Wiretap-Channels under Constrained Active and Passive Attacks

Carsten Rudolf Janda*, Moritz Wiese‡, Janis Nötzel†, Holger Boche† and Eduard A. Jorswieck*

*Communications Theory, Communications Laboratory Dresden University of Technology Dresden, Saxony, Germany
{Carsten.Janda, Eduard.Jorswieck}@tu-dresden.de

†Institute of Theoretical Information Technology Munich University of Technology München, Bavaria, Germany
{janis.noetzel, boche}@tum.de

‡ACCESS Linnaeus Center, School of Electrical Engineering, KTH Royal Institute of Stockholm, Stockholm, Sweden
moritzw@kth.se

***Abstract*—In this paper, the pessimistic multi letter common randomness assisted secrecy capacity for the Arbitrarily Varying Wiretap Channel (AVWC) under input and state constraints is derived.**

***Index Terms*—Active Eavesdroppers, AVWC, Constraints, Physical Layer Secrecy**

I. Introduction

Nowadays, information theoretic approaches to security are intensively discussed as a complement to cryptographic techniques. Such approaches jointly establish reliable communication and data confidentiality at the physical layer by taking the properties of the noisy channel into account.

What most of the previous studies have in common is that all channels (including those to a possible eavesdropper) are assumed to be perfectly known to all users and fixed during the entire duration of transmission. However, in practical systems, **C**hannel **S**tate **I**nformation (CSI) will always be limited due to the nature of the wireless channel and estimation/feedback inaccuracy. Furthermore, eavesdroppers will not provide any information about their channels to the legitimate users because this would make eavesdropping even harder. In order to design wireless systems resilient against failures caused by nature (fading, noise, etc.) and robust against malicious attacks, the correct system-theoretic model is the **C**ompound **C**hannel (CC) and the **A**rbitrarily **V**arying **C**hannel (AVC) model, respectively. The CC model applies if the state of the channel is constant for the duration of one codeword. This is an advisable model for the random impairments of nature, e.g., the quasi-static block fading channels. The AVC model is suitable if each channel use is affected by a different channel state. This correctly models malicious attacks, e.g., jamming attacks. In the literature, the characterization of the secrecy capacity of AVWCs relies on methods introduced by Ahlswede thirty years ago [1], [2], [3] and on methods introduced by Csiszár and Narayan in [4], [5]. In [6] and [7] the authors introduced the CC and the AVC, first. The author in [2] described the capacity region in an AVC for the average error probability and the maximum error probability condition using different types of codes, deterministic, stochastic encoding, and common randomness assisted codes. Therefore, two basic concepts, the **R**obustification **T**echnique (RT) and the **E**limination **T**echnique (ET) are developed. They are used to derive a common randomness assisted code capacity for an AVC from a deterministic code capacity of a CC, and to derive the deterministic code capacity of an AVC starting from the common randomness assisted code capacity of the same AVC. One famous result, the so called "Ahlswede's Dichotomy", states that the deterministic code capacity of an AVC equals its common randomness assisted code capacity or equals zero. Unfortunately, the ET technique does not hold if constraints are imposed. In [5] and [4], the authors introduce conditions on input and state constraints and conclude that the symmetrizability condition is necessary and sufficient in the case of no constraints, to render the capacity zero. In contrast to this, the authors are able to show that in the case of constraints, the symmetrizability condition is no longer sufficient, using a type-based proof technique. The authors consider peak constraints in [5]. In [4], peak- and average constraints are investigated. If the constraints are in an average sense, only ϵ capacities are shown to exist or in other words only a weak converse exists. In [8], the authors give an overview of the topics of AVCs, CCs, deterministic codes and common randomness assisted codes. The first who introduced the terms of secrecy and information theory was Shannon, in his work in [9]. The authors of [10], [11] and [12] continued that approach by investigating the degraded and the non-degraded **W**ire**t**ap **C**hannel (WTC) under the weak secrecy criterion and extended the considerations to the Gaussian scenario. In [13], [14] and [15], the authors have a look at WTCs with an active eavesdropper, which results in the investigation of **C**ompound **W**iretap **C**hannels (CWCs) and AVWCs. In [13], the authors establish a full coding theorem for the CWC under the strong secrecy criterion. They compute a lower bound on the secrecy

