Covert Communication via Non-Causal Cribbing from a Cooperative Jammer

Hassan ZivariFard[†], Matthieu R. Bloch[††] and Aria Nosratinia[†]
[†] The University of Texas at Dallas, Richardson, TX, USA, Email: {hassan, aria}@utdallas.edu
[††] Georgia Institute of Technology, Atlanta, GA, USA, Email: matthieu.bloch@ece.gatech.edu

2021 IEEE International Symposium on Information Theory (ISIT) | 978-1-5386-8209-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISIT45174.2021.9517883

***Abstract*—We consider the problem of covert communication in the presence of a cooperative jammer. Covert communication refers to communication that is undetectable by an adversary, i.e., a scenario in which, despite ongoing communication, the output distribution observed by an adversary called the "warden" is indistinguishable from the distribution that would have been induced by an innocent channel-input symbol. It is known that in general, a transmitter and a receiver can communicate only $O(\sqrt{n})$ covert bits over n channel uses, i.e., zero rate. This paper shows that a cooperative jammer can facilitate the communication of positive covert rates, subject to the transmitter having non-causal access to the jammer signal. An achievable rate region is calculated that highlights the relation between the covert communication rate, jammer's randomness (expressed as a rate), and rate of a secret key shared between transmitter and receiver.**

I. Introduction

Covert communication refers to scenarios in which a transmitter wishes to communicate reliably over a channel with a receiver while simultaneously ensuring that the distribution induced at a separate channel output (called "warden") is identical to that induced by an innocent channel symbol [1]–[5]. In a point-to-point Discrete Memoryless Channel (DMC) it is known that, if the distribution induced on the warden's observation by the innocent channel-input symbol is a convex combination of the distributions generated by the other input symbols, then it is possible to achieve a positive covert communication rate; otherwise the number of covert bits that can be reliably communicated over n channel transmissions scales at most as $O(\sqrt{n})$ [3]. These results has motivated the study of other models in which positive covert rates are achievable e.g., when the Channel State Information (CSI) is available at the transmitter and the receiver (or only at the transmitter) but not at the warden [6]–[8]. Also, it is possible to achieve positive covert rate when the warden has uncertainty about the power of noise or interference at its receiver [9]–[14].

Of particular relevance to the present work, the problem of secret communication over DMCs with random states has been studied in [15]–[17]. Furthermore, arbitrarily varying wiretap channels under strong and semantic secrecy criterion have been studied in [18]–[20] and Covert communication over adversarially jammed channels has been studied in [21]. Multiple-Access Channel (MAC) with cribbing encoders was first studied by Willems and van der Meulen [22], [23] and channel resolvability and strong secrecy for a discrete memoryless multiple-access channel with cribbing has been studied in [24].

In this paper we study the problem of covert communication over a DMC when a cooperative jammer [25] is present (see Fig. 1). Here we assume that the jammer's output is available non-causally at the transmitter and there is a shared secret key between the legitimate terminals. Since the jammer can simulate a random state (given sufficient resources), we expect to achieve a positive covert communication rate in the considered model. One of the main contributions of this work is to show that cribbing the jamming signal enables a positive covert communication rate via a Shannon strategy and Gel'fand-Pinsker coding. An achievable rate region is calculated that highlights the relation between the covert communication rate, jammer's randomness (expressed as a rate), and rate of the secret key shared between transmitter and receiver.

II. Preliminaries and Problem Statement

Throughout this paper, random variables are denoted by capital letters and their realizations are denoted by lower case letters. Calligraphic letters represent sets and the cardinality of a set is denoted by $|\cdot|$. P_X and P_{XY} represent probability distributions on discrete alphabets $\mathcal{X}$ and $\mathcal{X}\times\mathcal{Y}$, respectively. For brevity, we sometimes omit the subscripts in probability distributions if they are clear from the context, i.e., instead of $P_X(x)$ we write $P(x)$. The integer set $\{1,\dots,M\}$ is denoted by $[\![1,M]\!]$ and $\mathbb{1}_{\{\cdot\}}$ denotes the indicator function. The n-fold product distribution constructed from the same distribution P is denoted $P^{\otimes n}$. For two distributions P and Q on the same alphabet, the KL-divergence is defined as $\mathbb{D}(P||Q) \triangleq \sum_x P(x)\log\frac{P(x)}{Q(x)}$ and the total variation distance is defined by $||P-Q||_1 \triangleq \frac{1}{2}\sum_x |P(x)-Q(x)|$. Throughout the paper, $\log$ denotes the base 2 logarithm. $\mathbb{E}_X(\cdot)$ is the expectation with respect to the random variable X and for a set of random variables $\{X_i\}_{i\in\mathcal{A}}$ indexed over a countable set $\mathcal{A}$.

