

Arbitrary Jamming Can Preclude Secure Communication

Ebrahim MolavianJazi, Matthieu Bloch, J. Nicholas Laneman

Abstract—We investigate the effect of certain active attacks on the secrecy capacity of wiretap channels by considering arbitrarily varying wiretap channels. We establish a lower bound for the secrecy capacity with randomized coding of a class of such channels and an upper bound for that of all such channels. We show that if the arbitrarily varying wiretap channel possesses a bad “averaged” state, namely one in which the legitimate receiver is degraded with respect to the eavesdropper, then secure communication is not possible.

I. INTRODUCTION

The seminal works of Wyner [1] and Csiszár & Körner [2] on the secrecy capacity of the wiretap channel have unveiled the potential of coding for security at the physical layer; however, the scope of the wiretap channel model is essentially restricted to situations in which the adversary is a passive eavesdropper. With the exception of [3], [4], [5], little attention has been paid to the effect of adversarial jamming on the secrecy capacity of wiretap channels. For practical applications, being able to cope with active attackers is of paramount importance, and the passive eavesdropper assumption is often viewed as too simplistic.

As a first step towards understanding wiretap channels under active attacks, we consider discrete wiretap channels in which a jammer attempts to disrupt communication *independently of the eavesdropper*. The impact of this jammer is modeled as an arbitrarily varying state, as studied by Blackwell [6], Ahlswede [7], Csiszár & Körner [8], and Jahn [9]. A more general attack model would consider jamming strategies that depend on the eavesdropper’s observations, but even the results obtained for our simple model already highlight the significant impact of active attacks.

The remainder of the paper is organized as follows. Section II introduces our model of arbitrarily varying wiretap channel. Section III establishes achievable rates for a class of arbitrarily varying wiretap channels under randomized coding. Section IV derives a generic upper bound for the secrecy capacity of arbitrarily varying wiretap channels under randomized coding. Finally, Section V discusses a specific arbitrarily varying wiretap channel for which the secrecy capacity under randomized coding is known, and Section VI concludes the paper.

II. SYSTEM MODEL

As illustrated in Figure 1, a discrete memoryless arbitrarily varying wire-tap channel (AVWTC) is characterized by a

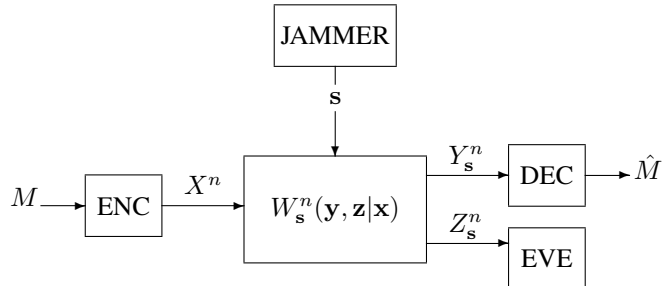


Fig. 1. Block diagram for the arbitrarily varying wiretap channel model.

finite input alphabet \mathcal{X} , two finite output alphabets \mathcal{Y} and \mathcal{Z} , an arbitrary “state” space \mathcal{S} , and a family of transition probabilities from \mathcal{X} to $\mathcal{Y} \times \mathcal{Z}$ indexed by \mathcal{S}

$$\mathcal{W} = \left\{ W_s(y, z|x) \triangleq W(y, z|x; s) : s \in \mathcal{S} \right\} .$$

The n -extension of the channel law for input $\mathbf{x} = (x_1, \dots, x_n) \in \mathcal{X}^n$ and outputs $\mathbf{y} = (y_1, \dots, y_n) \in \mathcal{Y}^n$ and $\mathbf{z} = (z_1, \dots, z_n) \in \mathcal{Z}^n$ under the *state sequence* $\mathbf{s} = (s_1, \dots, s_n) \in \mathcal{S}^n$ is defined as follows.

$$W_s^n(\mathbf{y}, \mathbf{z}|\mathbf{x}) \triangleq \prod_{i=1}^n W_{s_i}(y_i, z_i|x_i) = \prod_{i=1}^n W(y_i, z_i|x_i; s_i)$$

Although the input-output relationship in AVWTC is defined in a *memoryless* way, the channel state varies from letter to letter in the course of transmission of a single codeword and could be selected arbitrarily (probably with *memory*). By convention, the terminal observing the output $\mathbf{y} \in \mathcal{Y}^n$ is called the *legitimate receiver* while the terminal observing the output $\mathbf{z} \in \mathcal{Z}^n$ is called the *eavesdropper*. The state sequence $\mathbf{s} \in \mathcal{S}^n$ represents a *jamming attack* on the channel. We assume that the jammer’s attack \mathbf{s} is chosen independently of the eavesdropper’s observation \mathbf{z} . Moreover, the transmitter and receivers are assumed to know the state space \mathcal{S} , but not the actual realization of the state s at each time instant.

Definition 1: An (n, M) wiretap code for AVWTC consists of a message set $\mathcal{M} = \{1, \dots, M\}$, a stochastic encoder $f : \mathcal{M} \rightarrow \mathcal{X}^n$, and a decoder $\phi : \mathcal{Y}^n \rightarrow \mathcal{M}$.

For a given state sequence \mathbf{s} , let M be the random variable denoting the choice of a message drawn uniformly at random from the message set \mathcal{M} , let X^n denote the corresponding codeword transmitted over the channel, and let Y_s^n and Z_s^n be the corresponding channel outputs for the legitimate receiver and the eavesdropper, respectively. The *average error probability* of the wiretap code (f, ϕ) in the

Ebrahim MolavianJazi and J. Nicholas Laneman are with the Department of Electrical Engineering, University of Notre Dame, Fitzpatrick Hall, Notre Dame, IN, 46556, USA. {emolavia, jnl}@nd.edu

Matthieu Bloch is with the School of Electrical and Computer Engineering, Georgia Institute of Technology, and with the GT-CNRS UMI 2968, 2-3 rue Marconi, 57070 Metz, France. mbloch@ece.gatech.edu

state sequence \mathbf{s} is defined as

$$\bar{e}(W_{\mathbf{s}}^n, f, \phi) \triangleq \frac{1}{M} \sum_{m \in \mathcal{M}} \sum_{\mathbf{z} \in \mathcal{Z}^n} W_{\mathbf{s}}^n((\phi^{-1}(m))^c, \mathbf{z} | f(m)),$$

and the *leakage rate* of the wiretap code (f, ϕ) in the state sequence \mathbf{s} is defined as

$$L(W_{\mathbf{s}}^n, f, \phi) \triangleq \frac{1}{n} \mathbb{I}(M; Z_{\mathbf{s}}^n | (f, \phi)),$$

where the conditioning on (f, ϕ) accounts for the fact that the wiretap code (f, ϕ) is known to the eavesdropper.

