Capacity Results, Coordination Resources, and Super-Activation in Wiretap Channels

Holger Boche and Rafael F. Schaefer

Lehrstuhl für Theoretische Informationstechnik
Technische Universität München, Germany

***Abstract*—Availability of channel state information, especially to non-legitimate users, is one major challenge for secure communication in wireless systems. For arbitrarily varying channels (AVC), *coordination resources* such as common randomness have been shown to be important for reliable communication; especially for symmetrizable AVCs. In this paper, the *arbitrarily varying wiretap channel (AVWC) with active wiretapper* is studied. Such an wiretapper may or may not exploit his knowledge about the coordination resources to control the channel conditions. Secrecy capacity results are derived for different forms of coordination resources including common randomness and correlated sources. Finally, it is demonstrated how two orthogonal AVWCs, each with zero secrecy capacity, i.e., *useless* for secure transmission, can be super-activated to a *useful* channel allowing for secure communication at non-zero secrecy rates.**

I. Introduction

Wireless communication systems are inherently vulnerable for eavesdropping due to the open nature of the wireless medium. In this context, the concept of information theoretic security is becoming attractive, since it solely uses the physical properties of the wireless channel in order to establish security. It was initiated by Wyner, who introduced the *wiretap channel* [1]. This involves security with one legitimate transmitter-receiver pair and one wiretapper. Recently, there is growing interest in information theoretic security, cf. [2, 3].

Usually the wiretapper is assumed to be passive in the sense that he (or she) simply tries to eavesdrop the communication. In contrast to that, we consider in this paper more powerful wiretappers which 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) [4, 5] 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.

For AVCs it has been shown that *coordination resources*, such as *common randomness (CR)* or *correlated sources (CS)*, are important and often necessary for reliable communication, cf. [4] and [6]. They allow legitimate users to use more sophisticated strategies by coordinating their choice of encoder and decoder. But they also pave the way for more powerful wiretappers. An active wiretapper may exploit the available coordination resources for controlling the channel states.

First results for the AVWC with active wiretapper appeared in [7–9]. In these works, either no coordination resources, i.e., a deterministic design with pre-specified encoder and decoder, or full common randomness is assumed. In this paper, we also consider a weaker form of coordination resources given by correlated sources. Here, all users observe only correlated versions of a common random source which further might be available only causally, e.g., a common broadcast signal. We establish capacity results for different kinds of coordination resources. In particular, these yield a complete characterization for the AVWC with active wiretapper exploiting CR.

In this context, new phenomena of *super-activation* appear, which have been observed only for quantum communication systems [10–12]. We construct an example without feedback, how two AVWCs, each useless with zero secrecy capacity, can be used together to super-activate the whole system to allow for secure communication at non-zero secrecy rates. This shows that the classical additivity of basic resources does not hold anymore (in the sense that "$0 + 0 > 0$") if secrecy requirements are imposed.[1]

II. Arbitrarily Varying Wiretap Channels

Let $\mathcal{X}$ and $\mathcal{Y}$, $\mathcal{Z}$ be finite input and output sets and $\mathcal{S}$ be a finite state set. 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 $s^n \in \mathcal{S}^n$ of length n, the discrete memoryless channel to the legitimate receiver is given by $W^n(y^n|x^n, s^n) := \prod_{i=1}^n W(y_i|x_i, s_i)$ 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.,

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

This work was supported in part by the German Ministry of Education and Research (BMBF) under Grant 01BQ1050 and by the German Research Foundation (DFG) under Grant BO 1734/25-1.

[1] *Notation:* Discrete random variables are denoted by capital letters and their realizations and ranges by lower case and script letters; $\mathbb{N}$ is the set of positive integers; $I(\cdot;\cdot)$ is the mutual information; $\mathcal{P}(\cdot)$ is the set of all probability distributions and $\mathbb{E}_X[\cdot]$ is the expectation according to X.

