ON THE USE OF SECRET KEYS IN BROADCAST CHANNELS WITH RECEIVER SIDE INFORMATION

Rafael F. Schaefer[*]*, Ashish Khisti*[†]*, and Holger Boche*[‡]

[*]Dept. of EE
Princeton University
Princeton, USA

[†]Dept. of ECE
University of Toronto
Toronto, Canada

[‡]Lst. Theoret. Informationstechnik
Technische Universität München
München, Germany

ABSTRACT

The use of secret keys in broadcast channels with receiver side information is studied. The particular scenario is analyzed where a transmitter wants to send two confidential messages to two receivers, while keeping an external eavesdropper ignorant. Each receiver has one of the confidential messages as side information available for decoding. In addition to that, the transmitter shares independent secret keys of arbitrary rates with both receivers. The secret keys can be used in different ways: They can act as one-time pads to encrypt the confidential messages or they can be used as randomization resources for wiretap coding. Both approaches are discussed and an achievable rate region based on superposition coding is established for the one-time pad approach. For the wiretap coding approach, the secrecy capacity for degraded channels is derived. In the optimal coding scheme, the available secret keys are used as the randomization part of the wiretap code to keep the eavesdropper ignorant. In establishing the capacity region, a new upper bound on the sum-rate is derived. This bound shows that in an optimal coding scheme, in the degraded case, the total equivocation-rate of the (opposite) secret-keys at the legitimate receivers must equal the equivocation-rate of the secret-keys at the eavesdropper, when informed about the messages.

Index Terms— Broadcast channel with receiver side information, strong secrecy, secret key, capacity region.

1. INTRODUCTION

Ongoing developments in communication systems make information available almost everywhere. Along with this, it is an important task to secure sensitive information from unauthorized access. This applies in particular to wireless communication systems which are inherently vulnerable due to the open nature of the wireless medium. In fact, transmitted signals are received by intended users but are also easily eavesdropped by non-legitimate receivers.

The problem of secure communication from an information theoretic perspective was first studied by Shannon in [1]. In this work, transmitter and receiver share a secret key which is unknown to an external eavesdropper. Such a secret key can then be used by the legitimate users as a *one-time pad* to perfectly protect the confidential message from the eavesdropper.

The work of Rafael F. Schaefer was supported by the German Research Foundation (DFG) under Grant WY 151/2-1. The work of Holger Boche was supported by the German Ministry of Education and Research (BMBF) under Grant 01BQ1050. The work of Ashish Khisti was supported by QNRF, a member of Qatar Foundation, project NPRP 5-603-2-243.

Subsequently, Wyner introduced in [2] the so-called *wiretap channel* which models the scenario with one legitimate transmitter-receiver pair and one external eavesdropper to be kept ignorant. In contrast to [1], there is no secret key available so that secure communication must be established by solely exploiting the properties of the noisy channel. Later, this was generalized by Csiszár and Körner in [3] to the *broadcast channel with confidential messages*. Recently, this area of *information theoretic secrecy* has drawn attention as it provides a promising approach to embed secure communication in wireless networks; for instance see [4–7] and references therein. Information theoretic secrecy concepts have then been extended to multi-user scenarios such as several variations of the broadcast channel [3, 8–10], the multiple access channel [11], or the interference channel [12]. But all these works have in common that no shared secret keys are available at the legitimate users.

A shared secret key available at transmitter and receiver has only been studied for the wiretap channel [13–15], where [13, 14] studied this from a rate-distortion point of view. Then, [15] established the secrecy capacity of the wiretap channel with shared key for the case of no distortion allowed at the legitimate receiver. Related to this is the problem of the wiretap channel with secure feedback, where the feedback, basically, allows to create a shared secret key [16–18].

In this paper, we study the *broadcast channel (BC) with receiver side information and independent secret keys* as introduced in Section 2. In this communication scenario, the transmitter wants to send two confidential messages to two receivers, while keeping an external eavesdropper ignorant of them. Each receiver has one of the confidential messages as side information available for decoding. In addition to that, the transmitter shares independent secret keys, one with each receiver.

