Entropy **2014**, *16*, 1819-1841; doi:10.3390/e16031819

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Article

A Hybrid Cooperative Coding Scheme for the Relay-Eavesdropper Channel

Peng Xu [1,*], Zhiguo Ding [2] and Xuchu Dai [1]

[1] Department of Electronic Engineering and Information Science, University of Science and Technology of China, P.O.Box No.4, 230027, Hefei, Anhui, China; E-Mail: daixc@ustc.edu.cn

[2] School of Electrical, Electronic, and Computer Engineering, Newcastle University, Newcastle, NE1 7RU, UK; E-Mail: Zhiguo.Ding@newcastle.ac.uk

* Author to whom correspondence should be addressed; E-Mail: mxp484@mail.ustc.edu.cn; Tel.: +86-15056955356.

Received: 16 December 2013; in revised form: 18 March 2014 / Accepted: 19 March 2014 / Published: 24 March 2014

Abstract: This paper considers the four-node relay-eavesdropper channel, where a relay node helps the source to send secret messages to the destination in the presence of a passive eavesdropper. For the discrete memoryless case, we propose a hybrid cooperative coding scheme, which is based on the combination of the partial decode-forward scheme, the noise-forward scheme and the random binning scheme. The key feature of the proposed hybrid cooperative scheme is that the relay integrates the explicit cooperation strategy and the implicit cooperation strategy by forwarding source messages and additional interference at the same time. The derived achievable secrecy rate shows that some existing works can be viewed as special cases of the proposed scheme. Then, the achievable secrecy rate is extended to the Gaussian channel based on Gaussian codebooks, and the optimal power policy is also identified in the high power region. Both the analysis and numerical results are provided to demonstrate that the proposed hybrid cooperative coding scheme outperforms the comparable ones, especially in the high power region.

Keywords: information-theoretic secrecy; relay-eavesdropper channel; partial decode-forward; noise-forward

---

1. Introduction

The concept of information theoretic secrecy was first introduced by Shannon in [1], where a key is used to protect confidential messages over noiseless transmissions. When considering the noisy transmission, Wyner introduced the wiretap channel in [2], where the received signal at the eavesdropper was assumed to be a degraded version of the signal at the legitimate receiver. Csiszár and Körner extended this degraded wiretap channel to a more general broadcast channel with confidential messages and found the secrecy capacity in [3]. Wyner's channel has also been extended to the wiretap channel with side information, where the side information was assumed to be non-casually known to the transmitter [4,5]. Recently, secrecy problems have been considered in various multi-user setups. For example, multiple access channels (MACs) were studied in [6–9], where an external eavesdropper was introduced in [6,7], while each legitimate user in [8,9] acted as an eavesdropper for the messages intended to the other users. Broadcast channels (BCs) were considered in [10,11], where each user is also an eavesdropper for the messages intended to the others. Relay channels were studied in [12–17], where an external eavesdropper was introduced in [12–15], while the relay node in [16,17] was an untrusted helper, *i.e.*, this untrusted helper also acted as an eavesdropper to the main receiver.

Since user cooperation can potentially enhance the security, many existing works have designed cooperative secure transmission schemes for multi-user networks. These existing cooperation schemes can be divided into two different types: the explicit cooperation strategy and the implicit cooperation strategy. The explicit cooperation strategy means that the helper nodes send messages that are correlated to the intended messages, such as the decode-forward (DF) scheme [12] or the partial DF [13] for relay-eavesdropper channels. The implicit cooperation strategy requires helper nodes to send interference messages that are independent of the intended messages, such as cooperative jamming (CJ) [6], noise-forward (NF) [12] and the interference-assisted scheme [14].

Different from these works in [6,12–14] that consider these two types of cooperation strategies separately, this paper aims to design a hybrid cooperative coding scheme that integrates the explicit cooperation strategy and the implicit cooperation strategy together. Most recently, hybrid cooperative coding schemes have been considered in [7,15] for the MAC channel with conference and secrecy constraints. Compared to the works in [7,15], which are based on an assumption that there exist secret communication links between a source and its helper partner, the proposed hybrid cooperative coding scheme is applicable to a more practical relay-eavesdropper channel in which the transmissions from the source to the relay can be overheard by the eavesdropper.

The contributions of the this paper can be summarized as follows. Firstly, we propose a hybrid cooperative coding scheme for the four-node relay-eavesdropper channel, where a relay node helps the source to send secret messages to the destination in the presence of a passive eavesdropper. The basic idea is to combine the partial DF scheme [18] for relay channels, the NF [12] scheme for relay-eavesdropper channels and random binning [2] for wiretap channels. Note that the NF and random binning schemes can provide useful randomness to protect the secret messages. The key feature of the proposed hybrid cooperative scheme is that the relay integrates the explicit cooperation strategy and the implicit cooperation strategy by forwarding source messages and additional interference at the same time. The derived achievable secrecy rate shows that the proposed scheme generalizes some existing

works, such as the DF [12], partial DF [13] and NF [12] schemes for relay-eavesdropper channels. Secondly, the achievable rate result is extended to the memoryless Gaussian channel based on Gaussian codebooks. Then, the optimal power policy is developed for the proposed scheme in the high power region, and the result shows that the secrecy rate achieved by the proposed scheme can be sufficiently large in the high power region, even if the source-relay link is weak. This is benefited from the fact that the interference generated at the relay can protect the transmissions from the source to the relay by confusing the eavesdropper. Finally, we illustrate the proposed scheme through some examples of the Gaussian network topologies. The numerical results show that our scheme outperforms the comparable ones, especially when the transmit power is large.

In the following, the details about the differences between the proposed scheme and the existing ones are provided in order to further highlight the contribution of this paper.

- The channel model and the coding scheme developed in [19] are fundamentally different from those in this paper. First, the work in [19] considers the relay-eavesdropper channel model with parallel subchannels, whereas this paper considers the relay-eavesdropper channel model with only a single communication channel. Second, the coding scheme in [19] uses a subset of channels to perform the DF scheme and the remaining ones to perform the NF scheme, and the interaction between these two relaying schemes exists only across different subchannels. In contrary, by using the superposition coding scheme, the partial DF and NF schemes in the proposed coding scheme are strongly connected to each other in the same channel.

- The work in [20] combined partial DF, NF and compress-and-forward (CF) schemes for the discrete memoryless relay-eavesdropper channel. In Section 3.4, we will show that the use of the CF scheme does not offer any performance gains in terms of the secrecy rate. Compared to the scheme in [20] that is based on the successive decoding strategy for separately decoding different messages, the proposed scheme utilizes the backward decoding strategy to jointly decode the common part (known by both the source and relay) of the source messages. Moreover, the proposed scheme decodes the interference messages from the relay after decoding the common part of the source messages, whereas the scheme in [20] decodes these two types of messages in a reversed order. This results in different secrecy rates achieved by these two coding schemes, and their performances will be compared in detail in Section 3.4.

The rest of this paper is organized as follows. In Section 2, the notations, the channel model and the main result are given for the discrete memoryless relay-eavesdropper. Section 3 extends the main result to the Gaussian case, for which an achievable secrecy rate, a power policy in the high power region and some numerical results are provided. The achievable secrecy rate associated with the proposed hybrid coding scheme for the discrete memoryless relay-eavesdropper channel is established in Section 4. Finally, conclusions are provided in Section 5.

2. System Model and Achievable Secrecy Rate

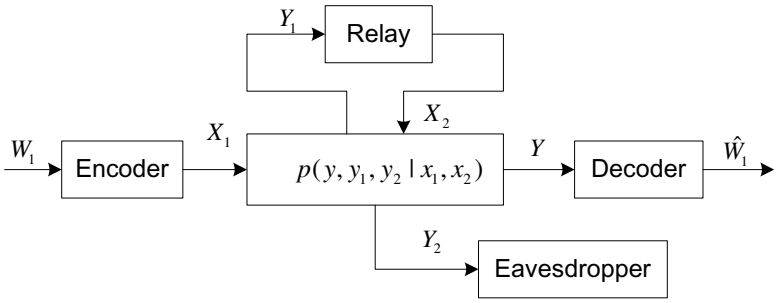
2.1. Notations

Throughout this paper, a random variable, its realization and its finite alphabet are denoted with an upper case letter (e.g., X), the corresponding lower case letter (e.g., x) and the corresponding calligraphic letter (e.g., $\mathcal{X}$), respectively. The probability distribution of the random variable, X, is denoted as $p(x) = p_X(x)$ for simplicity, where $x \in \mathcal{X}$. Furthermore, we use $\mathbf{X}^n$ to denote a random n-vector $(X_1, \cdots, X_n)$ and use $\mathbf{x}^n = (x_1, \cdots, x_n)$ to denote a specific n-vector value in $\mathcal{X}^n$, which is the n-th Cartesian power of $\mathcal{X}$.

Moreover, let $\mathbf{X}^i$ and $\mathbf{X}(]i[)$ denote the set $\{X(j), 1 \leq j < i\}$ and the set $\{X(j), 1 \leq j < i \text{ or } i < j \leq n\}$, respectively. In addition, $[1 : B] = \{1, 2, \cdots, B\}$, $[x]^+ = \max\{x, 0\}$, $C(x) = \frac{1}{2}\log(1 + x)$, and ϵ_k is arbitrarily small positive number for $\forall k$. Finally, $\mathcal{A}_\epsilon^{(n)}(X_1, X_2)$ denotes the set of jointly typical n-sequences with respect to $p(x_1, x_2)$ (more details can be seen in [21]).

2.2. Discrete Memoryless Relay-Eavesdropper Channel

Figure 1. Relay-eavesdropper channel.



As shown in Figure 1, this paper considers a four-node discrete memoryless channel, where the source (X_1) wishes to send a message $W_1 \in \mathcal{W}_1 = \{1, \cdots, M\}$ to the destination (Y), while keeping it secret from an external eavesdropper (Y_2), with the help of a full duplex relay node, (X_2, Y_1). This channel is first introduced in [12], termed as the relay-eavesdropper channel, which consists of a transition probability distribution $(\mathcal{X}_1 \times \mathcal{X}_2, p(y, y_1, y_2|x_1, x_2), \mathcal{Y} \times \mathcal{Y}_1 \times \mathcal{Y}_2)$. Here, the finite sets, $\mathcal{X}_1$, $\mathcal{X}_2$, denote the input alphabets at the source and the relay, respectively, while the finite sets, $\mathcal{Y}$, $\mathcal{Y}_1$, $\mathcal{Y}_2$, denote the output alphabets at the destination, the relay and the eavesdropper, respectively. The (M, n, P_e^n) code of this system consists of a stochastic encoder, f_1, at the source that maps the message, W_1, into a codeword, $X_1^n \in \mathcal{X}_1^n$, a stochastic encoder, f_2, at the relay that maps its received signals $(Y_{1,1}, \cdots, Y_{1,i-1})$ before time i into a channel input, $X_{2,i}$, and a decoding function $\phi : \mathcal{Y}^n \to W_1$. The average error probability is:

$$P_e^n = \frac{1}{M} \sum_{w_1 \in \mathcal{W}_1} Pr(\phi(\mathbf{Y}^n) \neq w_1 | w_1 \text{ was sent}). \tag{1}$$

The secrecy level is measured by the equivocation rate $(1/n)H(W_1|\mathbf{Y}_2^n)$. A prefect secrecy rate, R_s, is said to be achievable if for any $\epsilon > 0$, there exists a sequence of codes (M, n, P_e^n), such that:

$$M \geq 2^{nR_s},\ P_e^n \leq \epsilon$$
$$R_s - \epsilon \leq \frac{1}{n} H(W_1|\mathbf{Y}_2^n). \tag{2}$$

2.3. Achievable Secrecy Rate

Before the presentation of our main result, we first define some parameters as follows.