978-1-4673-7876-5/15/$31.00 ©2015 IEEE

capacity under the condition of CSI at the encoder. This bound equals the upper bound for general CWCs introduced by Liang. In [13],there is a stronger secrecy requirement than in [10], [11] and [12] and the maximum error probability is taken into account. The authors use a decoder which is robust against randomized encoding and prove a lower bound of the secrecy capacity of a CWC without CSI. Furthermore, a multiple-letter expression is provided. Additionally, hints on the operational meaning of strong secrecy are provided. By using the variational distance, the authors are able to prove that the error probability and the information leakage to the offender vanishes exponentially with the codeword block length. In [16], the authors investigate the effects of active attacks on wiretap channels and show that if the legitimate channel possesses a bad averaged state such that the channel is degraded with respect to the eavesdropping channel, secure communication is not possible. In [14] the authors calculate a lower bound on the common randomness assisted secrecy capacity under an average error probability condition and with the strong secrecy requirement in the presence of a "best" channel to the eavesdropper. They show that Ahlswede's Dichotomy [2] holds under secrecy conditions. The deterministic wiretap-code secrecy capacity is either zero in the case that the channel to the legitimate receiver is symmetrizable, or equals the common randomness assisted secrecy capacity. Using these relations, a lower bound for the deterministic wiretap-code secrecy capacity is given. Furthermore, upper bounds on the deterministic wiretap-code secrecy capacity in the general case are computed. So far, channels with states, without and with secrecy requirements have been considered, such as the CC, AVC, CWC, and AVWC. Only in the former case have constraints been investigated. In the following, we will state our notation in Section II, our system model in Section III, our main result in Section IV, give a hint on the proof in Section V and will discuss our result in Section VI.

II. Notation

We adapt our notation according to [17]. That means, all logarithms are taken to the base 2. Equivalently, the $\exp\{.\}$ function means $2^{\{.\}}$. Sets are denoted by calligraphic letters. The cardinality of a set $\mathcal{U}$ is denoted by $|\mathcal{U}|$. The set of all probability measures on a set $\mathcal{U}$ is denoted by $\mathcal{P}(\mathcal{U})$. For $p \in \mathcal{P}(\mathcal{U})$ we define $p^n \in \mathcal{P}(\mathcal{U}^n)$ as $p^n(x^n) = \prod_i p(x_i)$. The entropies, and mutual information terms will be written in terms of the involved probability functions. For example

$$H(W|p) := -\sum_{x,y} p(x)W(y|x)\log W(y|x)$$
$$I(p;W) := H(pW) - H(W|p).$$

Furthermore, let the type of a sequence $s^n = (s_1, s_2, ..., s_n)$ be the probability measure $q \in \mathcal{P}(\mathcal{S})$ defined by $q(a) = \frac{1}{n}N(a|s^n)$, where $N(a|s^n)$ denotes the number of occurrences of a in the sequence s^n. The set of all possible types of length n is denoted by $\mathcal{P}_0^n(\mathcal{S})$.

III. System Model

We consider a common randomness assisted AVWC as depicted in Fig. (1).

Definition 1 (**A**rbitrarily **V**arying **W**iretap **C**hannel)**.** We describe an AVWC by $(\mathcal{X}, \mathcal{S}, W_{Y|X,S}\ V_{Z|X,S}, \mathcal{Y}, \mathcal{Z})$. The family of channels to the legitimate receiver is $\mathcal{W} = \{W(Y|X,s),\ s \in \mathcal{S}\}$, and the family of channels to the illegitimate receiver is $\mathcal{V} = \{V(Z|X,s),\ s \in \mathcal{S}\}$. The channel is memoryless in that sense, that the probability of receiving the sequences $y^n = (y_1, y_2, ..., y_n)$ and $z^n = (z_1, z_2, ..., z_n)$, when sending $x^n = (x_1, x_2, ..., x_n)$ is

$$W^n(y^n|x^n, s^n) = \prod_{i=1}^n W(y_i|x_i, s_i),$$
$$V^n(z^n|x^n, s^n) = \prod_{i=1}^n V(z_i|x_i, s_i).$$

The AVWC is then defined as the pair $(\mathcal{W}, \mathcal{V})$.

Furthermore, we assume that the input and the state spaces are constrained.

Definition 2 (Peak Constraints [5], [4])**.** Let g_{up}, g_{lo} be nonnegative functions on $\mathcal{X}$ and l_{up}, l_{lo} nonnegative functions on $\mathcal{S}$. Then we define

$$g_{up}(\mathbf{x}) := \frac{1}{n}\sum_{i=1}^n g_{up}(x_i) \le \Gamma_{up}, \tag{1}$$
$$g_{lo}(\mathbf{x}) := \frac{1}{n}\sum_{i=1}^n g_{lo}(x_i) \ge \Gamma_{lo}, \tag{2}$$
$$l_{up}(\mathbf{s}) := \frac{1}{n}\sum_{i=1}^n l_{up}(s_i) \le \Lambda_{up}, \tag{3}$$
$$l_{lo}(\mathbf{s}) := \frac{1}{n}\sum_{i=1}^n l_{lo}(s_i) \ge \Lambda_{lo}, \tag{4}$$

as the peak input-, and peak state constraints, respectively.

