Arbitrarily Varying Wiretap Channels with Type Constrained States

Ziv Goldfeld, Paul Cuff and Haim H. Permuter

***Abstract*—The arbitrarily varying wiretap channel (AVWTC) is an open problem largely because of two main challenges. Not only does it capture the difficulty of the compound wiretap channel (another open problem) as a special case, it also requires that secrecy is ensured with respect to exponentially many possible channel state sequences. This work overcomes the second aforementioned difficulty. To that end, we consider an AVWTC with a type constraint on the allowed state sequences, and derive a single-letter characterization of its correlated-random (CR) assisted semantic-security (SS) capacity. The allowed state sequences are the ones in a typical set around a single constraining type. SS is established by showing that the mutual information between the message and the eavesdropper's observations is negligible even when maximized over all message distributions, choices of state sequences and realizations of the CR-code.**

Both the achievability and the converse proofs of the type constrained coding theorem rely on stronger claims than actually required. The direct part establishes a novel single-letter lower bound on the CR-assisted SS-capacity of an AVWTC with state sequences constrained by any convex and closed set of state probability mass functions. This bound achieves the best known single-letter secrecy rates for a corresponding compound wiretap channel over the same constraint set. In contrast to other single-letter results in the AVWTC literature, the derivation does not assume the existence of a best channel to the eavesdropper. Optimality is a consequence of an max-inf upper bound on the CR-assisted SS-capacity of an AVWTC with state sequences constrained to any collection of type-classes. When adjusted to the aforementioned compound WTC, the upper bound simplifies to a max-min structure, thus strengthening the previously best known single-letter upper bound by Liang *et al.* that has a min-max form.

I. INTRODUCTION

Modern communication systems usually present an architectural separation between error correction and data encryption. The former is typically realized at the physical layer by transforming the noisy communication channel into a reliable "bit pipe". The data encryption is implemented on top of that by applying cryptographic principles. The cryptographic approach assumes no knowledge on the quality of the eavesdropper's channel and relies solely on restricting the computational power of the eavesdropper. However, as the construction of quantum computers edges closer (D-Wave company recently reported a working prototype of a quantum computer with over than 1000 qbits), the validity of the restricted computational power assumption comes into question. Nonetheless, cryptography remains the main practical tool for protecting data, at least for the time being.

An alternative approach to secure communication is the so-called physical layer security, a concept that dates back to Wyner's celebrated paper on the wiretap channel (WTC) [1]. Essentially, Wyner's main idea was to exploit the noise of the communication channel along with proper physical layer coding to guarantee secrecy against a computationally-unlimited eavesdropper. Protection against such an eavesdropper, however, comes at a price of assuming that the eavesdropper's channel is perfectly known to the legitimate parties and stays fixed during the transmission. Many of the information-theoretic secrecy results that followed relied on extending Wyner's ideas, and therefore, are derived under the same hypothesis. Much of the critique by the cryptographic community towards information-theoretic security is aimed exactly at that assumption.

Practical systems suffer from limited channel state information (CSI) due to inaccuracies in the channel's estimation process and imperfect feedback. Furthermore, adversarial eavesdroppers will refrain from providing the legitimate parties with any information about their channels to make securing the data even harder. Accordingly, limited CSI (especially about the eavesdropper's channel) must be assumed to successfully model a practical communication system. The model of an arbitrarily varying WTC (AVWTC), that is the focus of this work, does just that. The AVWTC combines the WTC [1] and the arbitrarily varying channel (AVC) [2], [3]. It consists of a collection of discrete-memoryless WTCs indexed by elements in a finite state space. The state at each time instance is chosen in an arbitrary manner and is unknown to the legitimate parties. Being aware of the state space, however, the legitimate users can place the actual channel realization within a certain uncertainty set, which models their limited eavesdropper's CSI.

The challenge presented by the AVWTC is twofold. First, it subsumes the difficulty of the compound WTC (where the channel's state is constant in time), for which a single-letter secrecy-capacity characterization is also an open problem [4], [5]. A multi-letter description of the compound WTC's secrecy-capacity was found in [5]. It is, however, currently unknown how to single-letterize this expression. The underlying gap is that while reliability must be ensured with respect to the worst main channel, security is measured under the best eavesdropper channel; a single channel state under which these extremes simultaneously materialize, however, does not necessarily exist. The second difficulty concerning AVWTCs is that security must be ensured under all possible state sequences, whose number grows exponentially with the blocklength. To get single-letter results, the latter is usually dealt with by assuming the existence of *a best channel to the eavesdropper* and establishing secrecy with respect to that channel only (see, e.g., [6], [7]). Yet, the only single-letter secrecy-capacity characterization for an AVWTC that the authors are aware of assumes even more [6, Theorem 4]. On top of the existence of such a best channel, the derivation of [6, Theorem 4] also relies on the AVWTC being strongly-degraded and having independent (main channel and eavesdropper channel) states.

This work gives a full solution to the second difficulty. We consider a general AVWTC with a type constraint on the allowed state sequences, and establish in Theorem 1 a single-letter characterization of its CR-assisted semantic-security (SS) capacity. The type constraint essentially means that the viable state sequences are only the ones of the prescribed type. However, since a fixed distribution (even if rational) is not a valid type for all blocklengths, we define achievability by allowing the empirical distribution of the state sequences to be within a small gap from the type. By doing so, the type constrained AVWTC is well defined for all blocklengths. As a consequence, our uncertainty set is a typical set around the allowed type, which still contains exponentially many state sequences. The structure of the CR-assisted SS-capacity formula suggests that the legitimate users effectively see the averaged channel (i.e., the expectation of the main channels with respect to the type) while security must be ensured versus an eavesdropper with perfect CSI. A specific instance of a type constrained AVWTC that is related to binary symmetric - binary erasure (BS-BE) WTC that was studies in [8] is used to visualize the result.

