Secure Broadcasting of a Common Message with Independent Secret Keys

Rafael F. Schaefer
Department of Electrical Engineering
Princeton University
Princeton, NJ 08544, USA

Ashish Khisti
Department of Electrical and Computer Engineering
University of Toronto
Toronto, ON, M5S 3G4, Canada

***Abstract*—The problem of secure broadcasting with independent secret keys is studied. The particular scenario is analyzed where a common message has to be broadcasted to two legitimate receivers, while keeping an external eavesdropper ignorant of it. The transmitter shares independent secret keys of arbitrary rates with both legitimate receivers, which can be used in different ways: They can be used as one-time pads to encrypt the common message or they can be used as randomization resources for wiretap coding. Both approaches are studied in this paper. If both legitimate channels are degraded versions of the eavesdropper channel, it is shown that the one-time pad approach is optimal for several cases yielding corresponding capacity expressions. Reversely, the wiretap coding approach is shown to be optimal if the eavesdropper channel is degraded with respect to both legitimate channels establishing capacity in this case as well.**

I. Introduction

Rapid developments in communication systems make information easily accessible almost everywhere. Accordingly, an appropriate design which ensures the security of sensitive information is of high priority. Shannon was the first who studied in [1] the problem of secure communication from an information theoretic perspective. He considered a noiseless communication scenario, where transmitter and receiver share a secret key which is unknown to the non-legitimate eavesdropper. Used as a *one-time pad*, this secret key enables a secure transmission of the confidential message.

Subsequently, Wyner looked at the noisy case in [2], where he introduced the now-popular *wiretap channel*. He extended the problem studied by Shannon insofar that legitimate receiver and eavesdropper now observe noisy versions of the input. In addition, there is no secret key available as in [1] so that the communication must be secured solely by exploiting the properties of the noisy channel. Recently, this area of *information theoretic secrecy* has drawn attention especially in the area of wireless communication where it provides a promising complement to cryptographic approaches, cf. for example [3], [4], [5], [6] and references therein. These concepts have been extended to several multi-user scenarios such as the broadcast channel [7], [8], [9], [10], multiple access channel [11], [12], or interference channel [13]. All these works have in common that no secret key is available to the legitimate users.

These two approaches were combined in [14], [15], [16], which study the (noisy) wiretap channel with shared secret key. This was done from rate-distortion point of view in [14], [15], while [16] established the secrecy capacity for the case of no distortion allowed at the legitimate receiver. Related to this problem is the wiretap channel with secured feedback as this feedback can be used to create a shared secret key [17], [18], [19].

Surprisingly, to the best of our knowledge the use of secret keys in noisy multi-user communication scenarios has not been studied so far. Accordingly, the question of secure communication in *broadcast channels (BC) with independent secret keys* determines an interesting extension in this direction. A secret key shared between the transmitter and one receiver can be used to securely transmit to that receiver, but might harm other receivers which do not share this key. Thus, multiple shared keys can result in conflicting payoffs at different receivers making it a challenging and non-trivial problem. In this paper, we study the problem of securely broadcasting a common message to two legitimate receivers, while keeping an eavesdropper ignorant of it. The transmitter shares independent secret keys of arbitrary rates with both receivers, which is introduced in Section II.

Secure communication can now be realized by different approaches. As shared secret keys are available at transmitter and both receivers, it suggests itself to use them as *one-time pads* to encrypt the common message as in [1]. However, each receiver is aware of only one secret key. Thus, the more one secret key of one receiver is used to secure the message, the more the other receiver is hurt as the unknown secret key acts as interference to him. As the general case is challenging, we study this approach for the case where the eavesdropper channel is the "strongest" among all channels (in the sense that both legitimate channels are degraded versions of it). In Section III we determine the corresponding secrecy capacity. It is shown to be optimal to use both secret keys to create two encrypted messages and to encode and transmit them using superposition coding.

