

Arbitrarily Varying Wiretap Channels with Finite Coordination Resources

Holger Boche

Lehrstuhl für Theoretische Informationstechnik
Technische Universität München
80290 München, Germany

Rafael F. Schaefer

Department of Electrical Engineering
Princeton University
Princeton, NJ 08544, USA

Abstract—The wiretap channel models secure communication in the presence of a non-legitimate eavesdropper who has to be kept ignorant. In this paper, the *arbitrarily varying wiretap channel (AVWC)* is studied, in which the channel to both legitimate receiver and eavesdropper may vary in an unknown and arbitrary manner from channel use to channel use. It has been shown that for AVCs coordination between the transmitter and legitimate receiver based on *common randomness (CR)* is indispensable for reliable communication. Approaches taken so far yield CR-assisted strategies where the needed amount of CR increases unbounded with the block length. In this paper, it is shown that if we allow for a small but non-vanishing average probability of error and information leakage (in terms of weak secrecy), the amount of CR is always finite and independent of the block length. The corresponding secrecy capacity equals the one with asymptotically vanishing performance requirements. Furthermore, it is shown that the average decoding error at the eavesdropper can be made arbitrarily close to 1 regardless of the applied decoding strategy.

I. INTRODUCTION

The security of sensitive information from unauthorized access becomes more and more important as rapid developments in communications systems make information available almost everywhere. Common approaches to keep information secret rely on cryptographic techniques which are based on the assumption of insufficient computational capabilities of non-legitimate receivers. Such techniques are becoming more insecure due to increasing computational power but also due to improved algorithms and recent advances in number theory.

In particular, wireless communication systems are inherently vulnerable for eavesdropping as the wireless channel makes the communication easily accessible to external eavesdroppers. But on the other hand, it also offers the possibility to apply physical layer based security approaches. Such concepts are becoming more attractive, since they solely use the physical properties of the wireless channel to establish security.

The field of physical layer security or information theoretic security was initiated by Wyner, who introduced the *wiretap channel* [1]. It models secure communication with one legitimate transmitter-receiver pair and one eavesdropper to be

kept ignorant. Recently, there is growing interest in physical layer security as it is a promising approach to embed secure communication in wireless networks; see for instance [2–4].

Most of previous studies have in common that all channels are assumed to be perfectly known and fixed during the whole time of transmission. In contrast to that, we consider in this paper channels that may vary in an arbitrary and unknown manner from channel use to channel use. For example, such conditions apply to fast fading wireless channels but also to scenarios with more malicious eavesdroppers which jam the legitimate transmission. Such unknown varying channel conditions are perfectly captured by the concept of *arbitrarily varying channels (AVC)* [5–7]. Accordingly, the communication problem at hand is given by the *arbitrarily varying wiretap channel (AVWC)* which is introduced in Section II. In the context of AVCs, it has been shown that *common randomness (CR)* is an important and often necessary resource for reliable communication over AVCs; in particular, if the channel is symmetrizable [5–7]. CR enables transmitter and receiver to use *CR-assisted strategies* by coordinating their choice of encoder and decoder. This is discussed in Section III.

In previous works, the secrecy capacity of the AVWC is studied under the assumptions of asymptotically vanishing average probability of decoding error at the legitimate receiver and information leakage to the eavesdropper [8–10]. Constructions of optimal coding strategies then yield CR-assisted codes relying on CR whose amount increases unbounded with the block length. In this paper, we show that for small but non-vanishing probability of error and information leakage, the amount of such resources needed to achieve capacity is finite, i.e., in particular independent of the block length. The corresponding secrecy capacity equals the one with asymptotically vanishing performance requirements. Interestingly, the construction used here holds only for the weak secrecy criterion but not for the strong secrecy criterion. However, the CR-assisted code can be constructed in such a way that the average decoding error at the eavesdropper can be made arbitrarily close to 1 depending only on the non-vanishing performance requirements. This holds for any decoding strategy the eavesdropper might apply; even if it depends on the actual state sequence (which might be known to the eavesdropper but not to the legitimate users). Thus,

This work of Holger Boche was supported by the German Ministry of Education and Research (BMBF) under Grant 01BQ1050. This work of Rafael F. Schaefer was supported by the German Research Foundation (DFG) under Grant WY 151/2-1.

the confidential communication can be protected against this kind of attack. This is discussed in detail in Section IV and the corresponding proofs are given in Section V. Finally, a conclusion is given in Section VI.¹

II. ARBITRARILY VARYING WIRETAP CHANNELS

Let \mathcal{X} and \mathcal{Y} , \mathcal{Z} be finite input and output sets and \mathcal{S} be a finite state set. The channels to the legitimate receiver and the eavesdropper are given by $W : \mathcal{X} \times \mathcal{S} \rightarrow \mathcal{P}(\mathcal{Y})$ and $V : \mathcal{X} \times \mathcal{S} \rightarrow \mathcal{P}(\mathcal{Z})$ respectively. Then for a given state sequence $s^n \in \mathcal{S}^n$ of length n , the discrete memoryless channel to the legitimate receiver is given by $W^n(y^n|x^n, s^n) := \prod_{i=1}^n W(y_i|x_i, s_i)$ for all $y^n \in \mathcal{Y}^n$ and $x^n \in \mathcal{X}^n$. Then the *arbitrarily varying channel (AVC)* \mathcal{W} to the legitimate receiver is the family of channels for all state sequences $s^n \in \mathcal{S}^n$, i.e.,

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

Accordingly, for given state sequence $s^n \in \mathcal{S}^n$ the discrete memoryless channel to the eavesdropper is given by $V^n(z^n|x^n, s^n) := \prod_{i=1}^n V(z_i|x_i, s_i)$ for all $z^n \in \mathcal{Z}^n$ and $x^n \in \mathcal{X}^n$, and, further, $\mathcal{V} := \{V^n(\cdot|\cdot, s^n) : s^n \in \mathcal{S}^n\}$.

