information

MDPI

Article

Super-Activation as a Unique Feature of Secure Communication in Malicious Environments

Rafael F. Schaefer [1,*,†], Holger Boche [2,†] and H. Vincent Poor [3,†]

[1] Information Theory and Applications Chair, Technische Universität Berlin, 10587 Berlin, Germany
[2] Institute of Theoretical Information Technology, Technische Universität München, 80333 Munich, Germany; boche@tum.de
[3] Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA; poor@princeton.edu
* Correspondence: rafael.schaefer@tu-berlin.de; Tel.: +49-30-314-28463
† These authors contributed equally to this work.

Academic Editor: Willy Susilo
Received: 28 January 2016; Accepted: 27 April 2016; Published: 12 May 2016

Abstract: The wiretap channel models secure communication between two users in the presence of an eavesdropper who must be kept ignorant of transmitted messages. This communication scenario is studied for arbitrarily varying channels (AVCs), in which the legitimate users know only that the true channel realization comes from a pre-specified uncertainty set and that it varies from channel use to channel use in an arbitrary and unknown manner. This concept not only captures the case of channel uncertainty, but also models scenarios in which malevolent adversaries influence or jam the transmission of the legitimate users. For secure communication over orthogonal *arbitrarily varying wiretap channels* (AVWCs) it has been shown that the phenomenon of super-activation occurs; that is, there are orthogonal AVWCs, each having zero secrecy capacity, which allow for transmission with positive rate if they are used together. It is shown that for such orthogonal AVWCs super-activation is generic in the sense that whenever super-activation is possible, it is possible for all AVWCs in a certain neighborhood as well. As a consequence, a super-activated AVWC is robust and continuous in the uncertainty set, although a single AVWC might not be. Moreover, it is shown that the question of super-activation and the continuity of the secrecy capacity solely depends on the legitimate link. Accordingly, the single-user AVC is subsequently studied and it is shown that in this case, super-activation for non-secure message transmission is not possible making it a unique feature of secure communication over AVWCs. However, the capacity for message transmission of the single-user AVC is shown to be super-additive including a complete characterization. Such knowledge is important for medium access control and in particular resource allocation as it determines the overall performance of a system.

Keywords: wiretap channel; arbitrarily varying channel (AVC); secrecy capacity; super-activation; super-additivity; active attacks; malicious behavior

1. Introduction

The architecture of today's communication systems is designed such that data encryption and error correction are clearly separated. Data encryption is based on cryptographic principles and usually implemented at higher layers which abstracts out the underlying communication channel as an ideal bit pipe. The error correction is performed at the physical layer by adding redundancy into the message bits in order to combat the noisy channel. Such separation based approaches have been the typical solution in current communication systems.

In recent years there has been a growing interest in complementary approaches that realize security directly at the physical layer. Such *information theoretic approaches to security* establish data

confidentiality and reliable communication jointly at the physical layer by exploiting the noisy and imperfect nature of the communication channel. This line of thinking goes back to Wyner, who introduced the so-called wiretap channel in [1]. This area of research provides a promising approach to achieve secrecy and to embed secure communication into wireless networks. Not surprisingly, it has drawn considerable attention recently [2–7] and has also been identified by operators of communication systems and national agencies as a key technique to secure future communication systems [8–10].

These studies are in particular relevant for wireless communication systems as the open nature of the wireless medium makes such systems inherently vulnerable for eavesdropping: Transmitted signals are received not only by intended users, but also easily eavesdropped upon by non-legitimate receivers. A common assumption of many studies is that all channels to the intended receivers and also to the non-legitimate eavesdroppers are known perfectly to all users. However, practical systems will always be limited in the availability of channel state information (CSI) due to nature of the wireless medium but also due to practical limitations such as estimation/feedback inaccuracy. In addition to that, the assumption of knowing the eavesdropper's channel is often hard to justify in practice since malevolent eavesdroppers will not share any information about their channels to make eavesdropping even harder. Accordingly, such approaches to security must incorporate imperfect CSI assumptions to yield practically meaningful insights. A recent survey on secure communication under channel uncertainty and adversarial attacks can be found in [11].

In this paper, we model the uncertainty in CSI by assuming *arbitrarily varying channels* (AVCs) [12–14]. This concept assumes that the actual channel realization is unknown; rather, it is only known that this realization is from a known uncertainty set and that it may vary in an arbitrary and unknown manner from channel use to channel use. The concept of AVCs provides a very general and powerful framework as it not only models the case of channel uncertainty, but also captures scenarios with malevolent adversaries who maliciously influence or jam the legitimate transmission.

Secure communication over AVCs is then modeled by the *arbitrarily varying wiretap channel* (AVWC) which has been studied in [15–22]. It has been shown that it makes a substantial difference whether unassisted or common randomness (CR) assisted codes are used by the transmitter and the legitimate receiver. Specifically, if the AVC to the legitimate receiver possesses the so-called symmetrizability property, then the unassisted secrecy capacity is zero, while the CR-assisted secrecy capacity may be positive. A complete characterization of how unassisted and CR-assisted secrecy capacity relate to each other is given in [16,21]. However, a single-letter characterization of the secrecy capacity itself remains open. Only a multi-letter description of the CR-assisted secrecy capacity has been recently established in [20].

Wireless communication systems are usually composed of orthogonal sub-systems such as those that arise via orthogonal frequency division multiplexing (OFDM) or time division multiplexing (TDM). And the important issue in such systems is how the available resources should be allocated to these orthogonal sub-systems. Common sense tells us that the overall capacity of such a system is given by the sum of the capacities of all orthogonal sub-systems. The inherent world view of the additivity of classical resources is also reflected by Shannon who conjectured in [23] the additivity of the zero error capacity for orthogonal discrete memoryless channels (DMCs). This was later restated by Lovász in ([24], Problem 2) and recently further highlighted in [25].

To this end, let us consider a system consisting of two orthogonal ordinary DMCs W_1 and W_2. If both channels are accessed in an orthogonal way by using independent encoders and decoders, we obtain $C(\mathsf{W}_1) + C(\mathsf{W}_2)$ as an achievable transmission rate, where $C(\cdot)$ denotes the capacity of the corresponding channel.

An interesting question is: Are there gains in capacity to be had by bonding the orthogonal channels and jointly accessing the resulting system $\mathsf{W}_1 \otimes \mathsf{W}_2$ by using a joint encoder and decoder? From the operational definition of the capacity it is clear that we have

$$C(\mathsf{W}_1 \otimes \mathsf{W}_2) \geq C(\mathsf{W}_1) + C(\mathsf{W}_2) \tag{1}$$

since a joint use of both channels can only increase the capacity. However, it is known that the capacity of ordinary DMCs is *additive* under the average error criterion so that Equation (1) is actually satisfied with equality, *i.e.*,

$$C(\mathrm{W}_1 \otimes \mathrm{W}_2) = C(\mathrm{W}_1) + C(\mathrm{W}_2). \tag{2}$$

This means that joint encoding and decoding over orthogonal channels does not provide any gains in capacity and the overall capacity of an OFDM system is indeed given by the sum of the capacities of all orthogonal sub-channels.

Although this verifies what one usually would expect for the capacity of orthogonal channels, the question of additivity of the capacity function is in general by no means obvious or trivial to answer. As already mentioned, Shannon for example asked this question in 1956 for the zero error capacity [23]. He conjectured that the zero error capacity C_0 is additive, thus possessing the same behavior as ordinary DMCs: $C_0(\mathrm{W}_1 \otimes \mathrm{W}_2) = C_0(\mathrm{W}_1) + C_0(\mathrm{W}_2)$; similar to Equation (2). This problem was subsequently studied by Haemers [26] and later by Alon [27] who explicitly constructed counter-examples. Thus, there exist channels for which the zero error capacity is strictly greater when encoding and decoding are done jointly instead of independently. This means that the zero error capacity is *super-additive* and there exist channels for which "$\geq$" in Equation (1) can actually be replaced by "$>$" so that

$$C_0(\mathrm{W}_1 \otimes \mathrm{W}_2) > C_0(\mathrm{W}_1) + C_0(\mathrm{W}_2)$$

holds. To date, only certain explicit examples are known that possess this property of super-additivity. A general characterization of which channels are super-additive or what further properties such channels possess remains open. In 1970 it was Ahlswede who showed that the capacity of the AVC under the maximum error criterion includes the characterization of the zero error capacity as a special case [28]. This is only one example demonstrating that Shannon's question of additivity of the zero error capacity considerably influenced the research in discrete mathematics and graph theory, *cf.* for example ([29], Chapter 41). Thus, Shannon's zero error capacity is closely related to AVCs, making it worth studying this question also from an AVC perspective.

The extreme case of non-additivity in Equation (1) occurs when for a system consisting of two orthogonal "useless" channels, *i.e.*, having zero capacity $C(\mathrm{W}_1) = C(\mathrm{W}_2) = 0$, it holds that $C(\mathrm{W}_1 \otimes \mathrm{W}_2) > 0$. This phenomenon is called *super-activation*: Two channels each with zero capacity can be used together to super-activate the whole system giving it a positive capacity. This phenomenon has been observed and studied in particular in the area of quantum information theory [30,31].

Very recently the phenomenon of super-activation has been observed for classical communication as well. Super-activation can occur for secure communication over AVCs and there exist orthogonal "useless" AVWCs, *i.e.*, having zero secrecy capacity, whose overall secrecy capacity is strictly positive [17]. This phenomenon of super-activation and its resulting secrecy capacity have then been completely characterized in [21].

In this paper we further explore the phenomenon of super-activation for AVWCs and its contributions are as follows. After introducing the system model in Section 2, we show that super-activation is not an isolated phenomenon in the sense that whenever two AVWCs can be super-activated, this is also true for all AVWCs in a certain neighborhood. As a consequence, we show that the secrecy capacity of a super-activated AVWC is continuous in the underlying uncertainty set, although this might not be the case for one of the AVWCs itself. Furthermore, we show that the question of whether super-activation is possible or not depends only on the legitimate channel, making it independent of the eavesdropper channel. This is the content of Section 3.

From a super-activation and continuity perspective, the legitimate AVC is more important than the eavesdropper AVC. Accordingly, we subsequently study these issues for the single-user AVC in detail in Section 4. Surprisingly, this has not been done so far to the best of our knowledge and we show that super-activation is not possible for public message transmission, making this a unique phenomenon of secure communication over AVWCs. However, we show that the single-user AVC

indeed possesses the property of super-additivity which means that a joint use of orthogonal AVCs can provide gains in capacity. With this we provide a complete characterization of super-additivity and super-activation for the capacity of a single-user AVC. Finally, a discussion is given in Section 5.

Notation

Discrete random variables are denoted by capital letters and their realizations and ranges by lower case and script letters, respectively; all logarithms and information quantities are taken to the base 2; $X - Y - Z$ denotes a Markov chain of random variables X, Y, and Z in this order; $\mathcal{P}(\mathcal{X})$ is the set of all probability distributions on $\mathcal{X}$; the mutual information between the input random variable X and the output random variable Y of a channel W is denoted by $I(X;Y) = I(P_X, W)$, where the latter notation is interchangeably used to emphasize the dependence on the input distribution P_X and the channel.

