Wiretap Channels: Roles of Rate Splitting and Channel Prefixing

Omur Ozel Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland College Park, MD 20742
omur@umd.edu *ulukus@umd.edu*

***Abstract*—Csiszár and Körner's characterization of the rate-equivocation region of a general wiretap channel involves two auxiliary random variables: U, which represents rate splitting and V, which represents channel prefixing. For some channels, one or both of these auxiliary random variables are unnecessary, simplifying the expression and evaluation of the rate-equivocation region. In this paper, we provide new conditions under which channel prefixing or rate splitting does not improve the rate-equivocation region. In particular, we show that when the main channel is more capable than the eavesdropping channel, channel prefixing is unnecessary; the entire rate-equivocation region can be achieved by rate splitting alone. Conversely, we show under a mild assumption that if the main receiver is not more capable, then channel prefixing is strictly necessary. Moreover, we show that if the main channel is more capable but not less noisy, then rate splitting is strictly necessary. Next, we focus on the set of cyclic shift symmetric channels. We prove that for these channels, if in addition $I(X;Y)-I(X;Z)$ is maximized at the uniform distribution, then rate splitting is unnecessary. Our results apply to BSC-BEC and BEC-BSC wiretap channels. We identify the conditions on the parameters of the BSC and BEC under which channel prefixing and/or rate splitting are unnecessary.**

I. Introduction

We consider the discrete memoryless wiretap channel shown in Fig. 1. The capacity region of this channel is characterized by the rate, R, between the legitimate users Alice and Bob, and the equivocation, R_e, at the eavesdropper Eve. Wyner [1] characterized the rate-equivocation region when the received signal at Eve is a degraded version of the signal received at Bob. Csiszár and Körner [2] characterized the rate-equivocation region for general, not necessarily degraded, wiretap channels.

Csiszár and Körner's characterization involves two auxiliary random variables: U, for rate splitting, and V, for channel prefixing. Evaluation of capacity regions involving auxiliary random variables is generally difficult, and it is desirable to determine cases where auxiliary random variables are not needed. For the wiretap channel, under certain conditions, it is known that the use of one or both of these auxiliary random variables is unnecessary. For instance, if the wiretap channel is degraded, neither rate splitting nor channel prefixing is necessary, i.e., the selection $U=\phi$ and $V=X$ is optimal, for the entire rate-equivocation region [1]. In fact, the same conclusion holds if the wiretap channel is less noisy [2]. For general wiretap channels, for the purposes of characterizing the secrecy capacity, i.e., the largest equivocation, rate splitting is unnecessary, i.e., $U=\phi$ is optimal [2]; further, if the wiretap channel is more capable, then channel prefixing as well is unnecessary, i.e., $U=\phi$ and $V=X$ are optimal [2].

This work was supported by NSF Grants CCF 07-29127, CNS 09-64632, CCF 09-64645 and CCF 10-18185.

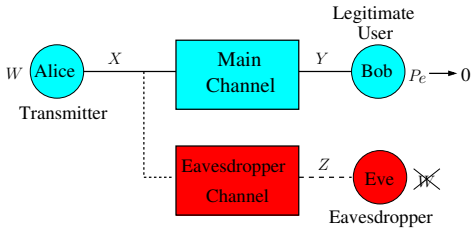

Fig. 1. The wiretap channel.

In this paper, we develop new conditions under which rate splitting and/or channel prefixing are unnecessary. The inclusion relations among the classes of wiretap channels considered in this paper are shown in Fig. 2. First, we show that if the wiretap channel is more capable, then channel prefixing is unnecessary for the entire rate-equivocation region; that is, the entire rate-equivocation region can be characterized by rate-splitting, i.e., $V=X$ is optimal and the boundary of the rate-equivocation region can be traced with optimal (U,X) only. Conversely, we prove under a mild condition that if the channel is not more capable, then channel prefixing is strictly necessary, i.e., $V\neq X$ is strictly needed. Moreover, we prove that if the wiretap channel is more capable but not less noisy, a non-trivial rate splitting, i.e., $U\neq\phi$, is strictly necessary. If the wiretap channel is more capable and cyclic shift symmetric (shaded region in Fig. 2), we show that the capacity of Bob's link and the largest equivocation can be achieved simultaneously. We then focus on cyclic shift symmetric channels, and show that if in addition $I(X;Y)-I(X;Z)$ is maximized at the uniform distribution, then rate splitting is unnecessary, i.e., $U=\phi$ is optimal. Finally, we investigate two examples that illustrate the considered cases: BSC-BEC and BEC-BSC wiretap channels. We identify the conditions on the BSC cross-over probability and the BEC erasure probability that guarantee that channel prefixing or rate splitting or both are unnecessary.