Consider a DMC as shown in Fig. 1. $\mathcal{X}$ and $\mathcal{S}$ are the channel input alphabets while $\mathcal{Y}$ and $\mathcal{Z}$ are the channel output alphabets at the legitimate receiver and the warden,

The work of H. ZivariFard and A. Nosratinia is supported by National Science Foundation (NSF) grant 1956213. The work of M. R. Bloch is supported by National Science Foundation (NSF) grant 1955401.

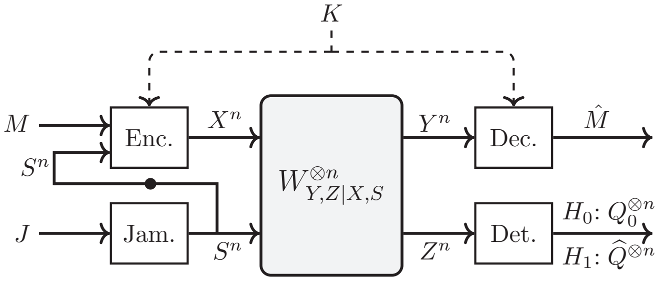

Fig. 1. Covert communication in presence of a jammer

respectively. Let $x_0 \in \mathcal{X}$ be an innocent symbol corresponding to the absence of communication with the receiver. Let

$$Q_0(\cdot) = \sum_{s\in\mathcal{S}} P_S(s) W_{Z|X,S}(\cdot|x_0, s), \tag{1a}$$

$$Q_Z(\cdot) = \sum_{s\in\mathcal{S}} \sum_{x\in\mathcal{X}} P_S(s) P_{X|S}(x|s) W_{Z|X,S}(\cdot|x, s), \tag{1b}$$

$Q_0^{\otimes n} \triangleq \prod_{i=1}^n Q_0$ and $Q_Z^{\otimes n} \triangleq \prod_{i=1}^n Q_Z$. We define non-negative costs $b_1(x)$ and $b_2(s)$ for channel inputs $x \in \mathcal{X}$ and $s \in \mathcal{S}$, respectively. The average cost of input sequences $x^n \in \mathcal{X}^n$ and $s^n \in \mathcal{S}^n$ are $b_1(x^n) = \frac{1}{n}\sum_{i=1}^n b_1(x_i)$ and $b_2(s^n) = \frac{1}{n}\sum_{i=1}^n b_2(s_i)$, respectively. The jammer's output is available non-causally at the transmitter. An $(|\mathcal{M}|, n)$ code consists of an encoder that maps (M, S^n) to $X^n \in \mathcal{X}^n$ and a decoder at the receiver that maps Y^n to $\widehat{M} \in \mathcal{M}$. The code is assumed known to all parties and the objective is to design a code that is both reliable and covert. The code is defined to be reliable if the average probability of error $P_e^{(n)} = \mathbb{P}(\widehat{M} \neq M)$ goes to zero when $n \to \infty$. The code is covert if the warden cannot determine whether communication is happening (hypothesis H_1) or not (hypothesis H_0). The probabilities of false alarm (warden deciding H_1 when H_0 is true) and missed detection (warden deciding H_0 when H_1 is true), are denoted by α_n and β_n, respectively. An uninformed, random decision by the warden satisfies $\alpha_n + \beta_n = 1$, which is the benchmark for covertness. When the channel carries communication, the warden's channel output distribution is denoted P_{Z^n}, and the optimal hypothesis test by the warden satisfies $\alpha_n + \beta_n \geq 1 - \sqrt{\mathbb{D}(P_{Z^n}||Q_0^{\otimes n})}$ [26]. Therefore, to show that the communication is covert, it suffices to show that $\mathbb{D}(P_{Z^n}||Q_0^{\otimes n}) \to 0$. Note that supp$(Q_0) = \mathcal{Z}$ otherwise $\mathbb{D}(P_{Z^n}||Q_0^{\otimes n}) \to \infty$. Consequently, our goal is to design a sequence of $(2^{nR}, n)$ codes such that

$$\lim_{n\to\infty} P_e^{(n)} \to 0, \tag{2a}$$

$$\lim_{n\to\infty} \mathbb{D}(P_{Z^n}||Q_0^{\otimes n}) \to 0, \tag{2b}$$

$$\limsup_{n\to\infty} \mathbb{E}[b_1(X^n)] \leq B_1, \tag{2c}$$

$$\limsup_{n\to\infty} \mathbb{E}[b_2(S^n)] \leq B_2. \tag{2d}$$

where B_1 and B_2 are the average constraints on cost per codeword. Here the goal is to design a code for the transmitter and the jammer in such a way that the transmitter can communicate covertly with receiver. We define the covert capacity as the supremum of all achievable covert rates and denote it by $C_{\text{CJ-NC}}$.

