Wiretap Channels: Implications of the More Capable Condition and Cyclic Shift Symmetry

Omur Ozel, *Student Member, IEEE*, and Sennur Ulukus, *Member, IEEE*

***Abstract*—Characterization of the rate-equivocation region of a general wiretap channel involves two auxiliary random variables: U, for rate splitting and V, for channel prefixing. In this paper, we explore specific classes of wiretap channels for which the evaluation of the rate-equivocation region is simpler. We show that if the wiretap channel is more capable, $V = X$ is optimal and the boundary of the rate-equivocation region is achieved by varying rate splitting U alone. Conversely, we show under a mild condition that if the wiretap channel is not more capable, then $V = X$ is strictly suboptimal. Next, we focus on the class of cyclic shift symmetric wiretap channels. We show that optimal rate splitting U that achieves the boundary of the rate-equivocation region is uniform with cardinality $|\mathcal{X}|$ and the prefix channel between optimal U and V is expressed as cyclic shifts of the solution of an auxiliary optimization problem over a single variable. We provide a special class of cyclic shift symmetric wiretap channels for which $U = \phi$ is optimal. We apply our results to the binary-input cyclic shift symmetric wiretap channels and thoroughly characterize the rate-equivocation regions of the BSC-BEC and BEC-BSC wiretap channels.**

***Index Terms*—Channel prefixing, rate-equivocation region, rate splitting, wiretap channel.**

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 the auxiliary random variables are either not needed or their optimal selection is simplified. 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, Th. 3]. 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].

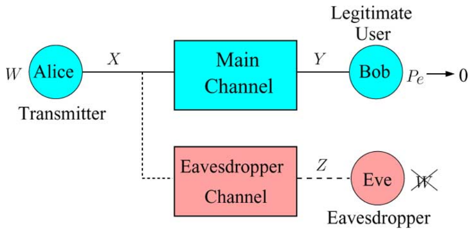

Fig. 1. Wiretap channel.

In this paper, we explore specific classes of wiretap channels for which calculation of the optimal rate splitting and/or channel prefixing parameters is simpler. 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; that is, the 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.

Next, we study the class of cyclic shift symmetric wiretap channels. We show that the optimal rate splitting U that achieves the boundary of the rate-equivocation region is uniform with cardinality $|X|$ and the prefix channel between optimal U and V is expressed as cyclic shifts of the solution of an auxiliary optimization problem over a single variable. This is a considerable reduction in the computation requirement for the calculation of (the boundary of) the rate-equivocation region. We provide the cardinality bound on this single auxiliary random variable appearing in the optimization problem. Then, we formulate the problem as a constrained optimization problem. We provide a sufficient condition under which rate splitting is unnecessary, i.e., $U = \phi$ is optimal and the boundary of the rate-equivocation region is obtained by varying V alone. In particular, we show that if $I(X;Y) - I(X;Z)$ is maximized at the uniform distribution, i.e., if the channel is dominantly cyclic

Manuscript received October 18, 2011; revised August 24, 2012; accepted October 02, 2012. Date of publication December 03, 2012; date of current version March 13, 2013.This work was supported by NSF Grants CCF 07-29127, CNS 09-64632, CCF 09-64645, and CCF 10-18185. This paper was presented in part at the 2011 IEEE International Symposium on Information Theory and in part at the Allerton Conference on Communication, Control, and Computing, Monticello, IL, September 2011.

The authors are with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mail: omur@umd.edu; ulukus@umd.edu).

Communicated by T. Uyematsu, Associate Editor for Shannon Theory.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2012.2231463

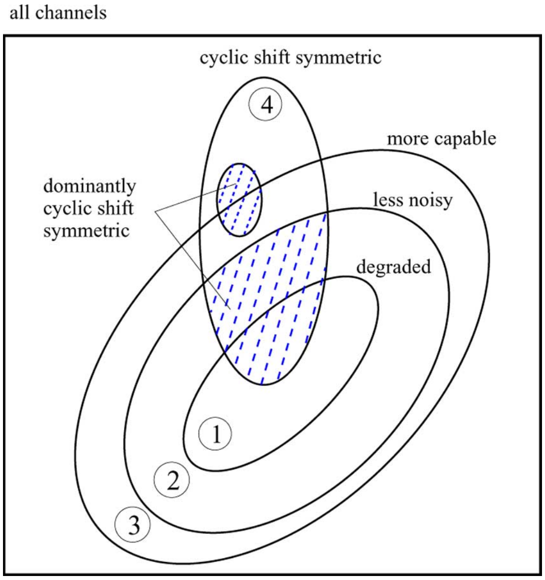

Fig. 2. Inclusion relations among the classes of wiretap channels.

shift symmetric, then this sufficient condition is satisfied, and hence, rate splitting is unnecessary. Moreover, we show that if the main channel is more capable and both channels are cyclic shift symmetric, then (C_B, C_s) rate-equivocation pair is achievable. We also discuss an extension of the notion of cyclic shift symmetry for continuous alphabets. Finally, we apply our results to the binary-input cyclic shift symmetric wiretap channels. We investigate two examples that illustrate the considered cases: BSC-BEC and BEC-BSC wiretap channels. We provide full characterizations for the rate-equivocation regions of the BSC-BEC and BEC-BSC wiretap channels. In particular, we find that rate splitting is never necessary for the BSC-BEC wiretap channel. We also provide a class of wiretap channels that are dominantly cyclic shift symmetric, more capable and not less noisy, for which $U = \phi$ and $V = X$ is optimal.

II. Model and Background

As in Fig. 1, Alice communicates with Bob in the presence of an eavesdropper, Eve. The input and output alphabets, $\mathcal{X}$, $\mathcal{Y}$, 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 $\psi : \mathcal{Y}^n \to \mathcal{W}$. The probability of error is: $P_e = \Pr[\psi(Y^n) \neq W]$. 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 the *secrecy capacity* C_s is the highest achievable perfectly secure rate R. The maximum possible equivocation is also C_s.

The input distribution P_x belongs to the $|\mathcal{X}|$ dimensional probability simplex denoted as

$$\Delta = \left\{ (p_1, \ldots, p_{|\mathcal{X}|}) \left| \sum_{i=1}^{|\mathcal{X}|} p_i = 1, \quad p_i \geq 0, \quad \forall i \right. \right\}. \tag{2}$$

Throughout the paper, $f_\mu(.)$ denotes the following function of the input distribution P_x:

$$f_\mu(P_x) = (\mu+1) I(X;Y) - I(X;Z) \tag{3}$$

where $\mu \geq 0$ is an arbitrary parameter. We denote $f_0(.)$ simply as $f(.)$. Note that $f_\mu(.)$ is continuous and differentiable in P_x for all $\mu \geq 0$.

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 if and only if there exist $U \to V \to X \to Y, Z$ 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

$$C_s = \max_{V \to X \to Y,Z} I(V;Y) - I(V;Z). \tag{6}$$

Finally, the cardinality bounds on the alphabets of the auxiliary random variables are[2]

$$|\mathcal{U}| \leq |\mathcal{X}| + 2 \tag{7}$$
$$|\mathcal{V}| \leq |\mathcal{X}|^2 + 3|\mathcal{X}| + 2. \tag{8}$$

The rate-equivocation region of a wiretap channel is a convex region. Therefore, the upper right boundary is traced by solving the following optimization problem for all $\mu \geq 0$, as in Fig. 3:

$$\max_{U,V,X} \quad \mu I(V;Y) + I(V;Y|U) - I(V;Z|U). \tag{9}$$

Note that this optimization problem is computable due to the bounds on the sizes of U and V in (7) and (8) in Theorem 1. In the sequel, we refer to the solution of the optimization problem in (9) as the optimal selections U^*, V^*, and X^*. These optimal selections depend implicitly on the value of μ. The optimal value of the objective function in (9) at $\mu = 0$ is the secrecy capacity C_s. In this case, U is unnecessary, and in fact, we get (6) [2]. Note that the bounds on the cardinalities of U and V in (7) and (8) in Theorem 1 are valid in general. However, the specific cardinality bound on V for (9) when $\mu = 0$, or equivalently (6), is

$$|\mathcal{V}| \leq |\mathcal{X}|. \tag{10}$$

To see (10), we first note the following:

$$\begin{aligned} I(V;Y) - I(V;Z) =& I(X;Y) - I(X;Z) \\ & - [I(X;Y|V) - I(X;Z|V)]. \end{aligned} \tag{11}$$

[1] We use the weak secrecy notion. However, for discrete wiretap channels, weak and strong secrecy are equivalent [3], [4].

[2] These bounds are originally given in [2] for the general problem with common messages as $|\mathcal{U}| \leq |\mathcal{X}| + 3$ and $|\mathcal{V}| \leq |\mathcal{X}|^2 + 4|\mathcal{X}| + 3$. In this paper, we do not consider common message.

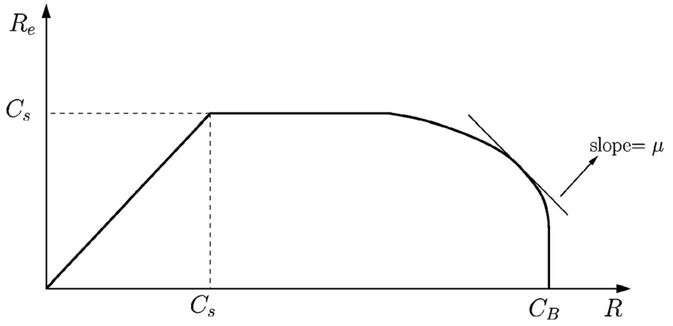

Fig. 3. Characterization of the upper right boundary of the rate-equivocation region.