2. Arbitrarily Varying Wiretap Channels

In this section we introduce the problem of secure communication over arbitrarily varying channels [12–14]. Such channel conditions appear for example in fast fading environments but also, more importantly, in scenarios in which malevolent adversaries actively influence or jam the legitimate transmission. This is the AVWC [15–22] which is depicted in Figure 1.

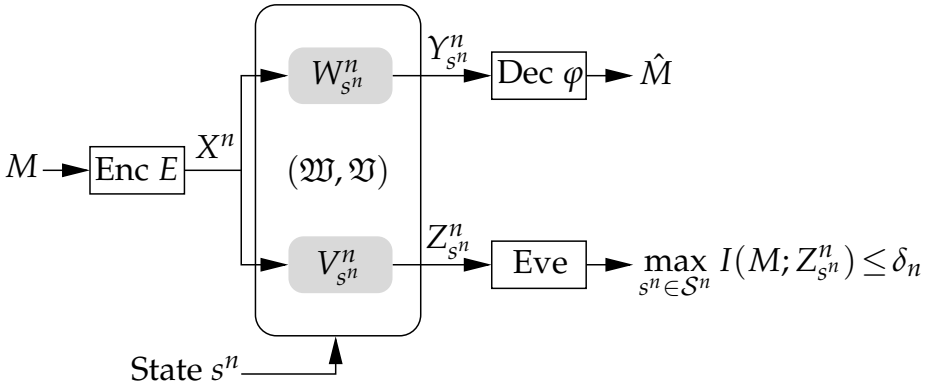

Figure 1. Arbitrarily varying wiretap channel. The transmitter encodes the message M into the codeword $X^n = E(M)$ and transmits it over the AVWC to the legitimate receiver, which has to decode its intended message $\hat{M} = \varphi(Y^n_{s^n})$ for any state sequence $s^n \in \mathcal{S}^n$. At the same time, the eavesdropper must be kept ignorant of M by requiring $\max_{s^n \in \mathcal{S}^n} I(M; Z^n_{s^n}) \leq \delta_n$.

2.1. System Model

The channel state may vary in an unknown and arbitrary manner from channel use to channel use and this uncertainty in CSI is modeled with the help of a finite state set $\mathcal{S}$. Then the communication links to the legitimate receiver and the eavesdropper are given by stochastic matrices $W : \mathcal{X} \times \mathcal{S} \to \mathcal{P}(\mathcal{Y})$ and $V : \mathcal{X} \times \mathcal{S} \to \mathcal{P}(\mathcal{Z})$ with $\mathcal{X}$ the finite input alphabet and $\mathcal{Y}$ and $\mathcal{Z}$ the finite output alphabets at the legitimate receiver and eavesdropper respectively. We interchangeably also write $W_s : \mathcal{X} \to \mathcal{P}(\mathcal{Y})$ and $V_s : \mathcal{X} \to \mathcal{P}(\mathcal{Z})$ with $s \in \mathcal{S}$.

For a fixed state sequence $s^n = (s_1, s_2, ..., s_n) \in \mathcal{S}^n$ of length n, the discrete memoryless channel to the legitimate receiver is given by $W^n_{s^n}(y^n|x^n) = W^n(y^n|x^n, s^n) = \prod_{i=1}^n W(y_i|x_i, s_i)$ for all input and output sequences $x^n \in \mathcal{X}^n$ and $y^n \in \mathcal{Y}^n$.

Definition 1. The *arbitrarily varying channel (AVC)* $\mathfrak{W}$ to the legitimate receiver is defined as the family of channels for all state sequences $s^n \in \mathcal{S}^n$ as

$$\mathfrak{W} = \{W^n_{s^n} : s^n \in \mathcal{S}^n\}.$$

We further need the definition of an *averaged channel* which is defined for any probability distribution $q \in \mathcal{P}(\mathcal{S})$ as

$$\overline{W}_q(y|x) = \sum_{s\in\mathcal{S}} W(y|x,s)q(s) \tag{3}$$

for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. An important property of an AVC is the so-called concept of symmetrizability as introduced next.

Definition 2. An AVC $\mathfrak{W}$ is called *symmetrizable* if there exists a channel (stochastic matrix) $\sigma : \mathcal{X} \to \mathcal{P}(\mathcal{S})$ such that

$$\sum_{s\in\mathcal{S}} W(y|x,s)\sigma(s|x') = \sum_{s\in\mathcal{S}} W(y|x',s)\sigma(s|x) \tag{4}$$

holds for all $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$.

Roughly speaking, symmetrizability means that the AVC can "simulate" a valid channel input which makes it impossible for the receiver to decide on the correct codeword sent by the transmitter. This can be seen by writing the left hand side of Equation (4) as $\widetilde{W}(y|x,x') = \sum_{s\in\mathcal{S}} W(y|x,s)\sigma(s|x')$. Now symmetrizability means that this channel is symmetric in both inputs x and x', *i.e.*, $\widetilde{W}(y|x,x') = \widetilde{W}(y|x',x)$.

In a similar way we can define the channel to the eavesdropper. For fixed $s^n \in \mathcal{S}^n$ the discrete memoryless channel is given by $V^n_{s^n}(z^n|x^n) = V^n(z^n|x^n,s^n) = \prod_{i=1}^n V(z_i|x_i,s_i)$. We also set $\mathfrak{V} = \{V^n_{s^n} : s^n \in \mathcal{S}^n\}$ and $\overline{V}_q(z|x) = \sum_{s\in\mathcal{S}} V(z|x,s)q(s)$ for $q \in \mathcal{P}(\mathcal{S})$.

Definition 3. The *arbitrarily varying wiretap channel (AVWC)* $(\mathfrak{W},\mathfrak{V})$ is given by its marginal AVCs $\mathfrak{W}$ and $\mathfrak{V}$ with common input as

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

Finally, we need a concept to measure the distance between two channels. As in [22] we define the distance between two channels $W_1, W_2 : \mathcal{X} \to \mathcal{P}(\mathcal{Y})$ based on the total variation distance as

$$d(W_1,W_2) = \max_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} \big|W_1(y|x) - W_2(y|x)\big|. \tag{5}$$

Now, this generalizes to a distance between two AVCs as follows. For two AVWCs $\mathfrak{W}_1$ and $\mathfrak{W}_2$ with finite state sets $\mathcal{S}_1$ and $\mathcal{S}_2$ we define uncertainty sets $\mathcal{W}_1 = \{W_{s_1} : s_1 \in \mathcal{S}_1\}$ and $\mathcal{W}_2 = \{W_{s_2} : s_2 \in \mathcal{S}_2\}$. Then the distance between these two sets of channels is

$$\begin{aligned} d_1(\mathcal{W}_1,\mathcal{W}_2) &= \max_{s_2\in\mathcal{S}_2} \min_{s_1\in\mathcal{S}_1} d(W_{s_1},W_{s_2}) \\ d_2(\mathcal{W}_1,\mathcal{W}_2) &= \max_{s_1\in\mathcal{S}_1} \min_{s_2\in\mathcal{S}_2} d(W_{s_1},W_{s_2}) \end{aligned}$$

so that the distance between the AVCs $\mathfrak{W}_1$ and $\mathfrak{W}_2$ is given as

$$D(\mathfrak{W}_1,\mathfrak{W}_2) = \max\big\{d_1(\mathcal{W}_1,\mathcal{W}_2), d_2(\mathcal{W}_1,\mathcal{W}_2)\big\}.$$

Roughly speaking, the distance $D(\mathfrak{W}_1,\mathfrak{W}_2)$ between two AVCs $\mathfrak{W}_1$ and $\mathfrak{W}_2$ is given by the largest distance in Equation (5) between all possible channel realizations in the corresponding state sets.

The distance $D(\mathfrak{V}_1,\mathfrak{V}_2)$ between two eavesdropper AVCs is defined accordingly so that the distance between two AVWCs $(\mathfrak{W}_1,\mathfrak{V}_1)$ and $(\mathfrak{W}_2,\mathfrak{V}_2)$ is finally given by

$$D((\mathfrak{W}_1,\mathfrak{V}_1),(\mathfrak{W}_2,\mathfrak{V}_2)) = \max\big\{D(\mathfrak{W}_1,\mathfrak{W}_2), D(\mathfrak{V}_1,\mathfrak{V}_2)\big\}.$$

2.2. Code Concepts

For communication over AVCs it makes a substantial difference whether unassisted (deterministic) or more sophisticated code concepts based on *common randomness (CR)* are used. Indeed, the unassisted capacity of an AVC can be zero, while the corresponding CR-assisted capacity is positive [12–14].

2.2.1. Unassisted Codes

Unassisted codes refer to codes whose encoder and decoder are pre-specified and fixed prior to the transmission as shown in Figure 1.

Definition 4. An *unassisted* (n, M_n)*-code* $\mathcal{C}$ consists of a stochastic encoder at the transmitter

$$E : \mathcal{M} \to \mathcal{P}(\mathcal{X}^n) \tag{6}$$

with a set of messages $\mathcal{M} = \{1, ..., M_n\}$ and a deterministic decoder at the legitimate receiver

$$\varphi : \mathcal{Y}^n \to \mathcal{M}. \tag{7}$$

Remark 1. Since the encoder in Equation (6) and the decoder in Equation (7) are fixed prior to the transmission of the message, they must be universally valid for all possible state sequences $s^n \in \mathcal{S}^n$ simultaneously.

The average probability of error of such a code for a given state sequence $s^n \in \mathcal{S}^n$ is given by

$$\bar{e}_n(s^n) = \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \sum_{x^n \in \mathcal{X}^n} \sum_{y^n : \varphi(y^n) \neq m} W^n(y^n | x^n, s^n) E(x^n | m).$$

The confidentiality of the message is ensured by requiring $\max_{s^n \in \mathcal{S}^n} I(M; Z^n_{s^n}) \leq \delta_n$ for some $\delta_n > 0$ with M the random variable uniformly distributed over the set of messages $\mathcal{M}$ and $Z^n_{s^n} = (Z_{s_1}, Z_{s_2}, ..., Z_{s_n})$ the output at the eavesdropper for state sequence $s^n \in \mathcal{S}^n$. This criterion is termed *strong secrecy* [32,33] and the reasoning is to control the total amount of information leaked to the eavesdropper. This yields the following definition.