III. One-Sided MAC Resolvability Lemma

The achievable rate region is based on Lemma 1 below. This lemma describes the rate required for a codebook exciting *one of* the inputs of a MAC so that the output distribution is indistinguishable from that arising from a random excitation of the same input, *while the other MAC input is being excited at the same time by a codebook with an arbitrary, prescribed rate.* A key distinction of this result from the usual resolvability results is that the target distribution may not be independent and identically distributed (i.i.d.).

We begin by characterizing the setup for this lemma. Consider a discrete memoryless MAC $(\mathcal{X}_1\times\mathcal{X}_2, W_{Z|X_1,X_2}, \mathcal{Z})$ over which two encoders transmit codewords as in Fig. 2. Let $C_i \triangleq \left\{X_i^n(m_i)\right\}_{m_i\in\mathcal{M}_i}$, where $\mathcal{M}_i = [\![1, 2^{nR_i}]\!]$, be a random codebook consisting of independent random sequences each generated according to $P_{X_i}^{\otimes n}$, for $i = 1, 2$. We denote a realization of C_i by $c_i \triangleq \left\{x_i^n(m_i)\right\}_{m_i\in\mathcal{M}_i}$. The codebook construction described above induces the Probability Mass Function (PMF) λ for the codebooks.

$$\lambda(c_1, c_2) = \prod_{m_1\in\mathcal{M}_1} \prod_{m_2\in\mathcal{M}_2} P_{X_1}^{\otimes n}\big(x_1^n(m_1)\big) P_{X_2}^{\otimes n}\big(x_2^n(m_2)\big).$$

We now consider two scenarios, under *both* of which Transmitter 2 emits a codeword chosen randomly and uniformly from the random codebook C_2. In the first scenario, Transmitter 1 emits an i.i.d. sequence according to P_{X_1}. The distribution induced at the output of the channel is

$$P_{Z^n|C_2}(z^n) \triangleq \frac{1}{2^{nR_2}} \sum_{m_2=1}^{2^{nR_2}} W_{Z|X_2}^{\otimes n}\big(z^n|X_2^n(m_2)\big), \tag{3}$$

where

$$W_{Z|X_2}(z|x_2) \triangleq \sum_{x_1\in\mathcal{X}_1} P(x_1) W_{Z|X_1,X_2}(z|x_1, x_2). \tag{4}$$

In the second scenario, Transmitter 1 emits a codeword uniformly at random from a random codebook C_1. The distribution induced at the channel output is

$$P_{Z^n|C_1,C_2}(z^n) \triangleq \sum_{m_1=1}^{2^{nR_1}} \sum_{m_2=1}^{2^{nR_2}} \frac{1}{2^{n(R_1+R_2)}} \times W_{Z|X_1,X_2}^{\otimes n}\big(z^n|X_1^n(m_1), X_2^n(m_2)\big). \tag{5}$$

We wish to find conditions under which the distributions induced at the channel output in the two scenarios are approximately equal. We call this problem *one-sided MAC resolvability.*

Definition 1. *A rate pair (R_1, R_2) is achievable for the one-sided resolvability of the discrete memoryless MAC $(\mathcal{X}_1 \times \mathcal{X}_2, W_{Z|X_1,X_2}, \mathcal{Z})$ if for a given $W_{Z|X_1,X_2}$ there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes such that $\mathbb{E}_{C_1,C_2}\Big[\mathbb{D}\big(P_{Z^n|C_1,C_2}||P_{Z^n|C_2}\big)\Big] \xrightarrow[n\to\infty]{} 0$. The one-sided MAC*

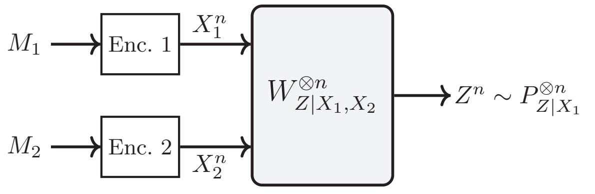

Fig. 2. Distribution Approximation in MAC

resolvability region $\mathcal{R}$ is the convex hull of the set of all achievable rate pairs (R_1, R_2).

The main difference between the resolvability region in Definition 1 and the standard resolvability defined in [27]–[29] is that here the target distribution $P_{Z^n|C_2}$ at the output of channel is not necessarily i.i.d.. We now find sufficient conditions on the size of the two codebooks such that the distributions induced at the channel output in the two scenarios in Eq. (5) and (3) are approximately equal in terms of expected KL divergence.

