, W_1, Y_1^{j-1}, Z_{j+1}^N, J) + \frac{\delta(P_{e1})}{N} \]

\[ = H(Y, Y_1|U_1) - H(Y, Y_1|U_1, U, V_1) + \frac{\delta(P_{e1})}{N} \]

\[ \leq I(U, V_1; Y, Y_1|U_1) + \frac{\delta(\epsilon)}{N}, \]

(A7)

By using \( \epsilon \to 0 \), \( R_0 + R_1 = \lim_{N \to \infty} \frac{H(W_0, W_1)}{N} \) and (A7), \( R_0 + R_1 \leq I(U, V_1; Y, Y_1|U_1) \) is obtained.

Therefore, \( R_0 + R_1 \leq \min\{I(U, U_1, V_1; Y), I(U, V_1; Y, Y_1|U_1)\} \) is proved.

(Proof of \( R \))

The proof of \( R_0 + R_2 \leq \min\{I(U, U_2, V_2; Z), I(U, V_2; Z, Y_1|U_2)\} \)

The inequality \( R_0 + R_2 \leq \min\{I(U, V_2, Y, Y_1|U_1)\} \) is analogous to the proof of \( R_0 + R_1 \leq \min\{I(U, U_1, V_1; Y), I(U, V_1; Y, Y_1|U_1)\} \) and it is omitted here.

(Proof of \( R \))

The inequality \( R_0 + R_2 \leq I(U, U_2, V_2; Y_1|U_1) + I(V_2; Z, Y_1|U_1, U_2, V_1) \)

The inequality \( R_0 + R_1 \leq I(U, U_2, V_1; Y_1|U_1) + I(V_2; Z, Y_1|U_1, U_2, V_1) \) is proved by the following (A8), (A9), (A10) and (A11).

First, note that

\[ \frac{1}{N} H(W_0, W_1, W_2) = \frac{1}{N} (H(W_0, W_1) + H(W_2|W_0, W_1)) \]

\[ = \frac{1}{N} [I(W_0, W_1; Y_1^N, Y^N) + H(W_0, W_1|Y_1^N, Y^N) + I(W_2; Y_1^N, Z^N|W_0, W_1) \]

\[ + H(W_2|W_0, W_1, Y_1^N, Z^N)] \]

\[ \leq \frac{1}{N} (I(W_0, W_1; Y_1^N, Y^N) + \delta(P_{e1}) + I(W_2; Y_1^N, Z^N|W_0, W_1) + \delta(P_{e2})), \]

(A8)

where (a) is from Fano’s inequality.

The character \( I(W_0, W_1; Y_1^N, Y^N) \) in (A8) is upper bounded by

\[ I(W_0, W_1; Y_1^N, Y^N) \]

\[ = \sum_{i=1}^{N} I(W_0, W_1; Y_1^i, Y_i|Y_1^{i-1}, Y^{i-1}) \]

\[ = \sum_{i=1}^{N} (H(Y_1^i, Y_i|Y_1^{i-1}, Y^{i-1}) - H(Y_1^i, Y_i|Y_1^{i-1}, Y^{i-1}, W_0, W_1) \]

\[ + H(Y_1^i, Y_i|Y_1^{i-1}, Y^{i-1}, W_0, W_1, Y_1^N, Z_{i+1}^N) - H(Y_1^i, Y_i|Y_1^{i-1}, Y^{i-1}, W_0, W_1, Y_1^N, Z_{i+1}^N)) \]

\[ = \sum_{i=1}^{N} (I(Y_1^i, Y_i; W_0, W_1, Y_1^N, Z_{i+1}^N|Y_1^{i-1}, Y^{i-1}) \]

\[ - I(Y_1^i, Y_i; Y_1^N, Z_{i+1}^N|Y_1^{i-1}, Y^{i-1}, W_0, W_1)), \]

(A9)

and the character \( I(W_2; Y_1^N, Z^N|W_0, W_1) \) in (A8) is upper bounded by

\[ I(W_2; Y_1^N, Z^N|W_0, W_1) \]

\[ = \sum_{i=1}^{N} I(W_2; Y_1^i, Z_i|Y_1^{i-1}, Z_{i+1}^N, W_0, W_1) \]
\[ \begin{align*}
&\quad \leq \sum_{i=1}^{N} I(W_2, Y_{i}^{i-1}, Y_1^{i-1}; Y_{1,i}, Z_i|Y_{1,i+1}^N, Z_{i+1}^N, W_0, W_1) \\
&= \sum_{i=1}^{N} (H(Y_{1,i}, Z_i|Y_{1,i+1}^N, Z_{i+1}^N, W_0, W_1) \\
&\quad - H(Y_{1,i}, Z_i|Y_{1,i+1}^N, Z_{i+1}^N, W_0, W_1, W_2, Y_{i}^{i-1}, Y_1^{i-1}) \\
&\quad + H(Y_{1,i}, Z_i|Y_{1,i+1}^N, Z_{i+1}^N, W_0, W_1, Y_{i}^{i-1}, Y_1^{i-1}) - H(Y_{1,i}, Z_i|Y_{1,i+1}^N, Z_{i+1}^N, W_0, W_1, Y_{i}^{i-1}, Y_1^{i-1}) \\
&= \sum_{i=1}^{N} (I(Y_{1,i}, Z_i; Y_{i}^{i-1}, Y_1^{i-1}|Y_{1,i+1}^N, Z_{i+1}^N, W_0, W_1) \\
&\quad + I(Y_{1,i}, Z_i; W_2|Y_{1,i+1}^N, Z_{i+1}^N, W_0, Y_{i}^{i-1}, Y_1^{i-1})). \\
&\quad (A10)
\end{align*} \]

Here note that \( \sum_{i=1}^{N} I(Y_{1,i}, Z_i; Y_{i}^{i-1}, Y_1^{i-1}|Y_{1,i+1}^N, Z_{i+1}^N, W_0, W_1) \) appeared in the last step of (A9) is equal to \( \sum_{i=1}^{N} I(Y_{1,i}, Z_i; Y_{i}^{i-1}, Y_1^{i-1}|Y_{1,i+1}^N, Z_{i+1}^N, W_0, W_1) \) appeared in the last step of (A10), i.e.,

\[ \begin{align*}
&\quad \sum_{i=1}^{N} I(Y_{1,i}, Z_i; Y_{i}^{i-1}, Y_1^{i-1}|Y_{1,i+1}^N, Z_{i+1}^N, W_0, W_1) \\
&= \sum_{i=1}^{N} I(Y_{1,i}, Z_i; Y_{i}^{i-1}, Y_1^{i-1}|Y_{1,i+1}^N, Z_{i+1}^N, W_0, W_1), \\
&\quad (A11)
\end{align*} \]

and it is proved by the following (A12) and (A13).

\[ \begin{align*}
&\quad \sum_{i=1}^{N} I(Y_{1,i}, Y_i; Y_{1,i+1}^N, Z_{i+1}^N|Y_{1}^{i-1}, Y_1^{i-1}, W_0, W_1) \\
&= \sum_{i=1}^{N} \sum_{j=i+1}^{N} I(Y_{1,i}, Y_i; Y_{1,j}, Z_{j}|Y_{1}^{i-1}, Y_1^{i-1}, W_0, W_1, Y_{1,j+1}^N, Z_{j+1}^N). \\
&\quad (A12)
\end{align*} \]

\[ \begin{align*}
&\quad \sum_{i=1}^{N} I(Y_{1,i}, Z_i; Y_{i}^{i-1}, Y_1^{i-1}|Y_{1,i+1}^N, Z_{i+1}^N, W_0, W_1) \\
&= \sum_{i=1}^{N} \sum_{j=1}^{i-1} I(Y_{1,i}, Z_i; Y_{1,j}, Y_i|Y_{1,i+1}^N, Z_{i+1}^N, W_0, W_1, Y_{j}^{j-1}, Y_1^{j-1}) \\
&= \sum_{j=1}^{N} \sum_{i=j}^{N} I(Y_{1,j}, Z_j; Y_{1,i}, Y_i|Y_{1,j+1}^N, Z_{j+1}^N, W_0, W_1, Y_{i}^{i-1}, Y_1^{i-1}) \\
&= \sum_{j=1}^{N} \sum_{i=j}^{N} I(Y_{1,j}, Z_j; Y_{1,i}, Y_i|Y_{1,j+1}^N, Z_{j+1}^N, W_0, W_1, Y_{i}^{i-1}, Y_1^{i-1}). \\
&\quad (A13)
\end{align*} \]

Finally, substituting (A9) and (A10) into (A8), and using the fact that (A11) holds, then we have

\[ \begin{align*}
&\quad \frac{1}{N} H(W_0, W_1, W_2) \\
&\leq \frac{1}{N} \sum_{i=1}^{N} \left( I(Y_{1,i}, Y_i; W_0, W_1, Y_{1,i+1}^N, Z_{i+1}^N|Y_{1}^{i-1}, Y_1^{i-1}) \\
&\quad + I(Y_{1,i}, Z_i; W_2|Y_{1,i+1}^N, Z_{i+1}^N, W_0, W_1, Y_{i}^{i-1}, Y_1^{i-1}) \right) + \frac{\delta(P_{e1}) + \delta(P_{e2})}{N}
\end{align*} \]
where (1) is from J is a random variable (uniformly distributed over \{1, 2, ..., N\}), and it is independent of \(Y^N, Y_1^N, Z^N, W_0, W_1 \) and \(W_2\). (2) is from J is uniformly distributed over \{1, 2, ..., N\} and \(P_{e1}, P_{e2} \leq \epsilon\), and (3) is from the definitions of the auxiliary random variables (see (A1)).

By using \(\epsilon \to 0\), \(R_0 + R_1 + R_2 = \lim_{N \to \infty} \frac{H(W_0, W_1, W_2)}{N}\) and (A14), \(R_0 + R_1 + R_2 \leq I(U, U_2, V_1; Y, Y_1|U_1) + I(V_2; Z, Y_1|U_1, U_2, V_1)\) is proved.

**Proof of** \(R_0 + R_1 + R_2 \leq I(U, U_1, V_1; Z, Y_1|U_2) + I(V_1; Y, Y_1|U_1, U_2, V_2)\)

The inequality \(R_0 + R_1 + R_2 \leq I(U, U_1, V_1; Z, Y_1|U_2) + I(V_1; Y, Y_1|U_1, U_2, V_2)\) is proved by letting \(H(W_0, W_1, W_2) = H(W_0, W_2) + H(W_1|W_0, W_2)\), and the remainder of the proof is analogous to the proof of \(R_0 + R_1 + R_2 \leq I(U, U_2, V_1; Y, Y_1|U_1) + I(V_2; Z, Y_1|U_1, U_2, V_1)\). Thus, we omit the proof here.

**Proof of** \(R_{e1} \leq I(V_1; Y|U, V_2) - I(V_1; Z|U, V_2)\)

The inequality \(R_{e1} \leq I(V_1; Y|U, V_2) - I(V_1; Z|U, V_2)\) is proved by the following (A15), (A16), (A17) and (A20).

First note that

\[
\begin{align*}
\frac{1}{N} H(W_1|Z^N) &= \frac{1}{N} (I(W_1; W_0, W_2|Z^N) + H(W_1|Z^N, W_0, W_2)) \\
&\leq \frac{1}{N} (H(W_1|Z^N, W_0, W_2) + \delta(\epsilon)) \\
&= \frac{1}{N} (H(W_1|W_0, W_2) - I(W_1; Z^N|W_0, W_2) + \delta(\epsilon)) \\
&= \frac{1}{N} (I(W_1; Y^N|W_0, W_2) + H(W_1|Y^N, W_0, W_2) - I(W_1; Z^N|W_0, W_2) + \delta(\epsilon)) \\
&\leq \frac{1}{N} (I(W_1; Y^N|W_0, W_2) - I(W_1; Z^N|W_0, W_2) + 2\delta(\epsilon)).
\end{align*}
\]

Then, the character \(I(W_1; Y^N|W_0, W_2)\) in (A15) is upper bounded by

\[
I(W_1; Y^N|W_0, W_2) = \sum_{i=1}^{N} I(W_1; Y_i|W_0, W_2, Y^{i-1})
\]
and these are from Csiszár’s equality \[20\].

Substituting (A16) and (A17) into (A15), and using the equalities (A18) and (A19), we have

\[
\sum_{i=1}^{N} \left( H(Y_i|W_0, W_2, Y^{i-1}) - H(Y_i|W_0, W_1, W_2, Y^{i-1}) \right)
+ H(Y_i|W_0, W_2, Y^{i-1}, W_1, Z_{i+1}^N) - H(Y_i|W_0, W_2, Y^{i-1}, W_1, Z_{i+1}^N)
= \sum_{i=1}^{N} \left( I(Y_i; W_1, Z_{i+1}^N|W_0, W_2, Y^{i-1}) - I(Y_i; Z_{i+1}^N|W_0, W_1, W_2, Y^{i-1}) \right)
= \sum_{i=1}^{N} \left( I(Y_i; Z_{i+1}^N|W_0, W_2, Y^{i-1}) + I(Y_i; W_1|W_0, W_2, Y^{i-1}, Z_{i+1}^N) \right)
- I(Y_i; Z_{i+1}^N|W_0, W_1, W_2, Y^{i-1})),
\]

(A16)

and the character \(I(W_1; Z^N|W_0, W_2)\) in (A15) is upper bounded by

\[
I(W_1; Z^N|W_0, W_2) = \sum_{i=1}^{N} I(W_1; Z_i|W_0, W_2, Z_{i+1}^N)
= \sum_{i=1}^{N} \left( H(Z_i|W_0, W_2, Z_{i+1}^N) - H(Z_i|W_0, W_1, W_2, Z_{i+1}^N) \right)
+ H(Z_i|W_0, W_2, Y^{i-1}, W_1, Z_{i+1}^N) - H(Z_i|W_0, W_2, Y^{i-1}, W_1, Z_{i+1}^N)
= \sum_{i=1}^{N} \left( I(Z_i; W_1, Y^{i-1}|W_0, W_2, Z_{i+1}^N) - I(Z_i; Y^{i-1}|W_0, W_1, W_2, Z_{i+1}^N) \right)
= \sum_{i=1}^{N} \left( I(Z_i; Y^{i-1}|W_0, W_2, Z_{i+1}^N) + I(Z_i; W_1|W_0, W_2, Y^{i-1}, Z_{i+1}^N) \right)
- I(Z_i; Y^{i-1}|W_0, W_1, W_2, Z_{i+1}^N)).
\]

(A17)

Note that

\[
\sum_{i=1}^{N} I(Y_i; Z_{i+1}^N|W_0, W_2, Y^{i-1}) = \sum_{i=1}^{N} I(Z_i; Y^{i-1}|W_0, W_2, Z_{i+1}^N),
\]

(A18)

and

\[
\sum_{i=1}^{N} I(Y_i; Z_{i+1}^N|W_0, W_1, W_2, Y^{i-1}) = \sum_{i=1}^{N} I(Z_i; Y^{i-1}|W_0, W_1, W_2, Z_{i+1}^N),
\]

(A19)

and these from Csiszár’s equality \[20\].