Definition 5. A rate $R_S > 0$ is an *achievable secrecy rate* for the AVWC $(\mathfrak{W}, \mathfrak{V})$ if for all $\tau > 0$ there exists an $n(\tau) \in \mathbb{N}$, positive null sequences $\{\lambda_n\}_{n \in \mathbb{N}}$, $\{\delta_n\}_{n \in \mathbb{N}}$, and a sequence of (n, M_n)-codes $\{\mathcal{C}_n\}_{n \in \mathbb{N}}$ such that for all $n \geq n(\tau)$ we have $\frac{1}{n} \log M_n \geq R_S - \tau$,

$$\max_{s^n \in \mathcal{S}^n} \bar{e}_n(s^n) \leq \lambda_n,$$

and

$$\max_{s^n \in \mathcal{S}^n} I(M; Z^n_{s^n}) \leq \delta_n.$$

The *unassisted secrecy capacity* $C_S(\mathfrak{W}, \mathfrak{V})$ of the AVWC $(\mathfrak{W}, \mathfrak{V})$ is given by the maximum of all achievable rates R_S.

Unfortunately, it has been shown that unassisted codes with a pre-specified encoder and decoder will not work for symmetrizable channels, *cf.* Definition 2. Thus the unassisted capacity will be zero [14] and more sophisticated code concepts based on CR are needed.

2.2.2. CR-Assisted Codes

CR is a powerful coordination resource and can be realized for example based on a common synchronization procedure or a satellite signal. It is modeled by a random variable Γ which takes

values in a finite set $\mathcal{G}_n$ according to a distribution $P_\Gamma \in \mathcal{P}(\mathcal{G}_n)$. This enables the transmitter and the receiver to choose their encoder in Equation (6) and decoder in Equation (7) according to the actual realization $\gamma \in \mathcal{G}_n$ as shown in Figure 2.

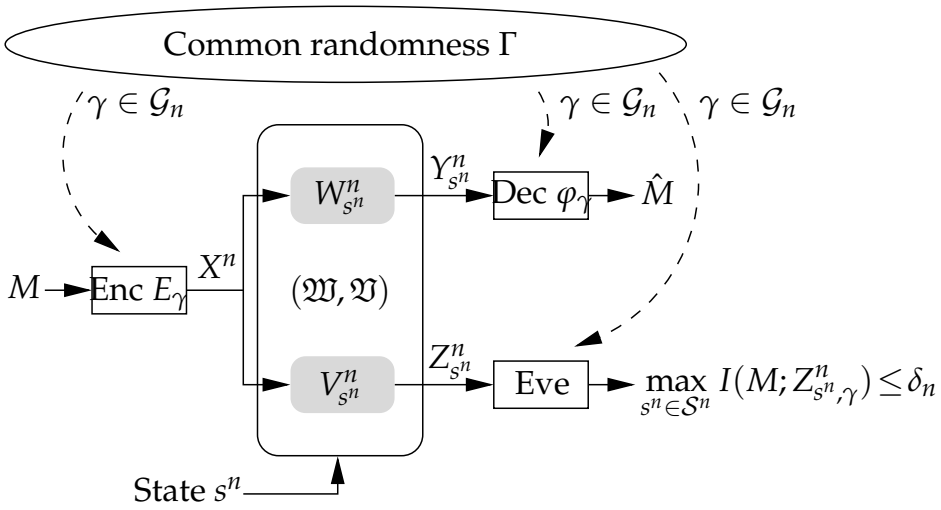

Figure 2. CR is available to all users including the eavesdropper. The transmitter and receiver can adapt their encoder and decoder according to the actual CR realization $\gamma \in \mathcal{G}_n$.

Definition 6. A *CR-assisted* $(n, M_n, \mathcal{G}_n, P_\Gamma)$*-code* $\mathcal{C}_{\mathbf{CR}}$ is given by a family of unassisted codes

$$\{\mathcal{C}(\gamma) : \gamma \in \mathcal{G}_n\}$$

together with a random variable Γ taking values in $\mathcal{G}_n$ with $|\mathcal{G}_n| < \infty$ according to $P_\Gamma \in \mathcal{P}(\mathcal{G}_n)$.

The reliability and secrecy constraints extend to CR-assisted codes in a natural way: The mean average probability of error is

$$\bar{e}_{\mathrm{CR}} = \max_{s^n \in \mathcal{S}^n} \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \sum_{\gamma \in \mathcal{G}_n} \sum_{x^n \in \mathcal{X}^n} \sum_{y^n : \varphi_\gamma(y^n) \neq m} W^n(y^n | x^n, s^n) E_\gamma(x^n | m) P_\Gamma(\gamma)$$

where E_γ and φ_γ indicate that the encoder and decoder are chosen according to the CR realization $\gamma \in \mathcal{G}_n$. Accordingly, the secrecy criterion becomes

$$\max_{s^n \in \mathcal{S}^n} \sum_{\gamma \in \mathcal{G}_n} I(M; Z^n_{s^n,\gamma}) P_\Gamma(\gamma) \leq \delta_n \tag{8}$$

where $Z^n_{s^n,\gamma}$ indicates that the observed output at the eavesdropper depends on the chosen encoder E_γ, $\gamma \in \mathcal{G}_n$.

Remark 2. Note that the secrecy criterion Equation (8) can further be strengthened by requiring

$$\max_{s^n \in \mathcal{S}^n} \max_{\gamma \in \mathcal{G}_n} I(M; Z^n_{s^n,\gamma}) \leq \delta_n,$$

i.e., the average over all CR in Equation (8) is replaced by the maximum. Surprisingly, this strengthening comes at no cost and does not decrease the secrecy capacity, *cf.* [20]. The stronger criterion has the advantage that it protects the message even in the scenario in which the eavesdropper is aware of the CR realization $\gamma \in \mathcal{G}_n$, *cf.* Figure 2.

Then the definitions of a *CR-assisted achievable secrecy rate* and the *CR-assisted secrecy capacity* $C_{S,\mathrm{CR}}(\mathfrak{W},\mathfrak{V})$ of the AVWC $(\mathfrak{W},\mathfrak{V})$ follow accordingly.

2.3. Capacity Results

There has been some work done in order to understand the secrecy capacity of the AVWC [15–22] which is briefly reviewed in the following. If CR is available, the transmitter and the legitimate receiver can coordinate their choice of encoder and decoder. This scenario has been studied in [15–18,20,22], but despite these efforts a single-letter characterization remains unknown to date (if it exists at all). Only a multi-letter description has been found in [20].

Theorem 1 ([20]). *A multi-letter description of the CR-assisted secrecy capacity $C_{S,CR}(\mathfrak{W},\mathfrak{V})$ of the AVWC $(\mathfrak{W},\mathfrak{V})$ is*

$$C_{S,CR}(\mathfrak{W},\mathfrak{V}) = \lim_{n\to\infty}\frac{1}{n}\max_{U-X^n-(\overline{Y}_q^n,Z_{s^n}^n)}\Big(\min_{q\in\mathcal{P}(\mathcal{S})} I(U;\overline{Y}_q^n) - \max_{s^n\in\mathcal{S}^n} I(U;Z_{s^n}^n)\Big)$$

with $\overline{Y}_q^n$ the random variable associated with the output of the averaged channel $\overline{W}_q^n = \sum_{s^n\in\mathcal{S}^n} q^n(s^n)W_{s^n}$, $q\in\mathcal{P}(\mathcal{S})$.

If CR is not available to the transmitter and legitimate receiver, unassisted codes must be used and the corresponding unassisted secrecy capacity has been completely characterized in terms of its CR-assisted secrecy capacity [16,21].

Theorem 2 ([16,21]). *The unassisted secrecy capacity $C_S(\mathfrak{W},\mathfrak{V})$ of the AVWC $(\mathfrak{W},\mathfrak{V})$ possesses the following symmetrizability properties:*

1. *If $\mathfrak{W}$ is symmetrizable, then $C_S(\mathfrak{W},\mathfrak{V}) = 0$.*
2. *If $\mathfrak{W}$ is non-symmetrizable, then $C_S(\mathfrak{W},\mathfrak{V}) = C_{S,CR}(\mathfrak{W},\mathfrak{V})$.*

The unassisted secrecy capacity displays a dichotomous behavior similar to the capacity of the single-user AVC: The unassisted secrecy capacity $C_S(\mathfrak{W},\mathfrak{V})$ either equals its CR-assisted secrecy capacity $C_{S,\mathrm{CR}}(\mathfrak{W},\mathfrak{V})$ or else is zero.

From Theorem 2 we see that it is only the symmetrizability of the legitimate AVC $\mathfrak{W}$ that controls whether the unassisted secrecy capacity is zero or positive. However, it does not specify the sensitivity, meaning how rapidly the AVC $\mathfrak{W}$ can change from symmetrizable to non-symmetrizable. This is addressed by the next result.

Theorem 3 ([21]). *If the unassisted secrecy capacity $C_S(\mathfrak{W},\mathfrak{V})$ of the AVWC $(\mathfrak{W},\mathfrak{V})$ satisfies $C_S(\mathfrak{W},\mathfrak{V}) > 0$, then there is an $\epsilon > 0$ such that for all AVWCs $(\mathfrak{W}',\mathfrak{V}')$ satisfying $D((\mathfrak{W},\mathfrak{V}),(\mathfrak{W}',\mathfrak{V}')) \le \epsilon$ we have $C_S(\mathfrak{W}',\mathfrak{V}') > 0$.*

This result shows the stability of positivity of the unassisted secrecy capacity: Wherever it is positive, *i.e.*, $C_S(\mathfrak{W},\mathfrak{V}) > 0$, it remains positive in a certain neighborhood, *i.e.*, $C_S(\mathfrak{W}',\mathfrak{V}') > 0$ for $D((\mathfrak{W},\mathfrak{V}),(\mathfrak{W}',\mathfrak{V}')) \le \epsilon$. Thus, if the AVC $\mathfrak{W}$ is non-symmetrizable, small changes in the uncertainty set will not make it symmetrizable.

To further explore the question of continuity for the AVWC, we need the function

$$F(\mathfrak{W}) = \min_{\sigma:\mathcal{X}\to\mathcal{P}(\mathcal{S})}\Big(\max_{x\neq x'}\sum_{y\in\mathcal{Y}}\Big|\sum_{s\in\mathcal{S}} W(y|x',s)\sigma(s|x) - \sum_{s\in\mathcal{S}} W(y|x,s)\sigma(s|x')\Big|\Big). \tag{9}$$

This function generalizes ideas from the concept of symmetrizability, *cf.* Definition 2. It is a continuous function of the legitimate AVC $\mathfrak{W}$ and the AVC $\mathfrak{W}$ is symmetrizable if and only if

$F(\mathfrak{W}) = 0$. This yields a characterization of when the unassisted secrecy capacity $C_S(\mathfrak{W}, \mathfrak{V})$ is discontinuous: The AVC $\mathfrak{W}$ changes from non-symmetrizable to symmetrizable and the capacity breaks down to zero.