In view of (11), we use the standard argument that follows from [5, Lemma 3] and the strengthened Caretheodory theorem of Fenchel–Eggleston in [6], where $|\mathcal{X}|$ real continuous functions of $p(x|v)$ (defined from Δ to real numbers) necessary in this argument are $p(j|v), j = 1, \ldots, |\mathcal{X}| - 1$ and $I(X;Y|V = v) - I(X;Z|V = v)$. Therefore, $|\mathcal{V}| \leq |\mathcal{X}|$ cardinality is sufficient to solve the optimization problem in (6); see also Appendix C in [7] and [8] for a rigorous justification of this bound.

III. More Capable Wiretap 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 $P_x \in \Delta$.

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

In [2, Th. 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 achieving the entire boundary of the rate-equivocation region. Conversely, we will prove, under a mild condition, that if the wiretap channel is not more capable, then $V = X$ is strictly suboptimal, i.e., there exists $V \neq X$ that improves the rate-equivocation region compared to $V = X$.

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 $\mathbf{e}_j$, $j = 1, \ldots, |\mathcal{X}|$, form the canonical basis for the $|\mathcal{X}|$ dimensional Euclidean space, and in particular, Δ is the convex hull of $\mathbf{e}_j$, $j = 1, \ldots, |\mathcal{X}|$. An important topological property of Δ is stated in the next lemma, namely a point in the simplex Δ partitions the simplex into $|\mathcal{X}|$ subsimplexes in a specific way.

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

$$\mathbf{p}' = q_1 \mathbf{p} + \sum_{i=1}^{|\mathcal{X}|-1} q_{i+1} \mathbf{e}_{j_i} \tag{12}$$

where $j_i \in J$ for $i = 1, \ldots, |\mathcal{X}| - 1$. In particular, $q_1 > 0$ if $\mathbf{p}'$ is an interior point of Δ.

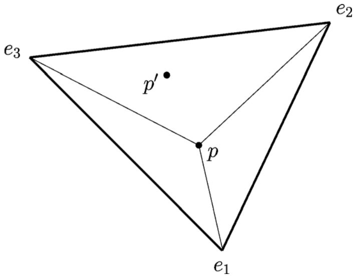

Fig. 4. Partitioning the probability simplex Δ.

Proof: The probability simplex Δ has corner points $\mathbf{e}_j$, $j = 1, \ldots, |\mathcal{X}|$. Given $\mathbf{p} \in \Delta$, we can find a triangulation [9] $\{\mathcal{D}_i\}_{i=1}^{|\mathcal{X}|}$ of $\{\mathbf{e}_1, \ldots, \mathbf{e}_{|\mathcal{X}|}, \mathbf{p}\}$ by combining $|\mathcal{X}| - 1$ of the corner points and $\mathbf{p}$. Then, we get $\Delta = \bigcup_{i=1}^{|\mathcal{X}|} \mathcal{D}_i$, where $\mathcal{D}_i$ is the convex hull of $\left[\{\mathbf{e}_1, \ldots, \mathbf{e}_{|\mathcal{X}|}\} \setminus \{\mathbf{e}_i\}\right] \cup \{\mathbf{p}\}$, $i = 1, \ldots, |\mathcal{X}|$. If $\mathbf{p}$ has a zero entry, then some $\mathcal{D}_i$ has smaller dimensionality; however, this does not violate the generality. Hence, a given PMF $\mathbf{p}'$ resides inside one of $\mathcal{D}_i$. Moreover, if $\mathbf{p}'$ has all nonzero entries, then it is not in the convex hull of any proper subset of $\mathbf{e}_j$, $j = 1, \ldots, |\mathcal{X}|$. Hence, $q_1 > 0$ in this case. ■

Lemma 1 says that a point in Δ partitions it into $|\mathcal{X}|$ subsimplexes which are convex hulls of $|\mathcal{X}| - 1$ of the vertices $\mathbf{e}_j$ and the point itself. We illustrate this partitioning for $|\mathcal{X}| = 3$ in Fig. 4. As a consequence, any PMF can be expressed as a convex combination of any other PMF and $|\mathcal{X}| - 1$ of the $|\mathcal{X}|$ canonical PMFs $\mathbf{e}_j$. In fact, this partition and hence the representation in (12) is unique. Only the existence of such a representation is sufficient for our arguments in this paper. In particular, we use this existence result to prove the main theorem of this section which is stated next. The proof of this theorem is provided in Appendix A.

Theorem 2: If the wiretap channel is more capable, $V^* = X$ is optimal for the entire boundary of the rate-equivocation region and the cardinality bound on U^* is $|\mathcal{U}^*| \leq |\mathcal{X}|$. Conversely, if the wiretap channel is not more capable, $V = X$ is strictly suboptimal provided that $f(P_x)$ is maximized at an interior point of Δ.

As a result, if the wiretap channel is more capable, channel prefixing is not necessary, and hence, the computation of the rate-equivocation region is considerably simplified. Moreover, the bound on the necessary rate splitting reduces by 2 compared to Csiszár and Körner's bound (from $|\mathcal{X}| + 2$ to $|\mathcal{X}|$). Another remark is that the direct part in Theorem 2 immediately extends for continuous alphabet wiretap channels, i.e., if a continuous alphabet wiretap channel is more capable, then rate splitting is unnecessary and optimal $V^* = X$. However, the converse part does not immediately extend as the proof presented for finite cardinality input alphabets does not directly extend to infinite-dimensional spaces of probability density functions.

We next review less noisy channels for future reference. 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 $I(U;Y) \geq I(U;Z)$ for all $U \to X \to Y, Z$.

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 ①and ②in Fig. 2), neither rate splitting nor channel prefixing is necessary for the entire rate-equivocation region [2, Th. 3].

IV. Cyclic Shift Symmetric Wiretap Channels

In this section, we focus on cyclic shift symmetric channels. Let A denote the $|\mathcal{X}| \times |\mathcal{X}|$ shifter matrix where

$$A_{ij} = \begin{cases} 1, & i = 1, \ldots, |\mathcal{X}| - 1, j = i + 1 \\ 1, & i = |\mathcal{X}|, j = 1 \\ 0, & \text{otherwise.} \end{cases} \tag{13}$$

For any input PMF $\left[p_1, \ldots, p_{|\mathcal{X}|}\right]$, we call the PMF $\left[p_1, \ldots, p_{|\mathcal{X}|}\right] A^k$, the kth cyclic shift of it. Cyclic shift symmetric channels are defined in terms of cyclic shifts of the input PMF:

Definition 3 ([10]): $p(y|x)$ is cyclic shift symmetric if $I(X;Y)$ is invariant under any cyclic shift of the input PMF.

Cyclic shift symmetric channels are an important class that includes binary symmetric, binary erasure, and type-writer channels. A wiretap channel is cyclic shift symmetric if both the main channel and the eavesdropping channel are cyclic shift symmetric. Two key properties of cyclic shift symmetric channels are 1) the kth cyclic shift of the input PMF for $k = 0, \ldots, |X| - 1$ yields the same mutual information $I(X;Y)$, and 2) uniform distribution maximizes $I(X;Y)$[10, Th. 2]. We remark that our development specifically uses these two properties of cyclic shift symmetric channels and it cannot be extended to the larger class of input invariance symmetric wiretap channels [10].

In the following theorem, we determine the structure of the optimal auxiliary random variables U^* and V^* as well as the channel input X^* for cyclic shift symmetric wiretap channels. Remarkably, the optimizing rate splitting U^* and channel prefixing V^* parameters can be determined by solving an auxiliary optimization problem over only one auxiliary random variable. In addition, the cardinality bounds on U^* and V^* are reduced to $|\mathcal{X}|$ and $|\mathcal{X}|^2$, respectively, compared to the general case in (7) and (8). We provide the proof of this theorem in Appendix B.

Theorem 3: In a cyclic shift symmetric wiretap channel, an optimal selection of the auxiliary random variables U^* and V^* in (9) has the cardinalities $|\mathcal{U}^*| \leq |\mathcal{X}|$ and $|\mathcal{V}^*| \leq |\mathcal{X}|^2$, respectively, with the following structure:

$$p(U^* = u) = \frac{1}{|\mathcal{X}|}, \qquad u \in \{1, \ldots, |\mathcal{X}|\} \tag{14}$$

$$p(V^* = (u-1)|\mathcal{X}| + v | U^* = u) = p(\hat{V} = v), \quad u, v \in \{1, \ldots, |\mathcal{X}|\} \tag{15}$$

$$p(V^* = v | U^* = u) = 0, \quad u \in \{1, \ldots, |\mathcal{X}|\}, v \notin \{(u-1)|\mathcal{X}| + 1, \ldots, u|\mathcal{X}|\} \tag{16}$$

$$p(x | V^* = v + (u-1)|\mathcal{X}|) = p(x|\hat{V} = v)(u-1), \quad u, v, x \in \{1, \ldots, |\mathcal{X}|\} \tag{17}$$

where $p(X = x|\hat{V} = v)(u-1)$ denotes the $(u-1)$st cyclic shift of the distribution $p(x|\hat{V} = v)$. Moreover, the distributions $p(\hat{V} = v)$ and $p(X = x|\hat{V} = v)$ with $|\hat{\mathcal{V}}| \leq |\mathcal{X}|$ are the optimizers of the following auxiliary optimization problem:

$$\max_{\hat{V} \to X \to Y,Z} \Bigg(I(X;Y) - I(X;Z) - \Big[(\mu+1) I(X;Y|\hat{V}) - I(X;Z|\hat{V})\Big] \Bigg)^+ \tag{18}$$

where $(x)^+ = \max\{0, x\}$.

