SECRECY CAPACITY UNDER LIST DECODING FOR A CHANNEL WITH A PASSIVE EAVESDROPPER AND AN ACTIVE JAMMER

Ahmed S. Mansour, Rafael F. Schaefer†, and Holger Boche**

* Lehrstuhl für Theoretische Informationstechnik
Technische Universität München
80290 Munich, Germany
Email:{ahmed.mansour, boche}@tum.de

† Information Theory and Applications Chair
Technische Universität Berlin
10587 Berlin, Germany
Email: rafael.schaefer@tu-berlin.de

ABSTRACT

We investigate secure communication over a channel that undergoes two different classes of attacks at the same time: passive eavesdropping and active jamming. This scenario is perfectly modeled by the concept of *arbitrarily varying wiretap channels (AVWCs)*. We derive a full characterization of the secrecy capacity of AVWCs under list decoding. We show that the list secrecy capacity is either equivalent to the correlated random secrecy capacity or zero depending on the order of symmetrizability of the legitimate AVC. Differently from correlated random codes, our coding scheme does not assume any restrictions on the communication between the eavesdropper and the jammer.

Index Terms— Arbitrarily varying wiretap channel, list decoding, strong secrecy.

1. INTRODUCTION

Information theoretic security is one of the most active research field nowadays [1]. It was first initiated by Wyner in [2], where he studied secure communication over a wiretap channel with a passive eavesdropper, where the channel state is perfectly known. This assumption is not suitable for real life scenarios, where it is very difficult to acquire a perfect channel state information because the channel usually varies rapidly over time. Additionally, many channels suffer from the presence of active jammers who are capable of maliciously manipulating the channel state in each channel use [3]. In order to capture such effects, the model of the arbitrarily varying channel (AVC) [4, 5, 6] and the arbitrarily varying wiretap channel (AVWC) [3, 7, 8] are considered.

It was shown in [6] that uncorrelated codes fail to establish reliable communication over symmetrizable AVCs, where the jammer can selects a channel state that emulates a valid channel input. In order to overcome this issue, correlated random codes were used [4]. However, the usage of such codes requires the existence of a common random source which is only shared between the transmitter and the receiver and must be kept unknown to the jammer. It was also shown that the amount of common randomness needed grows unbounded with the block length of the code. Consequently, correlated random codes are not always feasible in practice. As an alternative, list codes have been used to establish a reliable communication over AVCs [9, 10]. For a given AVC, it was shown that if the list size is greater than the order of symmetrizability of the channel, then the list capacity is equivalent to the correlated random capacity, where the order of symmetrizability identifies the number of valid channel inputs that an AVC can emulate.

The previous results motivated many researchers to investigate secure communication over AVWCs as well. In [11, 12], a full characterization of the correlated and uncorrelated secrecy capacities were given. In this paper, we extend these results and present a full characterization of the list secrecy capacity of an AVWC. In particular, we show that if the list size is greater than the order of symmetrizability of the legitimate channel, then the list secrecy capacity is equivalent to the correlated random secrecy capacity, otherwise it is zero. This result was first established in [13] by using a coding scheme that combines public list codes and correlated random codes. In this paper, we establish the achievability part of the secrecy capacity using a coding scheme based on a secure list code only and is totally independent of the concept of correlated random codes. Our result is also a continuation of our previous work in [14]. It is important to point out here that although the problem of secure communication over quantum AVWC has been recently solved in [15, 16, 17], the extension of these results to list decoding seems to be a very challenging problem. Moreover, the capacity regions for transmitting different kinds of messages (public, private and confidential) [18] over AVWCs is still unknown.

Before, we present our model, we need to highlight some important notations. For every finite set $\mathcal{A}$ and $n \in \mathbb{N}$,

This research was initiated by the Bundesamt für Sicherheit in der Informationstechnik (BSI). The work of H. Boche was supported by the German Ministry of Education and Research (BMBF) under Grant 01BQ1050, while the work of A. S. Mansour was supported by the German Research Foundation (DFG) under Grants BO 1734/23-1 and BO 1734/24-1.

