Capacity Results and Super-Activation for Wiretap Channels With Active Wiretappers

Holger Boche, *Fellow, IEEE*, and Rafael F. Schaefer, *Member, IEEE*

***Abstract*—The classical wiretap channel models secure communication in the presence of a nonlegitimate wiretapper who has to be kept ignorant. Traditionally, the wiretapper is passive in the sense that he only tries to eavesdrop the communication using his received channel output. In this paper, more powerful *active wiretappers* are studied. In addition to eavesdropping, these wiretappers are able to influence the communication conditions of all users by controlling the corresponding channel states. Since legitimate transmitters and receivers do not know the actual channel realization or the wiretapper's strategy of influencing the channel states, they are confronted with arbitrarily varying channel (AVC) conditions. The corresponding secure communication scenario is, therefore, given by the *arbitrarily varying wiretap channel (AVWC)*. In the context of AVCs, common randomness (CR) has been shown to be an important resource for establishing reliable communication, in particular, if the AVC is symmetrizable. But availability of CR also affects the strategy space of an active wiretapper as he may or may not exploit the common randomness for selecting the channel states. Several secrecy capacity results are derived for the AVWC. In particular, the CR-assisted secrecy capacity of the AVWC with an active wiretapper exploiting CR is established and analyzed in detail. Finally, it is demonstrated for active wiretappers how two orthogonal AVWCs, each *useless* for transmission of secure messages, can be super-activated to a *useful* channel allowing for secure communication at nonzero secrecy rates. To the best of our knowledge, this is not possible for passive wiretappers and, further, provides the first example of such super-activation, which has been expected to appear only in the area of quantum communication. Such knowledge is particularly important as it provides valuable insights for the design and the medium access control of future wireless communication systems.**

***Index Terms*—Wiretap channel, secrecy capacity, strong secrecy, arbitrarily varying channel, common randomness, active wiretapper, super-activation, embedded security, medium access control in secure communication systems.**

I. Introduction

RAPID developments in communication systems make information available almost everywhere. Along with this, the security of sensitive information from unauthorized access becomes an important task and a common approach is the use of cryptographic techniques to keep information secret. Such techniques have a wide variety of use and are based on the assumption of insufficient computational capabilities of nonlegitimate receivers. Due to the increase in computational power, improved algorithms, and recent advances in number theory, these techniques are becoming more and more insecure.

Wireless communication systems are inherently vulnerable for eavesdropping due to the open nature of the wireless medium. The physical properties of the wireless channel make the communication easily accessible to external wiretappers but, on the other hand, also offer possibilities to establish security by other approaches than cryptographic techniques.

In this context, the concept of information theoretic, or physical layer, security is becoming more and more attractive, since it solely uses the physical properties of the wireless channel in order to establish security. Information theoretic security was initiated by Wyner, who introduced the *wiretap channel* [1]. This is the simplest scenario involving security with one legitimate transmitter-receiver pair and one wiretapper to be kept ignorant. Recently, there is growing interest in information theoretic security as it provides a promising approach to embed secure communication in wireless networks; for instance see [2]–[5] and references therein. Along with this, the concept of *physical layer service integration* becomes more and more important [6].

All these previous studies have one thing in common: the wiretapper is usually assumed to be *passive* in the sense that he (or she) simply tries to eavesdrop upon the communication and to infer the confidential information by only using his received channel output. This scenario is briefly reviewed in Section II. In contrast to that, we consider in this paper more powerful wiretappers which are able to maliciously influence the channel conditions of all users. Since legitimate transmitter and receiver have no knowledge about how such an *active* wiretapper will influence the channel conditions, they have to be prepared for the worst, i.e., a channel which may vary in an unknown and arbitrary manner from channel use to channel use.

The concept of arbitrarily varying channels (AVC) [7]–[9] is a suitable model to capture the effects of such unknown varying channel conditions. Accordingly, the communication problem at hand is given by the corresponding *arbitrarily varying wiretap channel (AVWC)* with active wiretapper, which is introduced in Section III.

In the context of AVCs, it has been shown that *common randomness (CR)* is an important and often necessary resource for reliable communication over arbitrarily varying channels [7]–[9]. The availability of common randomness allows legitimate users to use more sophisticated, CR-assisted strategies

Manuscript received December 21, 2012; revised April 15, 2013 and July 17, 2013; accepted July 24, 2013. Date of publication August 01, 2013; date of current version August 15, 2013. This work was supported in part by the German Ministry of Education and Research (BMBF) under Grant 01BQ1050, and in part by the German Research Foundation (DFG) under Grant BO 1734/25-1. This work was presented in part at IEEE-WIFS, Tenerife, Spain, December 2012, and in part at the IEEE-ISIT, Istanbul, Turkey, July 2013. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Sviatoslav Slava Voloshynovskiy.

The authors are with the Lehrstuhl für Theoretische Informationstechnik, Technische Universität München, Munich 80290, Germany (e-mail: boche@tum.de; rafael.schaefer@tum.de).

Digital Object Identifier 10.1109/TIFS.2013.2276049

by coordinating their choice of encoder and decoder. But it also paves the way for more powerful wiretappers. An active wiretapper may or may not exploit the available common randomness for controlling the channel states.

Thus, this immediately defines different classes of attacks against which the communication should be protected. Section IV deals with *active wiretappers* who do not exploit available common randomness. First studies for the corresponding AVWC with active wiretapper can be found in [10], [11], where the latter use the *strong secrecy criterion* [12], [13]. In this paper, the main objective is the analysis of *active wiretappers exploiting CR*. This is done in Section V where the corresponding CR-assisted secrecy capacity of the AVWC with active wiretapper exploiting CR is analyzed in detail.

For wireless communication systems, it is important to understand how the overall performance of the system is determined. For example, the capacity of an OFDM system is given by the sum of the capacities of all subchannels. In particular, if two useless channels with zero capacity are used in an orthogonal way, the overall capacity of the system is still zero. In Section VI we use the previously developed theory to show that two orthogonal AVWCs, each useless for themselves in the sense that it has zero secrecy capacity, can be used together to super-activate the whole system to allow for secure communication at positive secrecy rates. This shows that the world view of classical additivity of orthogonal resources does not hold anymore (in the sense that "$0+0>0$") if secrecy requirements are imposed. We note that such phenomena as the aforementioned *super-activation* only appear for active wiretappers and are not possible for passive wiretappers. Until now, such effects have been observed only for quantum communication systems. To the best of our knowledge, this is the first example that the phenomenon of super-activation is observed for classical communication systems as well. Finally, the paper ends with a conclusion in Section VII.

Notation

Discrete random variables are denoted by capital letters and their realizations and ranges by lower case and script letters; $\mathbb{N}$ and $\mathbb{R}_+$ are the sets of positive integers and nonnegative real numbers; $I(\cdot;\cdot)$ and $H_2(\,\cdot\,)$ are the mutual information and the binary entropy; $X-Y-Z$ denotes a Markov chain of random variables X, Y, and Z in this order; all logarithms, exponentials, and information quantities are taken to the base 2; $\mathcal{P}(\,\cdot\,)$ is the set of all probability distributions and $(\,\cdot\,)^c$ is the complement of a set; $\mathbb{E}[\cdot]$ and $\mathbb{P}\{\cdot\}$ denote the expectation and probability; $\mathrm{lhs} := \mathrm{rhs}$ assigns the value of the right hand side (rhs) to the left hand side (lhs).

II. Classical Wiretap Channel

First, we briefly state the key ideas and main results for the classical wiretap channel. In this scenario, the wiretapper is assumed to be *passive* in the sense that he simply tries to eavesdrop upon the communication and to infer the confidential information by using only its received channel output.

Therefore we start with some basic definitions. Let $\mathcal{X}$ and $\mathcal{Y}, \mathcal{Z}$ be finite input and output sets. Then the channels $W: \mathcal{X} \to \mathcal{P}(\mathcal{Y})$ and $V: \mathcal{X} \to \mathcal{P}(\mathcal{Z})$ represent the communication links to the legitimate receiver and the wiretapper. For input and output sequences $x^n \in \mathcal{X}^n$ and $y^n \in \mathcal{Y}^n, z^n \in \mathcal{Z}^n$ of block length n, the discrete memoryless channels are given by $W^n(y^n\,|\,x^n) := \prod_{i=1}^n W(y_i\,|\,x_i)$ and $V^n(z^n\,|\,x^n) := \prod_{i=1}^n V(z_i\,|\,x_i)$. The *wiretap channel with passive wiretapper* is given by the pair of channels $\{W, V\}$ with common input.[1]

The task is now to establish a reliable communication between the transmitter and the legitimate receiver and, at the same time, to keep the confidential information secret from the passive wiretapper. This is formalized as follows.

Definition 1: An (n, J_n)*-code* $\mathcal{C}$ for the wiretap channel consists of a stochastic encoder

$$E: \mathcal{J}_n \to \mathcal{P}(\mathcal{X}^n), \tag{1}$$

i.e., a stochastic matrix, with a set of messages $\mathcal{J}_n := \{1, \dots, J_n\}$ and a decoder $\varphi: \mathcal{Y}^n \to \mathcal{J}_n$ given by a collection of disjoint decoding sets

$$\{\mathcal{D}_j \subset \mathcal{Y}^n : j \in \mathcal{J}_n\}.$$

Then for an (n, J_n)-code $\mathcal{C}$, the average probability of decoding error at the legitimate receiver is given by $\bar{e}_n(\mathcal{C}) := \frac{1}{|\mathcal{J}_n|}\sum_{j\in\mathcal{J}_n}\sum_{x^n\in\mathcal{X}^n} W^n(\mathcal{D}_j^c\,|\,x^n)E(x^n\,|\,j)$.

To keep the message secret from the wiretapper, we further require $I(J; Z^n\,|\,\mathcal{C}) \leq \epsilon_n$ for some (small) $\epsilon_n > 0$ with J the random variable uniformly distributed over the set of messages $\mathcal{J}_n$ and $Z^n = (Z_1, Z_2, \dots, Z_n)$ the channel output at the wiretapper. This criterion is known as *strong secrecy* [12], [13].

Definition 2: A nonnegative number R_S is an *achievable secrecy rate* for the wiretap channel with passive wiretapper if for all $\delta > 0$ there is an $n(\delta) \in \mathbb{N}$ and a sequence (n, J_n)-codes $\mathcal{C}$ such that for all $n \geq n(\delta)$ we have $\frac{1}{n}\log J_n \geq R_S - \delta$ and $I(J; Z^n\,|\,\mathcal{C}) \leq \epsilon_n$ and $\bar{e}_n(\mathcal{C}) \leq \lambda_n$ while $\epsilon_n, \lambda_n \to 0$ as $n \to \infty$. The *secrecy capacity* C_S is given by the supremum of all achievable secrecy rates R_S.

The discrete memoryless wiretap channel with passive wiretapper is well studied under several aspects and its secrecy capacity can be found for instance in [1], [12]–[14].

Theorem 1: The secrecy capacity C_S of the wiretap channel with passive wiretapper is

$$C_S = \max_{Q-X-(Y,Z)}\big(I(Q;Y) - I(Q;Z)\big)$$

where the random variables $Q - X - (Y, Z)$ form a Markov chain.

Remark 1: For the wiretap channel it turns out that stochastic encoding, cf. (1), is crucial to keep the wiretapper ignorant of the transmitted message and, therefore, to achieve the secrecy capacity. This is in contrast to the point-to-point link without any secrecy requirements, where deterministic encoding suffices to achieve the capacity.

[1] Note that it is sufficient to consider the marginal transition probabilities W and V only as the secrecy capacity depends only the marginal channels to the legitimate receiver and the wiretapper. In particular, two wiretap channels with different joint probability distributions $P_{YZ\,|\,X}: \mathcal{X} \to \mathcal{P}(\mathcal{Y}\times\mathcal{Z})$ and $\tilde{P}_{YZ\,|\,X}: \mathcal{X} \to \mathcal{P}(\mathcal{Y}\times\mathcal{Z})$ have the same secrecy capacity if they have the same marginal probability distributions $P_{Y\,|\,X}: \mathcal{X} \to \mathcal{P}(\mathcal{Y})$ and $P_{Z\,|\,X}: \mathcal{X} \to \mathcal{P}(\mathcal{Z})$, cf. [2, Lemma 2.1].

III. Arbitrarily Varying Wiretap Channels

A passive wiretapper does not influence the channel conditions of the legitimate users and, accordingly, simply tries to eavesdrop upon the communication. In contrast to that, we consider in this paper more powerful wiretappers which are further able to control the channel states of all users. To model such an *active* wiretapper, we introduce a function $f \in \mathcal{A}$, where f characterizes a certain strategy and $\mathcal{A}$ denotes the set of all possible active strategies of the wiretapper.

Since the legitimate users have no knowledge about how the active wiretapper will choose his strategy f and, thus, how he will influence the channel conditions, they have to be prepared for the worst, i.e., a channel which may vary in an unknown and arbitrary manner from channel use to channel use.