On the other hand, the properties of the noisy channels can be exploited by applying information theoretic secrecy

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

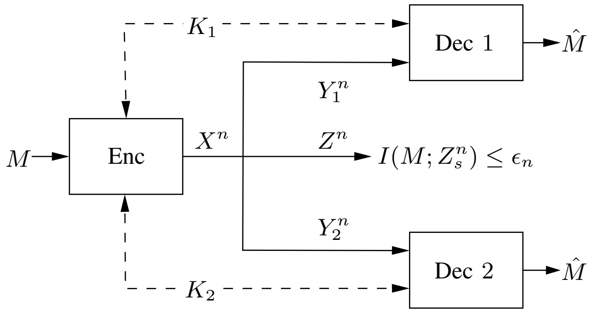

Fig. 1. Broadcast channel where the transmitter shares an independent secret key with each legitimate receiver.

concepts of *wiretap coding* [3], [4], [5], [6]. This approach is based on the idea of allocating some of the available resources for additional randomization to "confuse" the eavesdropper. The drawback is that this reduces the remaining resources available for the actual transmission of the message. We study this approach for the case where the eavesdropper channel is the "weakest" among all channels (in the sense that it is degraded with respect to both legitimate channels). In Section IV we establish the corresponding secrecy capacity and it is shown that using the available secret keys not as one-time pads but as the randomization part of the wiretap code is optimal.[1]

II. BC WITH INDEPENDENT SECRET KEYS

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

The transmitter broadcasts a common message M to receivers 1 and 2, while keeping the eavesdropper ignorant of it. The transmitter shares independent secret keys K_1 and K_2 of arbitrary rates with receivers 1 and 2. The message and both keys are assumed to be independent of each other and uniformly distributed over the sets $\mathcal{M} := \{1, ..., M_n\}$ and $\mathcal{K}_i := \{1, ..., K_{i,n}\}$, $i = 1, 2$. We also write $K_{12} = (K_1, K_2)$ and $\mathcal{K}_{12} = \mathcal{K}_1 \times \mathcal{K}_2$ for short.

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

$$E : \mathcal{M} \times \mathcal{K}_1 \times \mathcal{K}_2 \to \mathcal{P}(\mathcal{X}^n) \tag{1}$$

and decoders at receivers 1 and 2

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

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

Then the average probability of decoding error at receiver i, $i = 1, 2$, is given by

$$\begin{aligned}\bar{e}_{i,n} = \frac{1}{|\mathcal{M}||\mathcal{K}_{12}|} \sum_{m \in \mathcal{M}} \sum_{k_{12} \in \mathcal{K}_{12}} \sum_{x^n \in \mathcal{X}^n} \\ \times \sum_{y_i^n : \varphi_i(y_i^n, k_i) \neq m} P_{Y_i|X}^n(y_i^n|x^n) E(x^n|m, k_{12}).\end{aligned} \tag{3}$$

To ensure the confidentiality of the common message, we require

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

for $\delta_n > 0$ with M the random variable uniformly distributed over the set of messages $\mathcal{M}$ and $Z^n = (Z_1, ..., Z_n)$ the channel output at the eavesdropper. This condition is termed *strong secrecy* [20], [21] and the motivation is to control the total amount of information leaked to the eavesdropper.

Definition 2. A rate $R > 0$ is an *achievable secrecy rate* for the BC with independent secret keys if for any $\tau > 0$ there exists an $n(\tau) \in \mathbb{N}$ and a sequence of $(n, M_n, K_{1,n}, K_{2,n})$-codes such that for all $n \geq n(\tau)$ we have $\frac{1}{n} \log M_n \geq R - \tau$ and $I(M; Z^n) \leq \delta_n$ while $\bar{e}_{1,n}, \bar{e}_{2,n}, \delta_n \to 0$ as $n \to \infty$. The *secrecy capacity* C is given by the supremum of all achievable secrecy rates R.

From the problem setup, in principle there are different methods possible to keep the common message secret. The shared secret keys suggest itself to use a *one-time pad* approach which protects the message with the help of the secret keys [1]. On the other hand, the transmitter can exploit the nature of the wireless channel by using a channel code based on the idea of *information theoretic secrecy* or *wiretap coding* [2], [7], [3], [4], [5], [6]. In the following we will explore these different approaches and show that it depends on the channel conditions which particular approach is optimal.