Definition 1. The *arbitrarily varying wiretap channel (AVWC)* \mathfrak{W} is the family of pairs of channels with common input as

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

The task is now to establish a reliable communication between the transmitter and the legitimate receiver while keeping the eavesdropper completely ignorant of it.

Definition 2. An (n, J_n) -code \mathcal{C} for the AVWC \mathfrak{W} consists of a stochastic encoder

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

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

$$\{\mathcal{D}_j \subset \mathcal{Y}^n : j \in \mathcal{J}_n\}. \quad (2)$$

In contrast to the classical wiretap channel, the unknown varying channel states have to be taken into account for establishing reliable communication. Therefore, for given state sequence $s^n \in \mathcal{S}^n$, the average probability of decoding error at the legitimate receiver is given by

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

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

To ensure confidentiality of the message for all possible state sequences $s^n \in \mathcal{S}^n$ simultaneously, we require either

$$\max_{s^n \in \mathcal{S}^n} \frac{1}{n} I(J; Z_{s^n}^n | \mathcal{C}) \leq \delta_n \quad (3)$$

¹*Notation:* Discrete random variables are denoted by capital letters and their realizations and ranges by lower case and script letters; \mathbb{N} is the set of positive integers; $\mathcal{P}(\cdot)$ is the set of all probability distributions; $\|P_1 - P_2\|$ is the total variation distance of probability distributions P_1 and P_2 on \mathcal{A} defined by $\|P_1 - P_2\| := \frac{1}{2} \sum_{a \in \mathcal{A}} |P_1(a) - P_2(a)|$.

or

$$\max_{s^n \in \mathcal{S}^n} I(J; Z_{s^n}^n | \mathcal{C}) \leq \delta_n \quad (4)$$

for $\delta_n > 0$ with J the random variable uniformly distributed over the set of messages \mathcal{J}_n and $Z_{s^n}^n = (Z_{s_1}, \dots, Z_{s_n})$ the channel output at the eavesdropper for state sequence $s^n \in \mathcal{S}^n$. The first criterion (3) is known as *weak secrecy* [1, 11] while the latter (4) is named *strong secrecy* [12, 13] as it is strengthened by dropping the division by the block length n . Both expressions describe how much information of the confidential message is leaked to the eavesdropper. While (3) has the form of a leakage rate, the stronger version (4) actually corresponds to the total amount of information that is leaked.

Definition 3. A non-negative number R 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 $n \geq n(\tau)$ we have $\frac{1}{n} \log J_n \geq R - \tau$, $\max_{s^n \in \mathcal{S}^n} \bar{e}_n(s^n|\mathcal{C}) \leq \lambda_n$, and $\max_{s^n \in \mathcal{S}^n} I(J; Z_{s^n}^n | \mathcal{C}) \leq \delta_n$ (or $\max_{s^n \in \mathcal{S}^n} \frac{1}{n} I(J; Z_{s^n}^n | \mathcal{C}) \leq \delta_n$) while $\lambda_n, \delta_n \rightarrow 0$ as $n \rightarrow \infty$. The *secrecy capacity* C_S is given by the supremum of all achievable secrecy rates R .

It has been shown that such traditional (deterministic) approaches as given in Definition 2 might not suffice to establish reliable communication over AVCs; in particular, if the channel is *symmetrizable* then there is no communication possible [6, 7, 9, 10]. This necessitates the use of more sophisticated strategies based on coordination resources such as *common randomness (CR)* as discussed in the following section.

III. COMMON RANDOMNESS ASSISTED COMMUNICATION

If *common randomness* is available at all users, then the transmitter and legitimate receiver can use this resource to coordinate their choice of encoder and decoder. This is modeled by a random variable Γ taking values in \mathcal{G}_n according to the distribution $P_\Gamma \in \mathcal{P}(\mathcal{G}_n)$. Then, encoder (1) and decoder (2) depend on the particular realization $\gamma \in \mathcal{G}_n$.