That the unassisted secrecy capacity is indeed discontinuous has been observed in [22] for the first time by constructing a simple example of dimensions $|\mathcal{X}| = 2$, $|\mathcal{Y}| = 3$, and $|\mathcal{S}| = 2$. It is noteworthy that a state set consisting of two different states only is already sufficient to get a discontinuous behavior. From an adversarial point of view this means that two different strategies for the adversary suffice to break down the system. On the other hand, reducing the state set to have only one element, *i.e.*, $|\mathcal{S}| = 1$, the AVWC becomes a compound wiretap channel [34–36] (as the state remains constant for the entire duration of transmission) and the corresponding secrecy capacity becomes continuous [22]. Subsequently, the discontinuous behavior was then completely characterized in [21].

Theorem 4 ([21]). *The unassisted secrecy capacity $C_S(\mathfrak{W}, \mathfrak{V})$ of the AVWC $(\mathfrak{W}, \mathfrak{V})$ possesses the following discontinuity properties:*

1. *The AVWC $(\mathfrak{W}, \mathfrak{V})$ is a discontinuity point of $C_S(\mathfrak{W}, \mathfrak{V})$ if and only if the following holds: First, $C_{S,CR}(\mathfrak{W}, \mathfrak{V}) > 0$, and second, $F(\mathfrak{W}) = 0$ but for every $\epsilon > 0$ there is a finite $\mathfrak{W}'$ with $D(\mathfrak{W}, \mathfrak{W}') \leq \epsilon$ and $F(\mathfrak{W}') > 0$.*
2. *If $C_S(\mathfrak{W}, \mathfrak{V})$ is discontinuous in the point $(\mathfrak{W}, \mathfrak{V})$ then it is discontinuous for all $\mathfrak{V}'$ for which $C_{S,CR}(\mathfrak{W}, \mathfrak{V}') > 0$.*

This result has the following important consequence: Since the second condition relates the question of discontinuity to the function $F(\mathfrak{W})$ and therewith solely to the symmetrizability of the legitimate AVC $\mathfrak{W}$, the unassisted secrecy capacity $C_S(\mathfrak{W}, \mathfrak{V})$ is always a continuous function of the eavesdropper AVC $\mathfrak{V}$, while the discontinuity comes from the legitimate AVC $\mathfrak{W}$ only.

3. Super-Activation and Robustness

Medium access control and in particular resource allocation is one of the most important issues for wireless communication systems as it determines the overall performance of a system. For example, the overall capacity of an OFDM system is given by the sum of the capacities of all orthogonal sub-channels. To this end, a system consisting of two orthogonal ordinary DMCs, where both are "useless" in the sense of having zero capacity, the capacity of the whole system is zero as well. This reflects the world view of classical additivity of resources in the sense that "$0 + 0 = 0$."

Recently, it was shown in [17] that the additivity of basic resources does not hold anymore for secure communication over AVCs. Specifically, it was demonstrated that two orthogonal AVWCs which are themselves useless can be used jointly to allow for secure transmission with positive rate, *i.e.*, "$0 + 0 > 0$." This phenomenon of super-activation was then further studied in [21], which in particular provides a characterization of when super-activation is possible.

3.1. Secure Communication over Orthogonal AVWCs

To continue this line of research, we now introduce the corresponding system model in detail.

For finite state sets $\mathcal{S}_i$, input alphabets $\mathcal{X}_i$, and output alphabets $\mathcal{Y}_i$ and $\mathcal{Z}_i$, $i = 1, 2$, we define two AVWCs $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$ exactly as in Section 2.1, *cf.* Definitions 1 and 3. Then the parallel use of both AVWCs $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$ creates a combined AVWC

$$\begin{aligned}(\widetilde{\mathfrak{W}}, \widetilde{\mathfrak{V}}) &= (\mathfrak{W}_1, \mathfrak{V}_1) \otimes (\mathfrak{W}_2, \mathfrak{V}_2) \\ &= (\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2),\end{aligned}$$

where the notation $\otimes$ indicates the orthogonal use of $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$. Now, for given state sequences $\boldsymbol{s}^n = (s_1^n, s_2^n) \in \mathcal{S}_1^n \times \mathcal{S}_2^n$, the discrete memoryless channel to the legitimate receiver is

$$\begin{aligned} \widetilde{W}^n(\boldsymbol{y}^n|\boldsymbol{x}^n, \boldsymbol{s}^n) &= W_{1,s_1^n}^n(y_1^n|x_1^n) W_{2,s_2^n}^n(y_2^n|x_2^n) \\ &= W_1^n(y_1^n|x_1^n, s_1^n) W_2^n(y_2^n|x_2^n, s_2^n) \\ &= \prod_{i=1}^n W_1(y_{1,i}|x_{1,i}, s_{1,i}) \prod_{i=1}^n W_2(y_{2,i}|x_{2,i}, s_{2,i}) \end{aligned} \tag{10}$$

with $\boldsymbol{x}^n = (x_1^n, x_2^n) \in \mathcal{X}_1^n \times \mathcal{X}_2^n$ and $\boldsymbol{y}^n = (y_1^n, y_2^n) \in \mathcal{Y}_1^n \times \mathcal{Y}_2^n$. Accordingly, the AVC $\widetilde{\mathfrak{W}}$ is then given by

$$\begin{aligned} \widetilde{\mathfrak{W}} &= \left\{ \widetilde{W}_{\boldsymbol{s}^n}^n : \boldsymbol{s}^n \in \mathcal{S}_1^n \times \mathcal{S}_2^n \right\} \\ &= \left\{ W_{1,s_1^n}^n W_{2,s_2^n}^n : s_1^n \in \mathcal{S}_1^n, s_2^n \in \mathcal{S}_2^n \right\} \end{aligned} \tag{11}$$

and the AVWC $(\widetilde{\mathfrak{W}}, \widetilde{\mathfrak{V}})$ by

$$(\widetilde{\mathfrak{W}}, \widetilde{\mathfrak{V}}) = \left(\{ \widetilde{W}_{\boldsymbol{s}^n}^n : \boldsymbol{s}^n \in \mathcal{S}_1^n \times \mathcal{S}_2^n \}, \{ \widetilde{V}_{\boldsymbol{s}^n}^n : \boldsymbol{s}^n \in \mathcal{S}_1^n \times \mathcal{S}_2^n \} \right)$$

with $\widetilde{\mathfrak{V}}$ the AVC to the eavesdropper defined accordingly as in Equation (11).

Note that a parallel use of both AVWCs $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$ means that for each $(\mathfrak{W}_i, \mathfrak{V}_i)$ we have individual encoders $E_i : \mathcal{M}_i \to \mathcal{P}(\mathcal{X}_i^n)$ and decoders $\varphi_i : \mathcal{Y}_i^n \to \mathcal{M}_i$, $i = 1, 2$, according to Definitions 4 and 6. On the other hand, a joint use of both AVWCs results in a joint encoder $E : \mathcal{M} \to \mathcal{P}(\mathcal{X}_1^n \times \mathcal{X}_2^n)$ and a joint decoder $\varphi : \mathcal{Y}_1^n \times \mathcal{Y}_2^n \to \mathcal{M}$.

3.2. Super-Activation of Orthogonal AVWCs

For orthogonal AVWCs as described above, the phenomenon of super-activation has been completely characterized in [21].

Theorem 5 ([21]). *Let $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$ be two orthogonal AVWCs. Then the following properties hold:*

1. *If $C_S(\mathfrak{W}_1, \mathfrak{V}_1) = C_S(\mathfrak{W}_2, \mathfrak{V}_2) = 0$, then*

   $$C_S(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) > 0$$

   if and only if $\mathfrak{W}_1 \otimes \mathfrak{W}_2$ is non-symmetrizable and $C_{S,CR}(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) > 0$. If $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$ can be super-activated it holds that

   $$C_S(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) = C_{S,CR}(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2).$$

2. *If $C_{S,CR}$ shows no super-activation for $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$, then super-activation of C_S can only happen if $\mathfrak{W}_1$ is non-symmetrizable and $\mathfrak{W}_2$ is symmetrizable and $C_{S,CR}(\mathfrak{W}_1, \mathfrak{V}_1) = 0$ and $C_{S,CR}(\mathfrak{W}_2, \mathfrak{V}_2) > 0$. The statement is independent of the specific labeling.*
3. *There exist AVWCs that exhibit the behavior described by the second property.*

To give some intuition into why super-activation can happen, let us consider the following scenario: Assume there are two orthogonal AVWCs each having zero unassisted secrecy capacity. To this end, assume that one of the unassisted secrecy capacities is zero because the corresponding legitimate AVC is symmetrizable and the other capacity is zero because the eavesdropper AVC is "stronger" than the legitimate AVC. Since the latter legitimate AVC supports a positive rate (although non-secure), it can be used to transmit information to the legitimate receiver (and eavesdropper) to generate CR. Then the legitimate users can use CR-assisted codes to achieve a positive CR-assisted secrecy rate.

Theorem 5 provides a complete characterization of when super-activation can happen. In the following, we want to further explore this phenomenon. To this end, we first show that super-activation is generic in the sense that whenever two orthogonal AVWCs can be super-activated, it is possible for all AVWCs in a certain neighborhood as well.

Theorem 6. *Let $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$ be two useless AVWCs that can be super-activated, i.e., $C_S(\mathfrak{W}_1, \mathfrak{V}_1) = C_S(\mathfrak{W}_2, \mathfrak{V}_2) = 0$ and $C_S(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) > 0$. Then there exists an $\epsilon > 0$ such that for all useless AVWCs $(\mathfrak{W}_1', \mathfrak{V}_1')$ and $(\mathfrak{W}_2', \mathfrak{V}_2')$ with*

$$D((\mathfrak{W}_i, \mathfrak{V}_i), (\mathfrak{W}_i', \mathfrak{V}_i')) < \epsilon, \quad i = 1, 2,$$

we have

$$C_S(\mathfrak{W}_1' \otimes \mathfrak{W}_2', \mathfrak{V}_1' \otimes \mathfrak{V}_2') > 0,$$

i.e., all channels in the neighborhood of $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$ can be super-activated as well.