978-1-4799-0446-4/13/$31.00 ©2013 IEEE

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

Definition 1: The *arbitrarily varying wiretap channel (AVWC)* $\mathfrak{W}$ is given by the families of pairs of channels with common input as

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

III. Coordination Resources and Code Concepts

A. Traditional Wiretap Codes

If no coordination resources are available, a deterministic code design with pre-specified encoder and decoder is used.

Definition 2: An (n,J_n)*-code* $\mathcal{C}$ for the AVWC $\mathfrak{W}$ 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 $\mathcal{J}_n \coloneqq \{1,...,J_n\}$ and a decoder $\varphi : \mathcal{Y}^n \to \mathcal{J}_n$ given by a collection of disjoint decoding sets

$$\big\{\mathcal{D}_j \subset \mathcal{Y}^n : j \in \mathcal{J}_n\big\}. \tag{2}$$

Then the average probability of decoding error at the legitimate receiver for state sequence $s^n \in \mathcal{S}^n$ is given by

$$\bar{e}_n(s^n) \coloneqq \frac{1}{|\mathcal{J}_n|}\sum_{j\in\mathcal{J}_n}\sum_{x^n\in\mathcal{X}^n} W^n(\mathcal{D}_j^c|x^n,s^n)E(x^n|j).$$

We define the maximum as $\bar{e}_n \coloneqq \max_{s^n\in\mathcal{S}^n}\bar{e}_n(s^n)$.

To keep the message secret from the wiretapper for all state sequences $s^n \in \mathcal{S}^n$, we require

$$\max_{s^n\in\mathcal{S}^n} I(J;Z_{s^n}^n|\mathcal{C}) \le \epsilon_n \tag{3}$$

for $\epsilon_n > 0$ with J the random variable uniformly distributed over the set of messages $\mathcal{J}_n$ and $Z_{s^n}^n = (Z_{s_1}, Z_{s_2}, ..., Z_{s_n})$ the channel output at the wiretapper for state sequence $s^n \in \mathcal{S}^n$. This criterion is known as *strong secrecy*.

Definition 3: A number R_S is an *achievable secrecy rate* for the AVWC $\mathfrak{W}$ 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 $n \ge n(\delta)$ we have $\frac{1}{n}\log J_n \ge R_S - \delta$ and $\max_{s^n\in\mathcal{S}^n} I(J;Z_{s^n}^n|\mathcal{C}) \le \epsilon_n$ while $\bar{e}_n, \epsilon_n \to 0$ as $n \to \infty$. The *secrecy capacity* $C_S(\mathfrak{W})$ is given by the supremum of all achievable secrecy rates R_S.

B. Common-Randomness-Assisted Codes

If *common randomness* is available at all users including the wiretapper, then the legitimate users can use this to coordinate their choice of encoder and decoder. This is modeled by a random variable U distributed according to $P_U \in \mathcal{P}(\mathcal{U})$. Then, (1) and (2) depend now on the realization $u \in \mathcal{U}$.

Remark 1: If the wiretapper has no access to the CR, the legitimate users can immediately use this resource to create a secret key and therewith keeping the wiretapper ignorant.

A *CR-assisted* (n,J_n,U)*-code* $\mathcal{C}_{\text{ran}}$ for the AVWC $\mathfrak{W}$ is a family of encoders E_u and decoding sets $\{\mathcal{D}_{u,j} : j \in \mathcal{J}_n\}$, where $u \in \mathcal{U}$ is chosen according to $P_U \in \mathcal{P}(\mathcal{U})$.

The average probability of error for $s^n \in \mathcal{S}^n$ becomes

$$\bar{e}_{\text{ran},n}(s^n) \coloneqq \mathbb{E}_U \frac{1}{|\mathcal{J}_n|}\sum_{j\in\mathcal{J}_n}\sum_{x^n\in\mathcal{X}^n} W^n(\mathcal{D}_{u,j}^c|x^n,s^n)E_u(x^n|j)$$

and, accordingly, $\bar{e}_{\text{ran},n} \coloneqq \max_{s^n\in\mathcal{S}^n}\bar{e}_{\text{ran},n}(s^n)$. The secrecy constraint (3) becomes $\max_{s^n\in\mathcal{S}^n}\mathbb{E}_U I(J;Z_{s^n}^n|\mathcal{C}_{\text{ran}}) \le \epsilon_n$.