To combat the jammer and make the unknown “jamming” no more harmful than “noise”, it is useful to randomize the transmission by selecting different encoder-decoder pairs at random. This motivates the definition of randomized wiretap codes as follows.

Definition 2: An (n, M) *randomized wiretap code* for AVWTC consists of a message set $\mathcal{M} = \{1, \dots, M\}$ and a random variable (F, Φ) over a family of (n, M) wiretap codes $\mathcal{C} = \{(f, \phi)\}$.

The *mean average error probability* of the randomized wiretap code (F, Φ) in the state sequence \mathbf{s} is defined as the expected value of the average error probability random variable.

$$\bar{e}^{(\text{av})}(W_{\mathbf{s}}^n, F, \Phi) \triangleq \mathbb{E}_{(F, \Phi)} [\bar{e}(W_{\mathbf{s}}^n, F, \Phi)]$$

Similarly, the *mean leakage rate* of the randomized wiretap code (F, Φ) in the state sequence \mathbf{s} is defined as the expected value of the leakage rate random variable.

$$L^{(\text{av})}(W_{\mathbf{s}}^n, F, \Phi) \triangleq \mathbb{E}_{(F, \Phi)} [L(W_{\mathbf{s}}^n, F, \Phi)] = \frac{1}{n} \mathbb{I}(M; Z_{\mathbf{s}}^n | (F, \Phi)),$$

which is the usual conditional mutual information. Note that, the actual realization of the random variable (F, Φ) can be thought of as a *key* shared between the transmitter and the receivers *including the eavesdropper*, but *not available to the jammer*, although it might be cognizant of the family \mathcal{C} of the underlying wiretap codes and the statistics of the random variable (F, Φ) . The fact that the eavesdropper has access to the key is reflected in the conditioning on (F, Φ) in the expression of the mean leakage rate, and we emphasize that this does not provide any advantage to the legitimate receiver over the eavesdropper.

Definition 3: A *randomized-code secrecy rate* R_s is called *achievable* for AVWTC \mathcal{S} , if for every $\epsilon > 0$ there exists a sequence of (n, M) randomized wiretap codes such that

$$\begin{aligned} \frac{1}{n} \log M &\geq R_s - \epsilon, \\ \bar{e}^{(\text{av})}(W_{\mathbf{s}}^n, F, \Phi) &\leq \epsilon \quad \forall \mathbf{s} \in \mathcal{S}^n, \\ L^{(\text{av})}(W_{\mathbf{s}}^n, F, \Phi) &\leq \epsilon \quad \forall \mathbf{s} \in \mathcal{S}^n. \end{aligned}$$

Accordingly, the *randomized-code secrecy capacity* \hat{C}_s of AVWTC is defined as the supremum of all achievable randomized-code secrecy rates. Notice that the definition of the randomized-code secrecy rate and capacity ensures the reliable and secure communication under *any* state sequence,

taking into account the fact that neither the transmitter nor the receivers know the actual state sequence $\mathbf{s} \in \mathcal{S}^n$.

An essential concept in the analysis of an AVWTC is the notion of *convex closure* of an AVWTC. For an AVWTC $\mathcal{W} = \{W_{\mathbf{s}}(y, z|x) : \mathbf{s} \in \mathcal{S}\}$, denote by $\bar{\mathcal{S}}$ the closure of the set of all “averaged” states, *i.e.*, convex combinations of elements of \mathcal{S} .

$$\bar{\mathcal{S}} = \text{closure} \left(\left\{ \bar{\mathbf{s}} = \sum_{k=1}^r s_k p(s_k) : \right. \right. \\ \left. \left. r \in \mathbb{N}, s_k \in \mathcal{S}, p(s_k) \geq 0, \sum_{k=1}^r p(s_k) = 1 \right\} \right)$$

Then, the convex closure $\bar{\mathcal{W}}$ of the AVWTC is defined as the closure of the set of all corresponding “averaged” wiretap channels as follows.

$$\bar{\mathcal{W}} = \text{closure} \left(\left\{ W_{\bar{\mathbf{s}}}(y, z|x) = \sum_k p(s_k) W_{s_k}(y, z|x) : \right. \right. \\ \left. \left. \bar{\mathbf{s}} = \sum_k s_k p(s_k) \in \bar{\mathcal{S}} \right\} \right)$$

The “averaged” states play a significant role in obtaining a single-letter characterization of the channel capacity for arbitrarily varying channels [9]. Since an AVWTC and its convex closure are essentially characterized by the corresponding state space \mathcal{S} and “averaged” state space $\bar{\mathcal{S}}$, we will refer to the AVWTC \mathcal{W} also as the AVWTC \mathcal{S} and its convex closure $\bar{\mathcal{W}}$ also as $\bar{\mathcal{S}}$, provided there is no ambiguity.

III. LOWER BOUND FOR RANDOMIZED-CODE SECRECY CAPACITY OF AVWTC

In this section, we establish an achievable randomized-code secrecy rate for AVWTC’s that are such that the eavesdropper’s channel under *any* state $s \in \mathcal{S}$ is degraded with respect to the channel under fixed state $s^* \in \mathcal{S}$, *i.e.*,

$$\exists s^* \in \bar{\mathcal{S}} \quad \forall s \in \mathcal{S} \quad X \rightarrow Z_{s^*} \rightarrow Z_s. \quad (*)$$

Note that the condition $(*)$ implies that

$$\mathbb{I}(X; Z_{s^*}) = \sup_{s \in \mathcal{S}} \mathbb{I}(X; Z_s). \quad (1)$$

Moreover, since the mutual information is convex in the transition probability and the set $\bar{\mathcal{S}}$ is convex, we can also conclude that $\sup_{s \in \mathcal{S}} \mathbb{I}(X; Z_s) = \sup_{\bar{\mathbf{s}} \in \bar{\mathcal{S}}} \mathbb{I}(X; Z_{\bar{\mathbf{s}}})$; therefore,

$$\mathbb{I}(X; Z_{s^*}) = \sup_{\bar{\mathbf{s}} \in \bar{\mathcal{S}}} \mathbb{I}(X; Z_{\bar{\mathbf{s}}}). \quad (2)$$

We emphasize that, in general, conditions (1) and (2) do not imply the condition $(*)$.