The results are derived while adopting the prescription of [9] to replace the commonly used strong secrecy metric with the stricter SS metric. The authors of [9] advocate SS as the new standard for information-theoretic security, because from a cryptographic point of view, strong secrecy is insufficient to provide security of applications. Its main drawback lies in the assumption that the message is random and uniformly distributed, as real-life messages are neither (messages may be files, votes or any type of structured data, often with low entropy). In turn, the uniformly distributed message makes the strong secrecy metric an average quantity, that might converge even when many[1] of the messages are actually not secured. Furthermore, to eliminate the benefit of CR for secrecy purposes, we demand that SS holds for each realization of the CR (a similar approach was taken in [10] with respect to the strong secrecy metric). This essentially means that the transmission is semantically-secure even if the choice of the state sequence depends on the realization of the CR.

To prove our coding theorem for the type constrained AVWTC (i.e., the main result in Theorem 1), we provide both a stronger achievability and a stronger converse than is actually required. The broader achievability claim, found in Theorem 2, is a lower bound on the CR-assisted SS-capacity of an AVWTC with state sequences constrained by any convex and closed set of state PMFs. This bound shows that the best known achievable single-letter secrecy rates for a similarly constrained compound WTC [4], [5] can be achieved also in the AVWTC. The converse of Theorem 1 is a consequence of Theorem 3 that states an upper bound on CR-assisted SS-capacity of an AVWTC with state sequences from any collection of type-classes. The upper bound is of an max-inf form, i.e., first an infimum over the constraint set is taken, and then the result is maximized over the input distributions. When specializing the result to the aforementioned compound WTC, it produces an upper bound that improves upon the previously best known single-letter upper bound for this setting [4, Theorem 2]. The latter result has a min-max structure, while our upper bound has a max-min form.

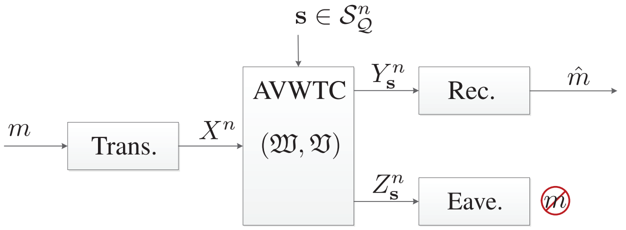

Fig. 1: The AVWTC with $\mathcal{Q}$-constrained states, i.e., when the allowed state sequences have empirical PMFs that belong to $\mathcal{Q}$.

II. Problem Setup and Definitions

We use notation from [11, Section II]. In particular, the set of all probability mass functions (PMFs) on a finite set $\mathcal{X}$ is denoted by $\mathcal{P}(\mathcal{X})$. The type $\nu_\mathbf{x}$ of a sequence $\mathbf{x}\in\mathcal{X}^n$ is $\nu_\mathbf{x}(x)\triangleq\frac{N(x|\mathbf{x})}{n}$, where $N(x|\mathbf{x})=\sum_{i=1}^n\mathbb{1}_{\{x_i=x\}}$. The subset of $\mathcal{P}(\mathcal{X})$ that contains all possible types of sequences $\mathbf{x}\in\mathcal{X}^n$ is denoted by $\mathcal{P}_n(\mathcal{X})$. For $P\in\mathcal{P}_n(\mathcal{X})$, the type-class $\big\{\mathbf{x}\in\mathcal{X}^n\big|\nu_\mathbf{x}=P\big\}$ is denoted by $\mathcal{T}_P^n$. We use $\mathcal{T}_\epsilon^n(P)$ to denote the set of letter-typical sequences with respect to the PMF $P\in\mathcal{P}(\mathcal{X})$ and the non-negative number ϵ defined by

$$\mathcal{T}_\epsilon^n(P)=\left\{\mathbf{x}\in\mathcal{X}^n\middle|\big|\nu_\mathbf{x}(x)-P(x)\big|\leq\frac{\epsilon}{|\mathcal{X}|}\mathbb{1}_{\{P(x)>0\}},\ \forall x\in\mathcal{X}\right\},$$

where $\mathbb{1}_\mathcal{A}$ is the indicator function on the event $\mathcal{A}$.

Let $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ and $\mathcal{S}$ be finite sets. A discrete-memoryless (DM) arbitrarily varying wiretap channel (AVWTC), as illustrated in Fig. 1, is defined by a pair $(\mathfrak{W},\mathfrak{V})$ of families of channels $\mathfrak{W}=\big\{W_s:\mathcal{X}\to\mathcal{P}(\mathcal{Y})\big|s\in\mathcal{S}\big\}$ and $\mathfrak{V}=\big\{V_s:\mathcal{X}\to\mathcal{P}(\mathcal{Z})\big|s\in\mathcal{S}\big\}$, from $\mathcal{X}$ to $\mathcal{Y}$ and $\mathcal{Z}$, respectively. Thus, $s\in\mathcal{S}$ denotes the state of the channels and can be interpreted as an index identifying a particular pair $(W,V)\in\mathfrak{W}\times\mathfrak{V}$.

The n-th extension of the channel laws for input $\mathbf{x}\in\mathcal{X}^n$ and outputs $\mathbf{y}\in\mathcal{Y}^n$ and $\mathbf{z}\in\mathcal{Z}^n$, under the state sequence $\mathbf{s}\in\mathcal{S}^n$ are $W_\mathbf{s}^n(\mathbf{y}|\mathbf{x})\triangleq\prod_{i=1}^n W_{s_i}(y_i|x_i)$ and $V_\mathbf{s}^n(\mathbf{z}|\mathbf{x})\triangleq\prod_{i=1}^n V_{s_i}(z_i|x_i)$. The corresponding families of n-fold channels $W_\mathbf{s}^n$ and $V_\mathbf{s}^n$, for $\mathbf{s}\in\mathcal{S}^n$, are denoted by $\mathfrak{W}^n$ and $\mathfrak{V}^n$, respectively, and $(\mathfrak{W}^n,\mathfrak{V}^n)$ is referred to as the (n-fold) AVWTC. The random variables representing the outputs of the AVWTC $(\mathfrak{W}^n,\mathfrak{V}^n)$ observed by the legitimate user

[1] The number of unsecured messages may even grow exponentially with the blocklength, while still having a converging strong secrecy metric.

and by the eavesdropper under the state sequence $\mathbf{s} \in \mathcal{S}^n$ are denoted by $Y^n_{\mathbf{s}}$ and $Z^n_{\mathbf{s}}$, respectively.