$\mathcal{P}(A)$ denotes the set of probability distributions on $\mathcal{A}$, while $\mathcal{P}_0^n(A)$ denotes the set of empirical distributions arising from all elements $a^n \in \mathcal{A}^n$. For two conditional distributions $p \in \mathcal{P}(\mathcal{A}|\mathcal{B})$ and $q \in \mathcal{P}(\mathcal{B}|\mathcal{C})$, we define $p \circ q \in \mathcal{P}(\mathcal{A}|\mathcal{C})$ to be a conditional distribution given by $p \circ q(a|c) = \sum_{b\in\mathcal{B}} p(a|b)q(b|c)$. While, for the distributions $p \in \mathcal{P}(\mathcal{A})$ and $q \in \mathcal{P}(B)$, we define $p \otimes q \in \mathcal{P}(\mathcal{A} \times \mathcal{B})$ to be the product distribution defined as follows: $p \otimes q(a, b) = p(a)q(b)$. Additionally, we define the conditional distribution $Id \in \mathcal{P}(\mathcal{A}|\mathcal{A})$, where $Id(a|\bar{a}) = 1$ if and only if $a = \bar{a}$.

2. SYSTEM MODEL

2.1. Arbitrarily Varying Wiretap Channels

Consider a communication scenario in which the channel undergoes two classes of attacks at the same time. The first attack is carried out by an active adversary also known as the jammer that can maliciously manipulate the channel state for each channel use. Simultaneously, a passive eavesdropper tries to extract some information about the transmitted message. This scenario is perfectly modeled by the concept of AVWCs as follows: For a finite state set $\mathcal{S}$, the jammer selects a certain channel state sequence $s^n \in \mathcal{S}^n$ of length n, which identifies the legitimate channel $\mathrm{W}_{s^n}^n(y^n|x^n)$ and the eavesdropper channel $\mathrm{V}_{s^n}^n(z^n|x^n)$, for all input and output sequences $x^n \in \mathcal{X}^n$, $y^n \in \mathcal{Y}^n$ and $z^n \in \mathcal{Z}^n$.

Definition 1. *A discrete memoryless arbitrarily varying wiretap channel (AVWC) is denoted by the pair $(\mathfrak{W}, \mathfrak{V})$ and is given by the family of pairs with common input as*

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

Our aim is to establish a reliable communication between the transmitter and the legitimate receiver for all state sequences $s^n \in \mathcal{S}^n$ selected by the jammer, while keeping the eavesdropper completely ignorant about the transmitted information. In order to understand the role played by the jammer, we need to highlight the concept of a symmetrizable AVC as introduced in [6].

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

$$\sum_{s\in\mathcal{S}} \mathrm{W}_s(y|x)\sigma(s|\tilde{x}) = \sum_{s\in\mathcal{S}} \mathrm{W}_s(y|\tilde{x})\sigma(s|x) \tag{1}$$

holds for every $x, \tilde{x} \in \mathcal{X}$ and $y \in \mathcal{Y}$.

The condition in (1) implies that a symmetrizable AVC can emulate a valid channel input making it impossible for the decoder to differentiate between the channel input x and the channel state s. It has been shown that uncorrelated codes with a pre-specified encoder-decoder pair fail to establish a reliable communication over AVWCs, if the legitimate AVC $\mathfrak{W}$ is symmetrizable [7, 12]. Unfortunately, a lot of channels of practical relevance fall into the class of symmetrizable channels [19]. To overcome this issue, correlated random codes in which the transmitter and the receiver coordinate their choice of an encoder-decoder pair based on a particular realization of a shared common randomness were used. However, correlated random codes only work under the assumption of restricted communication between the eavesdropper and the jammer [20].

2.2. List Codes

List codes are a special class of uncorrelated codes, in which the decoder outputs a list of L possible messages, instead of deciding on exactly one message. They have been used to overcome the problem of uncorrelated codes with symmetrizable AVCs [9, 10]. In this paper, we extend this usage to the problem of secure communication over AVWCs.