Substituting (A16) and (A17) into (A15), and using the equalities (A18) and (A19), we have
\[ I(Y; W|W_0, W_2, Y^{j-1}, Z_{j+1}, J) \]
\[ = I(Y; V_1 U, V_2) - I(Z; V_1 U|U, V_2) + \frac{2\delta(e)}{N}. \]  
(A20)

By using \( \epsilon \to 0 \), \( R_{e1} \leq \lim_{N \to \infty} \frac{H(W_1, Z_N)}{N} \) and (A20), \( R_{e1} \leq I(V_1; Y|U, V_2) - I(V_1; Z|U, V_2) \) is proved.

(Poof of \( R_{e1} \leq I(V_1; Y|U) - I(V_1; Z|U) \))

The inequality \( R_{e1} \leq I(V_1; Y|U) - I(V_1; Z|U) \) is proved by the following (A21), (A22), (A23) and (A26). First note that

\[ \frac{1}{N} H(W_1|Z_N) \]
\[ = \frac{1}{N} (I(W_1; W_0|Z_N) + H(W_1|Z_N, W_0)) \]
\[ \leq \frac{1}{N} (H(W_1|Z_N, W_0) + \delta(e)) \]
\[ = \frac{1}{N} (I(W_1; W_0) - I(W_1; Z_N|W_0) + \delta(e)) \]
\[ = \frac{1}{N} (I(W_1; Y_N|W_0) + H(W_1|Y_N, W_0) - I(W_1; Z_N|W_0) + \delta(e)) \]
\[ \leq \frac{1}{N} (I(W_1; Y_N|W_0) - I(W_1; Z_N|W_0) + 2\delta(e)). \]  
(A21)

Then, the character \( I(W_1; Y^i_N|W_0) \) in (A21) is upper bounded by

\[ I(W_1; Y^i_N|W_0) = \sum_{i=1}^{N} I(W_1; Y_i|W_0, Y^{i-1}) \]
\[ = \sum_{i=1}^{N} (H(Y_i|W_0, Y^{i-1}) - H(Y_i|W_0, W_1, Y^{i-1}) \]
\[ + H(Y_i|W_0, Y^{i-1}, W_1, Z_{i+1}^N) - H(Y_i|W_0, Y^{i-1}, W_1, Z_{i+1}^N)) \]
\[ = \sum_{i=1}^{N} (I(Y_i; W_1, Z_{i+1}^N|W_0, Y^{i-1}) - I(Y_i; Z_{i+1}^N|W_0, W_1, Y^{i-1})) \]
\[ = \sum_{i=1}^{N} (I(Y_i; W_1, Y^{i-1}) + I(Y_i; W_1|W_0, Y^{i-1}, Z_{i+1}^N) \]
\[ - I(Y_i; Z_{i+1}^N|W_0, W_1, Y^{i-1})), \]  
(A22)

and the character \( I(W_1; Z^i_N|W_0) \) in (A21) is upper bounded by

\[ I(W_1; Z^i_N|W_0) = \sum_{i=1}^{N} I(W_1; Z_i|W_0, Z_{i+1}^N) \]
\[ = \sum_{i=1}^{N} (H(Z_i|W_0, Z_{i+1}^N) - H(Z_i|W_0, W_1, Z_{i+1}^N) \]
\[ + H(Z_i|W_0, Y^{i-1}, W_1, Z_{i+1}^N) - H(Z_i|W_0, Y^{i-1}, W_1, Z_{i+1}^N)) \]
\[ = \sum_{i=1}^{N} (I(Z_i; W_1, Y^{i-1}|W_0, Z_{i+1}^N) - I(Z_i; Y^{i-1}|W_0, W_1, Z_{i+1}^N)) \]
Note that and auxiliary random variables. Thus, the proof of Theorem 1 is completed.

Substituting (A22) and (A23) into (A21), and using the equalities (A24) and (A25), we have

\[
\frac{1}{N} H(W_1|Z^N) \\
\leq \frac{1}{N} (I(W_1; Y^N|W_0) - I(W_1; Z^N|W_0) + 2\delta(\epsilon)) \\
= \frac{1}{N} \sum_{i=1}^{N} (I(Y_i; W_1|W_0, Y^{i-1}, Z^N_{i+1}) \\
- (Z_i; W_1|W_0, Y^{i-1}, Z^N_{i+1})) + \frac{2\delta(\epsilon)}{N} \\
= \frac{1}{N} \sum_{i=1}^{N} (I(Y_i; W_1|W_0, Y^{i-1}, Z^N_{i+1}, J = i) \\
- I(Z_i; W_1|W_0, Y^{i-1}, Z^N_{i+1}, J = i)) + \frac{2\delta(\epsilon)}{N} \\
= I(Y_j; W_1|W_0, Y^{j-1}, Z^N_{j+1}, J) \\
- I(Z_j; W_1|W_0, Y^{j-1}, Z^N_{j+1}, J) + \frac{2\delta(\epsilon)}{N} \\
= I(Y; V_1|U) - I(Z; V_1|U) + \frac{2\delta(\epsilon)}{N}. \tag{A26}
\]

By using $\epsilon \to 0$, $R_{e1} \leq \lim_{N \to \infty} \frac{H(W_1|Z^N)}{N}$ and (A26), $R_{e1} \leq I(V_1; Y|U) - I(V_1; Z|U)$ is proved.

**Proof of $R_{e2}$**

$R_{e2} \leq \min\{I(V_2; Z|U, V_1) - I(V_2; Y|U, V_1), I(V_2; Z|U) - I(V_2; Y|U)\}$

The proof of $R_{e2} \leq \min\{I(V_2; Z|U, V_1) - I(V_2; Y|U, V_1), I(V_2; Z|U) - I(V_2; Y|U)\}$ is analogous to the proof of $R_{e1} \leq \min\{I(V_1; Y|U, V_2) - I(V_1; Z|U, V_2), I(V_1; Y|U) - I(V_1; Z|U)\}$, and therefore, we omit the proof here.

The Markov chain $U \to (U_1, U_2, V_1, V_2) \to (X, X_1) \to (Y, Y_1, Z)$ is directly proved by the definitions of the auxiliary random variables. Thus, the proof of Theorem 1 is completed.

**Appendix B**

**Proof of Theorem 2**

Suppose $(R_0, R_1, R_2, R_{e1}, R_{e2}) \in \mathcal{R}^{(A1)}$, we will show that $(R_0, R_1, R_2, R_{e1}, R_{e2})$ is achievable, i.e., there exists encoder-decoder $(N, \Delta_1, \Delta_2, P_{e1}, P_{e2})$ such that (2.3) is satisfied. The existence of the encoder-decoder is
under the sufficient conditions that

\[ R_{e1} = I(V_1; Y|U, X_1) - I(V_1; V_2|U, X_1) - I(V_1; Z|U, X_1, V_2), \tag{A27} \]

and

\[ R_{e2} = I(V_2; Z|U, X_1) - I(V_1; V_2|U, X_1) - I(V_2; Y|U, X_1, V_1). \tag{A28} \]

The coding scheme combines the decode and forward (DF) strategy [35], random binning, superposition coding, block Markov coding and rate splitting techniques. The rate splitting technique is typically used in the interference channels to achieve a larger rate region as it enables interference cancellation at the receivers. Now we use it to split the confidential message \( W_1 \) into \( W_{10} \) and \( W_{11} \), and \( W_2 \) into \( W_{20} \) and \( W_{22} \), and the details are as follows.

Define the messages \( W_0, W_{10}, W_{11}, W_{20}, W_{22} \) taken values in the alphabets \( W_0, W_{10}, W_{11}, W_{20}, W_{22} \), respectively, where

\[
W_0 = \{1, 2, ..., 2^{NR_0}\},
\]
\[
W_{10} = \{1, 2, ..., 2^{NR_{10}}\},
\]
\[
W_{11} = \{1, 2, ..., 2^{NR_{11}}\},
\]
\[
W_{20} = \{1, 2, ..., 2^{NR_{20}}\},
\]
\[
W_{22} = \{1, 2, ..., 2^{NR_{22}}\},
\]

and \( R_{10} + R_{11} = R_1, R_{20} + R_{22} = R_2 \). Here note that the formulas (A27) and (A28) combined with the rate splitting and the fact that \( W_{10} \) and \( W_{20} \) are decoded by both receivers ensure that,

\[ R_{11} \geq R_{e1} = I(V_1; Y|U, X_1) - I(V_1; V_2|U, X_1) - I(V_1; Z|U, X_1, V_2), \tag{A29} \]

and

\[ R_{22} \geq R_{e2} = I(V_2; Z|U, X_1) - I(V_1; V_2|U, X_1) - I(V_2; Y|U, X_1, V_1). \tag{A30} \]

**Code Construction:** Fix the joint probability mass function \( P_{Y,Z,Y_1,X,X_1,V_1,V_2,U}(y, z, y_1, x, x_1, v_1, v_2, u) \). For arbitrary \( \epsilon > 0 \), define

\[
L_{11} = I(V_1; Y|U, X_1) - I(V_1; V_2|U, X_1) - I(V_1; Z|U, X_1, V_2), \tag{A31} \]
\[
L_{12} = I(V_1; Z|U, X_1, V_2), \tag{A32} \]
\[
L_{21} = I(V_2; Z|U, X_1) - I(V_1; V_2|U, X_1) - I(V_2; Y|U, X_1, V_1), \tag{A33} \]
\[
L_{22} = I(V_2; Y|U, X_1, V_1), \tag{A34} \]
\[
L_3 = I(V_1; V_2|U, X_1) - \epsilon. \tag{A35} \]

Note that

\[ L_{11} + L_{12} + L_3 = I(V_1; Y|U, X_1) - \epsilon, \tag{A36} \]
\[ L_{21} + L_{22} + L_3 = I(V_2; Z|U, X_1) - \epsilon. \]  
(A37)

- First, generate at random \(2^{NR_1}\) i.i.d. sequences at the relay node each drawn according to \(p_{X_1^N}(x_1^N) = \prod_{i=1}^{N} p_{X_1}(x_1, i)\), index them as \(x_1^N(a)\), \(a \in [1, 2^{NR_1}]\), where
  \[ R_1 = \min\{I(X_1; Y), I(X_1; Z)\} - \epsilon. \]  
(A38)

- Generate at random \(2^{N(R_{10}+R_{20}+R_0)}\) i.i.d. sequences \(u^N(b|a) \in [1, 2^{N(R_{10}+R_{20}+R_0)}]\) according to \(\prod_{i=1}^{N} p_{U|X_1}(u_i|x_1, i)\). In addition, partition \(2^{N(R_{10}+R_{20}+R_0)}\) i.i.d. sequences \(u^N\) into \(2^{NR_1}\) bins. These bins are denoted as \(\{S_1, S_2, \ldots, S_{2^{NR_1}}\}\), where \(S_i\) (\(1 \leq i \leq 2^{NR_1}\)) contains \(2^{N(R_{10}+R_{20}+R_0-R_1)}\) sequences about \(u^N\).

- For the transmitted sequences \(u^N\) and \(x_1^N\), generate \(2^{N(L_1+L_{12}+L_3)}\) i.i.d. sequences \(\nu^{N}(i', i'', i''')\), with \(i' \in \mathcal{I} = [1, 2^{NL_1}], i'' \in \mathcal{I}'' = [1, 2^{NL_{12}}]\) and \(i''' \in \mathcal{I}''' = [1, 2^{NL_3}]\), according to \(\prod_{i=1}^{N} p_{V_1|U,X_1}(v_1, i|x_1, i)\).

- Similarly, for the transmitted sequences \(u^N\) and \(x_1^N\), generate \(2^{N(L_{21}+L_{22}+L_3)}\) i.i.d. sequences \(\nu^{N}(j', j'', j''')\), with \(j' \in \mathcal{J} = [1, 2^{NL_{21}}], j'' \in \mathcal{J}'' = [1, 2^{NL_{22}}]\) and \(j''' \in \mathcal{J}''' = [1, 2^{NL_3}]\), according to \(\prod_{i=1}^{N} p_{V_2|U,X_1}(v_2, i|x_1, i)\).

- The \(x^N\) is generated according to a new discrete memoryless channel (DMC) with inputs \(x_1^N, u^N, v_1^N, v_2^N\) and output \(x^N\). The transition probability of this new DMC is \(p_{X^N|X_1^N,U^N,V_1^N,V_2^N}(x|x_1, u, v_1, v_2)\). The probability \(p_{X^N|X_1^N,U^N,V_1^N,V_2^N}(x|x_1^N, u^N, v_1^N, v_2^N)\) is calculated as follows.

\[ p_{X^N|X_1^N,U^N,V_1^N,V_2^N}(x|x_1^N, u^N, v_1^N, v_2^N) = \prod_{i=1}^{N} p_{X|X_1^N,U^N,V_1^N,V_2^N}(x_i|x_1, u_i, v_1, v_2_i). \]  
(A39)

Denote \(x^N\) by \(x^N(a, w_0, w_{10}, w_{20}, w_{11}, w_{22})\).

**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 [35], the loss induced by this scheme is negligible as the number of blocks \(n \to \infty\). For block \(i\) (\(1 \leq i \leq n\)), encoding proceeds as follows.

First, for convenience, define \(w_i^* = (w_0, w_{10}, w_{20})\), where \(w_0, w_{10}, w_{20}\) are the messages transmitted in the \(i\)-th block. The messages \(w_{11}\) and \(w_{22}\) transmitted in the \(i\)-th block are denoted by \(w_{11,i}\) and \(w_{22,i}\), respectively.

**Channel encoder**

1. The transmitter sends \((u^N(w_{0,1}^*|1), v_1^N(i_1', i_1'', i_1'''|1, w_{0,1}^*), v_2^N(j_1', j_1'', j_1'''|1, w_{0,1}^*))\) at the first block, \((u^N(w_{0,i}^*|a_{i-1}), v_1^N(i'_i, i''_i, i'''_i|a_{i-1}, w_{0,i}^*), v_2^N(j'_i, j''_i, j'''_i|a_{i-1}, w_{0,i}^*))\) from block 2 to \(n-1\), and \((u^N(1|a_{n-1}), v_1^N(1, 1, 1|a_{n-1}, 1), v_2^N(1, 1, 1|a_{n-1}, 1))\) at block \(n\). Here \(i'_i, i''_i, i'''_i, j'_i, j''_i, j'''_i\) are the indexes for block \(i\).

2. In the \(i\)-th block (\(1 \leq i \leq n\)), the indexes \(i'_i, i''_i, j'_i, j''_i\) are determined by the following methods.

   - If \(R_{11} \leq L_{11} + L_{12}\), define \(\mathcal{W}_{11} = \mathcal{I} \times \mathcal{K}_1\). Thus the index \(i'_i\) is determined by a given message \(w_{11,i}\).
     Evenly partition \(\mathcal{I}''\) into \(\mathcal{K}_1\) bins, and the index \(i''_i\) is drawn at random (with uniform distribution) from the bin \(k_1\).

