Individual Secrecy for Broadcast Channels with Receiver Side Information

Yanling Chen, O. Ozan Koyluoglu, and Aydin Sezgin

Abstract

This paper studies the problem of secure communication over the broadcast channel with receiver side information under the lens of individual secrecy constraints. That is, the transmitter wants to send two independent messages to two receivers which have, respectively, the desired message of the other receiver as side information, while keeping the eavesdropper ignorant of *each* message (i.e., the information leakage from *each* message to the eavesdropper is made vanishing). Building upon one-time pad, secrecy coding, and broadcasting schemes, achievable rate regions are investigated, and the capacity region for special cases of either a *weak* or *strong* eavesdropper (compared to both legitimate receivers) are characterized. Interestingly, the capacity region for the former corresponds to a line and the latter corresponds to a square with missing corners; a phenomenon occurring due to the coupling between user's rates. Moreover, the individual secrecy capacity region is also fully characterized for the case where the eavesdropper's channel is *deterministic*. In addition to discrete memoryless setup, Gaussian scenarios are studied. For the Gaussian model, in addition to the strong and weak eavesdropper cases, the capacity region is characterized for the low and high SNR regimes when the eavesdropper's channel is stronger than one receiver but weaker than the other. Remarkably, positive secure transmission rates are always guaranteed under the individual secrecy constraint, unlike the case of the joint secrecy constraint (i.e., the information leakage from *both* messages to the eavesdropper is made vanishing). Thus, this notion of secrecy serves as an appropriate candidate for trading off secrecy level and transmission rate; making secrecy more *affordable* but still *acceptable* to the end user.

I. Introduction

A. Background

The broadcast channel is a fundamental communication model that involves transmission of independent messages to different users. However, the broadcast nature makes the communication very susceptible to eavesdropping. Therefore, it is desirable to offer a reliable communication with a certain level of security guarantee, especially for ensuring sensitive information to be protected from unauthorized parties.

This paper was presented in part at International Zurich Seminar on Communications, Zurich, Switzerland, Feb. 2014 and IEEE International Symposium on Information Theory, Honolulu, HI, Jun. 2014.

Y. Chen and A. Sezgin are with the Institute of Digital Communication Systems, Ruhr University Bochum, Germany (e-mail: yanling.chen-q5g@rub.de, aydin.sezgin@rub.de). O. O. Koyluoglu is with the Department of Electrical and Computer Engineering, The University of Arizona, Tucson, AZ 85721, USA (e-mail: ozan@email.arizona.edu).

The problem of secure communication from an information theoretic point of view was first studied by Shannon [1]. In this work, a cipher system was introduced under the assumption that the transmitter and the intended receiver share a secret random key which is out of the eavesdropper's knowledge. For the purpose of a secure communication, the message is first encrypted into a ciphertext before being transmitted, and it is assumed that the eavesdropper has full access to the ciphertext as the intended receiver. A cipher system with *perfect secrecy* demands that knowing the ciphertext, however, gives no clue about the message. Such a perfect cipher system is shown to be possible via the so-called *one-time pad* scheme [1] (previously porposed by Vernam [2]), provided that the secret key is sufficient to randomize the message.

Wyner, in his seminal paper [3], introduced the wiretap channel, where he addressed the problem of secret message transmission from a transmitter to a legitimate receiver (without sharing keys beforehand) over a degraded broadcast channel in the presence of an eavesdropper. It is shown that the secure communication is still possible when the eavesdropper observes a degraded version of the legitimate receiver's observation. The fundamental limit of secure communication, i.e., *secrecy capacity*, is defined to be the maximum rate under a weak secrecy constraint, where the rate of information leaked to the eavesdropper is made vanishing. Later on, Csiszár and Körner [4] extended Wyner's work by considering a setup of transmitting secret and common message over a general broadcast channel, and provided a single-letter characterization of the secrecy capacity. Notably, the secrecy capacity results hold also under a strong secrecy constraint, where the total amount of information leaked to the eavesdropper is made vanishing, as demonstrated in [5].

For those wiretap channels where the legitimate receiver does not have any advantage over the eavesdropper, interestingly, Maurer [6] demonstrated that it is still possible to achieve a positive secret rate if a public feedback channel is made available. In parallel, Csiszár and Ahlswede [7] recognized that correlated source observations could be explored for generating secret key that could be used further for secret message transmission via one-time pad. These offer alternative solutions to achieve information theoretic secrecy, which are especially interesting in cases that the legitimate users have no advantage against the eavesdropper on the communication channels.

Inspired by these pioneering works, there has been a body of growing literature studying the problem of secret message transmission and/or secret key generation by exploring the resources available in different settings. Extensive types of resources have been taken into account in order to establish secret communications without much sacrifice, or turn the disadvantages into advantages so as to make the impossible possible or even improve the overall performance. Such resources include channel state information [8]–[12], side information [13], feedback [14]–[18], correlated sources [19]–[21] or shared keys [22]–[24], and so on. In the meantime, the channel, still serves as one of the most significant resource for secure communication. Several communication channels of particular practical interest have received intense research attention. Instances include but not limited to the broadcast channels [25]–[28], multiple access channels [29], two-way channel [30], [31], the interference channels [32], [33], and compound channels [34].

B. Contributions

In this paper, we consider the problem of secure communication over the broadcast channel with receiver side information (BC-RSI). The model is different from the wiretap channel with side information due to the broadcast nature of the communication channel. That is, in this model, the transmitter wants to send two independent messages to two receivers which have, respectively, the desired message of the other receiver (already available in their possession, e.g., due to previous communications) as side information. (See Fig. 1.) This is a simple setup of a general scenario, which consists of more than two legitimate receivers, each having a piece of partial information about the transmitted message. In the following, we summarize the main contributions of the paper:

- The linear deterministic model is studied and corresponding individual secrecy capacity region is characterized. Due to its relevance to the corresponding Gaussian case, study of this specific model provides insight into the individual secrecy capacity region of Gaussian case especially in the high SNR regime.
- To investigate the fundamental limits of communication under individual secrecy constraints, constructions building upon one-time pad, wiretap coding, superposition coding, and Marton's coding are proposed.
  - First construction, referred to as secret key approach, utilizes side information at receivers as secret keys of one-time pad signals, which further is encoded as *cloud centers* in broadcast coding schemes. This approach is shown to be capacity achieving for a *strong* eavesdropper (compared to both legitimate receivers).
  - Secret key approach is extended with secrecy coding, where the one-time pad signal is utilized as a *part of the randomization* to confuse the eavesdropper (i.e., to limit her ability to obtain information regarding each message). This approach is shown to be capacity achieving for a *weak* eavesdropper (compared to both legitimate receivers).
  - The proposed superposition coding can be considered as an extension of secret key approach and combined secret key and secrecy coding approach. It takes advantage of the rate splitting of one-time pad signals such that they serve for two distinct purposes: 1) as a cloud center; and 2) as a part of randomization within the satellite codewords to confuse the eavesdropper. Also, it is shown that the suggested rate splitting is sufficient within superpostion coding since further rate splitting does not improve the established region. Remarkably, superposition coding is shown to be optimal for special cases of either a *strong* or *weak* eavesdropper (compared to both legitimate receivers), and in case that the eavesdropper has a *deterministic* channel.
  - The proposed Marton's coding approach is built on the superposition coding but with one additional coding layer that employs Marton's coding. The idea is to further explore the advantage of rate splitting at the encoding phase (with introduction of joint distributed satellite codewords which carry independent message pieces intended for each legitimate receiver); and at the decoding phase

only the individual satellite codewords will be decoded. As a result, a general achievable individual secrecy rate region is established, which not only includes but further improves the region obtained by superposition coding approach. The improvement is demonstrated for the *mixed* case where the eavesdropper's channel is weaker than one of the legitimate receivers channels but stronger than the other.

  - As a by-product, two achievable *joint secrecy* rate regions are also obtained by the proposed superposition coding approach and Marton's coding approach, respectively; in which the former is included and potentially improved by the latter, i.e., Marton's coding approach.

- Gaussian model is studied. And, in addition to strong and weak eavesdropper scenarios, the capacity region for low and high SNR regimes are characterized for the *mixed* case when the eavesdropper is stronger than one legitimate receiver but weaker than the other.

C. Related Work

Our model can be thought of as a broadcast phase of a relay network after a multiple access phase where the nodes transmit their messages to the relay in the first phase. Remarkably, this two-way relay setting simply illustrates how the information are shared in today's networked world. To maximize the broadcasting throughput, the technique employed at the relay node is very relevant to network coding. As demonstrated in [35], the relay node (i.e., the transmitter in our model) can broadcast the XORed messages. Then, the legitimate receivers, utilizing the side information they have, can decode their intended message. The broadcasting capacity region (Fig. 1 without an eavesdropper) is characterized in [35].

In addition to the broadcasting to share information in the most efficient way, the secrecy aspect of the communication has been a growing concern. Considering the existence of an external eavesdropper in the model of the broadcast channel with receiver side information (BC-RSI), the authors in [36] proposed achievable rate regions and outer bounds subject to a *joint* secrecy constraint, whereby the information leakage from *both* messages to the eavesdropper is made vanishing. Differently from [36], we focus on the problem under *individual* secrecy constraints that aims to minimize the information leakage from *each* message to the eavesdropper. Other relevant works include [37]–[40]. The work [37] considered transmitting common and private messages to each user for the BC with side information model in addition to transmitting a confidential message to one of the users while treating the other as an eavesdropper. The same setting without common messages was considered in [38] and the secrecy capacity was characterized. Recently, in a parallel work [39], [40], Mansour et al. considered discrete memoryless broadcast channels with degraded message sets and message cognition. The model in [40], when the common messages are removed and individual secrecy constraint is imposed, reduces to the model considered in this paper. In particular, the scenarios of weak and stronger eavesdroppers (as characterized in Theorem 4 and Theorem 6 here) overlaps with the corresponding propositions in [40], in which the authors consider more capable/less noisy scenarios as well. Our initial results on this topic are presented in [41], [42], and, in addition to stronger/weaker

eavesdropper cases, we focus on other DMC models, deterministic channels, and Gaussian scenarios for BC-RSI with individual secrecy constraints in this paper.

Although the individual secrecy constraint is by definition weaker than the joint one, this notion nevertheless provides a security level that keeps each legitimate receiver away from non-negligible information leakage on its intended message, therefore acceptable to the end user. In addition, a joint secrecy constraint can be difficult or even impossible to fulfill in certain cases. For instance, when the eavesdropper has the same or a better channel observation than at least one of the legitimate receivers, imposing joint secrecy constraints result in a vanishing communication rate to the respective receiver. In this paper, we devote a particular attention to these *mixed* scenarios, where the eavesdropper can be stronger than one receiver but weaker than the other. In such cases, individual secrecy serves as a practical security solution that is attainable. In fact, such a weaker security constraint is shown to be preferable in large-scale networks. For instance, this notion has the same spirit as the concept of *weak security* as defined in [43] to guarantee that the eavesdropper is unable to get any *meaningful* information about the source in a multicast network scenario. In addition, a similar security criterion is considered to be sufficient for distributed storage systems. For instance, one can find its application in the design of secure cloud storage systems as proposed in [44], [45].

II. System model

Consider a discrete memoryless broadcast channel given by $p(y_1, y_2, z|x)$ with two legitimate receivers and one passive eavesdropper, as shown in Fig. 1. The transmitter aims to send messages m_1, m_2 to the legitimate receiver $1, 2$, respectively. Suppose x^n is the channel input to convey m_1, m_2 in n channel uses, whilst y_1^n (at receiver 1), y_2^n (at receiver 2) and z^n (at eavesdropper), are the channel outputs. Besides, m_2 (available at receiver 1) and m_1 (available at receiver 2) serve as side information that help to decode the desired message. (Unless otherwise specified, we use capital letters for random variables, the corresponding calligraphic letters for their alphabets and small cases for their realizations.)

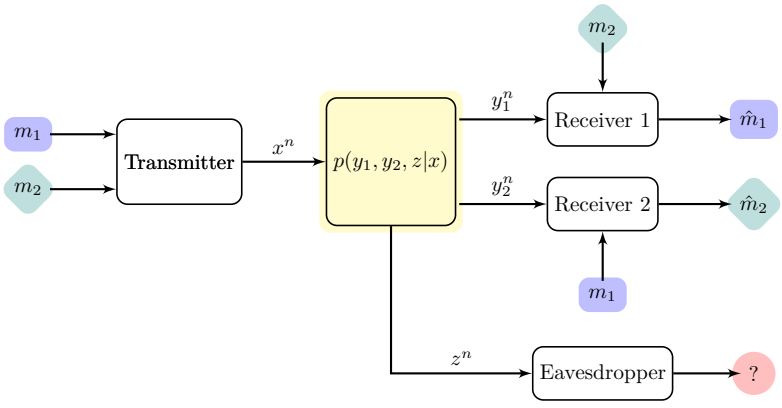


Fig. 1: BC-RSI with an external eavesdropper.

Encoder employed by the transmitter is a mapping $f : \mathcal{M}_1 \times \mathcal{M}_2 \to \mathcal{X}^n$, where $m_1 \in \mathcal{M}_1$, $m_2 \in \mathcal{M}_2$, and $x^n \in \mathcal{X}^n$. (Here, the channel input alphabet is $\mathcal{X}$). Decoder employed at receiver i is a mapping $g_i : \mathcal{Y}_i^n \times \mathcal{M}_j \to \mathcal{M}_i$, where $j \neq i$, and $y_i^n \in \mathcal{Y}_i^n$ for $i = 1, 2$. (Here, the channel output alphabet at receiver i is $\mathcal{Y}_i$.) Denote the average probability of decoding error at receiver i as $P_{e,i} = \Pr\{m_i \neq g_i(y_i^n, m_j)\}$ with $j \neq i$. The rate pair (R_1, R_2) is said to be *achievable*, if for any $\epsilon > 0$, there exists an encoder-decoder tuple (f, g_1, g_2) such that

$$\frac{1}{n} H(M_i) \geq R_i - \epsilon \tag{1}$$

$$P_{e,i} \leq \epsilon \tag{2}$$

$$\frac{1}{n} I(M_i; Z^n) \leq \epsilon, \tag{3}$$

for $i = 1, 2$ (and, for sufficiently large n). Note that (1) corresponds to the targeted transmission *rate*; (2) corresponds to the *reliability* constraint at the legitimate receivers; while (3) corresponds to the *individual* secrecy constraints against the eavesdropper. If the coding scheme fulfils a stronger condition that

$$\frac{1}{n} I(M_1, M_2; Z^n) \leq \epsilon, \tag{4}$$

then it is said to satisfy the *joint* secrecy constraint. Clearly, the joint secrecy constraint implies the individual secrecy constraints.

III. An illustrative example

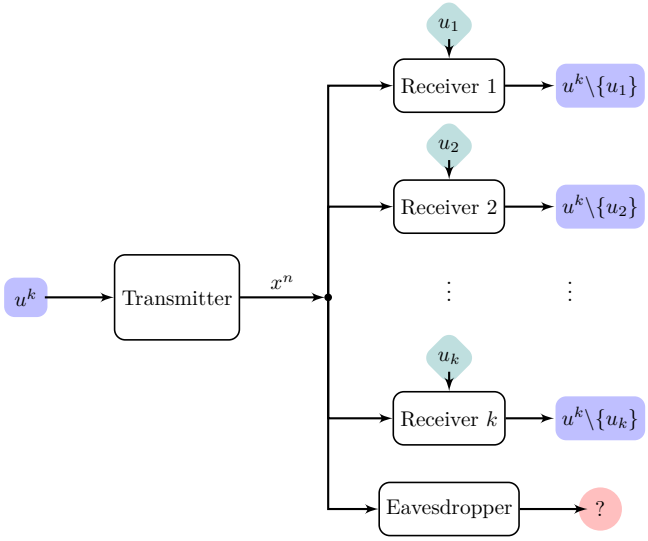


Fig. 2: Secure communication over 1-to-k broadcast channel with receiver side information.

In this section, we motivate the *individual secrecy* constraint by using the scenario of 1-to-k broadcasting as shown in Fig. 2. The model consists of one transmitter, k legitimate receivers, and one passive eavesdropper.

The transmitter aims to broadcast k information bits $U^k = (U_1, U_2, \cdots, U_k)$ to k legitimate receivers with $U_i \sim \text{Bern}(1/2)$; whilst each receiver i holds already one piece of information U_i as side information. Suppose that U^k is encoded into $X^n = (X_1, X_2, \cdots, X_n)$ and consider that this channel input is transmitted over noiseless channels. Then, for the purpose of broadcasting, each legitimate receiver i (which holds U_i and receives X^n) shall be able to recover the $k-1$ information bits $U^k \backslash \{U_i\}$, i.e.,

$$H(U^k|X^n, U_i) = 0. \tag{5}$$

Thus, we have

$$\begin{aligned} H(U^k|X^n) &= H(U^k, U_i|X^n) = H(U_i|X^n) + H(U^k|X^n, U_i) \\ &\overset{(5)}{=} H(U_i|X^n). \end{aligned} \tag{6}$$

Let us now consider the secrecy aspect of broadcasting by imposing the *joint* and *individual* secrecy constraints, respectively. We note that the eavesdropper also receives a perfect copy of X^n.

1) For the *joint* secrecy constraint, we have that

$$H(U^k|X^n) = H(U^k). \tag{7}$$

Recall (6). We obtain

$$H(U^k|X^n) = H(U_i|X^n) \leq H(U_i) < H(U^k),$$

where the last strict inequality follows since $U_i \sim \text{Bern}(1/2)$. Thus, equality in (7) is not possible. That is, for this example, no broadcasting scheme could fulfill the *joint* secrecy constraint.

2) For the *individual* secrecy constraint, we have that

$$H(U_i|X^n) = H(U_i), \quad \text{for } 1 \leq i \leq k. \tag{8}$$

Suppose there is a coding scheme that fulfills both purposes of broadcasting, i.e., (5), and the individual secrecy, i.e., (8). Then, we have

$$\begin{aligned} H(U^k, X^n) &= H(U_i, X^n) + H(U_1^{i-1}, U_{i+1}^n|U_i, X^n) \\ &\overset{(a)}{=} H(X^n) + H(U_i|X^n) \\ &\overset{(b)}{=} H(X^n) + H(U_i), \end{aligned} \tag{9}$$

where (a) is due to (5); and (b) is due to (8). Using $H(U^k, X^n) \geq H(U^k)$ in (9), we obtain that

$$H(X^n) \geq H(U^k) - H(U_i) = k - 1.$$

So to say, the optimal encoding scheme (with respect to the overall transmission rate k/n) from U^k to X^n is such that $H(X^n) = k-1$. Thus, to obtain the optimal rate, one shall take $n = k-1$. This is feasible. In fact, there are many coding schemes that could achieve this. One of the options is to take

$$x_i = u_1 \oplus u_{i+1}, \quad \text{for} \quad 1 \leq i \leq k-1.$$

The decoding at each receiver i is straightforward. Since u_i is available at receiver i as side information, it could first help to recover u_1 by $u_1 \triangleq x_{i-1} \oplus u_i$ if $i > 1$; and then sequentially recover u_j by $u_j \triangleq x_{j-1} \oplus u_1$ for $j \neq 1, i$. And, the transmission rate R_i to each receiver i, for $1 \leq i \leq k$, is equal to 1, since $k-1$ bits are received in $n = k-1$ channel uses. Noting that the capacity for a binary noiseless channel is one, we conclude that the above scheme actually achieves the individual secrecy capacity for all receivers.

The following insights immediately follow from this example:

- Joint secrecy might be impossible to achieve.
- Individual secrecy could be the highest secrecy level to offer (as shown in (6) on the equivocation at the eavesdropper).
- Individual secrecy could be achieved without any rate degradation (as compared to the capacity region without security constraints)!

In fact, joint secrecy could be impossible for a more general set-up as demonstrated in the following proposition.

Proposition 1. *For the communication model as shown in Fig. 1 under the joint secrecy constraint, any rate pair $(R_1, R_2) \in \mathbb{R}^+$ is infeasible if the channel to at least one of the receivers is more noisy than the channel to the eavesdropper.*

Proof: Assume that receiver 2 receives Y_2^n as a more noisy version of Z^n, the channel output at the eavesdropper. From the following analysis, we show that $R_2 > 0$ is not possible.

$$\begin{aligned} nR_2 = H(M_2) &= I(M_2; M_1, Y_2^n) + H(M_2|M_1, Y_2^n) \\ &\overset{(a)}{\leq} I(M_2; Y_2^n|M_1) + n\epsilon' \leq I(M_1, M_2; Y_2^n) + n\epsilon' \\ &\overset{(b)}{\leq} I(M_1, M_2; Z^n) + n\epsilon' \\ &\overset{(c)}{\leq} n(\epsilon + \epsilon'), \end{aligned}$$

where (a) is due to Fano's inequality (implying that $H(M_2|M_1, Y_2^n) \leq n\epsilon'$ for some $\epsilon' \to 0$ as $n \to \infty$) and the fact that $I(M_2; M_1, Y_2^n) = I(M_2; M_1) + I(M_2; Y_2^n|M_1) = I(M_2; Y_2^n|M_1)$ as M_1 and M_2 are independent; (b) is due to $I(M_1, M_2; Y_2^n) \leq I(M_1, M_2; Z^n)$ which follows from the fact that receiver 2 has a more noisy observation Y_2^n than the eavesdropper's observation Z^n; and (c) is due to the joint secrecy constraint (4).

This implies that $R_2 \leq \epsilon + \epsilon'$, which is arbitrarily small for an arbitrarily small $P_{e,2}$ (i.e., ϵ') and an arbitrarily small information leakage rate ϵ to the eavesdropper. ■

Nevertheless, an achievable rate region was established in [36] for the BC-RSI under joint secrecy constraint. In the following sections, we will focus on deriving the individual secrecy capacity or achievable rate regions for different BC-RSI models. In particular, we will start with a specific linear deterministic case, where we establish the individual secrecy capacity region. Then, we will address the general discrete memoryless model, where we obtain achievable rate regions with characterization of the capacity region in

special cases. Finally, we look into the Gaussian case and obtain inner and upper bounds for the individual secrecy capacity region.