A. Arbitrarily Varying Channels as a Model for Active Wiretappers

The concept of arbitrarily varying channels [7]–[9] is a suitable model to capture the aforementioned effects. To model the unknown varying channel states, we introduce a finite state set $\mathcal{S}$. Then the communication links to the legitimate receiver and the wiretapper are given by $W : \mathcal{X} \times \mathcal{S} \to \mathcal{P}(\mathcal{Y})$ and $V : \mathcal{X} \times \mathcal{S} \to \mathcal{P}(\mathcal{Z})$ respectively. For given state sequence $s^n = (s_1, s_2, \dots, s_n) \in \mathcal{S}^n$ of length n, the discrete memoryless channel to the legitimate receiver is given by

$$W^n(y^n \,|\, x^n, s^n) := \prod_{i=1}^{n} W(y_i \,|\, x_i, s_i) \tag{2}$$

for all $y^n \in \mathcal{Y}^n$ and $x^n \in \mathcal{X}^n$. Then the *arbitrarily varying channel (AVC)* $\mathcal{W}$ to the legitimate receiver is given by the family of channels for all state sequences $s^n \in \mathcal{S}^n$, i.e.,

$$\mathcal{W} := \{W^n(\cdot \,|\, \cdot, s^n) : s^n \in \mathcal{S}^n\}. \tag{3}$$

Further, for any probability distribution $\rho \in \mathcal{P}(\mathcal{S})$ we define the *averaged channel* to the legitimate receiver as

$$W_\rho(y \,|\, x) = \sum_{s \in \mathcal{S}} W(y \,|\, x, s)\rho(s). \tag{4}$$

Similarly, for the channel to the wiretapper, we define for given state sequence $s^n \in \mathcal{S}^n$ the discrete memoryless channel as $V^n(z^n \,|\, x^n, s^n) := \prod_{i=1}^{n} V(z_i \,|\, x_i, s_i)$ for all $z^n \in \mathcal{Z}^n$ and $x^n \in \mathcal{X}^n$, and, accordingly, $\mathcal{V} := \{V^n(\cdot \,|\, \cdot, s^n) : s^n \in \mathcal{S}^n\}$ and $V_\rho(z \,|\, x) = \sum_{s \in \mathcal{S}} V(z \,|\, x, s)\rho(s)$ for $\rho \in \mathcal{P}(\mathcal{S})$.

Definition 3: The *arbitrarily varying wiretap channel (AVWC)* $\mathfrak{W}$ *with active wiretapper* is given by the families of pairs of channels with common input as

$$\mathfrak{W} := \{(W^n(\cdot \,|\, \cdot, s^n), V^n(\cdot \,|\, \cdot, s^n)) : s^n \in \mathcal{S}^n\}.$$

In contrast to the classical wiretap channel with passive wiretapper, cf. Section II, we have to take the unknown varying channel states into account for establishing the communication. Therefore, the probability of decoding error slightly changes as follows. Using the wiretap code $\mathcal{C}$ from Definition 1, the probability of decoding error at the legitimate receiver for message $j \in \mathcal{J}_n$ and state sequence $s^n \in \mathcal{S}^n$ is given by

$$e_n(j, s^n \,|\, \mathcal{C}) := \sum_{x^n \in \mathcal{X}^n} W^n\left(\mathcal{D}_j^c \,\middle|\, x^n, s^n\right) E(x^n \,|\, j)$$

and the average probability of error for state sequence $s^n \in \mathcal{S}^n$ is

$$\bar{e}_n(s^n \,|\, \mathcal{C}) := \frac{1}{|\mathcal{J}_n|} \sum_{j \in \mathcal{J}_n} e(j, s^n \,|\, \mathcal{C}).$$

We further define the maximum as

$$\bar{e}_n(\mathcal{C}) := \max_{s^n \in \mathcal{S}^n} \bar{e}_n(s^n \,|\, \mathcal{C}). \tag{5}$$

To ensure that the transmitted message is kept secret from the wiretapper for all state sequences $s^n \in \mathcal{S}^n$, we now require

$$\max_{s^n \in \mathcal{S}^n} I\,(\,J; Z_{s^n}^n \,|\, \mathcal{C}) \le \epsilon_n \tag{6}$$

where $Z_{s^n}^n = (Z_{s_1}, Z_{s_2}, \dots, Z_{s_n})$ denotes the output at the wiretapper for state sequence $s^n \in \mathcal{S}^n$. The communication over the AVWC $\mathfrak{W}$ with active wiretapper is visualized in Fig. 1.

Definition 4: A nonnegative number R_S is an *achievable secrecy rate* for the AVWC $\mathfrak{W}$ with active wiretapper if for all $\delta > 0$ there is an $n(\delta) \in \mathbb{N}$ and a sequence of (n, J_n)-codes $\mathcal{C}$ such that for all $n \ge n(\delta)$ we have $\frac{1}{n} \log J_n \ge R_S - \delta$ and $\max_{s^n \in \mathcal{S}^n} I(J; Z_{s^n}^n \,|\, \mathcal{C}) \le \epsilon_n$ and $\bar{e}_n(\mathcal{C}) \le \lambda_n$ while $\epsilon_n, \lambda_n \to 0$ as $n \to \infty$. The *secrecy capacity* $C_S(\mathfrak{W}, \mathcal{A})$ is given by the supremum of all achievable secrecy rates R_S.

Remark 2: Recall that it is completely unknown to the legitimate users how the state sequence $s^n \in \mathcal{S}^n$ is chosen by the wiretapper. Neither it is known if $s^n \in \mathcal{S}^n$ is chosen according to an underlying distribution nor the distribution itself is known. Thus, it is required to find codes such that $\bar{e}_n(s^n \,|\, \mathcal{C}) \to 0$ and $I(J; Z_{s^n}^n \,|\, \mathcal{C}) \to 0$ as $n \to \infty$ for all $s^n \in \mathcal{S}^n$ simultaneously. This means the codes have to be universal with respect to the state sequences, which is also reflected by the maximum in (5) and (6).

B. Impact of Common Randomness

It has been shown that common randomness (CR) is an important resource for reliable communication over arbitrarily varying channels. Therefore we first briefly review the impact of available CR for the classical single-user AVC and then discuss how it affects communication strategies for the corresponding AVWC.

For the single-user AVC as given (3), it has been shown that its capacity highly depends on the coordination between encoder and decoder [7]–[9]. As shown in Fig. 2, there is the deterministic approach with prespecified encoder and decoder, and further the CR-assisted approach, where encoder and decoder are coordinated based on an access to a common random source. The latter strategy leads to the *CR-assisted capacity* $C_{\mathrm{ran}}(\mathcal{W})$ of the AVC $\mathcal{W}$ which is given by [7]

$$C_{\mathrm{ran}}(\mathcal{W}) = \max_{P_X \in \mathcal{P}(\mathcal{X})} \min_{\rho \in \mathcal{P}(\mathcal{S})} I(X; Y_\rho)$$

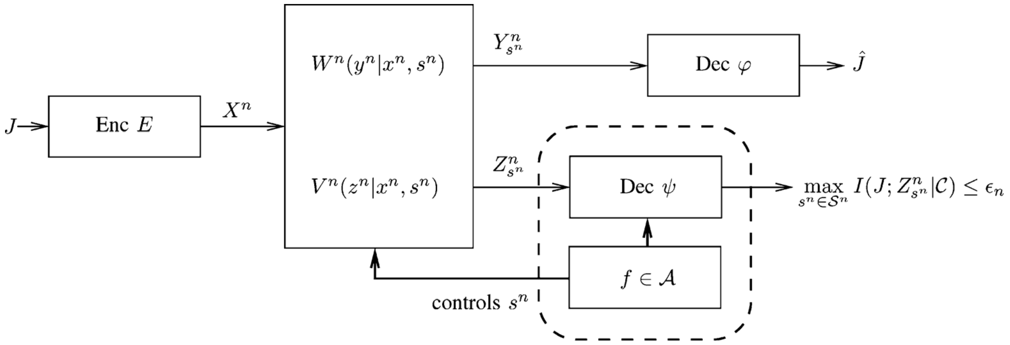

Fig. 1. Arbitrarily varying wiretap channel (AVWC) $\mathfrak{W}$ with active wiretapper. The wiretapper controls the channel conditions by choosing a corresponding state sequence $s^n \in \mathcal{S}^n$ based on his strategy $f \in \mathcal{A}$. The actual sequence $s^n \in \mathcal{S}^n$ is unknown to both sender and legitimate receiver. The sender encodes a message J into the codeword $X^n = E(J)$ and transmits it over the AVWC $\mathfrak{W}$ to the legitimate receiver, which has to decode the message $\hat{J} = \varphi(Y^n_{s^n})$ for any state sequence $s^n \in \mathcal{S}^n$. At the same time, the wiretapper has to be kept ignorant of J in the sense that $\max_{s^n\in\mathcal{S}^n} I(J;Z^n_{s^n}\,|\,\mathcal{C}) \leq \epsilon_n$.

where Y_ρ denotes the random variable associated with the output of the averaged channel W_ρ for $\rho \in \mathcal{P}(\mathcal{S})$, cf. (4).

For the *deterministic capacity* $C(\mathcal{W})$ it has been shown that it displays a dichotomy behavior: it either equals the CR-assisted capacity $C_{\mathrm{ran}}(\mathcal{W})$ or otherwise is zero [8]. This can be characterized in detail using the concept of symmetrizability [9].

Definition 5: An AVC $\mathcal{W}$ is called *symmetrizable* if there exists a stochastic matrix $U : \mathcal{X} \to \mathcal{P}(\mathcal{S})$ such that

$$\sum_{s\in\mathcal{S}} W(y\,|\,x_1,s)U(s\,|\,x_2) = \sum_{s\in\mathcal{S}} W(y\,|\,x_2,s)U(s\,|\,x_1) \quad (7)$$

holds for all $x_1, x_2 \in \mathcal{X}$ and $y \in \mathcal{Y}$.

Roughly speaking, Definition 5 means that a symmetrizable AVC can *"emulate"* a valid input, which makes it impossible for the decoder to decide on the correct codeword. With this, the deterministic capacity can be completely characterized as follows. If the AVC $\mathcal{W}$ is nonsymmetrizable, we have

$$C(\mathcal{W}) = C_{\mathrm{ran}}(\mathcal{W}).$$

In addition, we have $C(\mathcal{W}) = 0$ if and only if the AVC $\mathcal{W}$ is symmetrizable [9].

C. CR-Assisted Strategies

The previous discussion shows that common randomness is a necessary and important resource for reliable communication under arbitrarily varying channel conditions; in particular, if the channel is symmetrizable. Therefore, we assume in the following that all parties, i.e., the legitimate users and the active wiretapper, have access to a common randomness which we denote by Γ. This assumption can be motivated by the fact that this is realized over a public channel which is open to the wiretapper.

Remark 3: If the wiretapper has no access to the common randomness, the legitimate users can immediately use this resource to create a secret key corresponding to the size of the common randomness and therewith keep the confidential information completely secret from the wiretapper.

The legitimate users can use common randomness as a resource to coordinate their choice of encoder and decoder. This leads to the following definition.

Definition 6: A *CR-assisted* $(n, J_n, \mathcal{G}, \mu)$*-code* $\mathcal{C}_{\mathrm{ran}}$ for the AVWC $\mathfrak{W}$ with active wiretapper is given by a family of wiretap codes $\{\mathcal{C}(\gamma) : \gamma \in \mathcal{G}\}$ together with a random variable Γ taking values in $\mathcal{G}$ according to $\mu \in \mathcal{P}(\mathcal{G})$.

Using the CR-assisted code $\mathcal{C}_{\mathrm{ran}}$, the mean average probability of error at the legitimate receiver for state sequence $s^n \in \mathcal{S}^n$ is then given by $\bar{e}_n(s^n\,|\,\mathcal{C}_{\mathrm{ran}}) = \mathbb{E}_\Gamma[\bar{e}_n(s^n\,|\,\mathcal{C}(\Gamma))]$, i.e.,

$$\bar{e}_n(s^n\,|\,\mathcal{C}_{\mathrm{ran}}) := \frac{1}{|\mathcal{J}_n|}\sum_{j\in\mathcal{J}_n}\sum_{\gamma\in\mathcal{G}}\sum_{x^n\in\mathcal{X}^n} \times W^n\left(\mathcal{D}^c_{\gamma,j}\middle|\,x^n,s^n\right)E_\gamma(x^n\,|\,j)\mu(\gamma) \quad (8)$$

and, accordingly, the maximum by $\bar{e}_n(\mathcal{C}_{\mathrm{ran}}) := \max_{s^n\in\mathcal{S}^n}\bar{e}_n(s^n\,|\,\mathcal{C}_{\mathrm{ran}})$.

The definitions of a CR-assisted achievable secrecy rate and the corresponding CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W},\mathcal{A})$ are defined accordingly by replacing the code $\mathcal{C}$ by $\mathcal{C}_{\mathrm{ran}}$ in Definition 4.

Definition 7: A nonnegative number R_S is a *CR-assisted achievable secrecy rate* for the AVWC $\mathfrak{W}$ with active wiretapper if for all $\delta > 0$ there is an $n(\delta) \in \mathbb{N}$ and a sequence of $(n, J_n, \mathcal{G}, \mu)$-codes $\mathcal{C}_{\mathrm{ran}}$ such that for all $n \geq n(\delta)$ we have $\frac{1}{n}\log J_n \geq R_S - \delta$ and

$$\max_{s^n\in\mathcal{S}^n} I(J;Z^n_{s^n}\,|\,\mathcal{C}(\Gamma)) \leq \epsilon_n \quad (9)$$

and $\bar{e}_n(\mathcal{C}_{\mathrm{ran}}) \leq \lambda_n$ while $\epsilon_n, \lambda_n \to 0$ as $n \to \infty$. Here, $I(J;Z^n_{s^n}\,|\,\mathcal{C}(\Gamma)) = \sum_{\gamma\in\mathcal{G}} I(J;Z^n_{s^n}\,|\,\mathcal{C}(\gamma))\mu(\gamma)$ is the expectation over the whole ensemble of codebooks, where $I(J;Z^n_{s^n}\,|\,\mathcal{C}(\gamma))$ is the mutual information term for the particular code $\mathcal{C}(\gamma)$, cf. (6). The *CR-assisted secrecy capacity* $C_{S,\mathrm{ran}}(\mathfrak{W},\mathcal{A})$ is given by the supremum of all achievable secrecy rates R_S.

Common randomness allows the legitimate users to use more sophisticated strategies, but it also has an impact on the behavior and on the abilities of potential wiretappers. In particular, an *active wiretapper* might or might not exploit the knowledge about the common randomness for influencing the channel states. These two cases are further analyzed in the following.