     Analogously, if \(R_{22} \leq L_{21} + L_{22}\), define \(\mathcal{W}_{22} = \mathcal{J} \times \mathcal{K}_2\). Thus the index \(j'_i\) is determined by a given message \(w_{22,i}\).
     Evenly partition \(\mathcal{J}''\) into \(\mathcal{K}_2\) bins, and the index \(j''_i\) is drawn at random (with uniform distribution) from the bin \(k_2\).
If \( L_{11} + L_{12} \leq R_{11} \leq L_{11} + L_{12} + L_3 \), define \( \mathcal{W}_{11} = \mathcal{I}' \times \mathcal{I}'' \times \mathcal{K}_1 \). Thus the indexes \( i'_i \) and \( i''_i \) are determined by a given message \( w_{11,i} \). Evenly partition \( \mathcal{I}'' \) into \( \mathcal{K}_1 \) bins, and the codeword \( v^N_1(i'_i, i''_i, i''''_i | a_{i-1}, w^*_{0,i}) \) will be drawn from the bin \( k_1 \).

Analogously, if \( L_{21} + L_{22} \leq R_{22} \leq L_{21} + L_{22} + L_3 \), define \( \mathcal{W}_{22} = \mathcal{J}' \times \mathcal{J}'' \times \mathcal{K}_2 \). Thus the indexes \( j'_i \) and \( j''_i \) are determined by a given message \( w_{22,i} \). Evenly partition \( \mathcal{J}'' \) into \( \mathcal{K}_2 \) bins, and the codeword \( v^N_2(j'_i, j''_i, j''''_i | a_{i-1}, w^*_{0,i}) \) will be drawn from the bin \( k_2 \).

3) In the \( i \)-th block \((1 \leq i \leq n)\), the indexes \( i''''_i \) and \( j''''_i \) are determined as follows.

After the determination of \( i'_i, i''_i, j'_i \) and \( j''_i \), the transmitter tries to find a pair

\[
(v^N_1(i'_i, i''_i, i''''_i | a_{i-1}, w^*_{0,i}), v^N_2(j'_i, j''_i, j''''_i | a_{i-1}, w^*_{0,i}))
\]

such that \( (u^N(w^*_{0,i} | a_{i-1}), x^N_1(a_{i-1}), v^N_1(i'_i, i''_i, i''''_i | a_{i-1}, w^*_{0,i}), v^N_2(j'_i, j''_i, j''''_i | a_{i-1}, w^*_{0,i})) \) are jointly typical. If there are more than one such pair, randomly choose one; if there is no such pair, an error is declared. Thus, all the indexes of \( v^N_1 \) and \( v^N_2 \) (in block \( i \)) are determined. One can show that such a pair exists with high probability for sufficiently large \( N \) if (see [40])

\[
I(V_1; Y | U, X_1) - \epsilon - R_{11} + I(V_2; Z | U, X_1) - \epsilon - R_{22} \geq I(V_1; V_2 | U, X_1). \tag{A40}
\]

4) In the \( i \)-th block \((1 \leq i \leq n)\), the transmitter finally sends \( x^N_1(a_{i-1}, w_{0,i}, w_{10,i}, w_{20,i}, w_{11,i}, w_{22,i}) \).

**Relay encoder**

The relay sends \( x^N_1(1) \) at the first block, and \( x^N_1(\hat{a}_{i-1}) \) from block 2 to \( n \).

**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 \( a_{i-1} \) (denoted as \( \hat{a}_{i-1} \)), which was sent at block \( i-1 \), and will declare that it receives \( \hat{a}_i \), if this is the only triple such that \( (u^N(w^*_{0,i} | a_{i-1}), x^N_1(\hat{a}_{i-1}), y^N(i)) \) are jointly typical. Here note that \( y^N(i) \) indicates the output sequence \( y^N \) in block \( i \), and \( \hat{a}_i \) is the index of the bin that \( w^*_{0,i} \) belongs to. Based on the AEP, the probability \( Pr\{\hat{a}_i = a_i\} \) goes to 1 if

\[
R_0 + R_{10} + R_{20} \leq I(U; Y_1 | X_1). \tag{A41}
\]

2) (At receiver 1) Receiver 1 decodes from the last block, i.e., block \( n \). Suppose that at the end of block \( n-1 \), the relay decodes successfully, then receiver 1 will declare that \( \hat{a}_{n-1} \) is received if \( (x^N_1(\hat{a}_{n-1}), y^N(n)) \) jointly typical. By using (A38) and the AEP, it is easy to see that the probability \( Pr\{\hat{a}_{n-1} = a_{n-1}\} \) goes to 1. After getting \( \hat{a}_{n-1} \), receiver 1 can get an estimation of \( a_i \ (1 \leq i \leq n-2) \) in a similar way.

Having \( \hat{a}_{i-1} \), receiver 1 can get the estimation of the message \( w^*_{0,i} = (w_{0,i}, w_{10,i}, w_{20,i}) \) by finding a unique triple such that \( (u^N(w^*_{0,i} | \hat{a}_{i-1}), x^N_1(\hat{a}_{i-1}), y^N(i)) \) are jointly typical. Based on the AEP, the probability \( Pr\{\hat{w}^*_0 = w^*_{0,i}\} \) goes to 1 if

\[
R_0 + R_{10} + R_{20} - R_\epsilon \leq I(U; Y | X_1). \tag{A42}
\]

After decoding \( \hat{w}^*_0 \), receiver 1 tries to find a quadruple such that

\[
(v^N_1(i'_i, i''_i, i''''_i | \hat{a}_{i-1}, \hat{w}^*_0), u^N(\hat{w}^*_0 | \hat{a}_{i-1}), x^N_1(\hat{a}_{i-1}), y^N(i)) \]

are jointly typical. Based on the AEP, the probability
\( \Pr \{ \bar{w}_{11,i} = w_{11,i} \} \) goes to 1 if
\[
R_{11} \leq I(V_1; Y|U, X_1).
\] (A43)

If such \( v^N_{i_1, i_2, i_3, \bar{a}_{i-1}, \bar{w}_{0, i}} \) exists and is unique, set \( i^*_1 = i^*_2 = i^*_3 \) and \( \bar{i}^*_1 = \bar{i}^*_2 \); otherwise, declare an error.

From the values of \( \bar{v}^N_1, \bar{v}^N_2, \bar{v}^N_3, \) and the above encoding schemes, receiver 1 can calculate the message \( \bar{w}_{11,i} \).

(At receiver 2) The decoding scheme for receiver 2 is symmetric, and it is omitted here. Analogously, we have
\[
R_0 + R_{10} + R_{20} - R_c \leq I(U; Z|X_1),
\] (A44)

and
\[
R_{22} \leq I(V_2; Z|U, X_1).
\] (A45)

The following Table I shows the transmitted codewords in the first three blocks.

| Block | 1 | 2 | 3 |
|-------|---------------|---------------|---------------|
| \( x^N_1 \) | \( x^N_1(a_1) \) | \( x^N_1(\bar{a}_2) \) |
| \( u^N \) | \( u^N(w^0_{a,1}) \) | \( u^N(w^0_{a,2}|a_1) \) | \( u^N(w^0_{a,3}|a_2) \) |
| \( v^N_1 \) | \( v^N_1(i^*_1, i^*_2, i^*_3|1, w^0_{a,1}) \) | \( v^N_1(i^*_1, i^*_2, i^*_3|a_1, w^0_{a,2}) \) | \( v^N_1(i^*_1, i^*_2, i^*_3|a_2, w^0_{a,3}) \) |
| \( v^N_2 \) | \( v^N_2(j^*_1, j^*_2, j^*_3|1, w^0_{a,1}) \) | \( v^N_2(j^*_1, j^*_2, j^*_3|a_1, w^0_{a,2}) \) | \( v^N_2(j^*_1, j^*_2, j^*_3|a_2, w^0_{a,3}) \) |
| \( y^N_1 \) | \( \bar{w}^0_{0,1,1|a_1} \) | \( \bar{w}^0_{0,2,1|a_2} \) | \( \bar{w}^0_{0,3,1|a_3} \) |
| \( y^N_2 \) | \( 1 \) | \( \bar{a}_1, \bar{w}^0_{0,1,1}, \bar{w}^0_{0,2,1}, \bar{w}^0_{0,3,1} \) | \( \bar{a}_2, \bar{w}^0_{0,2,1}, \bar{w}^0_{0,3,1} \) |
| \( z^N \) | \( 1 \) | \( \bar{a}_1, \bar{w}^0_{0,1,2}, \bar{w}^0_{0,2,2} \) | \( \bar{a}_2, \bar{w}^0_{0,2,2}, \bar{w}^0_{0,3,2} \) |

**TABLE I: Decode and forward strategy for the model of Figure 1**

By using (A38), (A40), (A41), (A42), (A43), (A44), and (A45), it is easy to check that \( P_{e1} \leq \epsilon \) and \( P_{e2} \leq \epsilon \). Moreover, applying Fourier-Motzkin elimination on (A38), (A40), (A41), (A42), (A43), (A44), and (A45) with the definitions \( R_1 = R_{10} + R_{11} \) and \( R_2 = R_{20} + R_{22} \), we get
\[
R_0 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\},
\]
\[
R_0 + R_1 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\} + I(V_1; Y|U, X_1),
\]
\[
R_0 + R_2 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\} + I(V_2; Z|U, X_1),
\]
\[
R_0 + R_1 + R_2 \leq \min\{I(U; Y_1|X_1), I(U, X_1; Y), I(U, X_1; Z)\} + I(V_1; Y|U, X_1) + I(V_2; Z|U, X_1) - I(V_1; V_2|U, X_1).
\]

Note that the above inequalities are the same as those in Theorem 2.
Equivocation Analysis: Now, it remains to prove \( \lim_{N \to \infty} \Delta_1 \geq R_{\epsilon_1} = I(V_1; Y | U, X_1) - I(V_1; V_2 | U, X_1) - I(V_1; Z | U, X_1, V_2) \). The bound \( \lim_{N \to \infty} \Delta_2 \geq R_{\epsilon_2} = I(V_2; Z | U, X_1) - I(V_1; V_2 | U, X_1) - I(V_2; Y | U, X_1, V_1) \) follows by symmetry.

\[
H(W_1 | Z^N) \geq H(W_1 | Z^N, V_2^N, U^N, X_1^N) \\
= H(W_{10}, W_{11} | Z^N, V_2^N, U^N, X_1^N) \\
= H(W_{11} | Z^N, V_2^N, U^N, X_1^N) \\
\geq H(W_{11}, Z^N | V_2^N, U^N, X_1^N) - H(Z^N | V_2^N, U^N, X_1^N) \\
\geq H(V_1^N | W_{11}, Z^N, V_2^N, U^N, X_1^N) - H(Z^N | V_2^N, U^N, X_1^N)
\]

where (a) follows from the fact that given \( U^N, W_{10} \) is uniquely determined.

Consider the first term in (A46), the codeword generation and [24, Lemma 3] ensure that

\[
H(V_1^N | U^N, X_1^N) \geq \log 2^{N(L_{11} + L_{12} + L_3)} - \delta = N(I(V_1; Y | U, X_1) - \epsilon) - \delta,
\]

where \( \delta \) is small for sufficiently large \( N \).

For the second and third terms in (A46), using the same approach as that in [20, Lemma 3], we get

\[
I(V_1^N; V_2^N | U^N, X_1^N) \leq N(I(V_1; V_2 | U, X_1) + \epsilon'),
\]

and

\[
I(Z^N; V_1^N | V_2^N, U^N, X_1^N) \leq N(I(V_1; Z | U, X_1, V_2) + \epsilon''),
\]

where \( \epsilon', \epsilon'' \to 0 \) as \( N \to \infty \).

Now, we consider the last term of (A46). For the case that \( R_{11} \leq L_{11} + L_{12} \), given \( U^N, X_1^N, V_2^N \) and \( W_{11} \), the total number of possible codewords of \( V_1^N \) is

\[
N_1 \leq 2^{N(L_{11} + L_{12})} = 2^{N I(V_1; Z | U, X_1, V_2)}.
\]

By using the Fano’s inequality and [A50], we have

\[
H(V_1^N | W_{11}, Z^N, V_2^N, U^N, X_1^N) \leq N \epsilon''',
\]

where \( \epsilon''' \to 0 \).
For the case that $L_{11} + L_{12} \leq R_{11} \leq L_{11} + L_{12} + L_3$, given $U^N, X^N, V_2^N$ and $W_{11}, V_1^N$ is totally determined, and therefore

$$H(V_1^N|W_{11}, Z^N, V_2^N, U^N, X^N) = 0.$$  \tag{A52}

Substituting (A47), (A48), (A49) and (A51) (or (A52)) into (A46), and using the definition (2.3), we have $\lim_{N \to \infty} \Delta_1 \geq R_{c1} = I(V_1^N|Y^N, X_1^N) - I(V_1^N|Y^N, Z^N, V_2^N).$ This completes the proof of Theorem 2.

**APPENDIX C**

**Proof of Theorem 3**

We consider the proof of Theorem 3 for the case $I(X_1; Y) \geq I(X_1; Z|U, V_2)$, and the proof for $I(X_1; Z) \geq I(X_1; Y|U, V_1)$ follows by symmetry.

In Theorem 3, the relay node does not attempt to decode the messages but sends codewords that are independent of the transmitter’s messages, and these codewords aid in confusing the receivers. Since the channel between the relay and receiver 1 is better than the channel between the relay and receiver 2 ($I(X_1; Y) \geq I(X_1; Z|U, V_2) \geq I(X_1; Z)$), we allow receiver 1 to decode the relay codeword, and receiver 2 can not decode it. Therefore, in this case, the relay codeword can be viewed as a noise signal to confuse receiver 2.

Now we will prove that the quintuple $(R_0, R_1, R_2, R_{c1}, R_{c2}) \in R^{(A2)}$ with the conditions

$$R_{c1} = \min\{I(X_1; Z|U, V_1, V_2), I(X_1; Y)\} + I(V_1^N|Y^N, X_1^N) - I(V_1^N|V_2^N) - I(V_1^N|Y^N, Z^N, V_2^N),$$  \tag{A53}

and

$$R_{c2} = I(V_2^N|Z^N) - I(V_1^N|V_2^N) - I(V_2^N|Y^N, X_1^N),$$  \tag{A54}

is achievable.