Definition 3. *A list code $\mathcal{C}_{list}$ with list size L for the AVWC $(\mathfrak{W}, \mathfrak{V})$ consists of: a set of confidential messages $\mathcal{M}$, a stochastic encoder $E : \mathcal{M} \to \mathcal{P}(\mathcal{X}^n)$, and a list decoder $\varphi_L : \mathcal{Y}^n \to \mathfrak{P}_L(\mathcal{M})$, where $\mathfrak{P}_L(\mathcal{M})$ is the set of all subsets of $\mathcal{M}$ with cardinality at most L.*

The reliability performance of $\mathcal{C}_{\text{list}}$ is measured in terms of its average error probability $\bar{e}_L(\mathcal{C}_{\text{list}})$ as follows:

$$\begin{aligned}\bar{e}_L(\mathcal{C}_{\text{list}}) &= \max_{s^n\in\mathcal{S}^n} \bar{e}_L(s^n|\mathcal{C}_{\text{list}}) \\ &= \max_{s^n\in\mathcal{S}^n} \frac{1}{|\mathcal{M}|} \sum_m \sum_{x^n} \sum_{y^n:\varphi_L(y^n)\not\ni m} \mathrm{W}_{s^n}^n(y^n|x^n)E(x^n|m).\end{aligned}$$

On the other hand, the secrecy performance of $\mathcal{C}_{\text{list}}$ is guaranteed by assuring that the information leakage of the confidential message M to the eavesdropper with respect to the strong secrecy criterion is small as follows:

$$\lim_{n\to\infty} \max_{s^n\in\mathcal{S}^n} \mathbb{I}(\mathrm{M}; \mathrm{Z}_{s^n}^n|\mathcal{C}_{\text{list}}) = 0, \tag{2}$$

where $\mathrm{Z}_{s^n}^n$ is the channel observation of the eavesdropper for state sequence s^n.

Definition 4. *A non-negative number R is an achievable list secrecy rate for the AVWC $(\mathfrak{W}, \mathfrak{V})$ with list size L, if for all $\tau > 0$ and all $\lambda, \delta \in (0, 1)$, there is an $n(\tau, \lambda, \delta) \in \mathbb{N}$, such that for all $n > n(\tau, \lambda, \delta)$, there exists a sequence of list codes $(\mathcal{C}_{list})_n$, that satisfies the following:*

$$\frac{1}{n} \log \frac{|\mathcal{M}|}{L} \geq R - \tau \tag{3}$$

$$\max_{s^n\in\mathcal{S}^n} \bar{e}_L(s^n|\mathcal{C}_{list}) \leq \lambda \tag{4}$$

$$\max_{s^n\in\mathcal{S}^n} \mathbb{I}(\mathrm{M}; \mathrm{Z}_{s^n}^n|\mathcal{C}_{list}) \leq \delta. \tag{5}$$

The list secrecy capacity $C_S(\mathfrak{W}, \mathfrak{V}, L)$ is given by the supremum of all achievable list secrecy rates R.

In order to investigate the list capacity region, we need a generalization of the concept of symmetrizability as follows:

Definition 5. *An AVC $\mathfrak{W}$ is L-symmetrizable, if there exists an auxiliary channel $\sigma : \mathcal{X}^L \to \mathcal{P}(\mathcal{S})$, such that for every permutation π of the sequence $(1, \dots, L+1)$*

$$\sum_{s\in\mathcal{S}} \mathrm{W}_s(y|x_1)\sigma(s|x_2,\dots,x_{L+1}) = \sum_{s\in\mathcal{S}} \mathrm{W}_s(y|x_{\pi(1)})\sigma(s|x_{\pi(2)},\dots,x_{\pi(L+1)}) \quad (6)$$

holds for every $x^{L+1} \in \mathcal{X}^{L+1}$ and $y \in \mathcal{Y}$.

For a given AVC, the largest L for which this AVC is L-symmetrizable is called the order of symmetrizability and is denoted by $L(G)$.