IV. Active Wiretappers

We start with the case where the active wiretapper does not exploit his knowledge about the common randomness. Thus, his particular choice of $f \in \mathcal{A}$ does not depend on the observation

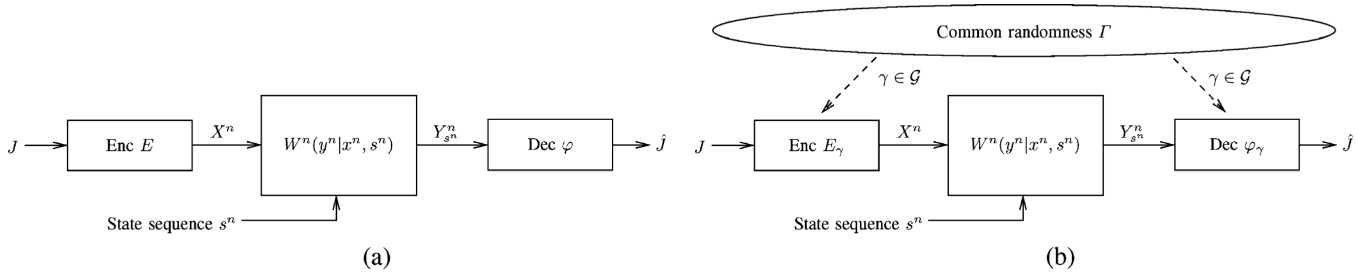

Fig. 2. Deterministic and CR-assisted coding strategies for the classical point-to-point AVC. For the deterministic approach in (a), encoder E and decoder φ are prespecified and independent of the common randomness. For the CR-assisted approach in (b), encoder E_γ and decoder φ_γ depend on the actual outcome of the common random experiment $\gamma \in \mathcal{G}$. (a) Deterministic approach. (b) CR-assisted approach.

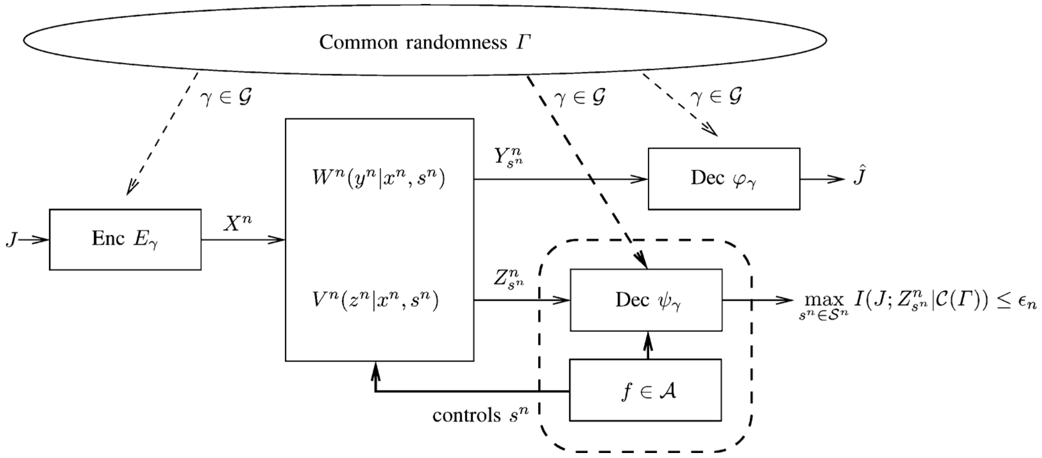

Fig. 3. All parties, i.e., legitimate users and the wiretapper, have access to a common randomness Γ. Accordingly, they can choose their encoder E_γ and decoders φ_γ and ψ_γ based on the observed realization $\gamma \in \mathcal{G}$. The wiretapper does not exploit the observation $\gamma \in \mathcal{G}$ for choosing his strategy $f \in \mathcal{A}$ and therewith the state sequence $s^n \in \mathcal{S}^n$.

$\gamma \in \mathcal{G}$. The corresponding communication scenario is visualized in Fig. 3 and first studies can be found in [11] for the strong secrecy criterion.

A. CR-Assisted Secrecy Capacity

For the *CR-assisted secrecy capacity* of the AVWC $\mathfrak{W}$ with active wiretapper, there are only partial results known. For this, we need the following definition.

Definition 8: A channel to the wiretapper is called a *best channel* if there exists a channel $V_{\rho^*} \in \{V_\rho : \rho \in \mathcal{P}(\mathcal{S})\}$ such that all other channels from $\{V_\rho : \rho \in \mathcal{P}(\mathcal{S})\}$ are degraded versions of V_{ρ^*}. Then it holds

$$X - Z_{\rho^*} - Z_\rho \qquad \text{for all } \rho \in \mathcal{P}(\mathcal{S})$$

where Z_ρ denotes the random variable associated with the output of the averaged channel $V_\rho, \rho \in \mathcal{P}(\mathcal{S})$.

With this we get a CR-assisted achievable secrecy rate for the AVWC with active wiretapper.

Proposition 1 ([11]): If there exists a best channel to the wiretapper, the CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W},\mathcal{A})$ of the AVWC $\mathfrak{W}$ with active wiretapper it holds that

$$C_{S,\mathrm{ran}}(\mathfrak{W},\mathcal{A}) \ge \max_{Q-X-(Y_\rho,Z_\rho)} \times \left(\min_{\rho\in\mathcal{P}(\mathcal{S})} I(Q,Y_\rho) - \max_{\rho\in\mathcal{P}(\mathcal{S})} I(Q,Z_\rho)\right) \quad (10)$$

where Y_ρ and Z_ρ denote the random variables associated with the outputs of the corresponding averaged channels W_ρ and $V_\rho, \rho \in \mathcal{P}(\mathcal{S})$.

B. Secrecy Capacity

A CR-assisted strategy requires common randomness between all users, since encoder and decoders depend all on the same observation of the common random experiment, cf. Definition 6. If this kind of resource is not available, a strategy with prespecified encoder and decoder is needed. For the characterization of the corresponding secrecy capacity of the AVWC with active wiretapper, a concept of symmetrizability is needed, similarly as for the single-user AVC, cf. Definition 5 and [9].

For deterministic encoding, there is a one-to-one mapping between the message $j \in \mathcal{J}_n$ and the corresponding codeword $x^n \in \mathcal{X}^n$. Therefore, a symmetrizability concept on the *"codeword level"* as in (7) suffices to characterize the deterministic capacity of the classical AVC without any secrecy requirements [8], [9]. On the other hand, in the context of information theoretic secrecy, it has been shown that randomized encoding is indispensable, cf. also Remark 1, which precludes a deterministic one-to-one mapping. Therefore, for the analysis of the AVWC with active wiretapper, there is the need of a more sophisticated definition of symmetrizability on the *"message level"* which takes randomized encoding into account. This was done in [11] in a more implicit way. Here, we present the corresponding definition and analysis in detail, which will be needed to analyze the case when $C_S(\mathfrak{W},\mathcal{A}) = 0$, cf. also Lemma 1 and Theorem 2. For this purpose, we define

$$\overline{W}^n(y^n \,|\, j, s^n) := \sum_{x^n \in \mathcal{X}^n} W^n(y^n \,|\, x^n, s^n) E(x^n \,|\, j).$$

Definition 9: An AVC $\mathcal{W}$ is called *symmetrizable under randomized encoding* if for all $n \in \mathbb{N}$ and any stochastic encoder $E : \mathcal{J}_n \to \mathcal{P}(\mathcal{X}^n)$, there is a stochastic matrix $\widetilde{U}^n : \mathcal{J}_n \to \mathcal{P}(\mathcal{S}^n)$ such that

$$\begin{aligned}\sum_{s^n \in \mathcal{S}^n} & \overline{W}^n(y^n \,|\, j_1, s^n)\widetilde{U}^n(s^n \,|\, j_2) \\ &= \sum_{s^n \in \mathcal{S}^n} \overline{W}^n(y^n \,|\, j_2, s^n)\widetilde{U}^n(s^n \,|\, j_1) \qquad (11)\end{aligned}$$

holds for all $j_1, j_2 \in \mathcal{J}_n$ and $y^n \in \mathcal{Y}^n$.

Note that due to the secrecy requirement, we need the general concept of randomized encoding. This concept is more powerful than deterministic encoding as it includes deterministic encoding as a special case. The important thing is that this necessitates a more general concept of symmetrizability as given in (11) which is a multiletter description for all block lengths $n \in \mathbb{N}$. This is in contrast to the single-user AVC with deterministic encoding for which a single-letter description of symmetrizability is sufficient, cf. (7).

Now the crucial observation is the following. If an AVC is symmetrizable in the sense of Definition 5, cf. (7), then it is also symmetrizable under randomized encoding, cf. Definition 9.

Lemma 1: Let the AVC $\mathcal{W}$ be symmetrizable in the sense of Definition 5, i.e., there is a stochastic matrix $U : \mathcal{X} \to \mathcal{P}(\mathcal{S})$ such that (7) holds. Then the AVC $\mathcal{W}$ is also symmetrizable under stochastic encoding, i.e., there exists a stochastic matrix $\widetilde{U}^n : \mathcal{J}_n \to \mathcal{P}(\mathcal{S}^n)$ such that for any stochastic encoder $E : \mathcal{J}_n \to \mathcal{P}(\mathcal{X}^n)$ condition (11) holds.

Proof: Let $E : \mathcal{J}_n \to \mathcal{P}(\mathcal{X}^n)$ be the stochastic encoder. We set $\widetilde{U}^n$ as shown at the bottom of the page. For any $j_1, j_2 \in \mathcal{J}_n$ with $j_1 \neq j_2$ we have the second equation shown at the bottom of the page, where the third equality follows from the symmetrizability, cf. (7). ■

With this we immediately obtain a similar result for randomized encoding as in [9, Lemma 1] for deterministic encoding.

Lemma 2: If the AVC $\mathcal{W}$ is symmetrizable under randomized encoding, then any code $\mathcal{C}$ with $|\mathcal{J}_n| \geq 2$ satisfies

$$\bar{e}_n(\mathcal{C}) \geq \frac{|\mathcal{J}_n| - 1}{2|\mathcal{J}_n|} > \frac{1}{4}.$$

Proof: The proof can be done as in [9, Lemma 1]. Let $\mathcal{C}$ be any code as in Definition 1. Let $\widetilde{U}^n : \mathcal{J}_n \to \mathcal{P}(\mathcal{S}^n)$ be satisfying (11). Consider random variables $S_j^n, j \in \mathcal{J}_n$ with $\mathbb{P}\{S_j^n = s^n\} = \widetilde{U}^n(s^n \,|\, j)$. Then for each pair of codewords $j_1, j_2 \in \mathcal{J}_n$ and every $y^n \in \mathcal{Y}^n$, we have

$$\begin{aligned}\mathbb{E}\left[\overline{W}^n\left(y^n \,|\, j_1, S_{j_2}^n\right)\right] &= \sum_{s^n \in \mathcal{S}^n} \overline{W}^n(y^n \,|\, j_1, s^n)\widetilde{U}^n(s^n \,|\, j_2) \\ &= \sum_{s^n \in \mathcal{S}^n} \overline{W}^n(y^n \,|\, j_2, s^n)\widetilde{U}^n(s^n \,|\, j_1) \\ &= \mathbb{E}\left[\overline{W}^n\left(y^n \,|\, j_2, S_{j_1}^n\right)\right] \qquad (12)\end{aligned}$$

where the second step follows from the symmetrizability under randomized encoding, cf. (11). With this, we get for the probability of error

$$\begin{aligned}&\mathbb{E}\left[e_n\left(j_1, S_{j_2}^n \,|\, \mathcal{C}\right)\right] + \mathbb{E}\left[e_n\left(j_2, S_{j_1}^n \,|\, \mathcal{C}\right)\right] \\ &\quad= \mathbb{E}\left[\overline{W}^n\left(\mathcal{D}_{j_1}^c \,|\, j_1, S_{j_2}^n\right)\right] + \mathbb{E}\left[\overline{W}^n\left(\mathcal{D}_{j_2}^c \,|\, j_2, S_{j_1}^n\right)\right] \\ &\quad= \mathbb{E}\left[\overline{W}^n\left(\mathcal{D}_{j_1}^c \,|\, j_1, S_{j_2}^n\right)\right] + \mathbb{E}\left[\overline{W}^n\left(\mathcal{D}_{j_2}^c \,|\, j_1, S_{j_2}^n\right)\right] \\ &\quad\geq \mathbb{E}\left[\overline{W}^n\left(\mathcal{D}_{j_1}^c \,|\, j_1, S_{j_2}^n\right)\right] + \mathbb{E}\left[\overline{W}^n\left(\mathcal{D}_{j_1} \,|\, j_1, S_{j_2}^n\right)\right] \\ &\quad= \mathbb{E}\left[\sum_{y^n \in \mathcal{Y}^n} \overline{W}^n(y^n \,|\, j_1, S_{j_2}^n)\right] = 1\end{aligned}$$

$$\widetilde{U}^n(s^n \,|\, j) = \sum_{\hat{x}^n \in \mathcal{X}^n} U(s_1 \,|\, \hat{x}_1)U(s_2 \,|\, \hat{x}_2) \times \ldots \times U(s_n \,|\, \hat{x}_n)E(\hat{x}^n \,|\, j)$$