Similar to the proof of Theorem 2, we split the confidential message $W_1$ into $W_{10}$ and $W_{11}$, and $W_2$ into $W_{20}$ and $W_{22}$, and the definitions of these messages are the same as those in Appendix B. Here note that the formulas (A53) and (A54) combined with the rate splitting and the fact that $W_{10}$ and $W_{20}$ are decoded by both receivers ensure that,

$$R_{11} \geq R_{c1} = \min\{I(X_1; Z|U, V_1, V_2), I(X_1; Y)\} + I(V_1^N|Y^N, X_1^N) - I(V_1^N|V_2^N) - I(V_1^N|Z^N, V_2^N),$$  \tag{A55}

and

$$R_{22} \geq R_{c2} = I(V_2^N|Z^N) - I(V_1^N|V_2^N) - I(V_2^N|Y^N, X_1^N).$$  \tag{A56}

**Code Construction:** Fix the joint probability mass function

$$P_{Y, Z, Y_1, X_1, V_1, V_2, U}(y, z, y_1, x, x_1, v_1, v_2, u) = P_{Y, Z, Y_1}|X_1, V_1, V_2}(y, z, y_1|x_1)P_{X_1|U, V_1, V_2}(x|u, v_1, v_2)P_{U, V_1, V_2, U}(u, v_1, v_2)P_{X_1}(x_1).$$

For arbitrary $\epsilon > 0$, define

$$L_{11} = I(V_1^N|Y^N, X_1^N) - I(V_1^N|V_2^N) - I(V_1^N|Z^N, V_2^N).$$  \tag{A57}
\[ L_{12} = I(V_1; Z|U, V_2), \] *(A58)\]
\[ L_{21} = I(V_2; Z|U) - I(V_1; V_2|U) - I(V_2; Y|U, X_1, V_1), \] *(A59)\]
\[ L_{22} = I(V_2; Y|U, X_1, V_1), \] *(A60)\]
\[ L_3 = I(V_1; V_2|U) - \epsilon. \] *(A61)\]

Note that
\[ L_{11} + L_{12} + L_3 = I(V_1; Y|U, X_1) - \epsilon, \] *(A62)\]
\[ L_{21} + L_{22} + L_3 = I(V_2; Z|U) - \epsilon, \] *(A63)\]
\[ L_{11} \geq R_{e1}. \] *(A64)\]

- First, generate at random \(2^{N R_r}\) i.i.d. sequences at the relay node each drawn according to \(p_{X_1}^N(x_1^N) = \prod_{i=1}^{N} p_{X_1}(x_{1,i})\), index them as \(x_1^N(a), a \in [1, 2^{N R_r}]\), where
\[ R_r = \min\{I(X_1; Z|U, V_1, V_2), I(X_1; Y)\} - \epsilon, \] *(A65)\]
and \(\epsilon \to 0^+\). Note that \(I(X_1; Z|U, V_2) \leq I(X_1; Z|U, V_1, V_2)\) and \(I(X_1; Z|U, V_2) \leq I(X_1; Y)\), and thus
\[ R_r \geq I(X_1; Z|U, V_2) - \epsilon, \] *(A66)\]
and
\[ R_r \leq I(X_1; Z|U, V_1, V_2) - \epsilon. \] *(A67)\]

- Generate at random \(2^{N(R_{10}+R_{20}+R_0)}\) i.i.d. sequences \(u^N(b) \in [1, 2^{N(R_{10}+R_{20}+R_0)}]\) according to \(\prod_{i=1}^{N} p_{U}(u_i)\).

- For the transmitted sequence \(u^N(b)\), generate \(2^{N(L_{11}+L_{12}+L_2)}\) i.i.d. sequences \(v_1^N(i', i'', i''')\), with \(i' \in I' = [1, 2^{N L_{11}}]\), \(i'' \in I'' = [1, 2^{N L_{12}}]\) and \(i''' \in I''' = [1, 2^{N L_2}]\), according to \(\prod_{i=1}^{N} p_{V_1|U}(v_{1,i}|u_i)\).

- Similarly, for the transmitted sequences \(u^N\) and \(x_1^N\), generate \(2^{N(L_{21}+L_{22}+L_3)}\) i.i.d. sequences \(v_2^N(j', j'', j''')\), with \(j' \in J' = [1, 2^{N L_{21}}]\), \(j'' \in J'' = [1, 2^{N L_{22}}]\) and \(j''' \in J''' = [1, 2^{N L_3}]\), according to \(\prod_{i=1}^{N} p_{V_2|U}(v_{2,i}|u_i)\).

- The \(x^N\) is generated according to a new discrete memoryless channel (DMC) with inputs \(u^N, v_1^N, v_2^N\) and output \(x^N\). The transition probability of this new DMC is \(p_{X|U,V_1,V_2}(x|u, v_1, v_2)\). The probability \(p_{X^N|U^N,V_1^N,V_2^N}(x^N|u^N, v_1^N, v_2^N)\) is calculated as follows.
\[ p_{X^N|U^N,V_1^N,V_2^N}(x^N|u^N, v_1^N, v_2^N) = \prod_{i=1}^{N} p_{X|U,V_1,V_2}(x_i|u_i, v_{1,i}, v_{2,i}). \] *(A68)\]

Denote \(x^N\) by \(x^N(w_0, w_{10}, w_{20}, w_{11}, w_{22})\).

**Encoding:** Similar to the definitions in Appendix B, define \(w_{0,i}^* = (w_{0,i}, w_{10,i}, w_{20,i})\), where \(w_{0,i}, w_{10,i}\) and \(w_{20,i}\) are the messages transmitted in the \(i\)-th block. The messages \(w_{11}\) and \(w_{22}\) transmitted in the \(i\)-th block are denoted by \(w_{11,i}\) and \(w_{22,i}\), respectively.

- (Channel encoder)
1) The transmitter sends \((u^N(\omega^i_{0,1}), v_1^N(i'_i, i''_i, i'''_i | \omega^i_{0,1}), v_2^N(j'_i, j''_i, j'''_i | \omega^i_{0,1}))\) for the \(i\)-th block (\(1 \leq i \leq n\)). Here \(i'_i, i''_i, i'''_i, j'_i, j''_i, j'''_i\) are the indexes for block \(i\).

2) The indexes \(i'_i, i''_i, j'_i\) and \(j''_i\) are determined by the following methods.
   - If \(R_{11} \leq L_{11}\), evenly partition \(I\) into \(\mathcal{W}_{11}\) bins, and the index \(i'_i\) is drawn at random (with uniform distribution) from the bin \(w_{11}\). The index \(i''_i\) is drawn at random (with uniform distribution) from \(I''\).
     
   Note that \(R_{22}\) always satisfies \(R_{22} \geq L_{22}\).
   - If \(L_{11} \leq R_{11} \leq L_{11} + L_{12}\), define \(\mathcal{W}_{11} = I' \times K_1\). Thus the index \(i'_i\) is determined by a given message \(w_{11,i}\). Evenly partition \(I''\) into \(K_1\) bins, and the index \(i''_i\) is drawn at random (with uniform distribution) from the bin \(k_1\).
     
   Analogously, if \(R_{22} \leq L_{21} + L_{22}\), define \(\mathcal{W}_{22} = J' \times K_2\). Thus the index \(j'_i\) is determined by a given message \(w_{22,i}\). Evenly partition \(J''\) into \(K_2\) bins, and the index \(j''_i\) is drawn at random (with uniform distribution) from the bin \(k_2\).
   - If \(L_{11} + L_{12} \leq R_{11} \leq L_{11} + L_{12} + L_3\), define \(\mathcal{W}_{11} = I' \times I'' \times K_1\). Thus the indexes \(i'_i, i''_i\) are determined by a given message \(w_{11,i}\). Evenly partition \(I''\) into \(K_1\) bins, and the codeword \(v_1^N((i'_i, i''_i, i'''_i | \omega^i_{0,1}))\) will be drawn from the bin \(k_1\).
     
   Analogously, if \(L_{21} + L_{22} \leq R_{22} \leq L_{21} + L_{22} + L_3\), define \(\mathcal{W}_{22} = J' \times J'' \times K_2\). Thus the indexes \(j'_i, j''_i\) are determined by a given message \(w_{22,i}\). Evenly partition \(J''\) into \(K_2\) bins, and the codeword \(v_2^N((j'_i, j''_i, j'''_i | \omega^i_{0,1}))\) will be drawn from the bin \(k_2\).

3) The indexes \(i''_i\) and \(j''_i\) are determined as follows.
   After the determination of \(i'_i, i''_i, j'_i\) and \(j''_i\), the transmitter tries to find a pair \((v_1^N(i'_i, i''_i, i'''_i | \omega^i_{0,1}), v_2^N(j'_i, j''_i, j'''_i | \omega^i_{0,1}))\) such that \((u^N(\omega^i_{0,1}), v_1^N(i'_i, i''_i, i'''_i | \omega^i_{0,1}), v_2^N(j'_i, j''_i, j'''_i | \omega^i_{0,1}))\) are jointly typical. If there are more than one such pair, randomly choose one; if there is no such pair, an error is declared. Thus, the indexes of \(v_1^N\) and \(v_2^N\) (in block \(i\)) are determined. One can show that such a pair exists with high probability for sufficiently large \(N\) if (see [40])

\[
I(V_1; Y|U, X_1) - \epsilon - R_{11} + I(V_2; Z|U) - \epsilon - R_{22} \geq I(V_1; V_2|U).
\]

(A69)

4) The transmitter finally sends \(x^N(\omega_{0,i}, \omega_{10,i}, \omega_{20,i}, \omega_{11,i}, \omega_{22,i})\).

- **(Relay encoder)**
  In the \(i\)-th block, the relay uniformly picks a codeword \(x^N_i(a_i)\) from \(a_i \in [1, 2^{NR_t}]\), and sends \(x^N_i(a_i)\).

**Decoding:** Decoding proceeds as follows.

(At receiver 1) At the end of block \(i\), receiver 1 will declare that \(a_i\) is received if \((x^N_i(\hat{a}_i), y^N(\hat{i}))\) are jointly typical. By using [A65] and the AEP, it is easy to see that the probability \(Pr\{\hat{a}_i = a_i\}\) goes to 1.

Having \(\hat{a}_i\), receiver 1 can get the estimation of the message \(\omega^i_{0,i} = (\omega_{0,i}, \omega_{10,i}, \omega_{20,i})\) by finding a unique triple such that \((u^N(\omega^i_{0,i}), x^N_i(\hat{a}_i), y^N(\hat{i}))\) are jointly typical. Based on the AEP, the probability \(Pr\{\hat{w}^i_{0,i} = \omega^i_{0,i}\}\) goes to 1 if

\[
R_0 + R_{10} + R_{20} \leq I(U; Y|X_1).
\]

(A70)
After decoding \( \hat{w}_{0,i} \), receiver 1 tries to find a quadruple such that
\[
(v^0_i (i_1', i_2, i_3' | \hat{w}_{0,i}^0), u^N (\hat{w}_{0,i}^0), x^N (\hat{a}_1), y^N (i))
\] are jointly typical. Based on the AEP, the probability \( \text{Pr}\{\hat{w}_{1,i} = w_{1,i}\} \) goes to 1 if
\[
R_{11} \leq I(V_1;Y|U,X_1). \tag{A71}
\]
If such \( v^N_i (i_1', i_2', i_3' | \hat{w}_{0,i}^0) \) exists and is unique, set \( i_1' = i_1', i_2' = i_2', i_3' = i_3' \); otherwise, declare an error. From the values of \( i_1', i_2', i_3' \), and the above encoding schemes, receiver 1 can calculate the message \( \hat{w}_{1,i} \).

(At receiver 2) The decoding scheme for receiver 2 is as follows.

Receiver 2 gets the estimation of the message \( w_{0,i}^0 \) by finding a unique pair such that \( (u^N (\hat{w}_{0,i}^0), z^N (i)) \) are jointly typical. Based on the AEP, the probability \( \text{Pr}\{\hat{w}_{0,i} = w_{0,i}^0\} \) goes to 1 if
\[
R_0 + R_{10} + R_{20} \leq I(U;Z). \tag{A72}
\]
After decoding \( \hat{w}_{0,i} \), receiver 2 tries to find a triple such that \( (v^N_2 (j_1', j_2, j_3' | \hat{w}_{0,i}^0), u^N (\hat{w}_{0,i}^0), z^N (i)) \) are jointly typical. Based on the AEP, the probability \( \text{Pr}\{\hat{w}_{2,i} = w_{2,i}\} \) goes to 1 if
\[
R_{22} \leq I(V_2;Z|U). \tag{A73}
\]
If such \( v^N_2 (j_1', j_2, j_3' | \hat{w}_{0,i}^0) \) exists and is unique, set \( j_1' = j_1', j_2 = j_2', j_3' = j_3' \); otherwise, declare an error. From the values of \( j_1', j_2, j_3' \), and the above encoding schemes, receiver 2 can calculate the message \( \hat{w}_{2,i} \).

By using (A65), (A69), (A70), (A72) and (A73), it is easy to check that \( P_{e1} \leq \epsilon \) and \( P_{e2} \leq \epsilon \). Moreover, applying Fourier-Motzkin elimination on (A65), (A69), (A70), (A71), (A72) and (A73) with the definitions \( R_1 = R_{10} + R_{11} \) and \( R_2 = R_{20} + R_{22} \), we get
\[
R_0 \leq \min\{I(U;Y|X_1), I(U;Z)\},
\]
\[
R_0 + R_1 \leq \min\{I(U;Y|X_1), I(U;Z)\} + I(V_1;Y|U,X_1),
\]
\[
R_0 + R_2 \leq \min\{I(U;Y|X_1), I(U;Z)\} + I(V_2;Z|U),
\]
\[
R_0 + R_1 + R_2 \leq \min\{I(U;Y|X_1), I(U;Z)\} + I(V_1;Y|U,X_1) + I(V_2;Z|U) - I(V_1;V_2|U).
\]
Note that the above inequalities are the same as those in Theorem 3.

**Equivocation Analysis:** Now, it remains to prove \( \lim_{N \to \infty} \Delta_1 \geq R_{e1} = \min\{I(X_1;Z|U,V_1,V_2),
\max\{I(X_1;Y), I(X_1;Z|U,V_2)\}\} + I(V_1;Y|U,X_1) - I(V_1;V_2|U) - I(X_1,V_1;Z|U,V_2) \) and \( \lim_{N \to \infty} \Delta_2 \geq R_{e2} = I(V_2;Z|U) - I(V_1;V_2|U) - I(V_2;Y|U,X_1,V_1). \)

**Proof of** \( \lim_{N \to \infty} \Delta_1 \geq R_{e1} = \min\{I(X_1;Z|U,V_1,V_2), I(X_1;Y) + I(V_1;Y|U,X_1) - I(V_1;V_2|U) - I(X_1,V_1;Z|U,V_2): \)
\[ H(W_1|Z^N) \geq H(W_1|Z^N, V_2^N, U^N) \]
\[ = H(W_{10}, W_{11}|Z^N, V_2^N, U^N) \]
\[ \overset{(a)}{=} H(W_{11}|Z^N, V_2^N, U^N) \]
\[ = H(W_{11}, Z^N|V_2^N, U^N) - H(Z^N|V_2^N, U^N) \]
\[ = H(W_{11}, Z^N, V_1^N, X_1^N|V_2^N, U^N) - H(V_1^N, X_1^N|W_{11}, Z^N, V_2^N, U^N) - H(Z^N|V_2^N, U^N) \]
\[ \geq H(Z^N, V_1^N, X_1^N|V_2^N, U^N) - H(V_1^N, X_1^N|W_{11}, Z^N, V_2^N, U^N) - H(Z^N|V_2^N, U^N) \]
\[ = H(V_1^N, X_1^N|V_2^N, U^N) + H(Z^N|V_1^N, V_2^N, U^N, X_1^N) - H(V_1^N, X_1^N|W_{11}, Z^N, V_2^N, U^N) \]
\[ \quad - H(Z^N|V_2^N, U^N) \]
\[ \overset{(b)}{=} H(X_1^N) + H(V_1^N|V_2^N, U^N) + H(Z^N|V_1^N, V_2^N, U^N, X_1^N) - H(V_1^N, X_1^N|W_{11}, Z^N, V_2^N, U^N) \]
\[ \quad - H(Z^N|V_2^N, U^N) \]
\[ = H(X_1^N) + H(V_1^N|U^N) - I(V_1^N; V_2^N|U^N) + H(Z^N|V_1^N, V_2^N, U^N, X_1^N) \]
\[ \quad - H(V_1^N, X_1^N|W_{11}, Z^N, V_2^N, U^N) - H(Z^N|V_2^N, U^N) \]
\[ = H(X_1^N) + H(V_1^N|U^N) - I(V_1^N; V_2^N|U^N) - I(Z^N; X_1^N, V_1^N|V_2^N, U^N) \]
\[ \quad - H(V_1^N, X_1^N|W_{11}, Z^N, V_2^N, U^N), \]  
(A74)

where (a) follows from the fact that given \( U^N, W_{10} \) is uniquely determined, and (b) is from that \( X_1^N \) is independent of \( V_1^N, V_2^N \) and \( U^N \).