3. LIST SECRECY CAPACITY OF THE AVWC

3.1. Main Result

For an AVWC $(\mathfrak{W}, \mathfrak{V})$, we define the following multi-letter expression:

$$C_S^*(\mathfrak{W},\mathfrak{V}) = \lim_{n\to\infty} \frac{1}{n} \max_{p\in\mathcal{P}(\mathcal{U}_n)} \max_{p_n\in\mathcal{P}(\mathcal{X}^n|\mathcal{U}_n)} \Big(\min_{q\in\mathcal{P}(\mathcal{S}^n)} \mathbb{I}(\mathrm{U}_n;\mathrm{Y}_q^n) - \max_{s^n\in\mathcal{S}^n} \mathbb{I}(\mathrm{U}_n;\mathrm{Z}_{s^n}^n)\Big). \quad (7)$$

Theorem 1. *The list secrecy capacity $C_S(\mathfrak{W},\mathfrak{V},L)$ of the AVWC $(\mathfrak{W},\mathfrak{V})$ is characterized by the following:*

$$C_S(\mathfrak{W},\mathfrak{V},L) = \begin{cases} 0 & \text{if } L \le L(G) \\ C_S^*(\mathfrak{W},\mathfrak{V}) & \text{if } L > L(G). \end{cases}$$

Theorem 1 implies that for an AVWC with an order of symmetrizability $L(G)$, a list code with list size $L > L(G)$ can provide a reliable and secure communication at the rate given by (7) which is equivalent to the correlated random secrecy capacity cf. [12]. This implies that with the proper selection of the list size L, we can always achieve the correlated random secrecy capacity even in the absence of a shared randomness between the transmitter and the legitimate receiver. Additionally, list codes do not enforce any restrictions on the communication between the eavesdropper and the jammer.

Coding Problem: We consider a coding scheme that combines the reliability list decoding scheme for a non L-symmetrizable AVC introduced in [10] and the strong secrecy techniques introduced in [11, 12]. The main issue of using this approach is that the rate in (7) is calculated with respect to the AVWC $(\mathfrak{W}\circ p_n, \mathfrak{V}\circ p_n)$ that arises from using the prefix channel $\mathcal{P}(\mathcal{X}^n|\mathcal{U}_n)$. It was shown in [12] that using a prefix channel can change a non-symmetrizable AVC to a symmetrizable one. This implies that, even if $\mathfrak{W}$ is not L-symmetrizable, $\mathfrak{W}\circ p_n$ might be one.

In order to solve this issue, we adapt the coding technique introduced in [12] to the concept of list decoding as follows: We restrict the calculation of $C_S^*(\mathfrak{W},\mathfrak{V})$ to a family of prefix channels given by $p_n' = Id \otimes p_{2,\dots,n}$. We then show that calculating $C_S^*(\mathfrak{W},\mathfrak{V})$, using this family of prefix channels is asymptotically as good as using the full set of prefix channels $\mathcal{P}(\mathcal{X}^n|\mathcal{U}_n)$. In addition, this family of prefix channels assures that $\mathfrak{W}\circ p_n'$ is not L-symmetrizable as long as $\mathfrak{W}$ is not.

3.2. Important Tools

Before we present the proof of Theorem 1, we need to highlight some of the main tools that play an important role in establishing our coding theorem.

Lemma 1. *[9, Lemma 1] [10, Lemma 4] For a given AVC $\mathfrak{W}$, if $\mathfrak{W}$ is L-symmetrizable, then the list capacity with list size L vanishes, i.e. $C(\mathfrak{W},L) = 0$.*

This lemma is an extension of the result established in [6, Theorem 1], where it was shown that symmetrizability makes it impossible to establish a reliable message transmission using uncorrelated codes.

