On Arbitrarily Varying Wiretap Channels for Different Classes of Secrecy Measures

Holger Boche
Lehrstuhl für Theoretische Informationstechnik
Technische Universität München
80290 München, Germany

Rafael F. Schaefer and H. Vincent Poor
Department of Electrical Engineering
Princeton University
Princeton, NJ 08544, USA

***Abstract*—The wiretap channel models secure communication in the presence of an eavesdropper who must be kept ignorant of transmitted messages. In this paper, the *arbitrarily varying wiretap channel (AVWC)*, in which the channel may vary in an unknown and arbitrary manner from channel use to channel use, is considered. For arbitrarily varying channels (AVCs) the capacity might differ depending on whether deterministic or *common randomness (CR)* assisted codes are used. The AVWC has been studied for both coding strategies and the relation between the corresponding secrecy capacities has been established. However, a characterization of the CR-assisted secrecy capacity itself or even a general CR-assisted achievable secrecy rate remain open in general for weak and strong secrecy. Here, the secrecy measure of high decoding error at the eavesdropper is considered, where the eavesdropper is further assumed to know channel states and to adapt its decoding strategy accordingly. For this secrecy measure a general CR-assisted achievable secrecy rate is established. The relation between secrecy capacities for different secrecy measures is discussed: The weak and strong secrecy capacities are smaller than or equal to the one for high decoding error. It is conjectured that this relation can be strict for certain channels.**

I. Introduction

Nowadays, physical layer or information theoretic approaches to security are intensively discussed as a complement to current cryptographic techniques [1, 2]. Physical layer security was initiated by Wyner, who introduced the *wiretap channel* [3]. It models the simplest scenario of secure communication between a transmitter and receiver in the presence of an eavesdropper (Eve) to be kept ignorant. The wiretap channel has been investigated under different secrecy measures including *weak secrecy* [1–3], *strong secrecy* [4–6], and *probability of decoding error at the eavesdropper* [7].

These studies have in common that all channels are assumed to be known and fixed during the entire duration of transmission. The concept of compound channels weakens the first assumption to imperfect channel information and the corresponding *compound wiretap channel* is studied in [8, 9]. In this paper, we further weaken the second assumption and consider channels that may vary in an arbitrary and unknown manner from channel use to channel use. Such conditions appear for example in fast fading environments but also in situations with malicious eavesdroppers that jam the legitimate transmission. This can be perfectly modeled with the concept of *arbitrarily varying channels (AVCs)* [10–12]. Accordingly, the communication problem at hand is the *arbitrarily varying wiretap channel (AVWC)* which is introduced in Section II.

In the context of AVCs, the capacity might differ depending on whether traditional (deterministic) codes or *common randomness (CR)* assisted codes are used [10–13]. This is in contrast to the case of perfect channel state information or the compound channel for which the capacities are the same for traditional and CR-assisted codes. The corresponding AVWC is studied for traditional and CR-assisted strategies in [14, 15]. The latter establishes a complete characterization of the relation between the traditional and CR-assisted secrecy capacity for the strong secrecy criterion. However, a characterization of the CR-assisted secrecy capacity itself remains an problem.

The classical approach to determining the CR-assisted capacity of an AVC is based on Ahlswede's *robustification technique* [16] which connects the AVC with a suitable compound channel. This provides an elegant way of making the corresponding compound results and techniques applicable to the AVC as well. Unfortunately, this approach breaks down for AVWCs as the common measures of weak and strong secrecy do not satisfy the required convexity and boundedness properties. Thus, even a general (meaning without any further assumptions on the channel) CR-assisted achievable secrecy rate is missing. This is discussed in Section III.

Motivated by this crucial observation, in this paper we look at other secrecy measures as well. In particular, we consider the criterion of decoding error, where we require the eavesdropper to have high probability of decoding error regardless of the applied decoding strategy or available computational resources. In addition, to be on the safe side from a secrecy perspective, we assume the eavesdropper to know the channel perfectly so that it can adapt its decoding strategy accordingly. It turns out that we are able to extend Ahlswede's robustification technique to work for this meaningful secrecy measure. As a result, a CR-assisted achievable secrecy rate for the AVWC is derived in Section IV. To the best of our knowledge, this is the first CR-assisted achievable secrecy

This work of H. Boche was supported by the German Research Foundation (DFG) under Grant BO 1734/33-1. This work of Rafael F. Schaefer was supported by the German Research Foundation (DFG) under Grant WY 151/2-1. This work of H. Vincent Poor was supported in part by the National Science Foundation Grant CCF-1016671, and in part by the Marie Curie Outgoing Fellowship Program under Award No. FP7-PEOPLE-IOF-2011-298532.