Then, the definition of the *CR-assisted secrecy capacity* $C_{S,\text{ran}}(\mathfrak{W})$ follows accordingly.

C. Correlation-Assisted Codes

A weaker form of coordination resources are *correlated sources* $(U^n,Q^n)_{n=1}^\infty$ with $I(U;Q) > 0$, where the transmitter observes U^n and the legitimate receiver Q^n. Then, the encoder depends only on $u^n \in \mathcal{U}^n$ and the decoder only on $q^n \in \mathcal{Q}^n$. The wiretapper is assumed to observe both U^n and Q^n.

Remark 2: Correlated sources $(U^n,Q^n)_{n=1}^\infty$ are in fact a weaker resource than common randomness U, since it is impossible to extract common randomness from correlated sources. Moreover, it is not robust in the sense that the set of all probability distributions, which would allow common randomness extraction, is closed, nowhere dense, and has zero Lebesgue measure, cf [13, Theorem 1 and Remark 2].

A *CS-assisted* $(n,J_n,(U,Q))$*-code* $\mathcal{C}_{\text{cor}}$ for the AVWC $\mathfrak{W}$ is given by a family of encoders E_{u^n} and decoding sets $\{\mathcal{D}_{q^n,j} : j \in \mathcal{J}_n\}$, where $(u^n,q^n) \in \mathcal{U}^n \times \mathcal{Q}^n$ are chosen according to $P_{U^nQ^n} = \prod_{i=1}^n P_{UQ} \in \mathcal{P}(\mathcal{U}^n \times \mathcal{Q}^n)$.

The average probability of error for $s^n \in \mathcal{S}^n$ becomes

$$\bar{e}_{\text{cor},n}(s^n) \coloneqq \mathbb{E}_{U^nQ^n}\frac{1}{|\mathcal{J}_n|}\sum_{j\in\mathcal{J}_n}\sum_{x^n\in\mathcal{X}^n} W^n(\mathcal{D}_{q^n,j}^c|x^n,s^n)E_{u^n}(x^n|j)$$

and accordingly $\bar{e}_{\text{cor},n} \coloneqq \max_{s^n\in\mathcal{S}^n}\bar{e}_{\text{cor},n}(s^n)$. Further, the secrecy criterion becomes

$$\max_{s^n\in\mathcal{S}^n}\mathbb{E}_{U^nQ^n} I(J;Z_{s^n}^n|\mathcal{C}_{\text{cor}}) \le \epsilon_n. \tag{4}$$

Then, the definition of the *CS-assisted secrecy capacity* $C_{S,\text{cor}}(\mathfrak{W},(U,Q))$ follows accordingly.

We can further weaken the coordination resources by considering causal encoding, where the encoder uses only its current observation u_i, $i = 1,2,...,n$ for encoding, i.e.,

$$E_{u^n}(x^n|j) = \big(E_{u_1}(x_1|j), E_{u_2}(x_2|j), ..., E_{u_n}(x_n|j)\big). \tag{5}$$

The decoding remains the same, since the receiver starts decoding after he received $y^n \in \mathcal{Y}^n$. Thus, the whole coordination resource $q^n \in \mathcal{Q}^n$ is available. We denote the *causal CS-assisted secrecy capacity* by $C_{S,\text{causal}}(\mathfrak{W},(U,Q))$.

Remark 3: The secrecy criterion (4) remains the same for the causal and non-causal case, since the wiretapper can wait until he received the whole sequence. Moreover, it depends only on U^n of the transmitter and not on Q^n of the receiver.

IV. Capacity Results for AVWCs

First studies for the *AVWC with active wiretapper*, who does not exploit available coordination resources, has been studied in [7, 8]. For this, we need the concept of symmetrizability.

Definition 4: An AVC $\mathcal{W}$ is called *symmetrizable* if there exists a stochastic matrix $\sigma : \mathcal{X} \to \mathcal{P}(\mathcal{S})$ such that

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

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

Roughly speaking, a symmetrizable AVC can "emulate" a valid input, which makes it impossible for the decoder to decide on the correct codeword.