Lemma 2. *[10, Lemma 3] For an AVC $\mathfrak{W}$ with an order of symmetrizability $L(G)$, let $L = L(G)+1$. Then for any $\delta,\gamma > 0$, there exists a list code $\mathcal{C}_{list}$ with list size L and block length n such that $\bar{e}_L(\mathcal{C}_{list}) < 2^{-n\gamma}$, as long as*

$$\min_{q\in\mathcal{P}(\mathcal{S})} \mathbb{I}(\mathrm{X};\mathrm{Y}_q) - \delta < \frac{1}{n}\log\frac{|\mathcal{M}|}{L} < \min_{q\in\mathcal{P}(\mathcal{S})} \mathbb{I}(\mathrm{X};\mathrm{Y}_q) - \frac{2\delta}{3}.$$

This lemma was proved in [10] by using a collection of codewords $x^n(m)$ that satisfy the constraints in [10, Lemma 4]. In addition to the previous two lemmas, we will need to extend the list decoder introduced in [10, Definition 4] such that instead of having one message $m \in \mathcal{M}$, we have a two messages $m \in \mathcal{M}$ and $m_r \in \mathcal{M}_r$. Finally, we highlight the following secrecy lemma:

Lemma 3. *[12, Lemma 2] For any $\tau > 0$, there exists a value $\delta_\tau > 0$ and an $n_0(\tau)$, such that for all $n \ge n_0(\tau)$, there exist codewords $x^n(m,m_r) \in \mathcal{T}_{\mathrm{X}}^n \subset \mathcal{X}^n$ where $\mathcal{T}_{\mathrm{X}}^n$ is the set of typical sequences of length n, such that for an AVC $\mathfrak{V}$, we have for all $s^n \in \mathcal{S}^n$ and $m \in \mathcal{M}$*

$$\text{if } \frac{\log|\mathcal{M}_r|}{n} \ge \max_{q\in\mathcal{P}(\mathcal{S})} \mathbb{I}(\mathrm{X};\mathrm{Z}_q) + \tau, \text{ then}$$

$$\left\| \frac{1}{|\mathcal{M}_r|} \sum_{m_r=1}^{|\mathcal{M}_r|} \mathrm{V}_{s^n}(\cdot|x^n(m,m_r)) - \mathbb{E}\left[\mathrm{V}_{s^n}(\cdot|\mathrm{X}^n)\right] \right\|_1 \le 2^{-n\delta_\tau}$$

where $\mathbb{E}[\cdot]$ is the expectation, X^n is distributed according to $\mathbb{P}(\mathrm{X}^n = x^n) := \frac{1}{|\mathcal{T}_{\mathrm{X}}^n|}\mathbb{1}_{\mathcal{T}_{\mathrm{X}}^n}(x^n)$ and $\lim_{\tau\to 0}\delta_\tau = 0$.

3.3. Proof of Theorem 1

For the achievability, we will only focus on the case where the AVC $\mathfrak{W}$ is not L-symmetrizable and present the following coding scheme:

1) Prefix Channel: We start by considering the input distributions p and the conditional distributions p_n arising from the optimization problem in (7). Without loss of generality, for every $r \in \mathbb{N}$, let $\mathcal{U}_r = \mathcal{X}^r$ and define the following:

$$C_r \coloneqq \max_{p\in\mathcal{P}(\mathcal{U}_r)} \max_{p_r\in\mathcal{P}(\mathcal{X}^r|\mathcal{U}_r)} \Big(\min_{q\in\mathcal{P}(\mathcal{S}^r)} \mathbb{I}(\mathrm{U}_r;\mathrm{Y}_q^r) - \max_{s^r\in\mathcal{S}^r} \mathbb{I}(\mathrm{U}_r;\mathrm{Z}_{s^r}^r)\Big), \quad (8)$$

where $\mathrm{W}_q^r(y^r|x^r) = \sum_{s^r} q(s^r)\mathrm{W}_{s^r}^r(y^r|x^r)$. Then, for an arbitrary but fixed $r \in \mathbb{N}$ and an arbitrary $\epsilon \geq 0$, let $p^* \in \mathcal{P}(\mathcal{U}_r)$ and $p_r^* \in \mathcal{P}(\mathcal{X}^r|\mathcal{U}_r)$ be such that

$$C_r - \epsilon = \min_{q\in\mathcal{P}(\mathcal{S}^r)} \mathbb{I}(\mathrm{U}_r^*;\mathrm{Y}_q^r) - \max_{s^r\in\mathcal{S}^r} \mathbb{I}(\mathrm{U}_r^*;\mathrm{Z}_{s^r}^r).$$