Lemma 1. *For a discrete memoryless MAC, $W_{Z|X_1,X_2}$ if (R_1, R_2) belongs to*

$$\bigcup_{P(x_1)P(x_2)} (\mathcal{R}_1 \cup \mathcal{R}_2) \tag{6}$$

where

$$\mathcal{R}_1 = \left\{ \begin{array}{l} (R_1, R_2) \in \mathbb{R}_+^{*2} : \\ R_1 > \mathbb{I}(X_1; Z) \\ R_2 > \mathbb{I}(X_2; Z) \\ R_1 + R_2 > \mathbb{I}(X_1, X_2; Z) \end{array} \right\}, \tag{7a}$$

$$\mathcal{R}_2 = \left\{ \ (R_1, R_2) \in \mathbb{R}_+^{*2} : \ R_1 > \mathbb{I}(X_1; Z|X_2) \ \right\}, \tag{7b}$$

then

$$\mathbb{E}_{C_1,C_2}\Big[\mathbb{D}\big(P_{Z^n|C_1,C_2} || P_{Z^n|C_2}\big)\Big] \xrightarrow[n\to\infty]{} 0. \tag{8}$$

We prove Lemma 1 by considering two different cases; first, when the size of the second transmitter's codebook operates above the capacity of its channel; second, when the size of the second transmitter's codebook operates below the capacity of its channel. The former case results in the region $\mathcal{R}_1$ and the latter results in the region $\mathcal{R}_2$. The proof does not fit in this submission and has been made available online [30].

Remark 1. *The region $\mathcal{R}_1$ is the channel resolvability region for MAC. Since X_1 and X_2 are independent therefore $\mathbb{I}(X_1; Z|X_2) = \mathbb{I}(X_1; X_2, Z)$, and the region $\mathcal{R}_2$ can be viewed as the resolvability region of a MAC against a wiretapper who has full access to the channel input X_2 while the first transmitter does not have access to X_2.*

Remark 2. *A related result [31, Theorem 3] states that if* (6) *holds then $\mathbb{E}_{C_1,C_2}\big|\big|P_{Z^n|C_1,C_2} - P_{Z^n|C_2}\big|\big|_1 \xrightarrow[n\to\infty]{} 0$. However, no proof is publicly available for [31, Theorem 3].*

IV. Main Result

Theorem 1. *The covert capacity of the DMC $W_{Y,Z|S,X}$ when the transmitter has non-causal access to the jammer's input is lower-bounded by*

$$C_{\text{CJ-NC}} \geq \max \big[\mathbb{I}(U; Y) - \mathbb{I}(U; V|S)\big], \tag{9}$$

where the maximum is over distributions of the form $P_S P_U P_{V|U,S}$ and $x(u, s)$, such that $\mathbb{E}[b_1(X)] \leq B_1$, $\mathbb{E}[b_2(S)] \leq B_2$, $Q_Z = Q_0$, $R_J > \mathbb{I}(S; Z)$, and

$$R_K > \max\big\{\mathbb{I}(U; Z), \mathbb{I}(U, S; Z) - R_J\big\} - \mathbb{I}(U; Y). \tag{10}$$

Remark 3. *The achievable rate region in Theorem 1 is still valid for the scenario in which the transmitter has access to the jammer's input, i.e., the dummy messages J.*

Two extremal cases for the jammer rate are instructive and are considered next. First, if the jammer has maximal rate $R_J = H(S)$, the key rate requirements are the same as in the problem of covert communication over a state-dependent channel [6], [8]. Since U and S are independent, one can show that (10) reduces to:

$$R_K > I(U; Z) - \mathbb{I}(U; Y). \tag{11}$$

This is the condition that has been derived in [6, Eq. (8)]. Second, if we set R_J as its minimum, i.e., $R_J = \mathbb{I}(S; Z) + \epsilon$, and since U and S are independent, one can show that (10) will reduce to

$$R_K > \mathbb{I}(U; Z|S) - \mathbb{I}(U; Y). \tag{12}$$

Since $\mathbb{I}(U; Z|S) \geq \mathbb{I}(U; Z)$, if the size of jammer's codebook is decreased, a higher rate is needed for the secret key shared between the legitimate terminals. From (10), the smallest jammer codebook allowing minimal secret key rate is $R_J = \mathbb{I}(S; Z|U)$.

Proof of Theorem 1. Fix $P_S(s)$, $P_U(u)$, $P_{V|U,S}(v|u, s)$, $x(u, s)$, and $\epsilon_1 > \epsilon_2 > 0$ subject to the conditions $Q_Z = Q_0$, $\mathbb{E}[b_1(X)] \leq \frac{B_1}{1+\epsilon_1}$, and $\mathbb{E}[b_2(S)] \leq \frac{B_2}{1+\epsilon_2}$.