Theorem 1: For any AVWTC \mathcal{S} satisfying the condition $(*)$, all randomized-code secrecy rates

$$R_s < \max_{P_X(x)} \left[\min_{\bar{\mathbf{s}} \in \bar{\mathcal{S}}} I(X; Y_{\bar{\mathbf{s}}}) - \max_{\bar{\mathbf{s}} \in \bar{\mathcal{S}}} I(X; Z_{\bar{\mathbf{s}}}) \right]$$

are achievable.

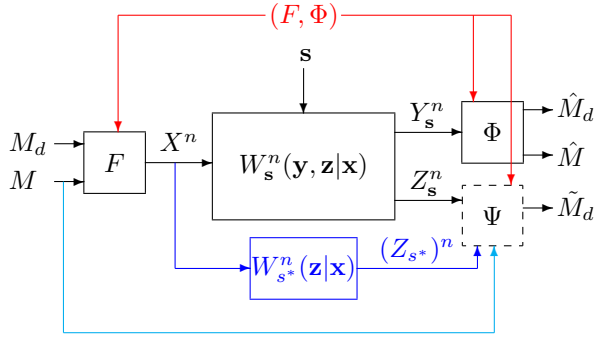


Fig. 2. The setup used for the proof of Theorem 1: The AVWTC $W_{\mathbf{s}}^n(\mathbf{y}, \mathbf{z}|\mathbf{x})$ in state sequence \mathbf{s} , the enhanced channel $W_{s^*}^n(\mathbf{z}|\mathbf{x})$ provided to the eavesdropper, the randomized wiretap code (F, Φ) , and the virtual receiver Ψ with access to the actual message M .

This result essentially suggests that, as far as randomized wiretap codes are concerned, the secrecy rate is determined by the *worst* “averaged” state of the main channel and the *best* “averaged” state of the eavesdropper’s channel. A similar observation has already been made for the compound wiretap channel [10], [11] with an unknown, but fixed state over time. Here, the varying nature of the channel is reflected by the presence of an “averaged” state in the equation.

Proof: The proof combines the strong typicality decoding method used by Jahn [9] to analyze arbitrarily varying channels, and the binning scheme introduced by Wyner [1] to establish the secrecy capacity of wiretap channel.

As illustrated in Figure 2, the proof relies on a *channel enhancement* argument. We assume that the eavesdropper is provided with an additional observation $(Z_{s^*})^n$, which is obtained through the discrete memoryless wiretap channel corresponding to the best state s^* defined by condition (*). That is,

$$W_{s^*}^n(\mathbf{z}|\mathbf{x}) \triangleq \prod_{i=1}^n W_{s^*}(z_i|x_i).$$

This enhancement does not affect the decoding ability of the legitimate receiver, but condition (*) and the memoryless property of the eavesdropper’s channel imply that, for any wiretap code (f, ϕ) and any state sequence $\mathbf{s} \in \mathcal{S}^n$,

$$\mathbb{I}(M; Z_{\mathbf{s}}^n) \leq \mathbb{I}(M; Z_{\mathbf{s}}^n (Z_{s^*})^n) = \mathbb{I}(M; (Z_{s^*})^n). \quad (3)$$

As a result, a randomized wiretap code achieving the secrecy rate R_s over the enhanced channel also achieves the secrecy rate R_s over the original channel; in addition, we can assume that the eavesdropper of the enhanced channel ignores $Z_{\mathbf{s}}^n$ when observing $(Z_{s^*})^n$.

We now construct and analyze a suitable randomized wiretap code for the enhanced channel. Given an input distribution $P_X(x)$ and an integer $M \cdot M_d > 0$, let the family of underlying wiretap codes be all the subsets of the set $(\mathcal{X}^n)^{M \cdot M_d}$, each consisting of a number $M \cdot M_d$ of n -length codewords $\{\mathbf{x}(i, j) : i = 1, \dots, M; j = 1, \dots, M_d\}$, i.e., distributed in M “bins” each of size M_d . Then, the *randomized wiretap code* takes each of these wiretap codes

as its “value” with probability

$$\prod_{i=1}^M \prod_{j=1}^{M_d} \prod_{q=1}^n P_X(x_{ijq}),$$

where $x_{ijq} \in \mathcal{X}$ denotes the element in the q -th position of the codeword $\mathbf{x}(i, j)$. Therefore, the randomized codewords X^n of this randomized wiretap code (F, Φ) are independent and distributed in an i.i.d fashion according to $P_X(x)$. Once the actual wiretap codebook is selected, it is revealed to the transmitter, the legitimate receiver, and the eavesdropper to play the role of the secret key which is not available to the jammer. Then, for the secure communication of the message m over the AVWTC, the encoder F chooses from the m -th bin of the selected codebook some codeword $X^n(m, m_d)$ uniformly at random, and transmits it to the legitimate receiver.

Let $\epsilon > 0$. The legitimate receiver Φ decodes his observation $Y_{\mathbf{s}}^n$ to the message (\hat{m}, \hat{m}_d) if it is the unique pair that satisfies

$$(X^n(\hat{m}, \hat{m}_d), Y_{\mathbf{s}}^n) \in \bigcup_{\bar{\mathbf{s}} \in \bar{\mathcal{S}}} T_{[X, Y_{\bar{\mathbf{s}}}]^n}(\epsilon),$$

where $T_{[X, Y_{\bar{\mathbf{s}}}]^n}(\epsilon)$ denotes the set of strongly jointly typical sequences according to the distribution $P_X(x)W_{\bar{\mathbf{s}}}(y|x)$. Such a decoding rule satisfies the requirement that the transmitter and the legitimate receiver must communicate without the knowledge of the actual state sequence \mathbf{s} : they look for strongly jointly typical sequences irrespective of the associated “averaged” state.

We also consider a *virtual decoder* Ψ who has access to the actual message (bin index) m , and based on the eavesdropping observation $Z_{\mathbf{s}}^n$ and the enhanced channel output $(Z_{s^*})^n$, tries to estimate the sequence index m_d of the transmitted codeword $X^n(m, m_d)$ within the m -th bin. Our previous discussion showed that it is sufficient for the virtual decoder to only consider the output of the enhanced channel. Therefore, the virtual decoder decides on the sequence index to be \tilde{m}_d , if this is only such index that satisfies

$$(X^n(m, \tilde{m}_d), (Z_{s^*})^n) \in T_{[X, Z_{s^*}]^n}(\epsilon),$$

where $T_{[X, Z_{s^*}]^n}(\epsilon)$ denotes the set of strongly jointly typical sequences according to the distribution $P_X(x)W_{s^*}(z|x)$.