For any $\mathcal{Q} \subseteq \mathcal{P}(\mathcal{S})$ define

$$\mathcal{S}^n_{\mathcal{Q}} \triangleq \left\{ \mathbf{s} \in \mathcal{S}^n \middle| \nu_{\mathbf{s}} \in \mathcal{Q} \right\}. \tag{1}$$

We impose a constraint $\mathcal{Q}$ on the allowed state sequences, i.e., only $\mathbf{s} \in \mathcal{S}^n_{\mathcal{Q}}$ are permitted. The triple $(\mathfrak{W}^n, \mathfrak{V}^n, \mathcal{Q})$ is referred to as the (n-fold) *$\mathcal{Q}$-constrained AVWTC*.

Definition 1 (Uncorrelated Code) *An uncorrelated (n, M_n)-code c_n for the AVWTC $(\mathfrak{W}^n, \mathfrak{V}^n)$ has a message set $\mathcal{M} = [1 : M_n]$, a stochastic encoder $f : \mathcal{M} \to \mathcal{P}(\mathcal{X}^n)$ and decoder $\phi : \mathcal{Y}^n \to \hat{\mathcal{M}}$, where $\hat{\mathcal{M}} \triangleq \mathcal{M} \cup \{e\}$ and $e \notin \mathcal{M}$ is an error symbol.*

For any uncorrelated (n, M_n)-code c_n and state sequence $\mathbf{s} \in \mathcal{S}^n$, the induced PMF on $\mathcal{M} \times \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n \times \hat{\mathcal{M}}$ is

$$\begin{aligned} P^{(c_n,\mathbf{s})}_{M,\mathbf{X},\mathbf{Y}_{\mathbf{s}},\mathbf{Z}_{\mathbf{s}},\hat{M}}(m, \mathbf{x}, \mathbf{y}, \mathbf{z}, \hat{m}) \triangleq& P_M(m) f(\mathbf{x}|m) W^n_{\mathbf{s}}(\mathbf{y}|\mathbf{x}) \\ &\times V^n_{\mathbf{s}}(\mathbf{z}|\mathbf{x}) \mathbb{1}_{\left\{\hat{m}=\phi(\mathbf{y})\right\}}, \end{aligned} \tag{2}$$

where $P_M \in \mathcal{P}(\mathcal{M})$. The performance of c_n on the type constrained AVWTC $(\mathfrak{W}^n, \mathfrak{V}^n, Q_S)$ is evaluated in terms of its rate $\frac{1}{n} \log M_n$, the maximal decoding error probability and the SS-metric. Reliability and security must be ensured with respect to every allowed constrained state sequence.

Definition 2 (Message Error Probability) *Let c_n be an uncorrelated (n, M_n)-code for the AVWTC $(\mathfrak{W}^n, \mathfrak{V}^n)$. For any $m \in \mathcal{M}$ and $\mathbf{s} \in \mathcal{S}^n$, let the error probability in decoding m under the state sequence $\mathbf{s}$ be*

$$e_m(W^n_{\mathbf{s}}, c_n) = \sum_{\mathbf{x} \in \mathcal{X}^n} f(\mathbf{x}|m) \sum_{\substack{\mathbf{y} \in \mathcal{Y}^n: \\ \phi(\mathbf{y}) \neq m}} W^n_{\mathbf{s}}(\mathbf{y}|\mathbf{x}). \tag{3}$$

Definition 3 (SS Metric) *Let c_n be an uncorrelated (n, M_n)-code for the AVWTC $(\mathfrak{W}^n, \mathfrak{V}^n)$. The information leakage to the eavesdropper under the state sequence $\mathbf{s} \in \mathcal{S}^n$ and the message PMF $P_M \in \mathcal{P}(\mathcal{M})$ is*

$$\ell(V^n_{\mathbf{s}}, P_M, c_n) = I_{c_n}(M; \mathbf{Z}_{\mathbf{s}}), \tag{4}$$

where the subscript c_n denotes that the mutual information term is taken with respect to the marginal PMF $P^{(c_n,\mathbf{s})}_{M,\mathbf{Z}_{\mathbf{s}}}$ of (2). *For any $\mathcal{Q} \subseteq \mathcal{P}(\mathcal{S})$, the SS metric with respect to c_n and the $\mathcal{Q}$-constrained AVWTC $(\mathfrak{W}^n, \mathfrak{V}^n, \mathcal{Q})$ is* [2]

$$\ell_{\mathrm{Sem}}(\mathfrak{V}^n, \mathcal{Q}, c_n) = \max_{\substack{\mathbf{s} \in \mathcal{S}^n_{\mathcal{Q}}, \\ P_M \in \mathcal{P}(\mathcal{M})}} \ell(V^n_{\mathbf{s}}, P_M, c_n). \tag{5}$$

Remark 1 *We use the convention that the maximum over an empty set is $-\infty$. Accordingly, if $\mathcal{Q}$ contains no rational distributions then $\ell_{\mathrm{Sem}}(\mathfrak{V}^n, \mathcal{Q}, c_n) = -\infty$, for all $n \in \mathbb{N}$. Even when there exists $Q_S \in \mathcal{P}_n(\mathcal{S})$ such that $Q_S \in \mathcal{Q}$, there are blocklengths n for which $\nu_{\mathbf{s}} \neq Q_S$ for every $\mathbf{s} \in \mathcal{S}^n$, and consequently, $\ell_{\mathrm{Sem}}(\mathfrak{V}^n, \mathcal{Q}, c_n) = -\infty$ for these values of n as well.*

Remark 2 *SS requires that the uncorrelated code c_n works well for all message PMFs. This means that the mutual information term in* (5) *is maximized over P_M when c_n is known. In other words, although not stated explicitly, the optimal P_M is a function of c_n.*

We proceed with defining correlated random (CR) codes, their associated maximal error probability and SS-metric, CR-assisted achievability and CR-assisted secrecy-capacity.