Proof. Let $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$ be two useless orthogonal AVWCs that can be super-activated and let $(\mathfrak{W}_1', \mathfrak{V}_1')$ and $(\mathfrak{W}_2', \mathfrak{V}_2')$ be two useless AVWCs with $D((\mathfrak{W}_i, \mathfrak{V}_i), (\mathfrak{W}_i', \mathfrak{V}_i')) < \epsilon$, $i = 1, 2$. Then it holds that

$$\begin{aligned}
&\sum_{y_1 \in \mathcal{Y}_1} \sum_{y_2 \in \mathcal{Y}_2} \left| W_1(y_1|x_1, s_1) W_2(y_2|x_2, s_2) - W_1'(y_1|x_1, s_1') W_2'(y_2|x_2, s_2') \right| \\
&\quad = \sum_{y_1 \in \mathcal{Y}_1} \sum_{y_2 \in \mathcal{Y}_2} \Big| W_1(y_1|x_1, s_1) W_2(y_2|x_2, s_2) - W_1'(y_1|x_1, s_1') W_2(y_2|x_2, s_2) \\
&\qquad\qquad + W_1'(y_1|x_1, s_1') W_2(y_2|x_2, s_2) - W_1'(y_1|x_1, s_1') W_2'(y_2|x_2, s_2') \Big| \\
&\quad \leq \sum_{y_1 \in \mathcal{Y}_1} \sum_{y_2 \in \mathcal{Y}_2} \left| \left(W_1(y_1|x_1, s_1) - W_1'(y_1|x_1, s_1')\right) W_2(y_2|x_2, s_2) \right| \\
&\qquad + \sum_{y_1 \in \mathcal{Y}_1} \sum_{y_2 \in \mathcal{Y}_2} \left| \left(W_2(y_2|x_2, s_2) - W_2'(y_2|x_2, s_2')\right) W_1'(y_1|x_1, s_1') \right| \\
&\quad = \sum_{y_1 \in \mathcal{Y}_1} \left| W_1(y_1|x_1, s_1) - W_1'(y_1|x_1, s_1') \right| + \sum_{y_2 \in \mathcal{Y}_2} \left| W_2(y_2|x_2, s_2) - W_2'(y_2|x_2, s_2') \right|.
\end{aligned}$$

Since $D((\mathfrak{W}_i, \mathfrak{V}_i), (\mathfrak{W}_i', \mathfrak{V}_i')) < \epsilon$, $i = 1, 2$, by assumption, we have

$$D((\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2)), (\mathfrak{W}_1' \otimes \mathfrak{W}_2', \mathfrak{V}_1' \otimes \mathfrak{V}_2') < 2\epsilon. \tag{12}$$

Now we can apply the stability result in Theorem 3. From this we know that for all AVWCs $(\widetilde{\mathfrak{W}}, \widetilde{\mathfrak{V}})$ with $\widetilde{W} : \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{S}_1 \times \mathcal{S}_2 \to \mathcal{P}(\mathcal{Y}_1 \times \mathcal{Y}_2)$ and $\widetilde{V} : \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{S}_1 \times \mathcal{S}_2 \to \mathcal{P}(\mathcal{Z}_1 \times \mathcal{Z}_2)$ and

$$D((\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2), (\widetilde{\mathfrak{W}}, \widetilde{\mathfrak{V}})) < \tilde{\epsilon}$$

we have

$$C_S(\widetilde{\mathfrak{W}}, \widetilde{\mathfrak{V}}) > 0.$$

Now we choose ϵ in Equation (12) small such that $2\epsilon < \tilde{\epsilon}$ holds. With this we obtain the desired positivity for all AVWCs $(\mathfrak{W}_1', \mathfrak{V}_1')$ and $(\mathfrak{W}_2', \mathfrak{V}_2')$ for which Equation (12) is satisfied. This completes the proof. □

This result shows that super-activation is not an isolated phenomenon of orthogonal AVWCs. In fact, whenever super-activation is possible for two AVWCs, it occurs for all AVWCs that are sufficiently close to them.

Corollary 1. *Let* $(\mathfrak{W}_1, \mathfrak{V}_1)$ *and* $(\mathfrak{W}_2, \mathfrak{V}_2)$ *be two useless orthogonal AVWCs that can be super-activated. Then* $(\mathfrak{W}_2, \mathfrak{V}_2)$ *super-activates all AVWCs* $(\mathfrak{W}_1', \mathfrak{V}_1')$ *that are close enough to* $(\mathfrak{W}_1, \mathfrak{V}_1)$.

Proof. The result follows immediately from Theorem 6. Note that we can even choose $\epsilon = \tilde{\epsilon}$ in this case to obtain the desired result. □

The previous result of Theorem 6 can even be strengthened. This formulation is more involved than the previous one, but the advantage is that it reveals the following behavior: The AVC to the legitimate receiver is much more important than the AVC to the eavesdropper in terms of super-activation. Specifically, there is no need of an explicit requirement on the distance between the eavesdropper channels. We obtain the following result.

Theorem 7. *Let* $(\mathfrak{W}_1, \mathfrak{V}_1)$ *and* $(\mathfrak{W}_2, \mathfrak{V}_2)$ *be two useless orthogonal AVWCs that can be super-activated. Then there exists an* $\epsilon > 0$ *such that all useless orthogonal AVWCs* $(\mathfrak{W}_1', \mathfrak{V}_1')$ *and* $(\mathfrak{W}_2', \mathfrak{V}_2')$ *that satisfy*

$$D(\mathfrak{W}_1, \mathfrak{W}_1') < \epsilon, \qquad D(\mathfrak{W}_2, \mathfrak{W}_2') < \epsilon,$$

and

$$C_{S,CR}(\mathfrak{W}_1' \otimes \mathfrak{W}_2', \mathfrak{V}_1' \otimes \mathfrak{V}_2') > 0,$$

can be super-activated as well.

Proof. We know that the combined AVC $\mathfrak{W}_1 \otimes \mathfrak{W}_2$ is non-symmetrizable, since otherwise super-activation would not be possible, *cf.* Theorem 5. Similarly as in the proof of Theorem 6 we can then show that $D(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{W}_1' \otimes \mathfrak{W}_2') < 2\epsilon$ holds. Next we consider the function $F(\mathfrak{W}_1 \otimes \mathfrak{W}_2)$, *cf.* Equation (9). Since $\mathfrak{W}_1 \otimes \mathfrak{W}_2$ is non-symmetrizable, we have $F(\mathfrak{W}_1 \otimes \mathfrak{W}_2) > 0$. In addition, since the function F depends in a continuous way on the channel, for all AVCs $\widetilde{\mathfrak{W}}$ with $\widetilde{W} : \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{S}_1 \times \mathcal{S}_2 \to \mathcal{P}(\mathcal{Y}_1 \times \mathcal{Y}_2)$ and $D(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \widetilde{\mathfrak{W}}) < \tilde{\epsilon}$ we always have $F(\widetilde{\mathfrak{W}}) > 0$. Here we have to choose $\tilde{\epsilon} > 0$ sufficiently small depending on $\mathfrak{W}_1 \otimes \mathfrak{W}_2$. Since $F(\widetilde{\mathfrak{W}}) > 0$, the AVC $\widetilde{\mathfrak{W}}$ is non-symmetrizable and from Theorem 2 it follows that

$$C_S(\mathfrak{W}_1' \otimes \mathfrak{W}_2', \mathfrak{V}_1' \otimes \mathfrak{V}_2') = C_{S,\mathrm{CR}}(\mathfrak{W}_1' \otimes \mathfrak{W}_2', \mathfrak{V}_1' \otimes \mathfrak{V}_2') > 0$$

which proves that these AVWCs can be super-activated. This completes the proof. □

In the following we briefly present an example in which super-activation is possible for all orthogonal AVWCs in a certain neighborhood. This example is based on an example given in ([22], Section V-C). This constructs suitable AVWCs, whose unassisted secrecy capacities are zero in a certain neighborhood, but who all can be super-activated to allow for secure communication at a positive rate.

Example 1. First, we construct an AVWC $(\mathfrak{W}^*, \mathfrak{V}^*)$ with $|\mathcal{X}| = 2$, $|\mathcal{Y}| = 3$, $|\mathcal{Z}| = 2$, and $|\mathcal{S}| = 2$ for which in a set of AVWCs $(\mathfrak{W}, \mathfrak{V})$ around this channel we always have $C_{S,\mathrm{CR}}(\mathfrak{W}^*, \mathfrak{V}^*) > 0$ and $C_S(\mathfrak{W}, \mathfrak{V}) = C_S(\mathfrak{W}^*, \mathfrak{V}^*) = 0$. To do so, we define the legitimate AVC as $\mathfrak{W}^* = \{W_1^*, W_2^*\}$ with

$$W_1^* = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{4} & 0 & \frac{3}{4} \end{pmatrix} \quad \text{and} \quad W_2^* = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

and the eavesdropper AVC as $\mathfrak{V}^* = \{V^*, V^*\}$ with

$$V^* = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}. \tag{13}$$

With this choice, the eavesdropper channel is fixed, while the legitimate channel allows appropriate variations. In particular, it is easy to show that $\mathfrak{W}^*$ is symmetrizable so that $C_S(\mathfrak{W}^*, \mathfrak{V}^*) = 0$ but $C_{S,\mathrm{CR}}(\mathfrak{W}^*, \mathfrak{V}^*) > 0$, *cf.* ([22], Section V-C). Further, for all AVWCs $(\mathfrak{W}, \mathfrak{V})$ with $D(\mathfrak{W}^*, \mathfrak{W}) < \epsilon$ for some $\epsilon > 0$ it holds that $C_S(\mathfrak{W}^*, \mathfrak{V}^*) = 0$ but $C_{S,\mathrm{CR}}(\mathfrak{W}^*, \mathfrak{V}^*) > 0$, *cf.* ([22], Theorem 6), which means that all AVWCs in a certain neighborhood have zero unassisted secrecy capacity. Now we can find another orthogonal AVWC $(\widetilde{\mathfrak{W}}, \widetilde{\mathfrak{V}})$ that super-activates the original AVWC $(\mathfrak{W}^*, \mathfrak{V}^*)$, but also all other AVWCs $(\mathfrak{W}, \mathfrak{V})$ with $D(\mathfrak{W}^*, \mathfrak{W}) < \epsilon$, *cf.* Corollary 1 and Theorem 7.

Remark 3. The previous considerations show that bonding of orthogonal resources can increase the performance significantly. Such bonding gains do not only appear if both unassisted secrecy capacities are equal to zero (super-activation), but also if only one of these is zero while the other one is positive (super-additivity). This follows by an easy adaptation of the discussion above.

Next we want to show that bonding of orthogonal resources reveals further effects and properties that are practically relevant. This is discussed in the following result.

Theorem 8. *Let $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$ be two useless orthogonal AVWCs that can be super-activated. Then the unassisted secrecy capacity $C_S(\mathfrak{W}_1' \otimes \mathfrak{W}_2', \mathfrak{V}_1' \otimes \mathfrak{V}_2')$ depends in a continuous way on the channels $(\mathfrak{W}_1', \mathfrak{V}_1')$ and $(\mathfrak{W}_2', \mathfrak{V}_2')$ with $D(\mathfrak{W}_i, \mathfrak{W}_i') < \epsilon$, $i = 1, 2$. Here, ϵ depends only on the orthogonal AVCs $\mathfrak{W}_1$ and $\mathfrak{W}_2$.*

Proof. Since the AVWCs $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$ can be super-activated, we know that $C_S(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) > 0$. Then we know that this is also true for all AVWCs $(\widetilde{\mathfrak{W}}, \widetilde{\mathfrak{V}})$ with $\widetilde{W} : \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{S}_1 \times \mathcal{S}_2 \to \mathcal{P}(\mathcal{Y}_1 \times \mathcal{Y}_2)$ and $\widetilde{V} : \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{S}_1 \times \mathcal{S}_2 \to \mathcal{P}(\mathcal{Z}_1 \times \mathcal{Z}_2)$ that are sufficiently close to $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$, *cf.* Theorem 3, so that

$$C_S(\widetilde{\mathfrak{W}}, \widetilde{\mathfrak{V}}) = C_{S,\mathrm{CR}}(\widetilde{\mathfrak{W}}, \widetilde{\mathfrak{V}})$$

holds. Since $C_{S,\mathrm{CR}}(\widetilde{\mathfrak{W}}, \widetilde{\mathfrak{V}})$ is a continuous function, *cf.* [20,22], the desired result follows then from Theorem 6. □

Remark 4. The unassisted secrecy capacity $C_S(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2)$ need not necessarily be continuous in $(\mathfrak{W}_1, \mathfrak{V}_1)$ or $(\mathfrak{W}_2, \mathfrak{V}_2)$. In particular, there are examples with a discontinuous behavior as discussed above.