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

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

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

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

$$\bar{e}_{CR,n}(s^n|\mathcal{C}_{CR}) := \frac{1}{|\mathcal{J}_n|} \sum_{j \in \mathcal{J}_n} \sum_{\gamma \in \mathcal{G}_n} \sum_{x^n \in \mathcal{X}^n} W^n(\mathcal{D}_j^c|x^n, s^n)E_\gamma(x^n|j)P_\Gamma(\gamma)$$

and $\bar{e}_{CR,n}(\mathcal{C}_{CR}) := \max_{s^n \in \mathcal{S}^n} \bar{e}_{CR,n}(s^n|\mathcal{C}_{CR})$. The strong secrecy criterion (4) becomes $\max_{s^n \in \mathcal{S}^n} I(J; Z_{s^n}^n | \mathcal{C}_{CR}) = \max_{s^n \in \mathcal{S}^n} \mathbb{E}_\Gamma[I(J; Z_{s^n}^n | \mathcal{C}(\Gamma))]$, i.e.,

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

The definition of the mean weak secrecy criterion (3) for CR-assisted codes follows accordingly.

Definition 5. A non-negative number R is a *CR-assisted 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 CR-assisted $(n, J_n, \mathcal{G}_n, P_\Gamma)$ -codes \mathcal{C}_{CR} such that for all $n \geq n(\tau)$ we have $\frac{1}{n} \log J_n \geq R - \tau$, $\max_{s^n \in \mathcal{S}^n} \bar{e}_{CR,n}(s^n | \mathcal{C}_{CR}) \leq \lambda_n$, and $\max_{s^n \in \mathcal{S}^n} I(J; Z_{s^n}^n | \mathcal{C}_{CR}) \leq \delta_n$ (or $\max_{s^n \in \mathcal{S}^n} \frac{1}{n} I(J; Z_{s^n}^n | \mathcal{C}_{CR}) \leq \delta_n$) while $\lambda_n, \delta_n \rightarrow 0$ as $n \rightarrow \infty$. The *CR-assisted secrecy capacity* $C_{S,CR}$ is given by the supremum of all achievable secrecy rates R .

From [9] we know that there exists CR-assisted codes which satisfy the following properties:

Theorem 1. For any CR-assisted secrecy rate $R < C_{S,CR}$, there exist a constant $\epsilon > 0$ and an $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ there exists a CR-assisted $(n, J_n, \mathcal{G}_n, P_\Gamma)$ -code with $\frac{1}{n} \log J_n \geq R$,

$$\max_{s^n \in \mathcal{S}^n} \sum_{\gamma \in \mathcal{G}_n} \bar{e}_n(s^n | \mathcal{C}(\gamma)) P_\Gamma(\gamma) \leq e^{-n\epsilon}, \quad (5)$$

and

$$\max_{s^n \in \mathcal{S}^n} \sum_{\gamma \in \mathcal{G}_n} I(J; Z_{s^n}^n | \mathcal{C}(\gamma)) P_\Gamma(\gamma) \leq e^{-n\epsilon}. \quad (6)$$

The result in Theorem 1 provides for any secrecy rate $R < C_{S,CR}$, a CR-assisted code whose average decoding error and strong secrecy decrease both exponentially fast, cf. (5)-(6). In addition, we know from [9] that the following is true as well:

Theorem 2. For any CR-assisted secrecy rate $R < C_{S,CR}$, there exist a constant $\epsilon > 0$ and an $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ there exists a CR-assisted $(n, J_n, \mathcal{G}_n, P_\Gamma)$ -code with $\frac{1}{n} \log J_n \geq R$, $\bar{e}_{CR,n}(\mathcal{C}_{CR}) \leq e^{-n\epsilon}$ as in (5), and

$$\max_{s^n \in \mathcal{S}^n} \sum_{\gamma \in \mathcal{G}_n} \|P_{JZ_{s^n}^n, \gamma} - P_{J, \gamma} P_{Z_{s^n}^n, \gamma}\| P_\Gamma(\gamma) \leq e^{-n\epsilon} \quad (7)$$

with $P_{JZ_{s^n}^n, \gamma}(j, z^n)$ for all $j \in \mathcal{J}_n$ and $z^n \in \mathcal{Z}^n$ is the joint distribution according to the codebook $\mathcal{C}(\gamma)$ and $\|\cdot\|$ is the total variation distance. Note that in this case, only the randomized encoding depends on the particular $\gamma \in \mathcal{G}_n$.

Having the total variation distance between the “true” joint distribution $P_{JZ_{s^n}^n, \gamma}$ and its corresponding product distribution $P_{J, \gamma} P_{Z_{s^n}^n, \gamma}$ small, cf. (7), is a desirable property. In fact, not only the mutual information (6) becomes small, but also this implies a worst behavior of decoding performance at the eavesdropper in the sense that its average decoding error approaches 1 exponentially fast for all possible decoding strategies the eavesdropper might use, cf. [9]. This establishes an operational meaning for the secrecy requirements.

However, such codes realizing (5)-(7) usually require a “strong” coordination between transmitter and receiver. In particular, with the construction above, cf. Theorems 1-2 and [9], the amount of common randomness, that is needed to meet the requirement of vanishing decoding error, strong secrecy,

and total variation distance increases unbounded with the block length.

Due to the need of unlimited coordination resources, such codes are far away from being applicable in practical systems. Therefore, the question arises if it is possible to control the amount of needed resources and to achieve the same rates with a fixed amount of CR (i.e. independent of the block length n) when we allow for fixed but non-vanishing probability of decoding error and non-vanishing information leakage.