IV. Linear Deterministic BC-RSI

Motivated by the success of the linear deterministic approach [12], [46] in approximating the (secrecy) capacity region within constant bits regardless of the received signal-to-noise ratio and its relevance particularly in the high SNR regime, we first take a look at the linear deterministic broadcast channel [46] with receiver side information. In this specific model, the received signals at the legitimate receivers and the eavesdropper are given by

$$\begin{aligned} Y_1 &= D^{q-n_1}X, \\ Y_2 &= D^{q-n_2}X, \\ Z &= D^{q-n_e}X, \end{aligned} \tag{10}$$

where X is the binary input vector of length $q = \max\{n_1, n_2, n_e\}$; D is the $q \times q$ down-shift matrix; n_1, n_2 and n_e are the integer channel gains of the channels from the transmitter to receiver 1, receiver 2, and the eavesdropper, respectively. Note that

1) as $q = n_1 \geq n_2 \geq n_e$, the channel is degraded in the manner that $X \to Y_1 \to Y_2 \to Z$ forms a Markov chain;
2) as $q = n_1 \geq n_e \geq n_2$, the channel is degraded in the manner that $X \to Y_1 \to Z \to Y_2$ forms a Markov chain;
3) as $q = n_e \geq n_1 \geq n_2$, the channel is degraded in the manner that $X \to Z \to Y_1 \to Y_2$ forms a Markov chain.

In all cases, we have the following theorem:

Theorem 2. *The individual secrecy capacity region of the linear deterministic broadcast channel with receiver side information is the set of the rate pairs (R_1, R_2) defined by*

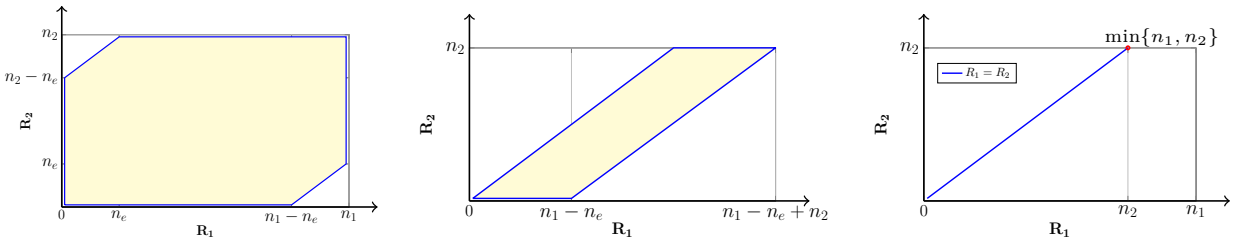
$$\begin{aligned} R_1 &\leq \min\{n_1, [n_1 - n_e]^+ + R_2\}; \\ R_2 &\leq \min\{n_2, [n_2 - n_e]^+ + R_1\}, \end{aligned}$$

where $[a]^+ = \max\{0, a\}$.

Proof: The converse follows directly from [35, Theorem 1] and Proposition 21 in Appendix A, where the former is the capacity region of the BC-RSI without any secrecy constraints; and the latter is an upper bound of the secrecy capacity region of BC-RSI.

The achievability follows by considering different scenarios, each is classified according to the relation between the channel gains n_1, n_2, n_e, and the relation between the rates R_1, R_2. For a given scenario, we consider the construction of the codeword X as a function of m_1, m_2. Note that, at the receiver side, according

to the system input-output relation as defined in (10), receiver 1 receives the first n_1 bits of X, receiver 2 gets the first n_2 bits of X, and the eavesdropper gets the first n_e bits of X. This holds for all scenarios. In order to achieve a *reliable* and *secure* communication under the individual secrecy constraint, X should be designed in such a way that both legitimate receivers could decode the desired message with the help of the side information (i.e., the other message); while the eavesdropper can only observe bits either in the form of $m_1 \oplus m_2$, or mixture of part of the messages, and/or random bits. This gives no information on m_1 and m_2 individually. In Appendix B, we provide a specific coding scheme for each scenario, achieving the corresponding individual secrecy capacity region. Putting all pieces together establishes the achievability of the stated region. ■



(a) $n_1 \geq n_2 \geq n_e$ (b) $n_1 \geq n_e \geq n_2$ (c) $n_e \geq n_1 \geq n_2$

Fig. 3: Individual secrecy capacity region of the linear deterministic BC-RSI

The individual secrecy capacity region of the linear deterministic BC-RSI is depicted in Fig. 3. We remark that the capacity region is

- a *rectangle* with two missing corners in case of $n_1 \geq n_2 \geq n_e$;
- a *parallelogram* in case of $n_1 \geq n_e \geq n_2$; and
- a *line* in case of $n_e \geq n_1 \geq n_2$.

Compared to the capacity region of the BC-RSI (following from [35, Theorem 1], this region is given by $R_1 \leq n_1$ and $R_2 \leq n_2$ as shown in Fig. 3), the missing parts reflect the loss in the transmission rates due to the individual secrecy constraints. And, as the eavesdropper gets stronger, the loss increases. Nevertheless, in the worst case, positive secrecy rate pairs are still possible under the individual secrecy constraint (as shown in Fig. 3c), unlike the case under the joint secrecy constraint (as demonstrated in Propostion 1).

V. Discrete Memoryless BC-RSI

In this section, we consider the discrete memoryless BC-RSI with an external eavesdropper (Fig. 1). When none of the secrecy constraints are taken into account, this model reduces to discrete memoryless BC-RSI, for which the capacity region is given by the union of rate pairs (R_1, R_2) satisfying $R_i \leq I(X; Y_i)$ for $i = 1, 2$, where the union is taken among all possible input probability distributions $p(x)$ [35, Theorem 1]. Here, we focus on coding schemes that can achieve not only reliability but also (individual) secrecy for this model. In

particular, we investigate to what extend this capacity region has to be modified in order to accommodate (individual) secrecy.

In order to investigate the fundamental limits of communication under individual secrecy constraints, we utilize coding approaches including one-time pad, wiretap coding, superposition coding, and Marton's coding, which have been proposed for communication scenarios such as Shannon's cipher system, wiretap channel, and broadcast channel [47]. The key ingredient of our proposed schemes is the utilization of side information at receivers as secret keys of one-time pad signals, which further is encoded as *cloud centers* in broadcast coding schemes. That is, one-time pad signals are constructed such that they can be decoded at both receivers, which can then extract their desired information utilizing the side information, whereas the eavesdropper will be left with full ambiguity regarding the information content for each message individually. We refer this signaling technique as the *secret key* approach.

As detailed in this section, we observe, for the case of a strong eavesdropper, that the secret key approach (i.e., coding via one-time pad by mixing the messages) is the best one can do; while, in case of a weak eavesdropper, the combined secret key and secrecy coding approach is required in order to achieve higher rates. (Here, we use the phrase *secrecy coding* in order to refer to the extension of wiretap coding technique to our broadcast model, where both users randomize their signals in order to confuse the eavesdropper.) After a characterization of achievable rates and special case capacity results with these strategies, we detail a universal approach by employing superposition coding and Marton's coding to establish (general) achievable individual secrecy rate regions.

A. Secret key approach and the capacity region for BC-RSI with a stronger eavesdropper

Consider the symmetric secret rate region where $R_1 = R_2 = R$, i.e., M_1 and M_2 are of the same entropy. Under these conditions, communicating the message $M_1 \oplus M_2$ readily provides individual secrecy, i.e., the following rate region is achievable.

Proposition 3. *Any* $(R_1, R_2) \in \mathbb{R}^+$ *satisfying*

$$R_1 = R_2 \leq \min\{I(X;Y_1), I(X;Y_2)\}, \tag{11}$$

for any $p(x)$ *is achievable.*

Proof: Randomly generate 2^{nR} codewords x^n according to $p(x)$. Given (m_1, m_2), send $x^n(m_k)$ with $m_k = m_1 \oplus m_2$ to the channel. See Fig. 4 for the construction of X^n. Both receivers can decode reliably by utilizing their side information to extract intended messages if $R_1 = R_2 \leq \min\{I(X;Y_1), I(X;Y_2)\}$. For the secrecy of M_i, $i = 1, 2$ we have

$$I(M_i; Z^n) \overset{(a)}{\leq} I(M_i; Z^n, M_k) \overset{(b)}{=} I(M_i; M_k) \overset{(c)}{=} 0, \tag{12}$$

where (a) is due to the non-negativity of the conditional mutual information, i.e., $I(M_i; M_k|Z^n) \geq 0$; (b)

is due to Markov chain $M_i \to M_k \to Z^n$, i.e., $I(M_i; Z_n|M_k) = 0$; and (c) follows as M_i is secured with a one-time pad M_j $(j \neq i)$ in M_k. ■

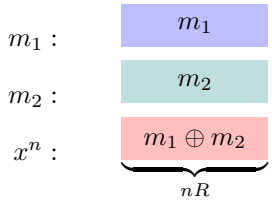


Fig. 4: Secret key approach: Encoding.

Note that the above achievable region is limited by the capacity of the worse channel of the legitimate receivers. Nevertheless, it serves as the individual secrecy capacity region when the eavesdropper has an advantage on the channel over both legitimate receivers.

Theorem 4. *If the channels to the legitimate receivers are degraded with respect to the channel to the eavesdropper, then the individual secrecy capacity region is given by the union of non-negative rate pairs* (R_1, R_2) *satisfying*

$$R_1 = R_2 \leq \min\{I(X;Y_1), I(X;Y_2)\}, \tag{13}$$

where the union is taken over $p(x)$.

Proof: The achievablity follows from the proof of Proposition 3. Here, we detail the converse.

$$\begin{aligned} nR_1 &= H(M_1) = I(M_1; M_2, Y_1^n) + H(M_1|M_2, Y_1^n) \\ &\overset{(a)}{\leq} I(M_1; Y_1^n|M_2) + n\epsilon' \leq I(M_1, M_2; Y_1^n) + n\epsilon'; \\ &\overset{(b)}{\leq} I(X^n; Y_1^n) + n\epsilon' \overset{(c)}{=} \sum_{i=1}^{n} I(X_i; Y_{1,i}) + n\epsilon' \\ &\overset{(d)}{=} nI(X_Q; Y_{1,Q}|Q) + n\epsilon' \overset{(e)}{\leq} nI(X;Y_1) + n\epsilon'; \end{aligned}$$

and, continuing from (a), we have

$$\begin{aligned} nR_1 &\leq I(M_1; Y_1^n|M_2) + n\epsilon' \leq I(M_1, M_2; Y_1^n) + n\epsilon' \\ &\overset{(f)}{\leq} I(M_1, M_2; Z^n) + n\epsilon' \overset{(g)}{\leq} I(M_2; Z^n|M_1) + n(\epsilon' + \epsilon) \\ &\leq H(M_2) + n(\epsilon' + \epsilon) \overset{(h)}{=} nR_2 + n(\epsilon' + \epsilon) \\ &\overset{(i)}{\leq} nI(X;Y_2) + n(\epsilon' + \epsilon) \end{aligned}$$

where (a) is due to Fano's inequality and the fact that $I(M_1; M_2) = 0$; (b) is due to Markov chain $(M_1, M_2) \to X^n \to Y_1^n$; (c) follows as the channel is memoryless; (d) is by introducing a time-sharing random variable Q which is uniform over $1, 2, \ldots, n$; (e) is by taking $X = X_Q, Y_1 = Y_{1,Q}$; (f) is due to the channel degradedness,

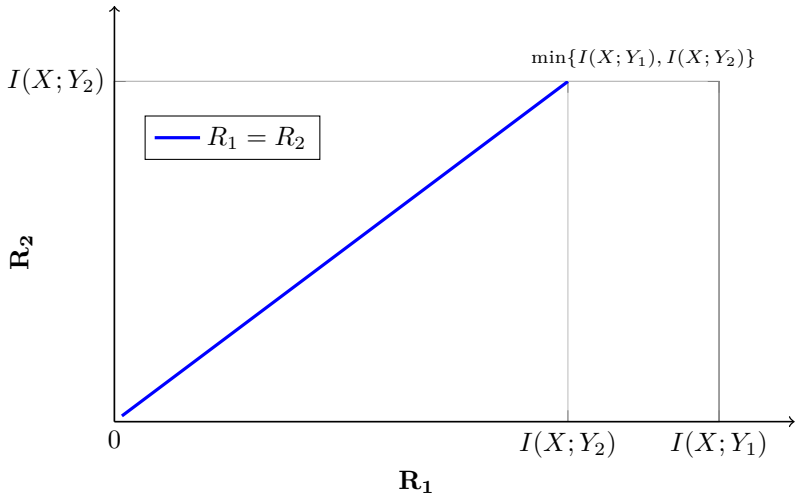


Fig. 5: Individual secrecy capacity region in case of a strong eavesdropper.

i.e., Markov chain $(M_1, M_2) \to Z^n \to Y_1^n$; (g) is by the individual secrecy constraint (3); (h) is due to $H(M_2) = nR_2$; and (i) is derived by applying a proof similar to $nR_1 \leq nI(X;Y_1) + n\epsilon'$ and by taking $Y_2 = Y_{2,Q}$. At this point, from (h), we have $R_1 \leq R_2$; and $R_1 \leq \min\{I(X;Y_1), I(X;Y_2)\}$. By symmetry, we have $R_2 \leq R_1$ and $R_2 \leq \min\{I(X;Y_1), I(X;Y_2)\}$. Thus, we establish that $R_1 = R_2 \leq \min\{I(X;Y_1), I(X;Y_2)\}$. ■

The individual secrecy capacity described in Theorem 4 is depicted in Fig. 5. That is, in case of a strong eavesdropper, the best transmission strategy is to send the one-time pad of the messages to both receivers, where both of them could recover its desired message with the help of side information; while the eavesdropper gets only the mixed copy, which gives no clue for each message individually.

B. Combined secret key and secrecy coding approach and the capacity region for BC-RSI with a weaker eavesdropper

Although the secret key approach is optimal in case of a strong eavesdropper, this scheme can be strictly suboptimal for other scenarios. In fact, a counter-example follows from the linear deterministic model, for the case where the eavesdropper is weak. In general, consider channel inputs $p(x)$ such that $I(X;Z) \leq \min\{I(X;Y_1), I(X;Y_2)\}$. We show in this section that, asymmetric rate pairs beyond the secret key approach can be achieved if we combine secret key with a secrecy coding approach. That is, besides using the receiver side information as secret key, one can further take the advantage over the channel against the eavesdropper by employing secrecy coding approach [3], [4]. First, we have the following proposition.

Proposition 5. *Any* $(R_1, R_2) \in \mathbb{R}^+$ *satisfying*

$$I(X;Z) \le R_1 \le I(X;Y_1)$$
$$I(X;Z) \le R_2 \le I(X;Y_2)$$

for $p(x)$ *such that* $I(X;Z) \le \min\{I(X;Y_1), I(X;Y_2)\}$ *is achievable.*

Proof: Rate splitting: Assume that $R_2 \le R_1$. As illustrated in Fig. 6, we split M_1 into two parts, i.e., $M_1 = (M_{1k}, M_{1s})$ with M_{1k} of entropy nR_2, the same as M_2; whilst M_{1s} of entropy nR_{1s}. Note that $R_1 = R_{1k} + R_{1s}$.

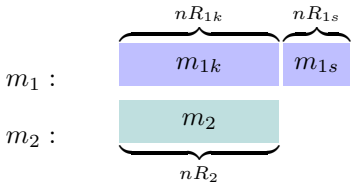


Fig. 6: Combined secret key and secrecy coding approach: Rate splitting.

Codebook generation: Randomly generate 2^{nR_1} codewords x^n according to $p(x)$. Throw them into $2^{nR_{1s}}$ bins [47] and index them by $x^n(i_k, i_{1s})$ with $(i_k, i_{1s}) \in [1 : 2^{nR_2}] \times [1 : 2^{nR_{1s}}]$.

Encoding: To send messages (m_1, m_2), choose $x^n(m_k, m_{1s})$ with $m_k = m_{1k} \oplus m_2$ and transmit it to the channel. The choice of the codeword x^n for given (m_1, m_2) is illustrated in Fig. 7.

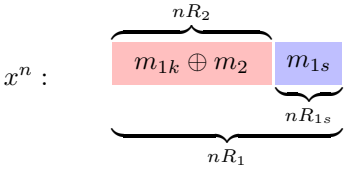


Fig. 7: Combined secret key and secrecy coding approach: Encoding

Decoding: Receiver 2 can decode m_k reliably using typical set decoding if

$$R_2 < I(X;Y_2) \tag{14}$$

with the knowledge of m_1, and thus extract m_2. Receiver 1 can decode both m_k and m_{1s} if

$$R_1 < I(X;Y_1) \tag{15}$$

and extract m_{1k} from the former with the knowledge of m_2.

Individual secrecy: At the eavesdropper, we see that M_{1k} is secured by capsuling with M_2 as a one-time pad (thus M_2 is also secured as in Section V-A), while M_{1s} is secured by using secrecy coding for classical

wiretap channels under the condition that

$$R_2 \geq I(X;Z). \tag{16}$$

More specifically, the secrecy of M_2 follows from

$$I(M_2;Z^n) \leq I(M_2;Z^n,M_k,M_{1s}) = I(M_2;M_k,M_{1s}) = 0.$$

And, the secrecy of M_1 is shown as follows. Since $R_2 \geq I(X;Z)$, for a fixed i_{1s}, one can further bin the codewords x^n and index them as $x^n(i_{kr},i_{ks},i_{1s})$ with $i_k = (i_{kr},i_{ks}) \in [1:2^{n(I(X;Z)-\epsilon)}]\times[1:2^{n(R_2-I(X;Z)+\epsilon)}]$, as illustrated in Fig. 8. Correspondingly, split $M_k = (M_{kr},M_{ks})$. We have

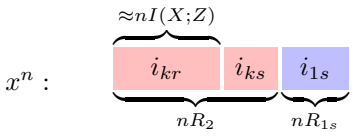


Fig. 8: secret key and secrecy coding approach: Secrecy analysis.

$$\begin{aligned}
H(M_{1s},M_{ks}|Z^n) =& H(M_{1s},M_{ks},X^n|Z^n) - H(X^n|M_{1s},M_{ks},Z^n)\\
\overset{(a)}{\geq}& H(M_{1s},M_{ks},X^n,Z^n) - H(Z^n) - n\epsilon_1\\
=& H(X^n) + H(Z^n|X^n) - H(Z^n) - n\epsilon_1\\
\overset{(b)}{\geq}& nR_1 + nH(Z|X) - nH(Z) - n\epsilon_1\\
\overset{(c)}{\geq}& H(M_{1s},M_{ks}) - n\delta(\epsilon),
\end{aligned}$$

where (a) follows as $H(X^n|M_{1s},M_{ks},Z^n) \leq n\epsilon_1$ due to Fano's inequality and that the eavesdropper can decode X^n reliably by using typical set decoder, given (M_{ks},M_{1s},Z^n); (b) is due to the fact that $H(X^n) = nR_1$; $H(Z^n|X^n) = nH(Z|X)$ since the channel is memoryless; and $H(Z^n) = \sum_{i=1}^n H(Z_i|Z_1^{i-1}) \leq \sum_{i=1}^n H(Z_i) = nH(Z)$; (c) follows that $H(M_{1s},M_{ks}) = nR_{1s} + n(R_2 - I(X;Z) + \epsilon) = nR_1 - nI(X;Z) + n\epsilon$ and $\delta(\epsilon) = \epsilon_1 + \epsilon$.

Above inequality implies $I(M_{1s};Z^n) \leq n\delta(\epsilon)$. Besides, due to Markov chain $M_{1k} \to (M_k,M_{1s}) \to Z^n$, we can bound $I(M_{1k};Z^n|M_{1s}) \leq I(M_{1k};Z^n,M_{1s},M_k) = I(M_{1k};M_k,M_{1s}) = 0$. Therefore, we obtain

$$I(M_1;Z^n) = I(M_{1s};Z^n) + I(M_{1k};Z^n|M_{1s}) \leq n\delta(\epsilon).$$

This concludes the proof of the individual secrecy.

Achievable rate region: Combining the sufficient conditions for reliable transmission to both receivers, i.e., (14) and (15), and the condition for individual secrecy, i.e., (16), we obtain

$$\begin{aligned}
I(X;Z) \leq& R_2 \leq I(X;Y_2)\\
R_2 \leq& R_1 \leq I(X;Y_1),
\end{aligned}$$

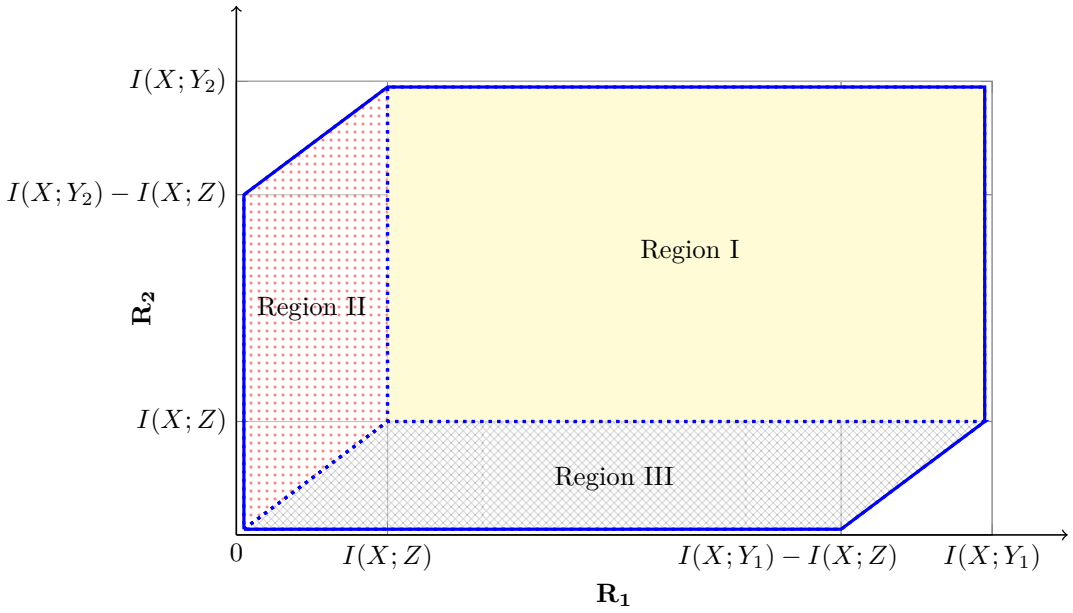


Fig. 9: Individual secrecy capacity region in case of a weak eavesdropper.

as the achievable rate region for the case $R_2 \leq R_1$. Furthermore, one can apply a similar proof to establish the rate region for the case $R_2 > R_1$. Putting them together completes the proof of the proposition. ■

Theorem 6. *If the channel to the eavesdropper is degraded with respect to the channels to both legitimate receivers, then the individual secrecy capacity region is given by the union of the non-negative rate pairs* (R_1, R_2) *satisfying*

$$R_1 \leq \min\{I(X;Y_1) - I(X;Z) + R_2,\ I(X;Y_1)\};$$
$$R_2 \leq \min\{I(X;Y_2) - I(X;Z) + R_1,\ I(X;Y_2)\},$$

where the union is taken over $p(x)$.

