THE SECRECY CAPACITY OF THE ARBITRARILY VARYING WIRETAP CHANNEL UNDER LIST DECODING

AHMED S. MANSOUR AND HOLGER BOCHE
Lehrstuhl für Theoretische Informationstechnik
Technische Universität München
80290 München, Germany

RAFAEL F. SCHAEFER
Information Theory and Applications Chair
Technische Universität Berlin
10587 Berlin, Germany

(Communicated by Vitaly Skachek)

ABSTRACT. We consider a communication scenario in which the channel undergoes two different classes of attacks at the same time: a passive eavesdropper and an active jammer. This scenario is modelled by the concept of arbitrarily varying wiretap channels (AVWCs). In this paper, we derive a full characterization of the list secrecy capacity of the AVWC, showing that the list secrecy capacity is equivalent to the correlated random secrecy capacity if the list size $L$ is greater than the order of symmetrizability of the AVC between the transmitter and the legitimate receiver. Otherwise, it is zero. Our result indicates that for a sufficiently large list size $L$, list codes can overcome the drawbacks of correlated and uncorrelated codes and provide a stable secrecy capacity for AVWCs. Furthermore, we investigate the effect of relaxing the reliability and secrecy constraints by allowing a non-vanishing error probability and information leakage on the list size $L$. We found that we can construct a list code whose rate is close to the correlated secrecy capacity using a finite list size $L$ that only depends on the average error probability requested. Finally, we point out that our capacity characterization is an important step in investigating the analytical properties of the capacity function such as: the continuity behavior, Turing computability and super-activation of parallel AVWCs.

1. INTRODUCTION

Communication systems nowadays require both reliable and secure information transmission. There is a common belief that establishing a reliable communication is much easier than assuring the secrecy of the communication especially for wireless channels. Over the last few decades, classical cryptographic techniques have been a useful tool to provide secrecy, in particular against eavesdroppers with limited computational powers. However, with the rapid progress in the fields of digital design and number theory, the need for additional secrecy techniques has increased [15]. Information theoretic security is considered as one of the most promising candidates.
to complement current cryptographic based systems [13, 14]. This is because it only depends on the physical characteristics of the channel and not on the capabilities of the eavesdroppers [5, 18, 24].

Information theoretic security was first studied by Wyner in [27], where he showed that secure communication can be established over a class of wiretap channel by exploiting the noise in the channel. Many researchers have extended Wyner’s work by investigating different scenarios of the wiretap channel. However, most of these works considered a wiretap channel, where the channel state is perfectly known by the transmitter. In real life communication scenarios such as fading channels, it is very difficult to acquire perfect channel state information as the channel usually varies over time. Additionally, some wiretap channels suffer from the presence of active jammers who are capable of maliciously manipulating the channel state in each channel use [21].

In order to capture the previous scenarios, the model of the arbitrarily varying channel (AVC) [3, 1, 11] and its corresponding wiretap channel (AVWC) [21, 2] were considered. An AVWC models a channel under two classes of attacks at the same time: an active jammer who maliciously manipulates the channel state and a passive eavesdropper [26] that listens to the transmitted signal. Our main task is to find a coding scheme that can overcome the different jamming strategies induced by the jammer, such that it establishes a reliable communication over the AVC between the transmitter and the legitimate receiver. Simultaneously, this coding scheme should assure the secrecy of the transmission against eavesdropping for all channel states.

Two main coding schemes have been used to investigate reliable communication over AVCs in [3, 1, 11]: uncorrelated and correlated random codes. It was shown in [3] that the availability of a correlated randomness between the transmitter and the receiver is crucial for the establishment of a reliable communication over AVCs. In fact, AVCs exhibit a dichotomy [1]: Their uncorrelated capacity either equals their correlated random capacity or it equals zero. This observation became clearer in [11], after showing that uncorrelated codes fail to establish a reliable communication over symmetrizable AVCs, while correlated random codes can overcome the symmetrizable problem. Beside correlated and uncorrelated codes, list codes have been a very useful tool for reliable communication over AVCs. It was shown in [4, 16] that if the list size $L$ is greater than the order of symmetrizability of the AVC then the list capacity is equivalent to the correlated random capacity, otherwise it is zero.

Similar to the non-secrecy case, uncorrelated and correlated random codes were the main coding scheme used to investigate secure communication over AVWCs [2, 26, 23]. It was shown therein that AVWCs exhibit the same dichotomy of the AVCs: Their uncorrelated secrecy capacity either equals their correlated random secrecy capacity or it vanishes. The results established in [26, 23] have some indications that constructing a coding scheme that can provide a reliable communication in the presence of an active jammer is more challenging than protecting this communication against passive eavesdropping. This is because jamming has a huge impact on the communication link as it can induce a symmetrizable channel making reliable communication impossible. On the contrary, one can always confuse the eavesdropper by employing wiretap coding with the appropriate amount of randomization resources according to the worst channel realization to the eavesdropper.
This observation motivates us to investigate the usage of list codes for secure communication over AVWCs. To the best of our knowledge, this investigation has never been considered in previous literature.

In this paper, we present a full characterization of the list secrecy capacity of an AVWC. We show that the list secrecy capacity is equivalent to the correlated random secrecy capacity if the list size $L$ is greater than the order of symmetrizability of the AVWC between the transmitter and the legitimate receiver, otherwise it is zero. This characterization indicates that list codes can provide a solution for the instability of the secrecy capacity of AVWCs under uncorrelated codes. This is because, if we choose the list size $L$ to be greater than the order of symmetrizability of the legitimate AVC, we can always achieve secrecy rates up to the correlated random secrecy capacity. However, it was shown in [4] that even for simple AVCs, the order of symmetrizability can be arbitrary large. This result motivates us to investigate another problem: For an AVWC, where we relax the reliability and secrecy constraints by allowing a non-vanishing error probability and information leakage, what is the maximum secrecy rate that we can achieve using list codes with finite list size $L$ that does not depend on the order of symmetrizability. For such scenario, we show that we can construct list codes with rate up to the correlated random secrecy capacity, where the list size $L$ only depends on the average error probability requested.

The rest of the paper is organized as follows: In Section 2, we describe the model of the AVWC and introduce the principle of correlated and uncorrelated codes along as the principle of list codes. In Section 3, we present our coding theorem that establishes a full characterization of the list secrecy capacity and gives a detailed proof for this theorem using two different coding schemes. In Section 4, we investigate the effect of relaxing the reliability and secrecy constraints on the list size $L$. Finally, we conclude the paper in Section 5.

Notation. In this paper, random variables are denoted by capital letters and their realizations by the corresponding lower case letters, while calligraphic letters are used to denote sets. Additionally, we use fraktur letters to denote a set of their realizations by the corresponding lower case letters, while calligraphic letters notations are used to denote sets. For a natural number $n$, we use $X^n$ to denote the sequence of random variables $(X_1, \ldots, X_n)$, where $X_i$ is the $i$th variable in the sequence. A probability distribution for the random variable $X$ is denoted by $P_X$, where $P_X(x)$ denotes the probability of the event: $\mathbb{P}[X = x]$. The set of all probability distributions on $\mathcal{X}$ is denoted by $\mathcal{P}(\mathcal{X})$, while we use $\mathcal{P}_0^0(\mathcal{X})$ to denote the set of types for all sequences $x^n \in \mathcal{X}^n$. For each distribution $P_X \in \mathcal{P}_0^0(\mathcal{X})$, we define the typical set $T_{P_X} = \{x^n : \hat{N}(\cdot|x^n) = P_X(\cdot)\}$, where $\hat{N}(\cdot|x^n)$ denotes the number of times the element $\hat{x}$ occurs in the sequence $x^n$. For the conditional distributions $P_{A|B} \in \mathcal{P}(\mathcal{A}|\mathcal{B})$ and $P_{B|C} \in \mathcal{P}(\mathcal{B}|\mathcal{C})$, we define $P_{A|C} = P_{A|B} \circ P_{B|C} \in \mathcal{P}(\mathcal{A}|\mathcal{C})$ as follows: $P_{A|C}(a|c) = \sum_{b \in \mathcal{B}} P_{A|B}(a|b) P_{B|C}(b|c)$. On the other hand, for the distributions $P_A \in \mathcal{P}(\mathcal{A})$ and $P_B \in \mathcal{P}(\mathcal{B})$, we define $P_{A,B} = P_A \otimes P_B \in \mathcal{P}(\mathcal{A} \times \mathcal{B})$ as follows: $P_{A,B}(a,b) = P_A(a) P_B(b)$. Additionally, for an alphabet $\mathcal{A}$, we define the conditional distribution $P_{A|A}^{id} \in \mathcal{P}(\mathcal{A}|\mathcal{A})$, such that $P_{A|A}^{id}(a|a) = 1$ if and only if $a = \bar{a}$. $\mathbb{R}_+$ is used to denote the set of non-negative real numbers. $\mathbb{H}(\cdot)$ and $I(\cdot; \cdot)$ are the traditional entropy and mutual information, while $\mathbb{E}[\cdot]$ is used to represent the expectation. Given two probability distributions $P_X, Q_X \in \mathcal{P}(\mathcal{X})$, we use $D(P_X \| Q_X)$ to denote the Kullback-Leibler divergence.
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 jammer that threatens the reliability of the communication by maliciously manipulating the channel state for each transmission. Simultaneously, a passive eavesdropper tries to extract any information about the transmitted message and consequently threatening the secrecy of the transmission. This communication scenario is shown in Fig. 1.

![Figure 1. Discrete memoryless arbitrarily varying wiretap channel (W, V).](image)

This scenario is perfectly captured by the model of the AVWC as follows: Let $S$ be a finite state set, while $X$, $Y$ and $Z$ represent finite input and output sets. For every state $s \in S$, the channel between the transmitter and the legitimate receiver is given by a stochastic matrix $W_s : X \to \mathcal{P}(Y)$, while the channel between the transmitter and the eavesdropper is given by a stochastic matrix $V_s : X \to \mathcal{P}(Z)$. Thus, for a state sequence $s^n \in S^n$ of length $n$ produced by the active jammer, an input sequence $x^n \in X^n$ produced by the transmitter, an output sequence $y^n \in Y^n$ observed by the legitimate receiver and an output sequence $z^n \in Z^n$ observed by the passive eavesdropper, we define the discrete memoryless channels

$$W^n_s(y^n|x^n) = \prod_{i=1}^{n} W_s(y_i|x_i) \quad \text{and} \quad V^n_s(z^n|x^n) = \prod_{i=1}^{n} V_s(z_i|x_i).$$

An AVWC is given by the collection of all channels in (1) for all possible state sequences $s^n$ as follows:

**Definition 2.1.** The discrete memoryless arbitrarily varying wiretap channel (AVWC) is denoted by the pair $(W, V)$ and is given by the family of pairs with common input as

$$(W, V) = \{(W^n_s, V^n_s) : s^n \in S^n, n = 1, 2, \ldots \},$$

where $W$ represents the AVC between the transmitter and the legitimate receiver, while $V$ represents the AVC between the transmitter and the eavesdropper.

Since the channel is memoryless, the behavior of the channel should depend on the number of times each channel state $s$ is imposed, and not on the order of these states. This observation motivates the introduction of the average channel. For any probability distribution $q \in \mathcal{P}(S)$, we define

$$W_q(y|x) = \sum_{s \in S} q(s)W_s(y|x) \quad \text{and} \quad V_q(z|x) = \sum_{s \in S} q(s)V_s(z|x).$$


In some literature, the average channel is defined over a block length $n$, such that for any probability distribution $\tilde{q} \in \mathcal{P}(\mathcal{S}^n)$, we have
\begin{align*}
W^n(y^n|x^n) &= \sum_{x^n \in \mathcal{X}^n} \tilde{q}(x^n) W^n_\sigma(y^n|x^n) \quad \text{and} \quad V^n(z^n|x^n) = \sum_{x^n \in \mathcal{X}^n} \tilde{q}(z^n) V^n_\sigma(z^n|x^n).
\end{align*}

Secure communication over an AVWC faces two challenges. The first one is due to the existence of the active jammer that aims to disturb any reliable communication over the AVC between the transmitter and legitimate receiver. The jammer carries out this role by selecting a certain jamming strategy, i.e., a channel state sequence $s^n \in \mathcal{S}^n$. In order to have a better understanding for the role of the jammer, we need to highlight the concept of a symmetrizable AVC introduced in [11].

**Definition 2.2.** An AVC $\mathfrak{W}$ is symmetrizable if there exists an auxiliary channel $\sigma : \mathcal{X} \to \mathcal{P}(\mathcal{S})$ such that
\begin{align*}
\sum_{s \in \mathcal{S}} W_s(y|x) \sigma(s|x) = \sum_{s \in \mathcal{S}} W_s(y|x) \sigma(s|x)
\end{align*}
holds for every $x, \tilde{x} \in \mathcal{X}$ and $y \in \mathcal{Y}$.