II. Model and Background

As in Fig. 1, Alice communicates with Bob in the presence of an eavesdropper, Eve. The input and output alphabets, $\mathcal{X}$,

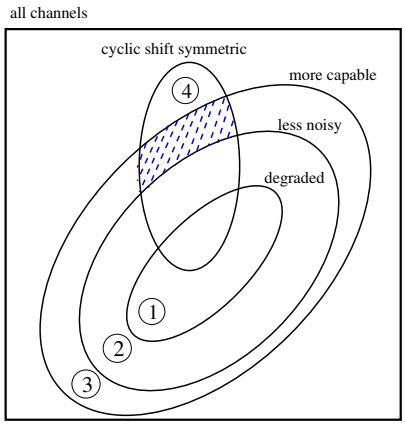

Fig. 2. Inclusion relations among the classes of wiretap channels.

$\mathcal{Y}$ and $\mathcal{Z}$, are finite. The main channel is characterized by $p(y|x)$ and has capacity $C_B = \max_{P_x} I(X;Y)$. Similarly the wiretapper channel is characterized by $p(z|x)$ and has capacity $C_E = \max_{P_x} I(X;Z)$. W represents the message to be sent to Bob and kept secret from Eve with $W \in \mathcal{W} = \{1, \ldots, 2^{nR}\}$. Alice uses an encoder $\varphi : \mathcal{W} \to \mathcal{X}^n$ to map each message to a channel input of length n. Bob uses a decoder $g : \mathcal{Y}^n \to \mathcal{W}$. Probability of error is: $P_e = \Pr[g(Y^n) \neq W]$. The rate R is achievable with equivocation R_e, if $P_e \to 0$ as $n \to \infty$, and

$$R_e = \lim_{n\to\infty} \frac{1}{n} H(W|Z^n) \tag{1}$$

Perfect secrecy[1] is achieved if $\frac{1}{n} I(W; Z^n) \to 0$ and secrecy capacity C_s is the highest achievable perfectly secure rate R. The maximum possible equivocation is also C_s.

Let $m = |\mathcal{X}|$, then the input distribution P_x belongs to the probability simplex denoted as

$$\Delta_m = \left\{ (p_1, \ldots, p_m) \,\middle|\, \sum_{i=1}^{m} p_i = 1, \quad p_i \geq 0, \ \forall i \right\} \tag{2}$$

Throughout the paper, $f(.)$ denotes the following function of the input distribution P_x

$$f(P_x) = I(X;Y) - I(X;Z) \tag{3}$$

Csiszár and Körner [2] characterized the entire rate-equivocation region as stated in the following theorem.

Theorem 1 ([2, Corollary 2]) *(R, R_e) pair is in the rate-equivocation region iff there exist $U \to V \to X \to YZ$ such that $I(U;Y) \leq I(U;Z)$, and*

$$0 \leq R_e \leq I(V;Y|U) - I(V;Z|U) \tag{4}$$

$$R_e \leq R \leq I(V;Y) \tag{5}$$

Further, the secrecy capacity is

$$C_s = \max_{V \to X \to YZ} [I(V;Y) - I(V;Z)] \tag{6}$$

[1]We use the weak secrecy notion. However, for discrete channels weak and strong secrecy are equivalent [3].

The rate-equivocation region of a wiretap channel is convex. Therefore, its upper right boundary is traced by solving the following optimization problem[2] for all $\mu \geq 0$

$$\max_{U,V} \quad \mu I(V;Y) + [I(V;Y|U) - I(V;Z|U)] \tag{7}$$

In particular, the optimal value of the objective in (7) at $\mu = 0$ is the secrecy capacity C_s. In this case, U is unnecessary, and in fact, we get (6) [2].