Definition 1. *Let $\mathcal{P}$ denote the set of all the joint distributions of the random variables $(U, V_1, X_1, X_2, Y_1, Y_2)$ that factor as:*

$$p(u, v_1, x_1, x_2, y, y_1, y_2) = p(u)p(x_1, v_1|u)p(x_2|u)p(y, y_1, y_2|x_1, x_2). \tag{3}$$

In this definition, one can observe that $(V_1, X_1) - U - X_2$ is a Markov chain, where U represents the common message known by the source and the relay. Conditioned on U, (V_1, X_1) and X_2 can be generated at the source and the relay, respectively.

Definition 2. *For a given $p \in \mathcal{P}$, define two rates, $R_{11}(p)$ and $R_{12}(p)$, as:*

$$\begin{aligned} R_{11}(p) \triangleq & I(X_1; Y|X_2, U, V_1) + \min\{I(X_2; Y|U, V_1), I(X_2; Y_2|U, X_1)\} \\ & - \min\{I(X_2; Y|U, V_1), I(X_2; Y_2|U, V_1)\} - I(X_1; Y_2|U, V_1, X_2), \end{aligned} \tag{4}$$
$$R_{12}(p) \triangleq \min\{I(U, V_1; Y), I(V_1; Y_1|X_2, U)\} - I(U, V_1; Y_2). \tag{5}$$

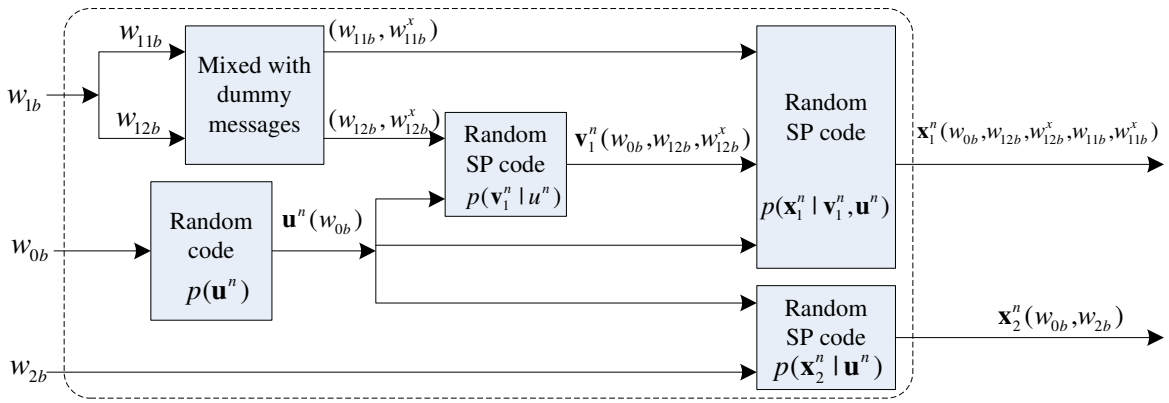
Note that $R_{11}(p)$ is the rate of the private secret message at the source that is not known by the relay, while $R_{12}(p)$ is the rate of the common secret message that is known by the source and the relay.

Based on the above definitions, the following theorem gives an achievable secrecy rate for the discrete memoryless relay-eavesdropper channel.

Theorem 1. *For the considered relay-eavesdropper channel, the following secrecy rate is achievable.*

$$R_s = \max_{p \in \mathcal{P}} \quad R_{11}(p) + R_{12}(p). \tag{6}$$

Figure 2. The encoder structure in Block b, $2 \leq b \leq B$, where the common message $w_{0b} = (w_{12b-1}, w_{12b-1}^x)$, which is transmitted by the source in the previous block, and "SP" is the abbreviation of the word "superposition".



Proof. The proposed achievable scheme is based on the careful combination of the partial DF [18] scheme for relay channels, the NF scheme [12] for relay-eavesdropper channels and random binning for wiretap channels [2]. Specifically, the proposed coding scheme integrates some essential techniques, such as rate splitting, superposition Markov block encoding [18] (Theorem 7), random binning [2], backward decoding and interference injecting [12], *etc*. In the following, we will outline the proposed hybrid cooperative coding scheme, and the details of the complete proof will be provided in Section 4. (Note that in the next paragraph, a message is said to be a common message if it has been known by both the source and the relay in a certain block, such as w_{0b} in Block b. Otherwise, it is said to be a private message, such as w_{11b} and w_{2b}, which are only known by the source and the relay, respectively.)

Briefly speaking, for a given joint distribution, $p \in \mathcal{P}$, the whole transmission duration is formed by B Markov blocks, in which $B-1$ secret messages will be sent. At Block b, the new secret message, w_{1b}, is first split into two parts: one part needs to be transmitted directly from the source to the destination (w_{11b}); and the other part needs to be decoded by the relay (w_{12b}). Here w_{11b} and w_{12b} are mixed with dummy messages w^x_{11b} and w^x_{12b}, respectively. In the encoding process, the random variable, U, in Theorem 1 represents the common message $w_{0b} = (w_{12b-1}, w^x_{12b-1})$. Note that w_{0b} was decoded by the relay at the end of the previous block, *i.e.*, Block $b-1$, and becomes the common message in this block. The random variable, V_1, represents the superposition code in which the new message (w_{12b}, w^x_{12b}) is superimposed on the common message, w_{0b}, where (w_{12b}, w^x_{12b}) needs to be decoded by the relay at the end of Block b and will become the common message, w_{0b+1}, in Block $b+1$. In this sense, V_1 also carries the common part of the source message, but for the next block. The channel input, X_1, represents the superposition code in which the private message (w_{11b}, w^x_{11b}) is superimposed on w_{0b} and (w_{12b}, w^x_{12b}). At the same block, noise injection is realized at the relay via sending the so-called "interference message", w_{2b}, *i.e.*, the relay randomly generates a private interference message, w_{2b}, in order to confuse the eavesdropper. The channel input, X_2, represents the superposition code in which the interference message, w_{2b}, is superimposed on the common message, w_{0b}, where w_{0b} has been decoded by the relay at the end of the previous block. The encoder structure of the proposed cooperative coding scheme is briefly illustrated in Figure 2.

□

Remark 1. *Since the relay simultaneously forwards the common part of the source messages and private interference, the proposed scheme can be viewed as a hybrid cooperative scheme that combines the explicit and implicit cooperation strategies. The key feature of such a hybrid cooperative scheme is that it can improve the signal strength through the main channel and suppress the eavesdropping capability at the same time.*

Remark 2. *The use of the channel prefixing technique (e.g., Appendices B and C in [12]) may further increase the secrecy rate. However, we do not consider this technique in this paper to avoid the intractability of its evaluation, which simplifies the achievable result in Theorem 1.*

The achievable secrecy rate in Theorem 1 generalizes some existing coding schemes for the relay eavesdropper channels.

Remark 3. *If we set $X_1 = V_1$ and $X_2 = U$ in Equations (4) and (5), Theorem 1 reduces to:*

$$R_s = \max_{p(x_1,x_2)} \min\{I(X_1, X_2; Y), I(X_1; Y_1|X_2)\} - I(X_1, X_2; Y_2), \tag{7}$$

which is consistent with the secrecy rate achieved by the DF scheme in [12] (Theorem 2).

Remark 4. *If we set $U = V_1 = \emptyset$ in Equations (4) and (5), Theorem 1 reduces to:*

$$R_s = \max_{p(x_1)p(x_2)} I(X_1;Y|X_2) + \min\{I(X_2;Y), I(X_2;Y_2|X_1)\} - \min\{I(X_2;Y), I(X_2;Y_2)\} - I(X_1;Y_2|X_2), \quad (8)$$

which is consistent with the secrecy rate achieved by the NF scheme in [12] (Theorem 3).

Remark 5. *If we set and $U = X_2$, Theorem 1 reduces to:*

$$R_s = \max_{p(v_1,x_1,x_2)} \min\{I(X_1,X_2;Y), I(X_1;Y|X_2,V_1) + I(V_1;Y_1|X_2)\} - I(X_1,X_2;Y_2), \quad (9)$$

which is consistent with the secrecy rate achieved by the partial DF scheme in [13] (Theorem 8).

3. Gaussian Relay-Eavesdropper Channel

In this section, the memoryless Gaussian relay-eavesdropper channel is considered, where the received symbols at the relay (Y_1), the destination (Y) and the eavesdropper (Y_2) are:

$$\begin{aligned} Y_1 &= h_{sr}X_1 + N_1, \\ Y &= h_{sd}X_1 + h_{rd}X_2 + N, \\ Y_2 &= h_{se}X_1 + h_{re}X_2 + N_2. \end{aligned} \quad (10)$$

Here, $N_1, N, N_2 \sim \mathcal{N}(0,1)$, which are the Gaussian adaptive noises; $h_{\alpha\beta}$ denotes the channel coefficient between node $\alpha \in \{s,r\}$ and node $\beta \in \{r,d,e\}$, $\alpha \neq \beta$. The average power constraints at the source and the relay are P_1 and P_2, respectively.

3.1. Achievable Secrecy Rate

In this subsection, we use a joint Gaussian distribution to get an achievable secrecy rate.

We let $U, V_{1,0}, X_{1,0}, X_{2,0} \sim \mathcal{N}(0,1)$, and they are independent of each other. Then ,the variables, V_1, X_1 and X_2, are set to be:

$$V_1 = \sqrt{P_1^u}U + \sqrt{P_1^{v_0}}V_{1,0}, \quad (11)$$

$$X_1 = V_1 + \sqrt{P_1^{x_0}}X_{1,0}, \quad (12)$$

$$X_2 = r\sqrt{P_2^u}U + \sqrt{P_2^{x_0}}X_{2,0}, \quad (13)$$

where $r \in \{-1,1\}$, which is used to determine the covariance of the channel inputs, X_1 and X_2, to be positive or negative. In these relationships, U represents the common message shared by both the source and the relay in a certain block; $V_{1,0}$ represents the new source message that needs to be decoded by the relay and will become the common message in the next block; $X_{1,0}$ represents the private source message; $X_{2,0}$ represents the private interference message at the relay.