We illustrate the specific structure of the optimal auxiliary random variables and the channel input in Fig. 5. In particular, each element of U^* generates the optimizing PMF $p(\hat{V})$ over $|\mathcal{X}|$ elements of V^*. The first $|\mathcal{X}|$ elements of V^* generate the optimizing conditional PMF $p(X|\hat{V} = v)$ over X. The remaining elements of V^* generate cyclic shifts of $p(X|\hat{V} = v)$ over X. An equivalent representation for the optimal selections can be obtained by letting $V^* = (V_1^*, V_2^*)$ with $|\mathcal{V}_1^*| = |\mathcal{V}_2^*| = |\mathcal{X}|$:

$$p(U^* = u) = \frac{1}{|\mathcal{X}|}, \quad u \in \{1, \ldots, |\mathcal{X}|\} \tag{19}$$

$$p(V^* = (v_1, v_2) | U^* = u) = p(\hat{V} = v_1) \delta(v_2 - u) \quad u, v_1, v_2 \in \{1, \ldots, |\mathcal{X}|\} \tag{20}$$

$$p(x | V^* = (v_1, v_2)) = p(x | \hat{V} = v_1)(v_2 - 1) \quad v_1, v_2 \in \{1, \ldots, |\mathcal{X}|\}. \tag{21}$$

Note that U^* is a deterministic function of V^*, as stated in [2, Th. 1]. This is verified easily from the equivalent representation in (19)–(21). Given $V^* = (V_1^* = v_1, V_2^* = v_2)$, $U^* = v_2$ with probability 1. However, V^* is a stochastic function of U^*. These can also be verified from Fig. 5.

The optimization problem in (18) is a constrained optimization problem over $|\mathcal{X}|^2 - 1$ variables: $|\mathcal{X}|$ probability distributions on X, $p(X = x|\hat{V} = v_i)$. Each probability distribution accounts for $|\mathcal{X}| - 1$ variables for $i = 1, \ldots, |\mathcal{X}|$. In addition, the distribution for $\hat{V}$ accounts for $|\mathcal{X}| - 1$ variables. Let us define $\lambda_i \overset{\triangle}{=} p(V = v_i)$ and $\left[p_1^{(i)} p_2^{(i)} \ldots p_{|\mathcal{X}|}^{(i)}\right] \overset{\triangle}{=} p(X = x|V = v_i)$. We have $\lambda_i \geq 0, p_j^{(i)} \geq 0$ and $\sum_i \lambda_i = 1, \sum_j p_j^{(i)} = 1$. The following is a restatement of the constrained optimization problem in (18):

$$\begin{aligned} \max_{\{\lambda_i\},\{p_j^{(i)}\}} \quad & f\left(\sum_i \lambda_i p_j^{(i)}\right) - \sum_i \lambda_i f_\mu(p_j^{(i)}) \\ \text{s.t.} \quad & \sum_i \lambda_i = 1, \ \sum_j p_j^{(i)} = 1 \\ & \lambda_i \geq 0, \ p_j^{(i)} \geq 0. \end{aligned} \tag{22}$$

Note that the cyclic shift symmetry assumption on Bob's and Eve's channels brings a significant reduction in the cardinalities of the auxiliary random variables. In particular, the bound on the rate splitting variable reduces from $|\mathcal{X}| + 2$ to $|\mathcal{X}|$ and the bound on the channel prefixing variable reduces from $|\mathcal{X}|^2 + 3|\mathcal{X}| + 2$ to $|\mathcal{X}|^2$. The problem in (18) for $\mu = 0$ is equivalent to finding the secrecy capacity C_s. Thus, in cyclic shift symmetric wiretap channels, solving a problem of the same number of variables as finding the secrecy capacity is sufficient to characterize the

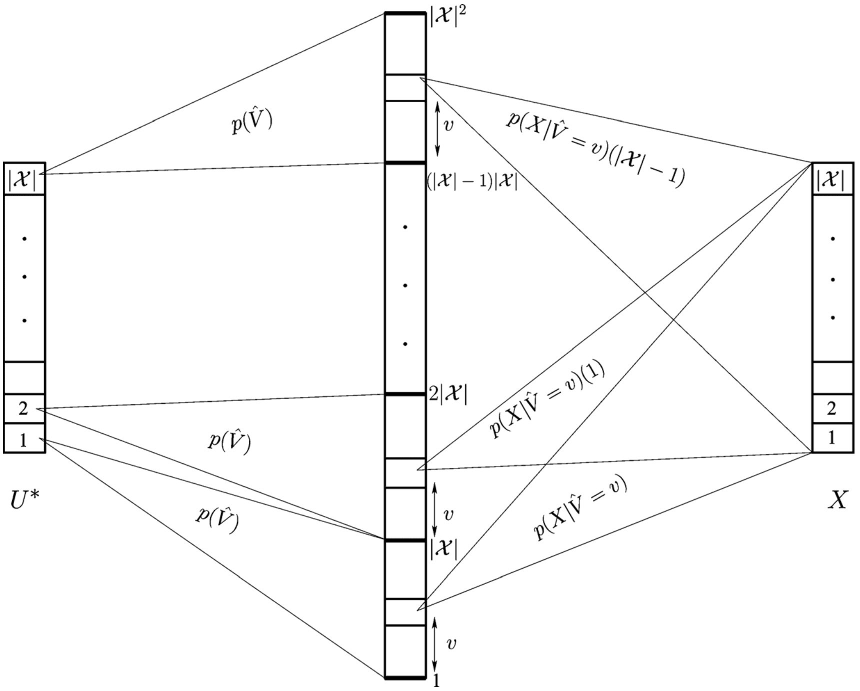

Fig. 5. Structure of the optimal $U^* \rightarrow V^* \rightarrow X$ for cyclic shift symmetric wiretap channels. $p(\hat{V})$ and $p(X|\hat{V}=v)$, $v \in \{1,\ldots,|\mathcal{X}|\}$ are the solutions of the auxiliary optimization problem in (18).

optimal selections of U and V for any point on the boundary of the rate-equivocation region.

The structure of the optimal auxiliary selections U^* and V^* for cyclic shift symmetric wiretap channels in Theorem 3 indicates a sufficient condition for $U=\phi$ to be an optimal selection: If the optimizing $p(\hat{V}=v_k)$ and $p(X=x|\hat{V}=v_k)$, $k=1,\ldots,|\mathcal{X}|$ in (18) are such that

$$p(\hat{V}=v_k)=\frac{1}{|\mathcal{X}|},$$
$$p(X=x|\hat{V}=v_k)=p(X=x|\hat{V}=v_1)(k-1), \quad \forall k \quad (23)$$

then rate splitting is not necessary. In this case, as $\hat{V}$ has cardinality $|\mathcal{X}|$, each element of $\hat{V}$ generates a cyclic shift of $p(X|\hat{V}=v_1)$, and a uniform distribution is generated over X. Therefore, the uniform $\hat{V}$ together with the cyclic prefix channel $\hat{V} \rightarrow X$ in (23) maximizes $I(X;Y)$, and hence, the objective function in (9) (cf., the proof of Theorem 3 in Appendix B). In other words, if (23) is satisfied, then U^* and V^* as selected in (14)–(17) yield a uniform PMF for $p(X|U^*=u)$ for all $u \in \{1,\ldots,|\mathcal{X}|\}$, i.e., U^* is independent of X. Therefore, if (23) is satisfied, $U=\phi$ can be selected without losing optimality, i.e., U is not necessary.

Next, we consider a subclass of cyclic shift symmetric channels, namely dominantly cyclic shift symmetric channels (cf., [11, Definition 5]).

Definition 4: A cyclic shift symmetric wiretap channel is dominantly cyclic shift symmetric if $f(\mathbf{u}) \geq f(P_x)$, $\forall P_x \in \Delta$, where $\mathbf{u}$ is the $|\mathcal{X}|$-dimensional uniform distribution.

Note that from [12, Th. 3] and the fact that the uniform distribution is capacity achieving for cyclic shift symmetric channels, a less noisy cyclic shift symmetric wiretap channel is also dominantly cyclic shift symmetric (see also [13]). We denote dominantly cyclic shift symmetric channels by the shaded region in Fig. 2. Note that all cyclic shift symmetric channels in regions ①and ②are shaded. In the following lemma, we prove the sufficiency of dominant cyclic shift symmetry for having the solution of (18) satisfy the property in (23). We provide the proof of this lemma in Appendix C.