Remark 1 (Lower Bounds)*.* In the literature, only upper bounds for the sequences x^n and s^n are considered. The lower bounds are usually assumed to be zero. We explicitly allow the lower bounds to take values different from zero.

Definition 3 (Constrained State and Input Spaces)**.** We define the constrained state and input spaces as

$$\mathcal{L}_n := \left\{ s^n \in \mathcal{S}^n : \frac{1}{n}\sum_{i=1}^n l_{up}(s_i) \le \Lambda_{up}, \ \frac{1}{n}\sum_{i=1}^n l_{lo}(s_i) \ge \Lambda_{lo} \right\} \quad \text{and}$$
$$\mathcal{G}_n := \left\{ x^n \in \mathcal{X}^n : \frac{1}{n}\sum_{i=1}^n g_{up}(x_i) \le \Gamma_{up}, \ \frac{1}{n}\sum_{i=1}^n g_{lo}(x_i) \ge \Gamma_{lo} \right\}.$$

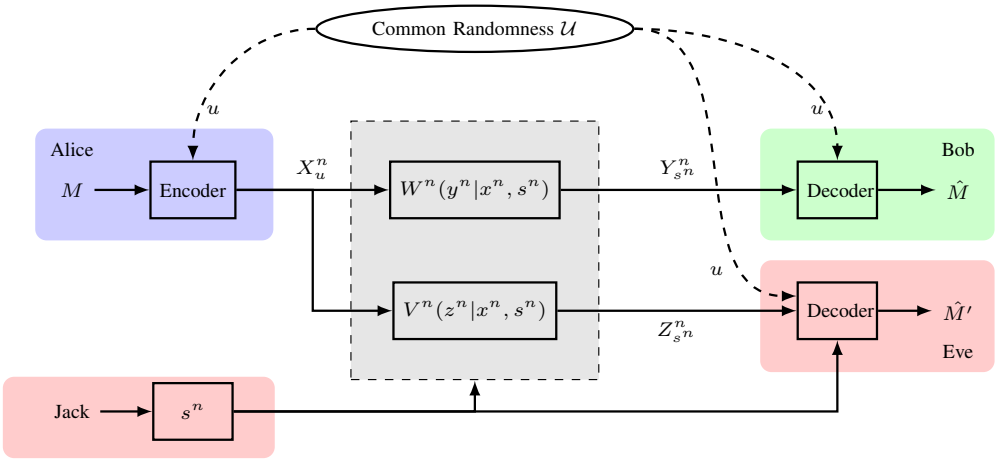

Fig. 1: System model.

Furthermore, we define the sets $\widetilde{\mathcal{L}}_n$ and $\widetilde{\mathcal{G}}_n$ as

$$\widetilde{\mathcal{L}}_n := \Bigg\{ q \in \mathcal{P}_0^n(\mathcal{S}) : \sum_{s\in\mathcal{S}} q(s) l_{up}(s) \le \Lambda_{up}, \sum_{s\in\mathcal{S}} q(s) l_{lo}(s) \ge \Lambda_{lo} \Bigg\} \quad \text{and}$$

$$\widetilde{\mathcal{G}}_n := \Bigg\{ q \in \mathcal{P}_0^n(\mathcal{X}) : \sum_{x\in\mathcal{X}} q(x) g_{up}(x) \le \Gamma_{up}, \sum_{x\in\mathcal{X}} q(x) g_{lo}(x) \ge \Gamma_{lo} \Bigg\}.$$

Definition 4 (Deterministic Wiretap-Code [2])**.** An (n, J_n) deterministic wiretap-code $\mathcal{K}_n$ consists of a stochastic encoder $E : \mathcal{J} \to \mathcal{P}(\mathcal{G}_n)$ and mutually disjoint decoding sets $\mathcal{D}_j : \mathcal{Y}^n \to \mathcal{J}$, with message set $\mathcal{J} : \{1, ..., J_n\}$. We denote $EW^n(y^n|j, s^n) : \mathcal{J}_n \to \mathcal{P}(\mathcal{Y}^n)$ and write

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

where we take only these encoders $E(x^n|j)$, whose outputs x^n lie in $\mathcal{G}_n$. The average error $e(\mathcal{K}_n)$ can be expressed as

$$e(\mathcal{K}_n) := \max_{s^n\in\mathcal{L}_n} \frac{1}{J_n} \sum_{j=1}^{J_n} \sum_{x^n\in\mathcal{X}^n} E(x^n|j) W^n(\mathcal{D}_j^c|x^n,s^n)$$
$$= \max_{s^n\in\mathcal{L}_n} \frac{1}{J_n} \sum_{j=1}^{J_n} EW^n(\mathcal{D}_j^c|j,s^n).$$