III. More Capable Channels

More capable condition is a partial ordering for discrete memoryless channels as formally defined below.

Definition 1 ([2]) *$p(y|x)$ is more capable than $p(z|x)$ if $f(P_x) \geq 0$ for all $P_x \in \Delta_m$.*

A wiretap channel is more capable if the main channel is more capable than the eavesdropping channel.

In [2, Theorem 3], Csiszár and Körner observe that if the wiretap channel is more capable, then channel prefixing is unnecessary, i.e., $V = X$ is optimal, for achieving the secrecy capacity. We will strengthen this result. We will prove that if the wiretap channel is more capable, then channel prefixing is unnecessary for the rate-equivocation region.

Let $\mathbf{e}_j$ denote the elementary PMF where all the mass is concentrated in the jth coordinate, i.e., its jth entry is 1 and all other entries are zero. Note that $\mathbf{e}_j$, $j = 1, \ldots, m$, form the canonical basis for the m dimensional Euclidean space, and in particular, Δ_m is the convex hull of $\mathbf{e}_j$, $j = 1, \ldots, m$. We have the following lemma.

Lemma 1 *Let $\mathbf{p}$ and $\mathbf{p}'$ be two PMFs in Δ_m. There exists a PMF $\mathbf{q}$ and an index set $J \subset \{1, \ldots, m\}$ with $|J| = m - 1$ such that*

$$\mathbf{p}' = q_1 \mathbf{p} + \sum_{i=1}^{m-1} q_{i+1} \mathbf{e}_{j_i} \tag{8}$$

where $j_i \in J$ for $i = 1, \ldots, m-1$. In particular, $q_1 > 0$ if $\mathbf{p}'$ is an interior point of Δ_m, i.e., $p'_i \neq 0$.

Proof: The probability simplex Δ_m has corner points $\mathbf{e}_j$, $j = 1, \ldots, m$. Given $\mathbf{p} \in \Delta_m$, we can find a triangulation [4] $\{\mathcal{D}_i\}_{i=1}^m$ of $\{\mathbf{e}_1, \ldots, \mathbf{e}_m, \mathbf{p}\}$ by combining $m-1$ of the corner points and $\mathbf{p}$. Then, we get $\Delta_m = \bigcup_{i=1}^m \mathcal{D}_i$ where $\mathcal{D}_i$ is the convex hull of $[\{\mathbf{e}_1, \ldots, \mathbf{e}_m\} \setminus \{\mathbf{e}_i\}] \cup \{\mathbf{p}\}$, $i = 1, \ldots, m$. Hence, a given PMF $\mathbf{p}'$ resides inside one of $\mathcal{D}_i$. This proves the first desired result. Moreover, if $\mathbf{p}'$ has all non-zero entries, then it is an interior point of some $\mathcal{D}_i$. Hence, $q_1 > 0$ in this case. ■

Lemma 1 says that any PMF over an m letter alphabet can be expressed as a convex combination of any other PMF and $m - 1$ of the m canonical PMFs $\mathbf{e}_j$, $j = 1, \ldots, m$. We use this result to prove the following theorem.

[2]Due to the bounds on the sizes of U and V [2], this optimization problem is computable.

Theorem 2 *If the wiretap channel is more capable, then channel prefixing does not improve the rate-equivocation region. Moreover, if the wiretap channel is not more capable and $f(P_x)$ is maximized at an interior point of Δ_m, then channel prefixing strictly improves the rate-equivocation region.*