$$\begin{aligned}&\sum_{s^n \in \mathcal{S}^n} \overline{W}^n(y^n \,|\, j_1, s^n)\widetilde{U}^n(s^n \,|\, j_2) \\ &\quad= \sum_{s^n \in \mathcal{S}^n}\sum_{x^n \in \mathcal{X}^n}\sum_{\hat{x}^n \in \mathcal{X}^n} W^n(y^n \,|\, x^n, s^n)E(x^n \,|\, j_1)U(s_1 \,|\, \hat{x}_1) \times \ldots \times U(s_n \,|\, \hat{x}_n)E(\hat{x}^n \,|\, j_2) \\ &\quad= \sum_{x^n \in \mathcal{X}^n}\sum_{\hat{x}^n \in \mathcal{X}^n} E(x^n \,|\, j_1)\left(\sum_{s^n \in \mathcal{S}^n} W^n(y^n \,|\, x^n, s^n)U(s_1 \,|\, \hat{x}_1) \times \ldots \times U(s_n \,|\, \hat{x}_n)\right)E(\hat{x}^n \,|\, j_2) \\ &\quad= \sum_{x^n \in \mathcal{X}^n}\sum_{\hat{x}^n \in \mathcal{X}^n} E(x^n \,|\, j_1)\left(\sum_{s^n \in \mathcal{S}^n} W^n(y^n \,|\, \hat{x}^n, s^n)U(s_1 \,|\, x_1) \times \ldots \times U(s_n \,|\, x_n)\right)E(\hat{x}^n \,|\, j_2) \\ &\quad= \sum_{s^n \in \mathcal{S}^n}\left(\sum_{\hat{x}^n \in \mathcal{X}^n} W^n(y^n \,|\, \hat{x}^n, s^n)E(\hat{x}^n \,|\, j_2)\right)\left(\sum_{x^n \in \mathcal{X}^n} E(x^n \,|\, j_1)U(s_1 \,|\, x_1) \times \ldots \times U(s_n \,|\, x_n)\right) \\ &\quad= \sum_{s^n \in \mathcal{S}^n} \overline{W}^n(y^n \,|\, j_2, s^n)\widetilde{U}^n(s^n \,|\, j_1)\end{aligned}$$

where the second step follows from (12) and the last step from $\mathcal{D}_{j_1} \cup \mathcal{D}_{j_1}^c = \mathcal{Y}^n$. This immediately implies for the average probability of error

$$\begin{aligned}\frac{1}{|\mathcal{J}_n|} \sum_{j_2 \in \mathcal{J}_n} \mathbb{E}\left[\bar{e}_n\left(S_{j_2}^n \middle| \mathcal{C}\right)\right] &= \frac{1}{|\mathcal{J}_n|^2} \sum_{j_1 \in \mathcal{J}_n} \sum_{j_2 \in \mathcal{J}_n} \mathbb{E}\left[e_n\left(j_1, S_{j_2}^n \middle| \mathcal{C}\right)\right] \\ &\geq \frac{1}{|\mathcal{J}_n|^2} \frac{|\mathcal{J}_n|(|\mathcal{J}_n|-1)}{2} = \frac{|\mathcal{J}_n|-1}{2|\mathcal{J}_n|}\end{aligned}$$

so that

$$\mathbb{E}\left[\bar{e}_n\left(S_j^n \middle| \mathcal{C}\right)\right] \geq \frac{|\mathcal{J}_n|-1}{2|\mathcal{J}_n|} > \frac{1}{4}$$

for some $j \in \mathcal{J}_n$. Finally, with

$$\bar{e}_n(\mathcal{C}) = \max_{s^n \in \mathcal{S}^n} \bar{e}_n(s^n \,|\, \mathcal{C}) \geq \mathbb{E}\left[\bar{e}_n\left(S_j^n \middle| \mathcal{C}\right)\right]$$

the desired result is proved. ■

This shows that a symmetrizable AVC $\mathcal{W}$ leads to a probability of decoding error at the receiver which satisfies $\bar{e}_n(\mathcal{C}) > \frac{1}{4}$ also under randomized encoding. The consequence is that also under randomized encoding, there is no communication possible if the AVC $\mathcal{W}$ is symmetrizable. Accordingly, the capacity for randomized encoding is zero and therewith also for the secrecy capacity $C_S(\mathfrak{W}, \mathcal{A}) = 0$ of the corresponding AVWC $\mathfrak{W}$ with active wiretapper. Thus, in this case the active wiretapper can choose a strategy $f \in \mathcal{A}$ so that the state sequence can emulate a valid input which causes ambiguities at the legitimate receiver.

On the other hand, if the AVC $\mathcal{W}$ is nonsymmetrizable, we have for the deterministic capacity $C(\mathcal{W}) > 0$, and so we have for randomized encoding. Accordingly, this allows us to characterize the behavior of the secrecy capacity $C_S(\mathfrak{W}, \mathcal{A})$ of the AVWC $\mathfrak{W}$ with active wiretapper in detail. To this end, we drop the assumption of a best channel to the wiretapper for a moment.

Theorem 2 ([11]): If the CR-assisted secrecy capacity satisfies $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}) > 0$, then the secrecy capacity is given by

$$C_S(\mathfrak{W}, \mathcal{A}) = C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A})$$

if and only if the AVC $\mathcal{W}$ to the legitimate receiver is nonsymmetrizable. If the AVC $\mathcal{W}$ is symmetrizable, then $C_S(\mathfrak{W}, \mathcal{A}) = 0$. If $C_S(\mathfrak{W}, \mathcal{A}) = 0$ and $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}) > 0$, then the AVC $\mathcal{W}$ is symmetrizable.

Remark 4: Interestingly, the secrecy capacity $C_S(\mathfrak{W}, \mathcal{A})$ is not longer characterized by entropic quantities. Although the mutual information terms and their differences, cf. (10), might be positive, the secrecy capacity is still zero if the corresponding AVC $\mathcal{W}$ is symmetrizable.

V. Active Wiretappers Exploiting CR

In this case, the active wiretapper is more powerful as he exploits his knowledge about the common randomness to maliciously influence the channel conditions of the legitimate users. Accordingly, the wiretapper can choose his strategy based on the outcome of the random experiment. To emphasize this dependency, we denote the set of all strategies by $\mathcal{A}(\Gamma)$ in the following. Now, the function $f \in \mathcal{A}(\Gamma)$ representing his strategy becomes

$$f : \mathcal{G} \to \mathcal{S}^n. \tag{13}$$

This means, for every observation $\gamma \in \mathcal{G}$, the wiretapper can choose the state sequence $s^n = f(\gamma) \in \mathcal{S}^n$ which governs the following transmission. Of course, the actual strategy $f \in \mathcal{A}(\Gamma)$ of the wiretapper is unknown to the legitimate users. The corresponding communication scenario is depicted in Fig. 4.

Then the definitions of a *CR-assisted achievable secrecy rate* and the *CR-assisted secrecy capacity* $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma))$ of the AVWC $\mathfrak{W}$ with active wiretapper exploiting CR are defined accordingly by letting the state sequence in (8) and (9) in Definitions 6 and 7 be $s^n = f(\gamma) \in \mathcal{S}^n, \gamma \in \mathcal{G}$.

With this, for function $f : \mathcal{G} \to \mathcal{S}^n$ the probability of decoding error at the legitimate receiver becomes

$$\begin{aligned}\bar{e}_n(f \,|\, \mathcal{C}_{\mathrm{ran}}) := \frac{1}{|\mathcal{J}_n|} &\sum_{j \in \mathcal{J}_n} \sum_{\gamma \in \mathcal{G}} \sum_{x^n \in \mathcal{X}^n} \\ &\times W^n\big(\mathcal{D}_{\gamma,j}^c \,|\, x^n, f(\gamma)\big) E_\gamma(x^n \,|\, j)\mu(\gamma)\end{aligned} \tag{14}$$

and, accordingly,

$$\bar{e}_n(\mathcal{C}_{\mathrm{ran}}) = \max_{f \in \mathcal{A}(\Gamma)} \bar{e}_n(f \,|\, \mathcal{C}_{\mathrm{ran}}). \tag{15}$$

The mean secrecy criterion becomes

$$\max_{f \in \mathcal{A}(\Gamma)} I\left(J; Z_{f(\Gamma)}^n \,|\, \mathcal{C}(\Gamma)\right) \leq \epsilon_n. \tag{16}$$

Conditions (14) and (16) show that an active wiretapper exploiting CR has different strategies, since (14) and (16) depend on the applied strategy $f \in \mathcal{A}(\Gamma)$. On the one hand, he can try to maximize the information leaked to him by choosing the state sequence such that (16) is maximized. Another strategy is to disturb the communication of the legitimate users by choosing the state sequence such that the probability of decoding error is maximized. Thus, it includes jamming models where the wiretapper acts as a jammer. Of course, any combination in between is also a valid strategy for the wiretapper and, thus, the legitimate users have to be prepared for all possible strategies which is reflected by the maximum in (15) and (16).

A. CR-Assisted Secrecy Capacity

In the following we will solve this problem and further characterize the optimal strategy of the wiretapper. This yields a complete characterization of the CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma))$ of the AVWC $\mathfrak{W}$ with active wiretapper exploiting CR.

Theorem 3: If $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}) > 0$, then the CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma))$ is given by

$$C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) = C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A})$$

if and only if the AVC $\mathcal{W}$ is to the legitimate receiver is nonsymmetrizable. If the AVC $\mathcal{W}$ is symmetrizable,

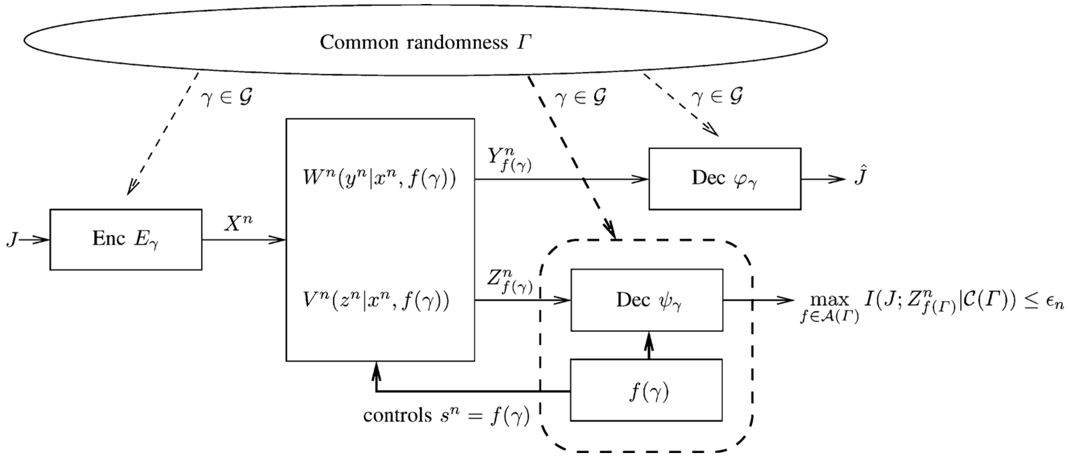
Common randomness Γ
$\gamma \in \mathcal{G}$
$\gamma \in \mathcal{G}$
$\gamma \in \mathcal{G}$
J
Enc E_γ
X^n
$W^n(y^n|x^n, f(\gamma))$
$V^n(z^n|x^n, f(\gamma))$
$Y^n_{f(\gamma)}$
Dec φ_γ
$\hat{J}$
$Z^n_{f(\gamma)}$
Dec ψ_γ
$\max_{f \in \mathcal{A}(\Gamma)} I(J; Z^n_{f(\Gamma)}|\mathcal{C}(\Gamma)) \le \epsilon_n$
$f(\gamma)$
controls $s^n = f(\gamma)$

Fig. 4. Arbitrarily varying wiretap channel (AVWC) $\mathfrak{W}$ with active wiretapper exploiting CR. The wiretapper exploits the knowledge about the observation $\gamma \in \mathcal{G}$ to control the state sequence $s^n = f(\gamma) \in \mathcal{S}^n$, which governs the transmission to the legitimate receiver and the wiretapper.

then $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) = 0$. If $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) = 0$ and $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}) > 0$, then the AVC $\mathcal{W}$ is symmetrizable.

Interestingly, it turns out that the CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma))$ of the AVWC $\mathfrak{W}$ with active wiretapper exploiting CR displays the same dichotomy behavior as the secrecy capacity $C_S(\mathfrak{W}, \mathcal{A})$: it either equals its CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A})$ (not exploiting CR) or else is zero. As a consequence, the characterization of $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma))$ is again nonentropic, cf. also Remark 4. Thus, with the result given in Theorem 2 we immediately obtain the following characterization of the CR-assisted secrecy capacity.

Corollary 1: The CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma))$ of the AVWC $\mathfrak{W}$ with active wiretapper exploiting CR is given by

$$C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) = C_S(\mathfrak{W}, \mathcal{A}).$$

Remark 5: For the dichotomy result above we assumed $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}) > 0$. For the case $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}) = 0$, we trivially have equality since $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) = C_S(\mathfrak{W}, \mathcal{A}) = C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}) = 0$.

In the following we prove Theorem 3. To do so, we start with a basic observation which yields a trivial upper bound on $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma))$. Since an active wiretapper exploiting CR is more powerful than an active wiretapper which does not exploit CR, we immediately obtain

$$C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) \le C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}). \tag{17}$$

For the proof it turns out to be beneficial distinguishing between $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) > 0$ and $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) = 0$. The corresponding proofs are carried out in the following two subsections.

B. Positive CR-Assisted Secrecy Capacity

First, we study the case, where the CR-assisted secrecy capacity is positive. We show that if $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) > 0$, we actually have equality in (17), i.e., $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) = C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A})$.

Theorem 4: If $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) > 0$, then

$$C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) = C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}).$$

Proof: To prove the desired result, we extend techniques for the ordinary AVC; more precisely the *random code reduction* [8], [11] and the *elimination of randomness* [8]. We have to extend and generalize these techniques in order to incorporate the secrecy requirement on the transmitted message and to include active wiretappers which exploit CR.