Proof: Under the degradedness condition, we have that $I(X;Z) \leq \min\{I(X;Y_1), I(X;Y_2)\}$ holds for any $p(x)$. Utilizing the scheme in Proposition 5, Region I in Fig. 9 is achievable. To show Region II is achievable, one can employ secrecy coding [4, Theorem 3] to achieve rate pairs (R_1, R_2) such that $R_1 = 0$ and $R_2 \leq I(X;Y_2) - I(X;Z)$. Then, applying time sharing with the left boundary rate pairs of Region I, one obtains the remaining rate pairs of Region II. A similar proof applies to establish the achievability of Region III.

The converse follows from the fact that the achievable region is equal to the intersection of upper bounds given in [35, Theorem 1], which is the capacity region of the BC-RSI without an external eavesdropper, and the upper bound given in Proposition 21, which is a partial upper bound by applying the results for wiretap channel with shared key for one receiver (while ignoring the requirement of reliable and secure

communication for the other). ■

As shown in Fig. 9, the individual secrecy capacity region for a weak eavesdropper is a rectangle with missing corners. Due to the symmetric roles of receiver 1 and receiver 2, the rate region is bounded in a symmetric manner as well. But, unlike the case of a strong eavesdropper, for which the individual secrecy capacity region is given in Fig. 5, asymmetric rate pairs are possible. Note that both receivers could benefit from each other due to the possession of the message of the other as side information. On one hand, higher rate for one receiver indicates more side information for the other. As a result, there is no loss in the high rate pair region (i.e., $R_1, R_2 \geq I(X;Z)$), compared to [35, Theorem 1] which gives the capacity region of the BC-RSI without any secrecy constraints. That is, individual secrecy to each legitimate receiver is offered for free in high rate region. On the other hand, lower rate for one receiver implies less side information for the other. In this case, the side information might be insufficient to facilitate the secure communication of the other message at a high transmission rate and additional randomness might be necessary. This results in a loss in the rate region, i.e., the missing corners. Another interesting observation is that, for communication under individual secrecy constraint, one may not claim that if (R_1, R_2) is achievable, then $(R_1 - c_1, R_2 - c_2)$ is achievable for any $c_1 \leq R_1, c_2 \leq R_2$. This follows as the individual secrecy rates are *coupled* in the BC-RSI setting.

C. Superposition coding

It is well-known that superposition coding is optimal for a degraded broadcast channel where $X \to Y_1 \to Y_2$ forms a Markov chain, wherein one can transmit a cloud center to the weak receiver and both the cloud center and satellite codewords to the strong receiver [47]. For the BC-RSI model, we consider utilizing the one-time pad signal as the cloud center and additional information on both messages being carried in the satellite codeword. This approach generalizes the aforementioned secret key approach and the combined secret key and secrecy coding approach, and thus achieves the optimality for stronger and weaker eavesdropper scenarios. In the following, we first provide the corresponding achievability region and then discuss the details of the proposed scheme together with the special cases.

Theorem 7. *The individual secrecy rate region for the BC-RSI with an external eavesdropper is achievable for the set of the non-negative rate pairs* (R_1, R_2) *such that*

$$\begin{aligned} R_1 &\leq \min\{I(V;Y_1), \quad I(V;Y_1|U) - I(V;Z|U) + R_2\}; \\ R_2 &\leq \min\{I(V;Y_2), \quad I(V;Y_2|U) - I(V;Z|U) + R_1\}. \end{aligned} \tag{17}$$

over all $p(u)p(v|u)p(x|v)$ *subject to* $I(V;Y_i|U) \geq I(V;Z|U)$ *for* $i = 1, 2$.

Proof: The proof is given in Appendix C. ■

The coding approach we develop here utilizes *cloud centers*, i.e., the U^n codewords, to carry a one-time pad signal constructed from parts of the messages. In particular, the message intended for receiver i

is splitted into $M_i = (M_{ik}, M_{isk}, M_{is})$, and the one-time pad signal carried by $u^n(m_k)$ is constructed as $M_k = M_{1k} \oplus M_{2k}$. This cloud center is designed to be decodable at both receivers, which then extract their desired messages utilizing the corresponding side information available. In addition, the code design utilizes *satellite codewords*, i.e., the V^n codewords, that are not only superimposed on the cloud centers but also carry additional information represented as $(M_{sk}, M_{1s}, M_{2s}, M_r)$. Here, M_{sk} is an additional one-time pad signal injected into V^n, and given by $M_{sk} = M_{1sk} \oplus M_{2sk}$, and M_r is additional randomness. We remark that both M_{sk} and M_r serve as randomness to confuse the eavesdropper in this scheme, in order to achieve secrecy of (M_{1s}, M_{2s}).

An interesting aspect of our superposition coding approach lies in the role of one-time pad signals. On one hand, one-time pad signal is utilized as the message of the cloud centers (i.e., M_k). On the other hand, it is also utilized as a part of randomization within the satellite codewords (i.e., M_{sk}). In other words, the coding scheme takes advantage of the rate splitting of one-time pad signals, in order to serve for these two distinct purposes.

One may wonder, whether further rate splitting helps to improve the current region or not. For instance, split M_i into $M_i = (M_{ik}, M_{isk}, M_{is}, M_{im})$, with an additional layer in the coding scheme, say T^n which carries information on M_{im} that is secured by employing secrecy coding. Interestingly, the answer is no if still using superposition coding. For a detailed proof of this, one can refer to Appendix D. However, if combining with Marton's coding, further rate splitting may improve the achievable rate region as we demonstrate in Section V-D.

Furthermore, we have the following observations:

- Setting $Y_2 = \emptyset$, the region coincides with the secrecy capacity region of the wiretap channel [4];
- Letting $U = \emptyset$ and $R_k = R_{sk} = 0$ in the proof as given in Appendix C and applying Fourier-Motzkin procedure, an achievable region under the joint secrecy constraint (follows from the secrecy proof in Appendix C) can be obtained. And this region (i.e., (23)) coincides with the one established in [36].
- Superposition coding remains optimal in the following cases.
    1) A *strong* eavesdropper, where the eavesdropper's channel is *less noisy* than both of the legitimate receivers. In this case, the individual secrecy capacity as shown in Fig. 5, can be achieved by taking $U = V = X$, whereby the superposition coding reduces to the secret key approach. (See Theorem 4.)
    2) A *weak* eavesdropper, where both of the legitimate receivers channels are *less noisy* than the one to the eavesdropper. In this case, the individual secrecy capacity is as shown in Fig. 9. Here, the left boundary rate pairs of Region II in Fig. 9 can be achieved by taking $R_2 = 0$, whereby the superposition coding reduces to the secrecy coding approach as proposed in [3], [4]. Similarly, the bottom boundary rate pairs of Region III in Fig. 9 can be achieved by taking $R_1 = 0$. Region I in Fig. 9 can be achieved by taking $U = \emptyset$ and $V = X$, whereby the superposition coding reduces

to the combined secret key and secrecy coding as given in Section V-B. These achievable points together with their time sharing provide the individual secrecy capacity region as shown in Fig. 9.

3) If the eavesdropper's channel is *deterministic* in the manner that Z is a function of X, superposition coding is optimal for achieving individual secrecy capacity as we demonstrate in the Theorem 8.

Theorem 8. *For the BC-RSI channel with an external eavesdropper, if the eavesdropper's channel is* deterministic *in the manner that Z is a function of X, then the individual secrecy capacity region is given by the convex hull of the non-negative rate pairs (R_1, R_2) satisfying*

$$\begin{aligned} R_1 &\leq \min\{I(X;Y_1), \quad I(X;Y_1|Z) + R_2\}, \\ R_2 &\leq \min\{I(X;Y_2), \quad I(X;Y_2|Z) + R_1\}. \end{aligned} \tag{18}$$

Proof: The achievability is obtained by taking $U = Z$ and $V = X$ in (17). The proof of the converse is given in Appendix E. ■

In particular, if Y_1, Y_2 and Z are all functions of X, the above corollary simplifies to the following:

Corollary 9. *If the BC-RSI channel with an external eavesdropper is* deterministic *in the manner that Z, Y_1, and Y_2 are deterministic functions of X, then the individual secrecy capacity region is given by the convex hull of the non-negative rate pairs (R_1, R_2) satisfying*

$$\begin{aligned} R_1 &\leq \min\{H(Y_1), \quad H(Y_1|Z) + R_2\}, \\ R_2 &\leq \min\{H(Y_2), \quad H(Y_2|Z) + R_1\}. \end{aligned} \tag{19}$$

Remark 10. *Note that the* deterministic *BC is a more general model than the* linear deterministic *BC model discussed in Section IV. As a direct consequence, Theorem 2 can be regarded as a special case of Corollary 9.*

The region given in Theorem 7 fails to achieve any positive rates if the condition $I(V;Y_i|U) \geq I(V;Z|U)$ is not satisfied for either $i = 1$ or $i = 2$. For instance, when $I(V;Y_1|U) > I(V;Z|U) > I(V;Y_2|U)$ for a given input probability distribution, the requirement of decoding randomness (in V^n codewords) at the second receiver becomes excessive. To resolve this problem, we develop a Marton's coding approach in the following section, where we further introduce two individual satellite codewords (V_1^n, V_2^n), and require V_i^n to be decoded only at receiver i. This allows us to get a larger rate region for the *mixed* scenarios where the eavesdropper is stronger than one legitimate receiver but weaker than the other one.

D. Marton's coding

Although superposition coding demonstrates its optimality for some broadcast channels wherein one receiver is stronger than the other, it is not optimal in general. In fact, for broadcast channels, Marton's coding can outperform superposition coding by not requiring either receiver to recover both messages (for broadcast channels without any secrecy constraints) [47]. In the following, we consider achieving the indivudual secrey of the BC-RSI model, by utilizing the one-time pad signal as the cloud center, further

information on both messages being carried in the satellite codewords, and additional information on each messages being conveyed in individual satellite codewords. This coding scheme is built on the previous superposition coding scheme but with one more layer that employs Marton's coding. As a direct result, it generalizes the rate region established by superpostion coding. Moreover, we provide a special case under which this Marton's coding approach outperforms the aforementioned superposition approach (the region given in Theorem 7).

Theorem 11. *The individual secrecy rate region for the BC-RSI with an external eavesdropper is achievable for the set of the non-negative rate pairs* (R_1, R_2) *such that*

$$\begin{aligned} R_1 \leq & I(V_0, V_1; Y_1|U) - I(V_0, V_1; Z|U) + \min\{R_2,\ I(U; Y_1) + I(V_0; Z|U)\}; \\ R_2 \leq & I(V_0, V_2; Y_2|U) - I(V_0, V_2; Z|U) + \min\{R_1,\ I(U; Y_2) + I(V_0; Z|U)\}, \end{aligned} \tag{20}$$

over any $p(u, v_0, v_1, v_2, x) = p(u)p(v_0|u)p(v_1, v_2|v_0)p(x|v_1, v_2)$ *subject to* $I(V_1; V_2|V_0) \leq I(V_1; Z|V_0) + I(V_2; Z|V_0) - I(V_1, V_2; Z|V_0)$, $I(V_i; Y_i|V_0) \geq I(V_i; Z|V_0)$ *and* $I(V_0, V_i; Y_i|U) \geq I(V_0, V_i; Z|U)$ *for* $i = 1, 2$.

Proof: The proof is given in Appendix F. ■

The coding approach we develop here is built on the superposition coding which is discussed in Section V-C, but with one additional coding layer that employs Marton's coding. That is, we split M_i into $M_i = (M_{ik}, M_{isk}, M_{iss}, M_{ism})$, for $i = 1, 2$, where M_{ik}, M_{isk}, M_{iss} are encoded into U^n, V_0^n codewords in the same way as by the superposition coding; while information on M_{1sm}, M_{2sm} are carried by individual satellite codewords V_1^n, V_2^n, respectively, via Marton's coding. Note that the secrecy of M_{1sm}, M_{2sm} is ensured by additional randomness with the spirit of secrecy coding approach [3], [4].

As reflected in the obtained region in (20), for legitimate receiver i, part of the message, i.e., (M_{ik}, M_{isk}), is secured via one-time pad; while the other part, i.e., (M_{iss}, M_{ism}), is secured via secrecy coding. More specifically, for receiver 1, on one hand, (M_{1k}, M_{1sk}) is secured via one-time pad (with key rate R_2) in the underneath superposition coding structure (at most $I(U; Y_i)$ bits in the cloud center U^n and at most $I(V_0; Z|U)$ bits as randomness in the satellite codeword V_0^n). Thus, in total at most $\min\{R_2,\ I(U; Y_1) + I(V_0; Z|U)\}$ bits can be secured via one-time pad. On the other hand, M_{1ss}, M_{1sm} are secured via secrecy coding in V_0^n and V_1^n, respectively, which in total contribute $I(V_0, V_1; Y_1|U) - I(V_0, V_1; Z|U)$ secret bits.

Furthermore, we have the following observations:

- Letting $U = \emptyset$ and $R_k = R_{sk} = 0$ in the proof as given in Appendix F and applying Fourier-Motzkin procedure, an achievable region under the joint secrecy constraint (follows from the secrecy proof in Appendix F) can be obtained. And this region (i.e., (24)) improves the one given in (23) which coincides with the one established in [36].
- If we set $V_1 = V_2 = V_0$, it reduces to the superposition coding approach and achieves the rate region in (17) as given in Theorem 7.
- For the case where the eavesdropper's channel is less noisy than one legitimate receiver, but more noisy

than the other, (e.g.: Z is less noisy than Y_2, if $I(U;Z) \geq I(U;Y_2)$ for all $p(u)$ such that $U \to X \to (Y_2, Z)$ [47]), Marton's coding approach gives an achievable rate region by setting $U = V_0 = V_2$ in (20) as provided below.

Corollary 12. *For the BC-RSI with an external eavesdropper, if Z is less noisy than Y_2, then an achievable individual secrecy rate region is given by the union of non-negative rate pairs (R_1, R_2) satisfying*

$$\begin{aligned} R_1 &\leq I(V_1;Y_1|U) - I(V_1;Z|U) + R_2; \\ R_2 &\leq \min\{I(U;Y_2), R_1\}, \end{aligned} \tag{21}$$

where the union is taken over $p(u)p(v_1|u)p(x|v_1,u)$.

We recall that superposition coding is optimal in cases of either a *strong* or *weak* eavesdropper (compared to both legitimate receivers). However, in the *mixed* case, where the eavesdropper's channel is less noisy than one legitimate receiver, but more noisy than the other, superposition coding is no longer optimal.

For instance, consider the case where Z is strictly less noisy than Y_2, i.e., $I(V;Z) > I(V;Y_2)$ for any $p(v)$ s.t. $V \to X \to (Y_2, Z)$. In order to apply superposition coding, one has to set $V = U$ to satisfy the condition that $I(V;Y_2|U) \geq I(V;Z|U)$ given in (17) in Theorem 7. Therefore, the region in (17) reduces to the set of the non-negative rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\leq R_2; \\ R_2 &\leq \min\{I(U;Y_2), R_1\}. \end{aligned} \tag{22}$$

Compare the obtained region in (22) by superposition coding with the one in (21) by Marton's coding. It is easy to see that the Marton's coding outperforms in this case by not requiring the decoding of the corresponding individual satellite codeword at the weak receiver.

E. Joint secrecy rate region for BC-RSI with an external eavesdropper

As a by-product, achievable joint secrecy rate regions can be obtained by letting $U = \emptyset$ and $R_k = R_{sk} = 0$ in the superposition coding approach and Marton's coding approach proposed in previous subsections, which validity follows from the secrecy proof in Appendix C for superposition coding; and the secrecy proof in Appendix F for Marton's coding, respectively. Note that the achievable joint secrecy rate region by Marton's coding, i.e., (24), is derived with the addition of a time-sharing random variable Q.

Corollary 13. *(Achievable joint secrecy rate region by superposition coding) For BC-RSI with an external eavesdropper, an achievable region under the joint secrecy constraint can be obtained by superposition coding as the set of the non-negative rate pairs (R_1, R_2) such that*

$$\begin{aligned} R_1 &\leq I(V;Y_1) - I(V;Z) \\ R_2 &\leq I(V;Y_2) - I(V;Z) \end{aligned} \tag{23}$$

where $V \to X \to (Y_1, Y_2, Z)$ forms a Markov chain such that $I(V;Y_i) \geq I(V;Z)$ holds for $i = 1, 2$.

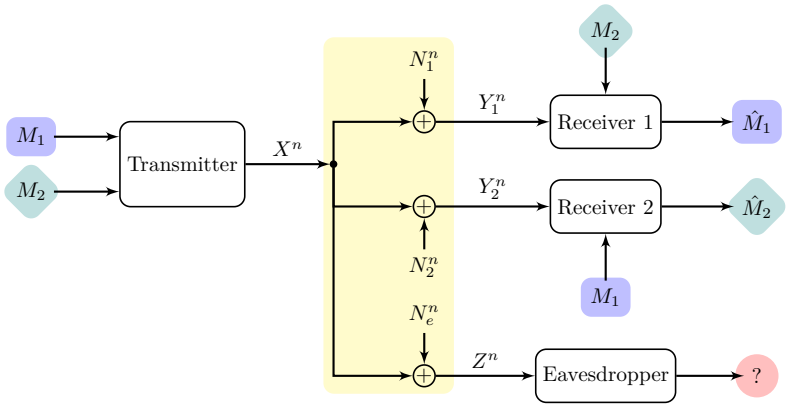


Fig. 10: Gaussian BC-RSI with an external eavesdropper.

Corollary 14. *(Achievable joint secrecy rate region by Marton's coding) For BC-RSI with an external eavesdropper, an achievable region under the joint secrecy constraint can be obtained by Marton's coding as the set of the non-negative rate pairs* (R_1, R_2) *such that*

$$\begin{aligned} R_1 &\le I(V_0, V_1; Y_1|Q) - I(V_0, V_1; Z|Q) \\ R_2 &\le I(V_0, V_2; Y_2|Q) - I(V_0, V_2; Z|Q) \\ R_1 + R_2 &\le I(V_0, V_1; Y_1|Q) + I(V_0, V_2; Y_2|Q) - 2I(V_0; Z|Q) - I(V_1; V_2|V_0, Q) \end{aligned} \tag{24}$$

over any $p(q, v_0, v_1, v_2, x) = p(q)p(v_0|q)p(v_1, v_2|v_0)p(x|v_1, v_2)$ *subject to* $I(V_1, V_2; Z|V_0) \le I(V_1; Z|V_0) + I(V_2; Z|V_0) - I(V_1; V_2|V_0)$ *and* $I(V_i; Z|V_0) \le I(V_i; Y_i|V_0)$ *for* $i = 1, 2$.

Remark 15. *The region by superposition coding given in* (23) *coincides with the one established in [36]. Note that* (23) *is included in* (24)*, i.e., the region by Marton's coding, as a special case of* (24) *by taking* $V_1 = V_2 = V_0$.

VI. Gaussian BC-RSI

In this section, we consider Gaussian broadcast channel with receiver side information (Gaussian BC-RSI) as shown in Fig. 10. It is known that one can apply the discretization procedure [47] to extend the coding schemes for finite alphabet channels to their Gaussian counterpart. Using this technique, we obtain an achievable individual secrecy rate region for the Gaussian BC-RSI. Furthermore, we derive an outer bound to the secrecy capacity region, and, show that, in the high SNR regime, one can approach the individual secrecy capacity region for the Gaussian BC-RSI by employing the superposition coding. This observation is consistent with the results suggested by the linear deterministic approach analyzed in Section IV.

Suppose X is the channel input with a power constraint P on it and the signals received by both receivers

and the eavesdropper are

$$Y_1 = X + N_1;$$

$$Y_2 = X + N_2;$$

$$Z = X + N_e,$$

where $N_1 \sim \mathcal{N}(0, \sigma_1^2)$, $N_2 \sim \mathcal{N}(0, \sigma_2^2)$ and $N_e \sim \mathcal{N}(0, \sigma_e^2)$ are additive white Gaussian noise (AWGN) independent of X. According to the noise level in the channels to both receives and the eavesdropper, the overall channel can be regarded to be *stochastically* degraded in different orders. For simplicity, we only consider their corresponding *physically* degraded instances. The reason is that the same analysis can be easily extended to the stochastically degraded cases. So the following scenarios are of our interest (without loss of generality we assume $\sigma_1 < \sigma_2$):

1) $\sigma_e^2 \geq \sigma_2^2 \geq \sigma_1^2$, i.e., $X \to Y_1 \to Y_2 \to Z$ forms a Markov chain,
2) $\sigma_2^2 \geq \sigma_1^2 \geq \sigma_e^2$, i.e., $X \to Z \to Y_1 \to Y_2$ forms a Markov chain, and
3) $\sigma_2^2 \geq \sigma_e^2 \geq \sigma_1^2$, i.e., $X \to Y_1 \to Z \to Y_2$ forms a Markov chain.

The individual secrecy capacity of the first two cases can be easily derived by extending the results for discrete memoryless channel model to the Gaussian scenario. For the third case, we show in the following that we can approach the individual secrecy capacity region as $P \gg \sigma_e^2$ or $P \ll \sigma_1^2$.

A. An outer bound

Proposition 16. *An outer bound of the individual secrecy capacity region for the Gaussian BC-RSI when $X \to Y_1 \to Z \to Y_2$ forms a Markov chain is given by the set of the rate pairs (R_1, R_2) satisfying*

$$\begin{aligned} R_2 \leq & C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P + \sigma_2^2}\right); \\ R_2 \leq R_1 \leq & C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_e^2}\right) + R_2, \end{aligned}$$

for some $\alpha, \gamma \in [0,1]$, and $C(x) = \frac{1}{2}\log(1+x)$ is the Gaussian capacity function.

Proof: We observe that

$$\begin{aligned} \frac{n}{2}\log 2\pi e\sigma_e^2 = h(Z^n|X^n) &= h(Z^n|M_1, M_2, X^n) \\ &\leq h(Z^n|M_1, M_2) \leq h(Z^n|M_2) \leq h(Z^n) \\ &\overset{(a)}{\leq} \frac{n}{2}\log 2\pi e(P + \sigma_e^2), \end{aligned}$$

where (a) is due to the fact that for a random variable with a fixed variance, Gaussian distribution maximizes the entropy. This shows that there exist $\alpha, \gamma \in [0,1]$, such that

$$h(Z^n|M_2) = \frac{n}{2}\log 2\pi e(\alpha P + \sigma_e^2); \tag{25}$$

$$h(Z^n|M_1, M_2) = \frac{n}{2}\log 2\pi e(\gamma\alpha P + \sigma_e^2). \tag{26}$$

In particular, we have

$$h(Z^n|M_1) = h(Z^n) - I(M_1; Z^n) \overset{(b)}{\geq} h(Z^n) - n\epsilon \geq h(Z^n|M_2) - n\epsilon = \frac{n}{2}\log 2\pi e(\alpha P + \sigma_e^2) - n\epsilon, \tag{27}$$

where (b) is due to the individual secrecy constraint.