Now, using the properties of typical sequences *under states* [9, Section III.A] and arguments similar to those in the proof of the channel coding theorem [12], one can show that the selection of the total codebook size

$$M \cdot M_d < 2^{n(\inf_{\bar{\mathbf{s}} \in \bar{\mathcal{S}}} I(X; Y_{\bar{\mathbf{s}}}) - o(\epsilon, n))} \quad (4)$$

and the bin size

$$M_d = 2^{n(I(X; Z_{s^*}) - o(\epsilon, n))} \quad (5)$$

will assure that the mean average error probabilities of both the legitimate receiver and the virtual decoder are negligible. Here, the notation $o(\epsilon, n)$ represents a sequence of real numbers satisfying $\lim_{\epsilon \rightarrow 0, n \rightarrow \infty} o(\epsilon, n) = 0$. Thus, we can

especially conclude that for any state sequence $\mathbf{s} \in \mathcal{S}^n$ and large n

$$\bar{e}^{(\text{av})}(W_{\mathbf{s}}^n, F, \Phi) \leq \epsilon.$$

For the secrecy analysis part of the proof, we note that (3) implies for any wiretap code (f, ϕ) that $L(W_{\mathbf{s}}^n, f, \phi) \leq L((W_{s^*})^n, f, \phi)$ and thus

$$L^{(\text{av})}(W_{\mathbf{s}}^n, F, \Phi) \leq L^{(\text{av})}((W_{s^*})^n, F, \Phi). \quad (6)$$

One can then use the ‘‘conditioning reduces mutual information’’ corollary of the data processing inequality [12, p. 33] with the Markov chain $M(F, \Phi) \rightarrow X^n \rightarrow (Z_{s^*})^n$ to show

$$L^{(\text{av})}((W_{s^*})^n, F, \Phi) \leq \frac{1}{n} \mathbb{I}(X^n; (Z_{s^*})^n) - \frac{1}{n} \mathbb{H}(X^n | M(F, \Phi)) + \frac{1}{n} \mathbb{H}(X^n | (Z_{s^*})^n M(F, \Phi)). \quad (7)$$

We now proceed to bound each term in (7). Since the randomized codewords are distributed i.i.d. according to $P_X(x)$, we can use the chain rule of mutual information and the memoryless property of the enhanced channel to conclude for the first term of (7) that

$$\frac{1}{n} \mathbb{I}(X^n; (Z_{s^*})^n) \leq \mathbb{I}(X; Z_{s^*}). \quad (8)$$

For the second term of (7), we have due to condition (5) on the construction of our randomized wiretap code (F, Φ) that

$$\frac{1}{n} \mathbb{H}(X^n | M(F, \Phi)) = \frac{1}{n} \mathbb{H}(M_d | M(F, \Phi)) = \mathbb{H}(X; Z_{s^*}) - o(\epsilon, n), \quad (9)$$

since the messages M and M_d , and the randomized wiretap code (F, Φ) are selected independently. Finally, the third term of (7) is bounded as follows.

$$\begin{aligned} & \frac{1}{n} \mathbb{H}(X^n | (Z_{s^*})^n M(F, \Phi)) \\ &= \frac{1}{n} \mathbb{H}(M_d | (Z_{s^*})^n M(F, \Phi)) \\ &= \frac{1}{n} \mathbb{H}(M_d | (Z_{s^*})^n M(F, \Psi)) \end{aligned} \quad (10)$$

$$\leq \frac{1}{n} [1 + \bar{e}^{(\text{av})}((W_{s^*})^n, F, \Psi) \log M_d] \quad (11)$$

$$= o(\epsilon, n). \quad (12)$$

where (10) follows since selection of the encoder F determines both the legitimate decoder Φ and the virtual decoder Ψ , (11) follows from the application of Fano’s inequality to the virtual decoder’s mean average error probability, and (12) from that being negligible due to our error probability analysis.

Substituting (8), (9), and (12) into (7), we conclude that

$$L^{(\text{av})}((W_{s^*})^n, F, \Phi) \leq o(\epsilon, n). \quad (13)$$

Taking (6) into account, (13) leads to the conclusion that for any state sequence $\mathbf{s} \in \mathcal{S}^n$ and large n

$$L^{(\text{av})}(W_{\mathbf{s}}^n, F, \Phi) \leq \epsilon.$$

Now, combining (4) and (5) with (2) establishes that all randomized-code secrecy rates R_s such that

$$R_s = \frac{1}{n} \log M < \inf_{\bar{\mathbf{s}} \in \bar{\mathcal{S}}} I(X; Y_{\bar{\mathbf{s}}}) - \sup_{\bar{\mathbf{s}} \in \bar{\mathcal{S}}} I(X; Z_{\bar{\mathbf{s}}}) \quad (14)$$

are achievable over an AVWTC satisfying the condition (*). The proof is complete, once we note that the functions $I(X; Y_{\bar{\mathbf{s}}})$ and $I(X; Z_{\bar{\mathbf{s}}})$ are continuous in the channel transition probabilities $W_{\bar{\mathbf{s}}}(y|x)$ and $W_{\bar{\mathbf{s}}}(z|x)$, respectively, and the set $\bar{\mathcal{S}}$ is compact. Hence, the operations sup and inf in (14) can be substituted by max and min, respectively. ■

Remark: One can apply a *prefix channel* argument to Theorem 1 to show that

$$\max_{p(u,x)} \left[\min_{\bar{\mathbf{s}} \in \bar{\mathcal{S}}} I(U; Y_{\bar{\mathbf{s}}}) - \max_{\bar{\mathbf{s}} \in \bar{\mathcal{S}}} I(U; Z_{\bar{\mathbf{s}}}) \right]$$

is also an achievable randomized-code secrecy rate for an AVWTC satisfying the condition (*), provided that $U \rightarrow X \rightarrow Y_{\bar{\mathbf{s}}} Z_{\bar{\mathbf{s}}}$ forms a Markov chain for all $\bar{\mathbf{s}} \in \bar{\mathcal{S}}$.

IV. UPPER BOUND FOR RANDOMIZED-CODE SECRECY CAPACITY OF AVWTC

In this section, we establish an upper bound for the randomized-code secrecy capacity of an AVWTC. The key element of the proof is the following proposition, which is the counterpart of [8, Corollary 6.3] and relates the randomized-code secrecy capacity of an AVWTC with state space \mathcal{S} to that of an AVWTC with state space $\bar{\mathcal{S}}$.

Proposition 1: The randomized-code secrecy capacity of AVWTC \mathcal{S} is equal to that of AVWTC $\bar{\mathcal{S}}$.