978-1-4799-5186-4/14/$31.00 ©2014 IEEE

rate that holds for the general case, i.e., without any further restrictions on the channel as in [14, 15].

The relation between secrecy capacities for different secrecy measures is discussed in Section V. It is shown that the weak and strong secrecy criteria yield a secrecy capacity that is smaller than or equal to the one for high decoding error.[1]

II. Arbitrarily Varying Wiretap Channels

Let $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ be finite input and output sets and $\mathcal{S}$ be a finite state set. For a fixed state sequence $s^n \in \mathcal{S}^n$ of length n, the discrete memoryless channel to the legitimate receiver is described by the transition probabilities $W^n_{s^n}(y^n|x^n) = W^n(y^n|x^n, s^n) := \prod_{i=1}^n W(y_i|x_i, s_i)$ for all $x^n \in \mathcal{X}^n$ and $y^n \in \mathcal{Y}^n$. Then the family of channels for all $s^n \in \mathcal{S}^n$ defines the AVC $\mathcal{W}$ as

$$\mathcal{W} := \big\{W^n_{s^n} : s^n \in \mathcal{S}^n\big\}. \tag{1}$$

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

$$W_q(y|x) = \sum_{s\in\mathcal{S}} q(s)W(y|x, s). \tag{2}$$

Accordingly, for $s^n \in \mathcal{S}^n$ we define the discrete memoryless channel to the eavesdropper by the transition probabilities $V^n_{s^n}(z^n|x^n) = V^n(z^n|x^n, s^n) := \prod_{i=1}^n V(z_i|x_i, s_i)$ for all $x^n \in \mathcal{X}^n$ and $z^n \in \mathcal{Z}^n$, and, further, $\mathcal{V} := \{V^n_{s^n} : s^n \in \mathcal{S}^n\}$ and $V_q(z|x) = \sum_{s\in\mathcal{S}} q(s)V(z|x, s)$ for $q \in \mathcal{P}(\mathcal{S})$.

Definition 1. The AVWC $\mathfrak{W}$ is the family of pairs of channels with common input as

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

A. Traditional Wiretap Codes

Definition 2. An (n, J_n)*-code* $\mathcal{C}$ consists of a stochastic encoder

$$E : \mathcal{J}_n \to \mathcal{P}(\mathcal{X}^n) \tag{3}$$

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

$$\big\{\mathcal{D}_j \subset \mathcal{Y}^n : j \in \mathcal{J}_n\big\}. \tag{4}$$

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

$$\bar{e}_n(s^n|\mathcal{C}) := \frac{1}{|\mathcal{J}_n|} \sum_{j\in\mathcal{J}_n} \sum_{x^n\in\mathcal{X}^n} W^n_{s^n}(\mathcal{D}^c_j|x^n)E(x^n|j).$$

The most common approach to ensure the confidentiality of the message is given by an information theoretic measure as

$$\max_{s^n\in\mathcal{S}^n} I(J; Z^n_{s^n}|\mathcal{C}) \le \delta_n \tag{5}$$

for $\delta_n > 0$ with J the random variable uniformly distributed over the set of messages $\mathcal{J}_n$ and $Z^n_{s^n} = (Z_{s_1}, ..., Z_{s_n})$ the channel output at the eavesdropper for $s^n \in \mathcal{S}^n$. This condition is termed *strong secrecy* [4, 5] and the motivation is to control the total amount of information leaked to the eavesdropper.

Definition 3. A rate $R_S > 0$ is an *achievable secrecy rate* for the AVWC $\mathfrak{W}$ if for all $\tau > 0$ there is an $n(\tau) \in \mathbb{N}$ and a sequence of (n, J_n)-codes $\mathcal{C}$ such that for all $n \ge n(\tau)$ we have $\frac{1}{n}\log J_n \ge R_S - \tau$, $\max_{s^n\in\mathcal{S}^n} \bar{e}_n(s^n|\mathcal{C}) \le \lambda_n$, and $\max_{s^n\in\mathcal{S}^n} I(J; Z^n_{s^n}|\mathcal{C}) \le \delta_n$ while $\lambda_n, \delta_n \to 0$ as $n \to \infty$. The *secrecy capacity* C_S is given by the supremum of all achievable secrecy rates R_S.

Such traditional approaches as given in Definition 2 do not suffice to establish reliable communication over *symmetrizable* AVCs; in fact, in this case the corresponding capacity is zero [11, 15, 17]. This necessitates the use of more sophisticated strategies based on *common randomness (CR)*.