Proof: Assume that $p(y|x)$ is more capable than $p(z|x)$. For any $U \to V \to X \to YZ$ and $\mu > 0$, we have

$$\begin{aligned}
&\mu I(V;Y) + I(V;Y|U) - I(V;Z|U) \\
&\quad = \mu[I(X;Y) - I(X;Y|V)] + I(X;Y|U) - I(X;Z|U) \\
&\qquad - [I(X;Y|V,U) - I(X;Z|V,U)] \qquad (9) \\
&\quad = \mu I(X;Y) + I(X;Y|U) - I(X;Z|U) \\
&\qquad - [(\mu+1)I(X;Y|V) - I(X;Z|V)] \qquad (10) \\
&\quad \leq \mu I(X;Y) + I(X;Y|U) - I(X;Z|U) \qquad (11)
\end{aligned}$$

where (9) and (10) follow from the Markov chain $U \to V \to X \to YZ$, and (11) follows from the more capable condition. Therefore, using a non-trivial channel prefixing yields a loss in the objective function $\mu I(V;Y) + I(V;Y|U) - I(V;Z|U)$ and $V = X$ is the optimal selection.

Now, assume that $p(y|x)$ is not more capable than $p(z|x)$ and $f(P_x)$ is maximized at an interior point of Δ_m. That is, one of possibly many PMFs P_x^* that satisfies $f(P_x^*) \geq f(P_x)$, $\forall P_x \in \Delta_m$, has all non-zero entries. We use that P_x^* in the proof. Moreover, as more capable condition does not hold, $f(\hat{P}_x) < 0$ for some input distribution $\hat{P}_x$. We will use $\hat{P}_x$ and P_x^* to construct a non-trivial channel prefixing V such that $V \to X \to (Y,Z)$ and

$$f(P_x^*) < I(V;Y) - I(V;Z) \qquad (12)$$

and this way we will show the existence of a non-trivial channel prefixing that provides a higher secrecy capacity compared to not using channel prefixing. Applying Lemma 1 to the distributions $\hat{P}_x$ and P_x^*, there exists a PMF $\boldsymbol{q} \in \Delta_m$, with $q_1 > 0$ such that

$$P_x^* = q_1 \hat{P}_x + \sum_{k=1}^{m-1} q_{k+1} \mathbf{e}_{j_k} \qquad (13)$$

for some index sets $J \subset \{1,\ldots,m\}$ with $|J| = m-1$, and $j_k \in J$. We construct V with $|V| = m$:

$$p_V(v_k) = q_k, \quad k = 1,\ldots,m \qquad (14)$$

In addition, we select $p_{X|V}(x|v_1) = \hat{P}_x$, $p_{X|V}(x|v_2) = \mathbf{e}_{j_1}$, $\ldots$, $p_{X|V}(x|v_m) = \mathbf{e}_{j_{m-1}}$. Evaluating $p_X = \sum_{k=1}^m p_V(v_k) p_{X|V}(x|v_k)$, we observe that, by (13), the constructed p_X and the maximizer P_x^* are the same. However, $I(X;Y|V) - I(X;Z|V) < 0$ because given $V = v_1$,

$$I(X;Y|V=v_1) - I(X;Z|V=v_1) = f(P_x^*) < 0$$

while $I(X;Y|V=v_k) - I(X;Z|V=v_k) = 0$ for all other $V = v_k$. As $q_1 > 0$, we have

$$I(X;Y|V) - I(X;Z|V) < 0 \qquad (15)$$

Using (15) in (10) we obtain (12), the desired result. ■

We next consider less noisy channels. Less noisy condition is a stronger partial ordering than more capable condition.

Definition 2 ([2]) *$p(y|x)$ is less noisy than $p(z|x)$ if for all $U \to X \to Y$, $I(U;Y) \geq I(U;Z)$.*

A wiretap channel is less noisy if the main channel is less noisy than the eavesdropping channel.

If a wiretap channel is less noisy (regions ① and ② in Fig. 2), neither rate splitting nor channel prefixing is necessary for the entire rate-equivocation region [2]. We showed in Theorem 2 that, if the channel is more capable, then channel prefixing is not necessary. We note here, as a converse statement, that if the channel is more capable but not less noisy (region ③ in Fig. 2), then rate splitting is strictly necessary. From Theorem 2, in this region, $V = X$. Also, as the channel is not less noisy, there exists a $U \neq \phi$ such that $I(U;Y) < I(U;Z)$. For that selection of U, we have

$$\begin{aligned}
&\mu I(X;Y) + I(X;Y|U) - I(X;Z|U) \\
&\quad = (\mu+1)I(X;Y) - I(X;Z) - [I(U;Y) - I(U;Z)] \qquad (16) \\
&\quad > (\mu+1)I(X;Y) - I(X;Z) \qquad (17)
\end{aligned}$$

proving that $U \neq \phi$ is strictly necessary.