To satisfy the power constraints, we require the power tuple $\mathbf{A} = (P_1^u, P_1^{v_0}, P_1^{x_0}, P_2^u, P_2^{x_0})$ in Equations (11)–(13) to lie in $\mathcal{A}$, where $\mathcal{A}$ denotes the power allocation set that is given by:

$$\begin{aligned}\mathcal{A} = \{(P_1^u, P_1^{v_0}, P_1^{x_0}, P_2^u, P_2^{x_0}) | P_1^u, P_1^{v_0}, P_1^{x_0}, P_2^u, P_2^{x_0} \geq 0 \\ P_1^u + P_1^{v_0} + P_1^{x_0} \leq P_1,\ P_2^u + P_2^{x_0} \leq P_2\}.\end{aligned} \tag{14}$$

Now, based on Theorem 1 and the above definitions, an achievable secrecy rate is given in the following lemma.

Lemma 1. *For the Gaussian relay-eavesdropper channel, the following secrecy rate is achievable:*

$$R_s^G = \max_{r=\pm 1, \mathbf{A}\in\mathcal{A}} R_{11}^G(r, \mathbf{A}) + R_{12}^G(r, \mathbf{A}), \tag{15}$$

where $R_{11}^G(r, \mathbf{A})$ *and* $R_{12}^G(r, \mathbf{A})$ *are defined as:*

$$\begin{aligned}R_{11}^G(r, \mathbf{A}) =& C(|h_{sd}|^2 P_1^{x_0}) + \min\left\{C\left(\frac{|h_{rd}|^2 P_2^{x_0}}{1+|h_{sd}|^2 P_1^{x_0}}\right), C\left(|h_{re}|^2 P_2^{x_0}\right)\right\} \\ &- \min\left\{C\left(\frac{|h_{rd}|^2 P_2^{x_0}}{1+|h_{sd}|^2 P_1^{x_0}}\right), C\left(\frac{|h_{re}|^2 P_2^{x_0}}{1+|h_{se}|^2 P_1^{x_0}}\right)\right\} - C(|h_{se}|^2 P_1^{x_0}),\end{aligned} \tag{16}$$

$$\begin{aligned}R_{12}^G(r, \mathbf{A}) =& \min\left\{C\left(\frac{|h_{sd}\sqrt{P_1^u} + r h_{rd}\sqrt{P_2^u}|^2 + |h_{sd}|^2 P_1^{v_0}}{1+|h_{sd}|^2 P_1^{x_0} + |h_{rd}|^2 P_2^{x_0}}\right), C\left(\frac{|h_{sr}|^2 P_1^{v_0}}{1+|h_{sr}|^2 P_1^{x_0}}\right)\right\} \\ &- C\left(\frac{|h_{se}\sqrt{P_1^u} + r h_{re}\sqrt{P_2^u}|^2 + |h_{se}|^2 P_1^{v_0}}{1+|h_{se}|^2 P_1^{x_0} + |h_{re}|^2 P_2^{x_0}}\right).\end{aligned} \tag{17}$$

Proof. We calculate each piece of mutual information in Equations (4) and (5) using the variables defined in Equations (11)–(13), and this lemma can be proven. □

3.2. Power Policy in the High Power Region

According to the achievable secrecy rate in Lemma 1, the following lemma takes an example to illustrate how to allocate the transmit powers at the source and the relay in the high power region.

Lemma 2. *Let* $a = \frac{|h_{se}|^2}{|h_{sd}|^2}$, $b = \frac{|h_{rd}|^2}{|h_{re}|^2}$, $c = \frac{|h_{sr}|^2}{|h_{sd}|^2}$, *and assume* $P_1 = P_2 = P$ *for simplicity. When* $P \to \infty$, $c > 0$ *and* $b \neq \frac{1}{a}$, *the optimal power allocation for Equation* (15) *satisfies:*

$$(P_1^u, P_1^{v_0}, P_1^{x_0}, P_2^u, P_2^{x_0}) \doteq (P^1, P^{\frac{1}{2}}, P^0, P^1, P^{\frac{1}{2}}), \tag{18}$$

where $f(x) \doteq x^y$ *denotes that* $f(x)$ *is exponentially equal to* x^y, *i.e.,* $\lim_{x\to\infty} \frac{\log f(x)}{\log x} = y$ ($\dot{\leq}$ *and* $\dot{\geq}$ *are defined similarly).*

Proof. Refer to Appendix A. □

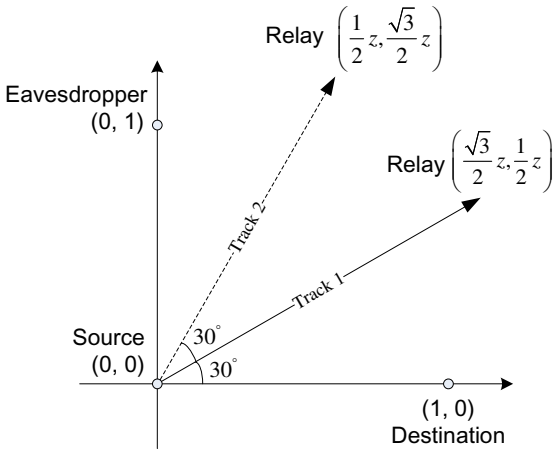
According to this power policy and the derivations in Appendix A, the achievable secrecy rate in Lemma 1 satisfies:

$$\lim_{P\to\infty} \frac{R_s^G}{\log P} = \frac{1}{4}. \tag{19}$$

The above relationship reflects that the achievable secrecy rate, R_s^G, is arbitrarily large as $P \to \infty$.

Remark 6. *Since we have only required the source-relay channel gain to be positive (i.e., $c > 0$) in Lemma 2, it shows that the proposed hybrid cooperative scheme can achieve a sufficiently large secrecy rate even for a weak source-relay channel (i.e., c is small). This is because the interference at the relay with the power, $P_2^{x_0}$, can protect the transmissions from the source to the relay by confusing the eavesdropper. In this case, the bottleneck of the source-relay channel (i.e., h_{sr}) suffered by the DF scheme ([12]) and partial DF scheme ([13]) can be greatly mitigated by introducing the interference at the relay node, and the proposed hybrid cooperative scheme can efficiently overcome the bottleneck of the source-relay channel.*

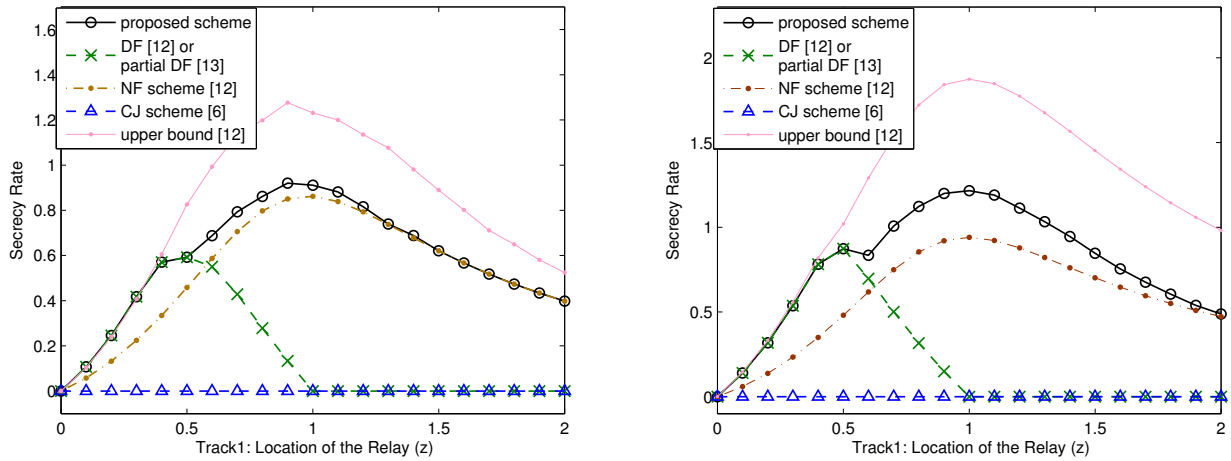
Figure 3. The considered Gaussian network topology.



3.3. Numerical Results

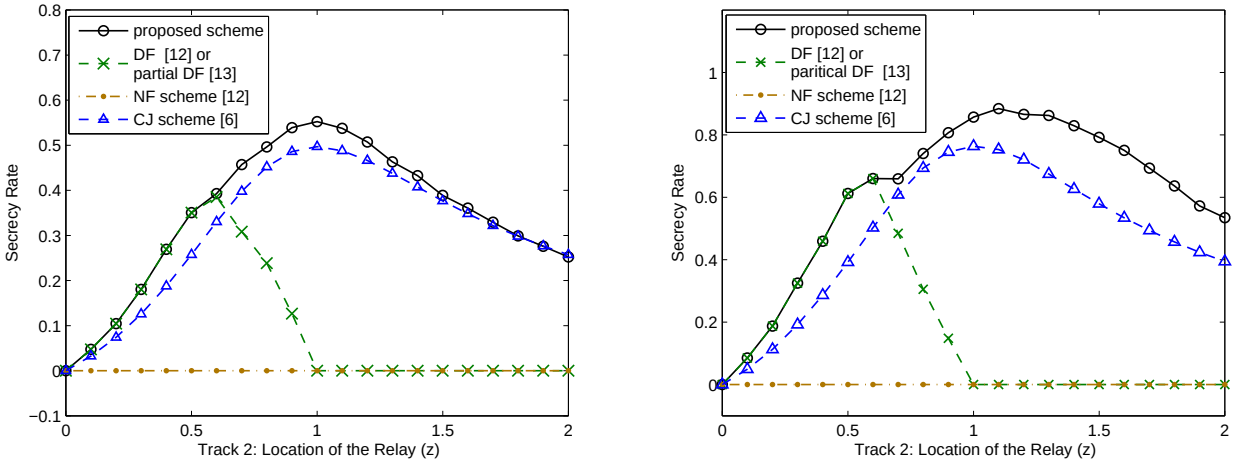
In this subsection, we will provide some numerical results to demonstrate the performance of the proposed hybrid cooperative scheme. Specifically, in the Gaussian relay-eavesdropper channel (10), the channel gain between node $\alpha \in \{s, r\}$ and node $\beta \in \{r, d, e\}$ ($\alpha \neq \beta$) is $h_{\alpha\beta} = d_{\alpha\beta}^{-\gamma/2}$. Here, $d_{\alpha\beta}$ is the distance between α and β and γ is the path loss exponent, which is set as $\gamma = 2$. Based on these definitions, we use the network geometry shown in Figure 3, where the source, the destination and the eavesdropper are located at (0,0), (1,0) and (0,1), respectively. In addition, the relay is located at $(\frac{\sqrt{3}}{2}z, \frac{1}{2}z)$ in Track 1 and $(\frac{1}{2}z, \frac{\sqrt{3}}{2}z)$ in Track 2, where $z > 0$. When the relay is in Track 1, it is nearer to the destination than to the eavesdropper; when the relay is in Track 2, it is nearer to the eavesdropper than to the destination. To show the performance of the proposed coding scheme, the DF scheme in [12], the partial DF scheme in [13], the NF scheme in [12] and the CJ scheme in [6] are taken to be the comparable ones. Note that when considering the network geometry in Figure 3, one will see that the DF scheme [12] achieves exactly the same secrecy rate as that of the partial DF scheme [13]. In computing the upper bound, following the same parameter setting in [12], we have used the upper bound in [12] (Theorem 1) using Gaussian inputs for the ease of computation. As discussed in [12], Gaussian inputs are not necessarily optimal for the upper bound.