Similarly, we have

$$\begin{aligned}\frac{n}{2}\log 2\pi e\sigma_2^2 = h(Y_2^n|X^n) &= h(Y_2^n|M_1, M_2, X^n)\\ &\leq h(Y_2^n|M_1, M_2) \leq h(Y_2^n|M_1) \leq H(Y_2^n)\\ &\overset{(a)}{\leq} \frac{n}{2}\log 2\pi e(P + \sigma_2^2).\end{aligned}$$

There must exist a β such that

$$h(Y_2^n|M_1, M_2) = \frac{n}{2}\log 2\pi e(\beta P + \sigma_2^2). \tag{28}$$

Therefore,

$$\begin{aligned}nR_2 = H(M_2) = H(M_2|M_1) &\overset{(c)}{=} I(M_2; Y_2^n|M_1) + nO(\epsilon)\\ &= h(Y_2^n|M_1) - h(Y_2^n|M_1, M_2) + nO(\epsilon)\\ &\overset{(d)}{\leq} \frac{n}{2}\log\frac{P + \sigma_2^2}{\beta P + \sigma_2^2} + nO(\epsilon),\end{aligned} \tag{29}$$

where (c) is due to the Fano's inequality and (d) is due to (28).

Recall the Markov chain $(M_1, M_2) \to X^n \to Y_1^n \to Z^n \to Y_2^n$. Applying the entropy power inequality (EPI) [47], we obtain

$$h(Y_2^n|M_1, M_2) \geq \frac{n}{2}\log\left[2^{\frac{2}{n}h(Z^n|M_1, M_2)} + 2\pi e(\sigma_2^2 - \sigma_e^2)\right].$$

Using (28) here, we obtain

$$h(Z^n|M_1, M_2) \leq \frac{n}{2}\log 2\pi e(\beta P + \sigma_e^2).$$

Comparing to (26) which gives that $h(Z^n|M_1, M_2) = \frac{n}{2}\log 2\pi e(\gamma\alpha P + \sigma_e^2)$, we have

$$\gamma\alpha \leq \beta. \tag{30}$$

Recall (29), we have

$$nR_2 \leq \frac{n}{2}\log\frac{P + \sigma_2^2}{\beta P + \sigma_2^2} + nO(\epsilon) \leq \frac{n}{2}\log\frac{P + \sigma_2^2}{\gamma\alpha P + \sigma_2^2} + nO(\epsilon) = nC\left(\frac{(1 - \gamma\alpha)P}{\gamma\alpha P + \sigma_2^2}\right) + nO(\epsilon).$$

Letting $\epsilon \to 0$, we obtain

$$R_2 \leq C\left(\frac{(1 - \gamma\alpha)P}{\gamma\alpha P + \sigma_2^2}\right). \tag{31}$$

Now we proceed to bound R_1. First we show $R_1 \geq R_2$ as follows.

$$\begin{aligned}nR_1 = H(M_1) &= H(M_1|M_2)\\ &\geq I(M_1; Y_1^n|M_2)\end{aligned}$$

$$
\begin{aligned}
&= I(M_1; Y_1^n, Z^n|M_2) - I(M_1; Z^n|M_2, Y_1^n) \\
&\overset{(e)}{=} I(M_1; Z^n|M_2) + I(M_1; Y_1^n|M_2, Z^n) \\
&= h(Z^n|M_2) - h(Z^n|M_1, M_2) + I(M_1; Y_1^n|M_2, Z^n) \\
&\geq h(Z^n|M_2) - h(Z^n|M_1, M_2) \\
&\overset{(f)}{\geq} h(Z^n) - h(Z^n|M_1, M_2) - nO(\epsilon) \\
&\geq h(Z^n|M_1) - h(Z^n|M_1, M_2) - nO(\epsilon) \\
&= I(M_2; Z^n|M_1) - nO(\epsilon) \\
&\overset{(g)}{\geq} I(M_2; Y_2^n|M_1) - nO(\epsilon) \\
&= H(M_2|M_1) - H(M_2|M_1, Y_2^n) - nO(\epsilon) \\
&\overset{(h)}{\geq} nR_2 - nO(\epsilon),
\end{aligned}
$$

where (e) follows by the fact that $I(M_1; Z^n|M_2, Y_1^n) = 0$, which is implied by $I(M_1, M_2; Z^n|Y_1^n) = 0$ due to the channel degradedness, i.e., the Markov chain $(M_1, M_2) \to X^n \to Y_1^n \to Z^n \to Y_2^n$; (f) is due to the individual secrecy constraint; and (g) is due to the channel degradedness, i.e., $(M_1, M_2) \to X^n \to Y_1^n \to Z^n \to Y_2^n$; (h) is due to the Fano's inequality.

Finally, letting $\epsilon \to 0$, we obtain

$$R_1 \geq R_2. \tag{32}$$

On the other hand, we have

$$
\begin{aligned}
nR_1 = H(M_1) &= H(M_1|M_2) \\
&\overset{(i)}{\leq} I(M_1; Y_1^n|M_2) + nO(\epsilon) \\
&= I(M_1; Y_1^n, Z^n|M_2) - I(M_1; Z^n|M_2, Y_1^n) + nO(\epsilon) \\
&\overset{(j)}{=} I(M_1; Z^n|M_2) + I(M_1; Y_1^n|M_2, Z^n) + nO(\epsilon) \\
&= h(Z^n|M_2) - h(Z^n|M_1, M_2) + I(M_1; Y_1^n|M_2, Z^n) + nO(\epsilon),
\end{aligned} \tag{33}
$$

where (i) is due to the Fano's inequality and (j) is due to the channel degradedness. Note that

$$
\begin{aligned}
I(M_1; Y_1^n|M_2, Z^n) &= h(Y_1^n|M_2, Z^n) - h(Y_1^n|M_1, M_2, Z^n) \\
&\leq h(Y_1^n|M_2, Z^n) - h(Y_1^n|M_1, M_2, X^n, Z^n) \\
&= h(Y_1^n|M_2, Z^n) - h(Y_1^n|X^n, Z^n) \\
&= h(Y_1^n, Z^n|M_2) - h(Z^n|M_2) - h(Y_1^n|X^n, Z^n) \\
&\overset{(k)}{=} h(Y_1^n|M_2) + h(Z^n|Y_1^n) - h(Z^n|M_2) - h(Y_1^n, Z^n|X^n) + h(Z^n|X^n) \\
&\overset{(k)}{=} h(Y_1^n|M_2) + h(Z^n|Y_1^n) - h(Z^n|M_2) - h(Y_1^n|X^n) - h(Z^n|Y_1^n) + h(Z^n|X^n)
\end{aligned}
$$

$$= h(Y_1^n|M_2) - h(Z^n|M_2) - h(Y_1^n|X^n) + h(Z^n|X^n), \tag{34}$$

where (k) follows by the fact that $h(Z^n|M_2, Y_1^n) = h(Z^n|Y_1^n)$ and $h(Z^n|X^n, Y_1^n) = h(Z^n|Y_1^n)$ due to the Markov chain $(M_1, M_2) \to X^n \to Y_1^n \to Z^n$.

Recall the Markov chain $(M_1, M_2) \to X^n \to Y_1^n \to Z^n \to Y_2^n$. We apply the EPI and obtain

$$h(Z^n|M_2) \geq \frac{n}{2} \log \left[2^{\frac{n}{2} h(Y_1^n|M_2)} + 2\pi e(\sigma_e^2 - \sigma_1^2) \right].$$

In addition to (25) which gives that $h(Z^n|M_2) = \frac{n}{2} \log 2\pi e(\alpha P + \sigma_e^2)$, we have

$$h(Y_1^n|M_2) \leq \frac{n}{2} \log 2\pi e(\alpha P + \sigma_1^2). \tag{35}$$

Combining (33) and (34), we have

$$\begin{aligned}
nR_1 &\leq h(Z^n|M_2) - h(Z^n|M_1, M_2) + I(M_1; Y_1^n|M_2, Z^n) \\
&\leq h(Y_1^n|M_2) - h(Z^n|M_1, M_2) - h(Y_1^n|X^n) + h(Z^n|X^n) \\
&= h(Z^n|M_1) - h(Z^n|M_1, M_2) + h(Y_1^n|M_2) - h(Z^n|M_1) - h(Y_1^n|X^n) + h(Z^n|X^n) \\
&= I(M_2; Z^n|M_1) + h(Y_1^n|M_2) - h(Z^n|M_1) - h(Y_1^n|X^n) + h(Z^n|X^n) \\
&\overset{(l)}{\leq} nR_2 + h(Y_1^n|M_2) - h(Z^n|M_1) - h(Y_1^n|X^n) + h(Z^n|X^n) \\
&= nR_2 + h(Y_1^n|M_2) - h(Z^n|M_1) - h(N_1^n) + h(N_e^n) \\
&\overset{(m)}{\leq} nR_2 + \frac{n}{2} \log \frac{(\alpha P + \sigma_1^2)\sigma_e^2}{(\alpha P + \sigma_e^2)\sigma_1^2} + nO(\epsilon) \\
&= nR_2 + nC\left(\frac{\alpha P}{\sigma_1^2}\right) - nC\left(\frac{\alpha P}{\sigma_e^2}\right) + nO(\epsilon),
\end{aligned}$$

where (l) is due to the fact that $I(M_2; Z^n|M_1) \leq H(M_2) = nR_2$; and (m) is due to (27) and (35).

Finally, letting $\epsilon \to 0$, we have

$$R_1 \leq C\left(\frac{\alpha P}{\sigma_1^2}\right) - \left(\frac{\alpha P}{\sigma_e^2}\right) + R_2. \tag{36}$$

Combining (31), (32), and (36) establishes the outer bound. ■

Remark 17. *Interestingly, $\gamma = 1$ corresponds to the joint secrecy constraint, since $\gamma = 1$ implies that $h(Z^n|M_1, M_2) = h(Z^n)$ according to* (26)*. However, in case of $(M_1, M_2) \to Y_1^n \to Z^n \to Y_2^n$, we have*

$$nR_2 = H(M_2) = I(M_2; Y_2^n|M_1) \leq I(M_1, M_2; Y_2^n) \leq I(M_1, M_2; Y_2^n, Z^n) = I(M_1, M_2; Z^n) = 0$$

under joint secrecy constraint. That is, only positive R_1 is possible. And, $R_1 \leq C\left(P/\sigma_1^2\right) - C\left(P/\sigma_e^2\right)$ is obtained by taking $\alpha = 1$ via Wyner's secrecy coding.

B. An inner bound

Proposition 18. *An inner bound of the individual secrecy capacity region for the Gaussian BC-RSI when $X \to Y_1 \to Z \to Y_2$ forms a Markov chain is given by the set of the rate pairs (R_1, R_2) satisfying*

$$\begin{aligned} R_2 \leq & C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P+\sigma_2^2}\right); \\ R_2 \leq R_1 \leq & C\left(\frac{\gamma\alpha P}{\sigma_1^2}\right) - C\left(\frac{\gamma\alpha P}{\sigma_e^2}\right) + R_2, \end{aligned}$$

where $\alpha, \gamma \in [0,1]$.

Proof: For a fixed pair $\alpha, \gamma \in [0,1]$, one can derive an inner bound of (R_1, R_2) by applying superposition coding as described in the following.

Codebook generation: Randomly and independently generate 2^{nR_2} sequences $u^n(k)$, $k \in [1 : 2^{nR_2}]$, each i.i.d. $\mathcal{N}(0, (1-\gamma\alpha)P)$; and $2^{n(R_1-R_2+R_r)}$ sequences $v^n(s,r)$, $(s,r) \in [1 : 2^{n(R_1-R_2)}] \times [1 : 2^{nR_r}]$, each i.i.d. $\mathcal{N}(0, \gamma\alpha P)$.

Encoding: To send the message pair (m_1, m_2) with $m_1 = (m_{1k}, m_{1s})$, where m_{1k} is of the same length as m_2, the encoder encapsulates m_{1k} and m_2 in m_k with $m_k \triangleq m_{1k} \oplus m_2$, randomly chooses $r \in [1 : 2^{nR_r}]$, and transmits $x^n(m_1, m_2) = u^n(m_k) + v^n(m_{1s}, r)$.

Decoding: Receiver 2 decodes m_k from $y_2^n = u^n(m_k) + (v^n(m_{1s}, r) + n_2^n)$ while treating $v^n(m_{1s}, r)$ as noise, and further recovers m_2 with his knowledge of m_1. The probability of decoding error tends to zero as $n \to \infty$ if $R_2 \leq C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P+\sigma_2^2}\right)$.

Receiver 1 uses successive cancellation. It first decodes m_k from $y_1^n = u^n(m_k) + (v^n(m_{1s}, r) + n_1^n)$ while treating $v^n(m_{1s}, r)$ as noise, and recovers part of m_1, i.e., m_{1k}, with the knowledge of m_2. The probability of this decoding error tends to zero as $n \to \infty$ if $R_2 \leq C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P+\sigma_2^2}\right)$, since it implies that $R_2 \leq C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P+\sigma_1^2}\right)$ due to the fact that $\sigma_1^2 \leq \sigma_2^2$. (This implies that $R_2 \leq R_1$.) Then, it subtracts off $u^n(m_k)$ and decodes $v^n(m_{1s}, r) + n_1^n$ to recover (m_{1s}, r) and thus m_{1s}, i.e., the rest of m_1. The probability of this decoding error tends to zero as $n \to \infty$ if $R_1 - R_2 + R_r \leq C\left(\frac{\gamma\alpha P}{\sigma_1^2}\right)$.

Secrecy: The eavesdropper could decode m_k from $z^n = u^n(m_k) + (v^n(m_{1s}, r) + n_e^n)$. However, m_k does not disclose any information about m_{1s} and m_2, individually. Subtracting off $u^n(m_k)$ from z^n, the eavesdropper gets a better observation $v^n(m_{1s}, r) + n_e^n$, which actually does not help to recover m_{1s} if $R_r \approx C\left(\frac{\gamma\alpha P}{\sigma_e^2}\right)$. In other words, the secrecy of m_{1s} is guaranteed by the embedded secrecy coding in the choice of v^n. The individual secrecy for m_1 then follows from an analysis similar to the previous sections.

As a conclusion, (R_1, R_2) is achievable under the individual secrecy constraints, once R_1, R_2, R_r satisfy

$$\begin{aligned} R_2 \leq & C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P+\sigma_2^2}\right); \\ R_1 - R_2 + R_r \leq & C\left(\frac{\gamma\alpha P}{\sigma_1^2}\right); \\ R_r \approx & C\left(\frac{\gamma\alpha P}{\sigma_e^2}\right). \end{aligned}$$

Eliminating R_r, we get the desired region of (R_1, R_2), which concludes our proof of achievability. ■

C. Individual secrecy capacity region

Proposition 19. *When $\sigma_2^2 \geq \sigma_e^2 \geq \sigma_1^2$, and $P \gg \sigma_2^2$ or $P \ll \sigma_1^2$, the individual secrecy capacity region for the Gaussian BC-RSI is given as the set of (R_1, R_2) satisfying*

$$\begin{aligned} R_2 \leq & C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P+\sigma_2^2}\right); \\ R_1 \leq & C\left(\frac{\gamma\alpha P}{\sigma_1^2}\right) - C\left(\frac{\gamma\alpha P}{\sigma_e^2}\right) + R_2, \end{aligned}$$

where $\gamma, \alpha \in [0,1]$.

Proof: Consider the gap between the inner and outer bounds derived in previous subsections. If we take the same choice of α, γ in both bounds, the gap occurs only in R_1, which is given by

$$C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_e^2}\right) - C\left(\frac{\gamma\alpha P}{\sigma_1^2}\right) + C\left(\frac{\gamma\alpha P}{\sigma_e^2}\right) = \frac{1}{2}\log\frac{(\alpha P+\sigma_1^2)(\gamma\alpha P+\sigma_e^2)}{(\alpha P+\sigma_e^2)(\gamma\alpha P+\sigma_1^2)} \to 0,$$

as $P \gg \sigma_e^2$ or $P \ll \sigma_1^2$, regardless of the values of α, γ. ■

As a conclusion, we characterize the individual secrecy capacity region for the Gaussian BC-RSI as follows.

Proposition 20. *The individual secrecy capacity region for the Gaussian BC-RSI is given by the following set of (R_1, R_2):*

- *If $\sigma_e^2 \geq \sigma_2^2 \geq \sigma_1^2$:*

$$\begin{aligned} R_1 \leq & \min\left\{C\left(\frac{P}{\sigma_1^2}\right) - C\left(\frac{P}{\sigma_e^2}\right) + R_2, C\left(\frac{P}{\sigma_1^2}\right)\right\}; \\ R_2 \leq & \min\left\{C\left(\frac{P}{\sigma_2^2}\right) - C\left(\frac{P}{\sigma_e^2}\right) + R_1, C\left(\frac{P}{\sigma_2^2}\right)\right\}, \end{aligned}$$

- *If $\sigma_2^2 \geq \sigma_1^2 \geq \sigma_e^2$:*

$$R_1 = R_2 \leq C\left(\frac{P}{\sigma_2^2}\right),$$

- *If $\sigma_2^2 \geq \sigma_e^2 \geq \sigma_1^2$, and, $P \gg \sigma_2^2$ or $P \ll \sigma_1^2$:*

$$\begin{aligned} R_1 \leq & C\left(\frac{\gamma P}{\sigma_1^2}\right) - C\left(\frac{\gamma P}{\sigma_e^2}\right) + R_2; \\ R_2 \leq & C\left(\frac{(1-\gamma)P}{\gamma P+\sigma_2^2}\right), \quad \textit{where } \gamma \in [0,1]. \end{aligned}$$

VII. Conclusion

In this paper, we studied the problem of secure communication over BC-RSI under the individual secrecy constraints. We first characterized the individual secrecy capacity region for the linear deterministic channel model. Then, utilizing secret key, secrecy coding, superposition coding, and Marton's coding approaches, we derived achievable rate regions for the discrete memoryless model. Together with converse arguments, these techniques allow us to characterize the individual secrecy capacity region for some specific scenarios

which include 1) the case of a *strong* eavesdropper (as a line on (R_1, R_2) plane); 2) the case of a *weak* eavesdropper (as a rectangle with missing corners); and 3) the case that the eavesdropper's channel is deterministic. Our results exhibit the coupling between the communication rates. In particular, we observe that one can not arbitrarily decrease one user's rate without sacrificing the rate of the other. Moreover, we studied the corresponding Gaussian scenario, where, in addition to the capacity regions for strong and weak eavesdropper cases, we established the individual secrecy capacity region for the low and high SNR regimes when the eavesdropper channel is weaker than one of the legitimate receivers but stronger than the other.

We here point out some avenues for further research. First, the characterization of the individual secrecy capacity region for the general case remains as an open problem. In particular, the characterization of the capacity region for the *mixed* case (where the eavesdropper channel is less noisy than one legitmate receiver but more noisy than the other) has resisted our best efforts thus far. (For the Gaussian case, we were able to establish low and high SNR individual secrecy capacity results in this scenario.) Remarkably, this mixed case is distinctive for the study on secure communication via broadcast channels (with RSI or without RSI) since in this case, positive rate pairs are attainable under the *individual secrecy* constraint but impossible under the *joint secrecy* constraint. We believe that our results will initiate the study of *individual secrecy* for other multi-terminal models. During the preparation of this manuscript, we have noticed that the parallel work [40] has considered the extension of BC-RSI model to include common messages. Studying other channel models under the lens of individual secrecy and comparing this notion to other secrecy constraints will be of interest.

Appendix A
Upper bound on the individual secrecy rate

An upper bound on the individual secrecy rate follows from the results for wiretap channel with shared key [24] as provided below.

Lemma 21. *For any R_2 in the achievable region, R_1 is upper bounded as*

$$R_1 \leq \max_{U \to V \to X \to (Y_1, Z)} \min\{I(V;Y_1|U) - I(V;Z|U) + R_2, I(V;Y_1)\}.$$

If the channel to the legitimate receiver 1 is degraded with respect to the channel to the eavesdropper, then for any R_2 in the achievable region, R_1 is upper bounded by

$$R_1 \leq \max_{X \to Y_1 \to Z} \min\{I(X;Y_1) - I(X;Z) + R_2, I(X;Y_1)\}.$$

Similar results hold for interchanging 1 *and* 2 *above.*

Proof: The proof follows by the result given for the wiretap channel with shared key [24, Theorem 1]. As the rate for M_2 is R_2, then the secrecy rate for receiver 1 can be upper bounded by the wiretap channel with shared key of rate R_2. ■

Appendix B
Achievability Proof for Theorem 2

For each scenario, a specific coding scheme is provided, where for a given $m_1 = [m_1(1), \cdots, m_1(R_1)]$ and $m_2 = [m_2(1), \cdots, m_2(R_2)]$, we construct the codeword $X = [x(1), x(2), \cdots, x(n_1)]^T$.

A. $q = n_1 \geq n_2 \geq n_e$

1) $R_1 < R_2$ and $R_1 < n_e$: We have

$$R_1 < n_e; \quad R_1 < R_2 \leq n_2 - n_e + R_1. \tag{37}$$

We set

$$x(k) = \begin{cases} m_1(k) \oplus m_2(k) & 1 \leq k \leq R_1 \\ r(k) & R_1 < k \leq n_e \\ m_2(k - n_e + R_1) & n_e < k \leq n_e + R_2 - R_1 \\ r(k) & n_e + R_2 - R_1 < k \leq n_1 \end{cases}$$

where $r(k)$ is randomly chosen from $\{0, 1\}$. The construction of X is illustrated in Fig. 11. In this scenario, receiver 2 could recover m_2 completely only if $R_2 - R_1 + n_e \leq n_2$. Combining this with the aforementioned conditions, $R_1 < R_2$ and $R_1 < n_e$, we obtain the desired region of (R_1, R_2) as specified in (37).