B. CR-Assisted Communication

CR is modeled by a random variable $\mathit{\Gamma}$ taking values in $\mathcal{G}_n$ according to the distribution $P_\mathit{\Gamma} \in \mathcal{P}(\mathcal{G}_n)$. It allows the transmitter and legitimate receiver to coordinate their choice of encoder (3) and decoder (4) according to $\gamma \in \mathcal{G}_n$.

Definition 4. A *CR-assisted* $(n, J_n, \mathcal{G}_n, P_\mathit{\Gamma})$*-code* $\mathcal{C}_{\text{CR}}$ is given by a family of (traditional) codes

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

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

Then the mean average probability of error for $s^n \in \mathcal{S}^n$ is given by $\bar{e}_{\text{CR},n}(s^n|\mathcal{C}_{\text{CR}}) = \mathbb{E}_\mathit{\Gamma}[\bar{e}_n(s^n|\mathcal{C}(\mathit{\Gamma}))]$, i.e.,

$$\bar{e}_{\text{CR},n}(s^n|\mathcal{C}_{\text{CR}}) := \frac{1}{|\mathcal{J}_n|} \sum_{j\in\mathcal{J}_n} \sum_{\gamma\in\mathcal{G}_n} \sum_{x^n\in\mathcal{X}^n} \times W^n_{s^n}(\mathcal{D}^c_{\gamma,j}|x^n)E_\gamma(x^n|j)P_\mathit{\Gamma}(\gamma). \tag{6}$$

With $I(J; Z^n_{s^n}|\mathcal{C}_{\text{CR}}) = \mathbb{E}_\mathit{\Gamma}[I(J; Z^n_{s^n}|\mathcal{C}(\mathit{\Gamma}))]$ the strong secrecy criterion (5) becomes

$$\max_{s^n\in\mathcal{S}^n} \sum_{\gamma\in\mathcal{G}_n} I(J; Z^n_{s^n}|\mathcal{C}(\gamma))P_\mathit{\Gamma}(\gamma) \le \delta_n.$$

The definitions of a *CR-assisted achievable secrecy rate* and the *CR-assisted secrecy capacity* $C_{S,\text{CR}}$ follow accordingly.

C. Capacity Results

First studies aiming to understand the secrecy capacity of the AVWC appeared in [14, 15, 17] with the latter using the strong secrecy criterion. In particular, the relation between the secrecy capacities for traditional and CR-assisted coding strategies has been completely characterized in [15].

Theorem 1 ([15]). If the CR-assisted secrecy capacity satisfies $C_{S,CR} > 0$, then the secrecy capacity is given by

$$C_S = C_{S,CR}$$

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

[1] *Notation:* $\mathcal{P}(\cdot)$ is the set of all probability distributions; $\|P_1 - P_2\|$ is the total variation distance of probability distributions P_1 and P_2; P_1P_2 is the product distribution defined by the product marginal distributions P_1 and P_2.

Although the secrecy capacity C_S of the AVWC $\mathfrak{W}$ is completely known in terms of its CR-assisted secrecy capacity $C_{S,\text{CR}}$, a characterization of $C_{S,\text{CR}}$ itself remains open.

Only for the special case of a best channel to the eavesdropper is an achievable secrecy rate known. A channel $V_{q^*} \in \{V_q : q \in \mathcal{P}(\mathcal{S})\}$ such that all other channels from this set are degraded versions of V_{q^*} is called *best channel* to the eavesdropper, i.e., V_{q^*} is a best channel if

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

holds with Z_q the random variable associated with the output of the averaged channel V_q, $q \in \mathcal{P}(\mathcal{S})$.

Theorem 2 ([15]). If there exists a best channel to the eavesdropper, an achievable secrecy rate R_S for the AVWC $\mathfrak{W}$ is

$$R_S = \max_X \Big(\min_{q\in\mathcal{P}(\mathcal{S})} I(X;Y_q) - \max_{q\in\mathcal{P}(\mathcal{S})} I(X;Z_q) \Big)$$

with Y_q and Z_q the random variables associated with the outputs of the averaged channels W_q and V_q, $q \in \mathcal{P}(\mathcal{S})$.

III. Revisiting Ahlswede's Approach To AVCs

In this section we want to revisit the classical approach of Ahlswede to the CR-assisted capacity of an AVC [11, 16]. Understanding how the CR-assisted capacity is established for the classical AVC yields important insights into why it is so difficult to obtain similar results for the AVWC. In particular, it becomes clear why an achievable secrecy rate is known only for the special case of a best channel to the eavesdropper.