III. SECRET KEYS AS ONE-TIME PAD

The obvious approach to secure the message is to use the available secret keys for encryption. Such a *one-time pad* approach will keep the message perfectly secret from the eavesdropper. To do so, we need secret keys of the same rate as the common message, i.e., $|\mathcal{K}_1| = |\mathcal{K}_2| = |\mathcal{M}|$, cf. [1]. Then we create *encrypted* messages based on a bit-wise XOR operation as

$$M_1 = M \otimes K_1 \qquad \text{and} \qquad M_2 = M \otimes K_2 \tag{5}$$

which are then encoded and transmitted to the corresponding receivers. Having decoded the XOR-ed messages M_1 and M_2, each receiver can then use its own secret key to obtain the desired original message M, i.e., $M_1 \otimes K_1 = M_1 \otimes K_1 \otimes K_1 = M$ and $M_2 \otimes K_2 = M_2 \otimes K_2 \otimes K_2 = M$ respectively. Since the message M and both keys K_1 and K_2 are uniformly distributed and independent of each other, M is kept perfectly secret from the eavesdropper, i.e., $I(M; Z^n) = 0$, even if it is able to decode the XOR-ed messages M_1 or M_2.

Using the secret keys in this way, basically, turns the problem of securely broadcasting a common message into the

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

problem of broadcasting two independent individual messages. Note that this approach solely relies on using the available secret keys as one-time pads. As it does not exploit the properties of the noisy channel, this approach might be suboptimal in general. However, we will discuss in the following that this approach is capacity-achieving for a special class of broadcast channels.

A. Equal Channel Outputs

To obtain the first insights, we start with the simplest scenario, where both legitimate receivers and the eavesdropper receive signals of the same quality, i.e., $Y = Y_1 = Y_2 = Z$.

Theorem 1. The secrecy capacity C of the BC with independent secret keys and equal channel outputs is

$$C = \max_{P_X} \frac{1}{2} I(X;Y) \tag{6}$$

with $Y = Y_1 = Y_2 = Z$, i.e., time-sharing between both legitimate receivers is optimal.

Proof: As both legitimate receivers and the eavesdropper all receive channel outputs of the same quality, we use the secret keys K_1 and K_2 as one-time pads to create encrypted individual messages M_1 and M_2 as discussed in (5). Since M, K_1, and K_2 are independent of each other, we immediately have ensured that $I(M;Z^n) = 0$. Thus, the communication problem becomes the reliable transmission of two independent individual messages. Obviously, the rate in (6) is easily achievable via time-sharing which establishes the achievability.

Thus, it remains to show that time-sharing is already optimal. At receiver i, $i = 1,2$, we have the following version of Fano's inequality

$$H(M|K_i, Y^n) \leq n\epsilon_{i,n} \tag{7}$$

with $\epsilon_{i,n} \to 0$ as $n \to \infty$. Making extensive use of the definition of mutual information and the chain rule, we get

$$\begin{aligned}
nR &= H(M|K_i) && \text{(8a)}\\
&\leq I(M;Y^n|K_i) + n\epsilon_{i,n} && \text{(8b)}\\
&\leq I(M;K_i,Y^n) + n\epsilon_{i,n} && \text{(8c)}\\
&= I(M;K_i|Y^n) + I(M;Y^n) + n\epsilon_{i,n} && \text{(8d)}\\
&\leq I(M;K_i|Y^n) + n\epsilon_{i,n} + n\delta_n && \text{(8e)}\\
&= H(K_i|Y^n) - H(K_i|M,Y^n) + n\epsilon_{i,n} + n\delta_n && \text{(8f)}\\
&\leq H(K_i) - H(K_i|M,Y^n) + n\epsilon_{i,n} + n\delta_n && \text{(8g)}
\end{aligned}$$

where (8a) follows from the independence of M and K_i, (8b) from Fano's inequality (7), and (8e) from the secrecy condition.