Lemma 2: In dominantly cyclic shift symmetric wiretap channels, rate splitting does not improve the rate-equivocation region and optimal channel prefixing has the cardinality $|\mathcal{V}^*| \leq |\mathcal{X}|$. In particular

$$C_s = \max_{P_x} f(P_x) - \min_{P_x} f(P_x). \quad (24)$$

We remark here that if the wiretap channel is dominantly cyclic symmetric, then known inner and outer bounds on the corresponding broadcast channel capacity region are shown to coincide in [11]. Therefore, the broadcast channel capacity region, which is in general an open problem, can be fully characterized for dominantly cyclic shift symmetric channels. We observe here that dominant cyclic symmetry yields a similar simplification for the wiretap channel, rendering rate splitting variable U unnecessary. However, note that the class of cyclic shift symmetric wiretap channels for which rate splitting is unnecessary is strictly larger than the class of dominantly cyclic shift symmetric channels. In fact, for all cyclic shift symmetric channels which satisfy (23), $U=\phi$ is optimal and dominant cyclic shift symmetry is just a sufficient but not necessary condition for the property (23). In Section V, we provide examples for binary-input cyclic shift symmetric wiretap channels that are not dominantly cyclic shift symmetric but for which rate splitting is still unnecessary.

Note that the secrecy capacity expression in (24) is the solution of the problem in (18) for $\mu = 0$. We also remark that (24) is generally an upper bound for the secrecy capacity:

$$\begin{aligned} C_s &= \max\ I(V;Y) - I(V;Z) && (25)\\ &= \max\ I(X;Y) - I(X;Z) \\ &\qquad - [I(X;Y|V) - I(X;Z|V)] && (26)\\ &\le \max_{P_x} f(P_x) - \min_{P_x} f(P_x) && (27) \end{aligned}$$

but it is attained for dominantly cyclic shift symmetric wiretap channels by Lemma 2.

Next, we consider more capable cyclic shift symmetric wiretap channels for which Theorems 2 and 3 are both applicable. According to Theorem 3, the optimal U^* and V^* have the transition probabilities as in (14)–(17) where the solution of the auxiliary optimization problem in (18) is $\hat{V} = X$ for all $\mu \geq 0$. We observe that the structure in (14)–(17) with $\hat{V} = X$ can be equivalently represented as uniform U^* with cardinality $|\mathcal{X}|$ and $V^* = X$, which is compatible with Theorem 2. In the following corollary, we show that the optimal U^* and V^* achieve (C_B, C_s) rate-equivocation pair. Furthermore, by Lemma 2, if the channel is more capable and dominantly cyclic shift symmetric, (C_B, C_s) pair is achieved by $V^* = X$ and $U^* = \phi$. We provide the proof of this corollary in Appendix D.

Corollary 1: In a more capable cyclic shift symmetric wiretap channel, $V^* = X$ and the rate-equivocation pair (C_B, C_s) is achievable. In a more capable dominantly cyclic shift symmetric wiretap channel, (C_B, C_s) pair is achieved by $V^* = X$ and $U^* = \phi$.

More capable cyclic shift symmetric wiretap channels have already been covered in [12] 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 [12], 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, in the same reference, 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 Corollary 1, (C_B, C_s) pair is achievable by a nontrivial U^* with uniform distribution and $V^* = X$ when r, p, and q are such that the wiretap channel is more capable.

We note that the results obtained for discrete alphabet cyclic shift symmetric channels naturally extend if the alphabets are bounded continuous intervals. In particular, the definition of cyclic shift symmetry extends naturally for $\mathcal{X} = [0, b)$: If $I(X;Y)$ is invariant under any modular shift in the input PDF, the channel is cyclic shift symmetric. Typical examples of continuous alphabet cyclic shift symmetric channels are modulo additive noise channels [14]. If cyclic shift symmetry holds, the channel capacity is achieved at uniform distribution over $\mathcal{X}$. Hence, if both the main and eavesdropping channels are cyclic shift symmetric, then the optimal selections U^* and V^* have the same structure as in Theorem 3. The definition of dominant cyclic shift symmetry also extends similarly for continuous alphabets and rate splitting is not necessary for continuous alphabet dominantly cyclic shift symmetric wiretap channels.

The result does not directly extend for unbounded input alphabets, i.e., for $b = \infty$, with an average power constraint. Even if the cyclic shift symmetry holds, it may not be possible to generate Bob's capacity achieving input PDF by shifting the solution of the auxiliary optimization problem, and therefore, the proof method in Theorem 3 is not directly applicable.

V. Binary-Input Cyclic Shift Symmetric Wiretap Channels

In this section, we consider cyclic shift symmetric wiretap channels with binary input: $|\mathcal{X}| = 2$. Note that the cardinality requirement on V to solve the problem in (18) is $|\mathcal{V}| = 2$ for binary input wiretap channels. Let $p(v_1) = \lambda$, $p(x|v_1) = [p_1, 1-p_1]$ and $p(x|v_2) = [p_2, 1-p_2]$. Let the resulting input distribution be $P_x = [p_x, 1-p_x]$. The optimization problem in (18) and (22) for the binary-input case reduces to

$$\begin{aligned} \max_{\lambda, p_1, p_2}\ & f(\lambda p_1 + (1-\lambda)p_2) - \lambda f_\mu(p_1) - (1-\lambda) f_\mu(p_2) \\ \text{s.t.}\ & 0 \leq \lambda, p_1, p_2 \leq 1. \end{aligned} \qquad (28)$$

The necessary optimality conditions for the problem in (28) are found by taking the derivative of the objective function with respect to p_1, p_2, and λ, respectively, and they have the following geometric interpretation as we show in [8]: If p_1^* or p_2^* are optimal and interior to $[0,1]$ interval, then the line drawn from $(p_1^*, f_\mu(p_1^*))$ and $(p_2^*, f_\mu(p_2^*))$ must be tangent to the f_μ curve at both points. If p_1^* or p_2^* are 0 or 1, then this tangency does not have to hold. This geometric interpretation provides a simple check if a point $p \in (0,1)$ is one of the optimal selections p_1^*, p_2^*: Draw the tangent line for f_μ at p. If this tangent line does not intersect f_μ other than p or if it intersects at a point $p' \in (0,1)$ but it is not tangent at p', then p cannot be an optimal selection. Also note that optimality conditions do not rule out the trivial selection $p_1 = 0$ and $p_2 = 1$.

A. BSC-BEC Wiretap Channel

Let the main channel be $\mathrm{BSC}(\epsilon)$ and the eavesdropper's channel be $\mathrm{BEC}(\alpha)$. Note that both BSC and BEC are cyclic shift symmetric. $\mathcal{X} = \mathcal{Y} = \{0,1\}$ and $\mathcal{Z} = \{0,e,1\}$. For $0 \leq \epsilon < 0.5$ and the input distribution $P_x = [p_x, 1-p_x]$, we have

$$f(p_x) = h((2\epsilon - 1)p_x + 1 - \epsilon) - h(\epsilon) - (1-\alpha)h(p_x) \quad (29)$$

where $h(.)$ is the binary entropy function. We first investigate some geometric properties of the function $f(p_x)$ in (29). It can be shown [11] that when $p(y|x)$ is $\mathrm{BSC}(\epsilon)$ and $p(z|x)$ is $\mathrm{BEC}(\alpha)$:

1) If $\alpha < 4\epsilon(1-\epsilon)$, then Eve is less noisy than Bob.
2) If $4\epsilon(1-\epsilon) \leq \alpha \leq h(\epsilon)$, Eve is more capable but not less noisy than Bob.

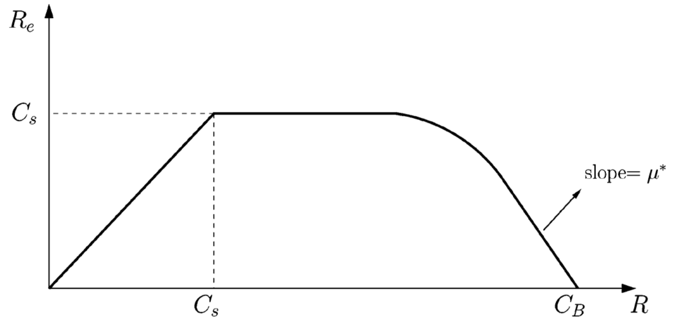

Fig. 6. General form of the rate-equivocation region of the BSC-BEC wiretap channel for $4\epsilon(1-\epsilon) \leq \alpha \leq h(\epsilon)$.

3) If $h(\epsilon) < \alpha$, the wiretap channel is dominantly cyclic shift symmetric.

We note that for the BSC-BEC channel 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 ④in Fig. 2. We observe that for $\alpha > h(\epsilon)$, case 3 above, $f(p_x)$ is maximized at $p_x = 0.5$, i.e., the channel satisfies dominant cyclic shift symmetry. By Lemma 2, rate splitting is not necessary for $\alpha > h(\epsilon)$, and moreover, the required channel prefixing has $|\mathcal{V}^*| = 2$ 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 $[(\mu+1)I(X;Y) - I(X;Z)]$. The secrecy capacity is

$$C_s = \max_{p_x} f(p_x) - \min_{p_x} f(p_x). \tag{30}$$

We give a specific numerical example by fixing $\epsilon = 0.1$ and $\alpha = 0.52$. Note that $\alpha > h(\epsilon)$ and hence this wiretap channel is dominantly cyclic shift symmetric. For this example, the main channel capacity is $C_B = 0.53$, eavesdropping channel capacity is $C_E = 0.48$, and secrecy capacity is $C_s = 0.073$, all in bits/channel use. Note that due to the gain provided by channel prefixing, the secrecy capacity is strictly greater than $C_B - C_E$.