Consider the first term in (A74), the codeword generation and [24] Lemma 3] ensure that
\[ H(X_1^N) \geq NR_r - \delta = N(\min\{I(X_1; Z|U, V_1, V_2), I(X_1; Y)\} - \epsilon) - \delta, \]  
(A75)

where \( \delta \) is small for sufficiently large \( N \).

For the second term in (A74), similarly we have
\[ H(V_1^N|U^N) \geq \log 2^{N(L_{11}+L_{12}+L_3)} - \delta_1 = N(I(V_1; Y|U, X_1) - \epsilon) - \delta_1, \]  
(A76)

where \( \delta_1 \) is small for sufficiently large \( N \).

For the third and fourth terms in (A74), using the same approach as that in [20] Lemma 3], we get
\[ I(V_1^N; V_2^N|U^N) \leq N(I(V_1; V_2|U) + \epsilon'), \]  
(A77)

and
\[ I(Z^N; X_1^N, V_1^N|V_2^N, U^N) \leq N(I(X_1, V_1; Z|U, V_2) + \epsilon''), \]  
(A78)

where \( \epsilon', \epsilon'' \to 0 \) as \( N \to \infty \).

Now, we consider the last term of (A74). Given \( W_{11} \), receiver 2 can do joint decoding.
• For the case that $R_{11} \leq L_{11}$, given $U^N, V_2^N, W_{11}$ and $\epsilon'' \to 0^+$,

$$H(V_1^N, X_1^N | W_{11}, Z^N, V_2^N, U^N) \leq N \epsilon''',$$  \hspace{1cm} (A79)

is guaranteed if $R_r \leq I(X_1; Z | V_1, V_2, U) - \epsilon$ and $R_r \geq I(X_1; Z | U, V_2) - \epsilon$ ($\epsilon \to 0^+$), and this is from the properties of AEP (similar argument is used in the proof of Theorem 3 in \cite{29}). By using (A66) and (A67), (A79) is obtained.

• For the case that $L_{11} \leq R_{11} \leq L_{11} + L_{12}$, given $U^N, V_2^N$ and $W_{11}$, the total number of possible codewords of $V_1^N$ is

$$N_1 \leq 2^{N L_{12}} = 2^{N I(V_1; Z | U, V_2)}.$$  \hspace{1cm} (A80)

By using the Fano’s inequality and (A80), we have

$$H(V_1^N | W_{11}, Z^N, V_2^N, U^N) \leq N \epsilon''',$$  \hspace{1cm} (A81)

where $\epsilon'' \to 0$.

Given $U^N, V_1^N, V_2^N$ and $W_{11}$, the total number of possible codewords of $X_1^N$ is

$$N_2 \leq 2^{N R_r} = 2^{N (\min(I(X_1; Y), I(X_1; Z | V_1, V_2, U)) - \epsilon)}.$$  \hspace{1cm} (A82)

By using the Fano’s inequality and (A82), we have

$$H(X_1^N | W_{11}, Z^N, V_1^N, V_2^N, U^N) \leq N \epsilon''',$$  \hspace{1cm} (A83)

where $\epsilon'' \to 0$.

By using (A81) and (A83),

$$\frac{1}{N} H(V_1^N, X_1^N | W_{11}, Z^N, V_2^N, U^N) \leq \epsilon \to 0,$$  \hspace{1cm} (A84)

is guaranteed.

• For the case that $L_{11} + L_{12} \leq R_{11} \leq L_{11} + L_{12} + L_3$, given $U^N, V_2^N$ and $W_{11}$, $V_1^N$ is totally determined, and therefore

$$H(V_1^N | W_{11}, Z^N, V_2^N, U^N) = 0.$$  \hspace{1cm} (A85)

Similarly, note that $R_r = \min \{ I(X_1; Z | U, V_1, V_2), I(X_1; Y) \} - \epsilon$, by using the Fano’s inequality, we have (A83). Thus

$$\frac{1}{N} H(V_1^N, X_1^N | W_{11}, Z^N, V_2^N, U^N) \leq \epsilon \to 0$$  \hspace{1cm} (A86)

is guaranteed.

Substituting (A75), (A76), (A77), (A78) and (A79) (or (A84), (A86)) into (A74), and using the definition \cite{2,3}, we have $\lim_{N \to \infty} \Delta_1 \geq R_{e1} = \min \{ I(X_1; Z | U, V_1, V_2), I(X_1; Y) \} + I(V_1; Y | U, X_1) - I(V_1; V_2 | U) - I(X_1, V_1; Z | U, V_2)$.

**Proof of** $\lim_{N \to \infty} \Delta_2 \geq R_{e2} = I(V_2; Z | U) - I(V_1; V_2 | U) - I(V_2; Y | U, X_1, V_1)$:
\[
H(W_2|Y^N) \geq H(W_2|Y^N, V_1^N, U^N, X_1^N)
\]

\[
= H(W_{20}, W_{22}|Y^N, V_1^N, U^N, X_1^N)
\]

\[
\overset{(a)}{=} H(W_{22}|Y^N, V_1^N, U^N, X_1^N)
\]

\[
= H(W_{22}, Y^N|V_1^N, U^N, X_1^N) - H(Y^N|V_1^N, U^N, X_1^N)
\]

\[
= H(W_{22}, Y^N, V_2^N|V_1^N, U^N, X_1^N) - H(V_2^N|W_{22}, Y^N, V_1^N, U^N, X_1^N) - H(Y^N|V_1^N, U^N, X_1^N)
\]

\[
\geq H(Y^N, V_2^N|V_1^N, U^N, X_1^N) - H(V_2^N|W_{22}, Y^N, V_1^N, U^N, X_1^N) - H(Y^N|V_1^N, U^N, X_1^N)
\]

\[
= H(V_2^N|V_1^N, U^N, X_1^N) + H(Y^N|V_2^N, V_1^N, U^N, X_1^N) - H(V_2^N|W_{22}, Y^N, V_1^N, U^N, X_1^N)
\]

\[
- H(Y^N|V_1^N, U^N, X_1^N)
\]

\[
\overset{(b)}{=} H(V_2^N|U^N) - I(V_1^N; V_2^N|U^N) - I(Y^N; V_2^N|V_1^N, U^N, X_1^N)
\]

\[
- H(V_2^N|W_{22}, Y^N, V_1^N, U^N, X_1^N)
\]

(A87)

where (a) follows from the fact that given \(U^N, W_{20}\) is uniquely determined, and (b) is from that \(X_1^N\) is independent of \(V_1^N, V_2^N\) and \(U^N\).

For the first term in (A87), we have

\[
H(V_2^N|U^N) \geq \log 2^{N(L_21+L_22+L_3)} - \delta_3 = N(I(V_2; Z|U) - \epsilon) - \delta_3,
\]

(A88)

where \(\delta_3\) is small for sufficiently large \(N\).

For the second and third terms in (A87), using the same approach as that in [20] Lemma 3, we get

\[
I(V_1^N; V_2^N|U^N) \leq N(I(V_1; V_2|U) + \epsilon'),
\]

(A89)

and

\[
I(Y^N; V_2^N|V_1^N, U^N, X_1^N) \leq N(I(V_2; Y|U, V_1, X_1) + \epsilon''),
\]

(A90)

where \(\epsilon', \epsilon'' \to 0\) as \(N \to \infty\).

Now, we consider the last term of (A87).

- For the case that \(R_{22} \leq L_{21} + L_{22}\), given \(U^N, V_1^N\) and \(W_{22}\), the total number of possible codewords of \(V_2^N\)

\[
N_3 \leq 2^{NL_{22}} = 2^{N I(V_2; Y|U, V_1, V_2)}.
\]

(A91)

By using the Fano’s inequality and (A91), we have

\[
H(V_2^N|W_{22}, Y^N, V_1^N, U^N, X_1^N) \leq N \epsilon''',
\]

(A92)

where \(\epsilon''' \to 0\).
For the case that \( L_{21} + L_{22} \leq R_{22} \leq L_{21} + L_{22} + L_3 \), given \( U^N, V_1^N \) and \( W_{22}, V_2^N \) is totally determined, and therefore
\[
H(V_2^N | W_{22}, Y^N, V_1^N, U^N, X_1^N) = 0. \tag{A93}
\]
Substituting (A88), (A89), (A90) and (A92) (or (A93)) into (A87), and using the definition (2.3), we have
\[
\lim_{N \to \infty} \Delta_2 \geq R_{c2} = I(V_2; Z|U) - I(V_1; V_2|U) - I(V_2; Y|U, X_1, V_1). \tag{A94}
\]
This completes the proof for Theorem 3.

**APPENDIX D**

**PROOF OF THEOREM 4**

We consider the proof of Theorem 4 for the case \( I(X_1; Y) \geq I(X_1; Z|U, V_2) \), and the proof for \( I(X_1; Z) \geq I(X_1; Y|U, V_1) \) follows by symmetry. Now we will prove that the quintuple \((R_0, R_1, R_2, R_{e1}, R_{e2}) \in \mathcal{R}^{(A3)}\) with the conditions
\[
R_{e1} = R^* + I(V_1; Y, \hat{Y}_1|U, X_1) - I(V_1; V_2|U) - I(X_1, V_1; Z|U, V_2), \tag{A94}
\]
and
\[
R_{e2} = I(V_2; Z|U) - I(V_1; V_2|U) - I(V_2; Y|U, X_1, V_1), \tag{A95}
\]
is achievable, where
\[
\min\{I(X_1; Z|U, V_1, V_2), I(X_1; Y)\} - R^* \geq I(Y_1; \hat{Y}_1|X_1).
\]

Similar to the proof of Theorem 3, we split the confidential message \( W_1 \) into \( W_{10} \) and \( W_{11} \), and \( W_2 \) into \( W_{20} \) and \( W_{22} \), and the definitions of these messages are the same as those in Appendix C. Here note that the formulas (A94) and (A95) combined with the rate splitting and the fact that \( W_{10} \) and \( W_{20} \) are decoded by both receivers ensure that,
\[
R_{11} \geq R_{e1} = R^* + I(V_1; Y, \hat{Y}_1|U, X_1) - I(V_1; V_2|U) - I(X_1, V_1; Z|U, V_2), \tag{A96}
\]
and
\[
R_{22} \geq R_{e2} = I(V_2; Z|U) - I(V_1; V_2|U) - I(V_2; Y|U, X_1, V_1). \tag{A97}
\]

1) **Code Construction:**

**Construction of the relay code-book:**

We first generate at random \( 2^{NR_0} \) i.i.d. sequences \( x_1^N \) at the relay node each drawn according to \( p(x_1^N) = \prod_{i=1}^{N} p(x_{1,i}) \), index them as \( x_1^N(s), \ s \in [1, 2^{NR_0}] \), where
\[
R_r = \min\{I(X_1; Z|U, V_1, V_2), I(X_1; Y)\} - \epsilon, \tag{A98}
\]
and
\[
I(X_1; Z|U, V_2) - \epsilon \leq R_r \leq I(X_1; Z|U, V_1, V_2) - \epsilon. \tag{A99}
\]

For each \( x_1^N(s) \), generate at random \( 2^{N(R_r - R^*)} \) i.i.d. \( \hat{y}_1^N \), each with probability \( p(\hat{y}_1^N|x_1^N(s)) = \prod_{i=1}^{N} p(\hat{y}_{1,i}|x_{1,i}(s)) \). Label these \( \hat{y}_1^N(m, s), \ m \in [1, 2^{N(R_r - R^*)}], s \in [1, 2^{NR_0}] \). Equally divide these \( 2^{NR_0} \) \( x_1^N \) sequences into \( 2^{N(R_r - R^*)} \) bins, hence there are \( 2^{NR^*} x_1^N \) sequences at each bin. Let \( f \) be this mapping, i.e., \( m = f(s) \).
Construction of $U^N$:
Generate at random $2^{N(R_1+R_2+R_0)}$ i.i.d. sequences $v^N(b)$ $(b \in [1, 2^{N(R_1+R_2+R_0)}])$ according to $\prod_{i=1}^{N} p_U(u_i)$. 

Constructions of $V_1^N$ and $V_2^N$:
For arbitrary $\epsilon > 0$, define

\begin{align}
L_{11} &= I(V_1; Y, \hat{Y}_1|U, X_1) - I(V_1; V_2|U) - I(V_1; Z|U, V_2), \\
L_{12} &= I(V_1; Z|U, V_2), \\
L_{21} &= I(V_2; Z|U) - I(V_1; V_2|U) - I(V_2; Y|U, X_1, V_1), \\
L_{22} &= I(V_2; Y|U, X_1, V_1), \\
L_3 &= I(V_1; V_2|U) - \epsilon.
\end{align}

Note that

\begin{align}
L_{11} + L_{12} + L_3 &= I(V_1; Y, \hat{Y}_1|U, X_1) - \epsilon, \\
L_{21} + L_{22} + L_3 &= I(V_2; Z|U) - \epsilon.
\end{align}

- For the transmitted sequence $u^N(b)$, generate $2^{N(L_{11}+L_{12}+L_3)}$ i.i.d. sequences $v_1^N(i', i'', i''')$, with $i' \in I' = [1, 2^{N_{11}}]$, $i'' \in I'' = [1, 2^{N_{12}}]$ and $i''' \in I''' = [1, 2^{N_3}]$, according to $\prod_{i=1}^{N} p_{V_1|U}(v_1|i_{u_i})$.

- Similarly, for the transmitted sequences $u^N$, generate $2^{N(L_{21}+L_{22}+L_3)}$ i.i.d. sequences $v_2^N(j', j'', j''')$, with $j' \in J' = [1, 2^{N_{21}}]$, $j'' \in J'' = [1, 2^{N_{22}}]$ and $j''' \in J''' = [1, 2^{N_3}]$, according to $\prod_{i=1}^{N} p_{V_2|U}(v_2|i_{u_i})$.