Remark 5. We see that bonding of orthogonal resources can also lead to a more robust system which is continuous. On the other hand, for a single AVC such continuous behavior cannot be guaranteed in general.

In the following we briefly present an example that demonstrates these effects. This example is based on an example in ([22], Section V-A). This constructs suitable AVWCs, whose unassisted secrecy capacity is continuous after super-activation although the unassisted secrecy capacity of one AVWC itself has a discontinuity point.

Example 2. First, we construct an AVWC $(\mathfrak{W}(\lambda), \mathfrak{V})$ for $0 \leq \lambda \leq 1$ with $|\mathcal{X}| = 2$, $|\mathcal{Y}| = 3$, $|\mathcal{Z}| = 2$, and $|\mathcal{S}| = 2$, whose unassisted secrecy capacity has a discontinuity point. To do so, for $0 \leq \lambda \leq 1$ we define the legitimate AVC as $\mathfrak{W}(\lambda) = \{W_1(\lambda), W_2(\lambda)\}$ with

$$W_1(\lambda) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & 1-\lambda \end{pmatrix} \text{ and } W_2(\lambda) = \begin{pmatrix} \lambda & 0 & 1-\lambda \\ 0 & 1 & 0 \end{pmatrix}$$

and the eavesdropper AVC as $\mathfrak{V} = \{V^*, V^*\}$ with V^* the useless channel as in (13) of Example 1. It can be shown that the unassisted secrecy capacity of the AVWC $(\mathfrak{W}(\lambda), \mathfrak{V})$ has a discontinuity point at $\lambda = 0$, *i.e.*, we have $C_S(\mathfrak{W}(0), \mathfrak{V}) = 0$, but $\lim_{\lambda \searrow 0} C_S(\mathfrak{W}(0), \mathfrak{V}) > 0$, *cf.* ([22], Theorem 4). Now we can find another orthogonal AVWC $(\widetilde{\mathfrak{W}}, \widetilde{\mathfrak{V}})$ that super-activates the original AVWC $(\mathfrak{W}(\lambda), \mathfrak{V})$. Then we know from Theorem 8 that the unassisted secrecy capacity of this super-activated AVWC is continuous.

4. Communication over Orthogonal AVCs

The previous results and in particular Theorem 7 have shown that super-activation of AVWCs is robust in the eavesdropper AVC. Specifically, it is sufficient to require the eavesdropper AVC to be such that the CR-assisted secrecy capacity of the corresponding AVWC is positive. Then this capacity is continuous in the eavesdropper AVC. As a consequence, the phenomenon of super-activation depends particularly on the legitimate AVC. Accordingly, it is interesting to drop the eavesdropper and the security requirement for a while and study reliable message transmission over single-user AVCs in more detail.

4.1. Capacity Results

The single-user AVC is given as in Section 2.1 by considering only the legitimate AVC between the transmitter and legitimate receiver. Reliable message transmission for the single-user AVC has been well studied and its capacity has been established for both unassisted [13,14] and CR-assisted [12] codes.

Theorem 9 ([12]). *The* CR-assisted capacity $C_{CR}(\mathfrak{W})$ *of the AVC* $\mathfrak{W}$ *is*

$$C_{CR}(\mathfrak{W}) = \max_{P_X \in \mathcal{P}(\mathcal{X})} \inf_{q \in \mathcal{P}(\mathcal{S})} I(X; \overline{Y}_q) \tag{14}$$

where $\overline{Y}_q$ *denotes the random variable associated with the output of the averaged channel* $\overline{W}_q$, $q \in \mathcal{P}(\mathcal{S})$, *cf. Equation* (3).

The unassisted capacity is then completely characterized in terms of its CR-assisted capacity.

Theorem 10 ([13,14]). *The* unassisted capacity $C(\mathfrak{W})$ *of the AVC* $\mathfrak{W}$ *is*

$$C(\mathfrak{W}) = \begin{cases} C_{CR}(\mathfrak{W}) & \text{if } \mathfrak{W} \text{ is non-symmetrizable} \\ 0 & \text{if } \mathfrak{W} \text{ is symmetrizable.} \end{cases}$$

To the best of our knowledge, reliable message transmission over orthogonal AVCs has not been studied previously. This is surprising as this is already implicitly addressed by Shannon's question of the additivity of the zero error capacity [23]. Specifically, Ahlswede showed in [28] that the capacity of the AVC under the maximum error criterion includes the characterization of the zero error capacity as a special case. To this end, Alon's example in [27] for the super-additivity of the capacity of reliable message transmission over orthogonal AVCs under the maximum error criterion can be seen as the first contribution towards understanding the behavior of the capacity of orthogonal AVCs. In the following, we completely characterize the behavior of the capacity of orthogonal AVCs for the average error criterion.

4.2. Additivity of CR-Assisted Capacity

We start with the CR-assisted capacity and show that it is additive. This means that the CR-assisted capacity of two orthogonal AVCs is the sum of its CR-assisted capacities.

Theorem 11. *Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two orthogonal AVCs. Then the CR-assisted capacity is additive, i.e.,*

$$C_{CR}(\mathfrak{W}_1 \otimes \mathfrak{W}_2) = C_{CR}(\mathfrak{W}_1) + C_{CR}(\mathfrak{W}_2). \tag{15}$$

Proof. From the definition of capacity it follows immediately that

$$C_{\mathrm{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2) \geq C_{\mathrm{CR}}(\mathfrak{W}_1) + C_{\mathrm{CR}}(\mathfrak{W}_2) \tag{16}$$

is satisfied since joint encoding and decoding over both AVCs can only increase the capacity compared to an individual encoding and decoding for both channels. Thus, to show equality in Equation (15) it remains to prove that the reversed inequality is also true, *i.e.*, $C_{\mathrm{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2) \leq C_{\mathrm{CR}}(\mathfrak{W}_1) + C_{\mathrm{CR}}(\mathfrak{W}_2)$.

For the following argumentation it is beneficial to write the CR-assisted capacity in Equation (14) as

$$\begin{aligned} C_{\mathrm{CR}}(\mathfrak{W}) &= \max_{P_X \in \mathcal{P}(\mathcal{X})} \inf_{q \in \mathcal{P}(\mathcal{S})} I(X; \overline{Y}_q) \\ &= \max_{P_X \in \mathcal{P}(\mathcal{X})} \min_{q \in \mathcal{P}(\mathcal{S})} I(P_X, \overline{W}_q) \end{aligned}$$

as the mutual information term is completely determined by the input distribution $P_X \in \mathcal{P}(\mathcal{X})$ and the averaged channel $\overline{W}_q$, $q \in \mathcal{P}(\mathcal{S})$, *cf.* Equation (3).

With this notation, the CR-assisted capacity of the combined AVC $\mathfrak{W}_1 \otimes \mathfrak{W}_2$, *cf.* also Equations (10) and (11), is given by

$$C_{\mathrm{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2) = \max_{P_{X_1X_2} \in \mathcal{P}(\mathcal{X}_1 \times \mathcal{X}_2)} \min_{q_{12} \in \mathcal{P}(\mathcal{S}_1 \times \mathcal{S}_2)} I(P_{X_1X_2}, \overline{W}_{q_{12}}) \tag{17}$$

where $\overline{W}_{q_{12}}$, $q_{12} \in \mathcal{P}(\mathcal{S}_1 \times \mathcal{S}_2)$, denotes the corresponding averaged channel.

Now, this mutual information quantity in Equation (17) is continuous, concave in $P_{X_1X_2}$, and convex in $\overline{W}_{q_{12}}$ so that the order of max and min can be exchanged to obtain

$$\begin{aligned} C_{\mathrm{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2) &= \min_{q_{12} \in \mathcal{P}(\mathcal{S}_1 \times \mathcal{S}_2)} \max_{P_{X_1X_2} \in \mathcal{P}(\mathcal{X}_1 \times \mathcal{X}_2)} I(P_{X_1X_2}, \overline{W}_{q_{12}}) \\ &\leq \max_{P_{X_1X_2} \in \mathcal{P}(\mathcal{X}_1 \times \mathcal{X}_2)} I(P_{X_1X_2}, \overline{W}_{\hat{q}_1 \otimes \hat{q}_2}) \end{aligned}$$

for some arbitrary but fixed $\hat{q}_1 \in \mathcal{P}(\mathcal{S}_1)$ and $\hat{q}_2 \in \mathcal{P}(\mathcal{S}_2)$. In addition, we have

$$\begin{aligned} &\overline{W}_{\hat{q}_1 \otimes \hat{q}_2}(y_1, y_2 | x_1, x_2) \\ &\quad = \Big(\sum_{s_1 \in \mathcal{S}_1} \hat{q}_1(s_1) W_{1,s_1}(y_1|x_1) \Big) \Big(\sum_{s_2 \in \mathcal{S}_2} \hat{q}_2(s_2) W_{2,s_2}(y_2|x_2) \Big) \\ &\quad = \overline{W}_{1,\hat{q}_1}(y_1|x_1) \overline{W}_{2,\hat{q}_2}(y_2|x_2) \end{aligned}$$

so that

$$\overline{W}_{\hat{q}_1 \otimes \hat{q}_2} = \overline{W}_{1,\hat{q}_1} \otimes \overline{W}_{2,\hat{q}_2}.$$

Since for ordinary DMCs under the average error criterion we have additivity, it holds that

$$\max_{P_{X_1X_2} \in \mathcal{P}(\mathcal{X}_1 \times \mathcal{X}_2)} I(P_{X_1X_2}, \overline{W}_{\hat{q}_1 \otimes \hat{q}_2}) = \max_{P_{X_1} \in \mathcal{P}(\mathcal{X}_1)} I(P_{X_1}, \overline{W}_{1,\hat{q}_1}) + \max_{P_{X_2} \in \mathcal{P}(\mathcal{X}_2)} I(P_{X_2}, \overline{W}_{2,\hat{q}_2}).$$

Since $\hat{q}_1 \in \mathcal{P}(\mathcal{S}_1)$ and $\hat{q}_2 \in \mathcal{P}(\mathcal{S}_2)$ are arbitrary, we obtain

$$\begin{aligned} C_{\mathrm{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2) &\leq \min_{\hat{q}_1 \in \mathcal{P}(\mathcal{S}_1), \hat{q}_2 \in \mathcal{P}(\mathcal{S}_2)} \Big(\max_{P_{X_1} \in \mathcal{P}(\mathcal{X}_1)} I(P_{X_1}, \overline{W}_{1,\hat{q}_1}) + \max_{P_{X_2} \in \mathcal{P}(\mathcal{X}_2)} I(P_{X_2}, \overline{W}_{2,\hat{q}_2}) \Big) \\ &= \min_{\hat{q}_1 \in \mathcal{P}(\mathcal{S}_1)} \max_{P_{X_1} \in \mathcal{P}(\mathcal{X}_1)} I(P_{X_1}, \overline{W}_{1,\hat{q}_1}) + \min_{\hat{q}_2 \in \mathcal{P}(\mathcal{S}_2)} \max_{P_{X_2} \in \mathcal{P}(\mathcal{X}_2)} I(P_{X_2}, \overline{W}_{2,\hat{q}_2}) \\ &= C_{\mathrm{CR}}(\mathfrak{W}_1) + C_{\mathrm{CR}}(\mathfrak{W}_2) \end{aligned} \tag{18}$$

where the last step follows again from the fact that the mutual information is concave in the input distribution and convex in the channel which allows an exchange of min and max.