IV. FINITE COORDINATION RESOURCES

We will study this question for CR-assisted codes that consist of a finite number of deterministic codes, i.e., $|\mathcal{G}_n| < \infty$, chosen according to a uniform distribution. Important is that we will stick to the weak secrecy criterion (3) in the following.

Definition 6. A non-negative number R is a (λ, δ) -achievable secrecy rate with resource L if for all $\tau > 0$ there is an $n(\tau) \in \mathbb{N}$ such that for all $n \geq n(\tau)$ there exist L deterministic (n, J_n) -codes $\mathcal{C}(\gamma_i)$, $\gamma_i = 1, \dots, L$, (each of rate $\frac{1}{n} \log J_n \geq R - \tau$) with

$$\max_{s^n \in \mathcal{S}^n} \frac{1}{L} \sum_{\gamma_i=1}^L \bar{e}_n(s^n | \mathcal{C}(\gamma_i)) \leq \lambda$$

and

$$\max_{s^n \in \mathcal{S}^n} \frac{1}{L} \sum_{\gamma_i=1}^L \frac{1}{n} I(J; Z_{s^n}^n | \mathcal{C}(\gamma_i)) \leq \delta.$$

The supremum of all (λ, δ) -achievable secrecy rates with resource L is denoted by $C_S(\lambda, \delta, L)$.

We have the following result.

Theorem 3. Let $\lambda \in (0, 1)$ and $\delta \in (0, 1)$ be arbitrary but fixed. Then for every secrecy rate $R < C_{S,CR}$ there exists a finite number L such that

$$R < C_S(\lambda, \delta, L).$$

Proof: The proof can be found in Section V-A. ■

Corollary 1. Every secrecy rate $R < C_{S,CR}$ is achievable with a finite amount of coordination resources.

This result shows that if we make the practical assumptions of finite, non-vanishing average probability of decoding error and secrecy leakage, then there exists a “good” CR-assisted code consisting of a finite number of L deterministic codes (independent of the block length n). Note that Theorem 3 only holds for the weak secrecy criterion. At least the proof technique used in this paper does not directly carry over to the strong secrecy criterion.

As discussed before in Section III, the property of small total variation distance, cf. (7), is desirable as well. Thus, it is further important and interesting to study the following:

Theorem 4. Let $\lambda \in (0, 1)$ and $\mu \in (0, 1)$ be arbitrary but fixed. Then for every secrecy rate $R < C_{S,CR}$ there exists an $n_0 \in \mathbb{N}$ and an $L_0 > 0$ such that for all $n \geq n_0$ and $L \geq L_0$,

there exists L deterministic codebooks $\mathcal{C}(\gamma_i)$, $\gamma_i = 1, \dots, L$ with

$$\max_{s^n \in \mathcal{S}^n} \frac{1}{L} \sum_{\gamma_i=1}^L \bar{e}_n(s^n | \mathcal{C}(\gamma_i)) \leq \lambda$$

and

$$\max_{s^n \in \mathcal{S}^n} \frac{1}{L} \sum_{\gamma_i=1}^L \|P_{JZ_{s^n}^n, \gamma_i} - P_{J, \gamma_i} P_{Z_{s^n}^n, \gamma_i}\| \leq \mu. \quad (8)$$

Proof: The proof can be found in Section V-B. ■

This result shows that if we allow for a finite, non-vanishing average probability of decoding error and total variation distance, then there exists a “good” CR-assisted code consisting of L deterministic codes (independent of the block length n).

Similarly as in [9], with this result we immediately obtain a bound on the decoding performance of the eavesdropper. To be on the safest side from a secrecy perspective, we assume the worst which is an eavesdropper who knows the particular state sequence $s^n \in \mathcal{S}^n$ and the used codebook $\mathcal{C}(\gamma_i)$, i.e., in particular the realization $\gamma_i \in \{1, \dots, L\}$. Then he may choose any decoder $\psi : \mathcal{Z}^n \times \mathcal{S}^n \times \{1, \dots, L\} \rightarrow \mathcal{J}_n$ given by disjoint decoding sets

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

Then, the associated average probability of error (for fixed $s^n \in \mathcal{S}^n$ and $\gamma_i \in \mathcal{G}_n$) is given by

$$\begin{aligned} \bar{e}_{\text{Eve}, n}(\{\tilde{\mathcal{D}}_{\gamma_i, s^n, j}\}, \gamma_i, s^n) \\ := \frac{1}{|\mathcal{J}_n|} \sum_{j \in \mathcal{J}_n} \sum_{x^n \in \mathcal{X}^n} V^n(\tilde{\mathcal{D}}_{\gamma_i, s^n, j}^c | x^n, s^n) E_{\gamma_i}(x^n | j). \end{aligned}$$

For a CR-assisted code with L elements we then have

$$\bar{e}_{\text{Eve}, n}(\{\tilde{\mathcal{D}}_{\gamma_i, s^n, j}\}, s^n) := \frac{1}{L} \sum_{\gamma_i=1}^L \bar{e}_{\text{Eve}, n}(\{\tilde{\mathcal{D}}_{\gamma_i, s^n, j}\}, \gamma_i, s^n).$$