Definition 5 (Common Randomness Assited Code [2])**.** An $(n, J_n, \mathcal{U}, p_U)$ common randomness assisted code $\mathcal{K}_n^{\text{ran}}$ consists of a family of stochastic encoders $E_u : \mathcal{J} \to \mathcal{X}^n$ and mutually disjoint decoding sets $\mathcal{D}_{j,u} : \mathcal{Y}^n \to \mathcal{J}$ with message set $\mathcal{J} : \{1, ..., J_n\}$, where $u \in \mathcal{U}$ has a distribution $p_U \in \mathcal{P}(\mathcal{U})$. Again, we take only those encoders, whose outputs lie in $\mathcal{G}_n$. The average error over all possible (randomly chosen deterministic wiretap) codebooks $e(\mathcal{K}_n^{\text{ran}})$ can be written as

$$e(\mathcal{K}_n^{\text{ran}}) := \max_{s^n\in\mathcal{L}_n} \frac{1}{J_n} \sum_{j=1}^{J_n} \sum_{u\in\mathcal{U}} \sum_{x^n\in\mathcal{X}^n} E_u(x^n|j) W^n(\mathcal{D}_{j,u}^c|x^n,s^n) p_U(u).$$

Definition 6 (Achievable Common Randomness Assisted Secrecy Rate and Common Randomness Assisted Secrecy Capacity [17])**.** A nonnegative number R_S is called an achievable common randomness assisted secrecy rate for the AVWC if there exists a sequence $(\mathcal{K}_n^{\text{ran}})_{n=1}^{\infty}$ of $(n, J_n, \mathcal{U}, p_U)$ common randomness assisted codes, such that the following requirements are fulfilled

$$\liminf_{n\to\infty} \frac{1}{n} \log J_n \ge R_S, \tag{5}$$
$$\lim_{n\to\infty} e(\mathcal{K}_u^{\text{ran}}) = 0, \tag{6}$$
$$\lim_{n\to\infty} \max_{s^n\in\mathcal{L}_n} \sum_{u\in\mathcal{U}} I(p_{J_n}; E_u V_{s^n}^n) p_U(u) = 0. \tag{7}$$

The supremum of all achievable common randomness assisted secrecy rates for the AVWC is called the common randomness assisted secrecy capacity of the AVWC $(\mathcal{W}, \mathcal{V})$ and is denoted by $C_S^{\text{ran}}(\mathcal{W}, \mathcal{V})$.

Definition 7 (Enhanced Achievable Common Randomness Assisted Secrecy Rate and Enhanced Common Randomness Assisted Secrecy Capacity [17])**.** A nonnegative number R_S is called an achievable enhanced common randomness assisted secrecy rate for the AVWC if there exists a sequence $(\mathcal{K}_n^{\text{ran}})_{n=1}^{\infty}$ of $(n, J_n, \mathcal{U}, p_U)$ common randomness assisted codes, such that (6) and (5) hold and

$$\lim_{n\to\infty} \max_{s^n\in\mathcal{L}_n} \max_{u\in\mathcal{U}} I(p_{J_n}; E_u V_{s^n}^n) = 0 \tag{8}$$

is fulfilled. The supremum of all achievable enhanced common randomness assisted secrecy rates for the AVWC is called the enhanced common randomness assisted secrecy capacity of the AVWC $(\mathcal{W}, \mathcal{V})$ and is denoted by $\widehat{C}_S^{\text{ran}}(\mathcal{W}, \mathcal{V})$.

IV. Common Randomness Code Secrecy Capacity for the AVWC with Constraints

Let us now state our main result.

Theorem 1. *The pessimistic enhanced common randomness assisted secrecy capacity and the pessimistic common randomness assisted secrecy capacity for the AVWC with input and state constraints as in (1), (2), (3) and (4) can be expressed as*

$$R_S^*(\mathcal{W},\mathcal{V}) := \liminf_{k\to\infty} \frac{1}{k} \sup_{\mathcal{Q}\subset\mathbb{N} \text{ finite}} \max_{p\in\mathcal{P}(\mathcal{Q})} \max_{Q:\mathcal{Q}\to\widetilde{\mathcal{G}}_k} \left(\min_{t\in\mathcal{P}(\mathcal{S})} I(p;QW_t^k) - \max_{s^k\in\mathcal{L}_k} I(p;QV_{s^k}^k) \right), \quad (9)$$

where $\max_{s^k\in\mathcal{L}_k} I(p;QV_{s^k}^k)$ *can be further expressed as*

$$\max_{s^k\in\mathcal{L}_k} I(p;QV_{s^k}^k) = \max_{\widetilde{q}^k\in\mathcal{P}(\mathcal{L}_k)} I(p;QV_{\widetilde{q}^k}^k),$$
$$V_{\widetilde{q}^k}^k = \sum_{s^k\in\mathcal{L}_k} \widetilde{q}^k(s^k) V_{s^k}^k,$$

due to the convexity of mutual information in the channel.