As (8g) must hold for both receivers simultaneously, we obtain

$$\begin{aligned}
nR &\leq \min_{i\in\{1,2\}} \Big\{ H(K_i) - H(K_i|M,Y^n) + n\epsilon_{i,n} + n\delta_n \Big\} && \text{(9a)}\\
&\leq \frac{1}{2}\Big[H(K_1) + H(K_2) \\
&\qquad - H(K_1|M,Y^n) - H(K_2|M,Y^n) + n\epsilon_n \Big] && \text{(9b)}\\
&\leq \frac{1}{2}\Big[H(K_{12}) - H(K_{12}|M,Y^n) + n\epsilon_n \Big] && \text{(9c)}\\
&= \frac{1}{2}\Big[H(K_{12}) + H(Y^n|M) - H(K_{12},Y^n|M) + n\epsilon_n \Big] && \text{(9d)}\\
&= \frac{1}{2}\Big[H(K_{12}) + H(Y^n|M) \\
&\qquad - H(K_{12}|M) - H(Y^n|M,K_{12}) + n\epsilon_n \Big] && \text{(9e)}\\
&= \frac{1}{2}\Big[H(Y^n|M) - H(Y^n|M,K_{12}) + n\epsilon_n \Big] && \text{(9f)}\\
&\leq \frac{1}{2}\Big[H(Y^n) - H(Y^n|M,K_{12}) + n\epsilon_n \Big] && \text{(9g)}\\
&= \frac{1}{2} I(M,K_{12};Y^n) + n\epsilon_n && \text{(9h)}\\
&\leq \frac{1}{2} I(X^n;Y^n) + n\epsilon_n && \text{(9i)}\\
&\leq \frac{1}{2} nI(X;Y) + n\epsilon_n && \text{(9j)}
\end{aligned}$$

with $\epsilon_n = \epsilon_{1,n} + \epsilon_{2,n} + 2\delta_n$ and $\epsilon_n \to 0$ as $n \to \infty$. This completes the converse and proves the desired result. ■

From this we immediately obtain the result for the noiseless case where the output at all receivers equals the input, i.e., $X = Y_1 = Y_2 = Z$.

Corollary 1. The secrecy capacity C of the noiseless BC with independent secret keys is

$$C = \max_{P_X} \frac{1}{2} H(X), \tag{10}$$

with $X = Y_1 = Y_2 = Z$, i.e., time-sharing between both legitimate receivers is optimal. ■

Remark 1. The result shows that in the case of equal channel outputs the simple strategy of time-sharing is already capacity-achieving. Thereby, the secret keys are used as one-time pads to transform the common message into two individual messages.

B. Degraded Channels

Next we turn to the case where all channel outputs are of different quality but satisfy a certain degradedness order where the eavesdropper has the strongest channel among all receivers. In particular, we assume that the following Markov chain relationship holds: $X - Z - Y_1 - Y_2$.

Theorem 2. The secrecy capacity of the BC with independent secret keys and reversely degraded channels is

$$C = \max_{P_{UX}} \min \big\{ I(X;Y_1|U), I(U;Y_2) \big\} \tag{11}$$

for any $P_{UX}(u,x)$ such that $U - X - Z - Y_1 - Y_2$ form a Markov chain, i.e., superposition coding is optimal. Further, the cardinality of the range of U can be bounded by $|\mathcal{U}| \leq |\mathcal{X}| + 1$.

Proof: As for the equal channel case in Theorem 1 we generate individual messages M_1 and M_2 by using the available secret keys K_1 and K_2 as one-time pads, cf. (5). Then the original message M is perfectly secure from the eavesdropper and the communication problem becomes again the transmission of two individual messages. Then the achievability of (11) follows immediately by superposition coding. Here, we choose the auxiliary random variable U to carry the individual message M_1 (as "cloud center") for the weaker receiver 2. The other message M_2 for the stronger receiver 1 is superimposed as "satellite codeword" in X.

Again, the crucial part is to show that this superposition coding strategy is already optimal. Using Fano's inequality (7) as in the proof of Theorem 1 we end up with (8b) from which we proceed as follows:

$$\begin{aligned} nR &\leq I(M;Y_i^n|K_i) + n\epsilon_{i,n} && \text{(12a)}\\ &\leq I(M,K_i;Y_i^n) + n\epsilon_{i,n} && \text{(12b)}\\ &= I(K_i;Y_i^n|M) + I(M;Y_i^n) - I(M;Z^n) + n\epsilon_n && \text{(12c)}\\ &\leq I(K_i;Y_i^n|M) + n\epsilon_n && \text{(12d)} \end{aligned}$$

with $\epsilon_n = \delta_n + \epsilon_{1,n}$ where (12c) follows from the chain rule and the secrecy condition, and (12d) from the degradedness so that $I(M;Y_i^n) - I(M;Z^n) \leq 0$.