Theorem 5. For any given CR-assisted $(n, J_n, \mathcal{G}_n, P_T)$ -code of Definition 4 of rate $R < C_{S, \text{CR}}$ with finite coordination resource $|\mathcal{G}_n| = L$ satisfying (8) of Theorem 4, we have for all possible decoding strategies of the eavesdropper

$$\min_{s^n \in \mathcal{S}^n} \frac{1}{L} \sum_{\gamma_i=1}^L \bar{e}_{\text{Eve}, n}(\{\tilde{\mathcal{D}}_{\gamma_i, s^n, j}\}, \gamma_i, s^n) \geq 1 - \frac{1}{2nR} - \mu. \quad (9)$$

Proof: The proof can be found in Section V-C. ■

The previous results show that if we allow for a small, but non-vanishing average probability of decoding error and information leakage, we are able to find a CR-assisted code with finite coordination resources if we stick to the weak secrecy criterion. Unfortunately, for the strong secrecy criterion the proof technique used above does not hold. However, we can construct this code in such a way that the decoding error at the eavesdropper is arbitrarily close to 1 regardless of the decoding strategy the eavesdropper applies. Moreover, the eavesdropper is able to choose his decoding sets depending on the particular state sequence $s^n \in \mathcal{S}^n$. But however, the decoding error approaches $1 - \mu$, where $\mu > 0$ is the information leakage that we tolerate.

V. PROOFS

In the following we present the proofs of the main results.

A. Proof of Theorem 3

Let $\lambda \in (0, 1)$, $\delta \in (0, 1)$, and $\alpha_1, \alpha_2 > 0$ be arbitrary but fixed. Then for any $R < C_{S, \text{CR}}$ we know from Theorem 1 that there is a CR-assisted code \mathcal{C}_{CR} such that the decoding error probability and information leakage satisfy (5) and (6). Thus, the probability that for finite $|\mathcal{G}_n| = L$ and fixed $s^n \in \mathcal{S}^n$ this is not satisfied, is given by

$$\begin{aligned} \mathbb{P}\left\{\frac{1}{L} \sum_{\gamma_i=1}^L \bar{e}_n(s^n | \mathcal{C}(\gamma_i)) \geq \lambda \text{ or } \frac{1}{L} \sum_{\gamma_i=1}^L \frac{1}{n} I(J; Z_{s^n}^n | \mathcal{C}(\gamma_i)) \geq \delta\right\} \\ \leq \mathbb{P}\left\{\exp\left(\alpha_1 \sum_{\gamma_i=1}^L \bar{e}_n(s^n | \mathcal{C}(\gamma_i))\right) \geq \exp(\alpha_1 \lambda L)\right\} \\ + \mathbb{P}\left\{\exp\left(\alpha_2 \sum_{\gamma_i=1}^L \frac{1}{n} I(J; Z_{s^n}^n | \mathcal{C}(\gamma_i))\right) \geq \exp(\alpha_2 \delta L)\right\} \\ \leq \exp(-\alpha_1 \lambda L) \prod_{\gamma_i=1}^L \mathbb{E}\left[\exp\left(\alpha_1 \bar{e}_n(s^n | \mathcal{C}(\gamma_i))\right)\right] \\ + \exp(-\alpha_2 \delta L) \prod_{\gamma_i=1}^L \mathbb{E}\left[\exp\left(\frac{\alpha_2}{n} I(J; Z_{s^n}^n | \mathcal{C}(\gamma_i))\right)\right]. \end{aligned} \quad (10)$$

In the following, we consider both terms in (10) separately. By the fact that $\bar{e}_n(s^n | \mathcal{C}(\gamma_i)) \leq 1$ always holds and by standard arguments, cf. also [14], we obtain for the expectation in the first term

$$\begin{aligned} \mathbb{E}\left[\exp\left(\alpha_1 \bar{e}_n(s^n | \mathcal{C}(\gamma_i))\right)\right] \\ = \mathbb{E}\left[\sum_{k=0}^{\infty} \frac{(\alpha_1 \bar{e}_n(s^n | \mathcal{C}(\gamma_i)))^k}{k!}\right] \\ \leq \mathbb{E}\left[1 + \sum_{k=1}^{\infty} \frac{\alpha_1^k}{k!} \bar{e}_n(s^n | \mathcal{C}(\gamma_i))\right] \\ \leq 1 + \left(\sum_{k=1}^{\infty} \frac{\alpha_1^k}{k!}\right) e^{-n\epsilon} \\ = 1 + e^{-n\epsilon} (e^{\alpha_1} - 1) \\ < 1 + \exp(-n\epsilon + \alpha_1) \end{aligned}$$

so that we obtain for the first term

$$\begin{aligned} \mathbb{P}\left\{\exp\left(\alpha_1 \sum_{i=1}^L \bar{e}_n(s^n | \mathcal{C}(\gamma_i))\right) \geq \exp(\alpha_1 \lambda L)\right\} \\ \leq \exp(-\alpha_1 \lambda L) (1 + \exp(-n\epsilon + \alpha_1))^L. \end{aligned}$$

Now, taking all state sequences $s^n \in \mathcal{S}^n$ into account yields

$$\begin{aligned} \mathbb{P}\left\{\exp\left(\alpha_1 \sum_{\gamma_i=1}^L \bar{e}_n(s^n | \mathcal{C}(\gamma_i))\right) \geq \exp(\alpha_1 \lambda L) \text{ for some } s^n \in \mathcal{S}^n\right\} \\ \leq \exp(-\alpha_1 \lambda L) (1 + \exp(-n\epsilon + \alpha_1))^L \exp(n \ln |\mathcal{S}|) \\ \leq \exp(-n\epsilon \lambda L + \ln 2L + n \ln |\mathcal{S}|) \\ = \exp\left(-n\epsilon \lambda \left(L - \left(\frac{\ln 2}{n\epsilon \lambda} + \frac{\ln |\mathcal{S}|}{\epsilon \lambda}\right)\right)\right) \end{aligned} \quad (11)$$

where the second step follows with the choice $\alpha_1 = n\epsilon$.