V. Sketch of the Proof of Theorem 1

We follow the proof strategy of [17] and adapt it to the case of input and state constraints. Due to the page limitation, we only give a sketch of the proof. For more details, please consult [17]. The results of the Method of Types and the Chernoff-Hoeffding bound are widely used in the proof. First, the achievable secrecy rate is shown for the mixed **C**ompound-**A**rbitrarily **V**arying **W**iretap **C**hannel (CAVWC). Then, using a modification of Ahlswede's RT we derive the achievable secrecy rate for the AVWC.

Definition 8 (A Mixed **C**ompound-**A**rbitrarily **V**arying **W**iretap **C**hannel [17])**.** A CAVWC is a channel, which is compound from transmitter to the legitimate receiver, but which is arbitrarily varying from transmitter to the eavesdropper. Hence, we describe a CAVWC by $(\overline{\mathcal{W}},\mathcal{V})$ where $\overline{\mathcal{W}} = \{W_q : q\in\mathcal{P}(\mathcal{S})\}$ and for every $q\in\mathcal{P}(\mathcal{S})$, $W_q(y|s) := \sum_{s\in\mathcal{S}} q(s)W(y|s,x)$ and $\mathcal{V} := \{V(Z|X,s) : s\in\mathcal{S}\}$. The probability of receiving the sequences y^n and z^n when x^n is sent and the jammer's choice is s^n is

$$\overline{W}^n(y^n|s^n,x^n) = \prod_{i=1}^n W_q(y_i|x_i), \text{where } q(s) := \tfrac{1}{n}N(s|s^n),$$
$$V^n(z^n|x^n,s^n) = \prod_{i=1}^n V(z_i|x_i,s_i).$$

This channel model will be used to derive the common randomness assisted secrecy capacity for the AVWC with constraints and is a tool for the proof.

Remark 2. Note that we do also include the case of different state spaces for the channels $\overline{\mathcal{W}}$ and $\mathcal{V}$, since one could define the state space $\mathcal{S} : \mathcal{S}_1\times\mathcal{S}_2$ such that $s = (s_1,s_2)$.

Definition 9 (Deterministic Wiretap-Codes for the CAVWC [17])**.** The difference to the definition before is that the channel to the legitimate receiver is compound. Hence, the average error probability changes to

$$\bar{e}_s(\mathcal{K}_n) := \max_{s\in\mathcal{S}} \frac{1}{J_n}\sum_{j=1}^{J_n} \sum_{x^n\in\mathcal{X}^n} E(x^n|j)W_s^n(\mathcal{D}_j^c|x^n)$$
$$= \max_{s\in\mathcal{S}} \frac{1}{J_n}\sum_{j=1}^{J_n} EW_s^n(\mathcal{D}_j^c|j).$$

Definition 10 (Achievable Deterministic Secrecy Rate and Deterministic Secrecy Capacity for the CAVWC [17])**.** A nonnegative number R_S is called an achievable deterministic secrecy rate for the CAVWC if there exists a sequence $(\mathcal{K}_n)_{n=1}^\infty$ of (n,J_n) deterministic wiretap-codes, such that the following requirements are fulfilled

$$\liminf_{n\to\infty} \frac{1}{n}\log J_n \geq R_S, \quad (10)$$
$$\lim_{n\to\infty} \bar{e}_s(\mathcal{K}_n) = 0, \quad (11)$$
$$\lim_{n\to\infty} \max_{s^n\in\mathcal{L}_n} I(p_{J_n};EV_{s^n}^n) = 0. \quad (12)$$

The supremum of all achievable deterministic secrecy rates for the CAVWC is called the deterministic secrecy capacity of the CAVWC $(\overline{\mathcal{W}},\mathcal{V})$ and is denoted by $C_S(\overline{\mathcal{W}},\mathcal{V})$.