Theorem 1 ([8]): If $C_{S,\text{ran}}(\mathfrak{W}) > 0$, then the secrecy capacity $C_S(\mathfrak{W})$ of the AVWC $\mathfrak{W}$ is

$$C_S(\mathfrak{W}) = C_{S,\text{ran}}(\mathfrak{W})$$

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

This shows that coordination resources are important and often indispensable for communication. In particular, for symmetrizable channels, the secrecy capacity is $C_S(\mathfrak{W}) = 0$, while more sophisticated strategies with additional coordination resources allow for non-zero secrecy rates $C_{S,\text{ran}}(\mathfrak{W}) > 0$.

Common randomness is powerful, since transmitter and receiver have exactly the same observation for encoding and decoding available. The question is now what happens if only a weaker form of coordination resources is available.

Theorem 2: Let U, Q be random variables with $I(U;Q) > 0$. Then the causal CS-assisted secrecy capacity $C_{S,\text{causal}}(\mathfrak{W},(U,Q))$ of the AVWC $\mathfrak{W}$ is

$$C_{S,\text{causal}}(\mathfrak{W},(U,Q)) = C_{S,\text{ran}}(\mathfrak{W}). \tag{6}$$

Sketch of Proof: The proof uses the result from [6], where the classical AVC $\mathcal{W}$ (without secrecy) for CS-assisted codes is studied. It is shown that the causal CS-assisted capacity $C_{\text{causal}}(\mathcal{W},(U,Q))$ of the AVC $\mathcal{W}$ equals its CR-assisted capacity $C_{\text{ran}}(\mathcal{W})$, i.e.,

$$C_{\text{causal}}(\mathcal{W},(U,Q)) = C_{\text{ran}}(\mathcal{W}). \tag{7}$$

Note that in [6] it is not explicitly stated that the coordination resources are available only causally, but a careful inspection of the corresponding proof, cf. [6, Equation (2.2)], reveals that the encoding is restricted to be causal as in (5).

This allows us to prove the desired result (6) for the AVWC $\mathfrak{W}$. If $C_{S,\text{ran}}(\mathfrak{W}) = 0$, there is nothing to prove, since we always have $C_{S,\text{causal}}(\mathfrak{W},(U,Q)) \le C_{S,\text{ran}}(\mathfrak{W})$. Therefore, let $C_{S,\text{ran}}(\mathfrak{W}) > 0$, which necessarily implies $C_{\text{ran}}(\mathcal{W}) > 0$ as well and further $C_{\text{causal}}(\mathcal{W},(U,Q)) > 0$ by (7).

Since $C_{\text{causal}}(\mathcal{W},(U,Q)) > 0$, we can use these resources to change over to CR-assisted strategies $\mathcal{C}_{\text{ran}}$, cf. Section III-B. Such codes consist of an ensemble of deterministic codes, where we know from [8] that an ensemble of polynomial size is sufficient to achieve $C_{S,\text{ran}}(\mathfrak{W})$. In more detail, following the *elimination of randomness* and having the secrecy constraint in mind [8], we first transmit the index of the code which is used in $\mathcal{C}_{\text{ran}}$. Since $C_{\text{causal}}(\mathcal{W},(U,Q)) > 0$ and $\mathcal{C}_{\text{ran}}$ is of polynomial size, the indication is possible and its resources are negligible. Then we use $\mathcal{C}_{\text{ran}}$ for transmission. ∎

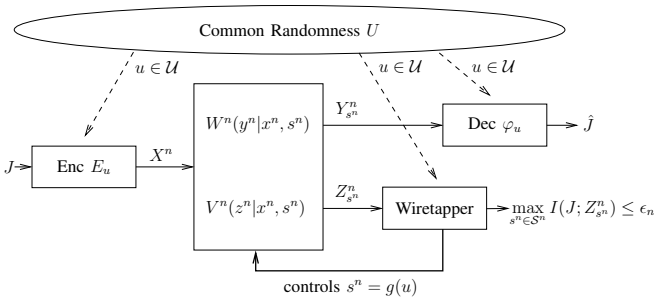

Fig. 1. Arbitrarily varying wiretap channel (AVWC) $\mathfrak{W}$ with active wiretapper. The wiretapper exploits the knowledge about the common randomness $u \in \mathcal{U}$ to control the state sequence $s^n = g(u) \in \mathcal{S}^n$.