Now, if we choose

$$L > \underline{L}_1 := \frac{1}{\epsilon\lambda} \ln |\mathcal{S}|, \quad (12)$$

then the probability that the average probability of error of the constructed code is smaller than the required λ is

$$\mathbb{P}\left\{\frac{1}{L} \sum_{\gamma_i=1}^L \bar{e}_n(s^n | \mathcal{C}(\gamma_i)) < \lambda \text{ for all } s^n \in \mathcal{S}^n\right\} \xrightarrow{n \rightarrow \infty} 1$$

exponentially fast as given by (11).

Now we turn to the second term in (10). We obtain for the expectation

$$\begin{aligned} & \mathbb{E}\left[\exp\left(\frac{\alpha_2}{n} I(J; Z_{s^n}^n | \mathcal{C}(\gamma_i))\right)\right] \\ &= \mathbb{E}\left[1 + \sum_{k=1}^{\infty} \frac{\alpha_2^k}{k!} \left(\frac{1}{n} I(J; Z_{s^n}^n | \mathcal{C}(\gamma_i))\right)^k\right] \\ &\leq \mathbb{E}\left[1 + \sum_{k=1}^{\infty} \frac{\alpha_2^k}{k!} \frac{I(J; Z_{s^n}^n | \mathcal{C}(\gamma_i))}{n} c^{k-1}\right] \\ &\leq \mathbb{E}\left[1 + \frac{1}{n} \frac{I(J; Z_{s^n}^n | \mathcal{C}(\gamma_i))}{c} \sum_{k=1}^{\infty} \frac{\alpha_2^k}{k!} c^k\right] \\ &\leq \mathbb{E}\left[1 + \frac{I(J; Z_{s^n}^n | \mathcal{C}(\gamma_i))}{nc} \exp(\alpha_2 c)\right] \\ &\leq 1 + \frac{\exp(-n\epsilon + \alpha_2 c)}{nc} \end{aligned}$$

with c a constant upper bound (depending only on the cardinalities of the message set and output alphabet of the eavesdropper) on the mutual information term $I(J; Z_{s^n}^n | \mathcal{C}(\gamma_i))$ so that the second term in (10) becomes

$$\begin{aligned} & \mathbb{P}\left\{\frac{1}{L} \sum_{\gamma_i=1}^L \frac{1}{n} I(J; Z_{s^n}^n | \mathcal{C}(\gamma_i)) \geq \delta\right\} \\ &\leq \exp(-\alpha_2 \delta L) \left(1 + \frac{\exp(-n\epsilon + \alpha_2 c)}{nc}\right)^L. \end{aligned}$$

Now, taking all state sequences $s^n \in \mathcal{S}^n$ into account yields

$$\begin{aligned} & \mathbb{P}\left\{\frac{1}{L} \sum_{\gamma_i=1}^L \frac{1}{n} I(J; Z_{s^n}^n | \mathcal{C}(\gamma_i)) \geq \delta \text{ for some } s^n \in \mathcal{S}^n\right\} \\ &\leq \exp(-\alpha_2 \delta L) \left(1 + \frac{\exp(-n\epsilon + \alpha_2 c)}{nc}\right)^L \exp(n \ln |\mathcal{S}|) \\ &\leq \exp\left(-\frac{n\epsilon\delta}{c} \left(L - \left(\frac{\ln 2c}{n\epsilon\delta} + \frac{\ln |\mathcal{S}|c}{\epsilon\delta}\right)\right)\right) \quad (13) \end{aligned}$$

with the choice $\alpha_2 = \frac{n\epsilon}{c}$.

Now, if we choose

$$L > \underline{L}_2 := \frac{c}{\epsilon\delta} \ln |\mathcal{S}|,$$

then the probability that the information leakage rate of the constructed code is greater than the required δ is

$$\mathbb{P}\left\{\frac{1}{L} \sum_{\gamma_i=1}^L \frac{1}{n} I(J; Z_{s^n}^n | \mathcal{C}(\gamma_i)) < \delta \text{ for all } s^n \in \mathcal{S}^n\right\} \xrightarrow{n \rightarrow \infty} 1$$

exponentially fast as given by (13).