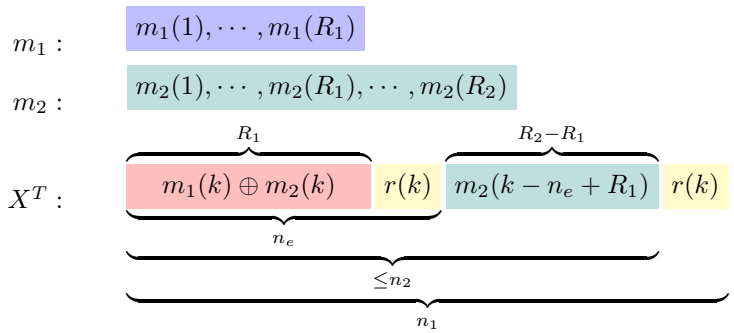


Fig. 11: Codeword X for $n_1 \geq n_2 \geq n_e$ and $R_1 < R_2, R_1 < n_e$.

2) $R_1 < R_2$ and $n_e \leq R_1$: We have

$$n_e \leq R_1 < R_2 \leq n_2. \tag{38}$$

We set

$$x(k) = \begin{cases} m_1(k) \oplus m_2(k) & 1 \leq k \leq R_1 \\ m_2(k) & R_1 < k \leq R_2 \\ r(k) & R_2 < k \leq n_1, \end{cases}$$

where $r(k)$ is randomly chosen from $\{0, 1\}$. The construction of X is illustrated in Fig. 12. In this scenario, receiver 2 could recover m_2 completely only if $R_2 \leq n_2$. Combining this with the aforementioned conditions, $n_e \leq R_1 < R_2$, we obtain the desired region of (R_1, R_2) as specified in (38).

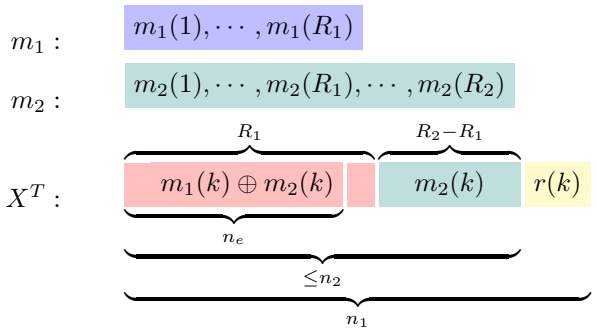


Fig. 12: Codeword X for $n_1 \geq n_2 \geq n_e$ and $n_e \leq R_1 < R_2$.

3) $R_1 \geq R_2$ and $R_2 < n_e$: We have

$$R_2 < n_e; \quad R_2 \leq R_1 \leq n_1 - n_e + R_2. \tag{39}$$

We set

$$x(k) = \begin{cases} m_1(k) \oplus m_2(k) & 1 \leq k \leq R_2 \\ r(k) & R_2 < k \leq n_e \\ m_1(k - n_e + R_2) & n_e + 1 \leq k \leq n_e + R_1 - R_2 \\ r(k) & n_e + R_1 - R_2 < k \leq n_1 \end{cases}$$

where $r(k)$ is randomly chosen from $\{0, 1\}$. The construction of X is illustrated in Fig. 13. In this scenario, receiver 1 could recover m_1 completely only if $R_1 - R_2 + n_e \leq n_1$. Combining this with the aforementioned conditions, i.e., $R_1 \geq R_2$ and $R_2 < n_2$, we obtain the desired region of (R_1, R_2) as specified in (39).

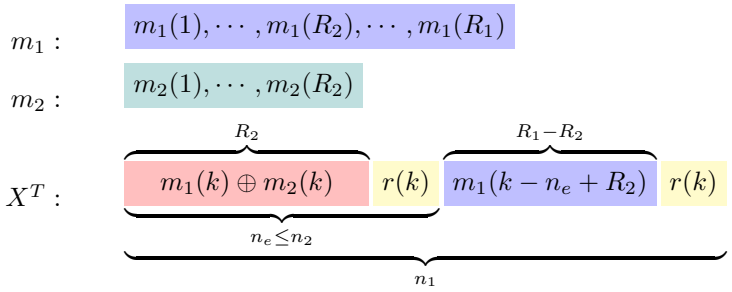


Fig. 13: Codeword X for $n_1 \geq n_2 \geq n_e$ and $R_1 \geq R_2, R_2 < n_e$.

4) $R_1 \geq R_2$ and $n_e \leq R_2$: We have

$$R_2 \leq n_2; \quad n_e \leq R_2 \leq R_1 \leq n_1. \tag{40}$$

We set

$$x(k) = \begin{cases} m_1(k) \oplus m_2(k) & 1 \leq k \leq R_2 \\ m_1(k) & R_2 < k \leq R_1 \\ r(k) & R_1 < k \leq n_1, \end{cases}$$

where $r(k)$ is randomly chosen from $\{0,1\}$. The construction of X is illustrated in Fig. 14. In this scenario, receiver 2 could recover m_2 completely only if $R_2 \leq n_2$; and receiver 1 could recover m_1 completely only if $R_1 \leq n_1$. Combining this with the aforementioned assumptions, $n_e \leq R_2 \leq R_1$, we obtain the desired region of (R_1, R_2) as specified in (40).

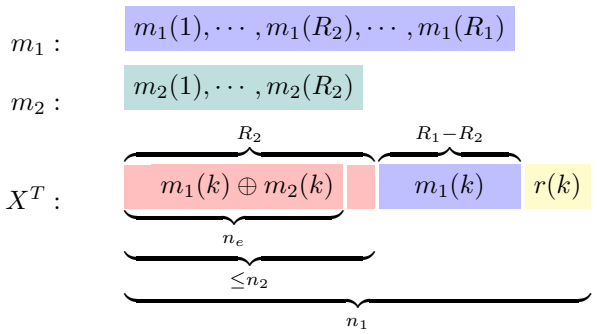


Fig. 14: Codeword X for $n_1 \geq n_2 \geq n_e$ and $n_e \leq R_2 \leq R_1$.

B. $q = n_1 \geq n_e \geq n_2$

Since $R_2 \leq n_2 \leq n_e$, we have

$$R_2 \leq n_2; \quad R_2 \leq R_1 \leq n_1 - n_e + R_2. \tag{41}$$

We set

$$x(k) = \begin{cases} m_1(k) \oplus m_2(k) & 1 \leq k \leq R_2 \\ r(k) & R_2 < k \leq n_e \\ m_1(k - n_e + R_2) & n_e < k \leq n_e + R_1 - R_2 \\ r(k) & n_e + R_1 - R_2 < k \leq n_1 \end{cases}$$

where $r(k)$ is randomly chosen from $\{0,1\}$. The construction of X is illustrated in Fig. 15. In this case, receiver 2 could recover m_2 completely only if $R_2 \leq n_2$; and receiver 1 could recover m_1 completely only if $R_1 - R_2 + n_e \leq n_1$. Combining these with the fact $R_1 - R_2 \geq 0$, which is implied by the code construction, we obtain the desired region of (R_1, R_2) as specified in (41).

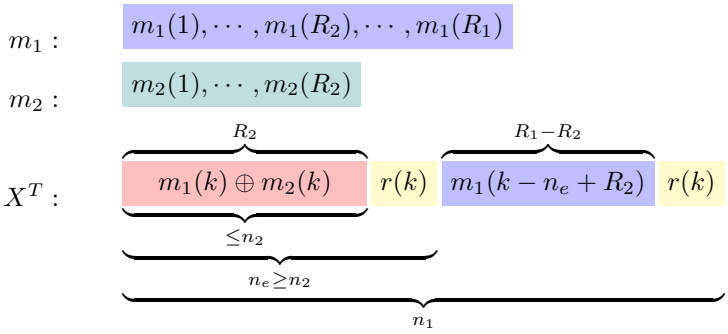


Fig. 15: Codeword X for $n_1 \geq n_e \geq n_2$.

C. $q = n_e \geq n_1 \geq n_2$

In this case, we have $R_1 \leq R_2$ and $R_2 \leq R_1$ both holds. This gives that

$$R_1 = R_2 = R \leq \min\{n_1, n_2\}. \tag{42}$$

We set

$$x(k) = \begin{cases} m_1(k) \oplus m_2(k) & 1 \leq k \leq R \\ r(k) & R < k \leq n_e, \end{cases}$$

where $r(k)$ is randomly chosen from $\{0, 1\}$. The construction of X is illustrated in Fig. 16. In this scenario, both receivers could recover m_1, m_2, respectively, only if $R \leq \min\{n_1, n_2\}$. Combining this with the fact $R_1 = R_2 = R$, which is implied by the code construction, we obtain the desired region of (R_1, R_2) as specified in (42).

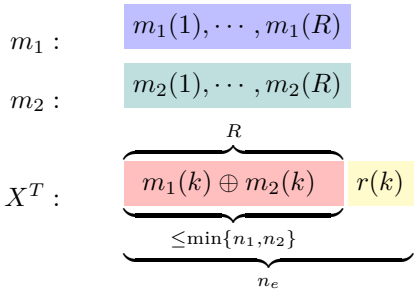


Fig. 16: Codeword X for $n_e \geq n_1 \geq n_2$.

Remark 22. *Note that in our achievability schemes, the elements of the input vector X are i.i.d. Bern($\frac{1}{2}$) in all scenarios. That is, Bern($\frac{1}{2}$) serves as an optimal input distribution to achieve the individual secrecy capacity. Nevertheless, this choice is not the only optimal one. As an alternative, instead of choosing as uniformly random, one can simply use zeros for the bits represented by $r(k)$ in our achievability schemes.*

Appendix C
Proof of Theorem 7

Rate splitting: As illustrated in Fig. 17, we split $M_1 = (M_{1k}, M_{1sk}, M_{1s})$ and $M_2 = (M_{2k}, M_{2sk}, M_{2s})$, with both M_{1k} and M_{2k} of entropy nR_k, both M_{1sk} and M_{2sk} of entropy nR_{sk}, M_{1s} of entropy nR_{1s} and M_{2s} of entropy nR_{2s}. Thus, we have $R_1 = R_k + R_{sk} + R_{1s}$ and $R_2 = R_k + R_{sk} + R_{2s}$.

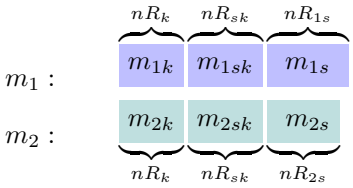


Fig. 17: Superposition coding: Rate splitting.

Codebook generation: Fix $p(u), p(v|u)$. First, randomly generate 2^{nR_k} i.i.d. sequences $u^n(k)$, $k \in [1 : 2^{nR_k}]$, according to $p(u)$. Secondly, for each $u^n(k)$, according to $p(v|u)$, randomly generate i.i.d. sequences $v^n(k, m_{sk}, m_{1s}, m_{2s}, r)$ with $(m_{sk}, m_{1s}, m_{2s}, r) \in [1 : 2^{nR_{sk}}] \times [1 : 2^{nR_{1s}}] \times [1 : 2^{nR_{2s}}] \times [1 : 2^{nR_r}]$.

Encoding: To send messages (m_1, m_2), choose $u^n(k)$, where $k = m_k \triangleq m_{1k} \oplus m_{2k}$. Given $u^n(k)$, randomly choose $r \in [1 : 2^{nR_r}]$ and find $v^n(k, m_{sk}, m_{1s}, m_{2s}, r)$, where $m_{sk} \triangleq m_{1sk} \oplus m_{2sk}$. The choice of u^n, v^n for given (m_1, m_2) is illustrated in Fig. 18. Generate x^n according to $p(x|v)$, and transmit it to the channel.

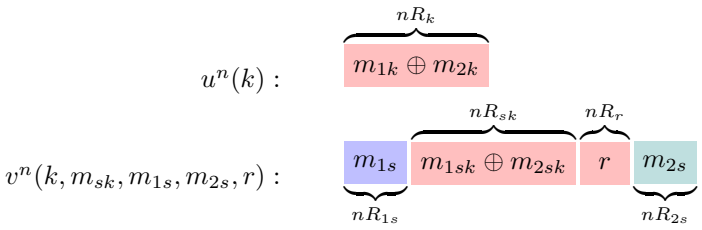


Fig. 18: Superposition coding: Encoding.

Decoding: Receiver 1, upon receiving y_1^n and with knowledge of m_2, decodes $\hat{m}_1 = (m_{2k} \oplus \hat{k}, m_{2sk} \oplus \hat{m}_{sk}, \hat{m}_{1s})$ if $(\hat{k}, \hat{m}_{sk}, \hat{m}_{1s}, m_{2s})$ is the unique quadruple such that $(u^n(\hat{k}), v^n(\hat{k}, \hat{m}_{sk}, \hat{m}_{1s}, m_{2s}, \hat{r}), y_1^n)$ is jointly typical.

Receiver 2, upon receiving y_2^n and with knowledge of m_1, decodes $\tilde{m}_2 = (m_{1k} \oplus \tilde{k}, m_{1sk} \oplus \tilde{m}_{sk}, \tilde{m}_{2s})$, if $(\tilde{k}, \tilde{m}_{sk}, m_{1s}, \tilde{m}_{2s})$ is the unique quadruple such that $(u^n(\tilde{k}), v^n(\tilde{k}, \tilde{m}_{sk}, m_{1s}, \tilde{m}_{2s}, \tilde{r}), y_2^n)$ is jointly typical.

Analysis of the error probability of decoding: Assume that $(M_1, M_2) = (m_1, m_2)$ with $m_1 = (m_{1k}, m_{1sk}, m_{1s})$, $m_2 = (m_{2k}, m_{2sk}, m_{2s})$ is sent. Or, more specifically, k, m_{sk}, m_{1s} and m_{2s} are sent, where $k \triangleq m_{1k} \oplus m_{2k}$ and $m_{sk} = m_{1sk} \oplus m_{2sk}$.

At receiver 1, i.e., for $P_{e,1}$, a decoding error happens if receiver 1's estimate is $u^n(\hat{k})$, $v^n(\hat{k}, \hat{m}_{sk}, \hat{m}_{1s}, m_{2s}, \hat{r})$ with $(\hat{k}, \hat{m}_{sk}, \hat{m}_{1s}) \neq (k, m_{sk}, m_{1s})$. In more details, the error event can be partitioned into the followings:

1) Error event corresponds to $\hat{k} \neq k$. Note that this event occurs with arbitrarily small probability if

$$R_1 + R_r \leq I(U, V; Y_1) = I(V; Y_1). \tag{43}$$

2) Error event corresponds to $\hat{k} = k$, but $(\hat{m}_{1s}, \hat{m}_{sk}) \neq (m_{1s}, m_{sk})$ Note that this event occurs with arbitrarily small probability if

$$R_{sk} + R_{1s} + R_r \leq I(V; Y_1|U). \tag{44}$$

Similar analysis can be done at the receiver 2, from which the decoding error probability $P_{e,2}$ can be made arbitrarily small if

$$R_2 + R_r \leq I(V; Y_2) \tag{45}$$

$$R_{sk} + R_{2s} + R_r \leq I(V; Y_2|U) \tag{46}$$

Analysis of individual secrecy: Due to the symmetric roles of receiver 1 and receiver 2, we only need to prove the secrecy of one message (e.g., M_1). The proof for the other case (e.g., the secrecy of M_2) follows similarly. For the secrecy of M_1, we have

$$\begin{aligned}
I(M_1;Z^n) =& I(M_{1k}, M_{1sk}, M_{1s}; Z^n) \\
=& I(M_{1k};Z^n) + I(M_{1sk}, M_{1s}; Z^n|M_{1k}) \\
\overset{(a)}{=}& I(M_{1sk}, M_{1s}; Z^n|M_{1k}) \\
=& I(M_{1sk};Z^n|M_{1k}) + I(M_{1s}; Z^n|M_{1k}, M_{1sk}) \\
\overset{(b)}{=}& I(M_{1s}; Z^n|M_{1k}, M_{1sk}) \\
=& H(M_{1s}) - H(M_{1s}|M_{1k}, M_{1sk}, Z^n) \\
\overset{(c)}{\leq}& nR_{1s} - H(M_{1s}|M_k, Z^n),
\end{aligned}$$

where (a) is due to the fact that $I(M_{1k};Z^n) = 0$ by $I(M_{1k};Z^n) \leq I(M_{1k};Z^n, M_k) = I(M_{1k};M_k) = 0$, which follows by the Markov chain $M_{1k} \to M_k \to Z^n$; (b) follows the fact that $I(M_{1sk};Z^n|M_{1k}) = 0$ as $H(M_{1sk}|Z^n, M_{1k}) \geq H(M_{1sk}|Z^n, M_{1k}, M_{sk}) = H(M_{1sk}|M_{sk}) = H(M_{1sk}) = H(M_{1sk}|M_{1k})$; (c) is due to the fact that $H(M_{1s}|M_{1k}, M_{1sk}, Z^n) \geq H(M_{1s}|M_{1k}, M_k, M_{1sk}, Z^n) = H(M_{1s}|M_k, Z^n)$, where the last equality follows as M_{1k}, M_{1sk} are independent of M_{1s} given M_k, Z^n, which is due to the Markov chain $M_{1s} \to (Z^n, M_k) \to (M_{1k}, M_{1sk})$.

To complete the proof that $I(M_1;Z^n) \leq n\delta'(\epsilon)$, we show in the following that $H(M_{1s}, M_{2s}|M_k, Z^n) \geq n(R_{1s} + R_{2s}) - n\delta'(\epsilon)$, which implies that $H(M_{1s}|M_k, Z^n) \geq nR_{1s} - n\delta'(\epsilon)$.

$$\begin{aligned}
H(M_{1s}, M_{2s}|M_k, Z^n) \overset{(d)}{=}& H(M_{1s}, M_{2s}|U^n, Z^n) \\
=& H(M_{1s}, M_{2s}, Z^n|U^n) - H(Z^n|U^n) \\
=& H(M_{1s}, M_{2s}, Z^n, V^n|U^n) - H(V^n|U^n, M_{1s}, M_{2s}, Z^n) - H(Z^n|U^n) \\
=& H(V^n|U^n) + H(Z^n|U^n, V^n) - H(V^n|U^n, M_{1s}, M_{2s}, Z^n) - H(Z^n|U^n) \\
\overset{(e)}{\geq}& n(R_{sk} + R_{1s} + R_{2s} + R_r) + nH(Z|U,V) - nH(Z|U) - n\epsilon \\
\overset{(f)}{=}& n(R_{1s} + R_{2s}) - n\delta'(\epsilon)
\end{aligned}$$

where (d) is due to the fact that U^n is uniquely determined by M_k; (e) follows by $H(V^n|U^n) = n(R_{sk} + R_{1s} + R_{2s} + R_r)$ by the codebook construction and the choice of V^n is randomly chosen based on $M_K, M_{sk}, M_{1s}, M_{2s}$ which are presumed to be uniformly distributed; Moreover, since the channel is discrete memoryless, we have $H(Z^n|U^n, V^n) = \sum_{i=1}^n H(Z_i|U_i, V_i) = nH(Z|U,V)$; and, $H(V^n|U^n, M_{1s}, M_{2s}, Z^n) \leq n\epsilon$ due to Fano's inequality by taking

$$R_{sk} + R_r \leq I(V;Z|U) - \epsilon', \tag{47}$$

since the eavesdropper can decode V^n reliably by using typical set decoding given $(U^n, M_{1s}, M_{2s}, Z^n)$; and $H(Z^n|U^n) = \sum_{i=1}^n H(Z_i|Z^{i-1}, U^n) \leq \sum_{i=1}^n H(Z_i|U_i) = nH(Z|U)$; (f) holds by taking

$$R_{sk} + R_r \geq I(V;Z|U) - 2\epsilon' \tag{48}$$

and $\delta'(\epsilon) = \epsilon + 2\epsilon'$.

Achievable rate region: Combining the followings:

- the non-negativity for rates, i.e.,
$$R_k, R_{sk}, R_{1s}, R_{2s}, R_r \geq 0;$$
- the rate relations imposed by rate splitting, i.e.,
$$R_1 = R_k + R_{sk} + R_{1s},$$
$$R_2 = R_k + R_{sk} + R_{2s};$$
- the constraints for a reliable communication to both legitimate receivers, i.e., (43)-(46):
$$R_1 + R_r \leq I(V;Y_1),$$
$$R_2 + R_r \leq I(V;Y_2),$$
$$R_{sk} + R_{1s} + R_r \leq I(V;Y_1|U),$$
$$R_{sk} + R_{2s} + R_r \leq I(V;Y_2|U);$$
- the constraints for individual secrecy of the messages at the eavesdropper, i.e., (47)-(48):
$$R_{sk} + R_r \approx I(V;Z|U).$$

Eliminating $R_r, R_k, R_{sk}, R_{1s}, R_{2s}$ by applying Fourier-Motzkin procedure [47], we obtain a region as the union of the set of non-negative (R_1, R_2) pairs satisfying

$$\begin{aligned} R_1 &\leq \min\{I(V;Y_1), \quad I(V;Y_1|U) - I(V;Z|U) + R_2\}; \\ R_2 &\leq \min\{I(V;Y_2), \quad I(V;Y_2|U) - I(V;Z|U) + R_1\}. \end{aligned} \tag{49}$$

where the union is taken over all $p(u)p(v|u)p(x|v)$ subject to $I(V;Y_i|U) \geq I(V;Z|U)$ for $i = 1, 2$.

Appendix D
Discussion on Rate splitting in Superposition Coding

Rate splitting: As illustrated in Fig. 19, we represent M_1, M_2 by $M_1 = (M_{1k}, M_{1sk}, M_{1s}, M_{1m})$ and $M_2 = (M_{2k}, M_{2sk}, M_{2s}, M_{2m})$ with M_{1k}, M_{2k} of entropy nR_k; M_{1sk}, M_{2sk} of entropy nR_{sk}; while M_{1s}, M_{1m} of entropy nR_{1s}, nR_{1m}; and M_{2s}, M_{2m} of entropy nR_{2s}, nR_{2m}, respectively. For simplicity, we denote $M_k = M_{1k} \oplus M_{2k}$, $M_{sk} = M_{1sk} \oplus M_{2sk}$, $M_{ss} = (M_{1s}, M_{2s})$ and $M_{sm} = (M_{1m}, M_{2m})$.

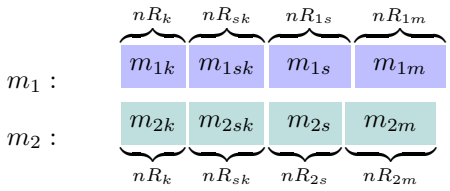


Fig. 19: Superposition coding: Rate splitting.

Codebook generation: Fix $p(u), p(v|u)$ and $p(t|v)$.

First, randomly generate 2^{nR_k} i.i.d. sequences $u^n(k)$, $k \in [1 : 2^{nR_k}]$, according to $p(u)$.