Construction of $X^N$:
The $x^N$ is generated according to a new discrete memoryless channel (DMC) with inputs $u^N, v_1^N, v_2^N$ and output $x^N$. The transition probability of this new DMC is $p_{X|U,V_1,V_2}(x|u, v_1, v_2)$. Denote $x^N$ by $x^N(w_0, w_{10}, w_{20}, w_{11}, w_{22})$.

2) Encoding:
Similar to the definitions in Appendix C define $w_{0,i}^N = (w_{0,i}, w_{10,i}, w_{20,i})$, where $w_{0,i}, w_{10,i}$ and $w_{20,i}$ are the messages transmitted in the $i$-th block. The messages $w_{11}$ and $w_{22}$ transmitted in the $i$-th block are denoted by $w_{11,i}$ and $w_{22,i}$, respectively.

- (Channel encoder)

1) The transmitter sends $(u^N(w_{0,i}^N), v_1^N(i'_i, i''_i, i'''_i|w_{0,i}^N), v_2^N(j'_i, j''_i, j'''_i|w_{0,i}^N))$ for the $i$-th block $(1 \leq i \leq n)$.

Here $i'_i$, $i''_i$, $i'''_i$, $j'_i$, $j''_i$ and $j'''_i$ are the indexes for block $i$. Especially note that for the $n$-th block, the transmitted messages are denoted by $(w_{0,n}^N, w_{11,n}, w_{22,n}) = (1, 1, 1)$.

2) The indexes $i'_i$, $i''_i$, $j'_i$, $j''_i$, $i'''_i$ and $j'''_i$ are determined exactly the same as those in Appendix C and we omit the details here.

3) The transmitter finally sends $x^N(w_{0,i}, w_{10,i}, w_{20,i}, w_{11,i}, w_{22,i})$.

- (Relay encoder)
At the end of block $i$ ($2 \leq i \leq n$), assume that $(x_i^N(s_i), y_i^N(i), \hat{y}_1^N(m_i, s_i))$ are jointly typical, then we choose $s_{i+1}$ uniformly from bin $m_i$, and the relay sends $x_{i+1}^N$ at block $i+1$. In the first block, the relay sends $x_1^N(1)$.

3) Decoding:

(At the relay) At the end of block $i$, the relay already has $s_i$, it then decides $m_i$ by choosing $m_i$ such that $(x_i^N(s_i), y_i^N(i), \hat{y}_1^N(m_i, s_i))$ are jointly typical. There exists such $m_i$, if

$$R_r - R^* \geq I(Y_1; \hat{Y}_1|X_1),$$

(A107)

and $N$ is sufficiently large. Choose $s_{i+1}$ uniformly from bin $m_i$.

(At receiver 1) Receiver 1 does backward decoding. The decoding process starts at the last block $n$, receiver 1 decodes $s_n$ by choosing unique $\hat{s}_n$ such that $(x_n^N(\hat{s}_n), y^N(n))$ are jointly typical. Since $R_r$ satisfies (A98), the probability $Pr\{\hat{s}_n = s_n\}$ goes to 1 for sufficiently large $N$.

Next, receiver 1 moves to the block $n - 1$. Now it already has $\hat{s}_n$, hence also we have $\tilde{m}_{n-1} = f(\hat{s}_n)$. It first declares that $\tilde{m}_{n-1}$ is received, if $\tilde{m}_{n-1}$ is the unique one such that $(x_{n-1}^N(\tilde{m}_{n-1}), y^N(n-1))$ are joint typical. If it is satisfied, $\tilde{m}_{n-1} = s_{n-1}$ with high probability. After knowing $\tilde{m}_{n-1}$, the destination gets an estimation of $w_{0,n-1}^*$ by picking the unique $\tilde{w}_{0,n-1}$ such that $(w_{0,n-1}^*, \hat{y}_1^N(\tilde{m}_{n-1}, \tilde{s}_{n-1}), y^N(n-1), x_{1}^N(\tilde{s}_{n-1}))$ are jointly typical. We will have $\tilde{w}_{0,n-1}^* = w_{0,n-1}^*$ with high probability, if

$$R_0 + R_{10} + R_{20} \leq I(U; Y, \hat{Y}_1|X_1),$$

(A108)

and $N$ is sufficiently large.

After decoding $\tilde{w}_{0,n-1}^*$, receiver 1 tries to find a quadruple such that

$$(u_1^N(\tilde{t}_{n-1}', \tilde{t}_{n-1}'', \tilde{t}_{n-1}'''|\tilde{w}_{0,n-1}^*), u_{N-1}(\tilde{w}_{0,n-1}^*), x_{1}^N(\tilde{s}_{n-1}), \hat{y}_1^N(\tilde{m}_{n-1}, \tilde{s}_{n-1}), y^N(n-1))$$

are jointly typical. Based on the AEP, the probability $Pr\{\tilde{u}_{11,n-1} = w_{11,n-1}\}$ goes to 1 if

$$R_{11} \leq I(V_1; Y, \hat{Y}_1|U, X_1).$$

(A109)

If such $v_{1}^N(\tilde{t}_{n-1}', \tilde{t}_{n-1}'', \tilde{t}_{n-1}''', |\tilde{w}_{0,n-1}^*)$ exists and is unique, set $\tilde{t}_{n-1}' = \tilde{t}_{n-1}'', \tilde{t}_{n-1}''' = \tilde{t}_{n-1}'''$; otherwise, declare an error. From the values of $\tilde{t}_{n-1}'$, $\tilde{t}_{n-1}'''$, and $\tilde{t}_{n-1}'''$, and the above encoding schemes, receiver 1 can calculate the message $\tilde{w}_{11,n-1}$.

The decoding scheme of receiver 1 in block $i$ ($1 \leq i \leq n - 2$) is similar to that in block $n - 1$, and we omit it here.

(At receiver 2) In block $i$ ($1 \leq i \leq n - 1$), since $R_r$ satisfies (A98), and note that $I(X_1; Y) \geq I(X_1; Z|V_2, U) \geq I(X_1; Z)$, and $I(X_1; Z|V_1, V_2, U) \geq I(X_1; Z)$, receiver 2 can not decode the relay codeword $x_1^N$. The decoding scheme for receiver 2 is as follows.

Receiver 2 gets the estimation of the message $w_{0,i}^*$ by finding a unique pair such that $(w_{0,i}^*, z^N(i))$ are jointly typical. Based on the AEP, the probability $Pr\{\tilde{w}_{0,i}^* = w_{0,i}^*\}$ goes to 1 if

$$R_0 + R_{10} + R_{20} \leq I(U; Z).$$

(A110)
After decoding $\hat{w}_{0,j}^*$, receiver 2 tries to find a triple such that $(v_2^N(\hat{j}_1', \hat{j}_i', \hat{j}_i'' | \hat{w}_{0,j}^*), u^N(\hat{w}_{0,j}^*), z^N(i))$ are jointly typical. Based on the AEP, the probability $Pr\{\hat{w}_{22,i} = w_{22,i}\}$ goes to 1 if

$$R_{22} \leq I(V_2; Z|U).$$

(A111)

If such $v_2^N(\hat{j}_1', \hat{j}_i', \hat{j}_i'' | \hat{w}_{0,j}^*)$ exists and is unique, set $\hat{j}_i' = j_i', \hat{j}_i'' = j_i''$ and $\hat{j}_i''' = j_i'''$; otherwise, declare an error. From the values of $\hat{j}_i, \hat{j}_i', \hat{j}_i''$, and the above encoding schemes, receiver 2 can calculate the message $\hat{w}_{22,i}$.

By using the above encoding-decoding scheme, it is easy to check that $P_{e1} \leq \epsilon$ and $P_{e2} \leq \epsilon$. Moreover, applying Fourier-Motzkin elimination on the above inequalities with the definitions $R_1 = R_{10} + R_{11}$ and $R_2 = R_{20} + R_{22}$, we get

$$R_0 \leq \min\{I(U; Y, \hat{Y}_1 | X_1), I(U; Z)\},$$

$$R_0 + R_1 \leq \min\{I(U; Y, \hat{Y}_1 | X_1), I(U; Z)\} + I(V_1; Y, \hat{Y}_1 | U, X_1),$$

$$R_0 + R_2 \leq \min\{I(U; Y, \hat{Y}_1 | X_1), I(U; Z)\} + I(V_2; Z|U),$$

$$R_0 + R_1 + R_2 \leq \min\{I(U; Y, \hat{Y}_1 | X_1), I(U; Z)\} + I(V_1; Y, \hat{Y}_1 | U, X_1) + I(V_2; Z|U) - I(V_1; V_2|U),$$

$$\min\{I(X_1; Y), I(X_1; Z|V_1, V_2, U)\} - R^* \geq I(Y_1; \hat{Y}_1 | X_1).$$

Note that the above bounds are the same as those in Theorem 4.

**Equivocation Analysis:** Now, it remains to prove $\lim_{N \to \infty} \Delta_1 \geq R_{e1} = R^* + I(V_1; Y, \hat{Y}_1 | U, X_1) - I(V_1; V_2|U) - I(X_1, V_1; Z|U, V_2)$ and $\lim_{N \to \infty} \Delta_2 \geq R_{e2} = I(V_2; Z|U) - I(V_1; V_2|U) - I(V_2; Y | U, X_1, V_1).

**Proof of** $\lim_{N \to \infty} \Delta_1 \geq R_{e1} = R^* + I(V_1; Y, \hat{Y}_1 | U, X_1) - I(V_1; V_2|U) - I(X_1, V_1; Z|U, V_2)$:

$$H(W_1|Z^N) \geq H(W_1|Z^N, V_2^N, U^N)$$

$$= H(W_{10}, W_{11}|Z^N, V_2^N, U^N)$$

$$\overset{(a)}{=} H(W_{11}|Z^N, V_2^N, U^N)$$

$$= H(W_{11}, Z^N|V_2^N, U^N) - H(Z^N|V_2^N, U^N)$$

$$= H(W_{11}, Z^N, X_1^N|V_2^N, U^N) - H(V_1^N, X_1^N|W_{11}, Z^N, V_2^N, U^N) - H(Z^N|V_2^N, U^N)$$

$$\geq H(Z^N, V_1^N, X_1^N|V_2^N, U^N) - H(V_1^N, X_1^N|W_{11}, Z^N, V_2^N, U^N) - H(Z^N|V_2^N, U^N)$$

$$= H(V_1^N, X_1^N|V_2^N, U^N) + H(Z^N|V_1^N, V_2^N, U^N, X_1^N) - H(V_1^N, X_1^N|W_{11}, Z^N, V_2^N, U^N)$$

$$- H(Z^N|V_2^N, U^N)$$
\[
\begin{align*}
(b) & \quad H(X_1^N) + H(V_1^N|V_2^N, U^N) + H(Z^N|V_1^N, V_2^N, U^N, X_1^N) - H(V_1^N, X_1^N|W_{11}, Z^N, V_2^N, U^N) \\
& \quad + H(Z^N|V_2^N, U^N) \\
& = \quad H(X_1^N) + H(V_1^N|U^N) - I(V_1^N; V_2^N|U^N) + H(Z^N|V_1^N, V_2^N, U^N, X_1^N) \\
& \quad - H(V_1^N, X_1^N|W_{11}, Z^N, V_2^N, U^N) - H(Z^N|V_2^N, U^N) \\
& = \quad H(X_1^N) + H(V_1^N|U^N) - I(V_1^N; V_2^N|U^N) - I(Z^N; X_1^N, V_1^N|V_2^N, U^N) \\
& \quad - H(V_1^N, X_1^N|W_{11}, Z^N, V_2^N, U^N),
\end{align*}
\]

where (a) follows from the fact that given \(U^N, W_{10}\) is uniquely determined, and (b) is from that \(X_1^N\) is independent of \(V_1^N, V_2^N\) and \(U^N\).

Consider the first term in (A112), the codeword generation and \cite{24} Lemma 3] ensure that
\[
H(X_1^N) \geq NR^* - \delta,
\]
where \(\delta\) is small for sufficiently large \(N\).

For the second term in (A112), similarly we have
\[
H(V_1^N|U^N) \geq \log 2^{N(L_1 + L_{12} + L_3)} - \delta_1 = N(I(V_1; V_2|U) - \epsilon) - \delta_1,
\]
where \(\delta_1\) is small for sufficiently large \(N\).

For the third and fourth terms in (A112), using the same approach as that in \cite{20} Lemma 3, we get
\[
I(V_1^N; V_2^N|U^N) \leq N(I(V_1; V_2|U) + \epsilon'),
\]
and
\[
I(Z^N; X_1^N, V_1^N|V_2^N, U^N) \leq N(I(X_1, V_1; Z|U, V_2) + \epsilon''),
\]
where \(\epsilon', \epsilon'' \to 0\) as \(N \to \infty\).

Now, we consider the last term of (A112).
\begin{itemize}
  \item For the case that \(R_{11} \leq L_{11}\), given \(U^N, V_2^N, W_{11}\) and \(\epsilon'' \to 0^+\),
  \[
  H(V_1^N, X_1^N|W_{11}, Z^N, V_2^N, U^N) \leq N\epsilon''
  \]
  is guaranteed if \(R_r \leq I(X_1; Z|V_1, V_2, U) - \epsilon\) and \(R_r \geq I(X_1; Z|U, V_2) - \epsilon\ (\epsilon \to 0^+)\), and this is from the properties of AEP (similar argument is used in the proof of Theorem 3 in \cite{29}). By using (A99), (A117) is obtained.
  \item For the case that \(L_{11} \leq R_{11} \leq L_{11} + L_{12}\), given \(U^N, V_2^N\) and \(W_{11}\), the total number of possible codewords of \(V_1^N\) is
  \[
  N_1 \leq 2^{N(L_{12})} = 2^{NI(V_1; Z|U, V_2)}
  \]
  By using the Fano’s inequality and (A118), we have
  \[
  H(V_1^N|W_{11}, Z^N, V_2^N, U^N) \leq N\epsilon''
  \]
\end{itemize}
where \( \epsilon''' \to 0 \).

Given \( U^N, V_1^N, V_2^N \) and \( W_{11} \), the total number of possible codewords of \( X_1^N \) is

\[
N_2 \leq 2^{N R_e} = 2^{N(\min\{I(X_1;Y), I(X_1;Z|V_1,V_2,U)\} - \epsilon)}.
\]

(A120)

By using the Fano’s inequality and (A120), we have

\[
H(X_1^N|W_{11},Z^N, V_1^N, V_2^N, U^N) \leq N \epsilon'''
\]

(A121)

where \( \epsilon''''' \to 0 \).

By using (A119) and (A121),

\[
\frac{1}{N} H(V_1^N, X_1^N|W_{11}, Z^N, V_2^N, U^N) \leq \epsilon \to 0,
\]

(A122)

is guaranteed.