So if

$$L > \max\{\underline{L}_1, \underline{L}_2\} = \frac{\ln |\mathcal{S}|}{\epsilon} \max\left\{\frac{1}{\lambda}, \frac{c}{\delta}\right\},$$

then the probability that the constructed CR-assisted code (consisting of finite L deterministic codes) does not satisfy the λ -requirement on the probability of error and the δ -requirement on the secrecy for all state sequences $s^n \in \mathcal{S}^n$ is exponentially small. This completes the proof. ■

B. Proof of Theorem 4

Basically, the proof follows the lines of Theorem 3 in Section V-A for the weak secrecy criterion so that we highlight only the main differences.

As in Section V-A let $\lambda, \mu \in (0, 1)$ and $\alpha_1, \alpha_3 > 0$ be arbitrary but fixed. Then we know from Theorem 2 that exists “good” CR-assisted codes for any secrecy rate $R < C_{S,CR}$ where the conditions (5) and (7) are satisfied. Similarly, the probability that for finite $|\mathcal{G}_n| = L$ and fixed $s^n \in \mathcal{S}^n$ this is not true, is given by

$$\begin{aligned} & \mathbb{P}\left\{\frac{1}{L} \sum_{\gamma_i=1}^L \bar{e}_n(s^n | \mathcal{C}(\gamma_i)) \geq \lambda \text{ or}\right. \\ & \quad \left.\frac{1}{L} \sum_{\gamma_i=1}^L \|P_{JZ_{s^n}^n, \gamma_i} - P_{J, \gamma_i} P_{Z_{s^n}^n, \gamma_i}\| \geq \mu\right\} \\ &\leq \exp(-\alpha_1 \lambda L) \prod_{\gamma_i=1}^L \mathbb{E}\left[\exp(\alpha_1 \bar{e}_n(s^n | \mathcal{C}(\gamma_i)))\right] \\ & \quad + \exp(-\alpha_3 \mu L) \prod_{\gamma_i=1}^L \mathbb{E}\left[\exp(\alpha_3 \|P_{JZ_{s^n}^n, \gamma_i} - P_{J, \gamma_i} P_{Z_{s^n}^n, \gamma_i}\|)\right]. \quad (14) \end{aligned}$$

The first term follows exactly as in the proof of Theorem 3, cf. Section V-A. So if we choose

$$L > \underline{L}_1 := \frac{1}{\epsilon\lambda} \ln |\mathcal{S}|,$$

then the probability that the average probability of decoding error at the legitimate receiver is smaller than the required λ goes exponentially fast to 1, cf. also (12).

The derivation of the second term in (14) basically follows by replacing the weak secrecy criterion by the total variation distance term. In more detail, for the expectation we get

$$\begin{aligned} & \mathbb{E}\left[\exp(\alpha_3 \|P_{JZ_{s^n}^n, \gamma_i} - P_{J, \gamma_i} P_{Z_{s^n}^n, \gamma_i}\|)\right] \\ &= 1 + \sum_{k=1}^{\infty} \frac{\alpha_3^k}{k!} \mathbb{E}\left[\|P_{JZ_{s^n}^n, \gamma_i} - P_{J, \gamma_i} P_{Z_{s^n}^n, \gamma_i}\|^k\right] \\ &= 1 + \sum_{k=1}^{\infty} \frac{\alpha_3^k}{k!} \mathbb{E}\left[\|P_{JZ_{s^n}^n, \gamma_i} - P_{J, \gamma_i} P_{Z_{s^n}^n, \gamma_i}\| \right. \\ & \quad \left. \times \|P_{JZ_{s^n}^n, \gamma_i} - P_{J, \gamma_i} P_{Z_{s^n}^n, \gamma_i}\|^{k-1}\right]. \quad (15) \end{aligned}$$

Since

$$\|P_{JZ_{s^n}^n, \gamma_i} - P_{J, \gamma_i} P_{Z_{s^n}^n, \gamma_i}\| \leq \|P_{JZ_{s^n}^n, \gamma_i}\| + \|P_{J, \gamma_i} P_{Z_{s^n}^n, \gamma_i}\| = 2$$

we get for the term in (15) the following bound

$$\begin{aligned} & \mathbb{E}\left[\exp(\alpha_3 \|P_{JZ_{s^n, \gamma_i}^n} - P_{J, \gamma_i} P_{Z_{s^n, \gamma_i}^n}\|)\right] \\ & \leq 1 + \sum_{k=1}^{\infty} \frac{\alpha_3^k \cdot 2^{k-1}}{k!} \mathbb{E}\left[\|P_{JZ_{s^n, \gamma_i}^n} - P_{J, \gamma_i} P_{Z_{s^n, \gamma_i}^n}\|\right] \\ & \leq 1 + \frac{e^{-n\epsilon}}{2} \sum_{k=1}^{\infty} \frac{\alpha_3^k \cdot 2^k}{k!} \\ & < 1 + \frac{\exp(-n\epsilon + 2\alpha_3)}{2}. \end{aligned}$$

Now, if we choose $\alpha_3 = \frac{n\epsilon}{2}$, we can follow the proof of Theorem 3 to arrive, similarly as in (13), at

$$\begin{aligned} & \mathbb{P}\left\{\frac{1}{L} \sum_{\gamma_i=1}^L \|P_{JZ_{s^n, \gamma_i}^n} - P_{J, \gamma_i} P_{Z_{s^n, \gamma_i}^n}\| \geq \mu \text{ for some } s^n \in \mathcal{S}^n\right\} \\ & \leq \exp(-\alpha_3 \mu L) \left(1 + \frac{\exp(-n\epsilon + 2\alpha_3)}{2}\right)^L \exp(n \ln |\mathcal{S}|) \\ & \leq \exp\left(-\frac{n\epsilon\mu}{2} \left(L - \left(\frac{2 \ln 2}{n\epsilon\mu} + \frac{\ln |\mathcal{S}|}{\epsilon\mu}\right)\right)\right). \end{aligned}$$