We also note that for $\alpha < 4\epsilon(1-\epsilon)$, case 1 above, Eve is less noisy than Bob, and the secrecy capacity is $C_s = 0$ [2]. We investigate the remaining case, which is case 2 above, in the next section.

1) Case $4\epsilon(1-\epsilon) \leq \alpha \leq h(\epsilon)$*:* When $4\epsilon(1-\epsilon) \leq \alpha \leq h(\epsilon)$ in the BSC-BEC channel, neither Eve is less noisy nor the dominant cyclic shift symmetry holds. Secrecy capacity is still nonzero in this case and the rate-equivocation region has a nonempty interior. We verified in [8] that for all $\mu \geq 0$ and for all $0 \leq \lambda, p_1, p_2 \leq 1$,

$$\begin{aligned} f(0.5) &- \min_{p_x} f_\mu(p_x) \\ &\geq f(\lambda p_1 + (1-\lambda)p_2) - \lambda f_\mu(p_1) - (1-\lambda) f_\mu(p_2). \end{aligned} \tag{31}$$

Therefore, the optimal selection is $p_1^* = \arg\min_{p_x} f_\mu(p_x)$, $p_2^* = 1 - p_1^*$ and $\lambda^* = \frac{1}{2}$. Note that this selection satisfies the property in (23). Therefore, $U = \phi$ is optimal, and the upper right boundary of the rate-equivocation region can be traced by V only. However, unlike the case of $h(\epsilon) \leq \alpha$, if $4\epsilon(1-\epsilon) \leq \alpha \leq h(\epsilon)$, there exists $\mu \geq 0$ such that $f(0.5) < \min_{p_x} f_\mu(p_x)$. We define μ^* as

$$\mu^* = \min\{\mu : f(0.5) \leq \min_{p_x} f_\mu(p_x)\}. \tag{32}$$

For $\mu > \mu^*$, V defined as above cannot improve the objective function. Thus, trivial V is the optimal selection for $\mu > \mu^*$. However, the highest achievable equivocation with a trivial V selection is zero as Eve's channel is more capable with respect to Bob's channel in this case. Hence, for $\mu > \mu^*$, the only possible achievable point is $(C_B, 0)$. The general form of the rate-equivocation region is given in Fig. 6. The upper right boundary includes the line segment that combines the point for which the supporting line slope is μ^* and the $(C_B, 0)$ point. This line segment has the slope μ^*.

In conclusion, rate splitting U is not necessary for determining the rate-equivocation region of the BSC-BEC wiretap channel and in particular the secrecy capacity is

$$C_s = f(0.5) - \min_{p_x} f(p_x). \tag{33}$$

Note that (33) is in agreement with (30), as in that case $\max_{p_x} f(p_x)$ is achieved at $p_x = 0.5$.

B. BEC-BSC Wiretap Channel

Now, let the main channel be $\mathrm{BEC}(\alpha)$ and the eavesdropper's channel be $\mathrm{BSC}(\epsilon)$. $\mathcal{X} = \mathcal{Z} = \{0, 1\}$ and $\mathcal{Y} = \{0, e, 1\}$. We have the following facts [11].

1) If $\alpha < 4\epsilon(1-\epsilon)$, then Bob is less noisy than Eve.

2) If $4\epsilon(1-\epsilon) \leq \alpha \leq h(\epsilon)$, then Bob is more capable but not less noisy than Eve.

Hence, if $4\epsilon(1-\epsilon) \leq \alpha \leq h(\epsilon)$, the wiretap channel is in region ③in Fig. 2. By [2], $C_s = \max_{p_x} f(p_x)$, and from Corollary 1, (C_B, C_s) is achievable. If $\alpha < 4\epsilon(1-\epsilon)$, as both channels are cyclic shift symmetric, by [12, Th. 3], $C_s = C_B - C_E$ and (C_B, C_s) is achievable. We investigate the remaining case, which is $\alpha \geq h(\epsilon)$, in the next section.

1) Case $\alpha \geq h(\epsilon)$*:* In the BEC-BSC wiretap channel, if $\alpha \geq h(\epsilon)$, neither less noisy nor more capable condition holds. We solve the optimization problem in (28) by inspecting the tangent lines drawn at interior points $p \in (0, 1)$ and find in [8] that there are two optimal selections which are represented as $p(X = 0|V = v_1) = 0$ and $p(X = 0|V = v_2) = p_1$ where the line segment that combines $(0, 0)$ and $(p_1, f_\mu(p_1))$ is tangent to the curve $(p_x, f_\mu(p_x))$. The other optimal selection is $p(X = 0|V = v_1) = 1$ and $p(X = 0|V = v_2) = 1 - p_1$. The rate equivocation region is traced by varying μ and finding p_1 that satisfies the tangency and λ^* that yields the optimal value of the objective function given p_1. In particular, we define μ^* as

$$\mu^* = \min\{\mu \geq 0 | \min_{p_x} f_\mu(p_x) \geq 0\}. \tag{34}$$

For $\mu \leq \mu^*$, we use the following U and V:

$$p(U=u_1)=p(U=u_2)=\frac{1}{2} \tag{35}$$
$$p(V=v_1|U=u_1)=\lambda^*, \quad p(V=v_2|U=u_1)=1-\lambda^*, \tag{36}$$
$$p(V=v_3|U=u_2)=\lambda^*, \quad p(V=v_4|U=u_2)=1-\lambda^*, \tag{37}$$
$$p(X=0|V=v_1)=0, \quad p(X=0|V=v_2)=p_1, \tag{38}$$
$$p(X=0|V=v_3)=1, \quad p(X=|V=v_4)=1-p_1. \tag{39}$$

For $\mu > \mu^*$, V is not necessary as $f_\mu(p_x) \geq 0$ in this case. We obtain a case similar to the more capable condition and one

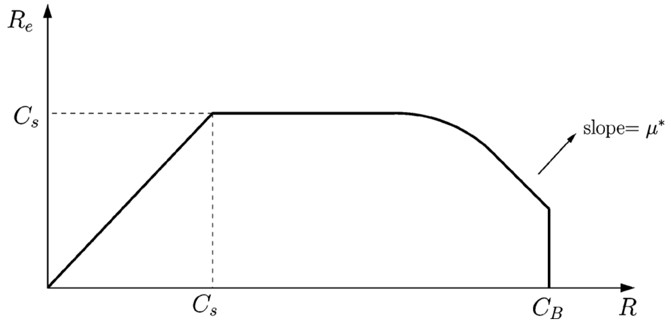

Fig. 7. General form of the rate-equivocation region of the BEC-BSC wiretap channel when $\alpha \geq h(\epsilon)$.

can easily show that a nontrivial V does not improve the objective function. As V is not used for $\mu > \mu^*$, the achieved rate $I(V;Y) = I(X;Y)$ and optimal selection of U as in Theorem 3 generates uniform distribution on the channel input X, which is capacity achieving for Bob's channel. Hence, for $\mu > \mu^*$, C_B is achieved. The general form of the rate-equivocation region is depicted in Fig. 7. Note that the supporting line with slope μ^* is on the boundary of the rate-equivocation region.

C. Existence of More Capable but Not Less Noisy Dominantly Cyclic Shift Symmetric Wiretap Channels

For the BSC-BEC and BEC-BSC wiretap channels, we observe that if the channel is more capable but not less noisy, dominant cyclic symmetry does not hold. Conversely, if dominant cyclic symmetry holds, the channel is not more capable. We question whether this property extends for general cyclic shift symmetric wiretap channels, i.e., we ask whether there exist more capable not less noisy cyclic shift symmetric wiretap channels that satisfy dominant cyclic shift symmetry. In this section, we answer this question in the affirmative direction.

We consider the following class of binary-input cyclic shift symmetric wiretap channels:

$$p(y|x) = \begin{pmatrix} 1-\epsilon & \epsilon \\ \epsilon & 1-\epsilon \end{pmatrix}$$
$$p(z|x) = \begin{pmatrix} 1-p-q & q & p \\ q & 1-p-q & p \end{pmatrix}.$$

Bob's channel $p(y|x)$ is $\mathrm{BSC}(\epsilon)$. Eve's channel $p(z|x)$ is parameterized by p and q and if $p = 0$, it reduces to $\mathrm{BSC}(q)$. In [8], we show that there exist selections of parameters ϵ, p, and q such that the resulting channel is more capable dominantly cyclic shift symmetric and not less noisy. One such example is obtained when we choose the parameters as $\epsilon = 0.4202, p = 0.6$, and $q = 0.25$. Via this example, we illustrate that there exist more capable, not less noisy, dominantly cyclic shift symmetric wiretap channels. Note that such channels lie in the intersection of the shaded region and region ③in Fig. 2. These channels demonstrate a desirable property: by Corollary 1, $U = \phi$ and $V = X$ is optimal for these channels, i.e., neither rate splitting nor channel prefixing is necessary.[3]

VI. Conclusion

In this paper, we provided new results on the roles of rate splitting and channel prefixing auxiliary random variables in a discrete memoryless wiretap channel. We identified general classes of wiretap channels in which one or both of these auxiliary random variables are not needed. In particular, we showed that if the wiretap channel is more capable, then channel prefixing is unnecessary and the entire boundary of the rate-equivocation region is traced by rate splitting alone. Conversely, if the channel is not more capable, we proved under a mild condition that a nontrivial channel prefixing is strictly necessary. Next, we showed that for cyclic shift symmetric wiretap channels, the boundary of the rate-equivocation region is achieved by a uniform U with cardinality $|\mathcal{X}|$ and the optimal prefix channel between U and V is expressed as cyclic shifts of the solution of an auxiliary optimization problem in a single variable. A specific consequence of this result is that if $I(X;Y) - I(X;Z)$ is maximized at the uniform distribution, i.e., if dominantly cyclic shift symmetry holds, then rate splitting is unnecessary. We applied our results to binary-input cyclic shift symmetric wiretap channels and characterized the boundaries of the rate-equivocation regions of the BSC-BEC and BEC-BSC wiretap channels. We found that rate splitting is not necessary for the BSC-BEC wiretap channel. Finally, we showed the existence of more capable, not less noisy, dominantly cyclic shift symmetric wiretap channels for which $U = \phi$ and $V = X$ are optimal. This demonstrates that there are larger classes of wiretap channels than less noisy wiretap channels for which the simple selections $U = \phi$ and $V = X$ are optimal.