Now, we define the auxiliary random variable

$$U_i := (M, K_2, Y_1^{i-1}) \tag{13}$$

and obtain for the weaker receiver 2

$$\begin{aligned} nR &\leq I(K_2;Y_2^n|M) + n\epsilon_n && \text{(14a)}\\ &\leq \sum_{i=1}^n I(M,K_2;Y_{2,i}|Y_2^{i-1}) + n\epsilon_n && \text{(14b)}\\ &\leq \sum_{i=1}^n I(M,K_2,Y_2^{i-1};Y_{2,i}) + n\epsilon_n && \text{(14c)}\\ &\leq \sum_{i=1}^n I(M,K_2,Y_1^{i-1},Y_2^{i-1};Y_{2,i}) + n\epsilon_n && \text{(14d)}\\ &= \sum_{i=1}^n I(M,K_2,Y_1^{i-1};Y_{2,i}) + n\epsilon_n && \text{(14e)}\\ &= \sum_{i=1}^n I(U_i;Y_{2,i}) + n\epsilon_n && \text{(14f)} \end{aligned}$$

where (14e) follows from the degradedness condition. Now, let Q be a time-sharing random variable independent of all others and uniformly distributed over $\{1,...,n\}$. We set $U = (U_Q, Q)$, $X = X_Q$, $Y_1 = Y_{1,Q}$, and $Y_2 = Y_{2,Q}$ and end up with

$$\begin{aligned} nR &\leq nI(U_Q;Y_{2,Q}|Q) + n\epsilon_n && \text{(15a)}\\ &\leq nI(U;Y_2) + n\epsilon_n. && \text{(15b)} \end{aligned}$$

With the same definition of U_i, cf. (13), we obtain for the stronger receiver 1

$$\begin{aligned} nR &\leq I(K_1;Y_1^n|M) + n\epsilon_n && \text{(16a)}\\ &\leq I(K_1;Y_1^n|M,K_2) + n\epsilon_n && \text{(16b)}\\ &= \sum_{i=1}^n I(K_1;Y_{1,i}|M,K_2,Y_1^{i-1}) + n\epsilon_n && \text{(16c)}\\ &\leq \sum_{i=1}^n I(K_1,X_i;Y_{1,i}|M,K_2,Y_1^{i-1}) + n\epsilon_n && \text{(16d)}\\ &= \sum_{i=1}^n I(X_i;Y_{1,i}|U_i) + n\epsilon_n && \text{(16e)}\\ &= nI(X_Q;Y_{1,Q}|U_Q,Q) + n\epsilon_n && \text{(16f)}\\ &= nI(X;Y_1|U) + n\epsilon_n && \text{(16g)} \end{aligned}$$

with $\epsilon_n = \delta_n + \epsilon_{2,n}$ which proves the converse.

The bound $|\mathcal{U}| \leq |\mathcal{X}| + 1$ on the cardinality of the range of the auxiliary random variable U follows from the strengthened version of Carathéodory's theorem, cf. for example [22], and standard arguments. The details are omitted for brevity. This completes the proof of the theorem. ■

Remark 2. The fact that the eavesdropper channel is the strongest among all channels (in the sense that both legitimate channels are degraded versions of it) suggests to use the secret keys as one-time pads to secure the message. In addition, the fact that both legitimate channels itself can be ordered due to their degradedness suggests to use a superposition coding scheme (as for the classical degraded BC). The previous result shows that this strategy is capacity-achieving.

IV. Secret Keys as Part of Wiretap Codes

Here we want to explore the approach, where the secret keys are incorporated in the wiretap code. The basic idea of wiretap coding is not to use all available resources for transmitting the message, but to allocate some of the resources to "confuse" the eavesdropper by applying randomized encoding strategies [3], [4], [5], [6]. If a sufficient amount of resources is spent for confusion, the eavesdropper will not be able to decode the transmitted message. Obviously, the more resources are allocated to this confusion, the less resources are available for the actual transmission of the message. Here is where the shared secret keys enter the picture in this approach. They will be used as randomization resources for this confusion which are (partly) already available at the legitimate receivers.

In the following we consider degraded channels $X - Y_1 - Z$ and $X - Y_2 - Z$, which means that the eavesdropper channel is degraded with respect to both legitimate channels. However, we impose no ordering between the legitimate channels itself.