The condition in (4) implies that for a symmetrizable AVC, the jammer can select a certain jamming strategy which emulate a valid channel input. An example for a symmetrizable AVC was given in [23] as follows: Consider an AVC, where $\mathcal{S} = \mathcal{X} = \{1, 2\}$, while $\mathcal{Y} = \{1, 2, 3\}$. For $\epsilon \in [0, 1]$, our AVC $\mathfrak{W}$ is defined by the following two stochastic matrices:
\begin{align*}
W_1 &:= \begin{pmatrix} 0 & 1 - \epsilon \\ \epsilon & 0 \\ 1 - \epsilon & \epsilon \end{pmatrix} \quad W_2 := \begin{pmatrix} 1 - \epsilon & 0 \\ \epsilon & 1 - \epsilon \\ 0 & \epsilon \end{pmatrix}.
\end{align*}

One can easily show that for every $\epsilon \in [0, 0.5]$, there exists an auxiliary channel $\sigma : \mathcal{X} \to \mathcal{P}(\mathcal{S})$, such that the symmetrizability condition in (4) is satisfied. This is because the condition in (4) implies the following system of equations:
\begin{align*}
W_1(\cdot | 1) \sigma(1|2) + W_2(\cdot | 1) \sigma(2|2) = W_1(\cdot | 2) \sigma(1|1) + W_2(\cdot | 2) \sigma(2|1)
\end{align*}
This system of linear equations leads to the following auxiliary channel $\sigma$: $\sigma(1|1) \triangleq \epsilon/(1 - \epsilon)$ and $\sigma(1|2) \triangleq (1 - 2\epsilon)/(1 - \epsilon)$. This implies that for this class of AVC, there exists a jamming strategy that makes it impossible for the receiver to differentiate between the channel input $x$ and the channel state $s$. A generalization for the concept of symmetrizable AVCs was given in [4, 16] as follows:

**Definition 2.3.** 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 $\pi$ of the sequence $(1, \ldots, L + 1)$
\begin{align*}
\sum_{s \in \mathcal{S}} W_s(y|x_1) \sigma(s|x_2, \ldots, x_{L+1}) = \sum_{s \in \mathcal{S}} W_s(y|x_{\pi(1)} \sigma(s|x_{\pi(2)}, \ldots, x_{\pi(L+1)})
\end{align*}
holds for every $x_{L+1} \in \mathcal{X}^{L+1}$ and $y \in \mathcal{Y}$.

Similar to the implication of the symmetrizability condition in (4), the condition in (5) implies that an $L$-symmetrizable AVC can emulate $L$ valid replicas of the channel input. This implies that for a given observation at the receiver $y^n$, there exists $L + 1$ input sequences that might have been sent. For a given AVC $\mathfrak{W}$, the largest $L$ for which this AVC is $L$-symmetrizable is called the order of symmetrizability and is denoted by $L(\mathfrak{W})$. An example for $L$-symmetrizable AVC was given in [4, Theorem 5].
Remark 1. One can easily see that the $L$-symmetrizability condition in (5) simplifies to the symmetrizability condition in (4) for $L = 1$. Eq. (5) also implies that any $L$-symmetrizable channel is also an $L'$-symmetrizable one, for all $0 \leq L' \leq L$.

From the previous discussion, one can see how establishing a reliable communication over the AVC between the transmitter and legitimate receiver is not an easy task specially under the following assumption: We assume that the transmitter and the legitimate receiver know the state space $\mathcal{S}$, but have no knowledge about the actual state sequence $s^n$ selected by the jammer. We also assume that there is no a priori distribution that guides the production of the state sequence $s^n$.

The second challenge that faces secure communication over AVWCs is the existence of a passive eavesdropper that tries to extract any information about the transmitted message. Our target is to construct a coding scheme that can overcome the different jamming strategies induced by the jammer and consequently establishing a reliable communication between the transmitter and the legitimate receiver for all state sequences $s^n \in \mathcal{S}^n$. At the same time our coding scheme should be able to keep the eavesdropper completely ignorant about the information transmitted. One of the main factors that we need to consider during the construction of such coding scheme is what information is allowed to be shared between the eavesdropper and the jammer.

2.2. Code concepts. Two main coding techniques have been used to establish a reliable and secure communication over AVWCs. The first technique is based on uncorrelated codes, in which a predefined (encoder, decoder) pair is used throughout the whole transmission. The second technique is known as correlated random codes, in which an (encoder, decoder) pair is selected based on some sort of common randomness shared between the transmitter and the legitimate receiver.

Definition 2.4. An uncorrelated code $\mathcal{C}^u_{uc}$ for the AVWC $(\mathcal{W}, \mathcal{V})$ consists of: a set of confidential messages $\mathcal{M}_c$, a stochastic encoder

\begin{equation}
E : \mathcal{M}_c \rightarrow \mathcal{P}(\mathcal{X}^n)
\end{equation}

that maps a confidential message $m_c \in \mathcal{M}_c$ to a codeword $x^n(m_c) \in \mathcal{X}^n$ according to the conditional probability $E(x^n|m_c)$, and a deterministic decoder

\begin{equation}
\varphi : \mathcal{Y}^n \rightarrow \mathcal{M}_c \cup \{?\}
\end{equation}

that maps each channel observation at the legitimate receiver to the corresponding intended message or an error message.

Now, in order to measure the reliability performance of an uncorrelated code $\mathcal{C}^u_{uc}$, we use the average probability of decoding error given by:

\begin{equation}
\tilde{e}(\mathcal{C}^u_{uc}) = \max_{s^n \in \mathcal{S}^n} \tilde{e}(s^n|\mathcal{C}^u_{uc})
= \max_{s^n \in \mathcal{S}^n} \frac{1}{|\mathcal{M}_c|} \sum_{m_c} \sum_{x^n} \sum_{y^n: \varphi(y^n) \neq m_c} W_s^n( y^n|x^n) E(x^n|m_c).
\end{equation}

On the other hand, the secrecy performance of $\mathcal{C}^u_{uc}$ is measured by investigating the information leakage of the confidential message to the eavesdropper for every state sequence $s^n \in \mathcal{S}^n$ with respect to the strong secrecy criterion as follows:

\begin{equation}
L(\mathcal{C}^u_{uc}) = \max_{s^n \in \mathcal{S}^n} L(s^n|\mathcal{C}^u_{uc})
= \max_{s^n \in \mathcal{S}^n} I(M_c; Z^n_s|\mathcal{C}^u_{uc}),
\end{equation}
where $M_c$ represents a uniformly distributed random variable over the confidential messages set $\mathcal{M}_c$, while $Z_{sn}^n$ is a random variable for the channel observation at the eavesdropper for state sequence $s^n$.

**Definition 2.5.** A non-negative number $R_{\text{uc}}^s$ is an achievable secrecy rate for the AVWC $(\mathcal{W}, \mathcal{V})$ if for all $\delta, \lambda, \tau > 0$ there is an $n(\delta, \lambda, \tau) \in \mathbb{N}$, such that for all $n > n(\tau, \lambda, \delta)$, there exists a sequence of uncorrelated codes $(C_{\text{uc}}^s)_n$ that satisfies the following constraints:

\begin{align*}
\frac{1}{n} \log |M_c| &\geq R_{\text{uc}}^s - \delta, \\
\bar{e}(C_{\text{uc}}^s) &\leq \lambda, \\
L(C_{\text{uc}}^s) &\leq \tau.
\end{align*}

The uncorrelated secrecy capacity $C_{\text{uc}}^s(\mathcal{W}, \mathcal{V})$ is given by the supremum of all achievable secrecy rates $R_{\text{uc}}^s$.

In [23], the uncorrelated secrecy capacity was established using a coding scheme that does not enforce any restrictions on the information shared between the eavesdropper and the jammer. In particular, the eavesdropper is allowed to know the jamming strategy used to manipulate the channel state or even the exact channel state selected by the jammer. At the same time, the jammer is allowed to know any information possessed by the eavesdropper. Nevertheless, it has been shown in [2, 11, 23] that uncorrelated codes can not establish reliable communication over AVWC, if the AVC between the transmitter and the legitimate receiver is symmetrizable. Unfortunately, a lot of channels of practical relevance fall into the class of symmetrizable AVCs [17].

**Definition 2.6.** A correlated random code $C_{\text{cr}}^s$ for the AVWC $(\mathcal{W}, \mathcal{V})$ consists of:

- a set of confidential messages $M_c$,
- a set $\mathcal{G}$ of values of the common randomness, a probability distribution $P_\Gamma$ that guides the selection of a certain realization of the common randomness $\gamma \in \mathcal{G}$, a set of stochastic encoders $E^{\gamma} : M_c \rightarrow \mathcal{P}(\mathcal{X}^n)$, that maps a confidential message $m_c \in M_c$ to a codeword $x^n(m_c) \in \mathcal{X}^n$ according to the conditional probability $E^{\gamma}(x^n|m_c)$ and a set of deterministic decoders $\varphi^{\gamma} : \mathcal{Y}^n \rightarrow M_c \cup \{?\}$, that maps each channel observation at the legitimate receiver to the corresponding intended message or an error message.

The previous definition implies that any correlated random code $C_{\text{cr}}^s$ can be interpreted as a family of uncorrelated codes of Definition 2.4 as follows:

\begin{align*}
C_{\text{cr}}^s = \{C_{\text{uc}}^s(\gamma) : \gamma \in \mathcal{G}\}.
\end{align*}

Similar to uncorrelated codes, we use the average probability of decoding error to evaluate the reliability performance of a correlated random code $C_{\text{cr}}^s$ as follows:

\begin{align*}
\bar{e}(C_{\text{cr}}^s) = \max_{s^n \in S^n} \bar{e}(s^n|C_{\text{cr}}^s) \quad &= \max_{s^n \in S^n} \frac{1}{|M_c|} \sum_{m_c} \sum_{\gamma} \sum_{x^n} \sum_{y^n : \varphi^{\gamma}(y^n) \neq m_c} W^{n}_n(y^n|x^n) E^{\gamma}(x^n|m_c) P_\Gamma(\gamma).
\end{align*}

On the other hand, the secrecy performance of $C_{\text{cr}}^s$ is evaluated with respect to two secrecy criteria. The first criterion is called the mean secrecy criterion and is
measured by the investigating the average information leakage of the confidential message to the eavesdropper with respect to the strong secrecy criterion, for every state sequence \( s^n \in S^n \) over all realizations of the shared common randomness \( \gamma \in \mathcal{G} \) as follows:

\[
L_{\text{mean}}(C_{s, \text{cr}}) = \max_{s^n \in S^n} \sum_{\gamma} I(M_c; Z^n_{s^n, \gamma} | C_{s, \text{cr}}) P_{\Gamma}(\gamma),
\]

where \( Z^n_{s^n, \gamma} \) is the channel output at the eavesdropper for a state sequence \( s^n \), when the encoder \( E_{\gamma} \) is used. The second criterion is more conservative criterion known as the maximum secrecy criterion and is given by

\[
L_{\text{max}}(C_{s, \text{cr}}) = \max_{s^n \in S^n} L_{\text{max}}(s^n | C_{s, \text{cr}}) = \max_{s^n \in S^n} \max_{\gamma \in \mathcal{G}} I(M_c; Z^n_{s^n, \gamma} | C_{s, \text{cr}}).
\]

It is important to highlight that both secrecy criteria assume that the eavesdropper has an access to the common randomness shared between the transmitter and the legitimate receiver. However, the mean secrecy criterion puts the distribution \( P_{\Gamma} \) into consideration, while the maximum secrecy criterion considers the information leakage for every realization \( \gamma \). It is also fair to assume that the eavesdropper has access to the shared common randomness because otherwise the transmitter and the legitimate receiver can use this common randomness to implement alternative secure encoding schemes such as one time pad, where the common randomness is used as a shared secret key.

**Definition 2.7.** A non-negative number \( R_{s, \text{mean}}(C_{s, \text{cr}}) \) is an achievable mean secrecy rate for the AVWC \((W, V)\) if for all \( \delta, \lambda, \tau > 0 \) there is an \( n(\delta, \lambda, \tau) \in \mathbb{N} \), such that for all \( n > n(\tau, \lambda, \delta) \), there exists a sequence of correlated random codes \( (C_{s, \text{cr}})^n \) that satisfies the following constraints:

\[
\frac{1}{n} \log |\mathcal{M}_c| \geq R_{s, \text{mean}}(C_{s, \text{cr}}) - \delta,
\]

\[
\bar{e}(C_{s, \text{cr}}) \leq \lambda,
\]

\[
L_{\text{mean}}(C_{s, \text{cr}}) \leq \tau.
\]

The correlated random mean secrecy capacity \( C_{s, \text{mean}}(W, V) \) is given by the supremum of all achievable mean secrecy rates \( R_{s, \text{mean}}(C_{s, \text{cr}}) \).

**Definition 2.8.** A non-negative number \( R_{s, \text{max}}(C_{s, \text{cr}}) \) is an achievable max secrecy rate for the AVWC \((W, V)\) if for all \( \delta, \lambda, \tau > 0 \) there is an \( n(\delta, \lambda, \tau) \in \mathbb{N} \), such that for all \( n > n(\tau, \lambda, \delta) \), there exists a sequence of correlated random codes \( (C_{s, \text{cr}})^n \) that satisfies the constraints in (19) and (20), in addition to:

\[
L_{\text{max}}(C_{s, \text{cr}}) \leq \tau.
\]

The correlated random max secrecy capacity \( C_{s, \text{max}}(W, V) \) is given by the supremum of all achievable max secrecy rates \( R_{s, \text{max}}(C_{s, \text{cr}}) \).

**Remark 2.** Although it is immediately clear that \( C_{s, \text{mean}}(W, V) \geq C_{s, \text{max}}(W, V) \), it was shown in [26, Theorem 6] that both secrecy capacities are equivalent. Thus, throughout the rest of the paper we will use \( C_{s, \text{cr}}(W, V) \) to denote the correlated random secrecy capacity of the AVWC \((W, V)\).
Although it was shown in [1, 2] that correlated random codes can establish a reliable communication over symmetrizable AVWCs, the usage of correlated random codes in most practical scenarios is still questionable. This because as highlighted by Definition 2.6, correlated random codes require some sort of a pre-established coordination between the transmitter and the legitimate receiver which might not always be available. In addition, it was shown that the amount of the coordination resources needed \(|G|\) grows with the code block length \(n\) [2, 26].

The previous results were derived under the assumption of limited communication between the eavesdropper and the jammer. In particular, the jammer is allowed to inform the eavesdropper about the jamming strategy used or even the exact channel state selected, but the eavesdropper is not allowed to inform the jammer about the exact realization of the common randomness. This is because the reliability analysis provided in [2] is only valid, if the jammer chooses \(s^n \in \mathcal{S}^n\) independently from the confidential message \(m_c\) and the selected encoder \(E^\gamma\).