The crucial idea of Ahlswede is to exploit the connection between the AVC $\mathcal{W} = \{W^n_{s^n} : s^n \in \mathcal{S}^n\}$, cf. (1), and a suitable compound channel $\overline{\mathcal{W}} = \{W_q : q \in \mathcal{P}(\mathcal{S})\}$ with $W_q(y|x) = \sum_{s\in\mathcal{S}} q(s)W(y|x,s)$, cf. (2).

For the compound channel $\overline{\mathcal{W}}$ we know from [12] that for every rate $R < \max_X \min_{q\in\mathcal{P}(\mathcal{S})} I(X;Y_q)$ there exists a (deterministic) code $\overline{\mathcal{C}}$ with codewords $x^n_j \in \mathcal{X}^n$ and decoding sets $\mathcal{D}_j \subset \mathcal{Y}^n$, $j \in \mathcal{J}_n$ such that the average probability of decoding error satisfies

$$\bar{e}_n(q|\overline{\mathcal{C}}) = \frac{1}{|\mathcal{J}_n|} \sum_{j\in\mathcal{J}_n} W_q(\mathcal{D}^c_j|x^n_j) \le e^{-n\epsilon'} \qquad (7)$$

for all $q \in \mathcal{P}(\mathcal{S})$ with $\epsilon' > 0$ a constant depending only on the rate R. This (deterministic) code $\overline{\mathcal{C}}$ for the compound channel $\overline{\mathcal{W}}$ is then used to obtain a CR-assisted code $\mathcal{C}_{\text{CR}}$ for the AVC $\mathcal{W}$. The crucial idea to achieve this is the so-called *robustification technique* [16].

Lemma 1 (Robustification technique [16]). Let $f_n : \mathcal{S}^n \to [0,1]$ be a function such that for some $\alpha \in (0,1)$ the inequality

$$\sum_{s^n\in\mathcal{S}^n} q^n(s^n) f_n(s^n) > 1 - \alpha \qquad \text{for all } q \in \mathcal{P}_0(n,\mathcal{S})$$

is satisfied. Here, $\mathcal{P}_0(n,\mathcal{S})$ is the set of probability distributions on $\mathcal{S}$ with $q(s) = \frac{n_s}{n}$, n_s integral, for all $s \in \mathcal{S}$, i.e., q is a type [12]. Then the inequality

$$\frac{1}{n!} \sum_{\pi\in\Pi_n} f_n(\pi(s^n)) > 1 - (n+1)^{|\mathcal{S}|}\alpha \qquad \text{for all } s^n \in \mathcal{S}^n$$

is also satisfied, where $\Pi_n : \{1,...,n\} \to \{1,...,n\}$ is the set of all n-permutations.

In fact, rewriting the average probability of error in (7) in terms of probability of successful transmission and using the definition of the average channel (2) results in

$$\sum_{s^n\in\mathcal{S}^n} q^n(s^n) \underbrace{\frac{1}{|\mathcal{J}_n|} \sum_{j\in\mathcal{J}_n} W^n_{s^n}(\mathcal{D}_j|x^n_j)}_{=: f_n(\pi(s^n))} > 1 - e^{-n\epsilon'} \qquad (8)$$

for all $q^n = \prod_{i=1}^n q$ and $q \in \mathcal{P}(\mathcal{S})$. Then with π being the identity map, Lemma 1 immediately yields

$$\frac{1}{n!} \sum_{\pi\in\Pi_n} \frac{1}{|\mathcal{J}_n|} \sum_{j\in\mathcal{J}_n} W^n_{\pi(s^n)}(\mathcal{D}_j|x^n_j) > 1 - (n+1)^{|\mathcal{S}|} e^{-n\epsilon'} \qquad (9)$$

for all $s^n \in \mathcal{S}^n$. Finally, by rewriting $W^n_{\pi(s^n)}(\mathcal{D}_j|x^n_j) = W^n_{s^n}(\pi^{-1}(\mathcal{D}_j)|\pi^{-1}(x^n_j))$, we obtain a CR-assisted (n, J_n, Π_n, μ)-code $\mathcal{C}_{\text{CR}}$ for the AVC $\mathcal{W}$ with codewords $\pi^{-1}(x^n_j)$, decoding sets $\pi^{-1}(\mathcal{D}_j)$, $j \in \mathcal{J}_n$, $\pi \in \Pi_n$, and μ the uniform distribution on Π_n.

Summarizing, a "good" code $\overline{\mathcal{C}}$ for the compound channel $\overline{\mathcal{W}}$ is used to construct a CR-assisted code $\mathcal{C}_{\text{CR}}$ that is also "good" for the corresponding AVC $\mathcal{W}$ in the sense that it achieves the same rate with an average probability of error that decreases exponentially fast, cf. (9). Thus, the crucial idea of Ahlswede's approach is to make achievability results for the compound channel applicable to the corresponding AVC setup and therewith establish achievability results for AVCs.