For each $u^n(k)$, according to $p(v|u)$, randomly generate $2^{n(R_{1s}+R_{2s}+R_{sk}+R_r)}$ i.i.d. sequences $v^n(k, ss_1, ss_2, sk, r)$ with $(ss_1, ss_2, sk, r) \in [1 : 2^{nR_{1s}}] \times [1 : 2^{nR_{2s}}] \times [1 : 2^{nR_{sk}}] \times [1 : 2^{nR_r}]$.

For each fixed $u^n(k)$ and $v^n(k, ss_1, ss_2, sk, r)$, randomly generate $2^{n(R_{1m}+R_{2m}+R_{r_1})}$ i.i.d. sequences t^n with indices $(k, ss_1, ss_2, sk, r, sm_1, sm_2, r_1)$, where $(sm_1, sm_2, r_1) \in [1 : 2^{nR_{1m}}] \times [1 : 2^{nR_{2m}}] \times [1 : 2^{nR_{r_1}}]$, according to $p(t|v)$.

Encoding: To send messages (m_1, m_2), choose $u^n(k)$, where $k = m_k \triangleq m_{1k} \oplus m_{2k}$.

Given $u^n(k)$, randomly choose $r \in [1 : 2^{nR_r}]$ and find the corresponding $v^n(k, m_{1s}, m_{2s}, m_{sk}, r)$, where $m_{sk} \triangleq m_{1sk} \oplus m_{2sk}$.

Given $u^n(k)$ and $v^n(k, m_{1s}, m_{2s}, m_{sk}, r)$, randomly choose $r_1 \in [1 : 2^{nR_{r_1}}]$, and send the corresponding codeword t^n with index $(k, m_{1s}, m_{2s}, m_{sk}, r, m_{1m}, m_{2m}, r_1)$.

The choice of u^n, v^n and t^n for given (m_1, m_2) is illustrated in Fig. 20.

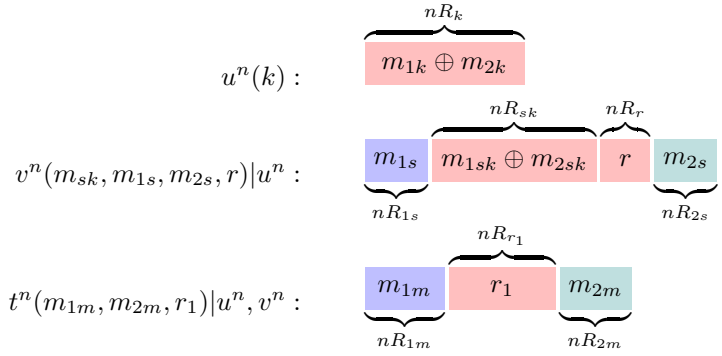


Fig. 20: Superposition coding: Encoding.

Decoding: Receiver 1, upon receiving y_1^n and with the side information m_2, decodes $\hat{m}_1 = (m_{2k} \oplus \hat{k}, m_{2sk} \oplus \hat{m}_{sk}, \hat{m}_{1s}, \hat{m}_{1m})$, if $(\hat{k}, \hat{m}_{sk}, \hat{m}_{1s}, m_{2s}, \hat{r}, \hat{m}_{1m}, m_{2m})$ is the unique tuple such that $(\hat{u}^n, \hat{v}^n, \hat{t}^n, y_1^n)$ is jointly typical, where $\hat{u}^n, \hat{v}^n, \hat{t}^n$ are with indices $(\hat{k}, \hat{m}_{sk}, \hat{m}_{1s}, m_{2s}, \hat{r}, \hat{m}_{1m}, m_{2m}, \hat{r}_1)$.

And, receiver 2, upon receiving y_2^n and with the side information m_1, decodes $\tilde{m}_2 = (m_{1k} \oplus \tilde{k}, m_{1sk} \oplus \tilde{m}_{sk}, \tilde{m}_{2s}, \tilde{m}_{2m})$, if $(\tilde{k}, \tilde{m}_{sk}, m_{1s}, \tilde{m}_{2s}, \tilde{r}, m_{1m}, \tilde{m}_{2m})$ is the unique tuple such that $(\tilde{u}^n, \tilde{v}^n, \tilde{t}^n, y_1^n)$ is jointly typical, where $\hat{u}^n, \hat{v}^n, \hat{t}^n$ are with indices $(\tilde{k}, \tilde{m}_{sk}, m_{1s}, \tilde{m}_{2s}, \tilde{r}, m_{1m}, \tilde{m}_{2m}, \tilde{r}_1)$.

Analysis of decoding error: Assume that $m_1 = (m_{1k}, m_{1sk}, m_{1s}, m_{1m})$, $m_2 = (m_{2k}, m_{2sk}, m_{2s}, m_{2m})$ is sent, i.e., more specifically, $k, m_{sk}, m_{1s}, m_{1m}$ and m_{2s}, m_{2m} are sent, where $k \triangleq m_{1k} \oplus m_{2k}$ and $m_{sk} = m_{1sk} \oplus m_{2sk}$.

For $P_{e,1}$, a decoding error happens if receiver 1's estimate is $(\hat{u}^n, \hat{v}^n, \hat{t}^n)$ with indices $(\hat{k}, \hat{m}_{1s}, m_{2s}, \hat{m}_{sk}, \hat{r}, \hat{m}_{1m}, m_{2m}, \hat{r}_1)$ such that $(\hat{k}, \hat{m}_{1s}, \hat{m}_{sk}, \hat{r}, \hat{m}_{1m}) \neq (k, m_{1s}, m_{sk}, r, m_{1m})$. In more details, the error event can be partitioned into the followings:

1) Error event corresponds to $\hat{k} \neq k$. Note that this event occurs with arbitrarily small probability if

$$R_1 + R_r + R_{r_1} \leq I(U, V, T; Y_1) = I(T; Y_1). \tag{50}$$

2) Error event corresponds to $\hat{k} = k$, but $(\hat{m}_{1s}, \hat{m}_{sk}, \hat{r}) \neq (m_{1s}, m_{sk}, r)$ Note that this event occurs with arbitrarily small probability if

$$R_1 - R_k + R_r + R_{r_1} \leq I(V, T; Y_1|U) = I(T; Y_1|U). \tag{51}$$

3) Error event corresponds to $(\hat{k}, \hat{m}_{1s}, \hat{m}_{sk}, \hat{r}) = (k, m_{1s}, m_{sk}, r)$ but $\hat{m}_{1m} \neq m_{1m}$. Note that this event occurs with arbitrarily small probability if

$$R_{1m} + R_{r_1} \leq I(T; Y_1|U, V) = I(T; Y_1|V). \tag{52}$$

Similar analysis can be done at the receiver 2, from which the decoding error probability $P_{e,2}$ can be made arbitrarily small if

$$R_2 + R_r + R_{r_1} \leq I(T; Y_2) \tag{53}$$

$$R_2 - R_k + R_r + R_{r_1} \leq I(T; Y_2|U) \tag{54}$$

$$R_{2m} + R_{r_1} \leq I(T; Y_2|V). \tag{55}$$

Analysis of individual secrecy: For the secrecy of M_1, we have

$$\begin{aligned}
I(M_1; Z^n) =& I(M_{1k}, M_{1sk}, M_{1s}, M_{1m}; Z^n) \\
=& I(M_{1k}, M_{1sk}; Z^n) + I(M_{1s}, M_{1m}; Z^n|M_{1k}, M_{1sk}) \\
\overset{(a)}{=}& I(M_{1s}, M_{1m}; Z^n|M_{1k}, M_{1sk}) \\
=& H(M_{1s}, M_{1m}) - H(M_{1s}, M_{1m}|M_{1k}, M_{1sk}, Z^n) \\
\leq& H(M_{1s}, M_{1m}) - H(M_{1s}, M_{1m}|M_k, M_{1k}, M_{1sk}, Z^n) \\
\overset{(b)}{=}& nR_{1s} + nR_{1m} - H(M_{1s}, M_{1m}|M_k, Z^n)
\end{aligned}$$

where

(a) is due to the fact that $I(M_{1k}, M_{1sk}; Z^n) = 0$ since

$$\begin{aligned}
I(M_{1k}, M_{1sk}; Z^n) &\leq I(M_{1k}, M_{1sk}; Z^n, M_k, M_{sk}, M_{1s}, M_{1m}, M_{2s}, M_{2m}) \\
&= I(M_{1k}, M_{1sk}; M_k, M_{sk}, M_{1s}, M_{1m}, M_{2s}, M_{2m}) \\
&= 0,
\end{aligned}$$

where the first equality is by the Markov chain $(M_{1k}, M_{2k}, M_{1sk}, M_{2sk}) \to (M_k, M_{sk}, M_{ss}, M_{sm}) \to Z^n$;

(b) is due to the fact that $I(M_{1s}, M_{1m}; M_{1k}, M_{1sk}|Z^n, M_k) = 0$, where the equality follows by:

1) $I(M_{1s}, M_{1m}; M_{1k}, M_{1sk}|Z^n, M_k) \geq 0$; and

2) $I(M_{1s}, M_{1m}; M_{1k}, M_{1sk}|Z^n, M_k) \leq 0$ since

$$\begin{aligned} H(M_{1k}, M_{1sk}|Z^n, M_k, M_{1s}, M_{1m}) &\geq H(M_{1k}, M_{1sk}|Z^n, M_k, M_{sk}, M_{1s}, M_{1m}) \\ &= H(M_{1k}, M_{1sk}|M_k, M_{sk}) \\ &= H(M_{1k}, M_{1sk}) \\ &\geq H(M_{1k}, M_{1sk}|Z^n, M_k). \end{aligned}$$

So far, we obtain

$$I(M_1; Z^n) \leq nR_{1s} + nR_{1m} - H(M_{1s}, M_{1m}|M_k, Z^n). \tag{56}$$

Similarly, for the secrecy of M_2, we have

$$I(M_2; Z^n) \leq nR_{2s} + nR_{2m} - H(M_{2s}, M_{2m}|M_k, Z^n). \tag{57}$$

In the following, we show that $H(M_{1s}, M_{1m}, M_{2s}, M_{2m}|M_k, Z^n) \geq n(R_{1s} + R_{1m} + R_{2s} + R_{2m}) - n\delta'(\epsilon)$ holds if the rates satisfy (59) and (62). This implies that $H(M_{1s}, M_{1m}|M_k, Z^n) \geq R_{1s} + R_{1m} - n\delta'(\epsilon)$ and $H(M_{2s}, M_{2m}|M_k, Z^n) \geq R_{2s} + R_{2m} - n\delta'(\epsilon)$. Further by (56) and (57), we obtain $I(M_1; Z^n) \leq n\delta'(\epsilon)$ and $I(M_2; Z^n) \leq n\delta'(\epsilon)$, thus completing the desired individual secrecy proof.

Note that

$$\begin{aligned} &H(M_{1s}, M_{1m}, M_{2s}, M_{2m}|M_k, Z^n) \\ \overset{(a)}{=}&H(M_{ss}, M_{sm}|U^n, Z^n) \\ =&H(M_{ss}, M_{sm}, V^n|U^n, Z^n) - H(V^n|U^n, M_{ss}, M_{sm}, Z^n) \\ \geq&H(M_{ss}, M_{sm}, V^n|U^n, Z^n) - H(V^n|U^n, M_{ss}, Z^n) \\ \overset{(b)}{\geq}&H(V^n|U^n, Z^n) + H(M_{sm}|U^n, V^n, Z^n) - n(R_{sk} + R_r - I(V; Z|U)) - n\epsilon_1, \end{aligned} \tag{58}$$

where (a) is due to the one-to-one correspondence between M_k and U^n; and the simplification by denoting $M_{ss} = (M_{1s}, M_{2s})$ and $M_{sm} = (M_{1m}, M_{2m})$; (b) follows from [48, Lemma 1] that $H(V^n|U^n, M_{ss}, Z^n) \leq n(R_{sk} + R_r - I(V; Z|U)) + n\epsilon_1$ if

$$R_{sk} + R_r \geq I(V; Z|U) + \epsilon. \tag{59}$$

For the first term in (58), i.e., $H(V^n|U^n, Z^n)$, we have

$$\begin{aligned} H(V^n|U^n, Z^n) &= H(V^n, Z^n|U^n) - H(Z^n|U^n) \\ &= H(V^n|U^n) + H(Z^n|U^n, V^n) - H(Z^n|U^n) \\ &= n(R_{1s} + R_{2s} + R_{sk} + R_r) + H(Z^n|U^n, V^n) - H(Z^n|U^n); \end{aligned} \tag{60}$$

And, for the second term in (58), i.e., $H(M_{1m}, M_{2m}|U^n, V^n, Z^n)$, we have

$$\begin{aligned}
&H(M_{1m}, M_{2m}|U^n, V^n, Z^n) = H(M_{sm}|U^n, V^n, Z^n)\\
=&H(M_{sm}, Z^n|U^n, V^n) - H(Z^n|U^n, V^n)\\
=&H(M_{sm}, Z^n, T^n|U^n, V^n) - H(Z^n|U^n, V^n) - H(T^n|U^n, V^n, M_{sm}, Z^n)\\
\geq&H(T^n|U^n, V^n) + H(Z^n|U^n, V^n, T^n) - H(Z^n|U^n, V^n) - H(T^n|U^n, V^n, M_{sm}, Z^n)\\
=&n(R_{1m} + R_{2m} + R_{r_1}) + H(Z^n|U^n, V^n, T^n) - H(Z^n|U^n, V^n) - H(T^n|U^n, V^n, M_{sm}, Z^n)\\
\overset{(a)}{\geq}&n(R_{1m} + R_{2m} + R_{r_1}) + H(Z^n|U^n, V^n, T^n) - H(Z^n|U^n, V^n) - n(R_{r_1} - I(T; Z|U, V)) - n\epsilon_2
\end{aligned} \tag{61}$$

where (a) follows from [48, Lemma 1] that $H(T^n|U^n, V^n, M_{sm}, Z^n) \leq n(R_{r_1} - I(T; Z|U, V)) + n\epsilon_2$ if

$$R_{r_1} \geq I(T; Z|V) + \epsilon. \tag{62}$$

Combining (60) and (61) in (58), we have

$$\begin{aligned}
&H(M_{1s}, M_{1m}, M_{2s}, M_{2m}|M_k, Z^n)\\
\geq&H(V^n|U^n, Z^n) + H(M_{1m}, M_{2m}|U^n, V^n, Z^n) - n(R_{sk} + R_r - I(V; Z|U)) - n\epsilon_1\\
\geq&n(R_{1s} + R_{2s} + R_{sk} + R_r) + H(Z^n|U^n, V^n) - H(Z^n|U^n)\\
&+ n(R_{1m} + R_{2m} + R_{r_1}) + H(Z^n|U^n, V^n, T^n) - H(Z^n|U^n, V^n) - n(R_{r_1} - I(T; Z|U, V)) - n\epsilon_2\\
&- n(R_{sk} + R_r - I(V; Z|U)) - n\epsilon_1\\
\overset{(a)}{\geq}&n(R_{1s} + R_{1m} + R_{2s} + R_{2m}) - nH(Z|U) + nH(Z|U, V, T) + nI(V, T; Z|U) + n\delta'(\epsilon)\\
=&n(R_{1s} + R_{1m} + R_{2s} + R_{2m}) - n\delta'(\epsilon)
\end{aligned}$$

where (a) follows from $H(Z^n|U^n) \leq \sum_{i=1}^n H(Z_i|U_i) = nH(Z|U)$; $H(Z^n|U^n, V^n, T^n) = nH(Z|U, V, T)$; and $\delta'(\epsilon) = \epsilon_1 + \epsilon_2$.

Achievable rate region: Combining the followings:

- the non-negativity for rates, i.e.,

$$R_k, R_{sk}, R_{1s}, R_{2s}, R_r \geq 0;$$

- the rate relations imposed by rate splitting, i.e.,

$$R_1 = R_k + R_{sk} + R_{1s} + R_{1m},$$

$$R_2 = R_k + R_{sk} + R_{2s} + R_{2m};$$

- the constraints for a reliable communication to both legitimate receivers, i.e., (50)-(55):

$$R_1 + R_r + R_{r_1} \leq I(T; Y_1)$$

$$R_2 + R_r + R_{r_1} \leq I(T; Y_2)$$

$$R_1 - R_k + R_r + R_{r_1} \leq I(T;Y_1|U)$$
$$R_2 - R_k + R_r + R_{r_1} \leq I(T;Y_2|U)$$
$$R_{1m} + R_{r_1} \leq I(T;Y_1|V)$$
$$R_{2m} + R_{r_1} \leq I(T;Y_2|V).$$

- the constraints for individual secrecy of the messages at the eavesdropper, i.e., (59) and (62):

$$R_{sk} + R_r \geq I(V;Z|U)$$
$$R_{r_1} \geq I(T;Z|V).$$

Applying Fourier-Motzkin procedure [47] to eliminate $R_k, R_{sk}, R_{1m}, R_{2m}, R_r, R_{r_1}$, we get an achievable region, which is the union of non-negative (R_1, R_2) pairs satisfying

$$R_1 \leq \min\{I(T;Y_1) - I(T;Z|V), \quad I(T;Y_1|U) - I(T;Z|U) + R_2\}; \tag{63}$$
$$R_2 \leq \min\{I(T;Y_2) - I(T;Z|V), \quad I(T;Y_2|U) - I(T;Z|U) + R_1\}, \tag{64}$$

where the union is taken over probability distributions satisfying $U \to V \to T \to (Y_1, Y_2, Z)$ forming a Markov chain and for $i = 1, 2$, both $I(T;Y_i|V) \geq I(T;Z|V)$ and $I(T;Y_i|U) \geq I(T;Z|U)$ hold.

Note that for fixed $p(t), p(t|u)$, the above region is outer bounded by the choice of $V = T$, i.e., the outer bounding region is given by the union of non-negative (R_1, R_2) pairs satisfying

$$R_1 \leq \min\{I(V;Y_1), \quad I(V;Y_1|U) - I(V;Z|U) + R_2\}; \tag{65}$$
$$R_2 \leq \min\{I(V;Y_2), \quad I(V;Y_2|U) - I(V;Z|U) + R_1\}, \tag{66}$$

where the union is taken over probability distributions satisfying $U \to V \to (Y_1, Y_2, Z)$ forming a Markov chain and $I(V;Y_i|U) \geq I(V;Z|U)$ holds for $i = 1, 2$. This reduces to the region provided in Theorem 7.

Appendix E
Proof of Converse for Theorem 8

Consider a BC-RSI with an external eavesdropper. In addition, the eavesdropper's channel is *deterministic* in the sense that Z is a function of X. For a reliable communication under individual secrecy constraint, we have

$$\begin{aligned} nR_1 =& H(M_1) = H(M_1|M_2) \\ =& I(M_1; Y_1^n|M_2) + H(M_1|M_2, Y_1^n) \\ \overset{(a)}{\leq}& I(M_1; Y_1^n|M_2) + n\epsilon \end{aligned}$$

where (a) is due to the reliability constraint, i.e., $H(M_1|M_2, Y_1^n) \leq n\epsilon_1$ by Fano's inequality.

On one hand, we have

$$\begin{aligned}
nR_1 \leq & I(M_1; Y_1^n|M_2) + n\epsilon \\
= & \sum_{i=1}^{n} I(M_1; Y_{1i}|M_2, Y_1^{i-1}) + n\epsilon \\
\leq & \sum_{i=1}^{n} I(M_1, M_2, Y_1^{i-1}; Y_{1i}) + n\epsilon \\
\overset{(b)}{\leq} & \sum_{i=1}^{n} I(X_i; Y_{1i}) + n\epsilon \\
\overset{(c)}{\leq} & nI(X; Y_1) + n\epsilon
\end{aligned}$$

where (b) is due to the Markov chain $(M_1, M_2, Y_1^{i-1}) \to X_i \to Y_{1i}$; (c) is by introducing a time-sharing random variable Q which is uniform over $1, 2 \cdots, n$ and by taking $X = X_Q, Y_1 = Y_{1,Q}$.

On the other hand, we have

$$\begin{aligned}
nR_1 \leq & I(M_1; Y_1^n|M_2) + n\epsilon \\
= & \underbrace{I(M_1; Y_1^n|M_2) - I(M_1; Z^n|M_2)}_{nR_1^s} + \underbrace{I(M_1; Z^n|M_2)}_{nR_1^k} + n\epsilon.
\end{aligned}$$

The first term R_1^s can be bounded as follows:

$$\begin{aligned}
nR_1^s = & I(M_1; Y_1^n|M_2) - I(M_1; Z^n|M_2) \\
\leq & I(M_1; Y_1^n, Z^n|M_2) - I(M_1; Z^n|M_2) \\
= & I(M_1; Y_1^n|M_2, Z^n) \\
= & \sum_{i=1}^{n} I(M_1; Y_{1i}|M_2, Z^n, Y_{1,1}^{i-1}) \\
\leq & \sum_{i=1}^{n} I(M_1, M_2, Y_1^{i-1}, Z_1^{i-1}, Z_{i+1}^n; Y_{1i}|Z_i) \\
\overset{(d)}{\leq} & \sum_{i=1}^{n} I(X_i; Y_{1i}|Z_i) \\
\overset{(e)}{\leq} & nI(X; Y_1|Z),
\end{aligned}$$

where (d) is due to the Markov chain $(M_1, M_2, Y_1^{i-1}, Z_1^{i-1}, Z_{i+1}^n) \to X_i \to (Y_{1i}, Z_i)$; (e) is by applying the time-sharing random variable Q which is uniform over $1, 2 \cdots, n$ and by taking $X = X_Q, Y_1 = Y_{1,Q}, Z = Z_Q$.

And the second term R_1^k can be bounded by

$$\begin{aligned}
nR_1^k = & I(M_1; Z^n|M_2) \\
\leq & I(M_1, M_2; Z^n) \\
\overset{(d)}{\leq} & I(M_2; Z^n|M_1) + n\epsilon
\end{aligned}$$

$$\leq H(M_2|M_1) + n\epsilon$$

$$= nR_2 + n\epsilon,$$

where (d) is due to the individual secrecy constraint, i.e., $I(M_1; Z^n) \leq n\epsilon$.

As a conclusion of above discussions, we have as $\epsilon \to 0$

$$R_1 \leq \min\{I(X;Y_1),\ I(X;Y_1|Z) + R_2\}.$$

A similar proof can be applied to R_2 and thus completes the proof of the converse.