Theorem 3. The secrecy capacity C of the BC with independent secret keys and degraded channels $X - Y_1 - Z$ and $X - Y_2 - Z$ is

$$C = \max_{P_X} \min \left\{ \begin{array}{l} I(X;Y_1) \\ I(X;Y_2) \\ \frac{1}{2}\big[I(X;Y_1) + I(X;Y_2) - I(X;Z)\big] \end{array} \right\}. \tag{17}$$

A. Proof of Achievability

The following equivalent description of (17) turns out to be beneficial for the proof of achievability.

Lemma 1. The rate expression in (17) *can equivalently be expressed as*

$$C = \max_{P_X} \max_{0\leq\alpha\leq 1} \min \left\{ \begin{array}{l} I(X;Y_1) - \alpha I(X;Z) \\ I(X;Y_2) - (1-\alpha) I(X;Z) \end{array} \right\}. \quad (18)$$

Proof: With the function

$$f(t) = \begin{cases} (1-t) I(X;Y_1) + t\big[I(X;Y_2) - I(X;Z)\big] & \text{if } t \leq \frac{1}{2} \\ (1-t)\big[I(X;Y_1) - I(X;Z)\big] + tI(X;Y_2) & \text{if } t \geq \frac{1}{2} \end{cases} \quad (19)$$

we can express rate expression in (17) as

$$C = \max_{P_X} \min_{0\leq t\leq 1} f(t). \quad (20)$$

As the function $f(t)$ is piecewise linear, it is sufficient to evaluate it at the corner points, i.e., when $t=0$, $t=1$, and $t=\frac{1}{2}$, to convince ourself that the rate expressions in (17) and (20) are equivalent.

Now we have to show that (20) is equivalent to the desired expression (18). Therefore, we rewrite (18) (where we omit the outer maximization for short) as

$$\begin{aligned} &\max_{0\leq\alpha\leq 1} \min_{0\leq t\leq 1} \Big[(1-t)\big[I(X;Y_1) - \alpha I(X;Z)\big] \\ &\qquad\qquad + t\big[I(X;Y_2) - (1-\alpha)I(X;Z)\big]\Big] \quad (21a) \\ &= \min_{0\leq t\leq 1} \max_{0\leq\alpha\leq 1} \Big[(1-t)\big[I(X;Y_1) - \alpha I(X;Z)\big] \\ &\qquad\qquad + t\big[I(X;Y_2) - (1-\alpha)I(X;Z)\big]\Big] \quad (21b) \end{aligned}$$

where the equality follows from the minimax theorem. Now eliminating α in (21b) yields for $t \leq \frac{1}{2}$ and $t \geq \frac{1}{2}$ the corresponding expressions in (20) which are then equivalent to the original formulation (17). ■

Thus, instead of proving the achievability of (17), we prove the achievability of (18) for any $0 \leq \alpha \leq 1$.

Next we sketch the proof of achievability. Basically, it follows the ideas of [23], [24], [25] which all present coding schemes that achieve strong secrecy as required in (4). Accordingly, for any input distribution $P_X \in \mathcal{P}(\mathcal{X})$ and $\alpha \in [0,1]$ we generate $|\mathcal{M}||\mathcal{K}_1||\mathcal{K}_2|$ independent codewords $x^n_{mk_1k_2} \in \mathcal{X}^n$ where

$$|\mathcal{K}_1| > 2^{n((1-\alpha)I(X;Z)+\epsilon)} \quad (22a)$$

$$|\mathcal{K}_2| > 2^{n(\alpha I(X;Z)+\epsilon)} \quad (22b)$$

$$|\mathcal{M}| < \min \left\{ \begin{array}{l} 2^{n(I(X;Y_1)-\alpha I(X;Z)-2\epsilon)} \\ 2^{n(I(X;Y_2)-(1-\alpha)I(X;Z)-2\epsilon)} \end{array} \right\}. \quad (22c)$$

The crucial idea is to use the available secret keys as randomization resources instead of generating "*dummy*" randomization indices as in the classical wiretap coding approach. As the size of the secret keys satisfy

$$\frac{1}{n}\log(|\mathcal{K}_1||\mathcal{K}_2|) > I(X;Z) + 2\epsilon \quad (23)$$

we have enough randomization resources to show that $I(M;Z^n) \leq \delta_n$ holds, i.e., strong secrecy (4) is satisfied. This can be done similarly as in [23], [24], [25].