Appendix A
Proof of Theorem 2

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

$$\begin{aligned} &\mu I(V;Y) + I(V;Y|U) - I(V;Z|U) \\ &\quad = \mu[I(X;Y) - I(X;Y|V)] + I(X;Y|U) - I(X;Z|U) \\ &\qquad - [I(X;Y|V,U) - I(X;Z|V,U)] && (40) \\ &\quad = \mu I(X;Y) + I(X;Y|U) - I(X;Z|U) \\ &\qquad - [(\mu+1)I(X;Y|V) - I(X;Z|V)] && (41) \\ &\quad \leq \mu I(X;Y) + I(X;Y|U) - I(X;Z|U) && (42) \end{aligned}$$

where (40) and (41) follow from the Markov chain $U \to V \to X \to Y, Z$, and (42) follows from the more capable condition. Therefore, using a nontrivial 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. In other words, in order to characterize the entire rate-equivocation region, it suffices to solve the following optimization problem:

$$\max_{U \to X \to Y,Z} \mu I(X;Y) + I(X;Y|U) - I(X;Z|U). \qquad (43)$$

We claim that $|\mathcal{U}| \leq |\mathcal{X}|$ is sufficient for the solution of (43). Given $U \to X \to Y, Z$, we fix the following $|\mathcal{X}|$ continuous functions of $P_{X|U}(x|u)$: $|\mathcal{X}| - 1$ components of $P_{X|U}(x|u)$, $x = 1, \ldots, |\mathcal{X}| - 1$ and $I(X;Y|U=u) - I(X;Z|U=u)$. By [5, Lemma 3] and the strengthened Caretheodory theorem of

[3] In a conference version of this work [15], we mistakenly claimed that rate splitting is strictly necessary for more capable but not less noisy channels. This also disproves [15, Corollary 1].

Fenchel–Eggleston in [6], there exists a random variable $U' \to X \to Y, Z$ such that

$$\mu I(X;Y) + I(X;Y|U) - I(X;Z|U) = \mu I(X;Y) + I(X;Y|U') - I(X;Z|U'). \quad (44)$$

Therefore, the optimization problem in (43) can be solved with the cardinality bound $|\mathcal{U}| \le |\mathcal{X}|$. Note the equivalence of the operations performed for proving the cardinality bounds in (43) and (6).

To prove the converse, assume that the wiretap channel is not more capable and $f(P_x)$ is maximized at an interior point $P_x^* \in \Delta$ that has all nonzero entries. Moreover, as the more capable condition does not hold, $f(\hat{P}_x) < 0$ for some input distribution $\hat{P}_x$. We use $\hat{P}_x$ and P_x^* to construct $V \ne X$ such that $V \to X \to Y, Z$ and

$$f(P_x^*) < I(V;Y) - I(V;Z) \quad (45)$$

and hence show the existence of a nontrivial channel prefixing that provides a higher secrecy capacity and therefore a larger rate-equivocation region. Applying Lemma 1 to the distributions $\hat{P}_x$ and P_x^*, there exists a PMF $\boldsymbol{q} \in \Delta$, with $q_1 > 0$ such that

$$P_x^* = q_1 \hat{P}_x + \sum_{k=1}^{|\mathcal{X}|-1} q_{k+1} \mathbf{e}_{j_k} \quad (46)$$

for some index set $J \subset \{1, \dots, |\mathcal{X}|\}$ with $|J| = |\mathcal{X}| - 1$, and $j_k \in J$. We construct V with $|\mathcal{V}| = |\mathcal{X}|$ in the following manner:

$$p_V(v_k) = q_k, \qquad k = 1, \dots, |\mathcal{X}|. \quad (47)$$

In addition, we select $p_{X|V}(x|v_1) = \hat{P}_x$, $p_{X|V}(x|v_2) = \mathbf{e}_{j_1}, \dots, p_{X|V}(x|v_{|\mathcal{X}|}) = \mathbf{e}_{j_{|\mathcal{X}|-1}}$. Evaluating $P_x = \sum_{k=1}^{|\mathcal{X}|} p_V(v_k) p_{X|V}(x|v_k)$, we observe that, by (46), the constructed P_x and the maximizer P_x^* are the same. However, $I(X;Y|V) - I(X;Z|V) < 0$ because given $V = v_1$,

$$I(X;Y|V = v_1) - I(X;Z|V = v_1) = f(\hat{P}_x) < 0 \quad (48)$$

while given $V = v_k$ for $k \ne 1$,

$$I(X;Y|V = v_k) - I(X;Z|V = v_k) = 0. \quad (49)$$

As $q_1 > 0$, we have

$$I(X;Y|V) - I(X;Z|V) < 0. \quad (50)$$

Using (50), and taking $\mu = 0$, i.e., the secrecy capacity point, we have for the constructed $V \to X \to Y, Z$

$$\begin{aligned} I(V;Y) - I(V;Z) &= I(X;Y) - I(X;Z) \\ &\quad - [I(X;Y|V) - I(X;Z|V)] \quad (51) \\ &> I(X;Y) - I(X;Z) \quad (52) \end{aligned}$$

which is (45), the desired result, since the generated input distribution P_x is equal to P_x^* and the left-hand side of (52) is $f(P_x^*)$.

Appendix B
Proof of Theorem 3

For given $\mu \ge 0$, the optimal selections U^* and V^* are the solutions of the following optimization problem:

$$\max_{U \to V \to X \to Y,Z} \mu I(V;Y) + I(V;Y|U) - I(V;Z|U). \quad (53)$$

By using the steps in (40) and (41), we obtain an equivalent statement for (53) as

$$\begin{aligned} \max_{U \to V \to X \to Y,Z} & \mu I(X;Y) + I(X;Y|U) - I(X;Z|U) \\ & - [(\mu+1) I(X;Y|V) - I(X;Z|V)]. \quad (54) \end{aligned}$$

We have the following bound for the objective function in (54):

$$\begin{aligned} & \mu I(X;Y) + I(X;Y|U) - I(X;Z|U) \\ & \quad - [(\mu+1) I(X;Y|V) - I(X;Z|V)] \\ & \le \max_{P_x} \mu I(X;Y) \\ & \quad + \max_{U \to V \to X \to Y,Z} I(X;Y|U) - I(X;Z|U) \\ & \qquad - [(\mu+1) I(X;Y|V) - I(X;Z|V)] \quad (55) \\ & \le \mu I_{\mathbf{u}}(X;Y) + \max_{\hat{V} \to X \to Y,Z} I(X;Y) - I(X;Z) \\ & \qquad - [(\mu+1) I(X;Y|\hat{V}) - I(X;Z|\hat{V})] \quad (56) \end{aligned}$$

where $\mathbf{u}$ denotes the $|\mathcal{X}|$-dimensional discrete uniform random variable, and $I_{\mathbf{u}}(X;Y)$ denotes the mutual information obtained by choosing the PMF of X as $\mathbf{u}$. In (56), we used the fact that $\max_{P_x} I(X;Y) = I_{\mathbf{u}}(X;Y)$ as Bob's channel is cyclic shift symmetric. Moreover, we used the fact that U is not needed, i.e., $U = \phi$, for maximizing $I(X;Y|U) - I(X;Z|U)$ $-[(\mu + 1)I(X;Y|V) - I(X;Z|V)]$. Because, for given $U \to V \to X \to Y, Z$, we can always pick $u_i \in \mathcal{U}$ that maximizes

$$\begin{aligned} \max_{u_i \in \mathcal{U}} & I(X;Y|U = u_i) - I(X;Z|U = u_i) \\ & - \sum_{v \in \mathcal{V}} [(\mu+1) I(X;Y|v) - I(X;Z|v)] p(v|u_i) \quad (57) \end{aligned}$$

and, therefore, choose a deterministic U with $U = u^*$, where u^* is the argument of the maximization in (57). Consequently, we have

$$\begin{aligned} & \max_{U \to V \to X \to Y,Z} I(X;Y|U) - I(X;Z|U) \\ & \quad - [(\mu+1) I(X;Y|V) - I(X;Z|V)] \\ & = \max_{\hat{V} \to X \to Y,Z} I(X;Y) - I(X;Z) \\ & \quad - [(\mu+1) I(X;Y|\hat{V}) - I(X;Z|\hat{V})]. \quad (58) \end{aligned}$$

Note that the right-hand side of (58) is the claimed auxiliary optimization problem in the statement of the theorem. We use $\hat{V}$ notation to emphasize that the auxiliary random variables on the right- and left-hand sides of (58) are different.