From this we immediately obtain the corresponding result, where the coordination resources are available non-causally.

Corollary 1: For U, Q with $I(U;Q) > 0$, the CS-assisted secrecy capacity $C_{S,\text{cor}}(\mathfrak{W},(U,Q))$ is

$$C_{S,\text{cor}}(\mathfrak{W},(U,Q)) = C_{S,\text{ran}}(\mathfrak{W}).$$

This shows that weaker forms of coordination resources such as correlated sources suffices to achieve the same secrecy rates as the CR-assisted strategy.

V. Exploitation of Coordination Resources

An active wiretapper can control the state sequence based on his knowledge about the coordination resources. For common randomness, this is modeled by introducing the function $g \in \mathcal{G}$ with

$$g : \mathcal{U} \to \mathcal{S}^n$$

which characterizes a certain strategy of the wiretapper. This means, based on $u \in \mathcal{U}$, the wiretapper can choose the state sequence $s^n = g(u) \in \mathcal{S}^n$ as shown in Figure 1.

Then for function $g : \mathcal{U} \to \mathcal{S}^n$, the probability of error becomes

$$\bar{e}_{\text{ran},n}(g) := \mathbb{E}_U \frac{1}{|\mathcal{J}_n|} \sum_{j\in\mathcal{J}_n} \sum_{x^n\in\mathcal{X}^n} W^n\big(\mathcal{D}^c_{u,j}|x^n,g(u)\big) E_u(x^n|j)$$

and the mean secrecy criterion

$$\max_{g\in\mathcal{G}} \mathbb{E}_U I(J;Z^n_{g(U)}|\mathcal{C}_{\text{ran}}) \le \epsilon_n.$$

The definition of the *CR-assisted secrecy capacity* $C^{\text{active}}_{S,\text{ran}}(\mathfrak{W})$ for active wiretappers exploiting CR follows accordingly.

In [9] we analyzed active wiretappers exploiting CR if $C^{\text{active}}_{S,\text{ran}}(\mathfrak{W}) > 0$. We showed that if $C^{\text{active}}_{S,\text{ran}}(\mathfrak{W}) > 0$ then

$$C^{\text{active}}_{S,\text{ran}}(\mathfrak{W}) = C_{S,\text{ran}}(\mathfrak{W}) \tag{8}$$

which means that if the CR-assisted secrecy capacity is positive for wiretappers not exploiting CR, then it has the same value for wiretappers exploiting CR. Thus, exploiting CR is as (in)effective as not exploiting and his strategy must be to destroy the communication of the users to get $C^{\text{active}}_{S,\text{ran}}(\mathfrak{W}) = 0$.

Unfortunately, in [9] we missed a complete characterization including $C^{\text{active}}_{S,\text{ran}}(\mathfrak{W}) = 0$. In the following we fill this gap and therewith completely solve and characterize the CR-assisted

secrecy capacity for active wiretappers exploiting CR. To do so, we need a refinement of the concept of symmetrizability, cf. Definition 4. To this end, for any strategy $g : \mathcal{U} \to \mathcal{S}^n$ of the active wiretapper let

$$\overline{W}_g^n(y^n|j,u) \coloneqq \sum_{x^n \in \mathcal{X}^n} W^n(y^n|x^n, g(u)) E_u(x^n|j).$$

Definition 5: An AVC $\mathcal{W}$ is called *actively symmetrizable* if there is a $\hat{\sigma}^n(g|j,u) : \mathcal{J}_n \times \mathcal{U} \to \mathcal{P}(\mathcal{G})$ with

$$\sum_{g\in\mathcal{G}} \overline{W}_g^n(y^n|j_1,u)\hat{\sigma}^n(g|j_2,u) = \sum_{g\in\mathcal{G}} \overline{W}_g^n(y^n|j_2,u)\hat{\sigma}^n(g|j_1,u)$$