1) Random Code Reduction: Let $\delta > 0$, $\lambda > 0$, and $\epsilon' > 0$ be arbitrary. Now, we start with a CR-assisted $(n, J_n, \mathcal{G}, \mu)$-code $\mathcal{C}_{\mathrm{ran}}$ for the AVWC $\mathfrak{W}$ with active wiretapper (not exploiting CR), cf. Definition 6, which is optimal in the sense that it achieves the secrecy rate

$$R_S \ge C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}) - \delta$$

with

$$\bar{e}_n(\mathcal{C}_{\mathrm{ran}}) = \max_{s^n \in \mathcal{S}^n} \mathbb{E}_\Gamma[\bar{e}_n(s^n \,|\, \mathcal{C}(\Gamma))] \le \lambda$$

and

$$\max_{s^n \in \mathcal{S}^n} I\,(\,J; Z^n_{s^n}|\,\mathcal{C}(\Gamma)) \le \epsilon'.$$

So far we cannot say anything about the common randomness Γ that is needed for this code to be optimal, especially the size $|\mathcal{G}|$ can be arbitrary large. But from the *random code reduction* in [11] we can conclude on the following.

Lemma 3 ([11]): Let $\mathcal{C}_{\mathrm{ran}}$ be a CR-assisted $(n, J_n, \mathcal{G}, \mu)$-code for the AVWC $\mathfrak{W}$ with active wiretapper consisting of a family $\{\mathcal{C}(\gamma) : \gamma \in \mathcal{G}\}$ of wiretap codes where γ is chosen according to the distribution $\mu \in \mathcal{P}(\mathcal{G})$. Then let

$$\bar{e}_n(\mathcal{C}_{\mathrm{ran}}) \le \lambda, \quad \text{and} \quad \max_{s^n \in \mathcal{S}^n} I\,(\,J; Z^n_{s^n}|\,\mathcal{C}(\Gamma)) \le \epsilon'. \tag{18}$$

Then for any ϵ and K that satisfy

$$\epsilon > 4\max\{\lambda, \epsilon'\} \quad \text{and} \quad K > \frac{2n \log|\mathcal{X}|}{\epsilon}(1 + n\log|\mathcal{S}|),$$

there exist K codes $\mathcal{C}(i), i=1,\dots,K$ chosen from the CR-assisted code $\mathcal{C}_{\text{ran}}$ by random selection such that

$$\frac{1}{K}\sum_{i=1}^{K}\bar{e}_n(s^n\,|\,\mathcal{C}(i))\le\epsilon \quad\text{and}\quad \frac{1}{K}\sum_{i=1}^{K}I\left(J;Z_{s^n}^n\,|\,\mathcal{C}(i)\right)\le\epsilon \tag{19}$$

for all $s^n\in\mathcal{S}^n$.

Lemma 3 shows that for any CR-assisted code $\mathcal{C}_{\text{ran}}$ for the AVWC $\mathfrak{W}$ with active wiretapper, there exists another *"reduced"* CR-assisted code $\tilde{\mathcal{C}}_{\text{ran}}$ uniformly distributed over K wiretap codes with an average probability of error and a mean secrecy criterion which fulfill (19).

Furthermore, from Lemma 3, cf. also [11], we see that it is sufficient to select no more than $K=n^3$ wiretap codes to obtain a CR-assisted code $\tilde{\mathcal{C}}_{\text{ran}}$ with the desired properties achieving the same secrecy rate as the original code $\mathcal{C}_{\text{ran}}$.

Up to now we have ensured that there is a CR-assisted code $\tilde{\mathcal{C}}_{\text{ran}}$ consisting of polynomial many wiretap codes for the AVWC $\mathfrak{W}$ with active wiretapper (not exploiting CR) with the desired properties. The next step is to make this code suitable for the case with an active wiretapper, which exploits CR, as well.

2) Elimination of Randomness: The crucial idea is to combine the reduced CR-assisted code $\tilde{\mathcal{C}}_{\text{ran}}$ with a code $\mathcal{C}_{\text{ran}}^{\text{CR}}$ suitable for the AVWC $\mathfrak{W}$ with active wiretapper exploiting CR. Since $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))>0$, there exists such a code which achieves positive secrecy rate and, thus, such a code is suitable to indicate which element of $\tilde{\mathcal{C}}_{\text{ran}}$ is actually used in the following. In more detail, since $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))>0$, there exists a CR-assisted code $\mathcal{C}_{\text{ran}}^{\text{CR}}$ for the AVWC $\mathfrak{W}$ with active wiretapper exploiting CR consisting of a family $\{\mathcal{C}(\gamma):\gamma\in\mathcal{G}\}$ with stochastic encoders

$$\{E'_\gamma:\{1,\dots,n^3\}\to\mathcal{P}(\mathcal{X}^{k_n}),\gamma\in\mathcal{G}\}$$

and collections of disjoint decoding sets

$$\{\mathcal{D}'_{\gamma,l}\subset\mathcal{Y}^{k_n}:l\in\{1,\dots,n^3\},\gamma\in\mathcal{G}\}$$

with $\frac{k_n}{n}\to0$ as $n\to\infty$ with probability of error

$$\frac{1}{n^3}\sum_{l=1}^{n^3}\sum_{\gamma\in\mathcal{G}}\sum_{x^{k_n}\in\mathcal{X}^{k_n}} \times W^{k_n}\left((\mathcal{D}'_{\gamma,l})^c\,|\,x^{k_n},f(\gamma)\right)E'_\gamma(x^{k_n}\,|\,l)\mu(\gamma)\le\epsilon_n$$

and further

$$I\left(L;Z_{f(\Gamma)}^{k_n}\,\middle|\,\mathcal{C}(\Gamma)\right)\le\epsilon_n$$

for all $f(\gamma)\in\mathcal{S}^{k_n}$ with $\epsilon_n\to0$ as $n\to\infty$.

Now, the final code for the AVWC $\mathfrak{W}$ with active wiretapper exploiting CR is given by the composition of both codes $\mathcal{C}_{\text{ran}}^{\text{CR}}$ and $\tilde{\mathcal{C}}_{\text{ran}}$. Thus, the final code consists of encoders $E'_\gamma(x^{k_n}\,|\,l)E_l(x^n\,|\,j)$ transmitting a message from $\{1,\dots,n^3\}\times\mathcal{J}_n$ of length k_n+n, and decoding sets $\mathcal{D}'_{\gamma,l}\mathcal{D}_{l,j}$, where the channel is determined by the state sequence $(s^{k_n},s^n)\in\mathcal{S}^{k_n+n}$.

Since $\frac{k_n}{n}\to0$ as $n\to\infty$, the resources "wasted" for indicating which code is actually used, vanishes so that we end up with $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))=C_{S,\text{ran}}(\mathfrak{W},\mathcal{A})$ completing the proof. Note that Lemma 3 ensures that the ratio $\frac{k_n}{n}$ vanishes by letting $\tilde{\mathcal{C}}_{\text{ran}}$ be of polynomial size only (since it is of order n^3).

3) Discussion: Theorem 4 shows that if the CR-assisted secrecy capacity is positive, an active wiretapper exploiting CR is as (in)effective as an active wiretapper who does not exploit CR. Thus, a strategy which maximizes the information leakage to the wiretapper, cf. (16), does not make sense in this case. Thus, the optimal strategy $f\in\mathcal{A}(\Gamma)$ of an active wiretapper exploiting CR must be to destroy the communication of the legitimate users. This means, the aim must be to choose the state sequence $f(\gamma)\in\mathcal{S}^n$ in such a way that the probability of error of the legitimate users in (14) is maximized. Then the CR-assisted secrecy capacity becomes zero, i.e., $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))=0$. Since otherwise, we have $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))=C_{S,\text{ran}}(\mathfrak{W},\mathcal{A})$, which means that the legitimate users can operate at the same rate as if the active wiretapper would not exploit CR.

C. Zero CR-Assisted Secrecy Capacity

The previous analysis shows that if $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))>0$ then $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))=C_{S,\text{ran}}(\mathfrak{W},\mathcal{A})$. Thus, the strategy of an active wiretapper exploiting CR must be to destroy the communication of the legitimate users. Therefore, we study now the case, where the CR-assisted secrecy capacity is zero. If $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A})=0$, we immediately obtain from (17) that $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))=0$ as well. Therefore, it remains to concentrate on $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A})>0$ in the following.

Next, we show that for $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A})>0$, we have $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))=0$ if and only if the AVC $\mathcal{W}$ to the legitimate receiver is symmetrizable. We start with the direct part, which establishes symmetrizability as a necessary condition for $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))=0$.

Lemma 4: Let $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A})>0$. If $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))=0$ then the AVC $\mathcal{W}$ to the legitimate receiver is symmetrizable.

Proof: We prove the proposition by contradiction. Therefore we assume the AVC $\mathcal{W}$ to be nonsymmetrizable. Then we know from [11] that the secrecy capacity $C_S(\mathfrak{W},\mathcal{A})$ and the CR-assisted secrecy capacity $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A})$ are equal, i.e., $C_S(\mathfrak{W},\mathcal{A})=C_{S,\text{ran}}(\mathfrak{W},\mathcal{A})>0$. This means that there exists a wiretap code which achieves the desired rate. Such a code can be considered as a special CR-assisted code with cardinality $|\mathcal{G}|=1$. The consequence is that, basically, the active wiretapper which exploits CR *"becomes"* an active wiretapper which does not exploit CR since his knowledge about the common randomness is useless. Thus, we end up with $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))>0$ which contradicts the assumption. This establishes symmetrizability as a necessary condition for $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))=0$. ■

The next lemma shows that if the AVC $\mathcal{W}$ to the legitimate receiver is symmetrizable, then the average probability of decoding error (14) is strictly positive which implies $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))=0$. Thus, it establishes symmetrizability also as a sufficient condition for $C_{S,\text{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))=0$. For this purpose, for strategy $f:\mathcal{G}\to\mathcal{S}^n$ of the active wiretapper exploiting CR we define

$$\overline{W}_f^n(y^n\,|\,j,\gamma):=\sum_{x^n\in\mathcal{X}^n}W^n(y^n\,|\,x^n,f(\gamma))E_\gamma(x^n\,|\,j).$$

Lemma 5: If the AVC $\mathcal{W}$ to the legitimate receiver is symmetrizable, then there is a function $f^* : \mathcal{G} \to \mathcal{S}^n$ such that for all $\mu \in \mathcal{P}(\mathcal{G})$ we have

$$\frac{1}{|\mathcal{J}_n|}\sum_{j\in\mathcal{J}_n}\sum_{\gamma\in\mathcal{G}}\overline{W}^n_{f^*}\left(\mathcal{D}^c_{\gamma,j}\,|\,j,\gamma\right)\mu(\gamma) > \frac{1}{4}. \tag{20}$$

Proof: Let $\{E_\gamma : \mathcal{J}_n \to \mathcal{P}(\mathcal{X}^n), \gamma \in \mathcal{G}\}$ be the set of stochastic encoders. We set $\widetilde{U}^n$ as shown at the bottom of the page. Now, for every $\gamma \in \mathcal{G}$, the wiretapper is able to choose a function $f \in \mathcal{A}(\Gamma)$, cf. also (13), to control the state sequence, i.e., he chooses $f(\gamma) \in \mathcal{S}^n$. In the following we construct a stochastic matrix $\widehat{U}^n(f\,|\,j,\gamma)$ such that for any $\gamma \in \mathcal{G}$ and for any $j_1, j_2 \in \mathcal{J}_n$ with $j_1 \neq j_2$ we have

$$\sum_{f\in\mathcal{A}(\Gamma)}\overline{W}^n_f(y^n\,|\,j_1,\gamma)\widehat{U}^n(f\,|\,j_2,\gamma) = \sum_{f\in\mathcal{A}(\Gamma)}\overline{W}^n_f(y^n\,|\,j_2,\gamma)\widehat{U}^n(f\,|\,j_1,\gamma) \tag{21}$$

for all $j_1, j_2 \in \mathcal{J}_n, \gamma \in \mathcal{G}$, and $y^n \in \mathcal{Y}^n$. Now, if (21) holds, the channel $\overline{W}^n_f(y^n\,|\,j,\gamma)$ is symmetrizable for all $\gamma \in \mathcal{G}$. From this follows immediately that the decoding error at the legitimate receiver is bounded from below, cf. (20). This can be verified exactly as in Lemma 2, cf. also [9, Lemma 1]. The details are omitted for brevity.

Thus, to prove the desired result, it only remains to show that (21) is actually satisfied. Therefore, let $\gamma \in \mathcal{G}$ be arbitrary and let $\mathcal{A}_\gamma \subset \mathcal{A}(\Gamma)$ be a smallest subset of $\mathcal{A}(\Gamma)$ with the following properties. For any $f_1, f_2 \in \mathcal{A}_\gamma$ with $f_1 \neq f_2$ we have $f_1(\gamma) \neq f_2(\gamma)$ and further $\bigcup_{f\in\mathcal{A}_\gamma} f(\gamma) = \mathcal{S}^n$. Thus, $\mathcal{A}_\gamma$ is the smallest set that covers the whole set $\mathcal{S}^n$. Then, we set

$$\widehat{U}^n(f\,|\,j,\gamma) = \begin{cases}\widetilde{U}^n(f(\gamma)\,|\,j,\gamma) & f \in \mathcal{A}_\gamma\\ 0 & f \notin \mathcal{A}_\gamma.\end{cases}$$

From the definition follows that for all $j \in \mathcal{J}_n$ we have

$$\sum_{f\in\mathcal{A}(\Gamma)}\widehat{U}^n(f\,|\,j,\gamma) = \sum_{f\in\mathcal{A}_\gamma}\widetilde{U}^n(f(\gamma)\,|\,j,\gamma) = \sum_{s^n\in\mathcal{S}^n}\widetilde{U}^n(s^n\,|\,j,\gamma) = 1.$$

This means $\widehat{U}^n$ is a stochastic matrix and we obtain for any $j_1, j_2 \in \mathcal{J}_n$ with $j_1 \neq j_2$ and any $\gamma \in \mathcal{G}$ the following

$$\begin{aligned}\sum_{f\in\mathcal{A}(\Gamma)}&\overline{W}^n_f(y^n\,|\,j_1,\gamma)\widehat{U}^n(f\,|\,j_2,\gamma)\\ &= \sum_{f\in\mathcal{A}_\gamma}\overline{W}^n_f(y^n\,|\,j_1,\gamma)\widetilde{U}^n(f(\gamma)\,|\,j_2,\gamma)\\ &= \sum_{s^n\in\mathcal{S}^n}\overline{W}^n(y^n\,|\,j_1,s^n)\widetilde{U}^n(s^n\,|\,j_2,\gamma)\\ &= \sum_{s^n\in\mathcal{S}^n}\overline{W}^n(y^n\,|\,j_2,s^n)\widetilde{U}^n(s^n\,|\,j_1,\gamma)\\ &= \sum_{f\in\mathcal{A}_\gamma}\overline{W}^n_f(y^n\,|\,j_2,\gamma)\widetilde{U}^n(f(\gamma)\,|\,j_1,\gamma)\\ &= \sum_{f\in\mathcal{A}(\Gamma)}\overline{W}^n_f(y^n\,|\,j_2,\gamma)\widehat{U}^n(f\,|\,j_1,\gamma)\end{aligned}$$

where the third equality follows from the fact the AVC $\mathcal{W}$ is symmetrizable. This proves (21) and therewith completes the proof of the theorem. ∎

D. Capacity Results

The AVWC with an active wiretapper, who is not exploiting CR, is studied in [11]. There, several capacity results are derived for the approach with prespecified encoder and decoder as well as for the CR-assisted approach where encoder and decoder are coordinated with the help of a common random source. In the following we will show that the results derived in this paper for the AVWC with active wiretapper exploiting CR, cf. Section V, allow to obtain similar capacity results.