Figure 4. Achievable secrecy rates of various coding schemes *versus* the location of the relay (*i.e.*, the value of z), where the relay is in Track 1.



(a) $P_1 = 10$, $P_2 = 20$ (b) $P_1 = 100$, $P_2 = 200$

Figure 5. Achievable secrecy rates of various coding schemes *versus* the location of the relay (*i.e.*, the value of z), where the relay is in Track 2.



(a) $P_1 = 10$, $P_2 = 20$ (b) $P_1 = 100$, $P_2 = 200$

Figure 4 shows that achievable secrecy rates achieved the proposed scheme and the comparable ones for the case that the relay is in Track 1. In the first sub-figure, *i.e.*, Figure 4a, we consider the moderate transmit power pair $(P_1, P_2) = (10, 20)$. From this sub-figure, one can see that the DF scheme [12] (or the partial DF scheme [13]) can only perform well when the relay is very near to the source (*i.e.*, z is small). However, the proposed hybrid cooperative scheme with artificial interference can still perform well when the relay is not near the source (*i.e.*, z is large). When $0 < z < 1.3$, the proposed scheme can achieve an exactly larger secrecy rate in comparison with the NF scheme [12]. Interestingly, the proposed scheme can still outperform the NF scheme when $1 < z < 1.3$, which means that partially

decoding the source message at the relay is useful, even if $h_{sr} < h_{se}$. This is because the interference at the relay can protect the transmissions from the source to the relay by confusing the eavesdropper. When $z > 1.3$, the proposed scheme reduces to the NF scheme, and the relay should not decode any source message in this case. In the second sub-figure, *i.e.*, Figure 4b, we consider the high transmit power pair $(P_1, P_2) = (100, 200)$. From this sub-figure, one can see that the performance gain between the proposed scheme and each comparable one is enlarged. This is because the performance of the proposed scheme can be greatly enhanced when the transmit powers at the source and the relay increase, as shown in Lemma 2 and Remark 6.

Figure 5 shows the achievable secrecy rates achieved by the proposed scheme and the comparable ones for the case that the relay is in Track 2. Figure 5a,b also considers the moderate power pair $(P_1, P_2) = (10, 20)$ and the high power pair $(P_1, P_2) = (100, 200)$, respectively. Since the relay is nearer the eavesdropper in Track 2, the NF scheme is invalid. In this case, the CJ scheme [6] can achieve a positive secrecy rate, since the artificial noise at the relay harms the eavesdropper more than it harms the destination. However, the achievable secrecy rate of the CJ scheme is bounded even at high transmit power, as shown in [14]. To the contrary, the achievable secrecy rate of the proposed scheme is unbounded at high transmit power, as shown in Equation (19) and Remark 6. This is mainly because the interference at the relay can protect the transmissions from the source to the relay by confusing the eavesdropper, as discussed in Remark 6. As a result, the proposed scheme outperforms the CJ scheme and the comparable ones, especially in the high power region, as shown in Figure 5a,b.

3.4. Comparison with the Secrecy Rate in [20]

Since it is intractable to compare the two secrecy rates achieved by the proposed scheme and the one in [20] in theory, in this subsection, some numerical examples will be illustrated to compare these two achievable secrecy rates. We will first prove that the CF relaying strategy is useless when considering the perfect secrecy rate. Since the random variables (V, U) in [20] have the same meaning as that of (U, V_1) in this paper, (V, U) in [20] are replaced by (U, V_1), respectively, for coherence. When considering the perfect secrecy rate, $R_1 = R_e$ in Equation (17) in [20] and R_e can be upper bounded as:

$$\begin{aligned} R_e &\overset{(a)}{\leq} \min\{I(X_2;Y|U), I(X_2;Y_2|U,X_1)\} - I(Y_1;\hat{Y}_1|X_2,V_1) + I(X_1;\hat{Y}_1|Y,X_2,V_1) \\ &\quad + I(X_1;Y|X_2,V_1) + \min\{I(V_1;Y_1|U,X_2), I(U;Y) + I(V_1;Y|U,X_2)\} - I(X_1,X_2;Y_2) \\ &\overset{(b)}{\leq} \min\{I(X_2;Y|U), I(X_2;Y_2|U,X_1)\} + I(X_1;Y|X_2,V_1) \\ &\quad + \min\{I(V_1;Y_1|U,X_2), I(U;Y) + I(V_1;Y|U,X_2)\} - I(X_1,X_2;Y_2) \end{aligned} \tag{20}$$

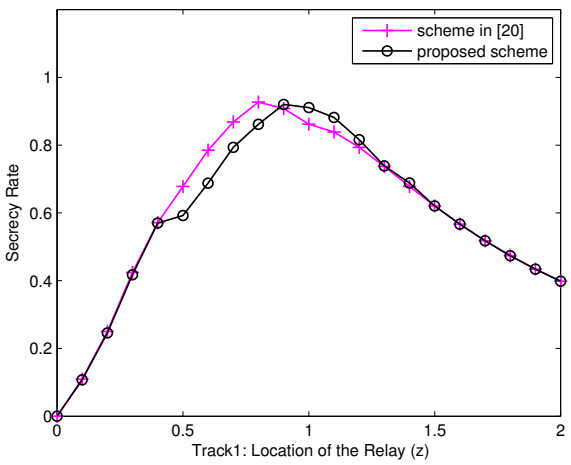
for some distribution $p(u, v_1, x_1, x_2, \hat{y}_1, y, y_1, y_2) = p(u)p(v_1|u)p(x_1|v_1)p(x_2|u)p(\hat{y}_1|y_1, v_1, x_2)$ $p(y, y_1, y_2|x_1, x_2)$, where (a) is due to Equation (18) in [20]; (b) is due to the Markov chain $(Y, X_1) \to (Y_1, X_2, V_1) \to \hat{Y}_1$, which leads to the fact that:

$$\begin{aligned} I(X_1;\hat{Y}_1|Y,X_2,V_1) &= H(\hat{Y}_1|Y,X_2,V_1) - H(\hat{Y}_1|Y,X_1,X_2,V_1) \\ &\leq H(\hat{Y}_1|X_2,V_1) - H(\hat{Y}_1|Y_1,Y,X_1,X_2,V_1) \\ &= H(\hat{Y}_1|X_2,V_1) - H(\hat{Y}_1|Y_1,X_2,V_1) \\ &= I(Y_1;\hat{Y}_1|X_2,V_1). \end{aligned} \tag{21}$$

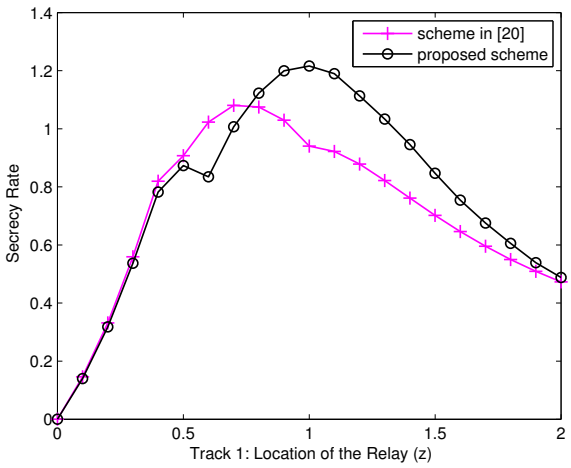
From Equation (20), obviously we should set $\hat{Y}_1 = \emptyset$, and the CF relaying strategy is useless. Now, the network geometry of Track 1 in Figure 3 is taken as an example to compare the proposed scheme and the one in [20]. To be fair, the random variables (U, V_1, X_1, X_2) in Equation (20) are also set according to Equations (11)–(13).

As shown in Figure 6a,b, the scheme in [20] outperforms the proposed scheme when the source-relay channel is strong (*i.e.*, z is small), but the proposed scheme outperforms the scheme in [20] when the source-relay channel is weak (*i.e.*, z is large). In other words, each of the two coding schemes has its own advantages, depending on the choices of z. This is mainly because different decoding strategies are utilized in this paper and [20]. Specifically, the scheme in [20] decodes the common part of the source messages (V_1) after decoding the interference messages (X_2) from the relay, which is beneficial for the receiver to decode the common part of the source message. When the source-relay channel is strong, such a scheme performs well, since most source messages should be allocated to the common part. To the contrary, the proposed scheme decodes these two messages in a reversed order, which is beneficial for the receiver to decode the the interference message. This implies that the proposed scheme can set the rate of the interference message larger to confuse the eavesdropper and, hence, performs better than the comparable one for a weak source-relay channel.

Figure 6. Achievable secrecy rates of two coding schemes *versus* the location of the relay (*i.e.*, the value of z), where the relay is in Track 1 in Figure 3.



(a) $P_1 = 10$, $P_2 = 20$



(b) $P_1 = 100$, $P_2 = 200$

4. Proof of Theorem 1

4.1. Preliminary Results

In the following, we first give a useful lemma with respect to the equivalency of two mutual information.

Lemma 3. *For a given joint distribution,* $p \in \mathcal{P}$, $I(X_2; Y_2|U, X_1) = I(X_2; Y_2|U, V_1, X_1)$.

Proof. Refer to Appendix B □

Moreover, we define some parameters as follows:

$$R_{12}^x \triangleq I(U, V_1; Y_2) - \epsilon_1, \tag{22}$$

$$R_2 \triangleq \min\{I(X_2; Y|U, V_1), I(X_2; Y_2|U, X_1)\} - \epsilon_1, \tag{23}$$

$$R_{11}^x \triangleq \min\{I(X_1, X_2; Y_2|U, V_1) - R_2, I(X_1; Y_2|U, V_1, X_2) + \epsilon_1\} - 2\epsilon_1. \tag{24}$$

Based on Lemma 3, R_{11}^x in Equation (24) can be rewritten as:

$$\begin{aligned} R_{11}^x = I(X_1; Y_2|U, V_1, X_2) &+ \min\{I(X_2; Y|U, V_1), I(X_2; Y_2|U, V_1)\} \\ &- \min\{I(X_2; Y|U, V_1), I(X_2; Y_2|U, X_1)\} - \epsilon_1. \end{aligned} \tag{25}$$

The proof of the above equality will be provided in Appendix C.