Codebook Generation: Let $C_1^{(n)} \triangleq \big\{U^n(k, m, \ell)\big\}_{(k,m,\ell)\in\mathcal{K}\times\mathcal{M}\times\mathcal{L}}$, where $\mathcal{K} = [\![1, 2^{nR_K}]\!]$, $\mathcal{M} = [\![1, 2^{nR}]\!]$, and $\mathcal{L} = [\![1, 2^{nR'}]\!]$, be a random codebook consisting of independent random sequences each generated according to $P_U^{\otimes n}$. We denote a realization of $C_1^{(n)}$ by $c_1^{(n)} \triangleq \big\{u^n(k, m, \ell)\big\}_{(k,m,\ell)\in\mathcal{K}\times\mathcal{M}\times\mathcal{L}}$. The indices (k, m, ℓ) can be viewed as a two-layer binning.

Let $C_2^{(n)} \triangleq \big\{S^n(j)\big\}_{j\in\mathcal{J}}$, where $\mathcal{J} = [\![1, 2^{nR_J}]\!]$, be a random codebook consisting of independent random sequences each generated according to $P_S^{\otimes n}$. We denote a realization of $C_2^{(n)}$ by $c_2^{(n)} \triangleq \big\{s^n(j)\big\}_{j\in\mathcal{J}}$.

Let, $C_n = \big\{C_1^{(n)}, C_2^{(n)}\big\}$ and $c_n = \big\{c_1^{(n)}, c_2^{(n)}\big\}$. The codebook construction described above induces the PMF $\lambda(c_n)$ for the codebooks.

$$\lambda(c_n) = \prod_{j\in\mathcal{J}} P_S^{\otimes n}\big(s^n(j)\big) \prod_{(k,m,\ell)\in\mathcal{K}\times\mathcal{M}\times\mathcal{L}} P_U^{\otimes n}\Big(u^n\big(k, m, \ell\big)\Big). \tag{13}$$

To facilitate the analysis, we define a so-called ideal joint PMF for all input, output, message, key, and auxiliary variables, conditioned on the choice of codebooks c_n,

$$\begin{aligned}&\Gamma^{(c_n)}_{K,M,J,L,S^n,U^n,V^n,Z^n}(k,m,j,\ell,\tilde{s}^n,\tilde{u}^n,v^n,z^n)\\&=2^{-n(R_K+R+R_J+R')}\mathbb{1}_{\left\{\tilde{s}^n=s^n(j)\right\}\cap\left\{\tilde{u}^n=u^n(k,m,\ell)\right\}}\\&\times P^{\otimes n}_{V|S,U}(v^n|\tilde{s}^n,\tilde{u}^n)W^{\otimes n}_{Z|U,S}(z^n|\tilde{u}^n,\tilde{s}^n),\end{aligned}\tag{14}$$

where $P_{V|S,U}$ is a test channel and $W_{Z|U,S}$ is the marginal distribution of $W_{Z,Y|U,S}$ defined in Theorem 1.

Encoding: The jammer selects an index j uniformly at random and transmits $s^n(j)$. The encoder cribs this s^n and, conditioned on it, generates a sequence v^n i.i.d. according to $P^{\otimes n}_{V|S}$. To do so, the encoder employs local randomness in a manner reminiscent of Csiszár and Körner's stochastic encoder [32]. Then, given v^n as well as the cribbed signal $s^n(j)$, the key k, and the message m, the encoder chooses the index ℓ via a likelihood encoder [29], [33], [34], according to the following distribution:

$$\begin{aligned}&f^{(c_n)}_{\text{LE}}(\ell|k,m,j,v^n)\\&=\frac{P^{\otimes n}_{V|U,S}\big(v^n|u^n(k,m,\ell),s^n(j)\big)}{\sum\limits_{\ell'\in[\![1,2^{nR'}]\!]}P^{\otimes n}_{V|U,S}\big(v^n|u^n(k,m,\ell'),s^n(j)\big)}.\end{aligned}\tag{15}$$

Using the resulting index ℓ as well as the key k and message m, the encoder computes $u^n(k,m,\ell)$ and transmits codeword x^n, where $x_i=x(u_i(k,m,\ell),s_i)$.

For a fixed codebook c_n, the induced joint distribution is

$$\begin{aligned}&P^{(c_n)}_{K,M,J,S^n,V^n,L,U^n,Z^n}(k,m,j,\tilde{s}^n,v^n,\ell,\tilde{u}^n,z^n)\\&=2^{-n(R_K+R+R_J)}\mathbb{1}_{\left\{\tilde{s}^n=s^n(j)\right\}}P^{\otimes n}_{V|S}(v^n|\tilde{s}^n)\\&\quad\times f^{(c_n)}_{\text{LE}}(\ell|k,m,j,v^n)\mathbb{1}_{\left\{\tilde{u}^n=u^n(k,m,\ell)\right\}}\\&\quad\times W^{\otimes n}_{Z|U,S}(z^n|\tilde{u}^n,\tilde{s}^n).\end{aligned}\tag{16}$$

Considering the random codebook generation, we have

$$\begin{aligned}&P(c_n,k,m,j,\tilde{s}^n,\ell,\tilde{u}^n,z^n)\\&=\lambda(c_n)\times P^{(c_n)}(k,m,j,\tilde{s}^n,\ell,\tilde{u}^n,z^n),\end{aligned}\tag{17}$$

where $\lambda\in\mathcal{P}$ is defined in (13).