In particular, if $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) > 0$, from the achievable secrecy rate for the AVWC with active wiretapper, cf. Proposition 1 and Theorem 4, we immediately obtain also an achievable secrecy rate for the AVWC with active wiretapper exploiting CR.

Corollary 2: If $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) > 0$ and if there exists a best channel to the wiretapper, then for $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma))$ of the AVWC $\mathfrak{W}$ with active wiretapper exploiting CR it holds that

$$C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) \geq \max_{Q-X-(Y_\rho,Z_\rho)} \times\left(\min_{\rho\in\mathcal{P}(\mathcal{S})} I(Q;Y_\rho) - \max_{\rho\in\mathcal{P}(\mathcal{S})} I(Q;Z_\rho)\right)$$

where Y_ρ and Z_ρ denote the outputs of the corresponding channels W_ρ and $V_\rho, \rho \in \mathcal{P}(\mathcal{S})$.

Since an active wiretapper, who is exploiting CR, is more powerful than a wiretapper who is not, we have $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) \leq C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A})$, cf. (17), so that every upper bound the CR-assisted secrecy capacity of the AVWC with active wiretapper immediately yields also an upper bound on the CR-assisted secrecy capacity of the AVWC with active wiretapper exploiting CR. Thus, (17) and [11, Theorem 3] yield the following upper bound on the CR-assisted secrecy capacity.

Proposition 2: The CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma))$ of the AVWC $\mathfrak{W}$ with active wiretapper exploiting CR is bounded from above by

$$C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma)) \leq \min_{\rho\in\mathcal{P}(\mathcal{S})}\max_{Q-X-(Y_\rho,Z_\rho)} \times\left(I(Q;Y_\rho) - I(Q;Z_\rho)\right).$$

$$\widetilde{U}^n(s^n\,|\,j,\gamma) := \sum_{x^n\in\mathcal{X}^n} U(s_1\,|\,x_1)U(s_2\,|\,x_2)\times\ldots\times U(s_n\,|\,x_n)E_\gamma(x^n\,|\,j)$$

Such a worst case assumption yields a very natural upper bound, since the CR-assisted secrecy capacity cannot exceed the capacities of each individual channel realization. Thus, this upper bound is dominated by the worst channel to the legitimate receiver and the best channel to the wiretapper. However, this bound is in general not tight. In addition, we obtain from [11, Theorem 4] a multiletter upper bound on the CR-assisted secrecy capacity.

Proposition 3: The CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))$ of the AVWC $\mathfrak{W}$ with active wiretapper exploiting CR is bounded from above by

$$C_{S,\mathrm{ran}}(\mathfrak{W},\mathcal{A}(\Gamma)) \leq \lim_{n\to\infty}\frac{1}{n}\max_{Q-X^n-(Y_\rho^n,Z_\rho^n)} \times\left(\inf_{\rho\in\mathcal{P}(\mathcal{S})} I\left(Q;Y_\rho^n\right) - \sup_{\rho\in\mathcal{P}(\mathcal{S})} I\left(Q;Z_\rho^n\right)\right)$$

where Y_ρ^n and Z_ρ^n the outputs of the channels W_ρ^n and V_ρ^n, $\rho\in\mathcal{P}(\mathcal{S})$.

Now, applying the achievability result given in Corollary 2 to the n-fold product of the channels $W_\rho^n = \prod_{i=1}^n W_\rho$ and $V_\rho^n = \prod_{i=1}^n V_\rho$, we obtain together with the multiletter upper bound in Proposition 3 a multiletter description of the CR-assisted secrecy capacity.

Theorem 5: If $C_{S,\mathrm{ran}}(\mathfrak{W},\mathcal{A}) > 0$ and if there exists a best channel to the wiretapper, then a multiletter description of the CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W},\mathcal{A}(\Gamma))$ of the AVWC $\mathfrak{W}$ with active wiretapper exploiting CR is given by

$$C_{S,\mathrm{ran}}(\mathfrak{W},\mathcal{A}(\Gamma)) = \lim_{n\to\infty}\frac{1}{n}\max_{Q-X^n-(Y_\rho^n,Z_\rho^n)} \times\left(\inf_{\rho\in\mathcal{P}(\mathcal{S})} I\left(Q;Y_\rho^n\right) - \sup_{\rho\in\mathcal{P}(\mathcal{S})} I\left(Q;Z_\rho^n\right)\right)$$

if and only if the AVC $\mathcal{W}$ to the legitimate receiver is nonsymmetrizable.

VI. Super-Activation

For wireless communication systems, such as cellular systems or sensor networks, resource allocation is an important issue as it determines the overall performance of the network. For example, the overall capacity of an OFDM system is given by the sum of the capacities of all orthogonal subchannels. Furthermore, a system consisting of two orthogonal AVCs, where both are "*useless*," i.e., with zero capacity, the capacity of the whole system is zero as well. This reflects the world view of classical additivity of basic resources in the sense that "$0+0=0$."

In contrast to that, in quantum information theory, it has been shown recently that the classical additivity of basic resources does not hold anymore. There are examples in quantum communication, where two channels which are themselves useless allow perfect transmission if they are used together, i.e., "$0+0>0$," cf. for example [15], [16]. To the best of our knowledge, such phenomena of *super-activation* of channels are not possible for passive wiretappers and, to date, it has been expected that they only appear in the area of quantum communication.

The natural question arises if such phenomena as super-activation, which have been observed only in the area of quantum communication until now, are also possible for classical communication systems. Such knowledge is particularly important as it has a direct impact on the design and the medium access control of communication systems.

A. Secure Communication Over Orthogonal AVWCs

In the following, we study what happens if certain secrecy requirements are imposed. We show that in this case, super-activation also appear in such classical communication systems. To do so, we consider secure communication over two orthogonal AVWCs with active wiretappers as depicted in Fig. 5.

For finite input sets $\mathcal{X}^{(i)}$, output sets $\mathcal{Y}^{(i)}$, $\mathcal{Z}^{(i)}$, and state sets $\mathcal{S}^{(i)}$, $\quad i=1,2$, we define two AVWCs $\mathfrak{W}^{(1)}$ and $\mathfrak{W}^{(2)}$ exactly as in Section III, cf. especially (2)–(3) and Definition 3. Now, the parallel use of both AVWCs $\mathfrak{W}^{(1)}$ and $\mathfrak{W}^{(2)}$ results in the combined AVWC $\widetilde{\mathfrak{W}} = \mathfrak{W}^{(1)}\otimes\mathfrak{W}^{(2)}$, where the notation $\otimes$ indicates the orthogonal use of $\mathfrak{W}^{(1)}$ and $\mathfrak{W}^{(2)}$. Then for given state sequences $\boldsymbol{s}^n = (s^{(1)},s^{(2)})^n \in (\mathcal{S}^{(1)}\times\mathcal{S}^{(2)})^n$, the discrete memoryless channel $\widetilde{W}^n = (W^{(1)}\otimes W^{(2)})^n$ to the legitimate receiver is

$$\begin{aligned}&\widetilde{W}^n(\boldsymbol{y}^n\,|\,\boldsymbol{x}^n,\boldsymbol{s}^n)\\ &\quad= W^{(1)n}\left(y^{(1)n}\middle|\,x^{(1)n},s^{(1)n}\right)W^{(2)n}\left(y^{(2)n}\middle|\,x^{(2)n},s^{(2)n}\right)\\ &\quad=\prod_{i=1}^n W^{(1)}\left(y_i^{(1)}\middle|\,x_i^{(1)},s_i^{(1)}\right)\prod_{i=1}^n W^{(2)}\left(y_i^{(2)}\middle|\,x_i^{(2)},s_i^{(2)}\right)\end{aligned}$$

with $\boldsymbol{x}^n = (x^{(1)},x^{(2)})^n \in (\mathcal{X}^{(1)}\times\mathcal{X}^{(2)})^n$ and $\boldsymbol{y}^n = (y^{(1)},y^{(2)})^n \in (\mathcal{Y}^{(1)}\times\mathcal{Y}^{(2)})^n$. Accordingly, the AVC $\widetilde{\mathcal{W}}$ is given by

$$\begin{aligned}\widetilde{\mathcal{W}} &= \left\{\widetilde{W}^n(\cdot\,|\,\cdot,\boldsymbol{s}^n) : \boldsymbol{s}^n\in\left(\mathcal{S}^{(1)}\times\mathcal{S}^{(2)}\right)^n\right\}\\ &= \Big\{W^{(1)n}\left(\cdot\,|\,\cdot,s^{(1)n}\right)W^{(2)n}\left(\cdot\,|\,\cdot,s^{(2)n}\right):\\ &\qquad\qquad s^{(1)n}\in\mathcal{S}^{(1)n}, s^{(2)n}\in\mathcal{S}^{(2)n}\Big\}\end{aligned}$$

and the AVWC $\widetilde{\mathfrak{W}}$ by

$$\widetilde{\mathfrak{W}} = \left\{\left(\widetilde{W}^n(\cdot\,|\,\cdot,\boldsymbol{s}^n),\widetilde{V}^n(\cdot\,|\,\cdot,\boldsymbol{s}^n)\right) : \boldsymbol{s}^n\in\left(\mathcal{S}^{(1)}\times\mathcal{S}^{(2)}\right)^n\right\}$$

where $\widetilde{V}^n$ is the discrete memoryless channel $\widetilde{V}^n = (V^{(1)}\otimes V^{(2)})^n$ to the wiretapper.

Next, we define two suitable AVWCs, which are themselves useless with zero secrecy capacity, and show that they lead to a positive secrecy capacity if they are used together. Therefore, we make use of an example which first appeared in [7] and which is later also discussed in [8, Example 1]. We use this example to construct the AVC $\mathcal{W}^{(1)}$ to the legitimate receiver. Therefore, let $|\mathcal{X}^{(1)}|=2$, $|\mathcal{Y}^{(1)}|=3$ and define $\mathcal{W}^{(1)} = \{W_1^{(1)},W_2^{(1)}\}$ with

$$W_1^{(1)} := \begin{pmatrix}1&0&0\\0&0&1\end{pmatrix},\qquad W_2^{(1)} := \begin{pmatrix}0&0&1\\0&1&0\end{pmatrix}.$$

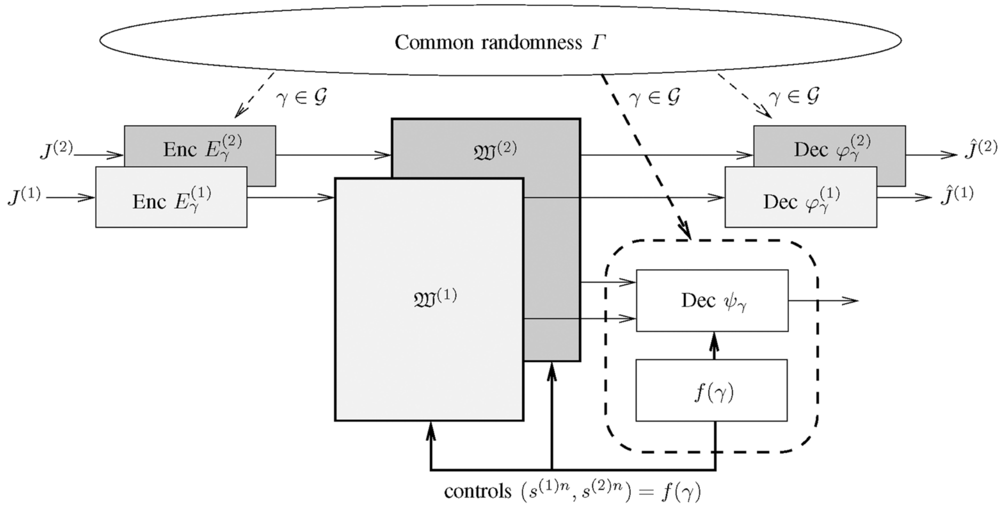

Fig. 5. Communication over two parallel AVWCs $\mathfrak{W}^{(1)}$ and $\mathfrak{W}^{(2)}$, where each of them is useless for transmission of secure communication, i.e., $C_S(\mathfrak{W}^{(1)}, \mathcal{A}(\Gamma)) = C_S(\mathfrak{W}^{(2)}, \mathcal{A}(\Gamma)) = 0$.