4.2. Proof of Theorem 1

The proposed achievable scheme is based on the careful combination of the partial DF [18] scheme for the relay channel, the NF scheme [12] for the relay-eavesdropper channel and the random binning for the wiretap channel [2]. We first consider the random code generation as follows.

Codebook Generation:

- For a given distribution, $p \in \mathcal{P}$, generate at random $2^{n(R_{12}+R_{12}^x)}$ independent and identically distributed (i.i.d.) n-sequences, each according to $p(\mathbf{u}^n) = \prod_{i=1}^n p(u_i)$. Then, randomly group these codewords into $2^{nR_{12}}$ bins, each with $2^{nR_{12}^x}$ codewords, and index them as $\mathbf{u}^n(w_{c,1}, w_{c,1}^x)$, where $w_{c,1} \in \{1, \cdots, 2^{nR_{12}}\}$, $w_{c,1}^x \in \{1, \cdots, 2^{nR_{12}^x}\}$. For simplicity, let

$$w_0 = (w_{c,1}, w_{c,1}^x).$$

- For each $\mathbf{u}^n(w_0)$, the relay generates at random 2^{nR_2} i.i.d. n-sequences, each according to $p(\mathbf{x}_2^n|\mathbf{u}^n) = \prod_{i=1}^n p(x_{2,i}|u_i)$. Index them as $\mathbf{x}_2^n(w_0, w_2)$, where $w_2 \in \{1, \cdots, 2^{nR_2}\}$.

- For each $\mathbf{u}^n(w_0)$, generate at random $2^{n(R_{12}+R_{12}^x)}$ i.i.d. n-sequences, each according to $p(\mathbf{v}_1^n|\mathbf{u}^n) = \prod_{i=1}^n p(v_{1,i}|u_i)$. Then, randomly group these codewords into $2^{nR_{12}}$ bins, each with $2^{nR_{12}^x}$ codewords, and index them as $\mathbf{v}_1^n(w_0, w_{12}, w_{12}^x)$, where $w_{12} \in \{1, \cdots, 2^{nR_{12}}\}$, $w_{12}^x \in \{1, \cdots, 2^{nR_{12}^x}\}$.

- For each tuple $(\mathbf{u}^n(w_0), \mathbf{v}_1^n(w_0, w_{12}, w_{12}^x))$, generate at random $2^{n(R_{11}+R_{11}^x)}$ i.i.d. n-sequences each according to $p(\mathbf{x}_1^n|\mathbf{v}_1^n, \mathbf{u}^n) = \prod_{i=1}^n p(x_{1,i}|v_{1,i}, u_i)$. Then, randomly group these codewords into $2^{nR_{11}}$ bins, each with $2^{nR_{11}^x}$ codewords, and index them as $\mathbf{x}_1^n(w_0, w_{12}, w_{12}^x, w_{11}, w_{11}^x)$, where $w_{11} \in \{1, \cdots, 2^{nR_{11}}\}$, $w_{11}^x \in \{1, \cdots, 2^{nR_{11}^x}\}$.

Encoding: The encoder structure of the proposed scheme is roughly illustrated in Figure 2.

At Block 1, the source sends $\mathbf{x}_1^n(w_{01}, w_{121}, w_{121}^x, w_{111}, w_{111}^x)$ and the relay sends $\mathbf{x}_2^n(w_{01}, w_{21})$, where $w_{01} = (1, 1)$.

At Block b ($2 \leq b \leq B-1$), the source wishes to send the new confidential message $w_{1b} \in \mathcal{W}_1 = \{1, \cdots, 2^{nR_1}\}$. It first splits this message into two independent sub-messages, *i.e.*, $w_{1b} = (w_{12b}, w_{11b})$, where $w_{12b} \in \{1, \cdots, 2^{nR_{12}}\}$, $w_{11b} \in \{1, \cdots, 2^{nR_{11}}\}$ and $R_1 = R_{12} + R_{11}$. Then, randomly choose some dummy messages, $w_{12b}^x \in \{1, \cdots, 2^{nR_{12}^x}\}$ and $w_{11b}^x \in \{1, \cdots, 2^{nR_{11}^x}\}$, to be mixed with them, respectively, and the source sends the codeword, $\mathbf{x}_1^n(w_{0b}, w_{12b}, w_{12b}^x, w_{11b}, w_{11b}^x)$, where $w_{0b} = (w_{12b-1}, w_{12b-1}^x)$. For the relay node, it is assumed to already have a correct estimation of $w_{0,b} = (w_{12b-1}, w_{12b-1}^x)$ at the end of Block $b-1$ (refer to the decoding part), then it randomly selects a dummy message, $w_{2b} \in \{1, \cdots, 2^{nR_2}\}$, and sends $\mathbf{x}_2^n(w_{0b}, w_{2b})$.

At Block B, the source sends $\mathbf{x}_1^n(w_{0B}, 1, 1, 1, 1)$, and the relay sends $\mathbf{x}_2^n(w_{0B}, 1)$, where $w_{0B} = (w_{12B-1}, w_{12B-1}^x)$.

Decoding: At the end of Block b, assume that the relay has already decoded $w_{0b} = (w_{12b-1}, w_{12b-1}^x)$, which was transmitted at Block $b-1$. Then, it will find a unique pair $(\hat{w}_{12b}, \hat{w}_{12b}^x)$, such that

$$(\mathbf{u}^n(w_{0b}), \mathbf{v}_1^n(w_{0b}, \hat{w}_{12b}, \hat{w}_{12b}^x), \mathbf{x}_2^n(w_{0b}, w_{2b}), \mathbf{y}_1^n(b)) \in \mathcal{A}_\epsilon^{(n)}(U, V_1, X_2, Y_1).$$

If there exist more than one or none such pairs, an error occurs. It is not difficult to prove that the error probability goes to zero, if the rates, R_{12} and R_{12}^x, satisfy:

$$R_{12} + R_{12}^x < I(V_1; Y_1|U, X_2). \tag{26}$$

The destination performs backward decoding. At the end of Block b ($2 \leq b \leq B-1$), assume that the destination has already correctly decoded $w_{0b+1} = (w_{12b}, w_{12b}^x)$ at the end of Block $b+1$. Then, the destination will perform separated decoding to decode w_{0b}, w_{2b} and (w_{11b}, w_{11b}^x), respectively. First, it finds a unique $\hat{w}_{0b}$, such that

$$(\mathbf{u}^n(\hat{w}_{0b}), \mathbf{v}_1^n(\hat{w}_{0b}, w_{12b}, w_{12b}^x), \mathbf{y}^n(b)) \in \mathcal{A}_\epsilon^{(n)}(U, V_1, Y).$$

The error probability goes to zeros if:

$$R_{12} + R_{12}^x < I(U, V_1; Y) \tag{27}$$

Second, knowing w_{0b}, the destination finds a unique $\hat{w}_{2b}$, such that

$$(\mathbf{u}^n(w_{0b}), \mathbf{v}_1^n(w_{0b}, w_{12b}, w_{12b}^x), \mathbf{x}_2^n(w_{0b}, \hat{w}_{2b}), \mathbf{y}^n(b)) \in \mathcal{A}_\epsilon^{(n)}(U, V_1, X_2, Y).$$

The error probability goes to zero, since we have fixed R_2 to satisfy $R_2 < I(X_2; Y|U, V_1)$ in Equation (23).

Third, knowing w_{0b} and w_{2b}, the destination finds a unique pair $(\hat{w}_{11b}, \hat{w}^x_{11b})$, such that:

$$(\mathbf{u}^n(w_{0b}), \mathbf{v}_1^n(w_{0b},w_{12b},w^x_{12b}), \mathbf{x}_1^n(w_{0b},w_{12b},w^x_{12b},\hat{w}_{11b},\hat{w}^x_{11b}), \mathbf{x}_2^n(w_{0b},w_{2b}), \mathbf{y}^n(b)) \in \mathcal{A}_\epsilon^{(n)}(U,V_1,X_1,X_2,Y).$$

The error probability goes to zeros if:

$$R_{11} + R^x_{11} < I(X_1; Y|U, V_1, X_2). \tag{28}$$

Equivocation Computation: We let $\mathbf{X}^{Bn}$ denote the set, $\{\mathbf{X}^n(1), \mathbf{X}^n(2), \cdots, \mathbf{X}^n(B)\}$. $\mathbf{X}^{bn}$ and $\mathbf{X}^n(]b[)$ denote the set, $\{\mathbf{X}^n(i), 1 \leq i \leq b\}$, and the set, $\{\mathbf{X}^n(i), 1 \leq i < b \text{ or } b < i \leq B\}$, respectively. The equivocation over the total B Markov blocks can be bounded as:

$$\begin{aligned}
H(W_1^{B-1}|\mathbf{Y}_2^{Bn}) &= H(W_1^{B-1}, \mathbf{Y}_2^{Bn}) - H(\mathbf{Y}_2^{Bn}) \\
&= H(W_1^{B-1}, \mathbf{Y}_2^{Bn}, \mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn}) \\
&\quad - H(\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn}|W_1^{B-1}, \mathbf{Y}_2^{Bn}) - H(\mathbf{Y}_2^{Bn}) \\
&= H(\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn}) + H(W_1^{B-1}, \mathbf{Y}_2^{Bn}|\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn}) \\
&\quad - H(\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn}|W_1^{B-1}, \mathbf{Y}_2^{Bn}) - H(\mathbf{Y}_2^{Bn}) \\
&= H(\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn}) - I(\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn}; \mathbf{Y}_2^{Bn}) \\
&\quad - H(\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn}|W_1^{B-1}, \mathbf{Y}_2^{Bn}).
\end{aligned} \tag{29}$$

The first term in Equation (29) is:

$$H(\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn}) = n(B-1)(R_{12} + R^x_{12} + R_{11} + R^x_{11} + R_2). \tag{30}$$

The second term can be bounded as:

$$\begin{aligned}
I(\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn}; \mathbf{Y}_2^{Bn}) &= \sum_{b=1}^{B} I\left(\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn}; \mathbf{Y}_2^n(b)|\mathbf{Y}_2^{(b-1)n}\right) \\
&\overset{(a)}{\leq} \sum_{b=1}^{B} \left[H\left(\mathbf{Y}_2^n(b)\right) - H\left(\mathbf{Y}_2^n(b)|\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn}, \mathbf{Y}_2^{(b-1)n}\right)\right] \\
&\overset{(b)}{=} \sum_{b=1}^{B} \left[H\left(\mathbf{Y}_2^n(b)\right) - H\left(\mathbf{Y}_2^n(b)|\mathbf{U}^n(b), \mathbf{V}_1^n(b), \mathbf{X}_1^n(b), \mathbf{X}_2^n(b)\right)\right] \\
&= \sum_{b=1}^{B} I\left(\mathbf{U}^n(b), \mathbf{V}_1^n(b), \mathbf{X}_1^n(b), \mathbf{X}_2^n(b); \mathbf{Y}_2^n(b)\right)
\end{aligned} \tag{31}$$

where (a) follows by the fact that conditioning does not increase entropy. (b) follows from the fact that $\mathbf{Y}_2^n(b) - (\mathbf{U}^n(b), \mathbf{V}_1^n(b), \mathbf{X}_1^n(b), \mathbf{X}_2^n(b)) - \left(\mathbf{U}^n(]b[), \mathbf{V}_1^n(]b[), \mathbf{X}_1^n(]b[), \mathbf{X}_2^n(]b[), \mathbf{Y}_2^{(b-1)n}\right)$ is a Markov chain. Such a Markov chain is due to the memoryless channel and can be observed from encoding process in which $\mathbf{Y}_2^n(b)$ depends on $\left(\mathbf{U}^n(]b[), \mathbf{V}_1^n(]b[), \mathbf{X}_1^n(]b[), \mathbf{X}_2^n(]b[), \mathbf{Y}_2^{(b-1)n}\right)$ only through $(\mathbf{U}^n(b), \mathbf{V}_1^n(b), \mathbf{X}_1^n(b), \mathbf{X}_2^n(b))$.