Secure communication can now be achieved by different approaches. As shared secret keys of arbitrary rates are available at the transmitter and both receivers, it suggests itself to use them as one-time pads to encrypt the confidential messages as in [1]. Unfortunately, each receiver is aware of only one secret key. Thus, the more one secret key is used to protect the message for one receiver, the more the other receiver is hurt as the (unknown) secret key acts as interference to him. This approach is analyzed in Section 3, where an achievable rate region based on superposition coding is derived.

On the other hand, the transmitter can apply the information theoretic secrecy concepts of wiretap coding by exploiting the properties of the noisy channels [2–7]. In this approach, parts of the available resources have to be used for additional randomization to "*confuse*" the eavesdropper reducing the remaining resources for the transmission of the confidential messages. In Section 4 this approach is analyzed and the secrecy capacity is derived for degraded channels. It is shown that it is optimal to use the available secret keys not

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

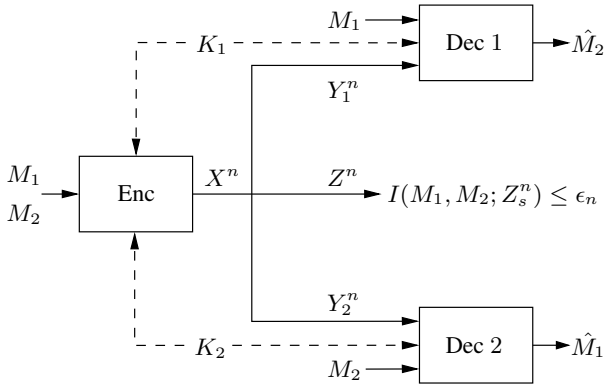

Fig. 1. Broadcast channel with receiver side information, where the transmitter shares an independent secret key with each receiver.

as one-time pads but as the randomization part of the wiretap code.

The communication problem at hand can be motivated, for example, by the concept of bidirectional relaying in a three-node network, in which a relay node establishes bidirectional communication between two other nodes using a decode-and-forward protocol [19–22]. In the initial multiple access phase, both nodes transmit their messages and also additional secret keys to the relay node. Then, the succeeding broadcast phase corresponds to the BC with receiver side information and independent secret keys considered here.[1]

2. BROADCAST CHANNEL WITH RECEIVER SIDE INFORMATION AND INDEPENDENT SECRET KEYS

In this paper we study the *broadcast channel (BC) with receiver side information and independent secret keys* as depicted in Fig. 1. Let $\mathcal{X}$ and $\mathcal{Y}_1$, $\mathcal{Y}_2$, $\mathcal{Z}$ be finite input and output sets. For input and output sequences $x^n \in \mathcal{X}^n$ and $y_1^n \in \mathcal{Y}_1^n$, $y_2^n \in \mathcal{Y}_2^n$, $z^n \in \mathcal{Z}^n$ of length n, the discrete memoryless broadcast channel is given by $P^n_{Y_1Y_2Z|X}(y_1^n, y_2^n, z^n|x^n) \coloneqq \prod_{i=1}^n P_{Y_1Y_2Z|X}(y_{1,i}, y_{2,i}, z_i|x_i)$.

The transmitter wants to send confidential messages M_2 and M_1 to receivers 1 and 2 respectively, while each receiver has the other message as side information available for decoding. The transmitter shares independent secret keys K_1 and K_2 of arbitrary rates with receivers 1 and 2. All messages and keys are assumed to be independent of each other and uniformly distributed over the sets $\mathcal{M}_i \coloneqq \{1, ..., M_{i,n}\}$ and $\mathcal{K}_i \coloneqq \{1, ..., K_{i,n}\}$, $i = 1, 2$. We also write $M_{12} = (M_1, M_2)$, $K_{12} = (K_1, K_2)$, $\mathcal{M}_{12} \coloneqq \mathcal{M}_1 \times \mathcal{M}_2$, and $\mathcal{K}_{12} \coloneqq \mathcal{K}_1 \times \mathcal{K}_2$ for short.