Next, we will show that the bound in (56) is satisfied with equality for any cyclic shift symmetric wiretap channel. Let

$\hat{V}$ with $p(\hat{V}=v)$ and $p(X|\hat{V}=v)$, $v \in \hat{\mathcal{V}}$, be the solution of the auxiliary problem in (58). First, we note that it suffices to consider $\hat{V}$ such that $|\hat{\mathcal{V}}| \leq |\mathcal{X}|$. This follows by the arguments we have used in the previous cardinality bound proofs. In particular, given $\hat{V} \rightarrow X \rightarrow Y, Z$, we fix $|\mathcal{X}|-1$ components of $P_{X|\hat{V}}(x|\hat{v})$, $j=1,\ldots,|\mathcal{X}|-1$, together with $(\mu+1)I(X;Y|\hat{V}=\hat{v}) - I(X;Z|\hat{V}=\hat{v})$. By [5, Lemma 3] and the strengthened Caretheodory theorem of Fenchel–Eggleston in [6], the problem in (58) can be solved with the cardinality bound $|\hat{\mathcal{V}}| \leq |\mathcal{X}|$. Note the equivalence of the operations performed for proving the bounds in this problem and those in (43) and (6).

Now, we construct the optimal U^*, V^* by using the optimal $\hat{V}$ for the auxiliary problem in (58) as in the statement of the theorem. In particular, we select the cardinalities as $|\mathcal{U}^*| = |\mathcal{X}|$ and $|\mathcal{V}^*| = |\mathcal{X}|^2$ with the distributions $p(U^*=u) = \frac{1}{|\mathcal{X}|}$ for $u \in \mathcal{U}^*$ and

$$p(V^*=v|U^*=1) = p(\hat{V}=v), \quad v \in \{1,\ldots,|\mathcal{X}|\} \tag{59}$$

$$p(V^*=v|U^*=1) = 0, \quad v \notin \{1,\ldots,|\mathcal{X}|\} \tag{60}$$

$$p(x|V^*=v) = p(x|\hat{V}=v), \quad v \in \{1,\ldots,|\mathcal{X}|\} \tag{61}$$

$$p(V^*=|\mathcal{X}|+v|U^*=2) = p(\hat{V}=v), \quad v \in \{1,\ldots,|\mathcal{X}|\} \tag{62}$$

$$p(V^*=v|U^*=2) = 0, \quad v \notin \{|\mathcal{X}|+1,\ldots,2|\mathcal{X}|\} \tag{63}$$

$$p(x|V^*=|\mathcal{X}|+v) = p(x|\hat{V}=v)(1), \quad v \in \{1,\ldots,|\mathcal{X}|\} \tag{64}$$

$$\vdots$$

$$p(V^*=(|\mathcal{X}|-1)|\mathcal{X}|+v|U^*=|\mathcal{X}|-1) = p(\hat{V}=v), \quad v \in \{1,\ldots,|\mathcal{X}|\} \tag{65}$$

$$p(V^*=v|U^*=|\mathcal{X}|) = 0, \quad v \notin \{(|\mathcal{X}|-1)|\mathcal{X}|+1,\ldots,|\mathcal{X}|^2\} \tag{66}$$

$$p(x|V^*=(|\mathcal{X}|-1)|\mathcal{X}|+v) = p(x|\hat{V}=v)(|\mathcal{X}|-1) \quad v \in \{1,\ldots,|\mathcal{X}|\}. \tag{67}$$

The structure of the construction in (59)–(67) is an expression of the $U^* \rightarrow V^* \rightarrow X^*$ in Fig. 5. Each element of U^* generates the optimizing selection $p(\hat{V})$ for the problem in (58) over disjoint $|\mathcal{X}|$ elements of V^*. Each disjoint $|\mathcal{X}|$ element of V^* generates cyclic shifts of the optimizing selection $p(X|\hat{V})$ for the input X. In (59)–(67), we denote the kth cyclic shift of the conditional PMF for the channel input X, $p(x|\hat{V}=v)$, as $p(x|\hat{V}=v)(k)$. Note that the cardinality of $\hat{V}$ is $|\mathcal{X}|$ while that of the optimum V^* is $|\mathcal{X}|^2$ and $|\mathcal{X}|^2$ conditional input PMFs, $p(x|V^*=v)$, are obtained by cyclic shifts of $|\mathcal{X}|$ conditional input PMFs, $p(x|\hat{V}=v)$.

We first observe that $p(x|U^*=i)$ are cyclic shifts of a fixed PMF over X for different i. In particular, in the construction in (59)–(67), we selected $p(x|V^*=v)$ as cyclic shifts of $p(x|\hat{V}=v)$ while we kept $p(V^*=v)$ the same as $p(\hat{V}=v)$. Hence, we have

$$p(x|U^*=i) = p_f(x)(i-1) \tag{68}$$

where $p_f(x) = \sum_{v=1}^{|\mathcal{X}|} p(x|\hat{V}=v)p(\hat{V}=v)$. Note that $p_f(x)$ is the maximizing input PMF for the auxiliary problem. Therefore, U^* and V^* generate a uniform PMF for X:

$$\begin{aligned} p(x) &= \sum_{i=1}^{|\mathcal{X}|} p(U^*=i)p(x|U^*=i) \\ &= \sum_{i=1}^{|\mathcal{X}|} \frac{1}{|\mathcal{X}|} p_f(x)(i-1) \\ &= \frac{1}{|\mathcal{X}|}. \end{aligned} \tag{69}$$

Moreover, by construction of U^* and V^* and the cyclic shift symmetry of the channels, we observe that, for any given i

$$\begin{aligned} &\sum_{v=1}^{|\mathcal{X}|} \big[(\mu+1)I(X;Y|V^*=v+(i-1)|\mathcal{X}|) \\ &\qquad - I(X;Z|V^*=v+(i-1)|\mathcal{X}|)\big] \\ &\qquad p(V^*=(i-1)|\mathcal{X}|+v|U=i) \\ &= \sum_{v=1}^{|\mathcal{X}|} \big[(\mu+1)I(X;Y|\hat{V}=v) - I(X;Z|\hat{V}=v)\big] p(\hat{V}=v) \qquad (70) \\ &= (\mu+1)I(X;Y|\hat{V}) - I(X;Z|\hat{V}). \qquad (71) \end{aligned}$$

Therefore, we have

$$\begin{aligned} &(\mu+1)I(X;Y|V^*) - I(X;Z|V^*) \\ &= \sum_{v=1}^{|\mathcal{X}|^2} \Big[(\mu+1)I(X;Y|V^*=v) \\ &\qquad - I(X;Z|V^*=v)\Big] p(V^*=v) \qquad (72) \\ &= \sum_{i=1}^{|\mathcal{X}|} \sum_{v=1}^{|\mathcal{X}|^2} \Big[(\mu+1)I(X;Y|V^*=v) \\ &\qquad - I(X;Z|V^*=v)\Big] p(v|U^*=i)p(U^*=i) \qquad (73) \\ &= \frac{1}{|\mathcal{X}|} \sum_{i=1}^{|\mathcal{X}|} \sum_{v=1}^{|\mathcal{X}|} \Big[(\mu+1)I(X;Y|V^*=v+(i-1)|\mathcal{X}|) \\ &\qquad - I(X;Z|V^*=v+(i-1)|\mathcal{X}|)\Big] p(\hat{V}=v) \qquad (74) \\ &= (\mu+1)I(X;Y|\hat{V}) - I(X;Z|\hat{V}) \qquad (75) \end{aligned}$$

where (75) is obtained by using (71) and the fact that $p(v|U^*=i)$ is nonzero only for $(i-1)|\mathcal{X}|+1 \leq v \leq i|\mathcal{X}|$. Note that

$$\begin{aligned} I(X;Y|U^*=i) - I(X;Z|U^*=i) &= f(p_f(x)(i-1)) \qquad (76) \\ &= f(p_f(x)), \qquad \forall i. \qquad (77) \end{aligned}$$

Hence, given $U^* = i$, we have

$$\begin{aligned} &I(X;Y|U^*=i) - I(X;Z|U^*=i) \\ &\qquad - [(\mu+1)I(X;Y|V^*) - I(X;Z|V^*)] \\ &= f(p_f(x)) - \left[(\mu+1)I(X;Y|\hat{V}) - I(X;Z|\hat{V})\right]. \end{aligned} \tag{78}$$

As $p_f(x)$ is the maximizing input PMF for the auxiliary problem, we have

$$\begin{aligned} &I(X;Y|U^*) - I(X;Z|U^*) \\ &\qquad - [(\mu+1)I(X;Y|V^*) - I(X;Z|V^*)] \\ &= \max_{\hat{V}\to X\to Y,Z} I(X;Y) - I(X;Z) \\ &\qquad - [(\mu+1)I(X;Y|\hat{V}) - I(X;Z|\hat{V})]. \end{aligned} \tag{79}$$

Since U^* and V^* generate a uniform PMF for X by (69), $I(X;Y)$ achieves its maximum, as well. Combining this with (79), we conclude that the constructed U^* and V^* achieve the upper bound in (56) and hence are optimal.