Next, we check the reliability constraints at the legitimate receivers. Receiver 1 has the secret key $k_1 \in \mathcal{K}_1$ as side information available and therefore the unknown indices of the transmitted codeword are $m \in \mathcal{M}$ and $k_2 \in \mathcal{K}_2$. As its size satisfy

$$|\mathcal{M}||\mathcal{K}_2| \leq 2^{n(I(X;Y_1)-\epsilon)}, \quad (24)$$

it is straight forward to show that receiver 1 can decode the remaining indices $m \in \mathcal{M}$ and $k_2 \in \mathcal{K}_2$. Similarly, receiver 2 has $k_2 \in \mathcal{K}_2$ as side information available and the unknown indices are $m \in \mathcal{M}$ and $k_1 \in \mathcal{K}_1$ of size

$$|\mathcal{M}||\mathcal{K}_1| \leq 2^{n(I(X;Y_2)-\epsilon)}. \quad (25)$$

Again, it is easy to show that receiver 2 can decode the remaining indices $m \in \mathcal{M}$ and $k_1 \in \mathcal{K}_1$. Thus, we conclude that (18) is an achievable rate.

Remark 3. For the classical wiretap coding, the amount of resources needed for additional randomization is roughly $I(X;Z)$. This suffices to keep the eavesdropper ignorant. The use of secret keys as the randomization resource has the advantage that parts of the needed randomization are already as side information available at the receivers. This reduces the loss in rate in the sense that it is only reduced by the remaining unknown randomization part (and not by the whole randomization part).

B. Proof of Converse

It remains to show the optimality of the above presented coding scheme. The first two bounds in (17) are the obvious single-user bounds and follow immediately. The crucial part is to prove the third "sum-rate"-like bound. We proceed as following:

$$\begin{aligned} n2R &\leq H(M) + H(M) = H(M|K_1) + H(M|K_2) \quad (26a) \\ &\leq I(M;Y_1^n|K_1) + I(M;Y_2^n|K_2) + n\epsilon_{1,n} + n\epsilon_{2,n} \quad (26b) \\ &\leq I(M;Y_1^n|K_1) + I(M;Y_2^n|K_2) \\ &\qquad - I(M;Z^n) + n\epsilon_n \quad (26c) \\ &\leq I(M,K_1;Y_1^n) + I(M,K_2;Y_2^n) \\ &\qquad - I(M;Z^n) + n\epsilon_n \quad (26d) \\ &= I(M,K_{12};Y_1^n) + I(M,K_{12};Y_2^n) \\ &\qquad - I(M,K_{12};Z^n) - I(K_2;Y_1^n|M,K_1) \\ &\qquad - I(K_1;Y_2^n|M,K_2) + I(K_{12};Z^n|M) + n\epsilon_n \quad (26e) \\ &\leq I(M,K_{12};Y_1^n) + I(M,K_{12};Y_2^n) \\ &\qquad - I(M,K_{12};Z^n) + n\epsilon_n \quad (26f) \end{aligned}$$

with $\epsilon_n = \delta_n + \epsilon_{1,n} + \epsilon_{2,n}$ and $\epsilon_n \to 0$ as $n \to \infty$. Here, (26b) follows from Fano's inequality, cf. (7), (26c) from the secrecy criterion, and (26f) from the fact that $-I(K_2;Y_1^n|M,K_1) - I(K_1;Y_2^n|M,K_2) + I(K_1,K_2;Z^n|M) \leq 0$. To see this last step, we write

$$\begin{aligned}
&- I(K_2;Y_1^n|M,K_1) - I(K_1;Y_2^n|M,K_2) + I(K_{12};Z^n|M) \\
&\quad = -H(K_2|M,K_1) + H(K_2|M,K_1,Y_1^n) \\
&\qquad - H(K_1|M,K_2) + H(K_1|M,K_2,Y_2^n) \\
&\qquad + H(K_{12}|M) - H(K_{12}|M,Z^n) && \text{(27a)} \\
&\quad = H(K_2|M,K_1,Y_1^n) - H(K_1|M,K_2,Y_2^n) \\
&\qquad - H(K_{12}|M,Z^n) && \text{(27b)} \\
&\quad \leq H(K_2|M,K_1,Z_1^n) - H(K_1|M,K_2,Z_2^n) \\
&\qquad - H(K_{12}|M,Z^n) && \text{(27c)} \\
&\quad \leq 0 && \text{(27d)}
\end{aligned}$$