Now the inequalities in Equations (16) and (18) establish the desired additivity of the CR-assisted capacity, thereby proving the result. □

This result shows that the CR-assisted capacity is always additive and therewith confirms Shannon's conviction of the additivity of the capacity. The consequence is that joint encoding and decoding for both AVCs does not yield any gains in terms of CR-assisted capacity.

4.3. Super-Additivity of Unassisted Capacity

Next, we consider the unassisted capacity of two orthogonal AVCs.

Proposition 1. *Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two orthogonal AVCs. If the unassisted capacities satisfy $C(\mathfrak{W}_1) > 0$ and $C(\mathfrak{W}_2) > 0$, then the unassisted capacity is additive, i.e.,*

$$C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) = C(\mathfrak{W}_1) + C(\mathfrak{W}_2). \tag{19}$$

Proof. From the additivity of the CR-assisted capacity, *cf.* Theorem 11, we have

$$\begin{aligned} C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) &\leq C_{\mathrm{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2) \\ &= C_{\mathrm{CR}}(\mathfrak{W}_1) + C_{\mathrm{CR}}(\mathfrak{W}_2) \\ &= C(\mathfrak{W}_1) + C(\mathfrak{W}_2) \end{aligned} \tag{20}$$

where the last equality follows from Theorem 10. On the other hand we have

$$\begin{aligned} C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) &\geq C(\mathfrak{W}_1) + C(\mathfrak{W}_2) \\ &= C_{\mathrm{CR}}(\mathfrak{W}_1) + C_{\mathrm{CR}}(\mathfrak{W}_2) \\ &= C_{\mathrm{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2) \\ &= C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) \end{aligned} \tag{21}$$

where the first equality is again due to Theorem 10 since $C(\mathfrak{W}_1) > 0$ and $C(\mathfrak{W}_2) > 0$, and the second equality follows from Theorem 11. Equations (20) and (21) yield the desired equality in Equation (19), thereby proving the result. □

Proposition 2. *Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two orthogonal AVCs. If the unassisted capacities satisfy $C(\mathfrak{W}_1) = C(\mathfrak{W}_2) = 0$, then the unassisted capacity is additive, i.e.,*

$$C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) = C(\mathfrak{W}_1) + C(\mathfrak{W}_2).$$

Proof. If $C(\mathfrak{W}_1) = C(\mathfrak{W}_2) = 0$, then both AVCs are symmetrizable according to Definition 2. This means there exist stochastic matrices $\sigma_i : \mathcal{X}_i \to \mathcal{P}(\mathcal{S}_i)$, $i = 1, 2$, such that

$$\sum_{s_i \in \mathcal{S}_i} W_i(y_i|x_i, s_i)\sigma_i(s_i|x_i') = \sum_{s_i \in \mathcal{S}_i} W_i(y_i|x_i', s_i)\sigma_i(s_i|x_i)$$

holds for all $x_i, x_i' \in \mathcal{X}_i$ and $y_i \in \mathcal{Y}_i$, $i = 1, 2$.

Then, the AVC $\mathfrak{W}_1 \otimes \mathfrak{W}_2$ is symmetrizable as well and

$$\begin{aligned}
&\sum_{s_1 \in \mathcal{S}_1} \sum_{s_2 \in \mathcal{S}_2} W_1(y_1|x_1, s_1) W_2(y_2|x_2, s_2)\sigma_1(s_1|x_1')\sigma_2(s_2|x_2') \\
&\quad = \Big(\sum_{s_1 \in \mathcal{S}_1} W_1(y_1|x_1, s_1)\sigma_1(s_1|x_1') \Big) \Big(\sum_{s_2 \in \mathcal{S}_2} W_2(y_2|x_2, s_2)\sigma_2(s_2|x_2') \Big) \\
&\quad = \Big(\sum_{s_1 \in \mathcal{S}_1} W_1(y_1|x_1', s_1)\sigma_1(s_1|x_1) \Big) \Big(\sum_{s_2 \in \mathcal{S}_2} W_2(y_2|x_2', s_2)\sigma_2(s_2|x_2) \Big) \\
&\quad = \sum_{s_1 \in \mathcal{S}_1} \sum_{s_2 \in \mathcal{S}_2} W_1(y_1|x_1', s_1) W_2(y_2|x_2', s_2)\sigma_1(s_1|x_1)\sigma_2(s_2|x_2)
\end{aligned}$$

holds for all $x_i, x_i' \in \mathcal{X}_i$ and $y_i \in \mathcal{Y}_i$, $i = 1, 2$. This implies that $C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) = 0$ as well which shows the additivity for this case as well as completing the proof. □

These two results show that when the unassisted capacities are both positive or both zero, the overall unassisted capacity is additive. In addition, from Proposition 2 it follows immediately that super-activation is not possible for reliable message transmission over orthogonal AVCs.

Corollary 2. *Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two orthogonal AVCs. If the unassisted capacities satisfy $C(\mathfrak{W}_1) = C(\mathfrak{W}_2) = 0$, then super-activation is not possible for the combined AVC $\mathfrak{W}_1 \otimes \mathfrak{W}_2$.*

Finally, the following result solves the remaining case for which the unassisted capacity is actually super-additive.

Theorem 12. *Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two orthogonal AVCs. The unassisted capacity $C(\mathfrak{W}_1 \otimes \mathfrak{W}_2)$ is super-additive, i.e.,*

$$C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) > C(\mathfrak{W}_1) + C(\mathfrak{W}_2), \tag{22}$$

if and only if either of $\mathfrak{W}_1$ or $\mathfrak{W}_2$ is symmetrizable and has a positive CR-assisted capacity.

Without loss of generality, let $\mathfrak{W}_1$ be symmetrizable; then

$$\begin{aligned}
C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) &= C_{CR}(\mathfrak{W}_1) + C(\mathfrak{W}_2) \\
&> C(\mathfrak{W}_1) + C(\mathfrak{W}_2) = C(\mathfrak{W}_2).
\end{aligned}$$

Proof. First we show that if $\mathfrak{W}_1$ is symmetrizable and $C_{\mathrm{CR}}(\mathfrak{W}_1) > 0$, then the unassisted capacity $C(\mathfrak{W}_1 \otimes \mathfrak{W}_2)$ is super-additive. To do so, we use the idea of Ahlswede's de-randomization [13]. Although CR is not available, CR-assisted codes can still be used if the transmitter is able to inform the receiver prior to the actual message transmission about which realization of encoder and decoder has to be used. From [13] we know that the amount of information that needs to be transmitted prior to transmission for this task is polynomial in the block length and therewith negligible for increasing block length.

Since $\mathfrak{W}_2$ is non-symmetrizable, we have $C_{\mathrm{CR}}(\mathfrak{W}_2) > 0$ and therefore also $C(\mathfrak{W}_2) > 0$. This allows us to use the second AVC to transmit information to the receiver to make CR available for the first AVC $\mathfrak{W}_1$. Then CR-assisted codes can be used for $\mathfrak{W}_1$ so that

$$\begin{aligned} C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) &\geq C_{\mathrm{CR}}(\mathfrak{W}_1) + C(\mathfrak{W}_2) \\ &= C_{\mathrm{CR}}(\mathfrak{W}_1) + C_{\mathrm{CR}}(\mathfrak{W}_2) \\ &= C_{\mathrm{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2) \end{aligned}$$

is achievable. Since $C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) \leq C_{\mathrm{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2)$ is obviously true, we have equality which means that we actually achieve

$$C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) = C_{\mathrm{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2)$$

which shows the super-additivity of $C(\mathfrak{W}_1 \otimes \mathfrak{W}_2)$.

Next we show the other direction: If $C(\mathfrak{W}_1 \otimes \mathfrak{W}_2)$ is super-additive, *i.e.*,

$$C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) > C(\mathfrak{W}_1) + C(\mathfrak{W}_2), \tag{23}$$

then either $\mathfrak{W}_1$ or $\mathfrak{W}_2$ must be symmetrizable so that $C(\mathfrak{W}_1) = 0$ or $C(\mathfrak{W}_2) = 0$.

Assume both unassisted capacities are strictly positive. Then from Theorem 10 it follows that $C(\mathfrak{W}_1) = C_{\mathrm{CR}}(\mathfrak{W}_1)$ and $C(\mathfrak{W}_2) = C_{\mathrm{CR}}(\mathfrak{W}_2)$ so that Equation (23) becomes

$$\begin{aligned} C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) &> C_{\mathrm{CR}}(\mathfrak{W}_1) + C_{\mathrm{CR}}(\mathfrak{W}_2) \\ &= C_{\mathrm{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2) \end{aligned}$$

where the last step follows from the additivity of the CR-assisted capacity, *cf.* Theorem 11. This contradicts $C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) \leq C_{\mathrm{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2)$ which always holds. Accordingly, without loss of generality, we must have $C(\mathfrak{W}_1) = 0$. However, $C_{\mathrm{CR}}(\mathfrak{W}_1) > 0$ must be true, since otherwise we would have

$$C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) > 0 + C_{\mathrm{CR}}(\mathfrak{W}_2) = C_{\mathrm{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2)$$

which would be a contradiction. Thus, it must hold that $C_{\mathrm{CR}}(\mathfrak{W}_1) > 0$ and $C(\mathfrak{W}_1) = 0$ so that $\mathfrak{W}_1$ is symmetrizable, proving the desired result. □

This result shows that the capacity of reliable message transmission over orthogonal AVCs is super-additive under certain circumstances. This breaks with the world view of classical additivity of resources.

Note that Example 1 discussed in Section 3.2 provides an AVC with $|\mathcal{S}| = 2$, which exactly displays the behavior characterized above. Interestingly, if the state set is reduced to $|\mathcal{S}| = 1$, such a behavior is not possible anymore.