Proof: We know that the performance of the AVWTC \mathcal{S} under the wiretap code (f, ϕ) is characterized by the following two criteria:

$$\begin{aligned} \bar{e}(\mathcal{S}^n, f, \phi) &\triangleq \sup_{\mathbf{s} \in \mathcal{S}^n} \bar{e}(W_{\mathbf{s}}^n, f, \phi), \\ L(\mathcal{S}^n, f, \phi) &\triangleq \sup_{\mathbf{s} \in \mathcal{S}^n} L(W_{\mathbf{s}}^n, f, \phi). \end{aligned}$$

We will show that for any wiretap code (f, ϕ)

$$\begin{cases} \bar{e}(\mathcal{S}^n, f, \phi) = \bar{e}(\bar{\mathcal{S}}^n, f, \phi), \\ L(\mathcal{S}^n, f, \phi) = L(\bar{\mathcal{S}}^n, f, \phi), \end{cases} \quad (15)$$

which in turn will imply that the secrecy capacities of AVWTC’s \mathcal{S} and $\bar{\mathcal{S}}$ are equal. Notice that, because of the definitions of $\bar{e}^{(\text{av})}(W_{\mathbf{s}}^n, F, \Phi)$ and $L^{(\text{av})}(W_{\mathbf{s}}^n, F, \Phi)$, establishing (15) will also prove that

$$\begin{cases} \bar{e}^{(\text{av})}(\mathcal{S}^n, F, \Phi) = \bar{e}^{(\text{av})}(\bar{\mathcal{S}}^n, F, \Phi), \\ L^{(\text{av})}(\mathcal{S}^n, F, \Phi) = L^{(\text{av})}(\bar{\mathcal{S}}^n, F, \Phi), \end{cases}$$

and that the randomized-code secrecy capacities of AVWTC’s \mathcal{S} and $\bar{\mathcal{S}}$ are also equal.

To prove (15), let us consider the main AVC with transition probabilities $\{W_s(y|x) : s \in \mathcal{S}\}$ and the eavesdropper’s AVC with transition probabilities $\{W_s(z|x) : s \in \mathcal{S}\}$. Given any

“averaged” state sequence $\bar{\mathbf{s}} \in \bar{\mathcal{S}}^n$, it holds for the main AVC that

$$\begin{aligned} W_{\bar{\mathbf{s}}}^n(\mathbf{y}|\mathbf{x}) &= \prod_{i=1}^n W_{\bar{s}_i}(y_i|x_i) = \prod_{i=1}^n \sum_{s_i \in \mathcal{S}} p_i(s_i) W_{s_i}(y_i|x_i) \\ &= \sum_{\mathbf{s} \in \mathcal{S}^n} \prod_{i=1}^n p_i(s_i) W_{s_i}(y_i|x_i) \\ &= \sum_{\mathbf{s} \in \mathcal{S}^n} p^n(\mathbf{s}) W_{\mathbf{s}}^n(\mathbf{y}|\mathbf{x}), \end{aligned} \quad (16)$$

where we have defined

$$p^n(\mathbf{s}) \triangleq \prod_{i=1}^n p_i(s_i). \quad (17)$$

Thus, for any wiretap code (f, ϕ) and any “averaged” state sequence $\bar{\mathbf{s}}$, we have

$$\begin{aligned} \bar{e}(W_{\bar{\mathbf{s}}}^n, f, \phi) &= \frac{1}{M} \sum_{m \in \mathcal{M}} W_{\bar{\mathbf{s}}}^n \left((\phi^{-1}(m))^c | f(m) \right) \\ &= \frac{1}{M} \sum_{m \in \mathcal{M}} \sum_{\mathbf{s} \in \mathcal{S}^n} p^n(\mathbf{s}) W_{\mathbf{s}}^n \left((\phi^{-1}(m))^c | f(m) \right) \\ &= \sum_{\mathbf{s} \in \mathcal{S}^n} p^n(\mathbf{s}) \bar{e}(W_{\mathbf{s}}^n, f, \phi) \\ &\leq \sup_{\mathbf{s} \in \mathcal{S}^n} \bar{e}(W_{\mathbf{s}}^n, f, \phi) = \bar{e}(\mathcal{S}^n, f, \phi). \end{aligned}$$

Therefore,

$$\bar{e}(\bar{\mathcal{S}}^n, f, \phi) \leq \bar{e}(\mathcal{S}^n, f, \phi).$$

The reverse inequality $\bar{e}(\bar{\mathcal{S}}^n, f, \phi) \geq \bar{e}(\mathcal{S}^n, f, \phi)$ is obvious, since $\mathcal{S}^n \subseteq \bar{\mathcal{S}}^n$. This completes the proof of the first assertion of (15). Now, notice that, similarly to (16), one can show that

$$P_{Z_{\bar{\mathbf{s}}}^n | M}(\mathbf{z}|m) = \sum_{\mathbf{s} \in \mathcal{S}^n} p^n(\mathbf{s}) P_{Z_{\mathbf{s}}^n | M}(\mathbf{z}|m), \quad (18)$$

where $p^n(\mathbf{s})$ was defined in (17). According to (18) and the convexity of the mutual information in the transition probability, Jensen’s inequality implies for any “averaged” state sequence $\bar{\mathbf{s}} \in \bar{\mathcal{S}}^n$ that

$$\begin{aligned} L(W_{\bar{\mathbf{s}}}^n, f, \phi) &= \frac{1}{n} \mathbb{I}(M; Z_{\bar{\mathbf{s}}}^n) \leq \sum_{\mathbf{s} \in \mathcal{S}^n} p^n(\mathbf{s}) \cdot \frac{1}{n} \mathbb{I}(M; Z_{\mathbf{s}}^n) \\ &\leq \sup_{\mathbf{s} \in \mathcal{S}^n} \frac{1}{n} \mathbb{I}(M; Z_{\mathbf{s}}^n) = L(\mathcal{S}^n, f, \phi). \end{aligned}$$

Hence,

$$L(\bar{\mathcal{S}}^n, f, \phi) \leq L(\mathcal{S}^n, f, \phi).$$

The reverse inequality $L(\bar{\mathcal{S}}^n, f, \phi) \geq L(\mathcal{S}^n, f, \phi)$ is again obvious, since $\mathcal{S}^n \subseteq \bar{\mathcal{S}}^n$. This establishes the second assertion of (15), and completes the proof of the theorem. \blacksquare

We are now ready to prove the following theorem, which generalizes for AVWTC the “degraded-same-marginal” bound on the secrecy capacity of the compound wiretap channel [13].