Although the robustification technique is a very elegant way to prove achievability results for AVCs, it is, at the same time, the reason why this approach breaks down for AVWCs. The key observation is the following: To make the robustification technique work, the function $f_n(s^n)$ in Lemma 1 has to be convex and bounded which is satisfied for the applied criterion of successful transmission in (8). If secrecy enters the picture, the robustification technique must be applied to the secrecy criterion (5) as well. Unfortunately, the required convexity is no longer fulfilled which prohibits the application of Lemma 1 for this secrecy criterion. Thus, general achievability results for the AVWC are missing. Only for the special case of a best channel to the eavesdropper, it was possible to overcome this problem [15]. See also Section V for further discussions.

IV. Secrecy Measure of Decoding Error at Eve

The previous discussion motivates us to look at other measures of secrecy as well. A meaningful and more signal processing inspired approach is to require the eavesdropper to have its average probability of decoding error high (i.e. close to 1) regardless of its computational capabilities or the decoding strategy it applies.

Further, we make worst case assumptions to be on the safe side from a security perspective. This means that we assume the eavesdropper to know the actual state sequence $s^n \in \mathcal{S}^n$. Then it can adapt its decoding sets

$$\{\widetilde{\mathcal{D}}_{s^n,j} \subset \mathcal{Z}^n : j \in \mathcal{J}_n\}$$

accordingly. We consider the case in which the legitimate users use a CR-assisted (n, J_n, Π_n, μ)-code $\mathcal{C}_{\text{CR}}$ as introduced and discussed in the previous Section III. Then for $s^n \in \mathcal{S}^n$ and $\pi \in \Pi_n$, the average probability of decoding error of the eavesdropper is

$$\bar{e}_{\text{Eve},n}(s^n, \{\widetilde{\mathcal{D}}_{s^n,j}\}|\mathcal{C}_{\text{CR}}) := \frac{1}{|\mathcal{J}_n|}\sum_{j\in\mathcal{J}_n}\frac{1}{n!}\sum_{\pi\in\Pi_n}\sum_{x^n\in\mathcal{X}^n} \times V_{s^n}^n\big(\pi^{-1}(\widetilde{\mathcal{D}}_{s^n,j}^c)|x^n\big)E_\pi(x^n|j)$$

with $E_\pi(x^n|j) = E(\pi(x^n)|j)$. Now, a rate $R_S > 0$ is a CR-assisted achievable secrecy rate if reliability is satisfied, i.e., (6) and (9), and we have high average decoding error at the eavesdropper, i.e.,

$$\min_{s^n\in\mathcal{S}^n}\min_{\{\widetilde{\mathcal{D}}_{s^n,j}\}} \bar{e}_{\text{Eve},n}(s^n, \{\widetilde{\mathcal{D}}_{s^n,j}\}|\mathcal{C}_{\text{CR}}) \geq 1 - \delta_n. \tag{10}$$

If we stick to the secrecy measure of average decoding error (10) instead of strong secrecy (5), we are able to get an achievable CR-assisted secrecy rate for the general case (instead of only for the best eavesdropper channel case).

Theorem 3. For the AVWC $\mathfrak{W}$, any rate $R_S > 0$ satisfying

$$R_S < \max_X\big(\min_{q\in\mathcal{P}(\mathcal{S})} I(X;Y_q) - \max_{q\in\mathcal{P}(\mathcal{S})} I(X;Z_q)\big)$$

is a CR-assisted achievable secrecy rate for secrecy measure of average decoding error approaching 1 exponentially fast.

Proof: In [9] the compound wiretap channel is studied, where the following is shown: Let

$$R_S < \max_X\big(\min_{q\in\mathcal{P}(\mathcal{S})} I(X;Y_q) - \max_{q\in\mathcal{P}(\mathcal{S})} I(X;Z_q)\big) \tag{11}$$

be arbitrary. Then there exists an $\epsilon \in (0,1)$ and an $n_0 = n_0(\epsilon)$ such that for all $n \geq n_0$ there exist as a compound code $\overline{\mathcal{C}}$ with a stochastic encoder $E : \mathcal{J}_n \to \mathcal{P}(\mathcal{X}^n)$ and a decoder $\varphi : \mathcal{Y}^n \to \mathcal{J}_n$ specified by disjoint decoding sets $\{\mathcal{D}_j\}_{j\in\mathcal{J}_n}$ with $\frac{1}{n}\log|\mathcal{J}_n| \geq R_S$,