So with

$$L > \underline{L}_3 := \frac{1}{\epsilon\mu} \ln |\mathcal{S}|,$$

the probability that the total variation distance is smaller than the required μ goes exponentially fast to 1; similarly as in Section V-A for the weak secrecy criterion. So with $L > \max\{\underline{L}_1, \underline{L}_3\}$ the theorem is proved. ■

C. Proof of Theorem 5

Let $\gamma_i \in \mathcal{G}_n$ with $1 \leq \gamma_i \leq L$ be fixed. Then for every $s^n \in \mathcal{S}^n$ and $\gamma_i \in \mathcal{G}_n$ the eavesdropper can choose his decoding sets $\{\tilde{\mathcal{D}}_{\gamma_i, s^n, j}\}$ accordingly and we obtain for each such choice

$$\begin{aligned} & \bar{e}_{\text{Eve}, n}(\{\tilde{\mathcal{D}}_{\gamma_i, s^n, j}\}, \gamma_i, s^n) \\ & \geq 1 - \frac{1}{2^{nR}} - \|P_{JZ_{s^n, \gamma_i}^n} - P_{J, \gamma_i} P_{Z_{s^n, \gamma_i}^n}\|. \end{aligned}$$

A similar derivation can be found for instance in [15, Section 2.2] for the compound wiretap channel or in [16, Section 3] for the wiretap channel with side information.

With this we get for the CR-assisted code with L elements

$$\begin{aligned} & \bar{e}_{\text{Eve}, n}(\{\tilde{\mathcal{D}}_{\gamma_i, s^n, j}\}, s^n) \\ & = \frac{1}{L} \sum_{\gamma_i=1}^L \bar{e}_{\text{Eve}, n}(\{\tilde{\mathcal{D}}_{\gamma_i, s^n, j}\}, \gamma_i, s^n) \\ & \geq 1 - \frac{1}{2^{nR}} - \frac{1}{L} \sum_{\gamma_i=1}^L \|P_{JZ_{s^n, \gamma_i}^n} - P_{J, \gamma_i} P_{Z_{s^n, \gamma_i}^n}\| \\ & \geq 1 - \frac{1}{2^{nR}} - \mu \end{aligned}$$

by Theorem 4. As this holds for all $s^n \in \mathcal{S}^n$ simultaneously, we obtain (9) completing the proof of the theorem. ■

VI. CONCLUSION

The AVWC models secure communication in the presence of a non-legitimate eavesdropper and unknown varying channel conditions. It has been shown that CR is indispensable for reliable communication under AVCs. If the average decoding error and information leakage are required to vanish asymptotically, the amount of needed CR increases unbounded with the block length. It is shown that allowing for a small, but non-vanishing average decoding error and information leakage, allows to use CR-assisted codes that require only a finite amount of CR independent of the block length. Surprisingly, the corresponding proof technique only holds for the weak secrecy criterion and the total variation distance. The latter has the practically relevant consequence that the decoding error at the eavesdropper can be made arbitrarily close 1 regardless of his decoding strategy. It holds for an eavesdropper who can adapt his decoding sets according to the actual state sequence. If these results extend to the strong secrecy criterion is unknown and an interesting question for future work.

REFERENCES

- [1] A. D. Wyner, "The Wire-Tap Channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.
- [2] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information Theoretic Security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.
- [3] E. A. Jorswieck, A. Wolf, and S. Gerbracht, "Secrecy on the Physical Layer in Wireless Networks," *Trends in Telecommunications Technologies*, pp. 413–435, Mar. 2010.
- [4] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.
- [5] 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.
- [6] R. Ahlswede, "Elimination of Correlation in Random Codes for Arbitrarily Varying Channels," *Z. Wahrscheinlichkeitstheorie verw. Gebiete*, vol. 44, pp. 159–175, 1978.
- [7] I. Csiszár and P. Narayan, "The Capacity of the Arbitrarily Varying Channel Revisited: Positivity, Constraints," *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 181–193, Mar. 1988.
- [8] 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.
- [9] 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.
- [10] 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.
- [11] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [12] I. Csiszár, "Almost Independence and Secrecy Capacity," *Probl. Pered. Inform.*, vol. 32, no. 1, pp. 48–57, 1996.
- [13] U. M. Maurer and S. Wolf, "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free," in *EUROCRYPT 2000, Lecture Notes in Computer Science*. Springer-Verlag, May 2000, vol. 1807, pp. 351–368.
- [14] R. Ahlswede and N. Cai, "Two Proofs of Pinsker's Conjecture Concerning Arbitrarily Varying Channels," *IEEE Trans. Inf. Theory*, vol. 37, no. 6, pp. 1647–1649, Nov. 1991.
- [15] 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.
- [16] 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.