### 2.3. 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. Such codes have been used for the AVC without secrecy constraints to overcome the problem of uncorrelated codes with symmetrizability and the need of correlated random codes to a shared common randomness [4, 16, 22, 6]. We start by presenting the following definition.

**Definition 2.9.** A public list code \(\mathcal{C}_{\text{list}}\) with size \(L\) for the AVC \(\mathcal{W}\) consists of: a set of public messages \(\mathcal{M}_p\), a deterministic encoder 
\[
E : \mathcal{M}_p \rightarrow \mathcal{X}^n
\]
that maps a message \(m_p \in \mathcal{M}_p\) into a codeword \(x^n(m_p) \in \mathcal{X}^n\) and deterministic list decoder given by 
\[
\varphi_L : \mathcal{Y}^n \rightarrow \mathcal{J}_L(\mathcal{M}_p) \cup \{?\}
\]
that maps each channel observation at the receiver to a list of up to \(L\) messages or an error message, where \(\mathcal{J}_L(\mathcal{M}_p)\) is the set of all subsets of \(\mathcal{M}_p\) with cardinality at most \(L\).

The reliability performance of \(\mathcal{C}_{\text{list}}\) is measured in terms of its average probability of error given by:
\[
\bar{e}_L(\mathcal{C}_{\text{list}}) = \max_{s^n \in \mathcal{S}^n} \bar{e}_L(s^n|\mathcal{C}_{\text{list}}) = \max_{s^n \in \mathcal{S}^n} \frac{1}{|\mathcal{M}_p|} \sum_{m_p : y^n : \varphi_L(y^n) \neq m_p} W^n_s(y^n|x^n(m_p)).
\]

**Definition 2.10.** A non-negative number \(R_p\) is an achievable public list rate for the AVC \(\mathcal{W}\) if for all \(\delta, \lambda > 0\) there is an \(n(\tau, \lambda) \in \mathbb{N}\), such that for all \(n > n(\tau, \lambda)\), there exists a sequence of list codes \((\mathcal{C}_{\text{list}})_n\), such that the following holds:
\[
\frac{1}{n} \log \frac{|\mathcal{M}_p|}{L} \geq R_p - \delta,
\]

\[
\bar{e}(\mathcal{C}_{\text{list}}) \leq \lambda.
\]

The list capacity \(C_{\text{list}}(\mathcal{W}, L)\) is given by the supremum of all achievable rates \(R_p\).

Now, we extend the concept of list decoding to fit the model of secure communication over an AVWC as follows:
Definition 2.11. A confidential list code $C_{\text{list}}^s$ with list size $L$ for the AVWC $(\mathcal{W}, \mathcal{V})$ consists of: a set of confidential messages $\mathcal{M}_c$, a stochastic encoder
\[
E : \mathcal{M}_c \rightarrow \mathcal{P}(\mathcal{X}^n)
\]
that maps a confidential message $m_c \in \mathcal{M}_c$ to a codeword $x^n \in \mathcal{X}^n$ according to the conditional probability $E(x^n|m_c)$, and a deterministic list decoder with list size $L$
\[
\varphi_L : \mathcal{Y}^n \rightarrow \mathcal{J}_L(\mathcal{M}_c) \cup \{\}
\]
that maps a channel observation at the legitimate receiver into a list of up to $L$ messages or an error message, where $\mathcal{J}_L(\mathcal{M}_c)$ is the set of all subsets of $\mathcal{M}_c$ with cardinality at most $L$.

Similar to the non-secrecy case, we use the average error probability to measure the reliability performance of the list code $C_{\text{list}}^s$ as follows:
\[
\bar{e}_L(C_{\text{list}}^s) = \max_{s^n \in S^n} \bar{e}_L(s^n|C_{\text{list}}^s)
\]
\[
= \max_{s^n \in S^n} \frac{1}{|\mathcal{M}_c|} \sum_{m_c} \sum_{x^n} \sum_{y^n} W^n_s(y^n|x^n) E(x^n|m_c).
\]

One the other hand, we use the information leakage of the confidential message $M_c$ to the eavesdropper with respect to the strong secrecy criterion to investigate the secrecy performance of the list code $C_{\text{list}}^s$ as follows:
\[
L(C_{\text{list}}^s) = \max_{s^n \in S^n} L(s^n|C_{\text{list}}^s)
\]
\[
= \max_{s^n \in S^n} I(M_c; Z^n_s|C_{\text{list}}^s).
\]

Definition 2.12. A non-negative number $R_{\text{list}}^s$ is an achievable secrecy rate for the AVWC $(\mathcal{W}, \mathcal{V})$, if for all $\delta, \lambda, \tau > 0$ there is an $n(\delta, \lambda, \tau) \in \mathbb{N}$, such that for all $n > n(\tau, \lambda, \delta)$, there exists a sequence of list codes $(C_{\text{list}}^s)_n$ with list size $L$ that satisfies the following constraints:
\[
\frac{1}{n} \log \frac{|\mathcal{M}_c|}{L} \geq R_{\text{list}}^s - \delta,
\]
\[
\bar{e}_L(C_{\text{list}}^s) \leq \lambda,
\]
\[
L(C_{\text{list}}^s) \leq \tau.
\]
The list secrecy capacity $C_{\text{list}}^s(\mathcal{W}, \mathcal{V}, L)$ is given by the supremum of all achievable secrecy rates $R_{\text{list}}^s$.

We now introduce an additional coding scheme that can be used to transmit public and confidential messages at the same time. This scheme turns out to be very useful in some of the investigated scenarios of AVWCs.

Definition 2.13. A public-confidential list code $C_{\text{ps}}^s$ with size $L$ for the AVWC $(\mathcal{W}, \mathcal{V})$ consists of: a set of public messages $\mathcal{M}_p$, a set of confidential messages $\mathcal{M}_c$, a stochastic encoder
\[
E : \mathcal{M}_p \times \mathcal{M}_c \rightarrow \mathcal{P}(\mathcal{X}^n)
\]
that maps a public message $m_p \in \mathcal{M}_p$ and a confidential message $m_c \in \mathcal{M}_c$ into a codeword $x^n(m_p, m_c) \in \mathcal{X}^n$ according to the conditional probability $E(x^n|m_p, m_c)$ and a deterministic list decoder given by
\[
\varphi_L : \mathcal{Y}^n \rightarrow \mathcal{J}_L(\mathcal{M}_p \times \mathcal{M}_c) \cup \{\}
\]
that maps a channel observation at the legitimate receiver into a list of up to $L$ public and confidential message pairs or an error message, where $\mathcal{J}_L(\mathcal{M}_p \times \mathcal{M}_c)$ is the set of all subsets of $(\mathcal{M}_p \times \mathcal{M}_c)$ with cardinality at most $L$.

The reliability performance of $C_{\text{list}}^{\text{ps}}$ is measured in terms of its average probability of error given by:

$$
\bar{e}_L(C_{\text{list}}^{\text{ps}}) = \max_{s^n \in \mathcal{S}^n} \frac{1}{|\mathcal{M}_p||\mathcal{M}_c|} \sum_{m_p, m_c} \sum_{x^n} \sum_{y^n : \varphi_L(y^n) \neq (m_p, m_c)} W^n_s(y^n|x^n) E(x^n|m_p, m_c).
$$

On the other hand, the secrecy performance of $C_{\text{list}}^{\text{ps}}$ is measured with respect to two secrecy criteria. The first criterion is called the mean secrecy criterion and is given by:

$$
L_{\text{mean}}(C_{\text{list}}^{\text{ps}}) = \max_{s^n \in \mathcal{S}^n} \max_{m_p \in \mathcal{M}_p} I(M_c; \bar{Z}_s^n | M_p C_{\text{list}}^{\text{ps}})
$$

$$
= \max_{s^n \in \mathcal{S}^n} \frac{1}{|\mathcal{M}_p|} \sum_{m_p} I(M_c; \bar{Z}_s^n, m_p | C_{\text{list}}^{\text{ps}}),
$$

where $\bar{Z}_s^n, m_p$ is the channel output at the eavesdropper for the state sequence $s^n$ when the public message $m_p$ is transmitted. $L_{\text{mean}}(C_{\text{list}}^{\text{ps}})$ measures the information leakage of the confidential message $M_c$ to the eavesdropper averaged over the public message $M_p$. The second criterion investigates the information leakage of the confidential message $M_c$ to the eavesdropper at different values of the public message $m_p \in \mathcal{M}_p$, then uses the maximum leakage as a measure for the secrecy performance of $C_{\text{list}}^{\text{ps}}$. That is why it is called the maximum secrecy criterion and is given by

$$
L_{\text{max}}(C_{\text{list}}^{\text{ps}}) = \max_{s^n \in \mathcal{S}^n} \max_{m_p \in \mathcal{M}_p} \bar{e}_L(C_{\text{list}}^{\text{ps}})(m_p, m_c).
$$

The previous two secrecy criteria given in (33) and (34) are similar to the two secrecy criterion used to investigate the secrecy performance of a correlated random code given in (17) and (18) respectively.

**Definition 2.14.** A rate pair $(R_p, R_c^{\text{mean}}) \in \mathbb{R}_+^2$ is an achievable public-confidential rate for the AVWC $(\mathcal{W}, \mathcal{V})$ with list size $L$ with respect to the mean secrecy criterion, if for all $\tau, \sigma, \lambda, \delta > 0$, there is an $n(\tau, \sigma, \lambda, \delta) \in \mathbb{N}$, such that for all $n > n(\tau, \sigma, \lambda, \delta)$, there exists a sequence of list codes $(C_{\text{list}}^{\text{ps}})_n$, that satisfies the following:

$$
\frac{1}{n} \log \frac{|\mathcal{M}_c|}{L} \geq R_c^{\text{mean}} - \delta,
$$

$$
\frac{1}{n} \log \frac{|\mathcal{M}_p|}{L} \geq R_p - \sigma,
$$

$$
\bar{e}_L(C_{\text{list}}^{\text{ps}}) \leq \lambda,
$$

$$
\bar{e}_L(C_{\text{list}}^{\text{ps}}) \leq \tau.
$$

The public-confidential list mean secrecy capacity $C_{\text{list}}^{\text{ps,mean}}(\mathcal{W}, \mathcal{V}, L)$ is given by the supremum of all achievable mean confidential rates $R_c^{\text{mean}}$.

**Definition 2.15.** A rate pair $(R_p, R_c^{\text{max}}) \in \mathbb{R}_+^2$ is an achievable public-confidential rate for the AVWC $(\mathcal{W}, \mathcal{V})$ with list size $L$ with respect to the maximum secrecy criterion, if for all $\tau, \sigma, \lambda, \delta > 0$, there is an $n(\tau, \sigma, \lambda, \delta) \in \mathbb{N}$, such that for all...
n > n(\tau, \sigma, \lambda, \delta), there exists a sequence of list codes \((C_{\text{ps}})_{n}\), that satisfies (35), (36) and (37), in addition to
\[ L_{\text{max}}(C_{\text{ps}}) \leq \delta. \]

The public-confidential list maximum secrecy capacity \(C_{\text{ps, max}}(\mathcal{M}, \mathcal{V}, L)\) is given by the supremum of all achievable maximum confidential rates \(R_{c}^{\text{max}}\).

Remark 3. 1) Although one can easily notice that \(C_{\text{ps, mean}}(\mathcal{M}, \mathcal{V}, L) \geq C_{\text{ps, max}}(\mathcal{M}, \mathcal{V}, L)\), we will show that the two capacities are equivalent. This result is similar to the one established in [26, Theorem 6] for the mean and maximum correlated random secrecy capacity. Thus, throughout the rest of the paper, we will use the notation \(C_{\text{ps}}(\mathcal{M}, \mathcal{V}, L)\) to denote both the mean and maximum list secrecy capacity.

2) In this paper, we will limit our investigation to the case where the public rate \(R_{p}\) vanishes as \(n \to \infty\). For this case, it follows immediately that \(C_{\text{ps}}(\mathcal{M}, \mathcal{V}, L)\) and \(C_{\text{ps}}(\mathcal{M}, \mathcal{V}, L)\) are equivalent.

3) Since we limit our investigation to the scenario where \(\lim_{n \to \infty} R_{p} = 0\), one might wonder about the role played by the public message \(m_{p}\). In general, the public message \(m_{p}\) can be used to perform some services like synchronization and channel estimation. Such services are very important for any communication in practice, yet they do not have much impact on the rate.

3. List secrecy capacity of the AVWC

In this section, we present a full characterization of the list secrecy capacity for AVWCs \(C_{\text{ps}}(\mathcal{M}, \mathcal{V}, L)\) using two different coding scheme. We start by stating the main tools needed to derive our results. We then state our first coding theorem and present a detailed proof for it, in which we use a list code of Definition 2.11. We then turn to our second coding theorem, where we use a public-confidential list code of Definition 2.13, then limit our investigation to the case where the public rate vanishes. Finally, we discuss and compare the two coding schemes, showing that they both lead to the same list secrecy capacity.

3.1. Important tools. Before we present our main contribution, we highlight some of the previously established results for AVCs and AVWCs. We start by presenting a lemma that shows that reliable communication can not be established over an \(L\)-symmetrizable AVC using list codes with list size \(L\) as follows:

**Lemma 3.1.** [4, Lemma 1] [16, Lemma 4] For a given AVC \(\mathcal{M}\), if \(\mathcal{M}\) is \(L\)-symmetrizable, then the list capacity with list size \(L\) vanishes, i.e. \(C_{\text{list}}(\mathcal{M}, L) = 0\).