Remark 3 (From Compound to Arbitrary, [17]). Later, we will use a modified version of Ahlswede's RT [3], [2] to obtain a random coding theorem for the AVWC from a deterministic wiretap-coding theorem for the CAVWC. For this we need an exponential decrease in the error probability as the blocklength goes to infinity. Furthermore, we define for a permutation $\pi\in\Pi_n$, where Π_n denotes the symmetric group of permutations of $\{1,2,...,n\}$ the stochastic encoder E^π obtained from a stochastic encoder E as

$$E^\pi(x^n|j) := E(\pi^{-1}(x^n)|j).$$

Definition 11 (Enhanced Achievable Deterministic Wiretap–Code Secrecy Rate and Enhanced Deterministic Wiretap-Code Secrecy Capacity for the CAVWC [17])**.** A nonnegative number R_S is called an enhanced achievable deterministic secrecy rate for the CAVWC if there exists a sequence $(\mathcal{K}_n)_{n=1}^\infty$ of (n,J_n) deterministic wiretap-codes and a $\beta>0$, such that the following requirements are fulfilled

$$\liminf_{n\to\infty} \frac{1}{n}\log J_n \geq R_S, \quad (13)$$
$$\limsup_{n\to\infty} -\frac{1}{n}\log \bar{e}_s(\mathcal{K}_n) \leq \beta, \quad (14)$$
$$\lim_{n\to\infty} \max_{s^n\in\mathcal{L}_n} \max_{\pi\in\Pi_n} I(p_{J_n};E^\pi V_{s^n}^n) = 0. \quad (15)$$

The supremum of all enhanced achievable deterministic secrecy rates for the CAVWC is called the enhanced deterministic secrecy capacity of the CAVWC $(\overline{\mathcal{W}},\mathcal{V})$ and is denoted by $\widehat{C}_S(\overline{\mathcal{W}},\mathcal{V})$.

The proof works as follows. First, the achievability for the CAVWC is shown. This is done by the consideration of three sub parts: The secrecy part, the existence of sufficiently many confusing messages and the reliability part. Fix a blocklength n and a probability distribution

$$p \in \widetilde{\mathcal{G}} := \left\{ p \in \mathcal{P}(\mathcal{X}) : \sum_x p(x) g_{lo}(x) \geq \Lambda_{lo} + \epsilon_0, \right. \\ \left. \sum_x p(x) g_{up}(x) \leq \Lambda_{up} - \epsilon_0 \right\}.$$

For sufficiently large n and sufficiently small δ_0 all sequences $x^n \in \mathcal{T}^n_{p,\delta_0}$ fulfill the input constraints. We randomly draw a family of input words $\mathfrak{X} := \{X_{jl} : j \in \mathcal{J}_n,\ l \in \mathcal{L}_n^*\}$ according to p^n and let $\mathcal{J}_n := \{1, 2, ..., J_n\}$ and $\mathcal{L}_n^* := \{1, 2, ..., L_n\}$. For an arbitrary, but positive τ_1, let

$$J_n := \left\lfloor \exp\left\{ n \left(\min_{t \in \mathcal{P}(\mathcal{S})} I(p; W_t) - \max_{q \in \mathcal{P}(\mathcal{S})} I(p; V_q) - \tau_1 \right) \right\} \right\rfloor$$

$$L_n := \left\lfloor \exp\left\{ n \left(\max_{q \in \mathcal{P}(\mathcal{S})} I(p; V_q) + \frac{\tau_1}{4} \right) \right\} \right\rfloor$$

To show that the secrecy requirements are fulfilled, we modify the channel in a certain way, use the triangle inequality in combination with the total variational distance and the connection to the difference of entropies and will show later that the modifications do not change the statements for the original channel. Then, as in [17], we have to show that the joint type of most codewords with a given $s^n \in \mathcal{L}_n$ is a product type. We prove the reliability for a finite subset of all possible channels. Then we use an the Approximation Lemma from **B**reiman, **B**lackwell and **T**homasian (BBT) [7] to show that codes with exponential error bounds on this subset of channels are also applicable codes for the infinite set of channels. Then we show that the probability that a code simultaneously fulfills the three parts (secrecy requirement, existence of sufficiently many confusing messages, reliability) is close to one. Additionally, we show that by prefixing a channel $Q \to \widetilde{\mathcal{G}}$ the achievable rate is increased. Having shown the achievability for the CAVWC, we can now derive an achievable secrecy rate for the AVWC using the following lemma.

Lemma 1 (Modification of Ahlswede's RT [3])**.** *If there exists a function $f : \mathcal{L}_n \to [0, 1]$ satisfying*

$$\sum_{s^n \in \mathcal{S}^n} f(s^n) q(s_1) q(s_2) ... q(s_n) \geq 1 - \epsilon, \quad \forall q \in \widetilde{\mathcal{L}}_n \tag{16}$$

$$\textit{then} \quad \frac{1}{n!} \sum_{\pi \in \Pi_n} f(\pi(s^n)) \geq 1 - \epsilon', \quad \forall s^n \in \mathcal{L}_n \tag{17}$$

$$\epsilon' = (n+1)^{|\mathcal{S}|} \epsilon. \tag{18}$$

Proof. We follow [3] and start with a q fulfilling (16).