Further, let the AVC $\mathcal{V}^{(1)}$ to the wiretapper be consisting of only one element, i.e., $\mathcal{V}^{(1)} = \{V^{(1)}\}$ so that the first AVWC $\mathfrak{W}^{(1)}$ is given by

$$\mathfrak{W}^{(1)} := \left\{ \left(W_1^{(1)}, W_2^{(1)} \right), V^{(1)} \right\}.$$

From [7] we know that the AVC $\mathcal{W}^{(1)}$ to the legitimate receiver is symmetrizable and, hence, we have $C(\mathcal{W}^{(1)}) = 0$ and $C_{\mathrm{ran}}(\mathcal{W}^{(1)}) > 0$. Since $\mathcal{W}^{(1)}$ is symmetrizable, we know from Theorem 2 that the secrecy capacity is zero, i.e., $C_S(\mathfrak{W}^{(1)}, \mathcal{A}) = 0$. Since the AVC $\mathcal{V}^{(1)}$ to the wiretapper consists of only one element, there obviously exists a best channel to the wiretapper so that Proposition 1 yields $C_{S,\mathrm{ran}}(\mathfrak{W}^{(1)}, \mathcal{A}) > 0$ if $V^{(1)}$ is chosen accordingly.[2]

Now, let us define the second AVWC $\mathfrak{W}^{(2)}$. Therefore, let $|\mathcal{X}^{(2)}| = |\mathcal{Y}^{(2)}| = |\mathcal{Z}^{(2)}| = 2$ and $0 < p < q < \frac{1}{2}$ and define $\mathcal{W}^{(2)} = \{W^{(2)}\}$ with

$$W^{(2)} := \begin{pmatrix} 1-q & q \\ q & 1-q \end{pmatrix}$$

so that $C(\mathcal{W}^{(2)}) = 1 - H_2(q) > 0$, and $\mathcal{V}^{(2)} = \{V^{(2)}\}$ with

$$V^{(2)} := \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$$

so that $C(\mathcal{V}^{(2)}) = 1 - H_2(p) > 0$ with $H_2(\,\cdot\,)$ the binary entropy function. With this, we construct the second AVWC $\mathfrak{W}^{(2)}$ as

$$\mathfrak{W}^{(2)} = \left\{ W^{(2)}, V^{(2)} \right\}.$$

Since $C(\mathcal{V}^{(2)}) > C(\mathcal{W}^{(2)})$, we obtain $C_S(\mathfrak{W}^{(2)}, \mathcal{A}) = C_{S,\mathrm{ran}}(\mathfrak{W}^{(2)}, \mathcal{A}) = 0$. Note that this provides an example for an AVWC with a nonsymmetrizable AVC to the legitimate receiver whose CR-assisted secrecy capacity is zero.

Thus, we have constructed two AVWCs $\mathfrak{W}^{(1)}$ and $\mathfrak{W}^{(2)}$, whose both secrecy capacities are zero, i.e., $C_S(\mathfrak{W}^{(1)}, \mathcal{A}) = C_S(\mathfrak{W}^{(2)}, \mathcal{A}) = 0$. In the following we denote the system which results from the parallel use of both channels by $\widetilde{\mathfrak{W}} = \mathfrak{W}^{(1)} \otimes \mathfrak{W}^{(2)}$, cf. also Fig. 5. Note that since both AVWCs are used in a orthogonal manner, we have for each AVWC $\mathfrak{W}^{(i)}$ encoders $\{E_\gamma^{(i)}\}_{\gamma \in \mathcal{G}}$ and decoders $\{\varphi_\gamma^{(i)}\}_{\gamma \in \mathcal{G}}$, $i = 1, 2$, according to Definitions 1 and 6 respectively.

B. Protocol for Super-Activation

Next, we argue how both channels, which are useless for secure transmission, can be used to *super-activate* the system to allow for secure communication at nonzero secrecy rates. The joint use of both AVWCs results in a joint encoder $E_\gamma : \mathcal{J}_n \rightarrow \mathcal{P}((\mathcal{X}^{(1)} \times \mathcal{X}^{(2)})^n)$ and a joint decoder $\varphi_\gamma : (\mathcal{Y}^{(1)} \times \mathcal{Y}^{(2)})^n \rightarrow \mathcal{J}_n$. The corresponding communication scenario is depicted in Fig. 6.

1) Active Wiretapper: Here we discuss the case where the wiretapper does not exploit his access to the common randomness. In the following we show that we have

$$C_S(\widetilde{\mathfrak{W}}, \mathcal{A}) = C_S\left(\mathfrak{W}^{(1)} \otimes \mathfrak{W}^{(2)}, \mathcal{A}\right) > 0$$

although $C_S(\mathfrak{W}^{(1)}, \mathcal{A}) = C_S(\mathfrak{W}^{(2)}, \mathcal{A}) = 0$.

The first observation is that $C_{S,\mathrm{ran}}(\widetilde{\mathfrak{W}}, \mathcal{A}) > 0$, which can easily be achieved by using only $\mathfrak{W}^{(1)}$ so that we obviously have $C_{S,\mathrm{ran}}(\widetilde{\mathfrak{W}}, \mathcal{A}) \geq C_{S,\mathrm{ran}}(\mathfrak{W}^{(1)}, \mathcal{A}) > 0$. The second crucial observation is the following.

Lemma 6: The combined AVC $\widetilde{\mathcal{W}} = \{(W_1^{(1)} \otimes W^{(2)}), (W_2^{(1)} \otimes W^{(2)})\}$ to the legitimate receiver is nonsymmetrizable.

Proof: It suffices to show that $\widetilde{\mathcal{W}}$ is nonsymmetrizable according to Definition 5, since then Lemma 1 immediately implies that it is also nonsymmetrizable under randomized encoding according to Definition 9.

In general, to show that a parallel AVC $\widetilde{\mathcal{W}}$ with channels $\widetilde{W} : \mathcal{X}^{(1)} \times \mathcal{X}^{(2)} \times \mathcal{S}^{(1)} \times \mathcal{S}^{(2)} \rightarrow \mathcal{P}(\mathcal{Y}^{(1)} \times \mathcal{Y}^{(2)})$ is nonsymmetrizable, we have to show that for all stochastic matrices $U : \mathcal{X}^{(1)} \times \mathcal{X}^{(2)} \rightarrow \mathcal{P}(\mathcal{S}^{(1)} \times \mathcal{S}^{(2)})$ there exists $\boldsymbol{x}_1 = (x_1^{(1)}, x_1^{(2)}), \boldsymbol{x}_2 =$

[2] For example, if we choose the useless channel $V^{(1)} := \begin{pmatrix} 1/3 & 1/3 & 1/3 \\ 1/3 & 1/3 & 1/3 \end{pmatrix}$ for $|\mathcal{X}^{(1)}| = 2$ and $|\mathcal{Z}^{(1)}| = 3$ as the channel to the wiretapper, we obviously have $C(\mathcal{V}^{(1)}) = 0$ so that $C_{S,\mathrm{ran}}(\mathfrak{W}^{(1)}, \mathcal{A}) > 0$.

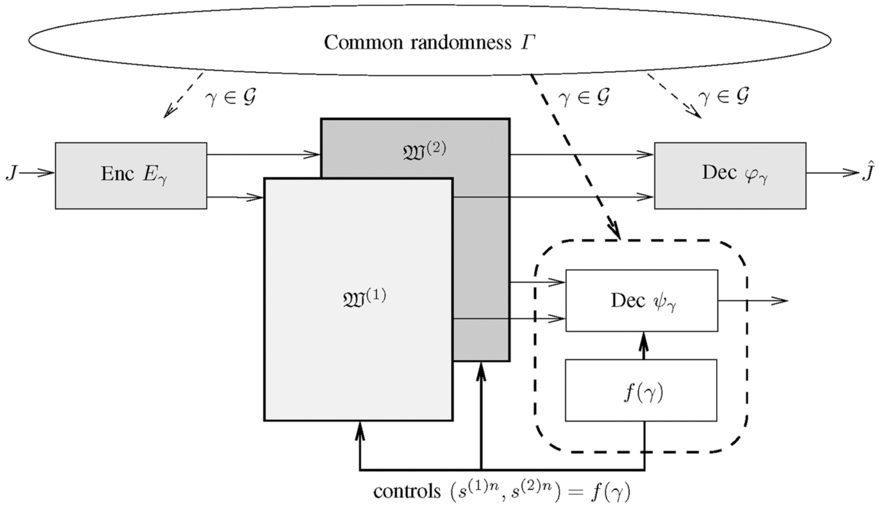

Fig. 6. Joint use of two parallel AVWCs $\mathfrak{W}^{(1)}$ and $\mathfrak{W}^{(2)}$, where each of them is useless for transmission of secure communication, i.e., $C_S(\mathfrak{W}^{(1)}, \mathcal{A}(\Gamma)) = C_S(\mathfrak{W}^{(2)}, \mathcal{A}(\Gamma)) = 0$.

$(x_2^{(1)}, x_2^{(2)}) \in \mathcal{X}^{(1)} \times \mathcal{X}^{(2)}$ and $\boldsymbol{y} = (y^{(1)}, y^{(2)}) \in \mathcal{Y}^{(1)} \times \mathcal{Y}^{(2)}$ such that

$$\sum_{\boldsymbol{s}} \widetilde{W}(\boldsymbol{y}|\boldsymbol{x}_1, \boldsymbol{s}) U(\boldsymbol{s}\,|\,\boldsymbol{x}_2) = \sum_{\boldsymbol{s}} \widetilde{W}(\boldsymbol{y}\,|\,\boldsymbol{x}_2, \boldsymbol{s}) U(\boldsymbol{s}\,|\,\boldsymbol{x}_1) \tag{22}$$

with $\boldsymbol{s} = (s^{(1)}, s^{(2)})$ does not hold, cf. also (7).

In our context, condition (22) reads as

$$\sum_{s=1}^{2} W_s^{(1)}\left(y^{(1)}\middle|\, x_1^{(1)}\right) W^{(2)}\left(y^{(2)}\middle|\, x_1^{(2)}\right) U\left(s\,|\, x_2^{(1)}, x_2^{(2)}\right)$$
$$= \sum_{s=1}^{2} W_s^{(1)}\left(y^{(1)}\middle|\, x_2^{(1)}\right) W^{(2)}\left(y^{(2)}\middle|\, x_2^{(2)}\right) U\left(s\,|\, x_1^{(1)}, x_1^{(2)}\right).$$

Next we argue that for any $U : \mathcal{X}^{(1)} \times \mathcal{X}^{(2)} \to \mathcal{P}(\mathcal{S}^{(1)} \times \mathcal{S}^{(2)})$ and a specific fixed choice of $\boldsymbol{x}_1, \boldsymbol{x}_2 \in \mathcal{X}^{(1)} \times \mathcal{X}^{(2)}$ and $\boldsymbol{y} \in \mathcal{Y}^{(1)} \times \mathcal{Y}^{(2)}$ this condition does not hold anymore. Therefore, we set $\boldsymbol{x}_1 = (x^{(1)}, x_1^{(2)})$, $\boldsymbol{x}_2 = (x^{(1)}, x_2^{(2)})$ and $\boldsymbol{y} = (y^{(1)}, y^{(2)})$ so that we get

$$\xi(x_2^{(2)}) W^{(2)}\left(y^{(2)}\middle|\, x_1^{(2)}\right) = \xi\left(x_1^{(2)}\right) W^{(2)}\left(y^{(2)}\middle|\, x_2^{(2)}\right) \tag{23}$$

with $\xi(x_2^{(2)}) = \sum_{s=1}^{2} W_s^{(1)}(y^{(1)}\,|\,x^{(1)}) U(s\,|\,x^{(1)}, x_2^{(2)})$ and $\xi(x_1^{(2)}) = \sum_{s=1}^{2} W_s^{(1)}(y^{(1)}\,|\,x^{(1)}) U(s\,|\,x^{(1)}, x_1^{(2)})$. If we sum up all $y^{(2)} \in \mathcal{Y}^{(2)}$ on both sides, we get

$$\begin{aligned}\xi(x_2^{(2)}) &= \xi\left(x_2^{(2)}\right) \sum_{y^{(2)} \in \mathcal{Y}^{(2)}} W^{(2)}\left(y^{(2)}\middle|\, x_1^{(2)}\right)\\ &= \xi\left(x_1^{(2)}\right) \sum_{y^{(2)} \in \mathcal{Y}^{(2)}} W^{(2)}\left(y^{(2)}\middle|\, x_2^{(2)}\right)\\ &= \xi\left(x_1^{(2)}\right)\end{aligned}$$

since $W^{(2)}$ is a stochastic matrix. With $\xi(x_2^{(2)}) = \xi(x_1^{(2)})$ we get from (23) that

$$W^{(2)}\left(y^{(2)}\middle|\, x_1^{(2)}\right) = W^{(2)}\left(y^{(2)}\middle|\, x_2^{(2)}\right)$$

for all $x_1^{(2)}, x_2^{(2)} \in \mathcal{X}^{(2)}$ and $y^{(2)} \in \mathcal{Y}^{(2)}$. But this only holds for the useless channel with zero capacity, i.e., $C(W^{(2)}) = 0$. But this contradicts the assumption of $C(W^{(2)}) > 0$ (cf. corresponding construction of the channel in Section VI-A), which proves the assertion that combined AVC $\widetilde{\mathcal{W}}$ is nonsymmetrizable. ■

Since $\widetilde{\mathcal{W}}$ is nonsymmetrizable, from Proposition 1 we then have $C_S(\widetilde{\mathfrak{W}}, \mathcal{A}) > 0$.

The protocol which actually achieves positive secrecy rates for the system $\widetilde{\mathfrak{W}}$ is given as follows. To securely transmit message $j \in \mathcal{J}_n$ to the legitimate receiver, the sender first creates $\gamma \in \mathcal{G}$.