Covert Analysis: We denote by $P^{(c_n)}$ the distributions induced by a fixed codebook c_n, and by $P_{\cdot|C_n}$ the distributions induced by a random codebook C_n. Consider a scenario in which the jammer selects a codeword from its codebook uniformly at random and the transmitter chooses the innocent sequence x^n_0. Under a fixed codebook $c_2^{(n)}$, the induced joint distribution is as follows

$$\Upsilon^{(c_2^{(n)})}_{J,S^n,Z^n}(j,s^n,z^n)=\frac{1}{2^{nR_J}}\mathbb{1}_{\{s^n=s^n(j)\}}W^{\otimes n}_{Z|X,S}\big(z^n|x^n_0,s^n\big).$$

Therefore, the distribution induced on the warden's observation is

$$\Upsilon^{(c_2^{(n)})}_{Z^n}(z^n)=\frac{1}{2^{nR_J}}\sum_{j=1}^{2^{nR_J}}W^{\otimes n}_{Z|X,S}\big(z^n|x^n_0,s^n(j)\big).\tag{18}$$

If $R_J>\mathbb{I}(S;Z)$ then according to the soft covering lemma [28, Theorem 4] or [29, Corollary VII.4],

$$\big|\big|\Upsilon^{(c_2^{(n)})}_{Z^n}-Q^{\otimes n}_0\big|\big|_1\xrightarrow[n\to\infty]{}0.\tag{19}$$

where $Q^{\otimes n}_0$ has been defined in (1a). Note that if $R_J<\mathbb{I}(S;Z)$ according to Shannon's channel coding theorem, the warden might be able to decode J, which reduces the problem to the point to point channel for which the covert rate will be zero.

We aim to show that the coding scheme described above guarantees

$$\mathbb{E}_{C_n}||P_{Z^n|C_n}-Q^{\otimes n}_Z||_1\xrightarrow[n\to\infty]{}0,\tag{20}$$

and therefore according to [35, eq. (323)] (also see, [36, Remark 1])

$$\mathbb{E}_{C_n}[\mathbb{D}(P_{Z^n|C_n}||Q^{\otimes n}_Z)]\xrightarrow[n\to\infty]{}0,\tag{21}$$

where $Q^{\otimes n}_Z$ has been defined in (1b).

By the triangle inequality,

$$\begin{aligned}\mathbb{E}_{C_n}||P_{Z^n|C_n}-Q^{\otimes n}_Z||_1\leq&\mathbb{E}_{C_n}||P_{Z^n|C_n}-\Gamma_{Z^n|C_n}||_1\\&+\mathbb{E}_{C_n}||\Gamma_{Z^n|C_n}-Q^{\otimes n}_Z||_1.\end{aligned}\tag{22}$$

We proceed to bound the first term on the Right Hand Side (RHS) of (22). For every codebook c_n,

$$\Gamma^{(c_n)}_{K,M,J}=2^{-n(R_K+R+R_J)}=P^{(c_n)}_{K,M,J},\tag{23a}$$

$$\Gamma^{(c_n)}_{S^n|K,M,J}=\mathbb{1}_{\left\{\tilde{s}^n=s^n(j)\right\}}=P^{(c_n)}_{S^n|K,M,J},\tag{23b}$$

$$\begin{aligned}\Gamma^{(c_n)}_{L|K,M,J,S^n,V^n}&=f^{(c_n)}_{\text{LE}}(\ell|k,m,j,v^n)\\&=P^{(c_n)}_{L|K,M,J,S^n,V^n},\end{aligned}\tag{23c}$$

$$\begin{aligned}\Gamma^{(c_n)}_{U^n|K,M,J,S^n,V^n,L}&=\mathbb{1}_{\left\{\tilde{u}^n=u^n(k,m,\ell)\right\}}\\&=P^{(c_n)}_{U^n|K,M,J,S^n,V^n,L},\end{aligned}\tag{23d}$$

$$\begin{aligned}\Gamma^{(c_n)}_{Z^n|K,M,J,S^n,V^n,L,U^n}&=W^{\otimes n}_{Z|U,S}(z^n|\tilde{u}^n,\tilde{s}^n)\\&=P^{(c_n)}_{Z^n|K,M,J,S^n,V^n,L,U^n},\end{aligned}\tag{23e}$$

where (23a)-(23b) and (23d)-(23e) follow directly from (14) and (16) and (23c) follow since for every codebook c_n,

$$\begin{aligned}&\Gamma^{(c_n)}_{L|K,M,J,V^n}(\ell|k,m,j,v^n)\\&=\frac{\Gamma^{(c_n)}_{K,M,L,J,V^n}(k,m,\ell,j,v^n)}{\Gamma^{(c_n)}_{K,M,J,V^n}(k,m,j,v^n)}\\&=f^{(c_n)}_{\text{LE}}(\ell|k,m,j,v^n).\end{aligned}\tag{24}$$