Appendix C
Proof of Lemma 2

It suffices to show that for dominantly cyclic shift symmetric wiretap channels, the optimal auxiliary selections satisfy the property in (23). Let the optimal selection of the auxiliary $\hat{V}$ in the following problem be $\hat{V}^*$:

$$\begin{aligned} &\max_{\hat{V}\to X\to Y,Z} I(X;Y) - I(X;Z) \\ &\qquad - [(\mu+1)I(X;Y|\hat{V}) - I(X;Z|\hat{V})]. \end{aligned} \tag{80}$$

We will prove that at least one such $\hat{V}^*$ satisfies the property in (23). Due to Theorem 3, we already know that the cardinality of $\hat{V}$ is bounded by $|\mathcal{X}|$.

Let $R_e^* = \max_{P_x} f(P_x)$. First, we obtain an upper bound for the objective function in (80):

$$\begin{aligned} &I(X;Y) - I(X;Z) - [(\mu+1)I(X;Y|\hat{V}) - I(X;Z|\hat{V})] \\ &\le R_e^* - [(\mu+1)I(X;Y|\hat{V}) - I(X;Z|\hat{V})] && (81) \\ &\le R_e^* - \min_{P_x}[(\mu+1)I(X;Y) - I(X;Z)] && (82) \end{aligned}$$

where (81) follows from $I(X;Y) - I(X;Z) \le R_e^*$ and (82) is obtained by replacing $[(\mu+1)I(X;Y|\hat{V}) - I(X;Z|\hat{V})]$ with its minimum possible value.

Now, we will show that the upper bound in (82) is achieved by an auxiliary $\hat{V}^*$ of cardinality $|\hat{\mathcal{V}}| \le |\mathcal{X}|$ with the desired property in (23). By the hypothesis, $\mathbf{u} = \arg\max_{P_x} I(X;Y) = \arg\max_{P_x} f(P_x)$. Moreover, let $P_x^* = \arg\min_{P_x}[(\mu+1)I(X;Y) - I(X;Z)]$. Note that P_x^* is different from the uniform distribution. By cyclic shift symmetry, there exist $|\mathcal{X}| - 1$ other input distributions that minimize $(\mu+1)I(X;Y) - I(X;Z)$, which are cyclic shifts of P_x^*, denoted by $P_x^*(i)$ for $i = 1,\ldots,|\mathcal{X}| - 1$. Therefore, we define the channel prefixing $\hat{V}^*$ with $|\hat{\mathcal{V}}^*| = |\mathcal{X}|$ as $p(\hat{V}^* = v_i) = 1/|\mathcal{X}|$ with transition probabilities $p(x|\hat{V}^* = v_1) = P_x^*$, $p(x|\hat{V}^* = v_2) = P_x^*(1),\ldots$, and $p(x|\hat{V}^* = v_{|\mathcal{X}|}) = P_x^*(|\mathcal{X}| - 1)$. Then, the input distribution is $P_x = \sum_{i=1}^{|\mathcal{X}|} p(\hat{V}^* = v_i)P_x^*(i) = \mathbf{u}$. For this selection of $\hat{V}^*$, we have

$$\begin{aligned} &I(X;Y) - I(X;Z) - [(\mu+1)I(X;Y|\hat{V}^*) - I(X;Z|\hat{V}^*)] \\ &= f(P_x = \mathbf{u}) - \min_{P_x}[(\mu+1)I(X;Y) - I(X;Z)] && (83) \\ &= R_e^* - \min_{P_x}[(\mu+1)I(X;Y) - I(X;Z)]. && (84) \end{aligned}$$

Note that (84) is equivalent to the upper bound in (82). Moreover, the specified channel prefixing $\hat{V}^*$ satisfies the desired property in (23) by construction.

Appendix D
Proof of Corollary 1

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 is compact.

There exist $|\mathcal{X}| - 1$ other input distributions (cyclic shifts of P_x^*) that achieve the maximum $f(P_x)$. Let us define the auxiliary U, with $\mathcal{U} = \{u_1,\ldots,u_{|\mathcal{X}|}\}$, with marginal distribution $p_U(u_i) = \frac{1}{|\mathcal{X}|}$, and transition probabilities $p_{X|U}(x|u_1) = P_x^*$, $p_{X|U}(x|u_2) = P_x^*(1),\ldots$, and $p_{X|U}(x|u_{|\mathcal{X}|}) = P_x^*(|\mathcal{X}| - 1)$, where $P_x^*(i)$ denotes the ith cyclic shift of P_x^*.

Evaluating (5) with the specified choice of U^* and with $V^* = X$, we have $I(V^*;Y) = C_B$, since $P_x = \sum_{u\in\mathcal{U}} p_U(u)p_{X|U}(x|u) = \frac{1}{|\mathcal{X}|}\sum_{i=1}^{|\mathcal{X}|} P_x^*(i) = \mathbf{u}$, where $\mathbf{u}$ is the uniform distribution, and since 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.

Note that if $P_x^* = \mathbf{u}$, i.e., if the channel satisfies dominant cyclic shift symmetry, then $U^* = \phi$ is optimal since any cyclic shift of $\mathbf{u}$ is $\mathbf{u}$ itself, and thus, U^* is independent of X.

References

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

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

[3] I. Csiszár, "Almost independence and secrecy capacity," *Prob. Inf. Trans.*, vol. 32, no. 1, pp. 48–57, 1996.

[4] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proc. EUROCRYPT*, 2000, pp. 351–368.

[5] R. Ahlswede and J. Körner, "Source coding with side information and a converse for degraded broadcast channels," *IEEE Trans. Inf. Theory*, vol. IT-21, no. 6, pp. 629–638, Nov. 1975.

[6] M. Salehi, Cardinality bounds on auxiliary variables in multiple user theory via the method of Ahlswede and Körner Stanford Univ.. Stanford, CA, Aug. 1978, Tech. Rep. 33.

[7] A. E. Gamal and Y.-H. Kim, Lecture notes on network information theory 2010 [Online]. Available: ArXiv:1001.3404

[8] O. Ozel and S. Ulukus, Wiretap channels: Implications of more capable condition and cyclic shift symmetry 2011 [Online]. Available: ArXiv:1110.4613, (Longer Version of the Present Paper With Detailed Proofs)

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

[10] B. Xie and R. Wesel, "A mutual information invariance approach to symmetry in discrete memoryless channels," in *Proc. Inf. Theory Appl. Workshop*, Feb. 2008, pp. 444–448.

[11] C. Nair, “Capacity regions of two new classes of two-receiver broadcast channels,” *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4207–4214, Sep. 2010.

[12] M. van Dijk, “On a special class of broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 43, no. 2, pp. 712–714, Mar. 1997.

[13] S. K. Leung-Yan-Cheung, “On a special class of wiretap channels,” *IEEE Trans. Inf. Theory*, vol. IT-23, no. 5, pp. 625–627, Sep. 1977.

[14] U. Erez and R. Zamir, “Noise prediction for channels with side information at the transmitter,” *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1610–1617, Jul. 2000.

[15] O. Ozel and S. Ulukus, “Wiretap channels: Roles of rate splitting and channel prefixing,” in *IEEE Int. Symp. Inf. Theory*, Jul. 2011, pp. 628–632.

Omur Ozel (S’08) received the B.Sc. and the M.S. degrees with honors in electrical and electronics engineering from the Middle East Technical University (METU), Ankara, Turkey, in June 2007 and July 2009, respectively. Since August 2009, he has been a graduate research assistant at the University of Maryland College Park, working towards Ph.D. degree in electrical and computer engineering. He is a graduate student member of IEEE.

Sennur Ulukus (S’90–M’98) is a Professor of Electrical and Computer Engineering at the University of Maryland at College Park, where she also holds a joint appointment with the Institute for Systems Research (ISR). Prior to joining UMD, she was a Senior Technical Staff Member at AT&T Labs-Research. She received her Ph.D. degree in Electrical and Computer Engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University, and B.S. and M.S. degrees in Electrical and Electronics Engineering from Bilkent University. Her research interests are in wireless communication theory and networking, network information theory for wireless communications, signal processing for wireless communications, information-theoretic physical-layer security, and energy-harvesting communications.

Dr. Ulukus received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications, the 2005 NSF CAREER Award, and the 2010–2011 ISR Outstanding Systems Engineering Faculty Award. She served as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY between 2007–2010, as an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS between 2003–2007, as a Guest Editor for the *Journal of Communications and Networks* for the special issue on energy harvesting in wireless networks, as a Guest Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY for the special issue on interference networks, as a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the special issue on multiuser detection for advanced communication systems and networks. She served as the TPC co-chair of the Communication Theory Symposium at the 2007 IEEE Global Telecommunications Conference, the Medium Access Control (MAC) Track at the 2008 IEEEWireless Communications and Networking Conference, theWireless Communications Symposium at the 2010 IEEE International Conference on Communications, the 2011 Communication Theory Workshop, the Physical-Layer Security Workshop at the 2011 IEEE International Conference on Communications, the Physical-Layer Security Workshop at the 2011 IEEE Global Telecommunications Conference. She was the Secretary of the IEEE Communication Theory Technical Committee (CTTC) in 2007–2009.