IV. Implications of Cyclic Shift Symmetry

In this section, we focus on a specific class of channels, namely cyclic shift symmetric channels.

Definition 3 ([5]) *$p(y|x)$ is cyclic shift symmetric if $I(X;Y)$ is invariant under cyclic shifts of the input distribution.*

Cyclic shift symmetric channels are an important class that includes binary symmetric, binary erasure, and type-writer channels[3]. A key property of cyclic shift symmetric channels is that the input distribution that maximizes the mutual information is the uniform distribution [5, Theorem 2]. A wiretap channel is cyclic shift symmetric if both the main channel and the eavesdropping channel are cyclic shift symmetric.

Theorem 3 *In a more capable cyclic shift symmetric wiretap channel, the rate-equivocation pair (C_B, C_s) is achievable.*

Proof: First, we select $V = X$ due to Theorem 2. Next, we note that there exists at least one input distribution, denoted by P_x^*, that maximizes $f(P_x)$, since it is a bounded continuous functional of P_x and the probability simplex Δ_m is compact. Let $\mathbf{u}$ denote the uniform distribution over the alphabet $\mathcal{X}$.

We let $P_x^* \neq \mathbf{u}$ without loss of generality, as otherwise, $U = \phi$ is optimal. There exist $m-1$ other input distributions (cyclic shifts of P_x^*) that achieve the maximum $f(P_x)$. Define

[3]A similar notion of channel symmetry is studied in [6], which is referred to as circular symmetry. We note that circular symmetric channels as defined in [6] are cyclic shift symmetric in our context but not vice versa in general. We thank an anonymous reviewer for informing us about the paper [6].

the auxiliary U, with $\mathcal{U} = \{u_1, \ldots, u_m\}$, with marginal distribution $p_U(u_i) = \frac{1}{m}$, and transition probabilities $p_{X|U}(x|u_1) = P_x^*$, $p_{X|U}(x|u_2) = P_x^*(1)$, …, and $p_{X|U}(x|u_m) = P_x^*(m-1)$, where $P_x^*(i)$ denotes i times cyclic shifted version of P_x^*.

Evaluating (5) with the specified choice of U, and with $V = X$, we have $I(V;Y) = C_B$, since $P_x = \sum_{u\in\mathcal{U}} p_U(u)p_{X|U}(x|u) = \frac{1}{m}\sum_{i=1}^{m} P_x^*(i) = \mathbf{u}$, and Bob's channel is cyclic shift symmetric. On the other hand, evaluating (4) for this specific choice, we get $I(X;Y|U) - I(X;Z|U) = C_s$, since for any $u \in \mathcal{U}$, $I(X;Y|U = u) - I(X;Z|U = u) = \max_{P_x} f(P_x) = C_s$. This proves that (C_B, C_s) pair is achievable. ■

The class of wiretap channels considered in Theorem 3 has already been covered in [7] in the following example.

$$p(y|x) = \frac{1}{2}\begin{pmatrix} 1-p & p & 1-q & q \\ p & 1-p & q & 1-q \\ 1-q & q & 1-p & p \\ q & 1-q & p & 1-p \end{pmatrix}$$

$$p(z|x) = \frac{1}{2}\begin{pmatrix} 1-r & 1-r & r & r \\ 1-r & 1-r & r & r \\ r & r & 1-r & 1-r \\ r & r & 1-r & 1-r \end{pmatrix}$$

In [7], it is shown that, for r close enough to $1/2$ (depending on the values of p and q), the wiretap channel is more capable. However, the channel is shown to be not less noisy for any r, p and q. We now observe that $p(y|x)$ and $p(z|x)$ are cyclic shift symmetric channels. Therefore, by Theorem 3, (C_B, C_s) pair is achievable by a non-trivial U and $V = X$ when r, p and q are such that the wiretap channel is more capable.