$$\epsilon \geq 1 - \sum_{s^n \in \mathcal{S}^n} f(s^n) q^n(s^n) = 1 - \sum_{s^n \in \mathcal{S}^n} f(\pi(s^n)) q^n(s^n)$$

$$\geq \sum_{s^n \in \mathcal{L}_n} (1 - f(\pi(s^n))) q^n(s^n)$$

$$\geq \sum_{\substack{s^n \in \mathcal{L}_n: \\ s^n \in \mathcal{T}_q^n}} \left(1 - \frac{1}{n!} \sum_{\pi \in \Pi_n} f(\pi(s^n)) \right) q^n(s^n),$$

where we take the sum of all $s^n \in \mathcal{L}_n$ having the same type.

$$\epsilon \geq \left(1 - \frac{1}{n!} \sum_{\pi \in \Pi_n} f(\pi(s^n)) \right) q(\mathcal{T}_q^n)$$

$$\left(\frac{1}{n!} \sum_{\pi \in \Pi_n} f(\pi(s^n)) \right) \geq 1 - (n+1)^{|\mathcal{S}|} \epsilon, \ \forall s^n \in \mathcal{L}_n,$$

where the last step follows from the fact that $q(\mathcal{T}_q^n) geq \frac{1}{(n+1)^{|\mathcal{S}|}}$. □

For the converse, we follow the approach of [17].

VI. Discussion

We gave a multi letter expression for the common randomness assisted secrecy capacity of an AVWC with input and state constraints. We have seen that the proof technique of [17] is applicable with some changes and adaptations. Nevertheless, we have to be careful when proving the existence and convergence of the limit of the multi letter expression. Ensuring that the constraints are fulfilled for the whole interval we have to start with sub intervals fulfilling the constraints, separately. Otherwise, we cannot guarantee that the constraints still hold. Next steps would be the consideration of deterministic wiretap codes for the AVWC with input and state constraints and a formula for the corresponding deterministic wiretap code secrecy capacity. Here, we have to consider a phenomenon called symmetrizability. Roughly speaking, if a channel is symmetrizable, then a valid channel output can be emulated by a malevolent attacker. In contrast to the case without input and state constraints, the symmetrizability condition is not sufficient to render the deterministic code capacity of an AVC zero. So, we can consider common randomness as a network resource to overcome not only a possible symmetrizable attack of a malevolent attacker, but also to achieve higher secrecy capacities than by using deterministic wiretap codes. Even though the proof techniques by Ahlswede do not hold in the case of constraints and in general different results may occur, we expect a similar behavior according to the symmetrizability and deterministic wiretap code secrecy rates for the AVWC with constraints. Hence, we expect that the symmetrizability condition is not sufficient in the case of a constrained AVWC, as well. We believe, that an attacker has to spend costs on symmetrizing the channel. These might be influenced by the input distribution chosen at the channel input. If the costs are too high then the attacker cannot symmetrize the channel. But the achievable deterministic wiretap code secrecy rate might even be strictly smaller than or equal to the common randomness assisted secrecy capacity, even if it is positive, in contrast to the case without constraints, where the dichotomous

behavior applies, since the input distributions to achieve the common randomness assisted secrecy capacity and to render the channel not symmetrizable may be different. In this aspect, we see again that the presence of common randomness at the legitimate communication partners not only is a countermeasure against attacks, but also provide higher secrecy capacities. Additionally, we immediately see the difference to the AVC with constraints but without secrecy requirements. If no secrecy requirements are imposed on the system, it is easy to show the existence and the convergence of the limit of the capacity for infinite blocklengths by using Fekete's lemma. If the inequality

$$a_{k_1} + a_{k_2} \leq a_{k_1+k_2}$$

holds for every $k_1, k_2 \in \mathbb{N}$, then the limit of $\lim_{k\to\infty} \frac{1}{k} a_k$ exists and can be expressed as

$$\lim_{k\to\infty} \frac{1}{k} a_k = \sup_{k\in\mathbb{N}} \frac{a_k}{k}.$$

The product structure property of the state spaces is lost when imposing constraints on the system. This does not affect the mutual information term to the legitimate communication partner Bob (and that is the reason why the results of [5] hold). Unfortunately, this property is crucial when considering the information leakage to the eavesdropper. When starting with a_{k_1} and a_{k_2} with sequences s^{k_1} and s^{k_2}, both fulfilling the constraints, it follows that for an $a_{k_1+k_2}$ the sequence $s^{k_1+k_2}$ fulfills the constraints, too. The converse does not hold! Hence, we can not upper bound the sum of two a_{k_1} and a_{k_2} with sequences s^{k_1} and s^{k_2} by $a_{k_1+k_2}$ with sequence $s^{k_1+k_2}$, since the set $\mathcal{L}_{k_1+k_2}$ is larger than the product set of $\mathcal{L}_{k_1}$ and $\mathcal{L}_{k_2}$ and contains more elements (those elements, fulfilling the constraints on the blocklength $k_1 + k_2$ but not necessarily on the sub intervals k_1 or k_2). So while without constraints the inequality