Thus, the first on the RHS of (22) is bounded as

$$\begin{aligned}&\mathbb{E}_{C_n}\big|\big|P_{Z^n|C_n}-\Gamma_{Z^n|C_n}\big|\big|_1\\&\leq\mathbb{E}_{C_n}\big|\big|P_{K,M,J,S^n,V^n,L,U^n,Z^n|C_n}\\&\qquad-\Gamma_{K,M,J,S^n,V^n,L,U^n,Z^n|C_n}\big|\big|_1\\&\overset{(a)}{=}\mathbb{E}_{C_n}\big|\big|P_{S^n,V^n,L,U^n,Z^n|K=1,M=1,J=1,C_n}\\&\qquad-\Gamma_{S^n,V^n,L,U^n,Z^n|K=1,M=1,J=1,C_n}\big|\big|_1\end{aligned}$$

$$\overset{(b)}{=} \mathbb{E}_{C_n}\big|\big|P_{V|S}^{\otimes n}\big(\,\cdot\,|S^n(1)\big) - \Gamma_{V^n|K=1,M=1,J=1,C_n}\big|\big|_1, \quad (25)$$

where (a) follows from (23a), the independence of (K, M, J) and C_n, and symmetry of codebook construction with respect to (K, M, J); and (b) follows from (23b)-(23e). According to Lemma 1 the RHS of (25) vanishes when n grows if

$$R' > \mathbb{I}(U; V|S). \quad (26)$$

This follows since conditioning on $M_2 = 1$ the distribution in (3) reduces to $P_{Z^n|M_2=1}(z^n) = W_{Z|X_2}^{\otimes n}(z^n|X_2^n(1))$ and the distribution in (5) reduces to

$$P_{Z^n|C_1,M_2=1}(z^n) \triangleq \sum_{m_1=1}^{2^{nR_1}} \frac{1}{2^{nR_1}} \times W_{Z|X_1,X_2}^{\otimes n}\big(z^n|X_1^n(m_1), X_2^n(1)\big).$$

Also, according to [31], [37] the second term on the RHS of (22) vanishes when n grows if

$$R_J > \mathbb{I}(S; Z), \quad (27a)$$

$$R_K + R + R' > \mathbb{I}(U; Z), \quad (27b)$$

$$R_K + R + R' + R_J > \mathbb{I}(U, S; Z). \quad (27c)$$

Now, by using the triangle inequality we have

$$\mathbb{E}_{C_n}\big|\big|P_{Z^n|C_n} - \Upsilon_{Z^n|C_2^{(n)}}\big|\big|_1 \leq \mathbb{E}_{C_n}\big|\big|P_{Z^n|C_n} - Q_0^{\otimes n}\big|\big|_1 + \mathbb{E}_{C_n}\big|\big|\Upsilon_{Z^n|C_2^{(n)}} - Q_0^{\otimes n}\big|\big|_1. \quad (28)$$

Using Pinsker inequality the first term on the RHS of (28) vanishes when n grows if we choose P_S, P_U, $P_{V|U,S}$ and $x(u, s)$ such that $Q_Z = Q_0$, (26), and (27) hold. Also, from (19) the second term on the RHS of (28) vanishes when n grows.

Decoding and Error Probability Analysis: We show that the average probability of error can be made arbitrarily small. By access to the key K the receiver declares that $\hat{M} = M$ if there exists a unique index $\hat{M}$ such that $(U^n(K, \hat{M}, \ell), Y^n) \in \mathcal{T}_\epsilon^{(n)}(U, Y)$. Then the error event $(\hat{M} \neq M)$ occurs only if one or more of the following error events occur:

$$\mathcal{E}_1 \triangleq \{(U^n(K, M, L), V^n) \notin \mathcal{T}_{\epsilon'}^{(n)}(U, V)\}, \quad (29a)$$

$$\mathcal{E}_2 \triangleq \{(U^n(K, M, L), Y^n) \notin \mathcal{T}_{\epsilon}^{(n)}(U, Y)\}, \quad (29b)$$

$$\mathcal{E}_3 \triangleq \{(U^n(K, m, \ell), Y^n) \in \mathcal{T}_{\epsilon}^{(n)}(U, Y) \text{ for some } m \neq M \text{ and } \ell \in [1 : 2^{rR'}]\}. \quad (29c)$$

Therefore, from the union bound we can bound the probability of error as follows

$$\mathbb{P}(\hat{M} \neq M) \leq \mathbb{P}(\mathcal{E}_1) + \mathbb{P}(\mathcal{E}_1^c \cap \mathcal{E}_2) + \mathbb{P}(\mathcal{E}_3). \quad (30)$$