Definition 1. *An* $(n, M_{1,n}, M_{2,n}, K_{1,n}, K_{2,n})$-code *for the BC with receiver side information and independent secret keys consists of a (stochastic) encoder*

$$E : \mathcal{M}_{12} \times \mathcal{K}_{12} \to \mathcal{P}(\mathcal{X}^n), \tag{1}$$

i.e., a stochastic matrix, and decoders at receivers 1 and 2

$$\varphi_1 : \mathcal{Y}_1^n \times \mathcal{M}_1 \times \mathcal{K}_1 \to \mathcal{M}_2 \tag{2a}$$

$$\varphi_2 : \mathcal{Y}_2^n \times \mathcal{M}_2 \times \mathcal{K}_2 \to \mathcal{M}_1. \tag{2b}$$

[1]*Notation:* $H(\cdot)$ and $I(\cdot;\cdot)$ are the traditional entropy and mutual information; $X - Y - Z$ denotes a Markov chain of random variables X, Y, and Z in this order; $\otimes$ denotes the bit-wise XOR operation.

Then for an $(n, M_{1,n}, M_{2,n}, K_{1,n}, K_{2,n})$-code, the average probability of decoding error at receiver 1 is given by

$$\bar{e}_{1,n} = \frac{1}{|\mathcal{M}_{12}||\mathcal{K}_{12}|} \sum_{m_{12}\in\mathcal{M}_{12}} \sum_{k_{12}\in\mathcal{K}_{12}} \sum_{x^n\in\mathcal{X}^n} \times \sum_{y_1^n:\varphi_1(y_1^n,m_1,k_1)\neq m_2} P^n_{Y_1|X}(y_1^n|x^n) E(x^n|m_{12}, k_{12}). \tag{3}$$

The average probability of decoding error $\bar{e}_{2,n}$ at receiver 2 is defined accordingly.

To keep the confidential messages secret from the eavesdropper, we impose the *strong secrecy* [23, 24] requirement

$$I(M_{12}; Z^n) \leq \delta_n \tag{4}$$

for $\delta_n > 0$ with $M_{12} = (M_1, M_2)$ and $Z^n = (Z_1, ..., Z_n)$ the output at the eavesdropper. This requires (M_1, M_2) to be jointly secure from the eavesdropper. Then, (4) implies that the individual criteria $I(M_1; Z^n) \leq \delta_n$ and $I(M_2; Z^n) \leq \delta_n$ are satisfied as well.

Definition 2. *A rate pair* $(R_1, R_2) \in \mathbb{R}_+^2$ *is said to be* achievable *for the BC with receiver side information and independent secret keys if for any* $\tau > 0$ *there exists an* $n(\tau) \in \mathbb{N}$ *and a sequence of* $(n, M_{1,n}, M_{2,n}, K_{1,n}, K_{2,n})$*-codes such that for all* $n \geq n(\tau)$ *we have* $\frac{1}{n}\log M_{2,n} \geq R_1 - \tau$, $\frac{1}{n}\log M_{1,n} \geq R_2 - \tau$, *and* $I(M_1, M_2; Z^n) \leq \delta_n$ *while* $\bar{e}_{1,n}, \bar{e}_{2,n}, \delta_n \to 0$ *as* $n \to \infty$. *The set of all achievable rate pairs is the* secrecy capacity region $\mathcal{C}_S$.[2]

In principle, there are two different methods possible to keep the confidential messages secret. The transmitter can follow the idea of *information theoretic secrecy* or *wiretap coding* by using a channel code that exploits the nature of the wireless channel to keep the messages secret [2–7]. On the other hand, the availability of shared secret keys suggests itself to use a *one-time pad* approach which protects the messages with the help of the secret keys [1]. In the following we analyze these different approaches in more detail.

3. SECRET KEYS AS ONE-TIME PAD

Let us start with the one-time pad approach, where the secret keys are used to mask the confidential messages keeping them perfectly secret from the eavesdropper. Basically, the idea is to use secret keys of the same rates as the corresponding messages, i.e., $|\mathcal{K}_1| = |\mathcal{M}_2|$ and $|\mathcal{K}_2| = |\mathcal{M}_1|$, to create "*new*" messages based on a bit-wise XOR operation as

$$\widetilde{M}_2 = M_2 \otimes K_1 \quad \text{and} \quad \widetilde{M}_1 = M_1 \otimes K_2 \tag{5}$$

and to encode and transmit these messages to the corresponding receivers. Having decoded the XOR-ed messages $\widetilde{M}_2$ and $\widetilde{M}_1$, each receiver can use his secret key to obtain the desired confidential message, i.e., $\widetilde{M}_2 \otimes K_1 = M_2 \otimes K_1 \otimes K_1 = M_2$ and $\widetilde{M}_1 \otimes K_2 = M_1 \otimes K_2 \otimes K_2 = M_1$ respectively. As all keys and messages are independent of each other, the confidential messages are kept perfectly secret from the eavesdropper, i.e., $I(M_1, M_2; Z^n) = 0$, even if he is able to decode the XOR-ed messages $\widetilde{M}_1$ and $\widetilde{M}_2$.