This lemma generalizes the result established in [11, Theorem 1] for uncorrelated codes which can be interpreted as list codes with list size \(L = 1\). The main idea of the proof is to show that if the AVC \(\mathcal{M}\) is \(L\)-symmetrizable, then for any list code \(C_{\text{list}}\) with list size \(L\), there exists a state sequence \(s^{n} \in S^{n}\) such that the average error probability is bounded away from zero, as \(n\) approaches infinity. In particular, we have
\[ \limsup_{n \to \infty} \bar{e}_{L}(C_{\text{list}}) \geq \liminf_{n \to \infty} \max_{s^{n} \in S^{n}} \bar{e}_{L}(s^{n}|C_{\text{list}}) \geq \frac{1}{L+1} > 0, \]
as long as the list size \(L\) is finite. This implies that no list code with list size \(L\) exists, such that the average decoding error probability vanishes as \(n \to \infty\), which
consequently means a zero capacity.

Next, we present the main tools that guides the encoding and decoding process for a list code $C^*$ of Definition 2.11. These tools help us to establish a reliable communication over an AVC $\mathcal{W}$ with an order of symmetrizability $L(\mathcal{W})$, using list codes with list size $L \geq L(\mathcal{W}) + 1$. We start by the encoding process and notice that $C^*$ requires a stochastic encoder as shown in (26). We transform this stochastic encoder to a deterministic one using a randomization message set $\mathcal{M}_r$ as follows:

$$E : \mathcal{M}_c \times \mathcal{M}_r \to \mathcal{X}^n.$$ 

We now present a lemma that guides the production of the codewords $x^n(m_c, m_r) \in \mathcal{X}^n$ that are produced by the previous encoder to construct the codebook of the list $C^*$.

**Lemma 3.2.** [16, Lemma 1] For any $L \geq 1$, $\epsilon > 0$ and $\beta > 0$, there exists an $n_0(\epsilon, L)$, such that for all $n \geq n_0(\epsilon, L)$, message sets $\mathcal{M}_c, \mathcal{M}_r$ satisfying $|\mathcal{M}_c| |\mathcal{M}_r| \geq L \cdot 2^n$ and type $P_X \in \mathcal{P}_0^L(\mathcal{X})$ satisfying $\min_{x : P_X(x) > 0} P_X(x) \geq \beta$, there exist codewords $x^n(m_c, m_r) \in T_{P_X} \subset \mathcal{X}^n$, for $m_c \in \mathcal{M}_c$ and $m_r \in \mathcal{M}_r$, such that upon setting $R = \frac{1}{n} \log \frac{|\mathcal{M}_c| |\mathcal{M}_r|}{L}$, we have for all $x^n \in T_{P_X}$, $s^n \in \mathcal{S}^n$ and the joint type $P_{X \times \mathcal{S}}$

$$|\{(m_c, m_r) : (x^n(m_c, m_r), s^n) \in T_{P_X s}\}| \leq |\mathcal{M}_c| |\mathcal{M}_r| 2^{-\frac{R}{2}},$$

(41)

if $I(X, S) \geq \epsilon$

$$|\{(m_c, m_r) : (x^n(m_c, m_r), x^n(\hat{m}_c, \hat{m}_r), s^n) \in T_{P_{X \times \mathcal{S}}} \text{ for some } (\hat{m}_c, \hat{m}_r) \neq (m_c, m_r)\}| \leq |\mathcal{M}_c| |\mathcal{M}_r| 2^{-\frac{R}{2}},$$

(42)

if $I(X; X \mathcal{S}) \geq |R - I(X_k; S)| + \epsilon$

$$|\{(m_c, m_r) : (x^n, x^n(m_c, m_r), s^n) \in T_{P_{X \mathcal{S}}}\}| \leq 2^n (|R - I(X_k; S)| + \epsilon)$$

(43)

for $k = 1, \ldots, L$. Moreover, if $R < \min_k I(X_k; S)$, then for $m_c \in \mathcal{M}_c$ and $m_r \in \mathcal{M}_r$, the codewords $x^n(m_c, m_r)$ can be selected to further satisfy

$$|\{|J : (x^n, x^n_J, s^n) \in T_{P_{X \mathcal{S}}}\}| \leq 2^{n\epsilon}$$

(44)

$$|\{(m_c, m_r) : (x^n(m_c, m_r), x^n_J, s^n) \in T_{P_{X \mathcal{S}}} \text{ and } (m_c, m_r) \notin J\}| \leq |\mathcal{M}_c| |\mathcal{M}_r| 2^{-\frac{R}{2}},$$

if $I(X; X \mathcal{S}) \geq \epsilon$

(45)

where $J = \{j_1, \ldots, j_L\} \in \mathcal{S}_L(\mathcal{M}_c \times \mathcal{M}_r)$ and $x^n_J$ denotes the ordered $L$-tuple $(x^n(j_1), \ldots, x^n(j_L))$.

The previous lemma can be viewed as a generalization of the result established in [11, Lemma 3] for uncorrelated codes, i.e. $L = 1$. In order to understand the role played by Lemma 3.2 in the encoding process of $C^*$, we need to analyze the statement of the lemma as follows:

**Assumptions.** Lemma 3.2 starts by defining a list size $L \geq 1$ that will be used during the decoding process. Then, for some constant $\epsilon > 0$, it defines the code block length $n$ to be sufficiently large, i.e. $n \geq n_0(\epsilon, L)$. Next, Lemma 3.2 addresses the messages needed to be transmitted from the sets $\mathcal{M}_c$ and $\mathcal{M}_r$, where a constraint on the product of the cardinality of the message sets must be fulfilled. Finally, Lemma 3.2 defines a probability distribution $P_X$ on $\mathcal{X}$, such that $P_X$ belongs to the set of types on $\mathcal{X}^n$ and the minimum non-zero probability of an element $x$ should be greater than or equal $\beta > 0$. 

**List decoding for AVWCs**

---

**Advances in Mathematics of Communications**

**Volume 13, No. 1 (2019), 11–39**
Results. For any sequence $x^n \in T_{P_X}$, a given sequence $s^n \in S^n$, a fixed type $P_{X^{X}S}$ and under the previous assumptions, Lemma 3.2 claims that using the probability distribution $P_X$, we can generate a random codebook $\{x^n(m_c,m_r) \in T_{P_X} : (m_c,m_r) \in M_c \times M_r \} \subset \mathcal{X}$ such that the conditions in (41) - (45) are satisfied. The first three conditions in (41), (42) and (43) are simple joint typicality constraints and are identical to the ones in [11, Lemma 3], for $L = 1$. On the other hand, the last two conditions in (44) and (45) are an extension of the joint typicality arguments to the principle of list decoding.

It was shown in [16] that any randomly generated set of codewords will satisfy the conditions in (41) - (45) of Lemma 3.2 with probability that approaches one exponentially fast as $n \to \infty$. Beside Lemma 3.2, we need to define a decoding algorithm for the list code $C^*_{\text{list}}$. Thus, we present the following definition:

**Definition 3.3.** [16, Definition 4] Given a received sequence $y^n$ and the set of codewords $x^n(m_c,m_r)$, for $m_c \in M_c$ and $m_r \in M_r$, we let $(m_c,m_r) \in \varphi_L(y^n)$, if and only if for an $n \geq 0$, the following holds:

1) There exists an $s^n \in S^n$ such that

$$D(P_{YXS}\|W \times P_X \times P_S) \leq \eta,$$

where $P_{YXS}$ is the joint type of $(y^n,x^n(m_c,m_r),s^n)$, $P_X$ is the type of $x^n(m_c,m_r)$, while $P_S$ is the type of $s^n$. Additionally, we have

$$(W \times P_X \times P_S)(y,x,s) = W_s(y|x)P_X(x)P_S(s).$$

2) For every choice of $L$ other distinct codewords $(x^n(j_1),\ldots,x^n(j_L))$, where $j_i \in M_c \times M_r$, such that each of them satisfies

$$D(P_{YX_{j_i}S_{j_i}}\|W \times P_{X_{j_i}} \times P_{S_{j_i}}) \leq \eta,$$

for some $S_{j_i} \in S^n$, where $P_{YX_{j_i}S_{j_i}}$ is the joint type of $(y^n,x^n(j_i),S_{j_i})$, $P_{X_{j_i}}$ is the type of $x^n(j_i)$, while $P_{S_{j_i}}$ is the type of $S_{j_i}$, we have

$$I(XY;X^L|S) \leq \eta,$$

where the previous mutual information is calculated with respect to the joint distribution $P_{XYXS}$ given by the joint type of $(x^n(m_c,m_r),y^n,x^n(j_1),\ldots,x^n(j_L),s^n)$.

The previous list decoder is a generalization of the decoder introduced in [11, Definition 3] for uncorrelated codes. Lemma 3.2 and Definition 3.3 are the main pillars needed to realize the encoding and decoding process of a list code $C^*_{\text{list}}$ given by Definition 2.11.

Now, we are ready to present the reliable communication results. We present a lemma that implies that if the AVC $\mathfrak{M}$ is not $L$-symmetrizable, then the list decoder in Definition 3.3 can not produce more than $L$ values as long as the rate is bounded by the minimum mutual information between the channel input $X$ and the average channel output $Y_q$.

**Lemma 3.4.** [16, Lemma 3] For an AVC $\mathfrak{M}$ with an order of symmetrizability $L(\mathfrak{M})$, let $L \geq L(\mathfrak{M}) + 1$ and $\beta > 0$. Then for any $\delta > 0$, $n \geq n_0(\beta, \delta)$ and any type $P_X \in P^*_0(X)$ such that $\min_{x: P_X(x) > 0} P_X(x) \geq \beta$, there exists a list code $C^*_{\text{list}}$ with list
size $L$ such that for $\zeta > 0$, we have

$$\min_{q \in \mathcal{P}(S)} I(X; Y_q) - 2\delta/3 \geq \frac{1}{n} \log \left( \frac{|M_c||M_r|}{L} \right) \geq \min_{q \in \mathcal{P}(S)} I(X; Y_q) - \delta,$$

$$\tilde{e}_L(C^e_{\text{list}}) = \max_{a^n \in S^n} \tilde{e}_L(s^n|C^e_{\text{list}}) \leq 2^{-n\zeta}.$$ 

This lemma was proved in [16] by using a list code $C^e_{\text{list}}$ given by the set of codewords $x^n(m_c, m_r)$, for $m_c \in M_c$ and $m_r \in M_r$ that satisfy the constraints in Lemma 3.2 along with the list decoder in Definition 3.3.

**Remark 4.** It worth mentioning that Lemmas 3.2 and 3.4 in addition to Definition 3.3 were originally presented using one message set $M$. However, in this paper, we present them using two message sets $M_c$ and $M_r$ so that they can fit our coding scheme. This modification does not affect the validity of these results because it makes no difference to enumerate the codewords by one index taken from a message set $M$ or by two indices taken from $M_c \times M_r$.

The final result that we need to highlight is related to secure communication over AVWCs. It gives a lower bound on the amount of randomization needed to confuse the eavesdropper.

**Lemma 3.5.** [23, Lemma 2] For any $\tau, \beta > 0$, there exists values $\delta(\tau) > 0$ and $n_0(\tau)$, such that for all $n \geq n_0(\tau)$ and type $P_X \in \mathcal{P}^0_0(\mathcal{X})$ satisfying $\min_{x: P_X(x) > 0} P_X(x) \geq \beta$, there exist codewords $x^n(m_c, m_r) \in T_X \subset \mathcal{X}^n$, where $m_c \in M_c$ and $m_r \in M_r$, such that for an AVC $\mathcal{G}$, we have for all $s^n \in S^n$ and $m_c \in M_c$

$$\frac{\log |M_r|}{n} \geq \max_{q \in \mathcal{P}(S)} I(X; Z_q) + \tau,$$

if

$$\left\lVert \frac{1}{|M_r|} \sum_{m_r=1}^{|M_r|} V_{s^n}(\cdot|x^n(m_c, m_r)) - \mathbb{E}[V_{s^n}(|X^n)] \right\rVert_1 \leq 2^{-n\delta(\tau)}$$

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

**Remark 5.** Using the triangle inequality along with the relation between the total variation distance and the mutual information established in [12, Lemma 2.7], it was shown in [23], that the condition in (47) assures that the information leakage of the confidential message to the eavesdropper with respect to the strong secrecy decays exponentially as follows:

$$\max_{s^n \in S^n} \mathbb{I}(M_c; Z^n_{s^n}) \leq 2^{-n\delta(\tau)}$$

3.2. First Coding Theorem. In this section, we present the main contribution of this paper, which is a full characterization of the list secrecy capacity of AVWCs. We start by defining the following multi-letter formula. Let $(\mathcal{G}, \mathcal{S})$ be an AVWC, then for every $n \in \mathbb{N}$, let $\mathcal{U}_n := [\mathcal{X}^n]$ and define $C^*(\mathcal{G}, \mathcal{S})$ as follows:

$$C^*(\mathcal{G}, \mathcal{S}) = \lim_{n \to \infty} \max_{P_{U_n} \in \mathcal{P}(\mathcal{U}_n)} \max_{P_{X^n|U_n} \in \mathcal{P}(\mathcal{X}^n|\mathcal{U}_n)} \left( \min_{q \in \mathcal{P}(S^n)} \mathbb{I}(U_n; Y^n_q) - \max_{a^n \in S^n} \mathbb{I}(U_n; Z^n_{a^n}) \right).$$

It was shown in [26, Theorem 6], that the correlated random secrecy capacity $C^c(\mathcal{G}, \mathcal{S})$ is equivalent to $C^*(\mathcal{G}, \mathcal{S})$. It was also shown that $C^*(\mathcal{G}, \mathcal{S})$ does
not change if the sets over which the minimum and the maximum are taken in (48) are replaced by different, but related ones. In particular, it was shown that \( \max_{s_n \in \mathcal{S}^n} \mathbb{I}(U_n; Z^n_{\tilde{q}W}) \) can be replaced by \( \max_{q \in \mathcal{P}(\mathcal{S}^n)} \mathbb{I}(U_n; Z^n_q) \). It was also shown that \( \min_{q \in \mathcal{P}(\mathcal{S}^n)} \mathbb{I}(U_n; Y^n_q) \) can be replaced by \( \min_{q \in \mathcal{P}(\mathcal{S})} \mathbb{I}(U_n; Y^n_q) \).