$$\begin{aligned}&\max_{s^{k_1}\in\mathcal{S}^{k_1}} \left[I(Q; Z^{k_1}_{s^{k_1}})\right] + \max_{s^{k_2}\in\mathcal{S}^{k_2}} \left[I(Q; Z^{k_2}_{s^{k_2}})\right] \\ &\geq \max_{s^{k_1+k_2}\in\mathcal{S}^{k_1+k_2}} \left[I(Q; Z^{k_1+k_2}_{s^{k_1+k_2}})\right]\end{aligned}$$

holds, we can not conclude the same for the case when constraints are imposed. So the inequality

$$\begin{aligned}&\max_{s^{k_1}\in\mathcal{L}_{k_1}} \left[I(Q; Z^{k_1}_{s^{k_1}})\right] + \max_{s^{k_2}\in\mathcal{L}_{k_2}} \left[I(Q; Z^{k_2}_{s^{k_2}})\right] \\ &\geq \max_{s^{k_1+k_2}\in\mathcal{L}_{k_1+k_2}} \left[I(Q; Z^{k_1+k_2}_{s^{k_1+k_2}})\right]\end{aligned}$$

does not necessarily hold in general. Thus, we here encounter a whole new problem while considering constraints and secrecy requirements at the same time. Our tools are quite strong to prove the achievability part of Theorem 1. The converse is causing problems, such that we can only give a pessimistic formula for the common randomness assisted secrecy capacity. Thus, it has to be mentioned that our result is strictly weaker than the results of [5], where no secrecy requirements are imposed. It still has to be shown that the limit of the right hand side of (9) exists and converges. Although we provide a multi letter description of the common randomness assisted secrecy capacity of an AVWC with input and state constraints, only, we can formulate statements about crucial properties of the AVWC such as the continuity or super additivity. Thus, we provide a useful result which has to be adapted to the case of deterministic wiretap codes. In future work, the joint encoding over parallel AVWCs with input and state constraints will be investigated. Recently, a phenomenon **S**uper-**A**ctivation has been proven to occur for parallel AVWCs. This is an even stronger effect than the violation of additivity of the zero-error capacity (Shannon conjectured additivity to hold in 1956, the statement was disproven by Alon in 1998): joint encoding on two parallel AVWCs which each have zero deterministic secrecy capacity alone might provide a secrecy capacity strictly larger than zero.

REFERENCES

[1] R. Ahlswede, "The capacity of a channel with arbitrarily varying additive Gaussian channel probability functions," in *Sixth Prague Conf. on Inf. Th., Stat. Dec. Fct's and Rand. Proc.*, House Czechosl. Academy of Sc, 1971.

[2] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, vol. 44, pp. 159–175, 1978.

[3] R. Ahlswede, "Arbitrarily varying channels with states sequence known to the sender," *IEEE Transactions on Information Theory*, vol. 32, no. 5, pp. 621–629, 1986.

[4] I. Csiszár and P. Narayan, "Arbitrarily varying channels with constrained inputs and states.," *IEEE Transactions on Information Theory*, vol. 34, no. 1, pp. 27–34, 1988.

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

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

[7] D. Blackwell, L. Breiman, and A. J. Thomasian, "The capacity of a class of channels," *Ann. Math. Statist.*, vol. 30, pp. 1229–1241, 12 1959.

[8] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Trans. Inform. Theory*, vol. 44, no. 6, pp. 2148–2177, 1998.

[9] C. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, Oct. 1948.

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

[11] L. Y. Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, pp. 451–456, 1978.

[12] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, pp. 339–348, May 1978.

[13] I. Bjelaković, H. Boche, and J. Sommerfeld, "Secrecy results for compound wiretap channels," *CoRR*, vol. abs/1106.2013, 2011.

[14] I. Bjelaković, H. Boche, and J. Sommerfeld, "Capacity results for arbitrarily varying wiretap channels," *CoRR*, vol. abs/1209.5213, 2012.

[15] H. Boche and R. F. Schaefer, "Capacity results, coordination resources, and super-activation in wiretap channels," in *IEEE International Symposium on Information Theory Proceedings (ISIT)*, pp. 1342–1346, 2013.

[16] E. MolavianJazi, M. Bloch, and J. Laneman, "Arbitrary jamming can preclude secure communication," in *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, pp. 1069–1075, Sept 2009.

[17] M. Wiese, J. Nötzel, and H. Boche, "The arbitrarily varying wiretap channel - deterministic and correlated random coding capacities under the strong secrecy criterion," *CoRR*, vol. abs/1410.8078, p. 37, 2014.