Applying the one-time pad approach in this way, the problem at hand reduces to the broadcast channel problem with two independent

[2]The rate between the transmitter and receiver i is denoted by R_i, $i = 1, 2$. However, the message associated to rate R_1 is M_2 which is motivated by the application of bidirectional relaying, where the M_2 originates from node 2 and, thus, looks "swapped." The same applies to M_1 and R_2.

individual messages. Thus, one can apply classical strategies such as superposition coding, cf. for example [25, Sec. 5.2], to encode and transmit the XOR-ed messages.

Proposition 1 (Superposition Coding)**.** *An achievable rate region for the BC with receiver side information and independent secret keys is given by all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ that satisfy*

$$R_1 \leq I(X;Y_1|U) \tag{6a}$$
$$R_2 \leq I(U;Y_2) \tag{6b}$$
$$R_1 + R_2 \leq I(X;Y_1) \tag{6c}$$

for random variables satisfying the Markov chain $U - X - (Y_1, Y_2)$.

This approach solely relies on using the secret keys as one-time pads and does not take advantage of the properties of the wireless channel by applying wiretap coding approaches. Thus, such an approach might not be optimal in general. However, for scenarios where the channel to the eavesdropper is "*stronger*" than the channels to the legitimate receivers, we observe the following.

Remark 1. *If the channels to the legitimate receivers are degraded with respect to the eavesdropper channel, i.e., we have the Markov chains $X - Z - Y_1$ and $X - Z - Y_2$, then the confidential messages can be kept secret from the eavesdropper by using the secret keys as one-time pads. Wiretap coding approaches will always fail in such scenarios as they require the legitimate channel to be "stronger" than the eavesdropper channel.*

4. SECRET KEYS AS PART OF WIRETAP CODES

Here we want to explore the case where the secret keys are used as parts of the wiretap code and not as one-time pads. The basic idea of wiretap coding is not to use all available resources for transmitting the desired messages, but to spend some of the resources to "*confuse*" the eavesdropper by applying randomized encoding strategies [2–7]. If a sufficient amount of resources is spent for the confusion, the eavesdropper will not be able to decode the desired confidential messages. Obviously, the more resources are spent for the confusion, the less resources are available for the actual message transmission. Here is where the secret keys enter the picture in this approach. They will not be used as a one-time pad, but as resources for the confusion.

In the following we consider the case where the legitimate channels are stronger than the eavesdropper channel in the sense that they form Markov chains $X - Y_1 - Z$ and $X - Y_2 - Z$. Then, the secrecy capacity region is given by the following theorem.

Theorem 1. *The secrecy capacity region for the degraded BC with receiver side information and independent secret keys is given by all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ that satisfy*

$$R_1 \leq I(X;Y_1) \tag{7a}$$
$$R_2 \leq I(X;Y_2) \tag{7b}$$
$$R_1 + R_2 \leq I(X;Y_1) + I(X;Y_2) - I(X;Z) \tag{7c}$$

for random variables satisfying $X - Y_1 - Z$ and $X - Y_2 - Z$.

4.1. Proof of Achievability

In the following we outline the proof of achievability. To do so, we first observe that for any fixed input distribution, the desired region given by (7) can equivalently be expressed as

$$R_1 \leq I(X;Y_1) - \alpha I(X;Z) \tag{8a}$$
$$R_2 \leq I(X;Y_2) - (1-\alpha) I(X;Z) \tag{8b}$$

for all $0 \leq \alpha \leq 1$. Thus, instead of proving the achievability of (7), we show that the rates given in (8) are achievable with strong secrecy for all $0 \leq \alpha \leq 1$.