Now, let $\tilde{p} \in \mathcal{P}(\mathcal{U}_{r+1})$, such that $\tilde{p} \coloneqq \pi \otimes p^*$, where $\pi \in \mathcal{P}(\mathcal{X})$ is defined as $\pi(x) \coloneqq |\mathcal{X}|^{-1}$ and $\tilde{p}_{r+1} \in \mathcal{P}(\mathcal{X}^{r+1}|\mathcal{X}\times\mathcal{U}_r)$, such that $\tilde{p}_{r+1} \coloneqq \sigma \otimes p_r^*$, where $\sigma \in \mathcal{P}(\mathcal{X}|\mathcal{X})$ is defined as $\sigma(x|\bar{x}) = 1$ iff $x = \bar{x}$. Then, from (8), it holds that

$$\begin{aligned} C_{r+1} &\geq \min_{q\in\mathcal{P}(\mathcal{S}^{r+1})} \mathbb{I}(\tilde{\mathrm{U}}_{r+1};\mathrm{Y}_q^{r+1}) - \max_{s^{r+1}\in\mathcal{S}^{r+1}} \mathbb{I}(\tilde{\mathrm{U}}_{r+1};\mathrm{Z}_{s^{r+1}}^{r+1}) \\ &\overset{(a)}{=} \min_{q\in\mathcal{P}(\mathcal{S}^{r+1})} \mathbb{I}(\mathrm{U}_r^*\mathrm{X}_\pi;\mathrm{Y}_q^{r+1}) - \max_{s^{r+1}\in\mathcal{S}^{r+1}} \mathbb{I}(\mathrm{U}_r^*\mathrm{X}_\pi;\mathrm{Z}_{s^{r+1}}^{r+1}) \\ &\overset{(b)}{\geq} \min_{q\in\mathcal{P}(\mathcal{S}^r)} \mathbb{I}(\mathrm{U}_r^*;\mathrm{Y}_q^r) - \max_{s^r\in\mathcal{S}^r} \mathbb{I}(\mathrm{U}_r^*;\mathrm{Z}_{s^r}^r) - \log|\mathcal{X}| \\ &= \quad C_r - \epsilon - \log|\mathcal{X}| \end{aligned} \quad (9)$$

where (a) follows from the definition of $\tilde{p}$ and $\tilde{p}_{r+1}$; (b) follows from the mutual information chain rule and the fact that $\mathbb{I}(\mathrm{X}_\pi;\mathrm{Z}_{s_1}) \leq \log|\mathcal{X}|$. Since $\mathfrak{W}$ is not L-symmetrizable, it follows that for every $r \geq 2$, the AVC $(\mathfrak{W}^{\otimes r}\circ\tilde{p}_r)$ is not L-symmetrizable as well.

2) Coding for the AVWC $(\mathfrak{W}^{\otimes r}\circ\tilde{p}_r, \mathfrak{V}^{\otimes r}\circ\tilde{p}_r)$: For every $t \in \mathbb{N}$ and $r \in \mathbb{N}\backslash\{1\}$, let $p \in \mathcal{P}_0^t(\mathcal{U}_r)$ and use it to construct the set of codewords $u_r^t(m, m_r) \in T_p \subset \mathcal{U}_r^t$, for $m \in \mathcal{M}$ and $m_r \in \mathcal{M}_r$. Using the union bound, we can show that the constructed codewords will satisfy the constraints in [10, Lemma 4] and Lemma 3 with probability approaches one as $t \to \infty$. Now, given a confidential message $m \in \mathcal{M}$, the encoder chooses a randomization message $m_r \in \mathcal{M}_r$ uniformly at random then outputs the codeword $u_r^t(m, m_r)$. At the legitimate receiver, we use a list decoder φ_L similar to the one given by [10, Definition 4].