**Theorem 3.6.** The list secrecy capacity \( C_{\text{list}}^*(\mathcal{W}, \mathcal{V}, L) \) of the AVWC \((\mathcal{W}, \mathcal{V})\) is characterized by the following:

\[
C_{\text{list}}^*(\mathcal{W}, \mathcal{V}, L) = \begin{cases} 
0 & \text{if } \mathcal{W} \text{ is } L\text{-symmetrizable} \\
C^*(\mathcal{W}, \mathcal{V}) & \text{otherwise}, 
\end{cases}
\]

where \( \mathcal{W} \) is the AVC between the transmitter and the legitimate receiver.

The previous capacity characterization implies that for an AVWC \((\mathcal{W}, \mathcal{V})\), with an order of symmetrizability \( L(\mathcal{W}) \) for the legitimate channel, a list code with list size \( L \geq L(\mathcal{W}) + 1 \) can provide a reliable and secure communication at the rate given by (48) which is equivalent to the correlated random secrecy capacity. Theorem 3.6 also implies that for an AVWC \((\mathcal{W}, \mathcal{V})\) where \( \mathcal{W} \) is symmetrizable and no common randomness is shared between the transmitter and the legitimate receiver, i.e. \( C_{\text{uc}}^*(\mathcal{W}, \mathcal{V}) = 0 \) and correlated random codes can not be used, we can still achieve a positive secrecy rate equivalent to the correlated random secrecy capacity using list decoding. This point implies that list codes can overcome the drawbacks of both uncorrelated and correlated random codes.

We now present a detailed proof for Theorem 3.6 based on the code concept of Definition 2.11. Our achievability proof is based on a coding scheme that combines the list decoding techniques used in [16] to establish a reliable communication over AVCs and the strong secrecy techniques introduced in [26, 23] for AVWCs. On the other hand, the converse follows using the standard techniques as in [26].

**Coding Problem.** The main issue of the proof of Theorem 3.6 is the achievability of the secrecy rate in (48) if the AVC \( \mathcal{W} \) between the transmitter and the legitimate receiver is not \( L\)-symmetrizable. This is because, the expression of \( C^*(\mathcal{W}, \mathcal{V}) \) in (48) is calculated with respect to the AVC \( \mathcal{W} \) instead of the AVC \( \mathcal{W}^* \), where \( \mathcal{W} = (\mathcal{W} \circ P_{X^n|U_n}) \) is the AVC that arises from combining the prefix channel \( P_{X^n|U_n} \in \mathcal{P}(\mathcal{X}^n|\mathcal{U}_n) \) and the AVC \( \mathcal{W} \). This point is very important because it was shown in [23, Example 1] that a prefix channel can change a non-symmetrizable AVC to a symmetrizable one. This implies that, although \( \mathcal{W} \) is not \( L\)-symmetrizable, \( \mathcal{W}^* \) might be \( L\)-symmetrizable.

The previous observation raises an important issue for our coding scheme because the achievability list decoding techniques introduced in [16] are only valid for AVCs that are not \( L\)-symmetrizable. In order to solve this issue, we used an approach similar to the one introduced in [23]. We start by restricting the calculation of \( C^*(\mathcal{W}, \mathcal{V}) \) to certain prefix channels of the form \( \tilde{P}_{X^n|U_n} = P_{X^n|\hat{X}} \otimes P_{X^{n-1}|U_{n-1}} \). We then show that using this restricted class of prefix channels to calculate \( C^*(\mathcal{W}, \mathcal{V}) \) is asymptotically as good as using the full set of prefix channels \( \mathcal{P}(\mathcal{X}^n|\mathcal{U}_n) \). In addition, this restricted class of prefix channels assures that the AVC \((\mathcal{W} \circ \tilde{P}_{X^n|U_n})\) is not \( L\)-symmetrizable as long as \( \mathcal{W} \) is not \( L\)-symmetrizable.

**Proof.** We start by proving the first condition of Theorem 3.6. According to Lemma 3.1, if the AVC \( \mathcal{W} \) between the transmitter and the legitimate receiver is \( L\)-symmetrizable, then no reliable communication is possible using a list code.
with list size $L$. This implies that the list secrecy capacity $C_{\text{list}}^s(\mathfrak{W}, \mathfrak{U}, L) = 0$, proving the first part of the theorem.

We now turn to the second condition of the theorem and assume that the AVC $\mathfrak{Y}$ is not $L$-symmetrizable and present an achievable coding scheme that consists of 4 main steps:

1) **Prefix Channel Optimization:** We start by considering the input distributions $P_{U_r}$ and the conditional distributions $P_{X_r|U_r}$ arising from the optimization problem in (48). Without loss of generality, for every $r \in \mathbb{N}$, let $\mathcal{U}_r = X^r$ and define the following:

$$C_r := \max_{P_{U_r} \in \mathcal{P}(\mathcal{U}_r)} \max_{P_{X_r|U_r} \in \mathcal{P}(X^r|\mathcal{U}_r)} \left( \min_{q \in \mathcal{P}(S^r)} \mathbb{I}(U_r; Y^r_q) - \max_{s^r \in S^r} \mathbb{I}(U_r; Z^r_{sr}) \right),$$

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

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

Now, let $\hat{P}_{U_{r+1}} \in \mathcal{P}(\mathcal{U}_{r+1})$, be such that $\hat{P}_{U_{r+1}} = P^*_r \otimes \pi$, where $\pi \in \mathcal{P}(X)$ is defined as $\pi(x) := |X|^{-1}$ and $\hat{P}_{X_{r+1}|U_{r+1}} = \mathcal{P}(X^{r+1}|\mathcal{U}_{r+1})$, be such that $\hat{P}_{X_{r+1}|U_{r+1}} := P^*_{X_{r+1}|U_r} \otimes \sigma$, where $\sigma \in \mathcal{P}(X|\mathcal{X})$ is defined as $\sigma(x|x) = 1$ if and only if $x = \tilde{x}$. Then, from (49), it holds that

$$C_{r+1} \geq \min_{q \in \mathcal{P}(S^{r+1})} \mathbb{I}(\hat{U}_{r+1}; Y^r_q) - \max_{s^{r+1} \in S^{r+1}} \mathbb{I}(\hat{U}_{r+1}; Z^r_{s^{r+1}}) \tag{50}$$

$$\overset{(a)}{=} \min_{q \in \mathcal{P}(S^{r+1})} \mathbb{I}(U^*_r X_r; Y^r_q) - \max_{s^{r+1} \in S^{r+1}} \mathbb{I}(U^*_r X_r; Z^r_{s^{r+1}}) \tag{51}$$

$$\overset{(b)}{=} \min_{q \in \mathcal{P}(S^{r+1})} \mathbb{I}(U^*_r X_r; Y^r_q) - \max_{s^r \in S^r} \mathbb{I}(U^*_r; Z^r_{sr}) - \max_{s^r \in S^r} \mathbb{I}(X^r; Z^r_{sr}) \tag{52}$$

$$\overset{(c)}{=} \min_{q \in \mathcal{P}(S^r)} \mathbb{I}(U^*_r; Y^r_q) - \max_{s^r \in S^r} \mathbb{I}(U^*_r; Z^r_{sr}) - \log |X|$$

where (a) follows from the definition of $\hat{P}_{U_{r+1}}$ and $\hat{P}_{X_{r+1}|U_{r+1}}$; (b) follows from the mutual information chain rule and the fact that $U_r^*$ and $Z_{sr+1}^*$ are independent as well as $X_r^*$ and $Z_{sr+1}^*$; while (c) follows because $\mathbb{I}(X^r; Z_{sr+1}) \leq \log |X|$. We now investigate the effect of the prefix channel $\hat{P}_{X_r|U_r}$ on the symmetrizability of the resultant channel $(\mathfrak{W} \circ \hat{P}_{X_r|U_r})$ as follows:

$$\mathfrak{W} \circ \hat{P}_{X_r|U_r} = \mathfrak{W} \circ \left( P^*_r \otimes \sigma \right) \tag{53}$$

$$= (\mathfrak{W} \circ \circ^{-1} \circ P^*_r \otimes \sigma) \otimes \mathfrak{W}$$

where the previous relation follows due to the properties of the operators $\circ$ and $\otimes$ along with the definition of the conditional distribution $\sigma$. Since the AVC $\mathfrak{W}$ is not $L$-symmetrizable, then for every $r \geq 2$, it follows that the AVC $(\mathfrak{W} \circ \hat{P}_{X_r|U_r})$ is not $L$-symmetrizable as well even if $(\mathfrak{W} \circ \circ^{-1} \circ P^*_r \otimes \sigma)$ is $L$-symmetrizable.

2) **Block Coding:** In this point, we describe the construction of a list code $C_{\text{list}}^s$ according to Definition 2.11 for the AVWC $(\mathfrak{W} \circ \hat{P}_{X_r|U_r}, \mathfrak{Y} \circ \hat{P}_{X_r|U_r})$. We start by generating our codebook as follows: For a code block length $t \in \mathbb{N}$
and \( r \in \mathbb{N}\setminus\{1\} \), let \( \mathcal{P}_{U_r} \subseteq \mathcal{P}(\mathcal{U}_t) \) and use it to generate the set of codewords \( u_t^r(m_c, m_r) \in T_{\mathcal{P}_{U_r}} \subseteq \mathcal{U}_t^r \), for \( m_c \in \mathcal{M}_c \) and \( m_r \in \mathcal{M}_r \). Using the union bound, we can show that the produced codewords satisfy the constraints in Lemma 3.2 and Lemma 3.5 with probability approaches one as \( t \to \infty \).

Next, we present our encoding and decoding algorithms. Given a confidential message \( m_c \in \mathcal{M}_c \), the encoder chooses a randomization message \( m_r \in \mathcal{M}_r \) uniformly at random then outputs the codeword \( u_t^r(m_c, m_r) \). At the legitimate receiver, we use a list decoder \( \varphi_L \) similar to the one given by Definition 3.3, that takes the received sequence \( y^n \) and outputs a list \( \mathcal{J} \in \mathcal{J}_L(\mathcal{M}_c \times \mathcal{M}_r) \).

3) Reliability and secrecy analysis: Lemma 3.4 implies that for an AVC which is not \( L \)-symmetrizable, there exists a list code \( C^*_\text{list} \) with list size \( L \) and block length \( t \) constructed as described in the previous point which can be used to transmit the messages \( (m_c, m_r) \) reliably over the AVC \( (\mathbb{M} \circ \hat{P}_{X_r} \sigma_{U_r}) \) as long as

\[
\min_{q \in \mathcal{P}(\mathcal{S}_t)} I(U_r; Y_r^t) - 2 \delta/3 > \frac{1}{t} \log |\mathcal{M}_r| L \geq \min_{q \in \mathcal{P}(\mathcal{S}_t)} I(U_r; Y_r^t) - \delta,
\]

where \( \delta > 0 \). The previous result is only valid if the AVC \( (\mathbb{M} \circ \hat{P}_{X_r} \sigma_{U_r}) \) is not \( L \)-symmetrizable. In addition, we mean by reliably transmitted message that the average decoding error of \( C^*_\text{list} \) decays exponentially fast. Thus, for \( \zeta > 0 \) we have

\[
\tilde{e}_L(C^*_\text{list}) = \max_{s^t \in \mathcal{S}_t^r} \tilde{e}_L(s^t|C^*_\text{list}) \leq 2^{-t\zeta}.
\]

On the other hand, based on the secrecy analysis in [23] that relates the strong secrecy constraint in (28) to variational distance in Lemma 3.5, we can show that the constructed list code is asymptotically secure in the strong sense, as long as

\[
\max_{s^t \in \mathcal{S}_t^r} I(M; Z_{s^t}^r) + \delta \leq \liminf_{t \to \infty} \frac{1}{t} \log |\mathcal{M}_r| \leq \max_{s^t \in \mathcal{S}_t^r} I(M; Z_{s^t}^r) + 2\delta.
\]

It is worth mentioning that by asymptotically secure in the strong sense, we mean that the information leakage of the confidential message to the eavesdropper decays exponentially fast. Thus, for \( \tau > 0 \), we have

\[
\max_{s^t \in \mathcal{S}_t^r} I(M; Z_{s^t}^r) \leq 2^{-t\tau}.
\]

Now, let \( \mathcal{P}_{U_r} \subseteq \mathcal{P}(\mathcal{U}_t) \) converges to \( \hat{\mathcal{P}}_{U_r} \in \mathcal{P}(\mathcal{U}_t) \) as \( t \to \infty \), such that \( \hat{\mathcal{P}}_{U_r} = P^*_{U_{r-1}} \otimes \pi \), where \( \pi \) is as defined before and \( P^*_{U_{r-1}} \in \mathcal{P}(\mathcal{U}_{r-1}) \) being an optimal choice for the optimization problem in (49), then from (51), (53) and (55) we have

\[
\liminf_{t \to \infty} \frac{1}{t} \log |\mathcal{M}_r| L \geq \min_{q \in \mathcal{P}(\mathcal{S}_t^r)} I(\hat{U}_r; Y_r^t) - \max_{s^t \in \mathcal{S}_t^r} I(\hat{U}_r; Z_{s^t}^r) - 3\delta.
\]

4) Code Transformation: Up until this point, we have shown that we can construct a list code \( C^*_\text{list} \) that can be used to establish a reliable and secure communication over the AVWC \( (\mathbb{M} \circ \hat{P}_{X_r} \sigma_{U_r} \sigma_{U_r}) \). Now, we want to use this code to establish a reliable and secure communication over the AVWC \( (\mathbb{M}, \mathcal{Y}) \).