Next, we consider a sub-class of cyclic shift symmetric channels, where the channels are such that, $f(P_x)$ is maximized at the uniform distribution. We show that, for these channels, rate splitting is unnecessary, and the entire rate-equivocation region can be attained by channel prefixing alone.

Theorem 4 *In a cyclic shift symmetric wiretap channel, if in addition, $f(P_x)$ is maximized at the uniform input distribution, then rate splitting does not improve the rate-equivocation region. In particular,*

$$C_s = \max_{P_x} f(P_x) - \min_{P_x} f(P_x) \tag{18}$$

Proof: Let $R_e^* = \max_{P_x} f(P_x)$. First, we obtain an upper bound for the objective function in (7):

$$\begin{aligned}
&\mu I(V;Y) + [I(V;Y|U) - I(V;Z|U)] \\
=&\mu I(V;Y) + [I(X;Y|U) - I(X;Z|U)] \\
&- [I(X;Y|V,U) - I(X;Z|V,U)] && (19)\\
\le&\mu I(V;Y) + R_e^* - [I(X;Y|V) - I(X;Z|V)] && (20)\\
=&R_e^* + \mu I(X;Y) - [(\mu+1)I(X;Y|V) - I(X;Z|V)] && (21)\\
\le&R_e^* + \mu C_B - \min_{P_x}[(\mu+1)I(X;Y) - I(X;Z)] && (22)
\end{aligned}$$

where (20) follows from $I(X;Y|U) - I(X;Z|U) \le R_e^*$ and the Markov chain $U \to V \to X \to YZ$, (21) follows from the same Markov chain, and (22) is obtained by replacing $I(X;Y)$ with its maximum possible value and $[(\mu+1)I(X;Y|V) - I(X;Z|V)]$ with its minimum possible value.

Now, we will show that the upper bound in (22) is achieved with no rate splitting. By the hypothesis, $\mathbf{u} = \arg\max_{P_x} I(X;Y) = \arg\max_{P_x} f(P_x)$. Thus, $R_e^* + \mu C_B = \max_{P_x}(\mu+1)I(X;Y) - I(X;Z)$. Moreover, let $P^* = \arg\min_{P_x}[(\mu+1)I(X;Y) - I(X;Z)]$. By cyclic shift symmetry [5], there exist $m-1$ other input distributions that optimize the objective $(\mu+1)I(X;Y) - I(X;Z)$, which are cyclic shifts of P^*, denoted by $P^*(i)$ for $i = 1, \ldots, m-1$. Therefore, we define the channel prefixing V with $|V| = m$ as $p(v_1) = \ldots = p(v_m) = 1/m$ with transition probabilities $p(x|v_1) = P^*$, $p(x|v_2) = P^*(1)$, …, and $p(x|v_m) = P^*(m-1)$. Then, the input distribution is $P_x = \sum_{i=1}^{m} p(v_i)p(x|v_i) = \mathbf{u}$. For this selection of V, we have

$$\begin{aligned}
&\mu I(V;Y) + [I(V;Y) - I(V;Z)] \\
=&\mu I(X;Y) + [I(X;Y) - I(X;Z)] \\
&- [(\mu+1)I(X;Y|V) - I(X;Z|V)] && (23)\\
=&\mu C_B + R_e^* \\
&- \sum_{i=1}^{m} p(v_i)[(\mu+1)I(X;Y|V=v_i) - I(X;Z|V=v_i)] \\
=&\mu C_B + R_e^* - \min_{P_x}[(\mu+1)I(X;Y) - I(X;Z)] && (24)
\end{aligned}$$

Note that (24) is equivalent to the upper bound in (22). Therefore, for any $\mu > 0$, the boundary of the rate-equivocation region can be achieved without rate splitting. In particular, setting $\mu = 0$, (24) yields the secrecy capacity in (18). ■

We remark here that the secrecy capacity achieved in Theorem 4 is generally an upper bound for a wiretap channel:

$$\begin{aligned}
C_s &= \max\ I(V;Y) - I(V;Z) \\
&= \max\ [I(X;Y) - I(X;Z)] - [I(X;Y|V) - I(X;Z|V)] \\
&\le \max_{P_x} f(P_x) - \min_{P_x} f(P_x) && (25)
\end{aligned}$$

Another remark is that the class of channels in Theorem 4 can reside in region ①, ② or ④ in Fig. 2. However, they cannot reside in region ③, i.e., the shaded region, as a direct corollary of Theorem 4, Theorem 2, and the discussion following it.