3) Reliability and secrecy analysis: Since the AVC $(\mathfrak{W}^{\otimes r}\circ\tilde{p}_r)$ is not L-symmetrizable, Lemma 2 implies that there exists a list code with list size L and block length t which can be used to transmit the messages (m, m_r) reliably, if

$$\liminf_{t\to\infty} \frac{1}{t}\log\frac{|\mathcal{M}||\mathcal{M}_r|}{L} = \min_{q\in\mathcal{P}(\mathcal{S}^r)} \mathbb{I}(\mathrm{U}_r;\mathrm{Y}_q^r) - \delta. \quad (10)$$

On the other hand, based on Lemma 3 along with the secrecy analysis in [12], the constructed code is asymptotically secure in the strong sense, as long as

$$\liminf_{t\to\infty} \frac{1}{t}\log|\mathcal{M}_r| \leq \max_{s^r\in\mathcal{S}^r} \mathbb{I}(\mathrm{U}_r;\mathrm{Z}_{s^r}^r) + 2\delta. \quad (11)$$

Now, let $p \in \mathcal{P}_0^t(\mathcal{U}_r)$ converges to $\tilde{p} \in \mathcal{P}(\mathcal{U}_r)$, such that $\tilde{p} = p^* \otimes \pi$, where π is as defined before and $p^* \in \mathcal{P}(\mathcal{U}_{r-1})$ being an optimal choice for the optimization problem in (8), then from (9), (10) and (11) we have

$$\liminf_{t\to\infty} \frac{1}{t}\log\frac{|\mathcal{M}|}{L} \geq C_{r-1} - \log|\mathcal{X}| - 3\delta. \quad (12)$$

4) From $(\mathfrak{W}^{\otimes r}\circ\tilde{p}_r, \mathfrak{V}^{\otimes r}\circ\tilde{p}_r)$ to $(\mathfrak{W}, \mathfrak{V})$: Let $\tilde{t} \in \{0, \ldots, r-1\}$, such that for every $n \in \mathbb{N}$, we define $n = t\cdot r + \tilde{t}$. Since we assumed without loss of generality that $\mathcal{U}_r = \mathcal{X}^r$, we can transform the constructed codewords $u_r^t(m, m_r)$ into $x^{t\cdot r}(m, m_r)$. We then construct the codewords $x^n(m, m_r)$ for $m \in \mathcal{M}$ and $m_r \in \mathcal{M}_r$ by concatenating a dummy codeword $x^{\tilde{t}}$ to the transformed codeword $x^{t\cdot r}(m, m_r)$. One can easily show that the dummy codeword $x^{\tilde{t}}$ will not affect the reliability and secrecy performance of the original code. This implies that the achievable rate for the AVWC $(\mathfrak{W}, \mathfrak{V})$ is given by:

$$\begin{aligned} R &= \liminf_{n\to\infty} \frac{1}{n}\log\frac{|\mathcal{M}|}{L} = \liminf_{t\to\infty} \frac{1}{t\cdot r + \tilde{t}}\log\frac{|\mathcal{M}|}{L} \\ &\geq \liminf_{t\to\infty} \frac{1}{r}\cdot\frac{1}{t}\cdot\frac{t}{t+1}\log\frac{|\mathcal{M}|}{L} = \liminf_{t\to\infty} \frac{1}{r}\cdot\frac{1}{t}\log\frac{|\mathcal{M}|}{L} \\ &= \frac{1}{r}(C_{r-1} - \log|\mathcal{X}| - 3\delta). \end{aligned} \quad (13)$$

Since $\lim_{r\to\infty}\frac{r-1}{r} = 1$, it follows that $C_S(\mathfrak{W}, \mathfrak{V}, L) \geq \lim_{r\to\infty}\frac{1}{r}C_r$. This completes our achievablity proof. One the other hand, the converse follows using the same steps used to establish the converse of the correlated random secrecy capacity in [11, Section VIII].