where (27b) follows from the fact that M, K_1, and K_2 are independent so that $-H(K_2|M,K_1) - H(K_1|M,K_2) + H(K_{12}|M) = 0$, and (27c) from the Markov chains $X-Y_1-Z$ and $X-Y_2-Z$ due to the degradedness. Now, with this we can proceed with the "sum-rate" in (26f) as

$$\begin{aligned}
n2R &\leq I(M,K_{12};Y_1^n) + I(M,K_{12};Y_2^n) \\
&\qquad - I(M,K_{12};Z^n) + n\epsilon_n && \text{(28a)} \\
&= I(M,K_{12};Y_1^n|Z^n) + I(M,K_{12};Y_2^n) + n\epsilon_n && \text{(28b)} \\
&\leq I(X^n;Y_1^n|Z^n) + I(X^n;Y_2^n) + n\epsilon_n && \text{(28c)} \\
&\leq n\big[I(X;Y_1|Z) + I(X;Y_2)\big] + n\epsilon_n && \text{(28d)} \\
&= n\big[I(X;Y_1) + I(X;Y_2) - I(X;Z)\big] + n\epsilon_n && \text{(28e)}
\end{aligned}$$

where (28b) and (28e) follow from the degradedness of the channels. This completes the proof of converse. ■

Remark 4. An interesting observation is that in an capacity-achieving coding scheme, the total equivocation-rate of the opposite secret keys at the legitimate receivers must be equal to the equivocation-rate of the secret keys at the eavesdropper, when informed about the message.

V. Conclusion

In this paper we studied the BC with independent secret keys. This describes a communication problem where multiple secret keys are shared among the legitimate users. Shared secret keys suggest itself to be used as one-time pads to encrypt confidential messages for keeping external eavesdropper ignorant. However, a secret key shared between the transmitter and one receiver might harm other receivers which do not share this key. Thus, multiple secret keys can result in conflicting payoffs at different receivers, which rises the question how these keys should be used in an optimal way.

For reversely degraded channels, which means the eavesdropper channel is the "stronger" than the legitimate channels, classical wiretap coding does not work and the confidential message can be protected by using the secret keys as one-time pads. For the full degraded case, it is shown that this strategy is actually capacity-achieving.

On the other hand, for degraded channels, in which the eavesdropper channel is the "weakest" channel, it is shown to be optimal to use the secret keys not as one-time pads but as randomization resources within the wiretap coding.

References

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

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

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

[4] R. Liu and W. Trappe, Eds., *Securing Wireless Communications at the Physical Layer*. Springer, 2010.

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

[6] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

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

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

[9] R. Liu, T. Liu, H. V. Poor, and S. 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] R. F. Wyrembelski, M. Wiese, and H. 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] Y. Liang and H. V. Poor, "Multiple-Access Channels With Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[12] M. Wiese and H. Boche, *Information Theory, Combinatorics, and Search Theory*. Springer, 2013, ch. Strong Secrecy for Multiple Access Channels, pp. 71–122.

[13] R. Liu, I. Marić, P. Spasojević, and R. 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, Jun. 2008.

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

[15] N. 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, Jun. 2008.

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

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

[18] D. Gündüz, D. R. B. III, and H. V. Poor, "Secret Communication with Feedback," in *Proc. Int. Symp. Inf. Theory Applications*, Auckland, New Zealand, Dec. 2008, pp. 1–6.

[19] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap Channel With Secure Rate-Limited Feedback," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5353–5361, Dec. 2009.

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

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

[22] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge University Press, 2011.

[23] I. Bjelaković, H. Boche, and J. Sommerfeld, "Secrecy Results for Compound Wiretap Channels," *Probl. Inf. Transmission*, vol. 49, no. 1, pp. 73–98, Mar. 2013.

[24] M. R. Bloch and J. N. Laneman, "Strong Secrecy from Channel Resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.

[25] J. Hou and G. Kramer, "Effective Secrecy: Reliability, Confusion and Stealth," available at http://arxiv.org/abs/1311.1411.