Furthermore, for $\forall b \in [1:B]$, we have:

$$\begin{aligned} & I\left(\mathbf{U}^n(b), \mathbf{V}_1^n(b), \mathbf{X}_1^n(b), \mathbf{X}_2^n(b); \mathbf{Y}_2^n(b)\right) \\ \overset{(c)}{\leq} & n[I(U, V_1, X_1, X_2; Y_2) + \epsilon_2] \\ = & n[I(U, V_1; Y_2) + I(X_1, X_2; Y_2|U, V_1) + \epsilon_2], \end{aligned} \tag{32}$$

$$\begin{aligned} \text{and:} \quad & I\left(\mathbf{U}^n(b), \mathbf{V}_1^n(b), \mathbf{X}_1^n(b), \mathbf{X}_2^n(b); \mathbf{Y}_2^n(b)\right) \\ = & I\left(\mathbf{U}^n(b), \mathbf{V}_1^n(b); \mathbf{Y}_2^n(b)\right) + I\left(\mathbf{X}_1^n(b), \mathbf{X}_2^n(b); \mathbf{Y}_2^n(b)|\mathbf{U}^n(b), \mathbf{V}_1^n(b)\right) \\ \overset{(d)}{\leq} & n[I(U, V_1; Y_2) + \epsilon_1] + I(\mathbf{X}_1^n(b); \mathbf{Y}_2^n(b)|\mathbf{U}^n(b), \mathbf{V}_1^n(b), \mathbf{X}_2^n(b)) \\ & + I(\mathbf{X}_2^n(b); \mathbf{Y}_2^n(b)|\mathbf{U}^n(b), \mathbf{V}_1^n(b)) \\ \overset{(e)}{\leq} & n[I(U, V_1; Y_2) + I(X_1; Y_2|U, V_1, X_2) + \epsilon_1 + \epsilon_2] + H(\mathbf{X}_2^n(b)|\mathbf{U}^n(b)) \\ = & n[I(U, V_1; Y_2) + I(X_1; Y_2|U, V_1, X_2) + R_2 + \epsilon_1 + \epsilon_2], \end{aligned} \tag{33}$$

where (c), (d) and (e) can be obtained using the same approach in [10] (Lemma 3). According to the above two inequalities, $I(\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn}; \mathbf{Y}_2^{Bn})$ in Equation (31) can be bounded as:

$$\begin{aligned} I(\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn}; \mathbf{Y}_2^{Bn}) \leq nB[I(U, V_1; Y_2) + \\ \min\{I(X_1, X_2; Y_2|U, V_1), I(X_1; Y_2|U, V_1, X_2) + R_2 + \epsilon_1\} + \epsilon_2]. \end{aligned} \tag{34}$$

To bound the third term, $H(\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn}|W_1^{B-1}, \mathbf{Y}_2^{Bn})$, we will prove that the eavesdropper can correctly decode $(\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn})$ with the side information, W_1^{B-1}. Note that $(\mathbf{U}^{Bn}, \mathbf{V}_1^{Bn}, \mathbf{X}_1^{Bn}, \mathbf{X}_2^{Bn})$ is determined by the message tuple $(w_{12b}, w_{12b}^x, w_{11b}, w_{11b}^x, w_{2b})$ for $\forall b \in [1:B]$. Thus, with the knowledge of $W_1(b) = w_{1b} = (w_{12b}, w_{11b})$ for $\forall b \in [1:B]$, the eavesdropper only needs to utilize backward decoding to decode $(w_{12b-1}^x, w_{2b}, w_{11b}^x)$ at the end of Block b. Then, the eavesdropper can determine the message tuple $(w_{12b}, w_{12b}^x, w_{11b}, w_{11b}^x, w_{2b})$ for $\forall b \in [1:B]$. Let $\lambda(w_1^{B-1})$ denote the average error probability of decoding $(w_{12b-1}^x, w_{2b}, w_{11b}^x)$ for $\forall b \in [1:B]$ at the eavesdropper. The following lemma shows that $\lambda(w_1^{B-1})$ is arbitrarily small.

Lemma 4. *$\lambda(w_1^{B-1}) \leq \epsilon_0$ for sufficiently large n.*

Proof. Refer to Appendix D. □

Then, based on Fano's inequality, it can be easily obtained that:

$$\begin{aligned} & \frac{1}{nB} H(\mathbf{U}^{nB}, \mathbf{V}_1^{nB}, \mathbf{X}_1^{nB}, \mathbf{X}_2^{nB}|W_1^{B-1} = w_1^{B-1}, \mathbf{Y}_2^{nB}) \\ \leq & \frac{1}{nB}\left[1 + \lambda(w_1^{B-1}) \log\left(|\mathcal{W}_{12}^x|^{B-1} \times |\mathcal{W}_{11}^x|^{B-1} \times |\mathcal{W}_2|^{B-1}\right)\right] \\ \leq & \frac{1}{nB}\left[1 + n(B-1)\epsilon_0(R_{12}^x + R_{11}^x + R_2)\right] \\ \triangleq & \epsilon_3. \end{aligned}$$

Hence, the third term in Equation (29) can be bounded as:

$$\begin{aligned}&\frac{1}{nB}H(\mathbf{U}^{nB},\mathbf{V}_1^{nB},\mathbf{X}_1^{nB},\mathbf{X}_2^{nB}|W_1^{B-1},\mathbf{Y}_2^{nB})\\=&\sum_{w_1^{B-1}}p(w_1^{B-1})\frac{1}{nB}H(\mathbf{U}^{nB},\mathbf{V}_1^{nB},\mathbf{X}_1^{nB},\mathbf{X}_2^{nB}|W_1^{B-1}=w_1^{B-1},\mathbf{Y}_2^{nB})\\\leq&\epsilon_3.\end{aligned}\tag{35}$$

Now, according to the definitions in Equations (22)–(24) and by combining Equation (29) with Equations (30), (34) and (35), we have:

$$\frac{1}{nB}H(W_1^{B-1}|\mathbf{Y}_2^{nB})\geq\frac{B-1}{B}(R_{12}+R_{11})-\frac{1}{B}(R_{12}^x+R_{11}^x+R_2)-3\epsilon_1-\epsilon_2-\epsilon_3.\tag{36}$$

Let $B\to\infty$; the secret constraint is satisfied. Furthermore, according to Equations (26), (27) and (28), one can verify that the secrecy rate, $R_{11}(p)+R_{12}(p)$ (defined in Equations (4) and (5)), is achievable by using the conversion of R_{11}^x in Equation (25).

5. Conclusions

In this paper, we have proposed a hybrid cooperative coding scheme, which enables the relay to integrate the explicit cooperation strategy and the implicit cooperation strategy by forwarding source messages and additional interference at the same time. The basic idea is to combine the partial DF scheme [18], the NF [12] scheme and random binning [2]. The derived achievable secrecy rate shows that the proposed scheme outperforms some existing works. Then, the achievable secrecy rate is extended to the memoryless Gaussian channel using Gaussian codebooks, and a power policy is developed in the high power region. The result shows that the secrecy rate achieved by the proposed scheme is sufficiently large in the high power region, even if the source-relay link is weak. This is benefited from the fact that the transmissions from the source to the relay can be protected by the interference generated at the relay. Finally, some numerical results have been carried out to demonstrate that the proposed scheme outperforms the comparable ones, especially in the high power region.

Due to the advantages of the hybrid cooperative coding schemes, a future direction of interest is to study the hybrid cooperative coding schemes for more complicated scenarios with more than one confidential message. One can also design more excellent coding schemes, such as combing the channel prefixing techniques [3] and utilizing a more general joint decoding approaches. For simplicity, the proposed scheme uses a separated decoding approach to decode the interference messages, as shown in Section 4, but it is worth pointing out that coding schemes associated with joint decoding may further enhance the security level.

Acknowledgment

The work of Peng Xu and Xuchu Dai was supported by the National Basic Research Program of China (973 Program: 2013CB329004), the National Natural Science Foundation of China (mo. 61271272) and the Intercollegiate Key Project of Nature Science of Anhui Province under Grant No. KJ2012A283. The authors are also grateful to the anonymous reviewers for their helpful suggestions.