Appendix F
Proof of Theorem 11

Rate splitting: As illustrated in Fig. 21, we represent M_1, M_2 by $M_1 = (M_{1k}, M_{1sk}, M_{1ss}, M_{1sm})$ and $M_2 = (M_{2k}, M_{2sk}, M_{2ss}, M_{2sm})$ with M_{1k}, M_{2k} of entropy nR_k; M_{1sk}, M_{2sk} of entropy nR_{sk}; while M_{1ss}, M_{1sm} of entropy nR_{1ss}, nR_{1sm}; and M_{2ss}, M_{2sm} of entropy nR_{2ss}, nR_{2sm}, respectively. For simplicity, we denote $M_k = M_{1k} \oplus M_{2k}$, $M_{sk} = M_{1sk} \oplus M_{2sk}$, $M_{ss} = (M_{1ss}, M_{2ss})$ and $M_{sm} = (M_{1sm}, M_{2sm})$.

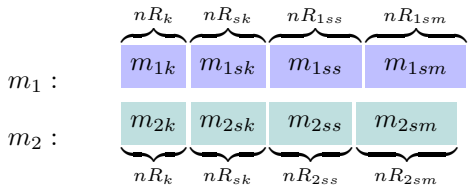


Fig. 21: Martion's coding: Rate splitting.

Codebook generation: Fix $p(u), p(v_0|u), p(v_1, v_2|v_0)$ and $p(x|v_1, v_2)$.

First, randomly generate 2^{nR_k} i.i.d. sequences $u^n(k)$, $k \in [1 : 2^{nR_k}]$, according to $p(u)$.

For each $u^n(k)$, randomly generate $2^{n(R_{1ss}+R_{2ss}+R_{sk}+R_r)}$ i.i.d. sequences $v_0^n(k, m_{1ss}, m_{2ss}, m_{sk}, r)$ with $(m_{1ss}, m_{2ss}, m_{sk}, r) \in [1 : 2^{nR_{1ss}}] \times [1 : 2^{nR_{2ss}}] \times [1 : 2^{nR_{sk}}] \times [1 : 2^{nR_r}]$, according to $p(v_0|u)$;

For each fixed $v_0^n(k, m_{1ss}, m_{2ss}, m_{sk}, r)$, randomly generate $2^{n(R_{1sm}+R_{1r}+R_{1c})}$ i.i.d. sequences $v_1^n(k, m_{1ss}, m_{2ss}, m_{sk}, r, sm_1, r_1, c_1)$ with $(sm_1, r_1, c_1) \in [1 : 2^{nR_{1sm}}] \times [1 : 2^{nR_{1r}}] \times [1 : 2^{nR_{1c}}]$, according to $p(v_1|v_0)$; and similarly generate $2^{n(R_{2sm}+R_{2r}+R_{2c})}$ i.i.d. sequences $v_2^n(k, m_{1ss}, m_{2ss}, m_{sk}, r, sm_2, r_2, c_2)$ with $(sm_2, r_2, c_2) \in [1 : 2^{nR_{2sm}}] \times [1 : 2^{nR_{2r}}] \times [1 : 2^{nR_{2c}}]$, according to $p(v_2|v_0)$.

Encoding: To send messages (m_1, m_2), choose $u^n(k)$, where $k = m_k \triangleq m_{1k} \oplus m_{2k}$.

Given $u^n(k)$, randomly choose $r \in [1 : 2^{nR_r}]$ and find $v_0^n(u^n, m_{1ss}, m_{2ss}, m_{sk}, r)$, where $m_{sk} \triangleq m_{1sk} \oplus m_{2sk}$.

Given $v_0^n(k, m_{1ss}, m_{2ss}, m_{sk}, r)$, randomly choose $(r_1, r_2) \in [1 : 2^{nR_{1r}}] \times [1 : 2^{nR_{2r}}]$, and pick (c_1, c_2) such that $v_1^n(k, m_{1ss}, m_{2ss}, sk, r, sm_1, r_1, c_1)$ and $v_2^n(k, m_{1ss}, m_{2ss}, sk, r, sm_2, r_2, c_2)$ are jointly typical. (If there is more than one such jointly typical pair, choose one of them uniformly at random. This is possible with high probability, if

$$R_{1c} + R_{2c} > I(V_1; V_2|V_0) \tag{67}$$

(refer to [49] for the proof).

Finally, for the chosen jointly typical pair (v_1^n, v_2^n), generate a codeword x^n at random according to $p(x|v_1, v_2)$ and transmit it.

The choice of u^n, v_0^n, v_1^n, v_2^n for given (m_1, m_2) is illustrated in Fig. 22.

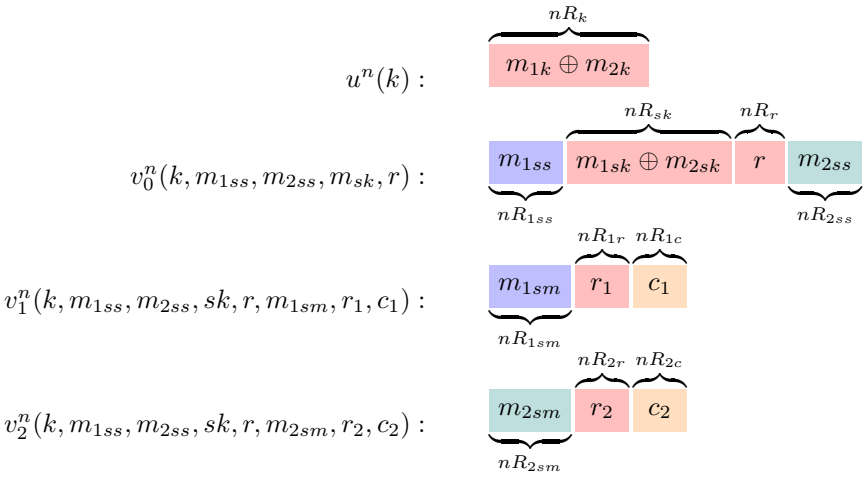


Fig. 22: Marton's coding: Encoding.

Decoding: Receiver 1, upon receiving y_1^n, finds a unique $v_1^n(\hat{k}, \hat{m}_{1ss}, m_{2ss}, \hat{m}_{sk}, \hat{r}, \hat{m}_{1sm}, \hat{r}_1, \hat{c}_1)$ such that (v_1^n, y_1^n) is jointly typical. And, receiver 2, upon receiving y_2^n, finds a unique $v_2^n(\tilde{k}, m_{1ss}, \tilde{m}_{2ss}, \tilde{m}_{sk}, \tilde{r}, m_{1sm}, \tilde{r}_2, \tilde{c}_2)$ such that (v_2^n, y_2^n) is jointly typical.

Analysis of decoding error: Assume that $m_1 = (m_{1k}, m_{1sk}, m_{1ss}, m_{1sm})$, $m_2 = (m_{2k}, m_{2sk}, m_{2ss}, m_{2sm})$ is sent, i.e., more specifically, $k, m_{sk}, m_{1ss}, m_{1sm}$ and m_{2ss}, m_{2sm} are sent, where $k \triangleq m_{1k} \oplus m_{2k}$ and $m_{sk} = m_{1sk} \oplus m_{2sk}$. For $P_{e,1}$, a decoding error happens if receiver 1's estimate is $u^n(\hat{k})$, $v_0^n(u^n, \hat{m}_{1ss}, m_{2ss}, \hat{m}_{sk}, \hat{r})$, $v_1^n(v_0^n, \hat{m}_{1sm}, \hat{r}_1, \hat{c}_1)$ with $(\hat{k}, \hat{m}_{1ss}, \hat{m}_{sk}, \hat{r}, \hat{m}_{1sm}, \hat{r}_1, \hat{c}_1) \neq (k, m_{1ss}, m_{sk}, r, m_{1sm}, r_1, c_1)$. In more details, the error event can be partitioned into the followings:

1) Error event corresponds to $\hat{k} \neq k$. Note that this event occurs with arbitrarily small probability if

$$R_1 + R_r + R_{1r} + R_{1c} \leq I(U, V_0, V_1; Y_1) = I(V_0, V_1; Y_1). \tag{68}$$

2) Error event corresponds to $\hat{k} = k$, but $(\hat{m}_{1ss}, \hat{m}_{sk}, \hat{r}) \neq (m_{1ss}, m_{sk}, r)$ Note that this event occurs with arbitrarily small probability if

$$R_1 - R_k + R_r + R_{1r} + R_{1c} \leq I(V_0, V_1; Y_1|U). \tag{69}$$

3) Error event corresponds to $(\hat{k}, \hat{m}_{1ss}, \hat{m}_{sk}, \hat{r}) = (k, m_{1ss}, m_{sk}, r)$ but $(\hat{m}_{1sm}, \hat{r}_1, \hat{c}_1) \neq (m_{1sm}, r_1, c_1)$. Note that this event occurs with arbitrarily small probability if

$$R_{1sm} + R_{1r} + R_{1c} \leq I(V_1; Y_1|U, V_0) = I(V_1; Y_1|V_0). \tag{70}$$

Similar analysis can be done at the receiver 2, from which the decoding error probability $P_{e,2}$ can be made arbitrarily small if

$$R_2 + R_r + R_{2r} + R_{2c} \leq I(V_0, V_2; Y_2) \tag{71}$$

$$R_2 - R_k + R_r + R_{2r} + R_{2c} \leq I(V_0, V_2; Y_2|U) \tag{72}$$

$$R_{2sm} + R_{2r} + R_{2c} \leq I(V_2; Y_2|U, V_0) = I(V_2; Y_2|V_0). \tag{73}$$

Analysis of individual secrecy: For the secrecy of M_1, we have

$$\begin{aligned}
I(M_1; Z^n) =& I(M_{1k}, M_{1sk}, M_{1ss}, M_{1sm}; Z^n) \\
=& I(M_{1k}, M_{1sk}; Z^n) + I(M_{1ss}, M_{1sm}; Z^n|M_{1k}, M_{1sk}) \\
\overset{(a)}{=}& I(M_{1ss}, M_{1sm}; Z^n|M_{1k}, M_{1sk}) \\
=& H(M_{1ss}, M_{1sm}) - H(M_{1ss}, M_{1sm}|M_{1k}, M_{1sk}, Z^n) \\
\leq& H(M_{1ss}, M_{1sm}) - H(M_{1ss}, M_{1sm}|M_k, M_{1k}, M_{1sk}, Z^n) \\
\overset{(b)}{=}& nR_{1ss} + nR_{1sm} - H(M_{1ss}, M_{1sm}|M_k, Z^n)
\end{aligned}$$

where

(a) is due to the fact that $I(M_{1k}, M_{1sk}; Z^n) = 0$ since

$$\begin{aligned}
I(M_{1k}, M_{1sk}; Z^n) &\leq I(M_{1k}, M_{1sk}; Z^n, M_k, M_{sk}, M_{1ss}, M_{1sm}, M_{2ss}, M_{2sm}) \\
&= I(M_{1k}, M_{1sk}; M_k, M_{sk}, M_{1ss}, M_{1sm}, M_{2ss}, M_{2sm}) \\
&= 0,
\end{aligned}$$

where the first equality is by the Markov chain $(M_{1k}, M_{2k}, M_{1sk}, M_{2sk}) \to (M_k, M_{sk}, M_{ss}, M_{sm}) \to Z^n$;

(b) is due to the fact that $I(M_{1ss}, M_{1sm}; M_{1k}, M_{1sk}|Z^n, M_k) = 0$, where the equality follows by:

1) $I(M_{1ss}, M_{1sm}; M_{1k}, M_{1sk}|Z^n, M_k) \geq 0$; and

2) $I(M_{1ss}, M_{1sm}; M_{1k}, M_{1sk}|Z^n, M_k) \leq 0$ since

$$\begin{aligned}
H(M_{1k}, M_{1sk}|Z^n, M_k, M_{1ss}, M_{1sm}) &\geq H(M_{1k}, M_{1sk}|Z^n, M_k, M_{sk}, M_{1ss}, M_{1sm}) \\
&= H(M_{1k}, M_{1sk}|M_k, M_{sk}) \\
&= H(M_{1k}, M_{1sk}) \\
&\geq H(M_{1k}, M_{1sk}|Z^n, M_k).
\end{aligned}$$

So far, we obtain

$$I(M_1; Z^n) \leq nR_{1ss} + nR_{1sm} - H(M_{1ss}, M_{1sm}|M_k, Z^n). \tag{74}$$

Similarly, for the secrecy of M_2, we have

$$I(M_2; Z^n) \leq nR_{2ss} + nR_{2sm} - H(M_{2ss}, M_{2sm}|M_k, Z^n). \tag{75}$$

In the following, we show that $H(M_{1ss}, M_{1sm}, M_{2ss}, M_{2sm}|M_k, Z^n) \geq n(R_{1ss}+R_{1sm}+R_{2ss}+R_{1sm})-n\delta'(\epsilon)$ holds if the rates satisfy (80), (82), (84) and (85). This implies that $H(M_{1ss}, M_{1sm}|M_k, Z^n) \geq R_{1ss} + R_{1sm} - n\delta'(\epsilon)$ and $H(M_{2ss}, M_{2sm}|M_k, Z^n) \geq R_{2ss} + R_{2sm} - n\delta'(\epsilon)$. Further by (74) and (75), we obtain $I(M_1; Z^n) \leq n\delta'(\epsilon)$ and $I(M_2; Z^n) \leq n\delta'(\epsilon)$, thus completing the desired individual secrecy proof.

Note that

$$\begin{aligned}
H(M_{1ss}, M_{1sm}, M_{2ss}, M_{2sm}|M_k, Z^n) &\overset{(a)}{=} H(M_{ss}, M_{sm}|U^n, Z^n) \\
&= H(M_{ss}, M_{sm}, V_0^n|U^n, Z^n) - H(V_0^n|U^n, M_{ss}, M_{sm}, Z^n) \\
&\geq H(M_{ss}, M_{sm}, V_0^n|U^n, Z^n) - H(V_0^n|U^n, M_{ss}, Z^n) \\
&\geq H(V_0^n|U^n, Z^n) + H(M_{sm}|U^n, V_0^n, Z^n) - H(V_0^n|U^n, M_{ss}, Z^n). \quad (76)
\end{aligned}$$

We now bound the terms above.

For the first term in (76), i.e., $H(V_0^n|U^n, Z^n)$, we have

$$\begin{aligned}
H(V_0^n|U^n, Z^n) &= H(V_0^n, Z^n|U^n) - H(Z^n|U^n) \\
&= H(V_0^n|U^n) + H(Z^n|U^n, V_0^n) - H(Z^n|U^n) \\
&= n(R_{1ss} + R_{2ss} + R_{sk} + R_r) + H(Z^n|U^n, V_0^n) - H(Z^n|U^n); \quad (77)
\end{aligned}$$

And, for the second term in (76), i.e., $H(M_{1sm}, M_{2sm}|U^n, V_0^n, Z^n)$, we have

$$\begin{aligned}
&H(M_{1sm}, M_{2sm}|U^n, V_0^n, Z^n) \\
&= H(M_{1sm}, M_{2sm}, Z^n|U^n, V_0^n) - H(Z^n|U^n, V_0^n) \\
&= H(M_{1sm}, M_{2sm}, Z^n, V_1^n, V_2^n|U^n, V_0^n) - H(Z^n|U^n, V_0^n) - H(V_1^n, V_2^n|U^n, V_0^n, M_{1sm}, M_{2sm}, Z^n) \\
&= H(Z^n, V_1^n, V_2^n|U^n, V_0^n) - H(Z^n|U^n, V_0^n) - H(V_1^n, V_2^n|U^n, V_0^n, M_{1sm}, M_{2sm}, Z^n) \\
&= H(Z^n|U^n, V_0^n, V_1^n, V_2^n) + H(V_1^n, V_2^n|U^n, V_0^n) - H(Z^n|U^n, V_0^n) - H(V_1^n, V_2^n|U^n, V_0^n, M_{1sm}, M_{2sm}, Z^n) \\
&\overset{(a)}{\geq} H(Z^n|U^n, V_0^n, V_1^n, V_2^n) + H(V_1^n, V_2^n|U^n, V_0^n) - H(Z^n|U^n, V_0^n) \\
&\quad - H(V_1^n|U^n, V_0^n, M_{1sm}, M_{2sm}, Z^n) - H(V_2^n|U^n, V_0^n, M_{1sm}, M_{2sm}, Z^n) \\
&\overset{(b)}{\geq} H(Z^n|U^n, V_0^n, V_1^n, V_2^n) + n(R_{1sm} + R_{1r} + R_{2sm} + R_{2r}) - H(Z^n|U^n, V_0^n) \\
&\quad - H(V_1^n|U^n, V_0^n, M_{1sm}, Z^n) - H(V_2^n|U^n, V_0^n, M_{2sm}, Z^n) \\
&\overset{(c)}{\geq} H(Z^n|U^n, V_0^n, V_1^n, V_2^n) + n(R_{1sm} + R_{1r} + R_{2sm} + R_{2r}) - H(Z^n|U^n, V_0^n) \\
&\quad - n(R_{1r} + R_{1c} - I(V_1; Z|V_0)) - n\epsilon_1 - n(R_{2r} + R_{2c} - I(V_2; Z|V_0)) - n\epsilon_1 \quad (78)
\end{aligned}$$

where (a) is due to the fact that $H(A, B|C) \leq H(A|C) + H(B|C)$, (b) follows as

$$\begin{aligned}
H(V_1^n, V_2^n|U^n, V_0^n) &= H(M_{1sm}, M_{2sm}, M_{1r}, M_{2r}|U^n, V_0^n) + H(V_1^n, V_2^n|U^n, V_0^n, M_{1sm}, M_{2sm}, M_{1r}, M_{2r}) \\
&\geq H(M_{1sm}, M_{2sm}, M_{1r}, M_{2r}|U^n, V_0^n) = H(M_{1sm}, M_{2sm}, M_{1r}, M_{2r})
\end{aligned}$$

$$= n(R_{1sm} + R_{1r} + R_{2sm} + R_{2r})$$

since the choice of $M_{1sm}, M_{2sm}, M_{1r}, M_{2r}$ are independent of U^n, V_0^n; (c) is due to the followings: First, we have

$$H(V_1^n|U^n, V_0^n, M_{1sm}, Z^n) = H(V_1^n|V_0^n, M_{1sm}, Z^n) \leq n(R_{1r} + R_{1c} - I(V_1; Z|V_0)) + n\epsilon_1 \tag{79}$$

if, for an arbitrarily small $\epsilon > 0$,

$$R_{1r} + R_{1c} \geq I(V_1; Z|V_0) + \epsilon. \tag{80}$$

This follows from [48, Lemma 1]. And, similarly, we have

$$H(V_2^n|U^n, V_0^n, M_{2sm}, Z^n) = H(V_2^n|V_0^n, M_{2sm}, Z^n) \leq n(R_{2r} + R_{2c} - I(V_2; Z|V_0)) + n\epsilon_1 \tag{81}$$

if, for an arbitrarily small $\epsilon > 0$,

$$R_{2r} + R_{2c} \geq I(V_2; Z|V_0) + \epsilon. \tag{82}$$

Finally, for the last term in (76), i.e., $H(V_0^n|U^n, M_{ss}, Z^n)$, we have

$$H(V_0^n|U^n, M_{ss}, Z^n) \leq n(R_{sk} + R_r - I(V_0; Z|U)) + n\epsilon_1, \tag{83}$$

if, for an arbitrarily small $\epsilon > 0$,

$$R_{sk} + R_r \geq I(V_0; Z|U) + \epsilon. \tag{84}$$

This follows from [48, Lemma 1].

Combining (77), (78) and (83) in (76), we have

$$\begin{aligned}
&H(M_{1ss}, M_{1sm}, M_{2ss}, M_{2sm}|M_k, Z^n) \\
&\geq H(V_0^n|U^n, Z^n) + H(M_{sm}|U^n, V_0^n, Z^n) - H(V_0^n|U^n, M_{ss}, Z^n) \\
&\geq n(R_{1ss} + R_{2ss} + R_{sk} + R_r) + H(Z^n|U^n, V_0^n) - H(Z^n|U^n) \\
&\quad + H(Z^n|U^n, V_0^n, V_1^n, V_2^n) + n(R_{1sm} + R_{1r} + R_{2sm} + R_{2r}) - H(Z^n|U^n, V_0^n) \\
&\quad - n(R_{1r} + R_{1c} - I(V_1; Z|V_0)) - n\epsilon_1 - n(R_{2r} + R_{2c} - I(V_2; Z|V_0)) - n\epsilon_1 \\
&\quad - n(R_{sk} + R_r - I(V_0; Z|U)) - n\epsilon_1 \\
&\overset{(a)}{\geq} n(R_{1ss} + R_{1sm} + R_{2ss} + R_{2sm}) \\
&\quad + n(-R_{1c} - R_{2c} - H(Z|U) + H(Z|U, V_0, V_1, V_2) + I(V_1; Z|V_0) + I(V_2; Z|V_0) + I(V_0; Z|U) - 3\epsilon_1) \\
&\overset{(b)}{\geq} n(R_{1ss} + R_{1sm} + R_{2ss} + R_{2sm}) - n\delta(\epsilon)
\end{aligned}$$

where (a) follows from $H(Z^n|U^n) \leq \sum_{i=1}^n H(Z_i|U_i) = nH(Z|U)$ and the fact that $H(Z^n|U^n, V_0^n, V_1^n, V_2^n) = nH(Z|U, V_0, V_1, V_2)$; and (b) follows by the rate choice

$$R_{1c} + R_{2c} \leq I(V_1; Z|V_0) + I(V_2; Z|V_0) - I(V_1, V_2; Z|V_0) \tag{85}$$

with $\delta(\epsilon) = 3\epsilon_1$.

Achievable rate region: Combining the non-negativity for rates, the conditions for reliable communication at both legitimate receivers, i.e., (67), (68)-(73), and individual secrecy at the eavesdropper, i.e., (80), (82), (84) and (85), we obtain the followings:

$$R_k, R_{sk}, R_{1ss}, R_{1sm}, R_{2ss}, R_{2sm}, R_r, R_{1c}, R_{2c}, R_{1r}, R_{2r} \geq 0 \tag{86}$$

$$\begin{aligned}
R_1 &= R_k + R_{sk} + R_{1ss} + R_{1sm} && (87)\\
R_2 &= R_k + R_{sk} + R_{2ss} + R_{2sm} && (88)\\
R_{1c} + R_{2c} &> I(V_1; V_2|V_0) && (89)\\
R_1 + R_r + R_{1r} + R_{1c} &\leq I(V_0, V_1; Y_1) && (90)\\
R_1 - R_k + R_r + R_{1r} + R_{1c} &\leq I(V_0, V_1; Y_1|U) && (91)\\
R_{1sm} + R_{1r} + R_{1c} &\leq I(V_1; Y_1|V_0) && (92)\\
R_2 + R_r + R_{2r} + R_{2c} &\leq I(V_0, V_2; Y_2) && (93)\\
R_2 - R_k + R_r + R_{2r} + R_{2c} &\leq I(V_0, V_2; Y_2|U) && (94)\\
R_{2sm} + R_{2r} + R_{2c} &\leq I(V_2; Y_2|V_0) && (95)\\
R_{sk} + R_r &\geq I(V_0; Z|U) && (96)\\
R_{1r} + R_{1c} &\geq I(V_1; Z|V_0) && (97)\\
R_{2r} + R_{2c} &\geq I(V_2; Z|V_0) && (98)\\
R_{1c} + R_{2c} &\leq I(V_1; Z|V_0) + I(V_2; Z|V_0) - I(V_1, V_2; Z|V_0), && (99)
\end{aligned}$$

where the union is taken over probability distributions satisfying

$$p(q, u, v_0, v_1, v_2, x) = p(q)p(u|q)p(v_0|u)p(v_1, v_2|v_0)p(x|v_1, v_2).$$

Eliminating $R_{1c}, R_{2c}, R_{1r}, R_{2r}, R_r, R_{1sm}, R_{2sm}, R_{1ss}, R_{2ss}, R_k, R_{sk}$, by applying Fourier-Motzkin procedure [47], we obtain the region of (R_1, R_2) as given in (20) in Theorem 11. Note that a sketch of this Fourier-Motzkin procedure is provided in Appendix G.