4.1.1. Key Ideas

The proof of achievability is based on the following two main ingredients:

1. Wiretap coding for strong secrecy. The transmitter uses a stochastic encoder so that the codewords x_{mk}^n consist of two indices: one for the confidential message $m \in \mathcal{M}$ and one for additional randomization $k \in \mathcal{K}$ to confuse the eavesdropper. In particular, for the classical wiretap channel, choosing the rate for the randomization as

$$\frac{1}{n} \log |\mathcal{K}| > I(X;Z) + \epsilon \tag{9}$$

for some small $\epsilon > 0$, i.e., $|\mathcal{K}| > 2^{n(I(X;Z)+\epsilon)}$, allows to show that strong secrecy, i.e., $I(M;Z^n) \leq \delta_n$, is satisfied at the eavesdropper. This has been demonstrated for example in [7, 26, 27] for the classical wiretap channel and in [10] for the BC with receiver side information. Traditionally, the legitimate receiver has to decode both the confidential message and the randomization index, which is possible as we have $|\mathcal{M}||\mathcal{K}| < 2^{n(I(X;Y)-\epsilon)}$ codewords in total. Thus, for the rate of the confidential message remains

$$R < I(X;Y) - I(X;Z) - 2\epsilon, \tag{10}$$

i.e., $|\mathcal{M}| < 2^{n(I(X;Y)-I(X;Z)-2\epsilon)}$, cf. also [4, 7].

2. Coding for the BC with receiver side information. The transmitter encodes both messages $m_1 \in \mathcal{M}_1$ and $m_2 \in \mathcal{M}_2$ into one codeword $x_{m_1 m_2}^n \in \mathcal{X}^n$ based on the network coding idea [21, 22]. The crucial observation is that the available complementary side information at the receivers allow them to reduce the number of possible messages. In more detail, we chose rates

$$R_1 < I(X;Y_1) - \epsilon \quad \text{and} \quad R_2 < I(X;Y_2) - \epsilon, \tag{11}$$

i.e., $|\mathcal{M}_2| < 2^{n(I(X;Y_1)-\epsilon)}$ and $|\mathcal{M}_1| < 2^{n(I(X;Y_2)-\epsilon)}$, so that in total we generate $|\mathcal{M}_1||\mathcal{M}_2|$ codewords $x_{m_1 m_2}^n \in \mathcal{X}^n$. In principle, the total rate of the codewords is above the respective capacities of the user's channels. However, the available side information allows each receiver to "cancel" out one index reducing the remaining rate below the respective capacity making reliable communication possible at the rates given in (11), cf. [21, 22, 28].

4.1.2. Sketch of Proof

Having these two main ideas in mind, we are ready to prove the achievability of the rates given in (8) for any $0 \leq \alpha \leq 1$. We follow the coding scheme presented in [10, 26] and define for any given input distribution $P_X \in \mathcal{P}(\mathcal{X})$ the probability measure

$$P'_{X^n}(x^n) \coloneqq \frac{P_X^n(x^n)}{\mathcal{T}_{X,\delta}^n} \tag{12}$$

if $x^n \in \mathcal{T}_{X,\delta}^n$ and $P'_{X^n}(x^n) = 0$ else, where $P_X^n(x^n) \coloneqq \prod_{i=1}^n P_X(x_i)$ and $\mathcal{T}_{X,\delta}^n$ is the set of δ-typical sequences, cf [29]. Now, according to P'_{X^n}, we generate $|\mathcal{M}_1||\mathcal{M}_2||\mathcal{K}_1||\mathcal{K}_2|$ independent codewords $x_{m_1 m_2 k_1 k_2}^n \in \mathcal{X}^n$ where

$$|\mathcal{M}_1| < 2^{n(I(X;Y_2)-\alpha I(X;Z)-2\epsilon)} \tag{13a}$$
$$|\mathcal{M}_2| < 2^{n(I(X;Y_1)-(1-\alpha)I(X;Z)-2\epsilon)} \tag{13b}$$
$$|\mathcal{K}_1| > 2^{n(\alpha I(X;Z)+\epsilon)} \tag{13c}$$
$$|\mathcal{K}_2| > 2^{n((1-\alpha)I(X;Z)+\epsilon)}. \tag{13d}$$

The important difference to the classical wiretap coding approach is that instead of generating "*dummy*" randomization indices, we use the available secret keys as randomization resources.

As the amount of randomization resources satisfy

$$\frac{1}{n}\log(|\mathcal{K}_1||\mathcal{K}_2|) > I(X;Z) + 2\epsilon, \tag{14}$$

we can show similarly as in [10, 26] that $I(M_1, M_2; Z^n) \leq \delta_n$ holds so that the strong secrecy requirement (4) is satisfied.