Author Contributions

All the authors contributed to the design, analysis, numerical results and presentation of the paper. All the three authors discussed, read and approved this manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

Appendix

A. Proof of Lemma 2

A.1. Simplified Expression of the Secrecy Rate

Here, we will simplify the expression of the secrecy rate in Equation (15). Specifically, let: $\bar{P}_1 = |h_{sd}|^2 P_1$, $\bar{P}_1^u = |h_{sd}|^2 P_1^u$, $\bar{P}_1^{v_0} = |h_{sd}|^2 P_1^{v_0}$, $\bar{P}_1^{x_0} = |h_{sd}|^2 P_1^{x_0}$ and $\bar{P}_2 = |h_{re}|^2 P_2$, $\bar{P}_2^u = |h_{re}|^2 P_2^u$, $\bar{P}_2^{x_0} = |h_{re}|^2 P_2^{x_0}$. Then, the power allocation set in Equation (14) becomes:

$$\begin{aligned}\bar{\mathcal{A}} = \{(\bar{P}_1^u, \bar{P}_1^{v_0}, \bar{P}_1^{x_0}, \bar{P}_2^u, \bar{P}_2^{x_0}) | \bar{P}_1^u, \bar{P}_1^{v_0}, \bar{P}_1^{x_0}, \bar{P}_2^u, \bar{P}_2^{x_0} \geq 0 \\ \bar{P}_1^u + \bar{P}_1^{v_0} + \bar{P}_1^{x_0} \leq \bar{P}_1,\ \bar{P}_2^u + \bar{P}_2^{x_0} \leq \bar{P}_2\}. \end{aligned} \tag{37}$$

Using the above conversions and the definitions of a, b, c in Lemma 2, for a $\bar{\mathbf{A}} \in \bar{\mathcal{A}}$, R_{11}^G and R_{12}^G in Equations (16) and (17) can be rewritten as:

$$\begin{aligned} R_{11}^G(r, \bar{\mathbf{A}}) =& C(\bar{P}_1^{x_0}) + \min\left\{ C\left(\frac{b\bar{P}_2^{x_0}}{1+\bar{P}_1^{x_0}}\right), C\left(\bar{P}_2^{x_0}\right) \right\} \\ & - \min\left\{ C\left(\frac{b\bar{P}_2^{x_0}}{1+\bar{P}_1^{x_0}}\right), C\left(\frac{\bar{P}_2^{x_0}}{1+a\bar{P}_1^{x_0}}\right) \right\} - C(a\bar{P}_1^{x_0}), \end{aligned} \tag{38}$$

$$\begin{aligned} R_{12}^G(r, \bar{\mathbf{A}}) =& \min\left\{ C\left(\frac{|\sqrt{\bar{P}_1^u} + r\sqrt{b\bar{P}_2^u}|^2 + \bar{P}_1^{v_0}}{1 + \bar{P}_1^{x_0} + b\bar{P}_2^{x_0}}\right), C\left(\frac{c\bar{P}_1^{v_0}}{1 + c\bar{P}_1^{x_0}}\right) \right\} \\ & - C\left(\frac{|\sqrt{a\bar{P}_1^u} + r\sqrt{\bar{P}_2^u}|^2 + a\bar{P}_1^{v_0}}{1 + a\bar{P}_1^{x_0} + \bar{P}_2^{x_0}}\right). \end{aligned} \tag{39}$$

A.2. Proof of Lemma 2

From Equation (39), obviously, we have:

$$R_{12}^G(r, \bar{\mathbf{A}}) \leq \min\left\{ C\left(\frac{|\sqrt{\bar{P}_1^u} + r\sqrt{b\bar{P}_2^u}|^2 + \bar{P}_1^{v_0}}{1 + \bar{P}_1^{x_0} + b\bar{P}_2^{x_0}}\right), C\left(\frac{c\bar{P}_1^{v_0}}{1 + c\bar{P}_1^{x_0}}\right) \right\} - C\left(\frac{a\bar{P}_1^{v_0}}{1 + a\bar{P}_1^{x_0} + \bar{P}_2^{x_0}}\right) \tag{40}$$

When $P_1 = P_2 = P \to \infty$, let $\bar{P}_1^{v_0} \doteq P^{\beta}$, $\bar{P}_2^{x_0} \doteq P^{\gamma}$ and $\bar{P}_1^{x_0} \doteq P^{\eta}$ with $0 \leq \beta, \gamma, \eta \leq 1$. Then, the three terms at the right-hand of Equation (40) can be upper bounded as:

$$\lim_{P\to\infty} \frac{1}{\log P} C\left(\frac{|\sqrt{\bar{P}_1^u} + r\sqrt{b\bar{P}_2^u}|^2 + \bar{P}_1^{v_0}}{1 + \bar{P}_1^{x_0} + b\bar{P}_2^{x_0}}\right) \leq \frac{1}{2}\left(1 - \max\{\gamma, \eta\}\right) \tag{41}$$

$$\lim_{P\to\infty} \frac{1}{\log P} C\left(\frac{c\bar{P}_1^{v_0}}{1 + c\bar{P}_1^{x_0}}\right) = \frac{1}{2}[\beta - \eta]^+ \tag{42}$$

$$\lim_{P\to\infty} \frac{1}{\log P} C\left(\frac{a\bar{P}_1^{v_0}}{1 + a\bar{P}_1^{x_0} + \bar{P}_2^{x_0}}\right) = \frac{1}{2}[\beta - \max\{\gamma, \eta\}]^+ \tag{43}$$

where Equation (41) holds, since it is maximized by $\bar{P}_1^u \doteq P^1$ and $\bar{P}_2^u \doteq P^1$.

Now, for $r = \pm 1$ and $\forall \bar{\mathbf{A}} \in \bar{\mathcal{A}}$, combining Equation (40) with the above three relationships, we have:

$$\lim_{P\to\infty} \frac{R_{12}^G(r, \bar{\mathbf{A}})}{\log P} \leq \frac{1}{2}\left(\min\left\{1 - \max\{\gamma, \eta\}, [\beta - \eta]^+\right\} - [\beta - \max\{\gamma, \eta\}]^+\right) \tag{44}$$

$$= \frac{1}{2}\min\left\{1 - \max\{\gamma, \eta\} - [\beta - \max\{\gamma, \eta\}]^+, [\beta - \eta]^+ - [\beta - \max\{\gamma, \eta\}]^+\right\} \tag{45}$$

$$\leq \frac{1}{2}\min\{1 - \gamma - [\beta - \gamma]^+, \beta - [\beta - \gamma]^+\} \tag{46}$$

$$\leq \frac{1}{4}, \tag{47}$$

where Equation (46) holds, since $\eta = 0$ maximizes Equation (45); Equation (47) holds, since $\beta = \gamma = \frac{1}{2}$ maximizes Equation (46). This can be seen from the following proof steps.

If $0 \leq \gamma \leq \beta \leq 1$, we have:

$$\begin{aligned} \min\{1 - \gamma - [\beta - \gamma]^+, \beta - [\beta - \gamma]^+\} &= \min\{1 - \beta, \gamma\} \\ &\overset{(a)}{\leq} \min\{1 - \beta, \beta\} \\ &\overset{(b)}{\leq} \frac{1}{2}, \end{aligned} \tag{48}$$

where "$\leq$" in both (a) and (b) can be replaced by "$=$" by choosing $\beta = \gamma = \frac{1}{2}$ in this case.

On the other hand, if $0 \leq \beta \leq \gamma \leq 1$, we have:

$$\begin{aligned} \min\{1 - \gamma - [\beta - \gamma]^+, \beta - [\beta - \gamma]^+\} &= \min\{1 - \gamma, \beta\} \\ &\overset{(c)}{\leq} \min\{1 - \gamma, \gamma\} \\ &\overset{(d)}{\leq} \frac{1}{2}, \end{aligned} \tag{49}$$

where "$\leq$" in both (c) and (d) can be replaced by "$=$" by choosing $\beta = \gamma = \frac{1}{2}$ in this case.

In addition, according to Equation (38) and [14] (Lemma 2), $\max_{\bar{\mathbf{A}}} R_{11}^G$ becomes a constant when $P \to \infty$, *i.e.*, $\lim_{P\to\infty} \frac{\max_{\bar{\mathbf{A}}} R_{11}^G}{\log P} = 0$. Therefore, the achievable secrecy rate in Equation (15) satisfies

$$\lim_{P\to\infty} \frac{R_s^G}{\log P} = \frac{\max_{r,\bar{\mathbf{A}}} R_{12}^G}{\log P} \leq \frac{1}{4}.$$

On the other hand, one can verify that $\lim_{P\to\infty}\frac{R_{12}^G}{\log P}=\frac{1}{4}$ can be achieved by setting $r=-1$, $\bar{P}_2^u=a\bar{P}_1^u$ and $(P_1^u,P_1^{v_0},P_1^{x_0},P_2^u,P_2^{x_0})\doteq(P^1,P^{\frac{1}{2}},P^0,P^1,P^{\frac{1}{2}})$. Thus, the power policy in Lemma 2 is optimal, and this lemma has been proven.

B. Proof of Lemma 3

Before the proof of the equivalency, we first prove that $V_1-(U,X_1)-Y_2$ forms a Markov chain for a joint distribution, $p\in\mathcal{P}$ (defined in Definition 1). Specifically,

$$\begin{aligned}p(y_2|v_1,u,x_1)&=\sum_{x_2\in\mathcal{X}_2}p(x_2,y_2|u,v_1,x_1)\\&=\sum_{x_2\in\mathcal{X}_2}p(x_2|u,v_1,x_1)p(y_2|u,v_1,x_1,x_2)\\&\overset{(a)}{=}\sum_{x_2\in\mathcal{X}_2}p(x_2|u)p(y_2|x_1,x_2)\\&\overset{(b)}{=}\sum_{x_2\in\mathcal{X}_2}p(x_2|u,x_1)p(y_2|u,x_1,x_2)\\&=p(y_2|u,x_1),\end{aligned}\tag{50}$$

where (a) is due to the two Markov chains: $(V_1,X_1)-U-X_2$ and $(U,V_1)-(X_1,X_2)-Y_2$, as shown in Definition 1; (b) is due to the two Markov chains: X_1-U-X_2 and $U-(X_1,X_2)-Y_2$.

Based on such a Markov chain, we have:

$$\begin{aligned}I(X_2;Y_2|U,V_1,X_1)&=H(Y_2|U,V_1,X_1)-H(Y_2|U,V_1,X_1,X_2)\\&=H(Y_2|U,X_1)-H(Y_2|X_1,X_2)\\&=H(Y_2|U,X_1)-H(Y_2|U,X_1,X_2)\\&=I(X_2;Y_2|U,X_1).\end{aligned}\tag{51}$$

C. Proof of Equation (25)

Before the proof steps, for a given $p\in\mathcal{P}$, we first show that $I(X_2;Y_2|U,X_1)\geq I(X_2;Y_2|U,V_1)$ as follows:

$$\begin{aligned}I(X_2;Y_2|U,X_1)&\overset{(a)}{=}I(X_2;Y_2|U,V_1,X_1)\\&\overset{(b)}{=}H(X_2|U)-H(X_2|Y_2,U,V_1,X_1)\\&\overset{(c)}{=}H(X_2|U,V_1)-H(X_2|Y_2,U,V_1,X_1)\\&\geq H(X_2|U,V_1)-H(X_2|Y_2,U,V_1)\\&=I(X_2;Y_2|U,V_1),\end{aligned}\tag{52}$$

where (a) is due to Lemma 3; (b) is due to the Markov chain: $(V_1,X_1)-U-X_2$; (c) is due to the Markov chain: V_1-U-X_2.