Let \( \mathcal{X} \subseteq \{0, \ldots, r - 1\} \), such that for every \( n \in \mathbb{N} \), we define \( n = t \cdot r + \mathcal{X} \). Since we assumed without loss of generality that \( \mathcal{U}_t = \mathcal{X}^r \), we can transform any codeword \( u_t^r(m_c, m_r) \) into a codeword \( x_t^{\mathcal{X}^r}(m_c, m_r) \). Next, we generate the codewords \( x^n(m_c, m_r) \) for \( m_c \in \mathcal{M}_c \) and \( m_r \in \mathcal{M}_r \) by concatenating a dummy codeword \( x_{\mathcal{X}}^t \) to the transformed codeword \( x_t^{\mathcal{X}^r}(m_c, m_r) \). Using this technique, we are able to
Now, we are ready to derive our converse. We start by rewriting Eq. (29) as follows:

\[
\begin{align*}
\tilde{e}_L(C_{\text{list}}) &= \max_{s^n \in \mathcal{S}^n} \frac{1}{|\mathcal{M}_c|} \sum_{m_c} \sum_{x^n} \sum_{y^n; \not\in \mathcal{C}_L} W^n_s(y^n|x^n) E(x^n|m_c) \\
&= \max_{q \in \mathcal{P}(\mathcal{S}^n)} \frac{1}{|\mathcal{M}_c|} \sum_{m_c} \sum_{x^n} \sum_{y^n; \not\in \mathcal{C}_L} W^n_q(y^n|x^n) E(x^n|m_c) \\
&\leq (a) \lambda,
\end{align*}
\]

where \(W^n_q(y^n|x^n) = \sum_{s^n} q(s^n) W^n_s(y^n|x^n)\) and (a) follows due to Eq. (30). If we use Eq. (59) along with Fano’s inequality, then for every \(q \in \mathcal{P}(\mathcal{S}^n)\), the following holds:

\[
\mathbb{H}(M|Y^n_q) \leq 1 + \lambda \log |\mathcal{M}_c|.
\]

Now, we are ready to derive our converse. We start by rewriting Eq. (29) as follows:

\[
\begin{align*}
R &\leq \frac{1}{n} \left[ \log |\mathcal{M}_c| - \log L \right] + \delta \\
&\leq \frac{1}{n} \left[ \mathbb{H}(M) - \log L \right] + \delta \\
&\leq (a) \frac{1}{n} \left[ \min_{\mathcal{P}(\mathcal{S}^n)} \mathbb{H}(M; Y^n_q) + 1 + \lambda \log |\mathcal{M}| - \log L \right] + \delta \\
&\leq (b) \frac{1}{n} \left[ \min_{\mathcal{P}(\mathcal{S}^n)} \mathbb{H}(M; Y^n_q) - \max_{s^n \in \mathcal{S}^n} \mathbb{H}(M; Z^n_{s^n}) \right] + \epsilon \\
&\leq (c) \frac{1}{n} \left[ \min_{\mathcal{P}(\mathcal{S}^n)} \mathbb{H}(U^n; Y^n_q) - \max_{s^n \in \mathcal{S}^n} \mathbb{H}(U^n; Z^n_{s^n}) \right] + \epsilon
\end{align*}
\]

where (a) follows by adding and subtracting the two sides of the inequality in (60); (b) follows similarly by applying the inequality in (31), where \(\epsilon = 1/n(\tau + 1 +\)

transform the list code \(C_{\text{list}}^t\) constructed on the alphabet \(U_t\) and with block length \(t\) into a new list code \(C_{\text{list}}^t\) constructed on the alphabet \(\mathcal{X}\) and with block length \(n\).

One can easily show that under this transformation mechanism, the newly constructed code \(\bar{C}_{\text{list}}^t\) will have the same reliability and secrecy performance of the original code \(C_{\text{list}}^t\). This implies that we have constructed a list code \(\bar{C}_{\text{list}}^t\) with list size \(L\) that can be used to establish a reliable and secure communication over the AVWC (29, 23).
We construct a list code
Given a confidential message
simplifies to the expression of
correlated random code
ing a codeword
Now, if we take the limit as
size
Theorem 3.7.
public rate vanishes.
list codes as in Definition 2.13, but we restrict our analysis to the case where the
3.3. SECOND CODING THEOREM. In this section, we derive another coding theorem
to characterize the list secrecy capacity of AVWCs using a class of public-confidential
list codes as in Definition 2.13, but we restrict our analysis to the case where the
public rate vanishes.

Theorem 3.7. The public-confidential list secrecy capacity
\( C^{ps}_{list}(\mathcal{M}, \mathcal{V}, L) \)
of the AVWC \( (\mathcal{M}, \mathcal{V}) \), when the public rate vanishes, i.e. \( R_p = 0 \) is characterized by the following:

\[
C^{ps}_{list}(\mathcal{M}, \mathcal{V}, L) = \begin{cases} 
0 & \text{if } \mathcal{M} \text{ is } L\text{-symmetrizable} \\
C^*(\mathcal{M}, \mathcal{V}) & \text{otherwise},
\end{cases}
\]

where \( \mathcal{M} \) is the AVC between the transmitter and the legitimate receiver.

Corollary 1. For an AVWC \( (\mathcal{M}, \mathcal{V}) \), the list secrecy capacity \( C^*_{list}(\mathcal{M}, \mathcal{V}, L) \) is equivalent to the public-confidential list secrecy capacity \( C^{ps}_{list}(\mathcal{M}, \mathcal{V}, L) \), when the public rate vanishes, i.e. \( R_p = 0 \), then
\[
C^*_{list}(\mathcal{M}, \mathcal{V}, L) = C^{ps}_{list}(\mathcal{M}, \mathcal{V}, L).
\]

Proof. We will only focus on achievability part of the second condition in Theorem 3.7, where the AVC \( \mathcal{M} \) is not \( L\)-symmetrizable. Our proof is based on a coding scheme that combines the reliability list decoding techniques introduced in [4] for AVCs along with the results established in [26] for correlated random codes.

1- Code Structure: We construct a list code \( C^{ps}_{list} \) of Definition 2.13 with list size \( L \) and block length \( n = \tilde{n} + \check{n} \) by concatenating a deterministic list code \( C_{list} \) of Definition 2.9 with list size \( L \) and block length \( \check{n} \) and a correlated random code \( C^*_c \) of Definition 2.6 with block length \( \tilde{n} \). Additionally, we let the set of public messages \( \mathcal{M}_p \) encoded by the list code \( C_{list} \) to be identical to the set of values of the common randomness \( \mathcal{G} \) used by the correlated random code \( C^*_c \).

2- Encoding: Given a confidential message \( m_c \in \mathcal{M}_c \), the encoder chooses an index \( \gamma \in \mathcal{G} \) uniformly at random and encodes it using the list code \( C_{list} \) producing a codeword \( x^n(\gamma) \). After that \( m_c \) and \( \gamma \) are then given to the encoder of the correlated random code \( C^*_c \) which outputs a codeword \( x^{\tilde{n}}_c(m_c) \). Finally the encoder concatenates the two codewords producing \( x^n(\gamma, m_c) = (x^n(\gamma), x^{\tilde{n}}_c(m_c)) \) and transmits it.

3- Decoding: Having received \( y^n = (y^n, \check{y}^{\tilde{n}}) \), the decoder works as follows: First it uses \( y^n \) and the decoder of the list code \( C_{list} \) to produce a list of size \( L \), i.e. \( \hat{\mathcal{G}} = \varphi_L(y^n) \). Then for every \( \hat{\gamma} \in \hat{\mathcal{G}} \), we use \( \check{y}^{\tilde{n}} \) along with the decoder \( \varphi^{\hat{\gamma}} \) of the correlated random code \( C^*_c \) to find a corresponding confidential message \( \hat{m}_c \in \mathcal{M}_c \). Thus, the final decoding output is a list of size \( L \) as follows:

\[
\{(\hat{\gamma}, \hat{m}_c) \in \hat{\mathcal{G}} \times \mathcal{M} : \exists \gamma \in \varphi_L(y^n) \text{ and } \hat{m}_c = \varphi^{\hat{\gamma}}(\check{y}^{\tilde{n}})\}.
\]

4- Reliability Analysis: Based on our coding scheme, we can bound the average probability of error of \( C^{ps}_{list} \) given by (32) in terms of the average error probability of \( C_{list} \) given by (23) and the average error probability of \( C^*_c \) given by (16) as follows:

\[
\hat{e}_L(C^{ps}_{list}) \leq \hat{e}_L(C_{list}) + \check{e}(C^*_c).
\]

Based on the results established in [2, 26], we can construct a correlated random code with a secrecy rate \( R_c \) close to \( C^*_c(\mathcal{M}, \mathcal{V}) \), such that \( \check{e}(C^*_c) \) decays exponentially fast.
It was also shown that the amount of common randomness required to construct such codes is quadratic in the block length as highlighted by [2, Lemma 6], i.e. $|\mathcal{G}| = \mathcal{O}(n^2)$. This implies that the public rate $R_p$ of the list code $\mathcal{C}_{\text{list}}$ is given by:

$$R_p = \frac{1}{n} \log |\mathcal{G}| = \frac{2}{n} \log \mathcal{O}(n).$$

Since the AVC $\mathcal{W}$ is not $L$-symmetrizable, [4, Lemma 3] implies that $\bar{e}_L(\mathcal{C}_{\text{list}})$ decays exponentially fast as long as $R_p$ is small enough. According to (63), as $n \to \infty$, $R_p$ vanishes. This implies that $\bar{e}_L(\mathcal{C}_{\text{list}})$ decays exponentially fast as long as $R_c \leq C^*_s(\mathcal{W}, \mathcal{V})$.

5- Secrecy Analysis: Let $\Gamma$ be a uniformly distributed random variable over the set $\mathcal{G}$. Then, based on the structure of our coding scheme, the mean secrecy constraint in (33) can be bounded as follows:

$$\max_{s^n \in \mathcal{S}^n} \mathbb{I}(M_c; Z_n | M_p \mathcal{C}_{\text{list}}^{ps}) \leq \max_{s^n \in \mathcal{S}^n} \mathbb{I}(M_c; Z_n | M_p \mathcal{C}_{\text{list}}^{ps}) + \max_{s^n \in \mathcal{S}^n} \mathbb{I}(M_c; Z_n | Z_{s^n} M_p \mathcal{C}_{\text{list}}^{ps})$$

$$\leq \max_{s^n \in \mathcal{S}^n} \mathbb{I}(M_c; Z_n | M_p \mathcal{C}_{\text{list}}^{ps})$$

$$\leq \max_{s^n \in \mathcal{S}^n} \mathbb{I}(M_c; Z_n | \Gamma \mathcal{C}_{\text{cr}}^{s})$$

$$\leq e^{-\hat{n}e},$$

where (a) follows from the mutual information chain rule; (b) follows because $M_c$ and $Z_n$ are independent; (c) follows because $\Gamma$ is identical to $M_p$ and the fact that $M_c$ is only encoded using $\mathcal{C}_{\text{cr}}$; (d) follows from the secrecy analysis of the correlated random codes in [2, 23], where $\epsilon > 0$. On the other hand, the maximum secrecy constraint in (34) can be bounded as follows:

$$\max_{s^n \in \mathcal{S}^n} \max_{m_p \in \mathcal{M}_p} \mathbb{I}(M_c; Z_n | m_p \mathcal{C}_{\text{list}}^{ps})$$

$$\leq \max_{s^n \in \mathcal{S}^n} \mathbb{I}(M_c; Z_n | \mathcal{C}_{\text{list}}^{ps})$$

$$\leq e^{-\hat{n}e},$$

where (a) follows as in (64); (b) follows because $\Gamma$ is identical to $M_p$; (c) follows from the secrecy analysis of the correlated random codes in [26].

The previous coding scheme shows that for an AVWC $(\mathcal{W}, \mathcal{V})$, where the AVC $\mathcal{W}$ is not $L$ symmetrizable, there exists a list code $\mathcal{C}_{\text{list}}^{ps}$ with list size $L$, a confidential rate $R_c = C^*_s(\mathcal{W}, \mathcal{V})$ and a public rate $R_p = 0$, such that $\mathcal{C}_{\text{list}}^{ps}$ satisfies the reliability constraint in (37), the mean secrecy criterion in (38) and the maximum secrecy criterion in (39). Since $C^*_s(\mathcal{W}, \mathcal{V}) = C^*(\mathcal{W}, \mathcal{V})$, this implies that $C_{\text{list}}^{ps, \text{mean}}(\mathcal{W}, \mathcal{V}) = C_{\text{list}}^{ps, \text{max}}(\mathcal{W}, \mathcal{V}) = C^*(\mathcal{W}, \mathcal{V})$. Since, we only consider the case where $R_p$ vanishes as $n \to \infty$, we have $C_{\text{list}}^{ps}(\mathcal{W}, \mathcal{V}) = C^*_s(\mathcal{W}, \mathcal{V})$ and this completes our achievability proof.

3.4. Discussion. Theorem 3.6 indicates that for an AVWC $(\mathcal{W}, \mathcal{V})$, regardless of the order of symmetrizability $L(\mathcal{W})$ of the AVC $\mathcal{W}$, we can always achieve a positive secrecy rate equivalent to the correlated random secrecy capacity by using a list code with list size $L \geq L(\mathcal{W}) + 1$. This implies that list codes are more powerful.
than uncorrelated codes because uncorrelated codes can only provide a positive secrecy if the AVC $\mathfrak{W}$ between the transmitter and the legitimate receiver is not symmetrizable. The construction of list codes also does not require the existence of a predefined coordination between the legitimate node which makes them more efficient than correlated random codes.

Theorem 3.6 also implies that list codes provide a solution for the instability of the secrecy capacity of the AVWC $(\mathfrak{W}, \mathfrak{V})$. This is because if we use a sufficiently large the list size $L$, such that $C_{\text{list}}^{s}(\mathfrak{W}, \mathfrak{V}, L) > 0$, then for all AVWCs $(\mathfrak{W}, \mathfrak{V})$ in the neighborhood of $(\mathfrak{W}, \mathfrak{V})$ the secrecy capacity $C_{\text{list}}^{s}(\mathfrak{W}, \mathfrak{V}, L)$ is also greater than zero.