Appendix G
Fourier-Motzkin Elimination for Theorem 11

Here we briefly outline the Fourier-Motzkin procedure in the proof of Theorem 11.

- To eliminate R_{1ss}, we consider the non-negativity of the rate and the equality (87). We end up with

$$R_{1sm} + R_k + R_{sk} \leq R_1 \tag{100}$$

- To eliminate R_{2ss}, we consider the non-negativity of the rate and the equality (88). We end up with

$$R_{2sm} + R_k + R_{sk} \leq R_2 \tag{101}$$

- To eliminate R_{1sm}, we consider the non-negativity of the rate and the inequalities (92) and (100) which involve R_{1sm}. We end up with

$$R_{1r} + R_{1c} \leq I(V_1; Y_1|V_0) \tag{102}$$

$$R_k + R_{sk} \leq R_1 \tag{103}$$

- To eliminate R_{2sm}, we consider the non-negativity of the rate and the inequalities (95) and (101) which involve R_{2sm}. We end up with

$$R_{2r} + R_{2c} \leq I(V_2; Y_2|V_0) \tag{104}$$

$$R_k + R_{sk} \leq R_2 \tag{105}$$

- To eliminate R_r, we consider the non-negativity of the rate and the inequalities (90), (91), (93), (94), (96) which involve R_r. We end up with

$$R_1 + R_{1r} + R_{1c} \leq I(V_0, V_1; Y_1) \tag{106}$$

$$R_1 - R_k + R_{1r} + R_{1c} \leq I(V_0, V_1; Y_1|U) \tag{107}$$

$$R_2 + R_{2r} + R_{2c} \leq I(V_0, V_2; Y_2) \tag{108}$$

$$R_2 - R_k + R_{2r} + R_{2c} \leq I(V_0, V_2; Y_2|U) \tag{109}$$

$$R_1 - R_{sk} + R_{1r} + R_{1c} \leq I(V_0, V_1; Y_1) - I(V_0; Z|U) \tag{110}$$

$$R_1 - R_k - R_{sk} + R_{1r} + R_{1c} \leq I(V_0, V_1; Y_1|U) - I(V_0; Z|U) \tag{111}$$

$$R_2 - R_{sk} + R_{2r} + R_{2c} \leq I(V_0, V_2; Y_2) - I(V_0; Z|U) \tag{112}$$

$$R_2 - R_k - R_{sk} + R_{2r} + R_{2c} \leq I(V_0, V_2; Y_2|U) - I(V_0; Z|U) \tag{113}$$

- To eliminate R_k, we consider the non-negativity of the rate and the inequalities (107), (109), (111), (113), (103), (105) which involve R_k. We end up with

$$R_{sk} \leq R_1 \tag{114}$$

$$R_{sk} \leq R_2 \tag{115}$$

$$R_{sk} + R_{1r} + R_{1c} \leq I(V_0, V_1; Y_1|U) \tag{116}$$

$$R_1 - R_2 + R_{sk} + R_{1r} + R_{1c} \leq I(V_0, V_1; Y_1|U) \tag{117}$$

$$R_2 - R_1 + R_{sk} + R_{2r} + R_{2c} \leq I(V_0, V_2; Y_2|U) \tag{118}$$

$$R_{sk} + R_{2r} + R_{2c} \leq I(V_0, V_2; Y_2|U) \tag{119}$$

$$R_{1r} + R_{1c} \leq I(V_0, V_1; Y_1|U) - I(V_0; Z|U) \tag{120}$$

$$R_1 - R_2 + R_{1r} + R_{1c} \leq I(V_0, V_1; Y_1|U) - I(V_0; Z|U) \tag{121}$$

$$R_2 - R_1 + R_{2r} + R_{2c} \leq I(V_0, V_2; Y_2|U) - I(V_0; Z|U) \tag{122}$$

$$R_{2r} + R_{2c} \leq I(V_0, V_2; Y_2|U) - I(V_0; Z|U) \tag{123}$$

- To eliminate R_{sk}, we consider the non-negativity of the rate and the inequalities (110), (112), (114), (115), (116), (117), (118), (119) which involve R_{sk}. We end up with the following inequalities after cancelling the redundant ones.

$$R_1 \geq 0 \tag{124}$$

$$R_2 \geq 0 \tag{125}$$

- To eliminate R_{1r}, we consider the non-negativity of the rate and the inequalities (97), (106), (102), (120), (121) which involve R_{1r}. We end up with the following inequalities after cancelling the redundant ones.

$$R_1 + R_{1c} \leq I(V_0, V_1; Y_1) \tag{126}$$

$$R_{1c} \leq I(V_1; Y_1|V_0) + [I(V_0; Y_1|U) - I(V_0; Z|U)]^- \tag{127}$$

$$R_1 - R_2 + R_{1c} \leq I(V_0, V_1; Y_1|U) - I(V_0; Z|U) \tag{128}$$

$$R_1 \leq I(V_0, V_1; Y_1) - I(V_1; Z|V_0) \tag{129}$$

$$I(V_1; Z|V_0) \leq I(V_1; Y_1|V_0) \tag{130}$$

$$I(V_0, V_1; Z|U) \leq I(V_0, V_1; Y_1|U) \tag{131}$$

$$R_1 - R_2 \leq I(V_0, V_1; Y_1|U) - I(V_0, V_1; Z|U) \tag{132}$$

  where $[a]^- = \min\{0, a\}$.

- To eliminate R_{2r}, we consider the non-negativity of the rate and the inequalities (98), (108), (104), (122), (123) which involve R_{2r}. We end up with the following inequalities after canceling the redundant ones.

$$R_2 + R_{2c} \leq I(V_0, V_2; Y_2) \tag{133}$$

$$R_{2c} \leq I(V_2; Y_2|V_0) + |I(V_0; Y_2|U) - I(V_0; Z|U)|^- \tag{134}$$

$$R_2 - R_1 + R_{2c} \leq I(V_0, V_2; Y_2|U) - I(V_0; Z|U) \tag{135}$$

$$R_2 \leq I(V_0, V_2; Y_2) - I(V_2; Z|V_0) \tag{136}$$

$$I(V_2; Z|V_0) \leq I(V_2; Y_2|V_0) \tag{137}$$

$$I(V_0, V_2; Z|U) \leq I(V_0, V_2; Y_2|U) \tag{138}$$

$$R_2 - R_1 \leq I(V_0, V_2; Y_2|U) - I(V_0, V_2; Z|U) \tag{139}$$

- To eliminate R_{1c}, we consider the non-negativity of the rate and the inequalities (89), (99), (126), (127) and (128) which involve R_{1c}. We end up with the following inequalities after canceling the redundant

ones.

$$R_{2c} \leq I(V_1;Z|V_0) + I(V_2;Z|V_0) - I(V_1,V_2;Z|V_0) \tag{140}$$

$$I(V_1;V_2|V_0) \leq I(V_1;Z|V_0) + I(V_2;Z|V_0) - I(V_1,V_2;Z|V_0) \tag{141}$$

$$R_1 - R_{2c} \leq I(V_0,V_1;Y_1) - I(V_1;V_2|V_0) \tag{142}$$

$$R_{2c} \geq I(V_1;V_2|V_0) - I(V_1;Y_1|V_0) - [I(V_0;Y_1|U) - I(V_0;Z|U)]^- \tag{143}$$

$$R_1 - R_2 - R_{2c} \leq I(V_0,V_1;Y_1|U) - I(V_0;Z|U) - I(V_1;V_2|V_0) \tag{144}$$

- To eliminate R_{2c}, we consider the non-negativity of the rate and the inequalities (133), (134), (135), (140), (142), (143), (144) which involve R_{2c}. We end up with the following inequalities after cancelling some redundant ones.

$$R_1 + R_2 \leq I(V_0,V_1;Y_1) + I(V_0,V_2;Y_2) - I(V_1;V_2|V_0) \tag{145}$$

$$R_1 \leq I(V_0,V_1;Y_1) - I(V_1;V_2|V_0) + I(V_2;Y_2|V_0) + [I(V_0;Y_2|U) - I(V_0;Z|U)]^- \tag{146}$$

$$R_2 \leq I(V_0,V_2;Y_2|U) - I(V_1;V_2|V_0) - I(V_0;Z|U) + I(V_0,V_1;Y_1) \tag{147}$$

$$R_1 \leq I(V_0,V_1;Y_1) - I(V_1;V_2|V_0) + I(V_1;Z|V_0) + I(V_2;Z|V_0) - I(V_1,V_2;Z|V_0) \tag{148}$$

$$R_2 \leq I(V_0,V_2;Y_2) - I(V_1;V_2|V_0) + I(V_1;Y_1|V_0) + [I(V_0;Y_1|U) - I(V_0;Z|U)]^- \tag{149}$$

$$\begin{aligned} R_2 - R_1 \leq\ & I(V_0,V_2;Y_2|U) - I(V_1;V_2|V_0) - I(V_0;Z|U) + I(V_1;Y_1|V_0) \\ & + [I(V_0;Y_1|U) - I(V_0;Z|U)]^- \end{aligned} \tag{150}$$

$$R_1 \leq I(V_0,V_1;Y_1|U) - I(V_1;V_2|V_0) - I(V_0;Z|U) + I(V_0,V_2;Y_2) \tag{151}$$

$$\begin{aligned} R_1 - R_2 \leq\ & I(V_0,V_1;Y_1|U) + I(V_2;Y_2|V_0) - I(V_1;V_2|V_0) - I(V_0;Z|U) \\ & + [I(V_0;Y_2|U) - I(V_0;Z|U)]^- \end{aligned} \tag{152}$$

$$\begin{aligned} R_1 - R_2 \leq\ & I(V_0,V_1;Y_1|U) - I(V_1;V_2|V_0) - I(V_0;Z|U) \\ & + I(V_1;Z|V_0) + I(V_2;Z|V_0) - I(V_1,V_2;Z|V_0) \end{aligned} \tag{153}$$

  Note that (145) is redundant due to (129), (136) and (141); (147) is redundant due to (139), (129) and (141); (148) is redundant due to (129) and (141); (150) is redundant due to (139), (130) or (131), and (141); (151) is redundant due to (132), (136) and (141); (152) is redundant due to (132), (137) or (138), and (141); (153) is redundant due to (132) and (141).

So far, we have for R_1 the inequalities (124), (129), (132), (146) and for R_2 the inequalities (125), (136), (139), (149). An individual secrecy rate region is obtained as a set of the non-negative rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 \leq & \min\{I(V_0,V_1;Y_1) - I_1, \quad I(V_0,V_1;Y_1|U) - I(V_0,V_1;Z|U) + R_2\}; \\ R_2 \leq & \min\{I(V_0,V_2;Y_2) - I_2, \quad I(V_0,V_2;Y_2|U) - I(V_0,V_2;Z|U) + R_1\}, \end{aligned}$$

with

$$I_1 = \max\{I(V_1;Z|V_0),\ I(V_1;V_2|V_0) - I(V_2;Y_2|V_0),\ I(V_1;V_2|V_0) + I(V_0;Z|U) - I(V_0,V_2;Y_2|U)\};$$
$$I_2 = \max\{I(V_2;Z|V_0),\ I(V_1;V_2|V_0) - I(V_1;Y_1|V_0),\ I(V_1;V_2|V_0) + I(V_0;Z|U) - I(V_0,V_1;Y_1|U)\},$$

Note that $U \to V_0 \to (V_1,V_2) \to (Y_1,Y_2,Z)$ forms a Markov chain such that (130), (131), (137), (138), (141) hold. Further, we notice that $I_1 = I(V_1;Z|V_0)$ since

$$I(V_1;V_2|V_0) - I(V_2;Y_2|V_0) \overset{(a)}{\leq} I(V_1;V_2|V_0) - I(V_2;Z|V_0) \overset{(b)}{\leq} I(V_1;Z|V_0);$$
$$I(V_1;V_2|V_0) + I(V_0;Z|U) - I(V_0,V_2;Y_2|U) \overset{(c)}{\leq} I(V_1;V_2|V_0) + I(V_0;Z|U) - I(V_0,V_2;Z|U) \overset{(b)}{\leq} I(V_1;Z|V_0),$$

where (a) is due to (137); (b) is due to (141); and (c) is due to (138). Similarly, we have $I_2 = I(V_2;Z|V_0)$. Thus the region could be simplified into

$$\begin{aligned} R_1 \leq& \min\{I(V_0,V_1;Y_1) - I(V_1;Z|V_0),\quad I(V_0,V_1;Y_1|U) - I(V_0,V_1;Z|U) + R_2\} \\ =& I(V_0,V_1;Y_1|U) - I(V_0,V_1;Z|U) + \min\{R_2,\ I(U;Y_1) + I(V_0;Z|U)\}; \\ R_2 \leq& \min\{I(V_0,V_2;Y_2) - I(V_2;Z|V_0),\quad I(V_0,V_2;Y_2|U) - I(V_0,V_2;Z|U) + R_1\} \\ =& I(V_0,V_2;Y_2|U) - I(V_0,V_2;Z|U) + \min\{R_1,\ I(U;Y_2) + I(V_0;Z|U)\}. \end{aligned}$$

This is the desired region in (20) in Theorem 11.

References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Systems Technical Journal*, vol. 28, pp. 656–715, 1949.

[2] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Transactions of the American Institute of Electrical Engineers*, vol. XLV, pp. 295–301, Jan. 1926.

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

[4] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[5] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proc. 19th International Conference on Theory and Application of Cryptographic Techniques*, ser. EUROCRYPT'00. Berlin, Heidelberg: Springer-Verlag, 2000, pp. 351–368. [Online]. Available: http://dl.acm.org/citation.cfm?id=1756169.1756202

[6] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[7] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. i. secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[8] C. Mitrpant, A. J. H. Vinck, and Y. Luo, "An achievable region for the gaussian wiretap channel with side information," *IEEE Transactions on Information Theory*, vol. 52, no. 5, pp. 2181–2190, May 2006.

[9] Y. Chen and A. Vinck, "Wiretap channel with side information," *IEEE Transactions on Information Theory*, vol. 54, no. 1, pp. 395–402, Jan. 2008.

[10] W. Liu and B. Chen, "Wiretap channel with two-sided channel state information," in *Proc. Forty-First Asilomar Conference on Signals, Systems and Computers (ACSSC 2007)*, Nov. 2007, pp. 893–897.

[11] Y.-K. Chia and A. El Gamal, "Wiretap channel with causal state information," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2838–2849, May 2012.

[12] M. El-Halabi, T. Liu, C. N. Georghiades, and S. Shamai, "Secret writing on dirty paper: A deterministic view," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3419–3429, Jun. 2012.

[13] H. Boche and R. Schaefer, "Wiretap channels with side information: Strong secrecy capacity and optimal transceiver design," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1397–1408, Aug. 2013.

[14] R. Ahlswede and N. Cai, "Transmission, identification and common randomness capacities for wire-tape channels with secure feedback from the decoder," in *General Theory of Information Transfer and Combinatorics*, R. Ahlswede, L. Bäumer, N. Cai, H. Aydinian, and V. Blinovsky, Eds. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 258–275. [Online]. Available: http://dl.acm.org/citation.cfm?id=2168005.2168021

[15] D. Gunduz, D. Brown, and H. Poor, "Secret communication with feedback," in *Proc. 2008 International Symposium on Information Theory and Its Applications (ISITA)*, Dec. 2008, pp. 1–6.

[16] L. Lai, H. El Gamal, and H. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Transactions on Information Theory*, vol. 54, no. 11, pp. 5059–5067, Nov. 2008.

[17] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5353–5361, Dec. 2009.

[18] Z. Rezki, A. Khisti, and M.-S. Alouini, "Ergodic secret message capacity of the wiretap channel with finite-rate feedback," *IEEE Transactions on Wireless Communications*, vol. 13, no. 6, pp. 3364–3379, Jun. 2014.

[19] A. Khisti, S. Diggavi, and G. W. Wornell, "Secret-key generation using correlated sources and channels," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 652–670, Feb. 2012.

[20] V. M. Prabhakaran, K. Eswaran, and K. Ramchandran, "Secrecy via sources and channels," *IEEE Transactions on Information Theory*, vol. 58, no. 11, pp. 6747–6765, Nov. 2012.

[21] Y. Chen, N. Cai, and A. Sezgin, "Wiretap channel with correlated sources," in *Proc. 2014 IEEE International Conference on Cloud Engineering (IC2E)*, Mar. 2014, pp. 472–477.

[22] H. Yamamoto, "Rate-distortion theory for the shannon cipher system," *IEEE Transactions on Information Theory*, vol. 43, no. 3, pp. 827–835, May 1997.

[23] N. Merhav, "Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2723–2734, Jun. 2008.

[24] W. Kang and N. Liu, "Wiretap channel with shared key," in *Proc. 2010 IEEE Information Theory Workshop (ITW)*, Aug. 2010, pp. 1–5.

[25] R. Liu, T. Liu, H. Poor, and S. Shamai, "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 59, no. 3, pp. 1346–1359, Mar. 2013.

[26] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "Secrecy rate region of the broadcast channel with an eavesdropper," *CoRR*, vol. abs/0910.3658, 2009.

[27] E. Ekrem and S. Ulukus, "Capacity-equivocation region of the gaussian mimo wiretap channel," *IEEE Transactions on Information Theory*, vol. 58, no. 9, pp. 5699–5710, Sep. 2012.

[28] R. Wyrembelski, M. Wiese, and H. Boche, "Strong secrecy in bidirectional broadcast channels with confidential messages," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 324–334, Feb. 2013.

[29] Y. Liang and H. Poor, "Multiple-access channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[30] A. Pierrot and M. Bloch, "Strongly secure communications over the two-way wiretap channel," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 595–605, Sep. 2011.

[31] A. El Gamal, O. O. Koyluoglu, M. Youssef, and H. El Gamal, "Achievable secrecy rate regions for the two-way wiretap channel," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8099–8114, Dec. 2013.

[32] R. Liu, I. Maric, P. Spasojević, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[33] O. O. Koyluoglu and H. El Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Transactions on Information Theory*, vol. 57, no. 9, pp. 5682–5694, Sep. 2011.

[34] E. Ekrem and S. Ulukus, "Degraded compound multi-receiver wiretap channels," *IEEE Transactions on Information Theory*, vol. 58, no. 9, pp. 5681–5698, Sep. 2012.

[35] G. Kramer and S. Shamai, "Capacity for classes of broadcast channels with receiver side information," in *Proc. 2007 IEEE Information Theory Workshop (ITW '07)*, Sep. 2007, pp. 313–318.

[36] R. Wyrembelski, A. Sezgin, and H. Boche, "Secrecy in broadcast channels with receiver side information," in *Proc. 2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Nov. 2011, pp. 290–294.

[37] R. Wyrembelski and H. Boche, "Physical layer integration of private, common, and confidential messages in bidirectional relay networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 9, pp. 3170–3179, Sep. 2012.

[38] ——, "Privacy in bidirectional relay networks," *IEEE Transactions on Communications*, vol. 60, no. 6, pp. 1659–1668, Jun. 2012.

[39] A. Mansour, R. Schaefer, and H. Boche, "Secrecy measures for broadcast channels with receiver side information: Joint vs individual," in *Proc. 2014 IEEE Information Theory Workshop (ITW)*, Hobart, TAS, Nov. 2014, pp. 426–430.

[40] A. S. Mansour, R. F. Schaefer, and H. Boche, "Capacity Regions for Broadcast Channels With Degraded Message Sets and Message Cognition Under Different Secrecy Constraints," *CoRR*, vol. abs/1501.04490, Jan. 2015. [Online]. Available: http://arxiv.org/abs/1501.04490

[41] O. O. Koyluoglu, Y. Chen, and A. Sezgin, "Broadcast channel with receiver side information: Achieving individual secrecy," in *Proc. 2014 International Zurich Seminar on Communications (IZS 2014)*, Zurich, Switzerland, Feb. 2014.

[42] Y. Chen, O. O. Koyluoglu, and A. Sezgin, "On the achievable individual-secrecy rate region for broadcast channels with receiver side information," in *Proc. 2014 IEEE International Symposium on Information Theory (ISIT 2014)*, Jun. 2014, pp. 26–30.

[43] K. Bhattad and K. Narayanan, "Weakly secure network coding," in *Proc. First Workshop on Network Coding, Theory, and Applications (NetCod)*, Apr. 2005.

[44] S. H. Dau, W. Song, and C. Yuen, "On block security of regenerating codes at the MBR point for distributed storage systems," *CoRR*, vol. abs/1309.2712, Sep. 2013. [Online]. Available: http://arxiv.org/abs/1309.2712

[45] J. Liu, H. Wang, M. Xian, and K. Huang, "A secure and efficient scheme for cloud storage against eavesdropper," in *Proc. 15th International Conference on Information and Communications Security ICICS, Beijing, China*, Nov. 2013, pp. 75–89.

[46] A. S. Avestimehr, S. N. Diggavi, and D. N. Tse, "Wireless network information flow: A deterministic approach," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 1872–1905, Apr. 2011.

[47] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. New York, NY, USA: Cambridge University Press, 2012.

[48] Y.-K. Chia and A. El Gamal, "Three-receiver broadcast channels with common and confidential messages," *Information Theory, IEEE Transactions on*, vol. 58, no. 5, pp. 2748–2765, May 2012.

[49] A. El Gamal and E. Van Der Meulen, "A proof of marton's coding theorem for the discrete memoryless broadcast channel (corresp.)," *IEEE Transactions on Information Theory*, vol. 27, no. 1, pp. 120–122, Jan. 1981.