Corollary 1 *In a more capable cyclic shift symmetric wiretap channel, $f(P_x)$ is maximized at uniform input distribution, if and only if the channel is further less noisy.*

V. The BSC-BEC Wiretap Channel

Let the main channel be BSC(ϵ) and the eavesdropper's channel be BEC(α). $\mathcal{X} = \mathcal{Y} = \{0,1\}$ and $\mathcal{Z} = \{0, e, 1\}$. For $0 \le \epsilon < 0.5$ and the input distribution $P_x = [p_x, 1-p_x]$,

$$f(P_x) = h((2\epsilon-1)p_x + 1 - \epsilon) - (1-\alpha)h(p_x) - h(\epsilon) \tag{26}$$

where $h(.)$ is the binary entropy function. We first investigate some geometric properties of the function $f(P_x)$ in (26) in

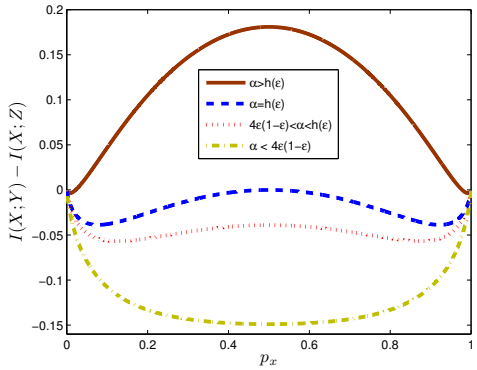

Fig. 3. $f(P_x)$ as a function of p_x for the BSC-BEC channel.

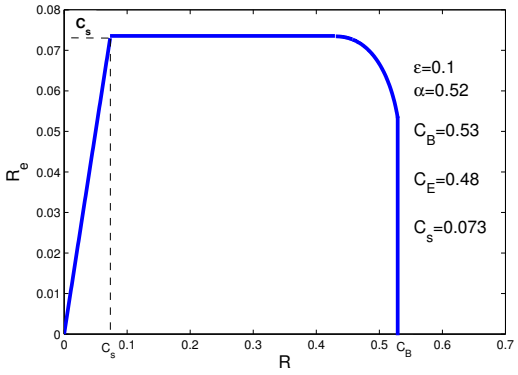

Fig. 4. Rate-equivocation region of BSC(0.1)-BEC(0.52) wiretap channel.

the following proposition, which are also observed in [6].

Proposition 1 ([6]) *Let $p(y|x)$ be BSC(ϵ) and $p(z|x)$ be BEC(α).*

1) *If $\alpha < 4\epsilon(1-\epsilon)$, then $f(P_x) \leq 0$, and it is convex.*
2) *If $4\epsilon(1-\epsilon) \leq \alpha \leq h(\epsilon)$, $f(P_x) \leq 0$ but not convex.*
3) *If $h(\epsilon) < \alpha$, $f(P_x)$ takes negative and positive values, it is not convex, and it is maximized at $P_x = [0.5, 0.5]$.*

An illustration of the proposition is provided in Fig. 3 for $\epsilon = 0.1$ and various α. Note that for any ϵ and α, $f(P_x) < 0$ for some P_x; thus, the channel is not more capable and is always in region ④ in Fig. 2. We observe that for $\alpha > h(\epsilon)$, $f(P_x)$ is maximized at $p_x = 0.5$. Being also a cyclic shift symmetric channel, from Theorem 4, rate splitting is not necessary in this case. We also note that for $\alpha < 4\epsilon(1-\epsilon)$, $f(P_x)$ is convex and always negative. In this case, using [7, Theorem 2], Eve is less noisy than Bob, and the secrecy capacity is zero [2].