$$\max_{q\in\mathcal{P}(\mathcal{S})}\frac{1}{|\mathcal{J}_n|}\sum_{j\in\mathcal{J}_n}\sum_{x^n\in\mathcal{X}^n} W_q^n(\mathcal{D}_j^c|x^n)E(x^n|j) \leq e^{-n\epsilon}, \tag{12}$$

and

$$\big\|P_{JV_q^n} - P_J P_{V_q^n}\big\| \leq e^{-n\epsilon}, \tag{13}$$

i.e., the actual joint distribution $P_{JV_q^n}$ of message J and channel V_q^n is close to its "independent" product distribution $P_J P_{V_q^n}$. Further, let $\psi : \mathcal{Z}^n \to \mathcal{J}_n$ be an arbitrary but fixed decoder at the eavesdropper specified by disjoint decoding sets $\{\widetilde{\mathcal{D}}_j\}_{j\in\mathcal{J}_n}$. Since (13) is satisfied, we have for the average decoding error $\bar{e}_{\text{Eve},n}(\{\widetilde{\mathcal{D}}_j\}|\overline{\mathcal{C}})$ at the eavesdropper

$$\begin{aligned}\bar{e}_{\text{Eve},n}(\{\widetilde{\mathcal{D}}_j\}|\overline{\mathcal{C}}) &:= \frac{1}{|\mathcal{J}_n|}\sum_{j\in\mathcal{J}_n}\sum_{x^n\in\mathcal{X}^n} V_q^n(\widetilde{\mathcal{D}}_j^c|x^n)E(x^n|j)\\ &\geq 1 - \frac{1}{|\mathcal{J}_n|} - e^{-n\epsilon} \geq 1 - e^{-n\frac{\epsilon}{2}}\end{aligned} \tag{14}$$

for all $q \in \mathcal{P}(\mathcal{S})$ and $n \geq n_1$ with n_1 sufficiently large, cf. [9, Section 2.2] for a proof and a detailed discussion. Thus, for any rate satisfying (11) the result in [9] guarantees the existence of a "good" code $\overline{\mathcal{C}}$ for the compound wiretap channel in the sense that the probabilities of error for the legitimate receiver and the eavesdropper simultaneously satisfy (12) and (14).

As argued in Section III, we want to use the robustification technique to convert this compound code $\overline{\mathcal{C}}$ to a "good" CR-assisted code $\mathcal{C}_{\text{CR}}$ for AVWC. Therefore, Lemma 1 must be applied to both the reliability criterion (12) and the secrecy criterion (14). Reliability (12) follows exactly as discussed in Section III, cf. also [15] in the AVWC context, and is omitted for brevity. The crucial secrecy part (14) is shown next.

In contrast to the strong secrecy criterion (5), the criterion of average decoding error (10) has the right properties of convexity and boundedness so that we can proceed as follows. We have

$$V_q^n(y^n|x^n) = \sum_{s^n\in\mathcal{S}^n} q^n(s^n)V_{s^n}^n(y^n|x^n)$$

so that we get for the average decoding error

$$\begin{aligned}&\frac{1}{|\mathcal{J}_n|}\sum_{j\in\mathcal{J}_n}\sum_{x^n\in\mathcal{X}^n} V_q^n(\widetilde{\mathcal{D}}_j^c|x^n)E(x^n|j)\\ &\quad= \sum_{s^n\in\mathcal{S}^n} q^n(s^n)\underbrace{\frac{1}{|\mathcal{J}_n|}\sum_{j\in\mathcal{J}_n}\sum_{x^n\in\mathcal{X}^n} V_{s^n}^n(\widetilde{\mathcal{D}}_j^c|x^n)E(x^n|j)}_{=:f_n(s^n,\{\widetilde{\mathcal{D}}_j\})}\\ &\quad= \sum_{s^n\in\mathcal{S}^n} q^n(s^n)f_n\big(s^n,\{\widetilde{\mathcal{D}}_j\}\big) \geq 1 - e^{-n\frac{\epsilon}{2}}.\end{aligned}$$

Thus, we are able to apply Ahlswede's robustification technique, cf. Lemma 1, to obtain for any fixed choice of decoding sets $\{\widetilde{\mathcal{D}}_j\}_{j\in\mathcal{J}_n}$ at the eavesdropper

$$\frac{1}{n!}\sum_{\pi\in\Pi_n} f_n\big(\pi(s^n),\{\widetilde{\mathcal{D}}_j\}\big) \geq 1 - (n+1)^{|\mathcal{S}|}e^{-n\frac{\epsilon}{2}} \tag{15}$$