Now, from Equation (24), we can rewrite R_{11}^x as:

$$R_{11}^x=I(X_1;Y_2|U,V_1,X_2)+\min\{I(X_2;Y_2|U,V_1)-R_2-\epsilon_1,0\}-\epsilon_1.\tag{53}$$

According to the definition of R_2 in Equation (23) and the relationship $I(X_2;Y_2|U,X_1) \geq I(X_2;Y_2|U,V_1)$ in Equation (52), R_{11}^x can be further expressed as:

$$\begin{aligned} R_{11}^x &= \begin{cases} I(X_1;Y_2|U,V_1,X_2)-\epsilon_1, & \text{if } I(X_2;Y_2|U,V_1) > I(X_2;Y|U,V_1) \\ I(X_1;Y_2|U,V_1,X_2)+I(X_2;Y_2|U,V_1)-R_2-2\epsilon_1, & \text{if } I(X_2;Y_2|U,V_1) \leq I(X_2;Y|U,V_1) \end{cases} \\ &= I(X_1;Y_2|U,V_1,X_2)+\min\{I(X_2;Y|U,V_1),I(X_2;Y_2|U,V_1)\} \\ &\quad -\min\{I(X_2;Y|U,V_1),I(X_2;Y_2|U,X_1)\}-\epsilon_1. \end{aligned} \tag{54}$$

D. Proof of Lemma 4

With the knowledge of $W_1(b)=w_{1b}=(w_{12b},w_{11b})$ for $\forall b \in [1:B-1]$, the eavesdropper utilizes backward decoding to decode $(w_{12b-1}^x, w_{2b}, w_{11b}^x)$ at the end of Block b. Assume that the eavesdropper has correctly decoded $w_{0b+1}=(w_{12b},w_{12b}^x)$ at the end of Block $b+1$; then, it first finds a unique $\hat{w}_{0b}=(w_{12b-1},\hat{w}_{12b-1}^x)$, such that:

$$(\mathbf{u}^n(\hat{w}_{0b}),\mathbf{v}_1^n(\hat{w}_{0b},w_{0b+1}),\mathbf{y}_2^n(b)) \in \mathcal{A}_\epsilon^{(n)}(U,V_1,Y_2). \tag{55}$$

Since the eavesdropper knows w_{12b-1}, it only needs to find a unique $\hat{w}_{12b-1}^x$.

After decoding w_{0b}, the eavesdropper finds a unique pair $(\hat{w}_{2b},\hat{w}_{11b}^x)$, such that:

$$\begin{aligned} &(\mathbf{u}^n(w_{0b}),\mathbf{v}_1^n(w_{0b},w_{0b+1}),\mathbf{x}_1^n(w_{0b},w_{0b+1},w_{11b},\hat{w}_{11b}^x),\mathbf{x}_2^n(w_{0b},\hat{w}_{2b}),\mathbf{y}_2^n(b)) \\ &\qquad \in \mathcal{A}_\epsilon^{(n)}(U,V_1,X_1,X_2,Y_2). \end{aligned} \tag{56}$$

Analysis of error probability: With out loss of generality, assume that the transmitted message tuple is $(w_{12b-1}^x,w_{2b},w_{11b}^x)=(1,1,1)$ at Block b. The decoding process discussed above contains the following error events:

E_1: $w_{12b-1}^x=1$ does not satisfy Equation (55) or $w_{12b-1}^x \neq 1$ satisfies Equation (55);

E_2: $(w_{2b},w_{11b}^x)=(1,1)$ does not satisfy Equation (56);

E_{31}: $(w_{2b},w_{11b}^x)=(i,1)$ satisfies Equation (56), where $i \neq 1$.

E_{32}: $(w_{2b},w_{11b}^x)=(1,j)$ satisfies Equation (56), where $j \neq 1$.

E_{33}: $(w_{2b},w_{11b}^x)=(i,j)$ satisfies Equation (56), where $i,j \neq 1$.

Then, the average error probability at Block b can be upper bounded as:

$$\begin{aligned} P_E^{(n)} &= P\{E_1 \cup E_2 \cup (\cup_{k=1}^3 E_{3k})\} \\ &= P\{E_1\}+P\left\{E_1^c \cap \left(E_2 \cup (\cup_{k=1}^3 E_{3k})\right)\right\} \\ &= P\{E_1\}+P\left\{(E_1^c \cap E_2) \cup \left(\cup_{k=1}^3 (E_1^c \cap E_{3k})\right)\right\} \\ &\leq P\{E_1\}+P\{E_1^c \cap E_2\}+\sum_{k=1}^3 P\{E_1^c \cap E_{3k}\} \\ &\leq P\{E_1\}+P\{E_{21}|E_1^c\}+\sum_{k=1}^3 P\{E_{3k}|E_1^c\} \end{aligned} \tag{57}$$

Now, we will calculate each term in the Equation (57). According to Equation (22), since $R_{12}^x < I(U,V_1;Y_2)$, it is not difficult to prove that $P\{E_1\} \leq \epsilon_1$ for sufficiently large n. When E_1^c occurs, the eavesdropper can correctly decode $w_{12b-1}^x = 1$. In this case, it is obvious that $P\{E_{21}|E_1^c\} \leq \epsilon_1$, according to the asymptotic equipartition property (AEP) [21]. Next, we will calculate $P\{E_{3k}|E_1^c\}$ for $k = 1, 2, 3$ according to the properties of the joint typicality [21].

$$\begin{aligned}
P\{E_{31}|E_1^c\} &= P\Big\{(\mathbf{u}^n(w_{0b}), \mathbf{v}_1^n(w_{0b}, w_{0b+1}), \mathbf{x}_1^n(w_{0b}, w_{0b+1}, w_{11b}, 1), \mathbf{x}_2^n(w_{0b}, i), \mathbf{y}_2^n(b)) \\
&\qquad\qquad \in \mathcal{A}_\epsilon^{(n)},\ \forall i \neq 1\Big\} \\
&\leq 2^{nR_2} \sum_{(\mathbf{u}^n, \mathbf{v}_1^n, \mathbf{x}_1^n, \mathbf{x}_2^n, \mathbf{y}_2^n) \in \mathcal{A}_\epsilon^{(n)}} p(\mathbf{u}^n)p(\mathbf{v}_1^n, \mathbf{x}_1^n|\mathbf{u}^n)p(\mathbf{x}_2^n|\mathbf{u}^n)p(\mathbf{y}_2^n|\mathbf{x}_1^n, \mathbf{v}_1^n, \mathbf{u}^n) \\
&\leq 2^{nR_2} 2^{n(H(U,V_1,X_1,X_2,Y_2)+\epsilon)} 2^{-n(H(U)-\epsilon)} 2^{-n(H(V_1,X_1|U)-\epsilon)} \\
&\quad \times 2^{-n(H(X_2|U)-\epsilon)} 2^{-n(H(Y_2|U,V_1,X_1)-\epsilon)} \\
&= 2^{-n(I(X_2;Y_2,V_1,X_1|U)-R_2-5\epsilon)} \\
&= 2^{-n(I(X_2;Y_2|U,V_1,X_1)-R_2-5\epsilon)} \\
&= 2^{-n(I(X_2;Y_2|U,X_1)-R_2-5\epsilon)}
\end{aligned} \tag{58}$$

where the last relationship is due to Lemma 3. Similarly, we have:

$$P\{E_{32}|E_1^c\} \leq 2^{-n(I(X_1;Y_2|U,V_1,X_2)-R_{11}^x-5\epsilon)} \tag{59}$$

and:

$$P\{E_{33}|E_1^c\} \leq 2^{-n(I(X_1,X_2;Y_2|U,V_1)-R_2-R_{11}^x-5\epsilon)} \tag{60}$$

Since we have set the rate pair (R_2, R_{11}^x) in Equations (23) and (24) to satisfy:

$$\begin{cases} R_2 < I(X_2;Y_2|U,X_1) \\ R_{11}^x < I(X_1;Y_2|U,V_1,X_2) \\ R_2 + R_{11}^x < I(X_1,X_2;Y_2|U,V_1) \end{cases},$$

the probability of $P(E_{3k}|E_1^c)$ is arbitrarily small for $\forall k \in \{1,2,3\}$, as long as n is sufficiently large.

Thus, $P_E^{(n)}$ in Equation (57) satisfies $P_E^{(n)} \leq \epsilon_2$ for sufficiently large n. Consequently, $\lambda(w_1^{B-1})$ in Lemma 4 can be arbitrarily small, and this lemma has been proven.

References

1. Shannon, C. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715.
2. Wyner, A. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387.
3. Csiszár, I.; Körner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory,* **1978**, *IT-24*, 339–348.
4. Chen, Y.; Han Vinck, A. Wiretap channel with side information. *IEEE Trans. Inf. Theory* **2008**, *54*, 395–402.

5. Dai, B.; Luo, Y. Some New Results on the Wiretap Channel with Side Information. *Entropy* **2012**, *14*, 1671–1702.
6. Tekin, E.; Yener, A. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory* **2008**, *54*, 2735–2751.
7. Xu, P.; Ding, Z.; Dai, X. Rate Regions for Multiple Access Channel with Conference and Secrecy Constraints. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1961–1974.
8. Liang, Y.; Poor, H. Multiple-access channels with confidential messages. *IEEE Trans. Inf. Theory* **2008**, *54*, 976–1002.
9. Liu, R.; Maric, I.; Yates, R.; Spasojevic, P. The discrete memoryless multiple access channel with confidential messages. In Proceedings of 2006 IEEE International Symposium on Information Theory, Seattle, WA, USA, 9–14 July 2006; pp. 957–961.
10. Liu, R.; Maric, I.; Spasojevic, P.; Yates, R. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Inf. Theory* **2008**, *54*, 2493–2507.
11. Ekrem, E.; Ulukus, S. Secrecy in cooperative relay broadcast channels. *IEEE Trans. Inf. Theory* **2011**, *57*, 137–155.
12. Lai, L.; El Gamal, H. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inf. Theory* **2008**, *54*, 4005–4019.
13. Vaneet, A.; Lalitha, S.; A Robert, C.; H Vincent, P. Secrecy capacity of a class of orthogonal relay eavesdropper channels. *EURASIP J. Wirel. Commun. Netw.* **2009**, *2009*, doi:10.1155/2009/494696.
14. Tang, X.; Liu, R.; Spasojevic, P.; Poor, H. Interference Assisted Secret Communication. *IEEE Trans. Inf. Theory* **2011**, *57*, 3153–3167.
15. Awan, Z.H.; Zaidi, A.; Vandendorpe, L. Multiaccess Channel with Partially Cooperating Encoders and Security Constraints. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1243–1254.
16. Oohama, Y. Relay channels with confidential messages. **2007**, arXiv:cs/0611125 [cs.IT].
17. He, X.; Yener, A. Cooperation with an untrusted relay: A secrecy perspective. *IEEE Trans. Inf. Theory* **2010**, *56*, 3807–3827.
18. Cover, T.; Gamal, A. Capacity theorems for the relay channel. *IEEE Trans. Inf. Theory* **1979**, *25*, 572–584.
19. Awan, Z.H.; Zaidi, A.; Vandendorpe, L. Secure communication over parallel relay channel. *IEEE Trans. Inf. Forensics Secur.* **2013**, *7*, 359–371.
20. Sonee, A.; Salimi, S. A new achievable rate-equivocation region for the relay-eavesdropper channel. In Proceedings of 18th Iranian Conference on Electrical Engineering (ICEE), Isfahan, Iran, 11–13 May 2010; pp. 188–193.
21. Cover, T.; Thomas, J. *Elements of Information Theory*, 2nd ed.; Wiley: New York, NY, USA, 2006.