The previous two points implies that we can always overcome the different jamming strategies induced by the jammer to disturb reliable communication over an AVWC $(\mathfrak{W}, \mathfrak{V})$ by using list codes with list size $L \geq L(\mathfrak{W}) + 1$. Although this feature advocates the usage of list codes, it was shown in [4, Theorem 3] that even for simple AVWCs, where $|\mathcal{X}| = |\mathcal{Y}| = |\mathcal{S}| = 2$, there exist some jamming strategies that lead to an arbitrarily large order of symmetrizability $L(\mathfrak{W})$. This implies that, for these AVWCs, we need to construct list codes with an arbitrarily large list size, which is not always feasible.

We need to highlight some of the differences between the two coding schemes used to establish Theorem 3.6. One of the major differences between these two schemes is the assumptions on the information shared between the eavesdropper and the jammer. In the first coding scheme we constructed a pure list code of Definition 2.11 using the techniques introduced in Lemma 3.2 and Definition 3.3 as shown in Section 3.2. Such coding scheme does not impose any restrictions on the information shared between the jammer and the eavesdropper. On the other hand, the second coding scheme is based on a list code of Definition 2.13 which is constructed by concatenating a non-secure list code of Definition 2.9 and a correlated random code of Definition 2.6 as shown in Section 3.3. Such coding scheme inherit the characteristics of correlated random codes, which implies that the eavesdropper is not allowed to inform the jammer about any information it can extract.

Another important difference between the two coding schemes used to establish Theorem 3.6 is related to the type of services they can provide: public and confidential. Some public services like synchronization and channel estimation are very important in real life scenarios, yet they do not need to be protected against eavesdropping. In the first coding scheme, we uses a list code $C_{\text{list}}$, which only consider a confidential message set $\mathcal{M}_c$. This implies that in this coding scheme both public and confidential services are protected against eavesdropping which is not needed. One the other hand the second coding scheme uses a list code $C_{\text{list}}^{\text{st}}$, which differentiate between public and confidential messages.

It is worth mentioning that Theorem 3.6 can be very helpful in investigating the analytical properties of $C_{\text{list}}^{s}(\mathfrak{W}, \mathfrak{V}, L)$, which allows us to understand how the capacity function behaves. For example, the continuity behavior studies whether a small change in the AVWC $(\mathfrak{W}, \mathfrak{V})$ will only lead to a small change in the capacity or a significant one. This question is not only related to the stability of the capacity function, but it also plays an important role in determining the computability of the capacity function on Turing machines [8, 9]. This implies that it is important to investigate the continuity behavior of $C_{\text{list}}^{s}(\mathfrak{W}, \mathfrak{V}, L)$ and in particular its discontinuity points. To do so, we need to extend the continuity analysis of the uncorrelated secrecy capacity $C_{\text{uc}}^{s}(\mathfrak{W}, \mathfrak{V})$ in [7] to the principle of list codes.
Another important analytical property is the additivity which investigates how the capacity of two orthogonal channels is related to the capacity of their orthogonal combination. This property allows us to decide between using a joint encoder-decoder pair for the combined channel or to simply use an individual one for each channel. In [23] and [25], it was shown that the uncorrelated secrecy capacity $C_{suc}(W, V)$ exhibits an extreme behavior of super-additivity known as super-activation: Although the uncorrelated secrecy capacity of each of two orthogonal AVWCs is zero, the joint decoding of their orthogonal combination can lead to a strictly positive secrecy rate. It would be of high interest to investigate such behavior for the list secrecy capacity $C_{s list}(W, V, L)$.

4. Finite list size

4.1. Motivation and main results. Theorem 3.6 shows that in order to achieve a reliable and secure communication over an AVWC $(W, V)$, using a list code $C_{s list}$ such that the average error probability $\bar{e}(C_{s list})$ given by (27) and the information leakage of the confidential message $L(C_{s list})$ given by (28) vanish, we need a list code with list size $L$ that depends on the order of symmetrizability of the $W$ between the transmitter and the legitimate receiver, i.e. $L \geq L(W) + 1$. This implies that the capability of list codes to overcome the different jamming strategies induced by the jammer depends on the order of symmetrizability of the AVC $W$. The problem is that it was shown in [4, Theorem 3] that even for simple AVCs, the order of symmetrizability $L(W)$ might be arbitrarily large. This implies that, for their corresponding AVWCs, we need list codes with an arbitrarily large list size, which is not always feasible.

The previous issue motivates the investigation of the following interesting question: Does relaxing the reliability and secrecy constraints affect the value of the list size. In order to answer this question, we consider the following scenario: Given an AVWC $(W, V)$, where we allow for a small non-vanishing probability of error $\lambda$ and a small non-vanishing information leakage $\tau$, what is the maximum rate that we can achieve using list codes and what is the smallest list size required to achieve such rate.

Definition 4.1. For an arbitrary but fixed $\lambda, \tau > 0$, a non negative number $R$ is a $(\lambda, \tau)$-achievable list secrecy rate with list size $L$ for the AVWC $(W, V)$, if for all $\delta > 0$, there is an $n(\delta) \in \mathbb{N}$, such that for all $n \geq n(\delta)$, there exists a sequence of list codes $(C_{s list})_n$, that satisfy the following:

\begin{align}
\frac{1}{n} \log \frac{|M_c|}{L} &\geq R - \delta, \\
\bar{e}_L(C_{s list}) &\leq \lambda, \\
L(C_{s list}) &\leq \tau.
\end{align}

The supremum of all $(\lambda, \tau)$-achievable list secrecy rates $R$ with list size $L$ is denoted by $C_{s list}(W, V, \lambda, \tau, L)$.

Remark 6. It is important to highlight the difference between this definition and Definition 2.12. In Definition 2.12, we need to find list codes that satisfy the reliability and secrecy constraints in (30) and (31) for all values of $\lambda, \tau > 0$, while in the previous definition we need to satisfy the reliability and secrecy constraints for a certain value of $\lambda$ and $\tau$. 
Theorem 4.2. For an AVWC \((\mathcal{W}, \mathcal{V})\) with correlated random secrecy capacity \(C_{cr}^s(\mathcal{W}, \mathcal{V})\), let \(\lambda, \tau > 0\) be arbitrary but fixed. Then for every secrecy rate \(R < C_{cr}^s(\mathcal{W}, \mathcal{V})\), there exists a finite list size \(L\), such that
\[
R < C_{list}^s(\mathcal{W}, \mathcal{V}, \lambda, \tau, L).
\]

Sketch of the proof. The proof consists of two main steps. In the first step, we show that there exists a capacity achieving correlated random code \(\tilde{C}_{cr}^s\) that only utilizes a finite amount of shared common randomness \(|\tilde{G}|\) such that its average error probability \(\bar{e}(\tilde{C}_{cr}^s)\) given by (16) is less than or equal to \(\lambda\), while the maximum information leakage of the confidential message \(L_{max}(\tilde{C}_{cr}^s)\) given by (18) is less than or equal to \(\tau\). In the second step, we show how the constructed correlated random code \(\tilde{C}_{cr}^s\) can be transformed to a list code. The detailed proof steps is given in the next two sections.

Corollary 2. For an AVWC \((\mathcal{W}, \mathcal{V})\), every secrecy rate \(R < C_{cr}^s(\mathcal{W}, \mathcal{V})\) is a \((\lambda, \tau)\)-achievable secrecy rate using a list code with list size \(L(\lambda)\) given by the smallest natural number that satisfy
\[
L(\lambda) > \frac{1}{\epsilon \lambda} \ln |S|,
\]
for \(\epsilon > 0\), \(\lambda \in (0, 1)\) and \(S\) is the channel state set, while \(\lim_{n \to \infty} \tau = 0\).

Theorem 4.2 and Corollary 2 provide an answer for the two questions raised at the beginning of this section as follows: Theorem 4.2 implies that we can construct list codes that achieve secrecy rates up to the correlated random secrecy capacity, if we allow for a small non-vanishing probability of error and information leakage. On the other hand, Corollary 2 specifies a sufficient condition for the list size \(L\) required for the construction of such codes, which interestingly only depends on the reliability parameter \(\lambda\) and is independent of the secrecy parameter \(\tau\).

4.2. Correlated random codes with finite resources. In this section, we derive an intermediate result that will help us to prove Theorem 4.2. We construct a correlated random code \(\tilde{C}_{cr}^s\) that only utilizes a finite amount of shared common randomness \(|\tilde{G}|\). The constructed code can provide a secure communication over the AVWC \((\mathcal{W}, \mathcal{V})\) at a rate equivalent to the correlated random secrecy capacity \(C_{cr}^s(\mathcal{W}, \mathcal{V})\) such that the information leakage of the confidential message to the eavesdropper given by (18) vanishes. However, the constructed codes only assures that the average error probability \(\bar{e}(\tilde{C}_{cr}^s)\) given by (16) does not exceed an arbitrary but fixed value \(\lambda \in (0, 1)\).

Lemma 4.3. For an AVWC \((\mathcal{W}, \mathcal{V})\), let \(\lambda \in (0, 1)\) be arbitrary but fixed. There exists a correlated random code \(\tilde{C}_{cr}^s\) that can achieve secrecy rates equivalent to the correlated random secrecy capacity \(C_{cr}^s(\mathcal{W}, \mathcal{V})\) using a finite set \(\tilde{G}\) of values of a shared common randomness, such that
\[
\bar{e}(\tilde{C}_{cr}^s) \leq \lambda
\]
\[
\lim_{n \to \infty} L_{mean}(\tilde{C}_{cr}^s) = \lim_{n \to \infty} L_{max}(\tilde{C}_{cr}^s) = 0.
\]

Remark 7. The previous lemma extends the result established in [10, Theorem 3] for correlated random codes with finite resources, where the work in [10] used the mean information leakage of the confidential message with respect to the weak secrecy criterion as to evaluate the secrecy performance of correlated random codes.
Proof. For an AVWC (\(\mathcal{M}, \mathcal{W}\)), we know from [26, Theorem 6] that there exists a correlated random code \(\mathcal{C}_{cr}^*\) that can achieve the correlated random capacity \(C_{cr}(\mathcal{M}, \mathcal{W})\) using a shared common randomness \(\mathcal{G}\) whose cardinality grows quadratic in the block length \(n\), i.e. \(|\mathcal{G}| = O(n^2)\). We also know that both the average error probability \(\bar{e}(\mathcal{C}_{cr}^*)\) given by (16) and the maximum information leakage \(\mathbb{L}_{\text{max}}(\mathcal{C}_{cr}^*)\) given by (18) decays exponentially fast as highlighted by the reliability and secrecy analysis in [26].

Consider a correlated random code \(\mathcal{C}_{cr}^*\) constructed by selecting \(|\mathcal{G}|\) uncorrelated codes from the correlated random code \(\mathcal{C}_{cr}^*\) used to prove the achievability of [26, Theorem 6], where \(\mathcal{G} \subset \mathcal{G}\) is a finite set whose cardinality is independent of \(n\). Now, let \(\alpha > 0\) be arbitrary but fixed, then for a fixed channel state sequence \(s^n \in \mathcal{S}^n\), we have

\[
\mathbb{P}\left[\frac{1}{|\mathcal{G}|} \sum_{\gamma \in \mathcal{G}} \bar{e}(s^n|\mathcal{C}_{uc}^*(\gamma)) \geq \lambda\right] = \mathbb{P}\left[\exp\left(\alpha \sum_{\gamma \in \mathcal{G}} \bar{e}(s^n|\mathcal{C}_{uc}^*(\gamma))\right) \geq \exp(\alpha \lambda |\mathcal{G}|)\right]
\leq \exp(-\alpha \lambda |\mathcal{G}|) \mathbb{E}\left[\exp\left(\alpha \sum_{\gamma \in \mathcal{G}} \bar{e}(s^n|\mathcal{C}_{uc}^*(\gamma))\right)\right]
\]

(71)

where (a) follows using the Markov inequality. If we let \(\epsilon > 0\) and use the Taylor expansion of \(\exp(t)\), we can bound the expectation term in (71) as follows:

\[
\mathbb{E}\left[\exp\left(\alpha \bar{e}(s^n|\mathcal{C}_{uc}^*(\gamma))\right)\right] = \mathbb{E}\left[\sum_{k=0}^{\infty} \frac{\left(\alpha \bar{e}(s^n|\mathcal{C}_{uc}^*(\gamma))\right)^k}{k!}\right]
\leq \mathbb{E}\left[1 + \sum_{k=1}^{\infty} \frac{\alpha^k}{k!} \bar{e}(s^n|\mathcal{C}_{uc}^*(\gamma))\right]
\leq \left(1 + \sum_{k=1}^{\infty} \frac{\alpha^k}{k!} \exp(-n\epsilon)\right)
\leq \left(1 + \exp(-n\epsilon + \alpha)\right)
\]

(72)

where (a) follows because \(\bar{e}(s^n|\mathcal{C}_{uc}^*(\gamma)) \leq 1\); while (b) follows as for a fixed channel state sequence \(s^n\) the expectation of \(\bar{e}(s^n|\mathcal{C}_{uc}^*(\gamma))\) is a negative exponential in \(n\) [23].