which holds for all $s^n \in \mathcal{S}^n$ simultaneously. The following crucial observation is important: Although the function f_n depends on the particular choice of decoding sets $\{\widetilde{\mathcal{D}}_j\}_{j\in\mathcal{J}_n}$ of the eavesdropper, the right hand side of (15) is independent of $s^n \in \mathcal{S}^n$ and $\{\widetilde{\mathcal{D}}_j\}_{j\in\mathcal{J}_n}$. Thus, even if the eavesdropper knows the state sequence $s^n \in \mathcal{S}^n$ and if it chooses its decoding sets $\widetilde{\mathcal{D}}_{s^n,j} = \widetilde{\mathcal{D}}_j(s^n)$ dependent on that particular $s^n \in \mathcal{S}^n$, we still end up with

$$\frac{1}{n!}\sum_{\pi\in\Pi_n} f_n\big(\pi(s^n),\{\widetilde{\mathcal{D}}_{s^n,j}\}\big) \geq 1 - (n+1)^{|\mathcal{S}|}e^{-n\frac{\epsilon}{2}}. \tag{16}$$

Now, we observe that

$$\begin{aligned}&f_n\big(\pi(s^n),\{\widetilde{\mathcal{D}}_{s^n,j}\}\big)\\ &\quad= \frac{1}{|\mathcal{J}_n|}\sum_{j\in\mathcal{J}_n}\sum_{x^n\in\mathcal{X}^n} V_{\pi(s^n)}^n\big(\widetilde{\mathcal{D}}_{s^n,j}^c|x^n\big)E(x^n|j)\\ &\quad= \frac{1}{|\mathcal{J}_n|}\sum_{j\in\mathcal{J}_n}\sum_{x^n\in\mathcal{X}^n} V_{s^n}^n\big(\pi^{-1}(\widetilde{\mathcal{D}}_{s^n,j}^c)|\pi^{-1}(x^n)\big)E(x^n|j)\\ &\quad= \frac{1}{|\mathcal{J}_n|}\sum_{j\in\mathcal{J}_n}\sum_{x^n\in\mathcal{X}^n} V_{s^n}^n\big(\pi^{-1}(\widetilde{\mathcal{D}}_{s^n,j}^c)|x^n\big)E_\pi(x^n|j).\end{aligned}$$

Substituting this into (16), we see that

$$\frac{1}{|\mathcal{J}_n|}\sum_{j\in\mathcal{J}_n}\frac{1}{n!}\sum_{\pi\in\varPi_n}\sum_{x^n\in\mathcal{X}^n} V^n_{s^n}\big(\pi^{-1}(\widetilde{\mathcal{D}}^c_{s^n,j})|x^n\big)E_\pi(x^n|j) \geq 1-(n+1)^{|\mathcal{S}|}e^{-n\frac{\epsilon}{2}} \qquad (17)$$

so that the average decoding error at the eavesdropper satisfies (10) as the right hand side of (17) is independent of the actual state sequence $s^n \in \mathcal{S}^n$, the actual permutation $\pi \in \varPi_n$, and the particular decoding strategy $\{\widetilde{\mathcal{D}}_{s^n,j}\}$ of the eavesdropper.

Thus, we have constructed a CR-assisted $(n, J_n, \varPi_n, \mu)$-code $\mathcal{C}_{\text{CR}}$ which is "good" for the AVWC in the sense that it achieves the desired rate (11) with the desired behavior of the decoding performance at the eavesdropper (16). ■

If we apply the achievability result in Theorem 3 to the n-fold products of the wiretap channel, we immediately obtain the following multi-letter version (similarly as in [9]).

Corollary 1. For the AVWC $\mathfrak{W}$, any rate $R_S > 0$ satisfying

$$R_S \leq \lim_{n\to\infty}\frac{1}{n}\max_{U-X^n-(Y^n_q,Z^n_q)} \times\Big(\min_{q\in\mathcal{P}(\mathcal{S})} I(U;Y^n_q) - \max_{q\in\mathcal{P}(\mathcal{S})} I(U;Z^n_q)\Big) \qquad (18)$$

is an achievable CR-assisted secrecy rate for the secrecy measure of average decoding error at the eavesdropper for random variables satisfying the Markov chain $U - X^n - (Y^n_q, Z^n_q)$.