Theorem 2: The randomized-code secrecy capacity of the AVWTC $\mathcal{W} = \{W(y, z|x) : s \in \mathcal{S}\}$ is upper bounded by

$$\hat{C}_s \leq \max_{P_X(x)} \min_{\bar{\mathbf{s}} \in \bar{\mathcal{S}}} \mathbb{I}(X; Y_{\bar{\mathbf{s}}} | Z_{\bar{\mathbf{s}}}).$$

Proof: Assume R_s is an achievable randomized-code secrecy rate for AVWTC \mathcal{S} . Then, by Proposition 1, R_s is also an achievable randomized-code secrecy rate for AVWTC $\bar{\mathcal{S}}$. Thus, for any given $\epsilon' > 0$, an $(n, 2^{nR_s})$ randomized wiretap code (F, Φ) exists for AVWTC $\bar{\mathcal{S}}$, such that for any message M drawn uniformly at random from \mathcal{M} and for all “averaged” state sequences $\bar{\mathbf{s}} \in \bar{\mathcal{S}}^n$

$$\mathbb{E}_{(F, \Phi)} [\Pr(\Phi(Y_{\bar{\mathbf{s}}}^n) \neq M | F(M))] \leq \epsilon', \quad (19)$$

$$\frac{1}{n} \mathbb{I}(M; Z_{\bar{\mathbf{s}}}^n | (F, \Phi)) \leq \epsilon'. \quad (20)$$

Then, (19) implies by Fano’s inequality that for all “averaged” state sequences $\bar{\mathbf{s}} \in \bar{\mathcal{S}}^n$

$$\frac{1}{n} \mathbb{H}(M | Y_{\bar{\mathbf{s}}}^n(F, \Phi)) \leq \frac{1}{n} + R_s \epsilon'. \quad (21)$$

Moreover, we can conclude from (20) that for all “averaged” state sequences $\bar{\mathbf{s}} \in \bar{\mathcal{S}}^n$ and large n

$$\begin{aligned} \frac{1}{n} \mathbb{H}(M | Z_{\bar{\mathbf{s}}}^n(F, \Phi)) &= \frac{1}{n} \mathbb{H}(M | (F, \Phi)) - \frac{1}{n} \mathbb{I}(M; Z_{\bar{\mathbf{s}}}^n | (F, \Phi)) \\ &\geq R_s - \epsilon'. \end{aligned} \quad (22)$$

Now, for any arbitrary “averaged” state $\bar{\mathbf{s}} \in \bar{\mathcal{S}}$, let the “averaged” state sequence be $\bar{\mathbf{s}} = (\bar{s}, \bar{s}, \dots, \bar{s}) \in \bar{\mathcal{S}}^n$. Combining (21) and (22) yields for such an “averaged” state sequence and $\epsilon \triangleq \frac{1}{n} + (1 + R_s) \epsilon'$ that

$$\begin{aligned} R_s &\leq \frac{1}{n} \mathbb{H}(M | Z_{\bar{\mathbf{s}}}^n(F, \Phi)) - \frac{1}{n} \mathbb{H}(M | Y_{\bar{\mathbf{s}}}^n(F, \Phi)) + \epsilon \\ &\leq \frac{1}{n} \mathbb{H}(M | Z_{\bar{\mathbf{s}}}^n(F, \Phi)) - \frac{1}{n} \mathbb{H}(M | Y_{\bar{\mathbf{s}}}^n Z_{\bar{\mathbf{s}}}^n(F, \Phi)) + \epsilon \\ &= \frac{1}{n} \mathbb{I}(M; Y_{\bar{\mathbf{s}}}^n | Z_{\bar{\mathbf{s}}}^n(F, \Phi)) + \epsilon \\ &\leq \frac{1}{n} \mathbb{I}(M X^n; Y_{\bar{\mathbf{s}}}^n | Z_{\bar{\mathbf{s}}}^n(F, \Phi)) + \epsilon \\ &= \frac{1}{n} \mathbb{I}(X^n; Y_{\bar{\mathbf{s}}}^n | Z_{\bar{\mathbf{s}}}^n(F, \Phi)) + \frac{1}{n} \mathbb{I}(M; Y_{\bar{\mathbf{s}}}^n | X^n Z_{\bar{\mathbf{s}}}^n(F, \Phi)) + \epsilon \\ &\leq \frac{1}{n} \mathbb{I}(X^n; Y_{\bar{\mathbf{s}}}^n | Z_{\bar{\mathbf{s}}}^n) + \epsilon \end{aligned} \quad (23)$$

$$\leq \frac{1}{n} \sum_{i=1}^n \mathbb{I}(X_i; Y_{\bar{s}_i} | Z_{\bar{s}_i}) + \epsilon \quad (24)$$

$$= \mathbb{I}(X_Q; Y_{\bar{s}_Q} | Z_{\bar{s}_Q} Q) + \epsilon \quad (25)$$

$$\leq \mathbb{I}(X; Y_{\bar{s}} | Z_{\bar{s}}) + \epsilon, \quad (26)$$

where (23) follows from the “conditioning reduces mutual information” corollary of the data processing inequality [12, p. 33] with the Markov chain $(F, \Phi) \rightarrow X^n Z_{\bar{\mathbf{s}}}^n \rightarrow Y_{\bar{\mathbf{s}}}^n$ which is itself implied by the Markov chain $M(F, \Phi) \rightarrow X^n \rightarrow Y_{\bar{\mathbf{s}}}^n Z_{\bar{\mathbf{s}}}^n$ and also from $\mathbb{I}(M; Y_{\bar{\mathbf{s}}}^n | X^n Z_{\bar{\mathbf{s}}}^n(F, \Phi)) = 0$ due to the Markov chain $M \rightarrow (F, \Phi) X^n Z_{\bar{\mathbf{s}}}^n \rightarrow Y_{\bar{\mathbf{s}}}^n$ which is itself implied again by the Markov chain $M(F, \Phi) \rightarrow X^n \rightarrow Y_{\bar{\mathbf{s}}}^n Z_{\bar{\mathbf{s}}}^n$. Additionally, (24) follows from the chain rule of mutual information and the memoryless property of the AVWTC, (25) from the definition of the time-sharing random variable Q uniformly over the set $\{1, \dots, n\}$ and independent of all other random variables, and (26) again from the “conditioning reduces mutual information” corollary of the data processing inequality [12, p. 33] with the

Markov chain $Q \rightarrow X_{\bar{s}_Q} Z_{\bar{s}_Q} \rightarrow Y_{\bar{s}_Q}$ (a consequence of $Q \rightarrow X_Q \rightarrow Y_{\bar{s}_Q} Z_{\bar{s}_Q}$) and also from the definition of new random variables

$$X \triangleq X_Q, \quad Y_{\bar{s}} \triangleq Y_{\bar{s}_Q}, \quad Z_{\bar{s}} \triangleq Z_{\bar{s}_Q}, \quad (27)$$

which satisfy the same probability distribution $W_{\bar{s}}(y, z|x)$ as the original one in the AVWTC $\bar{\mathcal{S}}$ since the ‘‘averaged’’ state \bar{s} is assumed to be fixed all over the time.