Let us now turn to the legitimate receivers. Receiver 1 has $m_1 \in \mathcal{M}_1$ and $k_1 \in \mathcal{K}_1$ as side information available and is interested in the confidential message $m_2 \in \mathcal{M}_2$. Due to his side information, the unknown indices to receiver 1 are $m_2 \in \mathcal{M}_2$ and $k_2 \in \mathcal{K}_2$ of size

$$|\mathcal{M}_2||\mathcal{K}_2| \approx 2^{n(I(X;Y_1)-\epsilon)}. \tag{15}$$

It can be easily shown that this means that he is able to decode the remaining indices $m_2 \in \mathcal{M}_2$ and $k_2 \in \mathcal{K}_2$ so that $R_1 \leq I(X;Y_1) - \alpha I(X;Z)$ is an achievable rate for the confidential message M_2, cf. (8a).

Similarly, receiver 2 has $m_2 \in \mathcal{M}_2$ and $k_2 \in \mathcal{K}_2$ as side information so that the number of possible unknown indices reduces to

$$|\mathcal{M}_1||\mathcal{K}_1| \approx 2^{n(I(X;Y_2)-\epsilon)} \tag{16}$$

which means that he is able to decode the remaining indices $m_1 \in \mathcal{M}_1$ and $k_1 \in \mathcal{K}_1$ so that $R_2 \leq I(X;Y_2) - (1-\alpha)I(X;Z)$ is an achievable rate for the confidential message M_1, cf. (8b).

4.1.3. Discussion

In the classical wiretap coding, a certain amount of resources ($\approx I(X;Z)$) has to be used for additional randomization to keep the eavesdropper ignorant. This results in a loss in rates of the confidential messages. Using the secret keys for this randomization has the advantage that parts of the additional randomization are already as side information available at the receivers. This reduces the loss in confidential rate in the sense that the rate is only reduced by the remaining unknown randomization part.

4.2. Proof of Converse

It remains to show the optimality of the above presented approach, i.e., there are no other rate pairs achievable than those given in (7).

The bounds (7a) and (7b) are the obvious single-user bounds and follow immediately. The main part is to prove the bound (7c) on the sum-rate.

We have the following versions of Fano's inequality $H(M_2|Y_1^n, M_1, K_1) \leq \epsilon_{1,n}$ and $H(M_1|Y_2^n, M_2, K_2) \leq \epsilon_{2,n}$. Following the classical approach for the wiretap channel [4, 7], we obtain for the sum-rate

$$\begin{aligned}
n(R_1+R_2) &\leq H(M_1,M_2|Z^n)+n\delta_n && \text{(17a)}\\
&\leq I(M_2;Y_1^n|M_1,K_1)+I(M_1;Y_2^n|M_2,K_2)\\
&\quad -I(M_{12};Z^n)+n\epsilon_n && \text{(17b)}\\
&\leq I(M_{12},K_1;Y_1^n)+I(M_{12},K_2;Y_2^n)\\
&\quad -I(M_{12};Z^n)+n\epsilon_n && \text{(17c)}\\
&= I(M_{12},K_{12};Y_1^n)+I(M_{12},K_{12};Y_2^n)\\
&\quad -I(M_{12},K_{12};Z^n)-I(K_2;Y_1^n|M_{12},K_1)\\
&\quad -I(K_1;Y_2^n|M_{12},K_2)+I(K_{12};Z^n|M_{12})+n\epsilon_n && \text{(17d)}\\
&\leq I(M_{12},K_{12};Y_1^n)+I(M_{12},K_{12};Y_2^n)\\
&\quad -I(M_{12},K_{12};Z^n)+n\epsilon_n && \text{(17e)}
\end{aligned}$$

with $\epsilon_n = \delta_n + \epsilon_{1,n} + \epsilon_{2,n}$ and $\epsilon_n \to 0$ as $n \to \infty$. The steps follow from the secrecy condition (4), Fano's inequalities, the chain rule for mutual information, and the fact that $-I(K_2;Y_1^n|M_{12},K_1) - I(K_1;Y_2^n|M_{12},K_2) + I(K_{12};Z^n|M_{12}) \leq 0$. To see the last step, we write