5. Discussion

In this paper, we have studied communication under arbitrarily varying channel conditions. For the case of public message transmission over orthogonal AVCs we have completely characterized the behavior of the unassisted and CR-assisted capacity. While the CR-assisted capacity is additive, the unassisted capacity is super-additive, which means that there are orthogonal AVCs for which joint encoding and decoding results in a higher capacity than individual encoding and decoding.

If secrecy requirements are imposed on the message transmission, the capacity behavior for orthogonal AVWCs becomes even more involved. In this case, the phenomenon of super-activation occurs. A joint use of two completely useless AVWCs, *i.e.*, with zero unassisted secrecy capacity, can result in a combined AVWC whose unassisted secrecy capacity is non-zero. From a practical

point of view this has important consequences for medium access control and in particular for resource allocation.

The problem of reliable communication over AVCs is closely related to Shannon's zero error capacity problem, as the latter turns out to be a special case of the capacity of the AVC under the maximum error criterion. Shannon conjectured in 1956 that the zero error capacity is additive. Accordingly, the phenomena of super-additivity and super-activation for AVCs and AVWCs respectively are remarkable as these properties show the non-additivity of the capacity of the AVC.

The phenomenon of super-activation has substantial consequences for jamming strategies of potential adversaries. Let us assume that there are two orthogonal AVWCs that can be super-activated. Further assume that for each AVWC an adversary has a suitable jamming strategy to drive the unassisted secrecy capacity to zero. In more detail, for each AVWC the adversary can choose a corresponding state sequence that symmetrizes the legitimate AVC, prohibiting any reliable communication between transmitter and legitimate receiver. Now, joint encoding and decoding allows super-activation of the combined AVWC to make the communication robust: They can now transmit at a positive secrecy rate. This means that for the adversary there is no suitable jamming strategy for the combined AVWC although there is one for each AVWC individually. As there are no restrictions on the strategy space of the adversary, this includes even the case of a product strategy consisting of both individually working jamming strategies.

Super-activation is not an isolated phenomenon. We have shown that whenever orthogonal AVWCs can be super-activated, this is also true for all AVWCs in a certain neighborhood. As a consequence the overall system becomes stable as well. If a super-activated AVWC allows for secure communication with a positive rate, then this is true for all AVWCs sufficiently close to this super-activated AVWC.

Finally we want to note that this also has a game-theoretic interpretation of a "*game against nature*" [37]. The legitimate users (player) and the adversary (nature) play a two-player zero-sum game [38,39] with the secure communication rate as the payoff function. In this game, the set of state sequences corresponds to nature's action space, and nature's intention is to establish the worst possible communication conditions by selecting the state sequence such that the legitimate AVC becomes symmetrizable. The set of input distributions corresponds to the action space of the player and, clearly, the aim is to maximize the secure communication rate. Within this game against nature framework, the player and nature move simultaneously without knowing the other's choice which leads to the max min expressions in the corresponding secrecy capacity results.

Acknowledgments: Holger Boche would like to thank John F. Nash, Jr. for the discussions they had about game theory, equilibrium concepts, and the application of such concepts to communication systems. He would further like to thank Damian Dudek for the numerous discussions they had about physical layer security under practically relevant communication constraints and his insistence on elaborating the differences between public and secure message transmission. The authors would also like to thank Eduard A. Jorswieck and Carsten Janda for insightful discussions and suggestions. The work of H. Vincent Poor was supported in part by the U. S. National Science Foundation under Grant CMMI-1435778.

Author Contributions: All authors contributed equally to this work. All authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387.
2. Liang, Y.; Poor, H.V.; Shamai, S. Information theoretic security. *Found. Trends Commun. Inf. Theory* **2009**, *5*, 355–580.
3. Liu, R., Trappe, W., Eds. *Securing Wireless Communications at the Physical Layer*; Springer: New York, NY, USA, 2010.
4. Jorswieck, E.A.; Wolf, A.; Gerbracht, S. Secrecy on the physical layer in wireless networks. In *Trends in Telecommunications Technologies*; Intech: Rijeka, Croatia, 2010; pp. 413–435.

5. Bloch, M.; Barros, J. *Physical-Layer Security: From Information Theory to Security Engineering*; Cambridge University Press: Cambridge, UK, 2011.
6. Zhou, X., Song, L., Zhang, Y., Eds. *Physical Layer Security in Wireless Communications*; CRC Press: Boca Raton, FL, USA, 2013.
7. Schaefer, R.F.; Boche, H. Physical layer service integration in wireless networks—Signal processing challenges. *IEEE Signal Process. Mag.* **2014**, *31*, 147–156.
8. Deutsche Telekom AG Laboratories. Next generation mobile networks: (R)evolution in mobile communications. *Technology Radar Edition III/2010, Feature Paper*, 2010. Available online: http://www.lti.ei.tum.de/fileadmin/w00bgd/www/pdf/2010-III_Feature_Paper_Next-Generation-Mobile-Networks_final.pdf (accessed on 28 April 2016).
9. Helmbrecht, U.; Plaga, R. New challenges for IT-security research in ICT. In *World Federation of Scientists International Seminars on Planetary Emergencies*; World Scientific: Singapore, 2008; pp. 1–6.
10. Fettweis, G.; Boche, H.; Wiegand, T.; Zielinksi, E.; Schotten, H.; Merz, P.; Hirche, S.; Festag, A.; Häffner, W.; Meyer, M.; *et al*. *The Tactile Internet*; Technology Watch Report of ITU (International Telecommunication Union): Geneva, Switzerland, 2014.
11. Schaefer, R.F.; Boche, H.; Poor, H.V. Secure communication under channel uncertainty and adversarial attacks. *Proc. IEEE* **2015**, *102*, 1796–1813.
12. Blackwell, D.; Breiman, L.; Thomasian, A.J. The capacities of certain channel classes under random coding. *Ann. Math. Stat.* **1960**, *31*, 558–567.
13. Ahlswede, R. Elimination of correlation in random codes for arbitrarily varying channels. *Z. Wahrscheinlichkeitstheorie Verw. Gebiete* **1978**, *44*, 159–175.
14. Csiszár, I.; Narayan, P. The capacity of the arbitrarily varying channel revisited: Positivity, constraints. *IEEE Trans. Inf. Theory* **1988**, *34*, 181–193.
15. MolavianJazi, E.; Bloch, M.; Laneman, J.N. Arbitrary jamming can preclude secure communication. In Proceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA, 30 September–2 October 2009; pp. 1069–1075.
16. Bjelaković, I.; Boche, H.; Sommerfeld, J. Capacity results for arbitrarily varying wiretap channels. In *Information Theory, Combinatorics, and Search Theory*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 123–144.
17. Boche, H.; Schaefer, R.F. Capacity results and super-activation for wiretap channels with active wiretappers. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1482–1496.
18. Boche, H.; Schaefer, R.F.; Poor, H.V. On arbitrarily varying wiretap channels for different classes of secrecy measures. In Proceedings of the IEEE International Symposium on Information Theory, Honolulu, HI, USA, 29 June–4 July 2014; pp. 2376–2380.
19. Janda, C.R.; Scheunert, C.; Jorswieck, E.A. Wiretap-channels with constrained active attacks. In Proceedings of the Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, 2–5 November 2014; pp. 1984–1988.
20. Wiese, M.; Nötzel, J.; Boche, H. A channel under simultaneous jamming and eavesdropping attack—Correlated random coding capacities under strong secrecy criteria. **2015**, arXiv:1410.8078.
21. Nötzel, J.; Wiese, M.; Boche, H. The arbitrarily varying wiretap channel—Secret randomness, stability and super-activation. In Proceedings of 2015 IEEE International Symposium on Information Theory, Hong Kong, China, 14–19 June 2015; pp. 2151–2155.
22. Boche, H.; Schaefer, R.F.; Poor, H.V. On the continuity of the secrecy capacity of compound and arbitrarily varying wiretap channels. *IEEE Trans. Inf. Forensics Secur.* **2015**, *12*, 2531–2546.
23. Shannon, C.E. The zero error capacity of a noisy channel. *IRE Trans. Inf. Theory* **1956**, *2*, 8–19.
24. Lovász, L. On the Shannon capacity of a graph. *IEEE Trans. Inf. Theory* **1979**, *25*, 1–7.
25. Ahlswede, A., Althöfer, I., Deppe, C., Tamm, U., Eds. *Rudolf Ahlswede's Lectures on Information Theory 3—Hiding Data: Selected Topics*; Springer: Cham, Switzerland, 2016.
26. Haemers, W. On some problems of Lovász concerning the Shannon capacity of a graph. *IEEE Trans. Inf. Theory* **1979**, *25*, 231–232.
27. Alon, N. The Shannon capacity of a union. *Combinatorica* **1998**, *18*, 301–310.
28. Ahlswede, R. A note on the existence of the weak capacity for channels with arbitrarily varying channel probability functions and its relation to Shannon's zero error capacity. *Ann. Math. Stat.* **1970**, *41*, 1027–1033.

29. Aigner, M.; Ziegler, G.M. *Proofs from THE BOOK*, 5th ed.; Springer: Berlin/Heidelberg, Germany, 2014.
30. Smith, G.; Smolin, J.A.; Yard, J. Quantum communication with Gaussian channels of zero quantum capacity. *Nat. Photonics* **2011**, *5*, 624–627.
31. Giedke, G.; Wolf, M.M. Quantum communication: Super-activated channels. *Nat. Photonics* **2011**, *5*, 578–580.
32. Csiszár, I. Almost independence and secrecy capacity. *Probl. Pered. Inform.* **1996**, *32*, 48–57.
33. Maurer, U.M.; Wolf, S. Information-theoretic key agreement: From weak to strong secrecy for free. In *Advances in Cryptology — EUROCRYPT 2000*; Springer: Berlin/Heidelberg, Germany, 2000; Volume 1807, pp. 351–368.
34. Liang, Y.; Kramer, G.; Poor, H.V.; Shamai, S. Compound wiretap channels. *EURASIP J. Wirel. Commun. Netw.* **2009**, doi:10.1155/2009/142374.
35. Bjelaković, I.; Boche, H.; Sommerfeld, J. Secrecy results for compound wiretap channels. *Probl. Inf. Transm.* **2013**, *49*, 73–98.
36. Schaefer, R.F.; Loyka, S. The secrecy capacity of compound MIMO Gaussian channels. *IEEE Trans. Inf. Theory* **2015**, *61*, 5535–5552.
37. Milnor, J. *Games against Nature*; RAND Corporation: Santa Monica, CA, USA, 1951; pp. 49–59.
38. Aumann, R.J.; Hart, S. *Handbook of Game Theory with Economic Applications*; Elsevier: Oxford, UK, 1994; Volume 2.
39. Basar, T.; Olsder, G.J. *Dynamic Noncooperative Game Theory*, 2nd ed.; SIAM: New York, NY, USA, 1999.