Definition 4 (CR Code, Error Probability and SS Metric) *A CR (n, M_n, K_n)-code $\mathbb{C}_n$ for the AVWTC $(\mathfrak{W}^n, \mathfrak{V}^n)$ is given by a family of uncorrelated (n, M_n)-codes $\mathcal{C}_n = \left\{c_n(\gamma)\right\}_{\gamma \in \Gamma_n}$, where $\Gamma_n = [1 : K_n]$, and a PMF $\mu_n \in \mathcal{P}(\Gamma_n)$. For any $m \in \mathcal{M}$ and $\mathbf{s} \in \mathcal{S}^n$, the associated error probability with respect to $\mathbb{C}_n$ is*

$$\mathcal{E}_m(W^n_{\mathbf{s}}, \mathbb{C}_n) = \sum_{\gamma \in \Gamma_n} \mu_n(\gamma) e_m\big(W^n_{\mathbf{s}}, c_n(\gamma)\big) \tag{6}$$

The maximal error probability and SS-metric of $\mathbb{C}_n$ for the $\mathcal{Q}$-constrained AVWTC $(\mathfrak{W}^n, \mathfrak{V}^n, \mathcal{Q})$ are defined as

$$\mathcal{E}(\mathfrak{W}^n, \mathcal{Q}, \mathbb{C}_n) = \max_{\substack{\mathbf{s} \in \mathcal{S}^n_{\mathcal{Q}}, \\ m \in \mathcal{M}}} \mathcal{E}_m(W^n_{\mathbf{s}}, \mathbb{C}_n) \tag{7a}$$

$$\mathcal{L}_{\mathrm{Sem}}(\mathfrak{V}^n, \mathcal{Q}, \mathbb{C}_n) = \max_{\gamma \in \Gamma_n} \ell_{\mathrm{Sem}}\big(\mathfrak{V}^n, \mathcal{Q}, c_n(\gamma)\big). \tag{7b}$$

Remark 3 *The choice of encoder-decoder in a CR code is based on a realization of a random experiment that is available to the transmitted and the legitimate receiver. However, this CR the legitimate users share should not be viewed as a cryptographic key to be exploited for secrecy. This is accounted for in* (7b) *by requiring that every uncorrelated code in the family $\mathcal{C}_n$ is semantically-secure. The choice of the state sequence, on the other hand, may depend on the family $\mathcal{C}_n$ and the PMF μ_n, but not on the realization itself.*

Definition 5 (CR-Assisted Achievability) *A number $R \in \mathbb{R}_+$ is called an achievable CR-assisted SS-rate for the $\mathcal{Q}$-constrained AVWTC $(\mathfrak{W}^n, \mathfrak{V}^n, \mathcal{Q})$, if for every $\epsilon > 0$ and sufficiently large n, there exists a CR (n, M_n, K_n)-code $\mathbb{C}_n$ with*

$$\frac{1}{n} \log M_n > R - \epsilon \tag{8a}$$

$$\mathcal{E}(\mathfrak{W}^n, \mathcal{Q}, \mathbb{C}_n) \leq \epsilon \tag{8b}$$

$$\mathcal{L}_{\mathrm{Sem}}(\mathfrak{V}^n, \mathcal{Q}, \mathbb{C}_n) \leq \epsilon. \tag{8c}$$

Remark 4 *Note that if there are no types in $\mathcal{Q}$ then any rate is achievable. Consequently, if $\mathcal{Q}_1 \subseteq \mathcal{Q}_2 \subseteq \mathcal{P}(\mathcal{S})$, then any R that is achievable for the $\mathcal{Q}_2$-constrained AVWTC is also achievable for the $\mathcal{Q}_1$-constrained AVWTC. The achievable rates are therefore an increasing set as the constraint set decreases.*

Definition 6 (CR-Assisted Capacity) *The CR-assisted SS-capacity $C_{\mathrm{R}}(\mathfrak{W}, \mathfrak{V}, \mathcal{Q})$ of the $\mathcal{Q}$-constrained AVWTC is the supremum of the set of achievable CR-assisted SS-rates.*

[2] $\ell_{\mathrm{Sem}}(\mathfrak{V}^n, \mathcal{Q}, c_n)$ is actually the mutual-information-security (MIS) metric, which is equivalent to SS by [9]. We use the representation in (5) rather than the formal definition of SS (see, e.g., [9, Equation (4)]) out of analytical convenience.

Our main goal is solving the type constrained AVWTC $(\mathfrak{W}^n,\mathfrak{V}^n,Q_S)$, for $Q_S\in\mathcal{P}_n(\mathcal{S})$. However, since a fixed rational distribution Q_S is not a valid type for all blocklengths, the definitions of the type constrained performance metrics and its achievability user a relaxation parameter. For any $Q_S\in\mathcal{P}(\mathcal{S})$ and $\delta>0$, let $\mathcal{Q}_\delta(Q_S)\triangleq\left\{\nu_{\mathbf{s}}\in\mathcal{P}_n(\mathcal{S})\middle|\mathbf{s}\in\mathcal{T}^n_\delta(Q_S)\right\}$.

The definitions of the error probability and the SS-metric for the type constrained AVWTC repeat those from Definition 4 with $\mathcal{Q}_\delta(Q_S)$ instead of $\mathcal{Q}$. The CR-assisted SS-capacity $C_{\mathrm{R}}(\mathfrak{W},\mathfrak{V},Q_S)$ of the type constrained AVWTC is defined as $C_{\mathrm{R}}(\mathfrak{W},\mathfrak{V},Q_S)=\sup_{\delta>0}C_{\mathrm{R}}\big(\mathfrak{W},\mathfrak{V},\mathcal{Q}_\delta(Q_S)\big)$.