To make $\gamma \in \mathcal{G}$ also available at the legitimate receiver, the sender transmits $E^{(2)}(\gamma)$ over the second AVWC $\mathfrak{W}^{(2)}$. Since the corresponding link $\mathcal{W}^{(2)}$ to the legitimate user is nonsymmetrizable, we have $C(\mathcal{W}^{(2)}) > 0$ and there exists decoding sets $\{\mathcal{D}_\gamma^{(2)} : \gamma \in \mathcal{G}\}$ making $\gamma \in \mathcal{G}$ at the legitimate receiver available. Note that as $C(V^{(2)}) > C(W^{(2)})$, it is very likely that $\gamma \in \mathcal{G}$ will be also available at the wiretapper. Thus, for the first AVWC $\mathfrak{W}^{(1)}$ we are in the same situation as in Section IV, i.e., common randomness is available at the legitimate users and the wiretapper.

For the first AVWC $\mathfrak{W}^{(1)}$, the legitimate users can use the common randomness created through the second AVWC $\mathfrak{W}^{(2)}$ to use a CR-assisted strategy. The sender transmits $E_\gamma^{(1)}(j)$ and the legitimate user uses decoding sets $\{\mathcal{D}_{\gamma,j}^{(1)} : j \in \mathcal{J}_n\}$ for decoding. As $C_{S,\mathrm{ran}}(\mathfrak{W}^{(1)}, \mathcal{A}) > 0$, secure communication at a positive secrecy rate is possible. This completes the protocol which achieves a secrecy rate $C_S(\widetilde{\mathfrak{W}}, \mathcal{A}) = C_S(\mathfrak{W}^{(1)} \otimes \mathfrak{W}^{(2)}, \mathcal{A}) > 0$.

2) Active Wiretapper Exploiting CR: From Theorem 3 we know that the CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma))$ of the AVWC $\mathfrak{W}$ with active wiretapper exploiting CR displays the same behavior as the secrecy capacity $C_S(\mathfrak{W}, \mathcal{A})$. Thus, it is convincing that the super-activation discussed above also holds for active wiretappers, i.e.,

$$C_{S,\mathrm{ran}}(\widetilde{\mathfrak{W}}, \mathcal{A}(\Gamma)) = C_{S,\mathrm{ran}}\left(\mathfrak{W}^{(1)} \otimes \mathfrak{W}^{(2)}, \mathcal{A}(\Gamma)\right) > 0$$

although we have $C_{S,\mathrm{ran}}(\mathfrak{W}^{(1)}, \mathcal{A}(\Gamma)) = C_{S,\mathrm{ran}}(\mathfrak{W}^{(2)}, \mathcal{A}(\Gamma)) = 0$ by construction and Theorem 3.

It is clear that the protocol for naive active wiretappers as discussed above also works in the case of active wiretappers exploiting CR as briefly outlined in the following. The common randomness available at all users is useless as the wiretapper can choose his state sequence accordingly based on this resource. Therefore, similarly to the previous case, the sender uses the second AVWC $\mathfrak{W}^{(2)}$ to create "new" common randomness at all users. This allows proceeding as in the previous case to achieve positive secrecy rates. Note that due to the communication model, the wiretapper is not allowed to adapt his state sequence on the new common randomness. Accordingly, this shows the limitations of the used model and encourages further investigations on more general setups as discussed below in the conclusions.

However, the following observation is noteworthy. For both AVWCs $\mathfrak{W}^{(1)}$ and $\mathfrak{W}^{(2)}$ the active wiretapper exploiting CR can control the corresponding state sequences. This means, in principle, he can choose for $\mathfrak{W}^{(1)}$ a function $f_1 : \mathcal{G}_1 \rightarrow \mathcal{S}_1^n$ and for $\mathfrak{W}^{(2)}$ a function $f_2 : \mathcal{G}_2 \rightarrow \mathcal{S}_2^n$. But for the parallel use $\widetilde{\mathfrak{W}} = \mathfrak{W}^{(1)} \otimes \mathfrak{W}^{(2)}$ he is further able to use a joint strategy $f' : \mathcal{G}_1 \times \mathcal{G}_2 \rightarrow \mathcal{S}_1^n \times \mathcal{S}_2^n$ so that his strategy space becomes larger. However, the wiretapper is not able to gain from his increased strategy space.

VII. Conclusion

In this paper, we studied the arbitrarily varying wiretap channel (AVWC) with active wiretappers, who may or may not exploit available common randomness. It was previously shown in [11] that the secrecy capacity $C_S(\mathfrak{W}, \mathcal{A})$ of the AVWC $\mathfrak{W}$ with active wiretapper (not exploiting CR) displays a dichotomy behavior: it either equals its CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A})$ or else is zero. The main techniques to characterize the secrecy capacity and its behavior are the *random code reduction*, *elimination of randomness*, and the *concept of symmetrizability*.

Here, we extended and generalized these techniques in a proper way such that imposed secrecy requirements and active wiretappers exploiting CR are incorporated. In particular, it has been shown that randomized encoding is crucial for achieving secrecy in AVWCs. This necessitated a more generalized concept of *symmetrizability for randomized encoding*, which is in contrast to the classical AVC (without secrecy constraints) where deterministic encoding suffices.

These generalized techniques allowed for proving that the CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma))$ of the AVWC $\mathfrak{W}$ with active wiretapper exploiting CR displays the same characteristic as the secrecy capacity $C_S(\mathfrak{W}, \mathcal{A})$: it either equals its CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A})$ or else is zero. Interestingly, this dichotomy behavior shows that the secrecy capacity is non longer solely characterized by entropic quantities. In particular, this determines the optimal strategy of an active wiretapper. If the CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma))$ is positive, it actually equals $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A})$. Thus, in this case an active wiretapper exploiting CR is as (in)effective as an active wiretapper, who does not exploit available CR. Thus, the only reasonable strategy for such a wiretapper must be to symmetrize the channel to the legitimate receiver to destroy their communication. This is completely characterized using the generalized concept of symmetrizability for randomized encoding.

The techniques developed in this paper are not only powerful enough to completely characterize the CR-assisted secrecy capacity of the AVWC with active wiretapper exploiting CR, but also allow for describing new phenomena. In particular, we gave an example how two useless AVWCs, each with zero secrecy capacity, can be used together such that the system is super-activated allowing for secure transmission at nonzero secrecy rates. The super-activation in AVWCs is a consequence of the imposed secrecy requirement, since in contrast to that, for classical AVCs without secrecy requirement, super-activation is not possible to the best of our knowledge. Such results are particularly important as they give valuable insights for the design and medium access control of communication systems with secrecy requirements. Moreover, to the best of our knowledge, this provides the first example for nonquantum communication systems where the world view of classical additivity of basic resources does not hold anymore in the sense that "$0 + 0 > 0$."

Although the secrecy capacities $C_S(\mathfrak{W}, \mathcal{A})$ and $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A}(\Gamma))$ of the AVWC are completely characterized in terms of the CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A})$ (they either equals $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A})$ or else are zero), a precise characterization of $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A})$ is still missing. This is in contrast to the classical AVC (without secrecy constraint), where a single-letter characterization of the CR-assisted capacity was successfully established by linking it to a suitable compound channel [8]. On the other hand, for the AVWC it is still unknown if its CR-assisted secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A})$ can be linked to a suitable compound wiretap channel. Only for some special cases, certain lower bounds on $C_{S,\mathrm{ran}}(\mathfrak{W}, \mathcal{A})$ have been established in terms of suitable compound wiretap channels [11]. In addition, in [17] the corresponding compound wiretap channel is studied for the strong secrecy criterion and a multiletter characterization of its secrecy capacity has been established. A precise single-letter characterization of the secrecy capacity has been established only for certain special cases [17], [18]. This determines an interesting and important direction of future work.

In this paper we studied active wiretappers which were able to select the state sequence based their the access to the common randomness, i.e., $s^n = f(\gamma)$ for $\gamma \in \mathcal{G}$. For future work, it would be interesting to analyze what happens if the legitimate users and the wiretapper do not observe the same realization $\gamma \in \mathcal{G}$, but only correlated versions. In addition, an interesting research direction would be the study of active wiretappers with other abilities. For example, the wiretapper could be able to select the state sequence based on the previous/current received channel outputs, i.e., $s_i = f(z^i), i = 1, \dots, n$, with $z^i = (z_1, \dots, z_i)$ the received output sequence. Another interesting scenario would be the case in which the wiretapper and the jammer, i.e., the one who selects the state sequence, are at distinct locations, and in which the jammer (but not the wiretapper) has access to the message. This offers the possibility for the jammer to select the state sequence in such a way that it reveals more information to the wiretapper, i.e., $s^n = f(j)$ for $j \in \mathcal{J}_n$.

ACKNOWLEDGMENT

The authors gratefully acknowledge valuable discussions with the Federal Office for Information Security (BSI) of Germany which raised the problem of secure communication in the presence of active wiretappers. The authors also thank the anonymous reviewer for valuable comments and suggestions and especially for discussing interesting directions of future work.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[2] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[3] E. A. Jorswieck, A. Wolf, and S. Gerbracht, "Secrecy on the physical layer in wireless networks," *Trends Telecomm. Technol.*, pp. 413–435, Mar. 2010.

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

[5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[6] R. F. Schaefer and H. Boche, "Physical layer service integration in wireless networks—Signal processing challenges," *IEEE Signal Process. Mag.*, to be published.

[7] D. Blackwell, L. Breiman, and A. J. Thomasian, "The capacities of certain channel classes under random coding," *Ann. Math. Stat.*, vol. 31, no. 3, pp. 558–567, 1960.

[8] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Z. Wahrscheinlichkeitstheorie verw. Gebiete*, vol. 44, pp. 159–175, 1978.

[9] I. Csiszár and P. Narayan, "The capacity of the arbitrarily varying channel revisited: Positivity, constraints," *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 181–193, Mar. 1988.

[10] E. MolavianJazi, M. Bloch, and J. N. Laneman, "Arbitrary jamming can preclude secure communication," in *Proc. Allerton Conf. Commun., Control, Computing*, Urbana-Champaign, IL, USA, Sep. 2009, pp. 1069–1075.

[11] I. Bjelaković, H. Boche, and J. Sommerfeld, "Capacity Results for Arbitrarily Varying Wiretap Channels," in *Information Theory, Combinatorics, and Search Theory*. New York, NY, USA: Springer, 2013, pp. 123–144.

[12] I. Csiszár, "Almost independence and secrecy capacity," *Probl. Pered. Inform.*, vol. 32, no. 1, pp. 48–57, 1996.

[13] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proc. EUROCRYPT 2000, Lecture Notes in Computer Science*, May 2000, vol. 1807, pp. 351–368, Springer-Verlag.

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

[15] G. Smith, J. A. Smolin, and J. Yard, "Quantum communication with Gaussian channels of zero quantum capacity," *Nature Photon.*, vol. 5, no. 10, pp. 624–627, Oct. 2011.

[16] G. Giedke and M. M. Wolf, "Quantum communication: Super-activated channels," *Nature Photon.*, vol. 5, no. 10, pp. 578–580, Oct. 2011.

[17] I. Bjelaković, H. Boche, and J. Sommerfeld, "Secrecy results for compound wiretap channels," *Probl. Inf. Transmission*, vol. 49, no. 1, pp. 73–98, Mar. 2013.

[18] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw.*, pp. 1–13, 2009, Article ID 142374.

Holger Boche (M'04–SM'07–F'11) received the Dipl.-Ing. and Dr.-Ing. degrees in electrical engineering from the Technische Universität Dresden, Dresden, Germany, in 1990 and 1994, respectively. He graduated in mathematics from the Technische Universität Dresden in 1992. From 1994 to 1997, he did postgraduate studies in mathematics at the Friedrich-Schiller Universität Jena, Jena, Germany. He received the Dr. rer. nat. degree in pure mathematics from the Technische Universität Berlin, Berlin, Germany, in 1998.

In 1997, he joined the Heinrich-Hertz-Institut (HHI) für Nachrichtentechnik Berlin, Berlin, Germany. Starting in 2002, he was a Full Professor for mobile communication networks with the Institute for Communications Systems, Technische Universität Berlin. In 2003, he became Director of the Fraunhofer German-Sino Lab for Mobile Communications, Berlin, Germany, and in 2004 he became the Director of the Fraunhofer Institute for Telecommunications (HHI), Berlin, Germany. Since October 2010, he has been with the Institute of Theoretical Information Technology and Full Professor at the Technische Universität München, Munich, Germany. He was a Visiting Professor with the ETH Zurich, Zurich, Switzerland, during the 2004 and 2006 Winter terms, and with KTH Stockholm, Stockholm, Sweden, during the 2005 Summer term.

Prof. Boche is a Member of IEEE Signal Processing Society SPCOM and SPTM Technical Committee. He was elected a Member of the German Academy of Sciences (Leopoldina) in 2008 and of the Berlin Brandenburg Academy of Sciences and Humanities in 2009. He received the Research Award "Technische Kommunikation" from the Alcatel SEL Foundation in October 2003, the "Innovation Award" from the Vodafone Foundation in June 2006, and the Gottfried Wilhelm Leibniz Prize from the Deutsche Forschungsgemeinschaft (German Research Foundation) in 2008. He was corecipient of the 2006 IEEE Signal Processing Society Best Paper Award and recipient of the 2007 IEEE Signal Processing Society Best Paper Award.

Rafael F. Schaefer (formerly Wyrembelski) (S'08–M'12) received the Dipl.-Ing. degree in electrical engineering and computer science, in 2007, from the Technische Universität Berlin, Germany, and the Dr.-Ing. degree in electrical engineering, in 2012, from the Technische Universität München.

Between 2007 and 2010, he worked as a research and teaching assistant at the Heinrich-Hertz-Lehrstuhl für Mobilkommunikation at the Technische Universität Berlin, Germany. Since November 2010, he has been with the Lehrstuhl für Theoretische Informationstechnik at the Technische Universität München, Germany, where he is currently working as a Postdoctoral researcher.