- For the case that \( L_{11} + L_{12} \leq R_{11} \leq L_{11} + L_{12} + L_3 \), given \( U^N, V_2^N \) and \( W_{11}, V_1^N \) is totally determined, and therefore

\[
H(V_1^N|W_{11}, Z^N, V_2^N, U^N) = 0.
\]

(A123)

Similarly, note that \( R_e = \min\{I(X_1;Y), I(X_1;Z|V_1,V_2,U)\} - \epsilon \), by using the Fano’s inequality, we have (A121). Thus

\[
\frac{1}{N} H(V_1^N, X_1^N|W_{11}, Z^N, V_2^N, U^N) \leq \epsilon \to 0
\]

(A124)

is guaranteed.

Substituting (A113), (A114), (A115), (A116) and (A117) (or (A122),(A124)) into (A112), and using the definition (2.3), we have \( \lim_{N \to \infty} \Delta_1 \geq R_{e1} = R_e + I(V_1;Y, \bar{Y}_1|U, X_1) - I(V_1;V_2|U) - I(X_1, V_1; Z|U, V_2) \).

**Proof of** \( \lim_{N \to \infty} \Delta_2 \geq R_{e2} = I(V_2;Z|U) - I(V_1;V_2|U) - I(V_2;Y|U, X_1, V_1) \):

The proof of \( \lim_{N \to \infty} \Delta_2 \geq R_{e2} = I(V_2;Z|U) - I(V_1;V_2|U) - I(V_2;Y|U, X_1, V_1) \) is exactly the same as that in Appendix C, and therefore, we omit the proof here.

The proof for Theorem 4 is completed.

**APPENDIX E**

**PROOF OF THEOREM 11**

The proof of Theorem 11 is a combination of the NF strategy [29] and Csiszár-Körner’s techniques on broadcast channels with confidential messages [20], see the remainder of this section.

Theorem 11 is proved by the following two cases.

- **(Case 1)** If the channel from the relay to receiver 1 is less noisy than the channel from the relay to receiver 2 \( I(X_1;Y) \geq I(X_1;Z|U) \), we allow receiver 1 to decode \( x_1^N \), and receiver 2 can not decode it.

  For case 1, it is sufficient to show that the triple \( (R_0, R_1, R_e) \in C^3 \) with the condition

\[
R_e = \min\{I(X_1;Z|U, V), I(X_1;Y)\} + I(V;Y|U, X_1) - I(X_1, V; Z|U),
\]

(A125)
is achievable.

• **(Case 2)** If the channel from the relay to receiver 1 is more noisy than the channel from the relay to receiver 2 \((I(X_1; Y) \leq I(X_1; Z))\), we allow both the receivers to decode \(x_1^N\).

For case 2, it is sufficient to show that the triple \((R_0, R_1, R_e) \in \mathcal{L}^{10}\) with the condition

\[
R_e = I(V; Y|U, X_1) - I(V; Z|U, X_1),
\]  

is achievable.

Now split the confidential message \(W_1\) into \(W_{10}\) and \(W_{11}\), and the details are as follows.

Define the messages \(W_0, W_{10}, W_{11}\) taken values in the alphabets \(\mathcal{W}_0, \mathcal{W}_{10}, \mathcal{W}_{11}\), respectively, where

\[
\mathcal{W}_0 = \{1, 2, \ldots, 2^{NR_0}\},
\]

\[
\mathcal{W}_{10} = \{1, 2, \ldots, 2^{NR_{10}}\},
\]

\[
\mathcal{W}_{11} = \{1, 2, \ldots, 2^{NR_{11}}\},
\]

and \(R_{10} + R_{11} = R_1\). Here note that the formulas \((A125)\) and \((A126)\) combined with the rate splitting and the fact that \(W_{10}\) is decoded by both receivers ensure that,

\[
R_{11} \geq R_e = \min\{I(X_1; Z|U, V), I(X_1; Y)\} + I(V; Y|U, X_1) - I(X_1, V; Z|U),
\]  

(A127)

and

\[
R_{11} \geq R_e = I(V; Y|U, X_1) - I(V; Z|U, X_1),
\]  

(A128)

respectively.

**Code-book Construction for the Two Cases:**

First, we define some parameters that will be used in the construction of \(v_N\), see the followings.

• For the case 1, fix the joint probability mass function \(P_{Y, Z, Y_1, X, X_1, V, U}(y, z, y_1, x, x_1, v, u)\), and define

\[
L_{11} = I(V; Y|U, X_1) - I(V; Z|U),
\]  

(A129)

\[
L_{12} = I(V; Z|U),
\]  

(A130)

\[
L_{13} = \min\{I(U; Y|X_1), I(U; Z)\},
\]  

(A131)

Note that \(L_{11} \geq R_e\).

• For the case 2, fix the joint probability mass function \(P_{Y, Z, Y_1, X, X_1, V, U}(y, z, y_1, x, x_1, v, u)\), and define

\[
L_{21} = I(V; Y|U, X_1) - I(V; Z|U, X_1),
\]  

(A132)

\[
L_{22} = I(V; Z|U, X_1),
\]  

(A133)

\[
L_{23} = \min\{I(U; Y|X_1), I(U; Z|X_1)\}.
\]  

(A134)

Then, the constructions of the code-books for the two cases are as follows.
• Code-book Construction for case 1:
  - First, generate at random $2^{N R_r}$ i.i.d. sequences at the relay node each drawn according to $p_{X_1^N}(x_1^N) = \prod_{i=1}^N p_{X_i}(x_{1,i})$, index them as $x_i^N(a)$, $a \in [1, 2^{N R_r}]$, where
    \[ R_r = \min\{I(X_1; Z|U, V), I(X_1; Y)\} - \epsilon, \]  
    \[ \text{and } \epsilon \text{ is an arbitrary small positive real number. Here note that} \]
    \[ I(X_1; Z|U) - \epsilon \leq R_r \leq I(X_1; Z|U) - \epsilon. \]  
  - Generate at random $2^{N(R_0+R_{10})}$ i.i.d. sequences $u^N(b)$ ($b \in [1, 2^{N(R_0+R_{10})}]$) according to $\prod_{i=1}^N p_U(u_i)$.
  - For the transmitted sequence $u^N(b)$, generate $2^{N(L_{11}+L_{12}+L_{13})}$ i.i.d. sequences $v^N(i', i'', i''')$, with $i' \in \mathcal{I} = [1, 2^{NL_{11}}]$, $i'' \in \mathcal{I}'' = [1, 2^{NL_{12}}]$ and $i''' \in \mathcal{I}''' = [1, 2^{NL_{13}}]$, according to $\prod_{i=1}^N p_{V|U}(v_i|u_i)$.
  - The $x^N$ is generated according to a new discrete memoryless channel (DMC) with inputs $u^N$, $v^N$, and output $x^N$. The transition probability of this new DMC is $p_{X|U,V}(x|u, v)$. The probability $p_{X^N|U^N,V^N}(x^N|u^N, v^N)$ is calculated as follows.
    \[ p_{X^N|U^N,V^N}(x^N|u^N, v^N) = \prod_{i=1}^N p_{X_i|U_i,V_i}(x_{1,i}|u_i, v_i). \]  

• Code-book Construction for case 2:
  - First, generate at random $2^{N R_r}$ i.i.d. sequences at the relay node each drawn according to $p_{X_1^N}(x_1^N) = \prod_{i=1}^N p_{X_i}(x_{1,i})$, index them as $x_i^N(a)$, $a \in [1, 2^{N R_r}]$, where
    \[ R_r = \min\{I(X_1; Y), I(X_1; Z)\} - \epsilon = I(X_1; Y) - \epsilon, \]  
    \[ \text{and } \epsilon \text{ is an arbitrary small positive real number.} \]
  - Generate at random $2^{N(R_0+R_{10})}$ i.i.d. sequences $u^N(b)$ ($b \in [1, 2^{N(R_0+R_{10})}]$) according to $\prod_{i=1}^N p_U(u_i)$.
  - For the transmitted sequence $u^N(b)$, generate $2^{N(L_{21}+L_{22}+L_{23})}$ i.i.d. sequences $v^N(i', i'', i''')$, with $i' \in \mathcal{I} = [1, 2^{NL_{21}}]$, $i'' \in \mathcal{I}' = [1, 2^{NL_{22}}]$ and $i''' \in \mathcal{I}''' = [1, 2^{NL_{23}}]$, according to $\prod_{i=1}^N p_{V|U}(v_i|u_i)$.
  - The $x^N$ is generated exactly the same as that of case 1, and it is omitted here.

Encoding:

• (Channel encoder)

1) For a given message triple $(w_0, w_{10}, w_{11})$, the transmitter sends $u^N(w_0, w_{10})$ and $v^N(i', i'', i''')|w_0, w_{10})$.
2) The indexes $i'$, $i''$ and $i'''$ are determined by the following methods.

  - Case 1:
    * If $R_{11} \leq L_{11}$, evenly partition $\mathcal{I}'$ into $\mathcal{W}_{11}$ bins, and the index $i'_1$ is drawn at random (with uniform distribution) from the bin $w_{11}$. The index $i''_1$ is drawn at random (with uniform distribution) from $\mathcal{I}''$.
      Let $\mathcal{W}_0 \times \mathcal{W}_{10} \subseteq \mathcal{I}''$, and the index $i''_1$ is determined by the messages $w_0$ and $w_{10}$.
    * If $L_{11} \leq R_{11} \leq L_{11} + L_{12}$, define $\mathcal{W}_{11} = \mathcal{I}' \times \mathcal{K}_1$. Thus the index $i'_1$ is determined by a given message $w_{11}$. Evenly partition $\mathcal{I}'$ into $\mathcal{K}_1$ bins, and the index $i''_1$ is drawn at random (with uniform distribution) from the bin $k_1$. Let $\mathcal{W}_0 \times \mathcal{W}_{10} \subseteq \mathcal{I}''$, and the index $i''_1$ is determined by the messages $w_0$ and $w_{10}$. 


Case 1:

Decoding: The relay uniformly picks a codeword \( \hat{\mathbf{w}} \) at receiver 1. Receiver 1 will declare that \( a = \hat{a} \) if \( \{\hat{a}, \hat{\mathbf{w}}_0, \hat{\mathbf{w}}_{10}\} \) jointly typical. Based on the AEP, the probability

\[
\Pr\{a = \hat{a}\} \to 1
\]

Having \( \hat{a} \), receiver 1 can get the estimation of the messages \( w_0 \) and \( w_{10} \) by finding a unique triple such that

\[
(u^N(\hat{w}_0, \hat{w}_{10}), x_1^N(\hat{a}), y^N) \quad \text{are jointly typical. Based on the AEP, the probability} \quad \Pr\{(\hat{w}_0, \hat{w}_{10}) = (w_0, w_{10})\} \quad \text{goes to 1 if}
\]

\[
R_0 + R_{10} \leq I(U; Y|X_1).
\]  

(A139)

After decoding \( \hat{w}_0 \) and \( \hat{w}_{10} \), receiver 1 tries to find a quadruple such that

\[
(u^N(i', i'', i'''), \hat{w}_0, \hat{w}_{10}), u^N(\hat{w}_0, \hat{w}_{10}), x_1^N(\hat{a}), y^N) \quad \text{are jointly typical. Based on the AEP, the probability} \quad \Pr\{\hat{w}_{11} = w_{11}\} \quad \text{goes to 1 if}
\]

\[
R_{11} \leq I(V; Y|U, X_1).
\]  

(A140)

If such \( u^N(i', i'', i''') \) exists and is unique, set \( \hat{i}' = i' \), \( \hat{i}'' = i'' \) and \( \hat{i}''' = i''' \); otherwise, declare an error. From the values of \( \hat{i}' \), \( \hat{i}'' \), \( \hat{i}''' \), and the above encoding schemes, receiver 1 can calculate the message \( \hat{w}_{11} \).

(At receiver 2) The decoding scheme for receiver 2 is as follows.

Receiver 2 gets the estimation of the messages \( w_0 \) and \( w_{10} \) by finding a unique pair such that \( (u^N(\hat{w}_0, \hat{w}_{10}), \hat{z}^N) \) are jointly typical. Based on the AEP, the probability \( \Pr\{(\hat{w}_0, \hat{w}_{10}) = (w_0, w_{10})\} \) goes to 1 if

\[
R_0 + R_{10} \leq I(U; Z).
\]  

(A141)

Case 2:

(At receiver 1) Receiver 1 will declare that \( \tilde{a} = \hat{a} \) if \( x_1^N(\tilde{a}), y^N \) are jointly typical. By using (A138) and the AEP, it is easy to see that the probability \( \Pr\{\tilde{a} = a\} \) goes to 1.
Having $\hat{a}$, receiver 1 can get the estimation of the messages $w_0$ and $w_{10}$ by finding a unique triple such that $(u^N(\hat{w}_0, \hat{w}_{10}), x_1^N(\hat{a}), y^N)$ are jointly typical.

After decoding $\hat{w}_0$ and $\hat{w}_{10}$, receiver 1 tries to find a quadruple such that

$$(v^N(\hat{i}', \hat{i}'', \hat{i}''', |\hat{w}_0, \hat{w}_{10}), u^N(\hat{w}_0, \hat{w}_{10}), x_1^N(\hat{a}), y^N)$$

are jointly typical. If such $v^N(\hat{i}', \hat{i}'', \hat{i}''', |\hat{w}_0, \hat{w}_{10})$ exists and is unique, set $\hat{i}' = i'$, $\hat{i}'' = i''$ and $\hat{i}''' = i'''$; otherwise, declare an error. From the values of $\hat{i}', \hat{i}'', \hat{i}'''$, and the above encoding schemes, receiver 1 can calculate the message $\hat{w}_{11}$.

(At receiver 2) Receiver 2 will declare that $\hat{a}$ is received if $(x_1^N(\hat{a}), z^N)$ jointly typical. By using (A138) and the AEP, it is easy to see that the probability $Pr\{\hat{a} = a\}$ goes to 1.

Having $\hat{a}$, receiver 2 can get the estimation of the messages $w_0$ and $w_{10}$ by finding a unique triple such that $(u^N(\hat{w}_0, \hat{w}_{10}), x_1^N(\hat{a}), z^N)$ are jointly typical. Based on the AEP, the probability $Pr\{ (\hat{w}_0, \hat{w}_{10}) = (w_0, w_{10}) \}$ goes to 1 if

$$R_0 + R_{10} \leq I(U; Z|X_1).$$

(A142)

By using (A135), (A139), (A140) and (A141), it is easy to check that $P_{e1} \leq \epsilon$ and $P_{e2} \leq \epsilon$. Moreover, applying Fourier-Motzkin elimination on (A135), (A139), (A140) and (A141) with the definition $R_1 = R_{10} + R_{11}$, we get

$$R_0 \leq \min\{I(U; Y|X_1), I(U; Z)\},$$

$$R_0 + R_1 \leq \min\{I(U; Y|X_1), I(U; Z)\} + I(V; Y|U, X_1).$$

Similarly, by using (A138), (A139), (A140) and (A142), it is easy to check that $P_{e1} \leq \epsilon$ and $P_{e2} \leq \epsilon$. Moreover, applying Fourier-Motzkin elimination on (A138), (A139), (A140) and (A142) with the definition $R_1 = R_{10} + R_{11}$, we get

$$R_0 \leq \min\{I(U; Y|X_1), I(U; Z|X_1)\},$$

$$R_0 + R_1 \leq \min\{I(U; Y|X_1), I(U; Z|X_1)\} + I(V; Y|U, X_1).$$

Equivocation Analysis: Now, it remains to prove $\lim_{N \to \infty} \Delta \geq R_e = \min\{I(X_1; Z|U, V), I(X_1; Y)\} + I(V; Y|U, X_1) - I(X_1, V; Z|U)$ for the case 1, and $\lim_{N \to \infty} \Delta \geq R_e = I(V; Y|U, X_1) - I(V; Z|U, X_1)$ for the case 2.