III. Single-Letter CR-Capacity Results and Discussion

Our main result is a single-letter characterization of the CR-assisted SS-capacity $C_{\mathrm{R}}(\mathfrak{W},\mathfrak{V},Q_S)$ of the type constrained AVWTC $(\mathfrak{W}^n,\mathfrak{V}^n,Q_S)$, for any $Q_S\in\mathcal{P}(\mathcal{S})$. To the best of our knowledge, the only single-letter characterization of a secrecy-capacity of an AVWTC outside the current work [6, Theorem 4] is under the following assumptions: (i) security under the weak secrecy metric (as shown in [10, Corollary 1] an upgrade to strong secrecy under the same conditions (ii)-(iv) is possible); (ii) the state space decomposes as $\mathcal{S}=\mathcal{S}_y\times\mathcal{S}_z$, where $s_y\in\mathcal{S}_y$ and $s_z\in\mathcal{S}_z$ are the states of the main AVC and of the AVC to the eavesdropper, respectively; (iii) the eavesdroppers output is a degraded version of the output of the main AVC under any pair of state, i.e., $X-Y_{s_y}-Z_{s_z}$ forms a Markov chain, for all $(s_y,s_z)\in\mathcal{S}_y\times\mathcal{S}_z$; (iv) there exists a best channel to the eavesdropper, i.e., the exists $s_z^\star\in\mathcal{S}_z$ such that $X-Z_{s_z^\star}-Z_{s_z}$ forms a Markov chain, for all $s_z\in\mathcal{S}_z$. [3]

Our single-letter CR-capacity characterization is derived without assuming any of the above, while upgrading the secrecy metric to SS.

Theorem 1 (AVWTC CR-Assisted SS-Capacity) *For any $Q_S\in\mathcal{P}(\mathcal{S})$, the CR-assisted SS-capacity of the type constrained AVWTC $(\mathfrak{W}^n,\mathfrak{V}^n,Q_S)$ is*

$$C_{\mathrm{R}}(\mathfrak{W},\mathfrak{V},Q_S)=\max_{Q_{U,X}}\Big[I(U;Y)-I(U;Z|S)\Big],\tag{9}$$

where the mutual information terms are calculated with respect to a joint PMF $Q_{U,X}Q_SQ_{Y|X,S}Q_{Z|X,S}$ with $Q_{Y|X,S}(y|x,s)=W_s(y|x)$ and $Q_{Z|X,S}(z|x,s)=V_s(z|x)$, for all $(s,x,y,z)\in\mathcal{S}\times\mathcal{X}\times\mathcal{Y}\times\mathcal{Z}$, and $|\mathcal{U}|\leq|\mathcal{X}|$.

Theorem 1 is an outcome of two other stronger results that state a lower and upper bound on the CR-assisted SS-capacity of a general $\mathcal{Q}$-constrained AVWTC. These bounds match when specialized to the type constrained scenario. The lower and upper bounds are given in Theorem 2 and 3, respectively. The derivation of Theorem 1 from Theorems 2 and 3 mostly relies on standard continuity of mutual information arguments and is omitted due to space limitations (see [11, Section IV-D] for the details).

Remark 5 (SS-Capacity Interpretation) *The characterization of the CR-assisted SS-capacity $C_{\mathrm{R}}(\mathfrak{W},\mathfrak{V},Q_S)$ in* (9) *has the common structure of two subtracted mutual information terms. The first term, which corresponds to the capacity of the main channel, suggests that the legitimate users effectively see the averaged DMC $W_Q:\mathcal{X}\to\mathcal{P}(\mathcal{Y})$ defined by $W_Q(y|x)\triangleq\sum_{s\in\mathcal{S}}Q_S(s)W_s(y|x)$. In general, the capacity of the averaged channel is no larger than the capacities of the main channels W_s associated with each $s\in\mathcal{S}$. Namely, denoting the capacity of a PTP channel $W:\mathcal{X}\to\mathcal{P}(\mathcal{Y})$ by $C(W)$, it holds that $C(W_Q)\leq\min_{s\in\mathcal{S}}C(W_s)$. This is due to the convexity of the mutual information in the conditional PMF (for a fixed marginal) and Jensen's inequality.*

The second (subtracted) mutual information term is the loss in capacity induced by the secrecy requirement. The independence of U and S allows one to rewrite the conditional mutual information as $I(U;S,Z)$, which implies that security must be ensured versus an eavesdropper with perfect CSI. The formula in (9) *can also be viewed as the secrecy-capacity of the WTC with state variables that are i.i.d. according to Q_S, when no CSI is available to the legitimate users while the eavesdropper has full CSI.*

We have the following lower bound on the CR-assisted SS-capacity of a $\mathcal{Q}$-constrained AVWTC.

Theorem 2 (Achievability with $\mathcal{Q}$-constrained States) *For any convex and closed $\mathcal{Q}\subseteq\mathcal{P}(\mathcal{S})$, the CR-assisted SS-capacity of the $\mathcal{Q}$-constrained AVWTC $(\mathfrak{W}^n,\mathfrak{V}^n,\mathcal{Q})$ is lower bounded as*

$$C_{\mathrm{R}}(\mathfrak{W},\mathfrak{V},\mathcal{Q})\geq\max_{Q_{U,X}}\left[\min_{Q_S^{(1)}\in\mathcal{Q}}I(U;Y)-\max_{Q_S^{(2)}\in\mathcal{Q}}I(U;Z|S)\right],\tag{10}$$

where the mutual information terms are calculated with respect to joint PMFs $Q_{U,X}Q_S^{(j)}Q_{Y|X,S}Q_{Z|X,S}$, for $j=1,2$, with $Q_{Y|X,S}(y|x,s)=W_s(y|x)$ and $Q_{Z|X,S}(z|x,s)=V_s(z|x)$, for all $(s,x,y,z)\in\mathcal{S}\times\mathcal{X}\times\mathcal{Y}\times\mathcal{Z}$, and $|\mathcal{U}|\leq|\mathcal{X}|$.