Since the choice of the ‘‘averaged’’ state $\bar{s} \in \bar{\mathcal{S}}$ has been arbitrary, we conclude that for any input distribution X

$$R_s \leq \min_{\bar{s} \in \bar{\mathcal{S}}} \mathbb{I}(X; Y_{\bar{s}} | Z_{\bar{s}}).$$

Note that we have used \min instead of \inf , since the function $\mathbb{I}(X; Y_{\bar{s}} | Z_{\bar{s}})$ is continuous in \bar{s} and the set $\bar{\mathcal{S}}$ is compact. This completes the proof. \blacksquare

An immediate consequence of Theorem 2 is that if the AVWTC is *reversely degraded*, i.e., the Markov chain $X \rightarrow Z_{\bar{s}} \rightarrow Y_{\bar{s}}$ holds, for *even a single ‘‘averaged’’ state* $\bar{s} \in \bar{\mathcal{S}}$, then the randomized-code secrecy capacity is zero. This suggests that the introduction of a jammer with arbitrary active attacks to the wiretap channel tremendously decreases the possibility of secure communication. The following examples illustrate this idea.

Example 1: Consider the *deterministic* AVWTC defined by $\mathcal{X} = \mathcal{S} = \mathcal{Z} = \{0, 1\}$, $\mathcal{Y} = \{0, 1, 2\}$, and the two AVC’s $Y = X + S$ and $Z = X \oplus S$. One can easily show that the randomized-code capacity of the main AVC is $\frac{1}{2}$ and that of the eavesdropper’s AVC is zero. However, the randomized-code secrecy capacity of the AVWTC is zero, since Theorem 2 implies

$$\hat{C}_s \leq \max_{P_X(x)} \mathbb{I}(X; Y_{\bar{s}} | Z_{\bar{s}})_{|\bar{s}=0} = \max_{P_X(x)} \mathbb{I}(X; X|X) = 0,$$

which is an intuitive result since in the state $s = 0$, both the legitimate receiver and the eavesdropper observe the actual input X .

Example 2: Let $\text{BSC}(p)$ denote a binary symmetric channel with crossover probability p . Now, assume that for an AVWTC, we have $\mathcal{X} = \mathcal{Y} = \mathcal{Z} = \{0, 1\}$, and the state space is the set of natural number, i.e., $\mathcal{S} = \mathbb{N}$. Let the main AVC be a noiseless binary channel, i.e., $\{\text{BSC}(0)\}_{s \in \mathcal{S}}$, and the eavesdropper’s AVC be $\{\text{BSC}(\frac{1}{2s})\}_{s \in \mathcal{S}}$. The randomized-code capacity of the main channel is 1 and that of the eavesdropper’s channel is zero; however, the randomized-code secrecy capacity of the AVWTC is zero, since Theorem 2 implies for the ‘‘averaged’’ state $\bar{s} = \infty \notin \mathcal{S}$ that

$$\hat{C}_s \leq \max_{P_X(x)} \mathbb{I}(X; Y_{\bar{s}} | Z_{\bar{s}})_{|\bar{s}=\infty} = \max_{P_X(x)} \mathbb{I}(X; X|X) = 0.$$

V. THE STRONGLY DEGRADED AVWTC WITH INDEPENDENT STATES

In this section, we introduce a special class of AVWTC’s for which our lower and upper bounds match and the randomized-code secrecy capacity is obtained.

A broadcast (and specially a wiretap) AVC with state space \mathcal{S} is called *degraded* if the Markov chain $X \rightarrow Y_s \rightarrow Z_s$

holds for all states $s \in \mathcal{S}$ [9]. Jahn observed that the convex closure of a degraded broadcast AVC usually fails to be a degraded broadcast AVC [9]. Thus, we need a stronger definition of degradedness. We define an AVWTC (or generally a broadcast AVC) with state space \mathcal{S} to be *strongly degraded* if the Markov chain $X \rightarrow Y_{\bar{s}} \rightarrow Z_{\bar{s}}$ is satisfied for all ‘‘averaged’’ states $\bar{s} \in \bar{\mathcal{S}}$.

A broadcast AVC *with independent states* [9] is another special class of broadcast AVC’s, for which the state of the main channel s_y and that of the eavesdropper’s channel s_z are independently selected from the corresponding state spaces \mathcal{S}_y and \mathcal{S}_z , respectively. The state of the channel is then described by the pair $s = (s_y, s_z)$ as an element of the state space $\mathcal{S} = \mathcal{S}_y \times \mathcal{S}_z$.

Combining these two concepts, we can now define the special class of our interest. An AVWTC \mathcal{S} is called *strongly degraded with independent states* if (i) the state space is decomposed as $\mathcal{S} = \mathcal{S}_y \times \mathcal{S}_z$ where the state of the main channel $s_y \in \mathcal{S}_y$ and that of the eavesdropper’s channel $s_z \in \mathcal{S}_z$ are independently selected and (ii) the Markov chain

$$X \rightarrow Y_{\bar{s}_y} \rightarrow Z_{\bar{s}_z}$$

is satisfied for all ‘‘averaged’’ states $\bar{s}_y \in \bar{\mathcal{S}}_y$ and $\bar{s}_z \in \bar{\mathcal{S}}_z$. The following theorem presents the randomized-code secrecy capacity of this special class of AVWTC’s.

Theorem 3: The randomized-code secrecy capacity of a strongly degraded AVWTC with independent states is

$$\hat{C}_s = \max_{P_X(x)} \left[\min_{\bar{s}_y \in \bar{\mathcal{S}}_y} \mathbb{I}(X; Y_{\bar{s}_y}) - \max_{\bar{s}_z \in \bar{\mathcal{S}}_z} \mathbb{I}(X; Z_{\bar{s}_z}) \right],$$

provided that the AVWTC satisfies the condition (*).