Finally, we need to highlight the main difference between this achievability proof and the one presented in [13] and why it is better to use a coding scheme like the one presented in this paper. In [13], we used a coding scheme that is based on the concatenation of a public list code and a correlated random secrecy code, where the public list code is used to establish the necessary common randomness required. Due to the dependence of this coding scheme on correlated random codes, it is only valid under the assumption of restricted communication between the jammer and the eavesdropper. Differently, the coding scheme presented in this paper is based on a pure list secrecy code. Thus, even if the eavesdropper and the jammer cooperate together, we can establish a reliable and secure communication over an AVWC.

4. REFERENCES

[1] R. F. Schaefer, H. Boche, A. Khisti, and H. V. Poor, *Information Theoretic Security and Privacy of Information Systems*, Cambridge University Press, 2017.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] E. MolavianJazi, M. Bloch, and J. N. Laneman, "Arbitrary jamming can preclude secure communication," in *Proceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, USA, September 2009, pp. 1069–1075.

[4] 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. 558–567, 1960.

[5] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, vol. 44, no. 2, pp. 159–175, 1978.

[6] I. Csiszar and P. Narayan, "The capacity of the arbitrarily varying channel revisited: positivity, constraints," *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 181–193, March 1988.

[7] I. Bjelaković, H. Boche, and J. Sommerfeld, "Capacity results for arbitrarily varying wiretap channels," in *Information Theory, Combinatorics, and Search Theory*, New York, NY, USA, 2013, pp. 123–144, Springer-Verlag.

[8] Z. Goldfeld, P. Cuff, and H. H. Permuter, "Arbitrarily varying wiretap channels with type constrained states," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7216–7244, December 2016.

[9] V. M. Blinovskii, P. Narayan, and M. S. Pinsker, "Capacity of the arbitrarily varying channel under list decoding," *Problems Inform. Transmission*, vol. 31, no. 2, pp. 99–113, 1995.

[10] B. L. Hughes, "The smallest list for the arbitrarily varying channel," *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 803–815, May 1997.

[11] M. Wiese, J. Nötzel, and H. Boche, "A channel under simultaneous jamming and eavesdropping attack – correlated random coding capacities under strong secrecy criteria," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3844–3862, July 2016.

[12] J. Nötzel, M. Wiese, and H. Boche, "The arbitrarily varying wiretap channel – secret randomness, stability, and super-activation," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3504–3531, June 2016.

[13] A. S. Mansour, H. Boche, and R. F. Schaefer, "Stabilizing the secrecy capacity of the arbitrarily varying wiretap channel and transceiver synchronization using list decoding," in *2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Sapporo, Japan, July 2017, pp. 1–5.

[14] A. S. Mansour, H. Boche, and R. F. Schaefer, "List decoding for arbitrarily varying wiretap channels," in *IEEE Conference on Communications and Network Security (CNS)*, Philadelphia, PA, USA, October 2016, pp. 611–615.

[15] H. Boche, M. Cai, C. Deppe, and J. Nötzel, "Classical–quantum arbitrarily varying wiretap channel: Ahlswede dichotomy, positivity, resources, super-activation," *Quantum Information Processing*, vol. 15, no. 11, pp. 4853–4895, November 2016.

[16] H. Boche, M. Cai, C. Deppe, and J. Nötzel, "Classical-quantum arbitrarily varying wiretap channel: common randomness assisted code and continuity," *Quantum Information Processing*, vol. 16, no. 1, January 2017.

[17] H. Boche, M. Cai, C. Deppe, and J. Nötzel, "Classical-quantum arbitrarily varying wiretap channel: Secret message transmission under jamming attacks," *Journal of Mathematical Physics*, vol. 58, no. 10, September 2017.

[18] R. F. Schaefer and H. Boche, "Physical layer service integration in wireless networks : Signal processing challenges," *IEEE Signal Processing Magazine*, vol. 31, no. 3, pp. 147–156, May 2014.

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

[20] H. Boche and R. F. Schaefer, "Capacity results and super-activation for wiretap channels with active wiretappers," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 9, pp. 1482–1496, September 2013.