The proof of Theorem 2 relies on the approach from [12] for the error probability analysis of a CR-code over a family of codes that grows doubly-exponentially with the blocklength. Since this family of codes is too large to establish SS in the sense of (7b), we use the Chernoff bound to show that a sub-family with no more than *polynomially* many codes is sufficient for reliability. Having that, the double-exponential decay that [11, Lemma 1] provides is leveraged to establish SS over the reduced CR-code. The fact that reliability and security must hold with respect to the worst case choice in $\mathcal{Q}$ is expressed in the minimization of $I(U;Y)$ over all $Q_S^{(1)}$ PMFs and the maximization of $I(U;Z|S)$ over $Q_S^{(2)}$. The interested reader is referred to the Section V of the full version of this work [11] for the proof of Theorem 2.

Although no converse proof accompanies Theorem 2, the lower bound it states is stronger than existing single-letter

[3] An even stronger version of assumptions (iii) and (iv) was used in [6]. Specifically, the degraded property and the existence of a best channel to the eavesdropper were assumed to hold not only for every pair of original states, but also for any pair of averaged states (defined as convex combinations of the original ones).

achievability results in the literature as it assumes no 'best channel to the eavesdropper', doesn't impose any specific structure on the state space, and ensures SS.

Remark 6 (Relation to Compound WTCs) *Theorem 2 establishes that the AVWTC is no worse than the best known single-letter secrecy rates for the compound WTC. Take the $\mathcal{Q}$-constrained AVWTC from Theorem 2 with some convex and closed $\mathcal{Q} \subseteq \mathcal{P}(\mathcal{S})$. Consider a compound WTC derived from this AVWTC. The state of the compound WTC is any point $Q_S \in \mathcal{Q}$. The compound WTC itself follows the probability law of the AVWTC, with the arbitrarily varying state S^n replaced by an i.i.d. state according to Q_S and the S^n sequence included in the channel output to the eavesdropper. For this compound WTC, the RHS of* (10) *coincides with the sharpest single-letter lower bound on the secrecy-capacity of the compound WTC in the literature (see [4, Theorem 1] and [5, Theorem]).*

A general upper bound on the CR-assisted SS-capacity of a $\mathcal{Q}$-constrained AVWTC is stated next. To state the result, for any countable alphabet $\mathcal{X}$ we defined $\mathcal{P}_{\mathbb{Q}}(\mathcal{X})$ as the set of rational PMFs on $\mathcal{X}$. Namely,

$$\mathcal{P}_{\mathbb{Q}}(\mathcal{X}) \triangleq \Big\{P \in \mathcal{P}(\mathcal{X}) \Big| P(x) \in \mathbb{Q}, \quad \forall x \in \mathcal{X}\Big\}, \tag{11}$$

where $\mathbb{Q}$ is the set of all rational numbers.

Theorem 3 (Upper Bound with $\mathcal{Q}$-constrained States) *For any $\mathcal{Q} \subseteq \mathcal{P}(\mathcal{S})$, the CR-assisted SS-capacity of the $\mathcal{Q}$-constrained AVWTC $(\mathfrak{W}^n, \mathfrak{V}^n, \mathcal{Q})$ is upper bounded as*

$$C_{\mathrm{R}}(\mathfrak{W}, \mathfrak{V}, \mathcal{Q}) \leq \max_{Q_{V,U,X}} \inf_{\substack{Q_S \in \\ \mathcal{Q} \cap \mathcal{P}_{\mathbb{Q}}(\mathcal{S})}} \Big[I(U;Y|V) - I(U;S,Z|V)\Big], \tag{12}$$

where the mutual information terms are calculated with respect to a joint PMF $Q_{V,U,X}Q_S Q_{Y|X,S}Q_{Z|X,S}$ with $Q_{Y|X,S}(y|x,s) = W_s(y|x)$ and $Q_{Z|X,S}(z|x,s) = V_s(z|x)$, for all $(s,x,y,z) \in \mathcal{S} \times \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$. Furthermore, one may restrict $|\mathcal{U}| \leq |\mathcal{X}|$ and $|\mathcal{V}| \leq |\mathcal{X}|^2 - 1$.

The max-inf structure of the RHS of (12) calls for a derivation that is uniform in $Q_S \in \mathcal{Q}$. The infimum is taken over $\mathcal{Q} \cap \mathcal{P}_{\mathbb{Q}}(\mathcal{S})$ (rather than over $\mathcal{Q}$) because the proof effectively considers only the rational distributions in $\mathcal{Q}$ while leveraging the monotonicity of the CR-assisted SS-capacity with respect to $\mathcal{Q}$ (see Remark 4). The proof shows that for each $Q_S \in \mathcal{Q} \cap \mathcal{P}_{\mathbb{Q}}(\mathcal{S})$, reliability and SS under a type constraint Q_S imply similar performance for the same channel but where the state sequence is i.i.d. according to Q_S. The main difficulty is in showing that even when transmitting over a DMC obtained by averaging the $W_s \in \mathfrak{W}$ with respect to Q_S, the normalized equivocation of the message given the output sequence at the *legitimate user* is still small. This is established via a novel argument based on distribution coupling.

Remark 7 (Time-Sharing Random Variable V) *The conditioning on V in the RHS of* (12) *effectively allows the legitimate user to choose a random mixture of $Q_{U,X}$ distributions. The advantage in doing so is that there might not exist a single state distribution that is bad for the whole mixture. This is reminiscent of a two-player zero-sum game, where the player who fixes the strategy first often benefits from a mixed strategy. When specializing to the type constrained scenario, however, the time-sharing random variable is removed. This is since when only one state distribution is allowed, the aforementioned distribution mixing outcomes with no gain.*

Remark 8 (Relation to Compound WTCs) *The best previously known single-letter upper bound on the secrecy-capacity of the compound WTC is due to Liang* et al. *[4, Theorem 2]. That upper bound has a min-max structure, and it is derived by claiming that the secrecy-capacity of the compound WTC is bounded above by this of the worst WTC in the set. This type of bounds are commonly related to knowledge of the channel's state at the transmitter (cf. e.g., [13]). Indeed, as shown in [5], the upper bound from [4] is tight for the compound WTC with encoder CSI.*