Corollary 2 *In the BSC-BEC wiretap channel, if $h(\epsilon) \leq \alpha$ then rate splitting does not improve the rate-equivocation region, and*

$$C_s = \max_{P_x} f(P_x) - \min_{P_x} f(P_x) \tag{27}$$

If $\alpha < 4\epsilon(1-\epsilon)$, then $C_s = 0$

If $h(\epsilon) \leq \alpha$, we can find the required channel prefixing as in the proof of Theorem 4 and thoroughly characterize the rate-equivocation region. We have $|V| = 2$ with $p(v_1) = p(v_2) = 1/2$ and $p(x|v_1) = [a, 1-a]$, $p(x|v_2) = [1-a, a]$ where $[a, 1-a]$ is an input distribution that maximizes $[(\mu+1)I(X;Y) - I(X;Z)]$. By spanning $\mu \geq 0$, we obtain the rate-equivocation region. We illustrate this in Figure 4.

VI. The BEC-BSC Wiretap Channel

Now, let the main channel be BEC(α) and the eavesdropper's channel be BSC(ϵ). $\mathcal{X} = \mathcal{Z} = \{0, 1\}$ and $\mathcal{Y} = \{0, e, 1\}$.

Proposition 2 ([6]) *Let $p(y|x)$ be BEC(α) and $p(z|x)$ be BSC(ϵ).*

1) *If $\alpha < 4\epsilon(1-\epsilon)$, $f(P_x)$ is concave in P_x.*
2) *If $4\epsilon(1-\epsilon) \leq \alpha \leq h(\epsilon)$, $f(P_x) \geq 0$, and it is not maximized at $P_x = [0.5, 0.5]$.*
3) *If $h(\epsilon) < \alpha$, then $f(P_x)$ takes both positive and negative values, and it is minimized at $P_x = [0.5, 0.5]$.*

From Proposition 2, if $4\epsilon(1-\epsilon) \leq \alpha \leq h(\epsilon)$, the wiretap channel is in the shaded region in Fig 2. By [2], $C_s = \max_{P_x} f(P_x)$, and from Theorem 3, (C_B, C_s) is achievable. If $\alpha < 4\epsilon(1-\epsilon)$, as both channels have their capacity achieving input distributions as uniform, by [7, Theorem 3], $C_s = C_B - C_E$ and (C_B, C_s) is achievable.

Corollary 3 *For $\alpha < 4\epsilon(1-\epsilon)$, secrecy capacity is $C_s = C_B - C_E$ and (C_B, C_s) is achievable. If $4\epsilon(1-\epsilon) < \alpha < h(\epsilon)$, $C_s = \max_{P_x} f(P_x)$, and (C_B, C_s) is achievable.*

VII. Conclusions

In this paper, we provided new results on the roles of rate splitting and channel prefixing in evaluating the rate-equivocation regions of wiretap channels. We proved that if the channel is more capable, then channel prefixing is unnecessary. We also proved that in more capable cyclic shift symmetric channels (C_B, C_s) is achieveable. We next proved that for cyclic shift symmetric channels if $I(X;Y) - I(X;Z)$ is maximized at the uniform input distribution, then rate splitting is unnecessary. Finally, we applied our results to the BSC-BEC and BEC-BSC wiretap channels.

References

[1] A. Wyner, "The wire-tap channel," *Bell Sys. Tech. Journal*, vol. 54, no. 8, pp. 1355–1387, October 1975.

[2] I. Csizár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. on Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: from weak to strong secrecy for free," in *EUROCRYPT*, 2000.

[4] M. van Berg, O. Cheong, M. van Kreveld, and M. Overmars, *Computational Geometry: Algorithms and Applications*. Springer Verlag, 2008.

[5] B. Xie and R. Wesel, "A mutual information invariance approach to symmetry in discrete memoryless channels," in *UCSD ITA*, Feb. 2008.

[6] C. Nair, "Capacity regions of two new classes of two-receiver broadcast channels," *IEEE Trans. on Inform. Theory*, vol. 56, no. 9, pp. 4207–4214, September 2010.

[7] M. van Dijk, "On a special class of broadcast channels with confidential messages," *IEEE Trans. on Inform. Theory*, vol. 43, no. 2, pp. 712–714, March 1997.