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

Lemma 1: If the AVC $\mathcal{W}$ to the legitimate receiver is symmetrizable, then there is a function $g^* : \mathcal{U} \to \mathcal{S}^n$ such that for all $P_U \in \mathcal{P}(\mathcal{U})$ we have

$$\frac{1}{|\mathcal{J}_n|} \sum_{j\in\mathcal{J}_n} \sum_{u\in\mathcal{U}} \overline{W}_{g^*}^n(\mathcal{D}_{u,j}^c|j,u) P_U(u) > \frac{1}{4},$$

i.e., there is a strategy g^* of the active wiretapper which yields a non-zero probability of error at the legitimate receiver.

Proof: The proof follows the lines of [5, Lemma 1] where the corresponding result for the classical AVC (without secrecy) is given. Basically, it can be adapted accordingly by using the refinement of symmetrizability of Definition 5, which takes actively chosen state sequences into account. ∎

This allows us to completely characterize the CR-assisted secrecy capacity for active wiretappers exploiting CR.

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

$$C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = C_{S,\text{ran}}(\mathfrak{W})$$

if and only if the AVC $\mathcal{W}$ to the legitimate receiver is non-symmetrizable. If $\mathcal{W}$ is symmetrizable, then $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = 0$. If $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = 0$ and $C_{S,\text{ran}}(\mathfrak{W}) > 0$, then $\mathcal{W}$ is symmetrizable.

Sketch of Proof: The first part follows from [9], cf. (8). The second part follows from Lemma 1, since for a symmetrizable AVC the probability of decoding error is shown to be bounded away from zero implying zero capacity. ∎

Interestingly, it turns out that $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W})$ displays the same dichotomy behavior as the secrecy capacity $C_S(\mathfrak{W})$: it either equals $C_{S,\text{ran}}(\mathfrak{W})$ or else is zero.

Applying the ideas of Section IV, it is straightforward to also establish the (causal) CS-assisted secrecy capacities for the active wiretapper exploiting coordination resources.

Theorem 4: Let U, Q be random variables with $I(U;Q) > 0$. The (causal) CS-assisted secrecy capacities $C_{S,\text{causal}}^{\text{active}}(\mathfrak{W},(U,Q))$ and $C_{S,\text{cor}}^{\text{active}}(\mathfrak{W},(U,Q))$ are given by

$$C_{S,\text{causal}}^{\text{active}}(\mathfrak{W},(U,Q)) = C_{S,\text{cor}}^{\text{active}}(\mathfrak{W},(U,Q)) = C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}).$$

VI. Super-Activation

For wireless communication systems, 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 sub-channels. 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 in general. 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 [10–12]. To date, it has been expected that such phenomena of *super-activation* of channels only appear in the area of quantum communication. The natural question arises if such phenomena as super-activation are also possible for classical communication systems.

In the following, we study what happens if certain secrecy requirements are imposed. We show that in this case, super-activation also appears in such classical communication systems. Therefore, we define two suitable AVWCs, which are themselves useless with zero secrecy capacity, but lead to a positive secrecy capacity if they are used together. Important is that no other resources such as a public channel or feedback are required or used in this case.

We make use of an example given in [4, Example 1] to construct the AVC $\mathcal{W}^{(1)}$ to the legitimate receiver. Let $|\mathcal{X}| = 2$, $|\mathcal{Y}| = 3$ and define $\mathcal{W}^{(1)} = \{W_1^{(1)}, W_2^{(1)}\}$ with

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

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

$$\mathfrak{W}^{(1)} \coloneqq \big\{(W_1^{(1)}, W_2^{(1)}), V^{(1)}\big\}.$$

From [4] we know that the AVC $\mathcal{W}^{(1)}$ to the legitimate receiver is symmetrizable and, hence, we have $C(\mathcal{W}^{(1)}) = 0$ and $C_{\text{ran}}(\mathcal{W}^{(1)}) > 0$. Since $\mathcal{W}^{(1)}$ is symmetrizable, we know from Theorem 1 that the secrecy capacity is zero, i.e., $C_S(\mathfrak{W}^{(1)}) = 0$. 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 [8, Proposition 3.9] yields $C_{S,\text{ran}}(\mathfrak{W}^{(1)}) > 0$ if $V^{(1)}$ is chosen accordingly.