Specializing the max-inf upper bound from Theorem 3 to the compound WTC described in Remark 6 (i.e., over an appropriate constraint set), results in a strengthening of the claim from [4, Theorem 2]. The obtained bound first minimizes the difference of mutual information terms from the RHS of (12) *over the constraint set, and then maximizes the outcome over the input distribution. It is easily observed the difference between the two bounds can be strict. In fact, for the special case of a PTP compound channel (i.e., without an eavesdropper) our bound is the actual capacity, while the bound from [4] is loose. A simple example is a channel that consist of two orthogonal binary channels: one is noise free while the other one is purely noise (i.e., binary symmetric channel with crossover probability $\frac{1}{2}$). The state determines which channel is noisy, and the transmitter selects a binary input, which is unknown to the receiver, specifying which channel to use (both channels give an output each time, with one being pure noise). For this instance, the compound capacity is $\frac{1}{2}$ [bit/use], but the looser min-max bound gives 1 [bit/use].*

IV. An Example

Let $\mathcal{X} = \mathcal{Y} = \{0,1\}$ and $\mathcal{Z} = \{0,1,?\}$, where ? is an erased symbol. Further assume that the state space $\mathcal{S}$ decomposes as $\mathcal{S} = \mathcal{S}_1 \times \mathcal{S}_2$, where $\mathcal{S}_j = \{0,1\}$, for $j = 1,2$. Let $(\mathfrak{W}, \mathfrak{V})$ be an AVWTC, where the elements of $\mathfrak{W}$ and $\mathfrak{V}$ are indexed by $s_1 \in \mathcal{S}_1$ and $s_2 \in \mathcal{S}_2$, respectively. Define the main channel $W_{s_1} : \mathcal{X} \to \mathcal{P}(\mathcal{Y})$, for $s_1 \in \mathcal{S}_1$, as $W_{s_1}(y|x) = \mathbb{1}_{\{y = x \oplus s_1\}}$, where $\oplus$ denotes the modulo 2 addition. For the eavesdropper, let $V_0 : \mathcal{X} \to \mathcal{P}(\mathcal{Z})$ be a noiseless channel, while $V_1 : \mathcal{X} \to \mathcal{P}(\mathcal{Z})$ outputs the symbol ? with probability 1. Namely,

$$V_{s_2}(z|x) = \begin{cases} \mathbb{1}_{\{z=x\}}, & s_2 = 0 \\ \mathbb{1}_{\{z=?\}}, & s_2 = 1 \end{cases}. \tag{13}$$

Finally, we introduce a type constraint $Q_{S_1,S_2} = Q_{S_1}Q_{S_2}$ on the state sequences, where $Q_{S_1}(1) = \epsilon$ and $Q_{S_2}(1) = \alpha$, for some $\epsilon \in \left[0, \frac{1}{2}\right]$ and $\alpha \in [0,1]$. Denote the CR-assisted SS-capacity of this AVWTC by $C_{\mathrm{R}}(\epsilon,\alpha)$.

By Theorem 1, The CR-assisted SS-capacity is

$$C_{\mathrm{R}}(\epsilon,\alpha) = \max_{Q_{U,X}} \Big[I(U;Y) - I(U;Z|S_2) \Big], \tag{14}$$

where the mutual information terms are calculated with respect to the joint distribution $Q_{S_1}(s_1)Q_{S_2}(s_2)Q_{U,X}(u,x)W_{s_1}(y|x)V_{s_2}(z|x)$.

Note that for any $Q_{U,X} \in \mathcal{P}(\mathcal{U}\times\mathcal{X})$, we have

$$\begin{aligned} I(U;Z|S_2) &= Q_{S_2}(0)I(U;Z|S_2{=}0) + Q_{S_2}(1)I(U;Z|S_2{=}1) \\ &\overset{(a)}{=} (1-\alpha)I(U;X), \end{aligned} \tag{15}$$

where (a) is because $Z = ?$ whenever $S_2 = 1$ (thus nullifying the second mutual information term), while given on $S_2 = 0$, we have $Z = X$ and the conditioning is removed due to the independence of S_2 and (U,X). Consequently, (14) reduces to

$$C_{\mathrm{R}}(\epsilon,\alpha) = \max_{Q_{U,X}} \Big[I(U;Y) - (1-\alpha)I(U;X) \Big], \tag{16}$$

which is calculated with respect to $Q_{S_1}(s_1)Q_{U,X}(u,x)W_{s_1}(y|x)$. Now, since S_1 does not appear in any of the mutual information terms, their value remains unchanged if the above joint distribution is replaced with $Q_{U,X}(u,x)W_{Q_1}(y|x)$, where $W_{Q_1} : \mathcal{X} \to \mathcal{P}(\mathcal{Y})$ is the average DMC $W_{Q_1}(y|x) = \sum_{s_1\in\mathcal{S}_1} Q_{S_1}(s_1)W_{s_1}(y|x)$ (see Remark 5). Noting that the DMC W_{Q_1} is a binary symmetric channel with crossover probability ϵ (BSC(ϵ)), we have that $C_{\mathrm{R}}(\epsilon,\alpha)$ is the secrecy-capacity of BS-BE WTC with a BSC(ϵ) between the legitimate users and a binary erasure channel with erasure probability α (BEC(α)) to the eavesdropper [8].

Remark 9 *Interestingly,* (16) *is also the SS-capacity of the WTC of type II (WTCII) with a BSC(ϵ) to the legitimate user and an eavesdropper who can actively choose any $\lfloor n(1-\alpha)\rfloor$ of the transmitted symbols to observe. [14]. This is not surprising since the WTCII with a noisy main channel is a particular instance of a type constrained AVWTC.*

Fig. 2 depicts the CR-assisted SS-capacity of the considered AVWTC as a function of type constraints on the main and on the eavesdropper's channels. The variation of $C_{\mathrm{R}}(\epsilon,\alpha)$ as a function of $Q_{S_1}(1) = \epsilon$ for a fixed $\alpha = 0.4$ is shown in Fig. 2(a), while Fig. 2(b) presents the SS-capacity as a function of $Q_{S_2}(1) = \alpha$ when $\epsilon = 0.1$ is fixed. The curves are plotted by parametrizing the joint PMF of the binary random variables U and X and spanning over the possible probability values.