Proof of $\lim_{N \to \infty} \Delta \geq R_e = \min\{I(X_1; Z|U, V), I(X_1; Y)\} + I(V; Y|U, X_1) - I(X_1, V; Z|U)$ for the case 1:
\[ H(W_1|Z^N) \geq H(W_1|Z^N, U^N) \]
\[ = H(W_{10}, W_{11}|Z^N, U^N) \]
\[ \overset{(a)}{=} H(W_{11}|Z^N, U^N) \]
\[ = H(W_{11}, Z^N|U^N) - H(Z^N|U^N) \]
\[ = H(W_{11}, Z^N, V^N, X_1^N|U^N) - H(V^N, X_1^N|W_{11}, Z^N, U^N) - H(Z^N|U^N) \]
\[ \geq H(Z^N, V^N, X_1^N|U^N) - H(V^N, X_1^N|W_{11}, Z^N, U^N) - H(Z^N|U^N) \]
\[ = H(V^N, X_1^N|U^N) + H(Z^N|V^N, U^N, X_1^N) - H(V^N, X_1^N|W_{11}, Z^N, U^N) \]
\[ - H(Z^N|U^N) \]
\[ \overset{(b)}{=} H(X_1^N) + H(V^N|U^N) + H(Z^N|V^N, U^N, X_1^N) - H(V^N, X_1^N|W_{11}, Z^N, U^N) \]
\[ - H(Z^N|U^N) \]
\[ = H(X_1^N) + H(V^N|U^N) + H(Z^N|V^N, U^N, X_1^N) \]
\[ - H(V^N, X_1^N|W_{11}, Z^N, U^N) H(Z^N|U^N) \]
\[ = H(X_1^N) + H(V^N|U^N) - I(Z^N; X_1^N, V^N|U^N) \]
\[ - H(V^N, X_1^N|W_{11}, Z^N, U^N), \] (A143)

where (a) follows from the fact that given \( U^N, W_{10} \) is uniquely determined, and (b) is from that \( X_1^N \) is independent of \( V^N \) and \( U^N \).

Consider the first term in (A143), the codeword generation and \([24, \text{Lemma 3}]\) ensure that
\[ H(X_1^N) \geq NR_1 - \delta = N\min\{I(X_1; Z|U, V), I(X_1; Y)\} - \epsilon - \delta, \] (A144)
where \( \delta \) is small for sufficiently large \( N \).

For the second term in (A143), similarly we have
\[ H(V^N|U^N) \geq \log 2^{N(L_{11} + L_{12})} - \delta_1 = NI(V; Y|U, X_1) - \delta_1, \] (A145)
where \( \delta_1 \) is small for sufficiently large \( N \).

For the third term in (A143), using the same approach as that in \([20, \text{Lemma 3}]\), we get
\[ I(Z^N; X_1^N, V^N|U^N) \leq N(I(X_1, V; Z|U) + \epsilon''), \] (A146)
where \( \epsilon'' \to 0 \) as \( N \to \infty \).

Now, we consider the last term of (A143). Given \( W_{11} \), receiver 2 can do joint decoding.

- For the case that \( R_{11} \leq L_{11} \), given \( U^N, Z^N, W_{11} \) and \( \epsilon'' \to 0^+ \),
\[ H(V^N, X_1^N|W_{11}, Z^N, U^N) \leq N\epsilon'' \], (A147)
is guaranteed if \( R_r \leq I(X_1; Z|U) - \epsilon \) and \( R_r \geq I(X_1; Z|U) - \epsilon \) \((\epsilon \to 0^+)\), and this is from the properties of AEP (similar argument is used in the proof of Theorem 3 in [29]). By using (A136), (A147) is obtained.

- For the case that \( L_{11} \leq R_{11} \leq L_{11} + L_{12} \), given \( U^N \), and \( W_{11} \), the total number of possible codewords of \( V^N \) is
  \[
  N_1 \leq 2^{N L_{12}} = 2^{N I(V; Z|U)}.
  \]
  By using the Fano’s inequality and (A148), we have
  \[
  H(V^N|W_{11}, Z^N, U^N) \leq N \epsilon^{'''},
  \]
  where \( \epsilon^{'''} \to 0 \).
  Given \( U^N \), \( V^N \) and \( W_{11} \), the total number of possible codewords of \( X_1^N \) is
  \[
  N_2 \leq 2^{N R_r} = 2^{N (\min \{I(X_1; Y), I(X_1; Z|U)\} - \epsilon)}.
  \]
  By using the Fano’s inequality and (A150), we have
  \[
  H(X_1^N|W_{11}, Z^N, V^N, U^N) \leq N \epsilon^{''''}
  \]
  where \( \epsilon^{''''} \to 0 \).
  By using (A149) and (A151),
  \[
  \frac{1}{N} H(V^N, X_1^N|W_{11}, Z^N, U^N) \leq \epsilon \to 0,
  \]
  is guaranteed.

- For the case that \( L_{11} + L_{12} \leq R_{11} \leq L_{11} + L_{12} + L_{13} \), given \( U^N \) and \( W_{11} \), \( V^N \) is totally determined, and therefore
  \[
  H(V^N|W_{11}, Z^N, U^N) = 0.
  \]
  Similarly, note that \( R_r = \min \{I(X_1; Z|U, V), I(X_1; Y)\} - \epsilon \), by using the Fano’s inequality, we have (A151). Thus
  \[
  \frac{1}{N} H(V^N, X_1^N|W_{11}, Z^N, U^N) \leq \epsilon \to 0
  \]
  is guaranteed.
  Substituting (A144), (A145), (A146) and (A147) (or (A152), (A154)) into (A143), and using the definition (4.10), we have \( \lim_{N \to \infty} \Delta \geq R_r = \min \{I(X_1; Z|U, V), I(X_1; Y)\} + I(V; Y|U, X_1) - I(X_1, V; Z|U) \). The proof of case 1 is completed.

**Proof of** \( \lim_{N \to \infty} \Delta \geq R_r = I(V; Y|U, X_1) - I(V; Z|U, X_1) \) **for the case 2:**
\[
H(W_1|Z^N) \geq H(W_1|Z^N, U^N, X_1^N)
= H(W_{10}, W_{11}|Z^N, U^N, X_1^N)
\stackrel{(a)}{=} H(W_{11}|Z^N, U^N, X_1^N)
= H(W_{11}, Z^N|U^N, X_1^N) - H(Z^N|U^N, X_1^N)
= H(W_{11}, Z^N, V^N|U^N, X_1^N) - H(V^N|W_{11}, Z^N, U^N, X_1^N) - H(Z^N|U^N, X_1^N)
\geq H(V^N|U^N, X_1^N) + H(Z^N|V^N, U^N, X_1^N) - H(V^N|W_{11}, Z^N, U^N, X_1^N)
\]
\[
- H(Z^N|U^N, X_1^N)
\stackrel{(b)}{=} H(V^N|U^N) + H(Z^N|V^N, U^N, X_1^N) - H(V^N|W_{11}, Z^N, U^N, X_1^N)
- H(Z^N|U^N, X_1^N)
= H(V^N|U^N) - I(Z^N; V^N|U^N, X_1^N) - H(V^N|W_{11}, Z^N, U^N, X_1^N),
\tag{A155}
\]
where (a) follows from the fact that given \(U^N, W_{10}\) is uniquely determined, and (b) is from that \(X_1^N\) is independent of \(V^N\) and \(U^N\).

For the first term in (A155), the codeword generation ensures that
\[
H(V^N|U^N) \geq \log 2^{N(L_{21}+L_{22})} - \delta_1 = NI(V; Y|U, X_1) - \delta_1,
\tag{A156}
\]
where \(\delta_1\) is small for sufficiently large \(N\).

For the second term in (A155), using the same approach as that in \([20\text{ Lemma 3}]\), we get
\[
I(Z^N; V^N|U^N, X_1^N) \leq N(I(V; Z|U, X_1) + \epsilon''),
\tag{A157}
\]
where \(\epsilon'' \to 0\) as \(N \to \infty\).

Now, we consider the last term of (A155).

- For the case that \(R_{11} \leq L_{21} + L_{22}\), given \(U^N, X_1^N\) and \(W_{11}\), the total number of possible codewords of \(V^N\) is
\[
N_1 \leq 2^{NL_{22}} = 2^{N I(V; Z|U, X_1)}.
\tag{A158}
\]

By using the Fano’s inequality and (A158), we have
\[
H(V^N|W_{11}, Z^N, U^N, X_1^N) \leq N \epsilon''',
\tag{A159}
\]
where \(\epsilon''' \to 0\).

- For the case that \(L_{21} + L_{22} \leq R_{11} \leq L_{21} + L_{22} + L_{23}\), given \(U^N, X_1^N\) and \(W_{11}\), \(V^N\) is totally determined, and therefore
\[
H(V^N|W_{11}, Z^N, U^N, X_1^N) = 0.
\tag{A160}
\]
Substituting (A156), (A157) and (A159) (or (A160)) into (A155), and using the definition (4.10), we have 
\[ \lim_{N \to \infty} \Delta \geq R_e = I(V; Y|U, X_1) - I(V; Z|U, X_1). \]
The proof of case 2 is completed.

The proof of Theorem 11 is completed.

APPENDIX F
PROOF OF THEOREM 12

Theorem 12 is proved by the following two cases.

- **(Case 1)** If \( I(X_1; Y) \geq I(X_1; Z|U) \), we allow receiver 1 to decode \( x_1^N \), and receiver 2 can not decode it.
- **(Case 2)** If \( I(X_1; Y) \leq I(X_1; Z) \), we allow both the receivers to decode \( x_1^N \).

1) Letting \( V_2 = \text{const} \) and removing \( R_{e2} \), the proof of case 1 is along the lines of the proof of Theorem 4 and therefore, the proof is omitted here.

2) By allowing both receivers to decode the relay codeword \( x_1^N \), the proof of case 2 is directly obtained from the proof of Theorem 4 and the proof of case 2 in Theorem 11, thus, the proof is omitted here.

The proof of Theorem 12 is completed.

REFERENCES

[1] C. E. Shannon, “Communication theory of secrecy systems,” *The Bell System Technical Journal*, vol. 28, pp. 656-714, 1949.

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

[3] 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.

[4] N. Merhav, “Shannon’s secrecy system with informed receivers and its application to systematic coding for wiretapped channels,” *IEEE Trans Inf Theory*, special issue on Information-Theoretic Security, vol. IT-54, no. 6, pp. 2723-2734, June 2008.

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

[6] L. Lai, H. El Gamal and V. Poor, “The wiretap channel with feedback: encryption over the channel,” *IEEE Trans Inf Theory*, vol. IT-54, pp. 5059-5067, 2008.

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

[8] C. Mitrpanit, A. J. Han Vinck and Y. Luo, “An Achievable Region for the Gaussian Wiretap Channel with Side Information,” *IEEE Trans Inf Theory*, vol. IT-52, no. 5, pp. 2181-2190, 2006.

[9] Y. Chen, A. J. Han Vinck, “Wiretap channel with side information,” *IEEE Trans Inf Theory*, vol. IT-54, no. 1, pp. 395-402, January 2008.

[10] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, “Compound wiretap channels,” in *Proceedings of the 45th Annual Allerton Conference on Communication, Control and Computing*, USA, 2007.

[11] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, “Recent results on compound wiretap channels,” in *Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, France, 2008.

[12] T. Liu, V. Prabhakaran, and S. Vishwanath, “The secrecy capacity of a class of parallel Gaussian wiretap channels,” in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Canada, 2008.

[13] A. Khisti, A. Tchamkerten, and G. Wornell, “Secure broadcasting,” *IEEE Trans Inf Theory*, vol. IT-54, pp. 2453-2469, 2008.

[14] P. Wang, G. Yu, and Z. Zhang, “On the secrecy capacity of fading wireless channel with multiple eavesdroppers,” in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, France, 2007.
[15] H. Yamamoto, “Coding theorem for secret sharing communication systems with two noisy channels,” IEEE Trans Inf Theory, vol. IT-35, pp. 572-578, 1989.
[16] H. Yamamoto, “A coding theorem for secret sharing communication systems with two Gaussian wiretap channels,” IEEE Trans Inf Theory, vol. IT-37, pp. 634-638, 1991.
[17] M. Cagalj, S. Capkun, and J. P. Hubaux, “Key agreement in peer-to-peer wireless networks,” Proceedings of the IEEE, vol. IT-94, pp. 467-478, 2006.
[18] N. Cai, A. Winter, and R. W. Yeung, “Quantum privacy and quantum wiretap channels,” Problems of Information Transmission, vol. 94, no. 4, pp. 318-336, 2004.
[19] N. Cai, and R. W. Yeung, “Secure network coding,” in Proceedings of the IEEE International Symposium on Information Theory (ISIT), 2002.
[20] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” IEEE Trans Inf Theory, vol. IT-24, no. 3, pp. 572-578, 1978.
[21] 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.
[22] 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.
[23] 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.
[24] 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.
[25] 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.
[26] 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.
[27] 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.
[28] 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.
[29] 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.
[30] Y. Oohama, “Coding for relay channels with confidential messages,” in Proceedings of IEEE Information Theory Workshop, Australia, 2001.
[31] E. Ekrem and S. Ulukus, “Secrecy in cooperative relay broadcast channels,” IEEE Trans Inf Theory, vol. IT-57, pp. 137-155, 2011.
[32] 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.
[33] Y. Liang, H. V. Poor and S. Shamai, “Secure communication over fading channels,” IEEE Trans Inf Theory, vol. IT-54, pp. 2470-2492, 2008.
[34] C. Nair and A. El Gamal, “An outer bound to the capacity region of the broadcast channel,” IEEE Trans Inf Theory, vol. IT-53, pp. 350-355, 2007.
[35] T. M. Cover and A. El Gamal, “Capacity theorems for the relay channel,” IEEE Trans Inf Theory, vol. IT-25, pp. 572-584, 1979.
[36] K. Marton, “A coding theorem for the discrete memoryless broadcast channel,” IEEE Trans Inf Theory, vol. IT-25, pp. 306-311, 1979.
[37] I. Csiszár and J. Körner, Information Theory. Coding Theorems for Discrete Memoryless Systems. London, U.K.: Academic, 1981.
[38] A. A. El Gamal and E. C. van der Meulen, “A proof of Marton’s coding theorems for the discrete memoryless broadcast channel,” IEEE Trans Inf Theory, vol. IT-27, pp. 120-122, 1981.
[39] S. Lall, “Advanced Topics in Computation for Control,” Lecture Notes for Engr210b at Stanford University. Stanford, CA.