Now, if we take all the state sequences \(s^n \in \mathcal{S}^n\) into consideration, we reach

\[
\mathbb{P}\left[\frac{1}{|\mathcal{G}|} \sum_{\gamma \in \mathcal{G}} \bar{e}(s^n|\mathcal{C}_{uc}^*(\gamma)) \geq \lambda, \forall s^n \in \mathcal{S}^n\right] \leq \exp(-\alpha \lambda |\mathcal{G}|)(1 + \exp(-n\epsilon + \alpha))|\mathcal{G}|^n\ln |\mathcal{S}|
\leq \exp(-n\epsilon \lambda |\mathcal{G}| + |\mathcal{G}| \ln 2 + n \ln |\mathcal{S}|)
\]

(73)

where (a) follows due to (71) and (72); while (b) by choosing \(\alpha = n\epsilon\). Now, if we make sure that

\[
|\mathcal{G}| > \frac{1}{\epsilon \lambda} \ln |\mathcal{S}|
\]

(74)

then by (73) the average probability of error of \(\mathcal{C}_{cr}^*\) is smaller than \(\lambda\) with a probability that approaches one exponentially fast. We now turn to the secrecy performance.
of $\tilde{C}_s$. Due to the way $\tilde{C}_s$ was constructed, we have
\begin{equation}
\max_{s^n \in \mathbb{S}^n} \max_{\gamma \in \tilde{G}} I(M; Z^n_{\gamma, s^n}|\tilde{C}_s) \\
\leq \max_{s^n \in \mathbb{S}^n} \max_{\gamma \in \tilde{G}} I(M; Z^n_{\gamma, s^n}|C^s_{cr}) \\
\leq e^{-n\tilde{C}}
\end{equation}
where $\tilde{C} > 0$. The last step follows from the achievability proof of [23, Theorem 6]. This implies that for an AVWC ($\mathcal{W}, \mathcal{Y}$), we can construct a correlated random code that only utilizes a finite set of shared common randomness, where the cardinality of $\tilde{G}$ is given by (74), such that the constraints in (69) and (70) are satisfied with high probability. This completes our proof. $\square$

4.3. Proof of Theorem 4.2. In this section, we derive a coding scheme to prove Theorem 4.2. Our coding scheme is based on transforming the correlated random code with finite resources $C_{cr}$ constructed in the previous section into a list code. This transformation is similar to one used in Section 3.3.

Proof: Our proof consists of 5 main steps as follows:

1- Code Structure: We construct a list code $C^s_{list}$ of Definition 2.13 with list size $L$ and block length $n = n + \tilde{n}$ by concatenating a deterministic list code $C_{list}$ of Definition 2.9 with list size $L$ and block length $n$ and the correlated random code $\tilde{C}$ with block length $\tilde{n}$ constructed as described in the previous section such that it only utilizes a finite set of shared common randomness $\tilde{G}$. In our construction, we let the set of public messages $C_p$ encoded by the list code $C_{list}$ to be identical to the set of values of the common randomness $\tilde{G}$ used by the correlated random code $\tilde{C}$, i.e. $C_p = \tilde{G}$. Additionally, we set the list size $L$ as follows: $L = |\tilde{G}| = |C_p|$.

2- Encoding: Given a confidential message $m_c \in C_c$, the encoder chooses an index $\gamma \in \tilde{G}$ uniformly at random and encodes it using the list code $C_{list}$ producing a codeword $\tilde{x}^{\tilde{n}}(\gamma)$. After that $m_c$ and $\gamma$ are then given to the encoder of the correlated random code $\tilde{C}$ which outputs a codeword $\tilde{x}^\tilde{n}(m_c)$. Finally the encoder concatenates the two codewords producing $x^n(\gamma, m_c) = (\tilde{x}^\tilde{n}(m_c), \tilde{x}^\tilde{n}(m_c))$ and transmits it.

3- Decoding: Having received $y^n = (y^\tilde{n}, y^\tilde{n})$, the decoding process is sequential as follows: First $y^\tilde{n}$ is given to the decoder of the list code $C_{list}$ to produce a list of size $L$, i.e. $\varphi_L(y^\tilde{n}) = \tilde{J} \in \mathbb{J}_L(\tilde{G})$. Then for every $\tilde{\gamma} \in \tilde{J}$, we use $y^\tilde{n}$ along with the decoder $\varphi^\tilde{n}$ of the correlated random code $\tilde{C}$ to find a corresponding confidential message $\tilde{m}_c \in C_c$. Thus, our decoder can be expressed as follows:
\[
\varphi_L(y^n) = \tilde{J} \in \mathbb{J}_L(\tilde{G} \times C_c) \\
= \{(\tilde{\gamma}, \tilde{m}_c) \in \tilde{G} \times C_c : \tilde{\gamma} \in \varphi_L(y^\tilde{n}) \text{ and } \tilde{m}_c = \varphi^\tilde{n}(y^\tilde{n})\}.
\]

4- Reliability Analysis: Based on our coding scheme, we can bound the average probability of error of $C^s_{list}$ given by (32) in terms of the average error probability of $C_{list}$ given by (23) and the average error probability of $\tilde{C}$ given by (16) as follows:
\begin{equation}
\varepsilon_L(C^s_{list}) \leq \varepsilon_L(C_{list}) + \varepsilon(\tilde{C}_s).
\end{equation}
$C_{list}$ is a deterministic list code with list size $L$ used to transmit the public message $\gamma \in C_p$ where $L = |C_p|$. This implies that $C_{list}$ always makes a correct decoding decision. Thus, the first term in (76) vanishes, i.e. $\varepsilon_L(C_{list}) = 0$. On the other hand,
according to the proof of Lemma 4.3 if we choose the amount of shared randomness $\hat{\Gamma}$ utilized by the correlated random code $\hat{\mathcal{C}}_{cr}$ such that $|\mathcal{G}|$ satisfies the constraint in (74), then the second term in (76) is less than $W$.

Thus, we have

$$P[\varepsilon_L(\mathcal{C}_{list}) \leq \lambda] \xrightarrow{n \to \infty} 1.$$

(77)

5- Secrecy Analysis: Let $\hat{\Gamma}$ be a uniformly distributed random variable over the set $\mathcal{G}$. Then, based on the structure of our coding scheme, the secrecy constraint in (33) can be bounded as follows:

$$\max_{s^n \in \mathcal{S}^n} I(M_c; Z^n_{s^n} | M_c \mathcal{C}_{list}) \overset{(a)}{=} \max_{s^n \in \mathcal{S}^n} I(M_c; Z^n_{s^n} | M_c \mathcal{C}_{list}^s) + \max_{s^n \in \mathcal{S}^n} I(M_c; Z^n_{s^n} | \hat{\mathcal{C}}_{cr}^s)$$

$$\overset{(b)}{=} \max_{s^n \in \mathcal{S}^n} I(M_c; Z^n_{s^n} | M_c \mathcal{C}_{list}^s)$$

$$\overset{(c)}{=} \max_{s^n \in \mathcal{S}^n} I(M_c; Z^n_{s^n} | \hat{\mathcal{C}}_{cr}^s)$$

$$\leq \max_{s^n \in \mathcal{S}^n} \frac{1}{|\mathcal{G}|} \sum_{\gamma \in \mathcal{G}} I(M_c; Z^n_{s^n, \gamma} | \hat{\mathcal{C}}_{cr}^s)$$

$$\leq \max_{s^n \in \mathcal{S}^n} \frac{1}{|\mathcal{G}|} \sum_{\gamma \in \mathcal{G}} \frac{1}{\gamma}$$

(78)

where $(a)$ follows from the mutual information chain rule; $(b)$ follows because $M_c$ and $Z^n_{s^n} \in \mathcal{S}$ are independent; $(c)$ follows because $\hat{\Gamma}$ is identical to $M_p$ and the fact that $M_c$ is only encoded using $\hat{\mathcal{C}}_{cr}^s$; $(d)$ follows from the secrecy analysis of the correlated random code $\hat{\mathcal{C}}_{cr}^s$ as in (75), where $\epsilon > 0$.

Now in order to finalize our proof, we need to show that the overall transmission rate of the constructed list code $\mathcal{C}_{list}$ is equivalent to the transmission rate of the correlated random code $\hat{\mathcal{C}}_{cr}^s$. Since $\hat{n} = \mathcal{O}(\log L)$ where $L$ is given by (74). This implies that $\hat{n} + n \to n$ as $n \to \infty$, which means that using the prefix code $\hat{\mathcal{C}}_{pre}$ on top of $\hat{\mathcal{C}}_{ran}$ does not affect the overall transmission rate.

5. Conclusion and Future Work

In this paper, we studied secure communication over AVWCs. We showed that list codes can overcome the drawbacks of both correlated and uncorrelated codes, such that they can be used to establish a reliable and secure communication over a symmetrizable AVWCs in the absence of coordination resources. We provided a full characterization of the list secrecy capacity of the AVWC (29, 30) showing that if the list size $L$ is greater than the order of symmetrizability of $\mathcal{W}$ denoted by $L(\mathcal{W})$, then the list secrecy capacity is equivalent to the correlated random secrecy capacity. Otherwise it is zero. Our analysis emphasizes that their exist list codes that can achieve such capacity without enforcing any assumptions on the communication between the active jammer and the passive eavesdropper. This results implies for a sufficiently large list size $L$, list codes can always provide a secrecy rate up to the correlated random secrecy capacity. Thus, list codes can solve the instability of the secrecy capacity of AVWCs. Finally, we showed that if we relax the reliability constraint, we can construct list codes whose rates is close to the correlated random...
secrecy capacity using a finite list size $L$ that only depends on the requested average error probability and is independent of the order of symmetrizability.

The characterization of the list secrecy capacity established in this paper is a necessary step in understanding the behavior of the secrecy capacity function of AVWCs under list decoding. In future work, it would be of high interest to analyze the continuity behavior of the capacity function which will allow us to investigate its Turing computability. Further, it would be also interesting to study, whether the list secrecy capacity exhibits super-additivity and super-activation behavior or not. The answers to these questions require a better understanding of the $L$-symmetrizability condition and the development of more explicit examples.

ACKNOWLEDGMENTS

The work of A. S. Mansour was supported by the Gottfried Wilhelm Leibniz program of the German Research Foundation (DFG) under Grant BO 1734/20-1. The work of H. Boche was supported by the German Research Foundation (DFG) under Grants BO 1734/24-3 and BO 1734/25-1.

REFERENCES

[1] R. Ahlswede, Elimination of correlation in random codes for arbitrarily varying channels, Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete, 44 (1978), 159–175.
[2] I. Bjelaković, H. Boche and J. Sommerfeld, Capacity results for arbitrarily varying wiretap channels, Information Theory, Combinatorics, and Search Theory, Springer-Verlag, New York, NY, USA, 7777 (2013), 123–144.
[3] D. Blackwell, L. Breiman and A. J. Thomasian, The capacities of certain channel classes under random coding, The Annals of Mathematical Statistics, 31 (1960), 558–567.
[4] V. M. Blinovskii, P. Narajan and M. S. Pinsker, Capacity of the arbitrarily varying channel under list decoding, Problems Inform. Transmission, 2 (1995), 99–113.
[5] M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering, Cambridge University Press, 2011.
[6] H. Boche and R. F. Schaefer, Arbitrarily varying multiple access channels with conferencing encoders: List decoding and finite coordination resources, Adv. in Math. of Comm., 10 (2016), 333–354.
[7] H. Boche, R. F. Schaefer and H. V. Poor, On the continuity of the secrecy capacity of compound and arbitrarily varying wiretap channels, IEEE Trans. Inf. Forensics and Security, 10 (2015), 2531–2546.
[8] H. Boche, R. F. Schaefer and H. V. Poor, Identification over Channels with Feedback: Discontinuity Behavior and Super-Activation IEEE International Symposium on Information Theory Proceedings (ISIT), Colorado, USA, (2018), 256–260.
[9] H. Boche, R. F. Schaefer and H. V. Poor, Identification Capacity of Channels with Feedback: Discontinuity Behavior, Super-Activation, and Turing Computability, Under submission, 2018.
[10] H. Boche and R. F. Schaefer, Arbitrarily varying wiretap channels with finite coordination resources, 2014 IEEE International Conference on Communications Workshops (ICC), Sydney, Australia, (2014), 746–751.
[11] I. Csiszar and P. Narayan, The capacity of the arbitrarily varying channel revisited: Positivity, constraints, IEEE Trans. Inf. Theory, 34 (1988), 181–193.
[12] I. Csiszár and J. Körner, Information Theory: Coding Theorems for Discrete Memoryless Systems, Cambridge University Press, 2011.
[13] G. Fettweis, H. Boche, T. Wiegand and E. Zieglsieni et al., The tactile Internet, ITU-T Technology Watch, August, 2014, Available at: http://www.itu.int/oth/T2301000023/en.
[14] Deutsche Telekom AG Laboratories, Next Generation Mobile Networks – (R)evolution in Mobile Communications, Technology Radar Edition III, 2010.
[15] U. Helmbrecht and R. Plaga, New challenges for IT-security research in ICT, 40th World Federation of Scientists, International Seminars on Planetary Emergencies, Erice, Italy, August, (2008), 1–6.
B. L. Hughes, The smallest list for the arbitrarily varying channel, *IEEE Trans. Inf. Theory*, **43** (1997), 803–815.

A. Lapidoth and P. Narayan, Reliable communication under channel uncertainty, *IEEE Trans. Inf. Theory*, **44** (1998), 2148–2177.

Y. Liang, H. V. Poor and S. Shamai, Information theoretic security, *Found. Trends Commun. Inf. Theory*, **5** (2009), 355–580.

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

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

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

S. Nitinawarat, On the deterministic code capacity region of an arbitrarily varying multiple-access channel under list decoding, *IEEE Trans. Inf. Theory*, **59** (2013), 2683–2693.

J. Nötzel, M. Wiese and H. Boche, The arbitrarily varying wiretap channel – secret randomness, stability, and super-activation, *IEEE Trans. Inf. Theory*, **62** (2016), 3504–3531.

R. F. Schaefer and H. Boche, Physical layer service integration in wireless networks: Signal processing challenges, *IEEE Signal Processing Magazine*, **31** (2014), 147–156.

R. F. Schaefer, H. Boche and H. V. Poor, Super-Activation as a Unique Feature of Secure Communication in Malicious Environments, *Information*, **7** (2016), 24.

M. Wiese and 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*, **62** (2016), 3841-3862.

A. D. Wyner, The wire-tap channel, *Bell Syst. Tech. J.*, **54** (1975), 1355–1387.