$$\begin{aligned}
&-I(K_2;Y_1^n|M_{12},K_1)-I(K_1;Y_2^n|M_{12},K_2)+I(K_{12};Z^n|M_{12})\\
&\quad = -H(K_1|M_{12},K_2)+H(K_1|Y_2^n,M_{12},K_2)\\
&\qquad\quad -H(K_2|M_{12},K_1)+H(K_2|Y_1^n,M_{12},K_1)\\
&\qquad\quad +H(K_{12}|M_{12})-H(K_{12}|Z^n,M_{12}) && \text{(18a)}\\
&\quad = H(K_1|Y_2^n,M_{12},K_2)+H(K_2|Y_1^n,M_{12},K_1)\\
&\qquad\quad -H(K_{12}|Z^n,M_{12}) && \text{(18b)}\\
&\quad \leq H(K_1|Z^n,M_{12},K_2)+H(K_2|Z^n,M_{12},K_1)\\
&\qquad\quad -H(K_{12}|Z^n,M_{12}) && \text{(18c)}\\
&\quad \leq 0 && \text{(18d)}
\end{aligned}$$

where the first step follows from the definition of mutual information, the second step from the fact that M_1, M_2, K_1, and K_2 are independent so that $-H(K_1|M_{12},K_2) - H(K_2|M_{12},K_1) + H(K_{12}) = 0$, the third step from the Markov chains $X - Y_1 - Z$ and $X - Y_2 - Z$ due to the degradedness of the channels, and the last step from the chain rule of entropy. Now, we can bound the sum-rate as follows

$$\begin{aligned}
&n(R_1+R_2)\\
&\quad \leq I(M_{12},K_{12};Y_1^n)+I(M_{12},K_{12};Y_2^n)\\
&\qquad -I(M_{12},K_{12};Z^n)+n\epsilon_n && \text{(19a)}\\
&\quad = I(M_{12},K_{12};Y_1^n|Z^n)+I(M_{12},K_{12};Y_2^n)+n\epsilon_n && \text{(19b)}\\
&\quad \leq I(X^n;Y_1^n|Z^n)+I(X^n;Y_2^n)+n\epsilon_n && \text{(19c)}\\
&\quad \leq n\big(I(X;Y_1|Z)+I(X;Y_2)\big)+n\epsilon_n && \text{(19d)}\\
&\quad = n\big(I(X;Y_1)+I(X;Y_2)-I(X;Z)\big)+n\epsilon_n && \text{(19e)}
\end{aligned}$$

where the second step follows from the degradedness of the channels, the third step from the data processing inequality, the fourth step from the memoryless property of the channel, and the last step again from the degradedness.

The upper bound on the sum-rate shows that in an optimal coding scheme, the total equivocation-rate of the (opposite) secret-keys at the legitimate receivers must equal the equivocation-rate of the secret-keys at the eavesdropper, when informed about the messages.

5. CONCLUSION

In this paper, we studied the BC with receiver side information and independent secret keys. In this communication problem, multiple secret keys are shared among the legitimate users. We asked the question how these keys should be used to securely transmit confidential messages to their respective receivers keeping an external eavesdropper ignorant of them. For reversely degraded channels, i.e., the eavesdropper channel is "stronger" than the legitimate channels, the confidential messages can be securely transmitted by using the secret keys as one-time pads. On the other hand, if the channels are degraded in the sense that the legitimate channels are "stronger" than the eavesdropper channel, it is optimal to use the secret keys not as one-time pads but as randomization resources for wiretap coding. Thus, the optimal use of secret keys is not obvious and open for the general case.

6. REFERENCES

[1] Claude E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656715, Oct. 1949.

[2] Aaron D. Wyner, "The Wire-Tap Channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[3] Imre Csiszár and János Körner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] Yingbin Liang, H. Vincent. Poor, and Shlomo Shamai (Shitz), "Information Theoretic Security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

[5] Ruoheng Liu and Wade Trappe, Eds., *Securing Wireless Communications at the Physical Layer*, Springer, 2010.

[6] Eduard A. Jorswieck, Anne Wolf, and Sabrina Gerbracht, "Secrecy on the Physical Layer in Wireless Networks," *Trends in Telecommunications Technologies*, pp. 413–435, Mar. 2010.

[7] Matthieu Bloch and João Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[8] Ersen Ekrem and Sennur Ulukus, "Capacity Region of Gaussian MIMO Broadcast Channels With Common and Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5669–5680, Sept. 2012.