Proof: According to Theorem 1, we know that all randomized-code secrecy rates

$$R_s < \max_{P_X(x)} \left[\min_{\bar{s} \in \bar{\mathcal{S}}} \mathbb{I}(X; Y_{\bar{s}}) - \max_{\bar{s} \in \bar{\mathcal{S}}} \mathbb{I}(X; Z_{\bar{s}}) \right]$$

are achievable for an AVWTC satisfying the condition (*). Since the AVWTC has independent states, the term $\min_{\bar{s} \in \bar{\mathcal{S}}} \mathbb{I}(X; Y_{\bar{s}})$ does not depend on \bar{s}_z , and the term $\max_{\bar{s} \in \bar{\mathcal{S}}} \mathbb{I}(X; Z_{\bar{s}})$ does not depend on \bar{s}_y . Therefore,

$$\hat{C}_s \geq \max_{P_X(x)} \left[\min_{\bar{s}_y \in \bar{\mathcal{S}}_y} \mathbb{I}(X; Y_{\bar{s}_y}) - \max_{\bar{s}_z \in \bar{\mathcal{S}}_z} \mathbb{I}(X; Z_{\bar{s}_z}) \right]. \quad (28)$$

On the other hand, since the AVWTC is strongly degraded, Theorem 2 implies that

$$\hat{C}_s \leq \max_{P_X(x)} \min_{\bar{s} \in \bar{\mathcal{S}}} [\mathbb{I}(X; Y_{\bar{s}}) - \mathbb{I}(X; Z_{\bar{s}})].$$

Taking again into account that the AVWTC has independent states, we obtain

$$\hat{C}_s \leq \max_{P_X(x)} \left[\min_{\bar{s}_y \in \bar{\mathcal{S}}_y} \mathbb{I}(X; Y_{\bar{s}_y}) - \max_{\bar{s}_z \in \bar{\mathcal{S}}_z} \mathbb{I}(X; Z_{\bar{s}_z}) \right]. \quad (29)$$

Combining (28) and (29) proves the theorem. \blacksquare

In the following, we give an example for this special class of AVWTC’s.

Example 3: Denote again by $\text{BSC}(p)$ a binary symmetric channel with crossover probability p . Now, consider an

AVWTC defined by $\mathcal{X} = \mathcal{Y} = \mathcal{Z} = \mathcal{S}_y = \mathcal{S}_z = \{0, 1\}$, the main AVC $\{\text{BSC}(\frac{1}{6}), \text{BSC}(\frac{1}{5})\}$, and the eavesdropper's AVC $\{\text{BSC}(\frac{1}{4}), \text{BSC}(\frac{1}{3})\}$, where the first elements correspond to the state $s = 0$, the second elements correspond to the state $s = 1$, and the states are selected independently for each AVC. One can easily verify that the randomized-code capacity of the main AVC is $\hat{C}_m = 1 - H_b(\frac{1}{5})$, and that of the eavesdropper's AVC is $\hat{C}_e = 1 - H_b(\frac{1}{3})$, where $H_b(\cdot)$ is again the binary entropy function. Also, it is easy to check that the AVWTC is strongly degraded and the condition (*) is satisfied. Therefore, Theorem 3 gives the randomized-code secrecy capacity of AVWTC as $\hat{C}_s = H_b(\frac{1}{4}) - H_b(\frac{1}{5})$. This is an intuitive result, since $\text{BSC}(\frac{1}{5})$ is the *worst* "averaged" main channel, and $\text{BSC}(\frac{1}{4})$ is the *best* "averaged" eavesdropper's channel. Additionally, notice that the randomized-code secrecy capacity of the AVWTC is less than the difference of the randomized-code capacities of the main and eavesdropper's channels.

VI. CONCLUSIONS AND FUTURE WORK

We have characterized bounds for the randomized-code secrecy capacity of (a class of) arbitrarily varying wiretap channels, which show that active attacks have a significant impact on secure communications. Since our model can be viewed as the resulting combination of modulation and demodulation schemes for a waveform channel, this suggests that the implementation of modulation schemes resistant to jamming is critical to enable secure communication.

At this stage, our results lack operational significance because randomized coding presupposes the existence of a source of randomness common to the transmitter, the receiver, and the eavesdropper; however, the code-reduction argument of Ahlswede [7] can be adapted to obtain results without randomization. In future work, we will also consider the generalization of our lower bound to all arbitrarily varying wiretap channels.

REFERENCES

- [1] A.D. Wyner, *The Wire-Tap Channel*, The Bell Systems Technical Journal, vol. 54, no. 8, pp. 1355-1387, 1975.
- [2] I. Csiszár and J. Körner, *Broadcast Channels with Confidential Messages*, IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 339-348, 1978.
- [3] U. Maurer and S. Wolf, *Secret-Key Agreement over Unauthenticated Public Channels I: Definitions and a Completeness Result*, IEEE Transactions on Information Theory, vol. 49, no. 4, pp. 822-831, 2003.
- [4] L. Lai, H. El Gamal, and H.V. Poor, *Authentication over Noisy Channels*, IEEE Transactions on Information Theory, vol. 55, no. 2, pp. 906-916, 2009.
- [5] V. Aggarwal, L. Lai, A.R. Calderbank, and H.V. Poor, *Wiretap Channel Type II with an Active Eavesdropper*, in Proc. of IEEE International Symposium on Information Theory, Seoul, Korea, 2009, pp. 1944-1948.
- [6] D. Blackwell, L. Breiman, and A.J. Thomasian, *The Capacities of Certain Channel Classes under Random Coding*, The Annals of Mathematical Statistics, vol. 31, no. 3, pp. 558-567, 1960.
- [7] R. Ahlswede, *Elimination of Correlation in Random Codes for Arbitrarily Varying Channels*, Probability Theory and Related Fields, vol. 44, no. 2, pp. 159-175, 1978.
- [8] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, New York: Academic, 1981.
- [9] J.-H. Jahn, *Coding of Arbitrarily Varying Multiuser Channels*, IEEE Transactions on Information Theory, vol. 27, no. 2, pp. 212-226, 1981.
- [10] Y. Liang, G. Kramer, H.V. Poor, and S. Shamai (Shitz), *Compound Wire-Tap Channels*, in Proc. 45th Annual Allerton Conference on Communications Control and Computing, Monticello, IL, USA, 2007, pp. 136-143.
- [11] M. Bloch and J.N. Laneman, *On the Secrecy Capacity of Arbitrary Wiretap Channels*, in Proc. 46th Annual Allerton Conference on Communications Control and Computing, Monticello, IL, USA, 2008, pp. 818-825.
- [12] T.M. Cover and J.A. Thomas, *Elements of Information Theory*, New York: Wiley, 1991.
- [13] T. Liu, V. Prabhakaran, and S. Vishwanath, *The Secrecy Capacity of a Class of Parallel Gaussian Compound Wiretap Channels*, in Proc. IEEE International Symposium on Information Theory, Toronto, Canada, 2008, pp. 116-120.