Sketch of Proof: Consider n-fold products of the channels $W^n_q : \mathcal{X}^n \to \mathcal{P}(\mathcal{Y}^n)$ and $V^n_q : \mathcal{X}^n \to \mathcal{P}(\mathcal{Z}^n)$ and further the auxiliary channel $P_{X^n|U} : \mathcal{U} \to \mathcal{P}(\mathcal{X}^n)$. Then applying the achievability result in Theorem 3 to the "blocked" channels $\widehat{W}_q(y^n|u) := \sum_{x^n\in\mathcal{X}^n} W^n_q(y^n|x^n)P_{X^n|U}(x^n|u)$ and $\widehat{V}_q(z^n|u) := \sum_{x^n\in\mathcal{X}^n} V^n_q(z^n|x^n)P_{X^n|U}(x^n|u)$ yields (18). ■

V. Discussion

Previous works have studied the AVWC solely for the weak and strong secrecy criteria with the consequence that no general CR-assisted achievable secrecy rate was known. In this paper, we have considered the secrecy measure of high average decoding error at the eavesdropper instead of the (strong) secrecy criterion. This criterion is weaker since the strong secrecy criterion implies high average decoding error (but not vice versa), cf. for example [7, 9].

However, this secrecy measure has allowed us to establish a general CR-assisted achievable secrecy rate for the AVWC. Interestingly, the corresponding rate (18) equals the multi-letter description of the secrecy capacity for the corresponding compound wiretap channel $\{(W_q, V_q) : q \in \mathcal{P}(\mathcal{S})\}$ with W_q and V_q the averaged channels, cf. (2), for the strong secrecy criterion, cf. [9]. Thus, the CR-assisted secrecy capacity of the AVWC for the decoding error measure is greater than or equal to the corresponding compound secrecy capacity for the strong secrecy criterion.

On the other hand, for the AVWC with a strong secrecy criterion we observe the following: Assume that there is a "good" CR-assisted code for the AVWC for strong secrecy, i.e. $I(J; Z^n_{s^n}) \leq \delta_n$ is satisfied. Then we have for all $q \in \mathcal{P}(\mathcal{S})$

$$I(J;Z_q) \leq \sum_{s^n\in\mathcal{S}^n} q^n(s^n)I(J;Z^n_{s^n}) \leq \sum_{s^n\in\mathcal{S}^n} q^n(s^n)\delta_n = \delta_n$$

which follows from the fact that the mutual information is convex in the channel. This means that this code is also "good" for the corresponding compound channel. The consequence is that the CR-assisted secrecy capacity of the AVWC for the strong secrecy criterion is smaller than or equal to the corresponding compound secrecy capacity for the strong secrecy criterion.

Thus, the CR-assisted secrecy capacity of the AVWC might differ depending on which secrecy measure is applied. Certainly, strong secrecy yields a secrecy capacity smaller than or equal to the corresponding one for the average decoding error criterion. We expect that there might be examples where the strong secrecy capacity is in fact strictly smaller.

References

[1] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information Theoretic Security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

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

[3] A. D. Wyner, "The Wire-Tap Channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[4] I. Csiszár, "Almost Independence and Secrecy Capacity," *Probl. Pered. Inform.*, vol. 32, no. 1, pp. 48–57, 1996.

[5] U. M. Maurer and S. Wolf, "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free," in *EUROCRYPT 2000, Lecture Notes in Computer Science*. Springer-Verlag, May 2000, vol. 1807, pp. 351–368.

[6] M. R. Bloch and J. N. Laneman, "Strong Secrecy from Channel Resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.

[7] H. Boche and R. F. Schaefer, "Wiretap Channels with Side Information – Strong Secrecy Capacity and Optimal Transceiver Design," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 8, pp. 1397–1408, Aug. 2013.

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

[9] I. Bjelaković, H. Boche, and J. Sommerfeld, "Secrecy Results for Compound Wiretap Channels," *Probl. Inf. Transmission*, vol. 49, no. 1, pp. 73–98, Mar. 2013.

[10] D. Blackwell, L. Breiman, and A. J. Thomasian, "The Capacities of Certain Channel Classes under Random Coding," *Ann. Math. Stat.*, vol. 31, no. 3, pp. 558–567, 1960.

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

[12] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge University Press, 2011.

[13] A. D. Sarwate and M. Gastpar, "List-Decoding for the Arbitrarily Varying Channel Under State Constraints," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1372–1384, Mar. 2012.

[14] E. MolavianJazi, M. Bloch, and J. N. Laneman, "Arbitrary Jamming Can Preclude Secure Communication," in *Proc. Allerton Conf. Commun., Control, Computing*, Urbana-Champaign, IL, USA, Sep. 2009, pp. 1069–1075.

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

[16] R. Ahlswede, "Arbitrarily Varying Channels with States Sequence Known to the Sender," *IEEE Trans. Inf. Theory*, vol. 32, no. 5, pp. 621–629, Sep. 1986.

[17] H. Boche and R. F. Schaefer, "Capacity Results and Super-Activation for Wiretap Channels With Active Wiretappers," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 9, pp. 1482–1496, Sep. 2013.