[9] Ruoheng Liu, Tie Liu, H. Vincent Poor, and Shlomo Shamai (Shitz), "New Results on Multiple-Input Multiple-Output Broadcast Channels With Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1346–1359, Mar. 2013.

[10] Rafael F. Wyrembelski, Moritz Wiese, and Holger Boche, "Strong Secrecy in Bidirectional Broadcast Channels with Confidential Messages," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 2, pp. 324–334, Feb. 2013.

[11] Yingbin Liang and H. Vincent. Poor, "Multiple-Access Channels With Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[12] Ruoheng Liu, Ivana Marić, Predrag Spasojević, and Roy D. Yates, "Discrete Memoryless Interference and Broadcast Channels With Confidential Messages: Secrecy Rate Regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, June 2008.

[13] Hirosuke Yamamoto, "Rate-Distortion Theory for the Shannon Cipher System," *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 827–835, May 1997.

[14] Neri Merhav, "Shannon's Secrecy System With Informed Receivers and its Application to Systematic Coding for Wiretapped Channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2723–2734, June 2008.

[15] Wei Kang and Nan Liu, "Wiretap Channel with Shared Key," in *Proc. IEEE Inf. Theory Workshop*, Dublin, Ireland, Aug. 2010, pp. 1–5.

[16] Rudolf Ahlswede and Ning Cai, *General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science*, vol. 4123, chapter Transmission, Identification and Common Randomness Capacities for Wire-Tape Channels with Secure Feedback from the Decoder, pp. 258–275, Springer, 2006.

[17] Deniz Gündüz, D. Richard Brown III, and H. Vincent Poor, "Secret Communication with Feedback," in *Proc. Int. Symp. Inf. Theory Applications*, Auckland, New Zealand, Dec. 2008, pp. 1–6.

[18] Ehsan Ardestanizadeh, Massimo Franceschetti, Tara Javidi, and Young-Han Kim, "Wiretap Channel With Secure Rate-Limited Feedback," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5353–5361, Dec. 2009.

[19] Peter Larsson, Niklas Johansson, and Kai-Erik Sunell, "Coded Bi-directional Relaying," in *Proc. 5th Scandinavian Workshop on Ad Hoc Networks*, Stockholm, Sweden, May 2005, pp. 851–855.

[20] Boris Rankov and Armin Wittneben, "Spectral Efficient Protocols for Half-Duplex Fading Relay Channels," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 2, pp. 379–389, Feb. 2007.

[21] Tobias J. Oechtering, Clemens Schnurr, Igor Bjelaković, and Holger Boche, "Broadcast Capacity Region of Two-Phase Bidirectional Relaying," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 454–458, Jan. 2008.

[22] Sang Joon Kim, Patrick Mitran, and Vahid Tarokh, "Performance Bounds for Bidirectional Coded Cooperation Protocols," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5235–5241, Nov. 2008.

[23] Imre Csiszár, "Almost Independence and Secrecy Capacity," *Probl. Pered. Inform.*, vol. 32, no. 1, pp. 48–57, 1996.

[24] Ueli M. Maurer and Stefan Wolf, "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free," in *EUROCRYPT 2000, Lecture Notes in Computer Science*, vol. 1807, pp. 351–368. Springer-Verlag, May 2000.

[25] Abbas El Gamal and Young-Han Kim, *Network Information Theory*, Cambridge University Press, 2011.

[26] Igor Bjelaković, Holger Boche, and Jochen Sommerfeld, "Secrecy Results for Compound Wiretap Channels," *Probl. Inf. Transmission*, vol. 49, no. 1, pp. 73–98, Mar. 2013.

[27] Jie Hou and Gerhard Kramer, "Informational Divergence Approximations to Product Distributions," in *Proc. Canadian Workshop Inf. Theory*, Toronto, ON, Canada, June 2013, pp. 76–81.

[28] Gerhard Kramer and Shlomo Shamai (Shitz), "Capacity for Classes of Broadcast Channels with Receiver Side Information," in *Proc. IEEE Inf. Theory Workshop*, Tahoe City, CA, USA, Sept. 2007, pp. 313–318.

[29] Imre Csiszár and János Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Cambridge University Press, 2 edition, 2011.