As mentioned before, $C_{\mathrm{R}}(\epsilon,\alpha)$ is also the secrecy-capacity of a BS-BE WTC, which was studied in [8]. In that work it was shown that the secrecy-capacity is zero if $\alpha < 4\epsilon(1-\epsilon)$. When $\epsilon = 0.1$ the threshold value of α is 0.36. Indeed, Fig. 2(b) reveals that $C_{\mathrm{R}}(0.1,\alpha) = 0$ for any $\alpha < 0.36$. Beyond 0.36, the SS-capacity monotonically increases with α, since the larger the probability of an erasure, the worse the channel to the eavesdropper is. From the opposite perspective, a fixed $\alpha = 0.4$ induces two real solutions to the equation $0.4 = 4\epsilon(1-\epsilon)$, which are $\epsilon_1 \approx 0.1127$ and $\epsilon_2 \approx 0.8872$. The condition $0.4 < 4\epsilon(1-\epsilon)$ is then satisfied for any $\epsilon \in (\epsilon_1, \epsilon_2)$, which gives a zero SS-capacity in that region in Fig. 2(b). Also observe that as a function of ϵ, $C_{\mathrm{R}}(\epsilon, 0.4)$ grows as the crossover probability approaches the extreme values of 0 or 1.

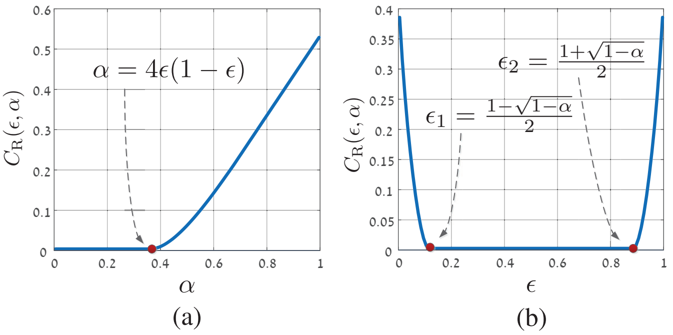

Fig. 2: CR-assisted SS-capacity $C_{\mathrm{R}}(\epsilon,\alpha)$ versus: (a) the proscribed type for the main channel $Q_{S_1}(1) = \epsilon$, which corresponds to the portion of flipped symbols in the BS-BE WTC; (b) CR-assisted SS-capacity $C_{\mathrm{R}}(\epsilon,\alpha)$ versus: (a) the proscribed type for the eavesdropper's channel $Q_{S_2}(1) = \alpha$, which corresponds to the portion of erasures in the BS-BE WTC.

References

[1] A. D. Wyner. The wire-tap channel. *Bell Sys. Techn.*, 54(8):1355–1387, Oct. 1975.

[2] R. Ahlswede. Elimination of correlation in random codes for arbitrarily varying channels. *Z. Wahrscheinlichkeitstheorie verw. Gebiete*, 44(2):159–175, 1978.

[3] I. Csiszár and P. Narayan. Arbitrarily varying channels with constrained inputs and states. *IEEE Trans. Inf. Theory*, 34(1):27–34, Jan. 1988.

[4] Y. Liang, G. Kramer, V. H. Poor, and S. Shamai. Compound wiretap channels. *EURASIP Journal on Wireless Commun. and Netw., Special Issue on Wireless Physical Layer Security*, 2009, 2009.

[5] I. Bjelaković, H. Boche, and J. Sommerfeld. Secrecy results for compound wiretap channels. *Prob. Pered. Inf. (Problems of Inf. Transm.)*, 49(1):73–98, Jan. 2013.

[6] E. MolavianJazi. Secure communication over arbitrarily varying wiretap channels. Master's thesis, Graduate School of the University of Notre Dame, Notre Dame, Indiana ,USA, Dec. 2009.

[7] I. Bjelaković, H. Boche, and J. Sommerfeld. Capacity results for arbitrarily varying wiretap channels. In *Information Theory, Combinatorics, and Search Theory*, pages 123–144. Springer, 2013.

[8] O. Ozel and S. Ulukus. Wiretap channels: Roles of rate splitting and channel prefixing. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT-2011)*, Saint Petersburg, Russia, Jul.-Aug. 2011.

[9] M. Bellare, S. Tessaro, and A. Vardy. A cryptographic treatment of the wiretap channel. In *Proc. Adv. Crypto. (CRYPTO 2012)*, Santa Barbara, CA, USA, Aug. 2012.

[10] M. Wiese, J. Nötzel, and H. Boche. A channel under simultaneous jamming and eavesdropping attack - correlated random coding capacities under strong secrecy criteria. *Submitted for publication to IEEE Trans. Inf. Theory*, 2015. Available on ArXiv at http://arxiv.org/abs/1410.8078v2.

[11] Z. Goldfeld, P. Cuff, and H. H. Permuter. Arbitrarily varying wiretap channels with type constrained states. *Submitted for publication to IEEE Trans. Inf. Theory*, 2016. Available on ArXiv at http://arxiv.org/abs/1601.03660.

[12] I. Csiszár and P. Narayan. Arbitrarily varying channels with constrained inputs and states. *IEEE Trans. Inf. Theory*, 34(1):27–34, Jan. 1988.

[13] B. Shrader and H. H. Permuter. Feedback capacity of the compound channel. *IEEE Trans. Inf. Theory*, 55(8):3629–3644, Aug. 2009.

[14] Z. Goldfeld, P. Cuff, and H. H. Permuter. Semantic-security capacity for wiretap channels of type II. *IEEE Trans. Inf. Theory*, 62(7):1–17, Jul. 2016.