Now, let us define the second AVWC $\mathfrak{W}^{(2)}$. Therefore, let $0 < p < q < \frac{1}{2}$ and

$$W^{(2)} \coloneqq \begin{pmatrix} 1-q & q \\ q & 1-q \end{pmatrix}, \qquad V^{(2)} \coloneqq \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}.$$

Then, define $\mathcal{W}^{(2)} = \{W^{(2)}\}$ so that $C(\mathcal{W}^{(2)}) = 1 - H_2(q) > 0$, and $\mathcal{V}^{(2)} = \{V^{(2)}\}$ so that $C(\mathcal{V}^{(2)}) = 1 - H_2(p) > 0$. With this, we construct the second AVWC $\mathfrak{W}^{(2)}$ as

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

Since $C(\mathcal{V}^{(2)}) > C(\mathcal{W}^{(2)})$, we obtain $C_S(\mathfrak{W}^{(2)}) = C_{S,\text{ran}}(\mathfrak{W}^{(2)}) = 0$.

Thus, we have constructed two AVWCs $\mathfrak{W}^{(1)}$ and $\mathfrak{W}^{(2)}$, whose both secrecy capacities are zero, i.e., $C_S(\mathfrak{W}^{(1)}) =$

$C_S(\mathfrak{W}^{(2)}) = 0$. Next, we argue how both channels can be used to *super-activate* the whole system to allow for secure communication at non-zero secrecy rates. In the following we denote the system which results from the parallel use of both channels by $\widetilde{\mathfrak{W}} = \mathfrak{W}^{(1)} \otimes \mathfrak{W}^{(2)}$.

A. Active Wiretapper

Here we discuss the case where the wiretapper does not exploit available CR. In the following we show that we have

$$C_S(\widetilde{\mathfrak{W}}) = C_S(\mathfrak{W}^{(1)} \otimes \mathfrak{W}^{(2)}) > 0$$

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

The first observation is that $C_{S,\text{ran}}(\widetilde{\mathfrak{W}}) > 0$, which can easily be achieved by using only $\mathfrak{W}^{(1)}$ so that we obviously have $C_{S,\text{ran}}(\widetilde{\mathfrak{W}}) \geq C_{S,\text{ran}}(\mathfrak{W}^{(1)}) > 0$. The second crucial observation is that the combined AVC $\widetilde{\mathcal{W}} = \{(W_1^{(1)} \otimes W^{(2)}), (W_2^{(1)} \otimes W^{(2)})\}$ to the legitimate receiver is non-symmetrizable. Using only the non-symmetrizable channel $W^{(2)}$ immediately yields that the combination is non-symmetrizable as well. Thus, from [8] we then have $C_S(\widetilde{\mathfrak{W}}) > 0$.

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

To make $u \in \mathcal{U}$ also available at the legitimate receiver, the sender transmits $E^{(2)}(u)$ over the second AVWC $\mathfrak{W}^{(2)}$. Since the corresponding link $\mathcal{W}^{(2)}$ to the legitimate user is non-symmetrizable, we have $C(\mathcal{W}^{(2)}) > 0$ and there exists decoding sets $\{\mathcal{D}_u^{(2)} : u \in \mathcal{U}\}$ making $u \in \mathcal{U}$ at the legitimate receiver available. Note that as $C(V^{(2)}) > C(W^{(2)})$, it is very likely that $u \in \mathcal{U}$ 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. To this end, the sender transmits $E_u^{(1)}(j)$ and the legitimate receiver uses decoding sets $\{\mathcal{D}_{u,j}^{(1)} : j \in \mathcal{J}_n\}$ for decoding. As $C_{S,\text{ran}}(\mathfrak{W}^{(1)}) > 0$, secure communication at a positive secrecy rate is possible. This completes the protocol which achieves a secrecy rate $C_S(\widetilde{\mathfrak{W}}) = C_S(\mathfrak{W}^{(1)} \otimes \mathfrak{W}^{(2)}) > 0$.

B. Active Wiretapper Exploiting CR

From Theorem 3 we know that the CR-assisted secrecy capacity $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W})$ for wiretappers exploiting CR displays the same behavior as the secrecy capacity $C_S(\mathfrak{W})$. Thus, it is convincing that the super-activation discussed above also holds for such wiretappers, i.e.,

$$C_{S,\text{ran}}^{\text{active}}(\widetilde{\mathfrak{W}}) = C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}^{(1)} \otimes \mathfrak{W}^{(2)}) > 0$$

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

It is clear that the previous protocol as discussed above also works in the case of active wiretappers exploiting CR.

VII. Conclusion

We studied the AVWC with active wiretapper under different kinds of coordination resources. In particular, we established a complete characterization of the CR-assisted secrecy capacity $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W})$ for wiretappers exploiting CR which was missing until now. It displays the same characteristics as the secrecy capacity $C_S(\mathfrak{W})$: it either equals its CR-assisted secrecy capacity $C_{S,\text{ran}}(\mathfrak{W})$ or else is zero. Moreover, the influence of the available coordination resources was analyzed and it is shown that weaker forms of coordination resources than common randomness suffice to achieve capacity, i.e., $C_{S,\text{causal}}(\mathfrak{W}, (U,Q)) = C_{S,\text{cor}}(\mathfrak{W}, (U,Q)) = C_{S,\text{ran}}(\mathfrak{W})$ and $C_{S,\text{causal}}^{\text{active}}(\mathfrak{W}, (U,Q)) = C_{S,\text{cor}}^{\text{active}}(\mathfrak{W}, (U,Q)) = C_{S,\text{ran}}^{\text{active}}(\mathfrak{W})$.

To this end, the existence of new phenomena has been shown. We gave an example how two useless AVWCs can be used together without feedback such that the system is super-activated allowing for secure transmission at non-zero 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.

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," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

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

[4] R. Ahlswede, "Elimination of Correlation in Random Codes for Arbitrarily Varying Channels," *Z. Wahrscheinlichkeitstheorie verw. Gebiete*, vol. 44, pp. 159–175, 1978.

[5] 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.

[6] R. Ahlswede and N. Cai, "Correlated Sources Help Transmission Over an Arbitrarily Varying Channel," *IEEE Trans. Inf. Theory*, vol. 43, no. 4, pp. 1254–1255, Jul. 1997.

[7] 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.

[8] I. Bjelaković, H. Boche, and J. Sommerfeld, *Information Theory, Combinatorics, and Search Theory*. Springer, 2013, ch. Capacity Results for Arbitrarily Varying Wiretap Channels, pp. 123–144.

[9] H. Boche and R. F. Wyrembelski, "Comparison of Different Attack Classes in Arbitrarily Varying Wiretap Channels," in *Proc. IEEE Int. Workshop Inf. Forensics and Security*, Tenerife, Spain, Dec. 2012, pp. 270–275.

[10] K. Li, A. Winter, X. Zou, and G. Guo, "Private Capacity of Quantum Channels is Not Additive," *Phys. Rev. Lett.*, vol. 103, no. 12, p. 120501, 2009.

[11] G. Smith, J. A. Smolin, and J. Yard, "Quantum Communication with Gaussian Channels of Zero Quantum Capacity," *Nature Photonics*, vol. 5, no. 10, pp. 624–627, Oct. 2011.

[12] G. Giedke and M. M. Wolf, "Quantum Communication: Super-Activated Channels," *Nature Photonics*, vol. 5, no. 10, pp. 578–580, Oct. 2011.

[13] H. Boche and J. Nötzel, "Arbitrarily Small Amounts of Correlation for Arbitrarily Varying Quantum Channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Instanbul, Turkey, Jul. 2013.