According to the typicality lemma the second term on the RHS of (30) goes to zero as $n \to \infty$ [38]. The third term on the RHS of (30) goes to zero as $n \to \infty$ if [38],

$$R + R' < \mathbb{I}(U; Y). \quad (31)$$

We now show that the first term on the RHS of (30) also vanishes as $n \to \infty$. For a fix $\epsilon > 0$ consider the PMF Γ defined in (14). With respect to the random experiment described by Γ we have

$$\mathbb{E}_{C_n}\mathbb{P}_\Gamma\Big(\big(U^n(m, k, L), V^n, S^n(j)\big) \notin \mathcal{T}_{\epsilon'}^{(n)}|C_n\Big) \xrightarrow[n\to\infty]{} 0, \quad (32)$$

this follows because V^n is derived by passing $U^n(k, m, L) \sim P_U^{\otimes n}$, for every $(m, k) \in (\mathcal{M}, \mathcal{K})$, and $S^n(j) \sim P_S^{\otimes n}$, for every $j \in \mathcal{J}$, through the DMC $P_{V|U,S}^{\otimes n}$. Therefore (32) holds by weak law of large numbers. We also have

$$\begin{aligned}&\mathbb{E}_{C_n}||P_{U^n,S^n,V^n|C_n} - \Gamma_{U^n,S^n,V^n|C_n}||_1 \\ &\leq \mathbb{E}_{C_n}||P_{J,K,M,S^n,L,U^n,V^n,Z^n|C_n} \\ &\qquad - \Gamma_{J,K,M,S^n,L,U^n,V^n,Z^n|C_n}||_1,\end{aligned} \quad (33)$$

where based on (25) the RHS of (33) vanishes when n grows.

We now define $g_n : \mathcal{U}^n \times \mathcal{V}^n \times \mathcal{S}^n \to \mathbb{R}$ as $g_n(u^n, s^n, v^n) \triangleq \mathbb{1}_{\{(u^n,s^n,v^n)\notin\mathcal{T}_{\epsilon'}^{(n)}\}}$. We now have

$$\begin{aligned}&\mathbb{E}_{C_n}\mathbb{P}_P\Big(\big(U^n(k, m, L), S^n(j), V^n\big) \notin \mathcal{T}_{\epsilon'}^{(n)}|C_n\Big) \\ &= \mathbb{E}_{C_n}\mathbb{E}_P\Big[g_n(U^n(k, m, L), S^n(j), V^n)|C_n\Big] \\ &\leq \mathbb{E}_{C_n}\mathbb{E}_\Gamma\Big[g_n(U^n(k, m, L), S^n(j), V^n)|C_n\Big] \\ &\quad + \mathbb{E}_{C_n}\Big|\mathbb{E}_P\Big[g_n(U^n(k, m, L), S^n(j), V^n)|C_n\Big] \\ &\quad - \mathbb{E}_\Gamma\Big[g_n(U^n(k, m, L), S^n(j), V^n)|C_n\Big]\Big| \\ &\overset{(a)}{\leq} \mathbb{E}_{C_n}\mathbb{E}_\Gamma\Big[g_n(U^n(k, m, L), S^n(j), V^n)|C_n\Big] \\ &\quad + \mathbb{E}_{C_n}||P_{U^n,V^n,S_j^n|C_n} - \Gamma_{U^n,V^n,S_j^n|C_n}||_1,\end{aligned} \quad (34)$$

where (a) follows from [39, Property 1] for g_n being bounded by 1. From (32) and (33) the RHS of (34) vanishes when n grows.

Input Cost Analysis: From (32) average over a random codebook C_n we have

$$\begin{aligned}\mathbb{P}(\mathcal{E}) &= \mathbb{P}\Big(\big(U^n(m, k, L), V^n, S^n(j)\big) \notin \mathcal{T}_{\epsilon'}^{(n)}|C_n\Big) \\ &= \mathbb{P}\Big(\big(U^n(m, k, L), V^n, S^n(j), X^n\big) \notin \mathcal{T}_{\epsilon'}^{(n)}|C_n\Big) \xrightarrow[n\to\infty]{} 0.\end{aligned} \quad (35)$$

From Typical Average Lemma [38, Section 2.4] if $x^n \in \mathcal{T}_\epsilon^{(n)}$ then $b_1(x^n) \leq B_1$. Therefore,

$$\begin{aligned}&\mathbb{E}_{C_n,K,M}[b_1(X^n)] \\ &= \mathbb{P}(\mathcal{E})\mathbb{E}_{C_n,K,M}[b_1(X^n)|\mathcal{E}] + \mathbb{P}(\mathcal{E}^c)\mathbb{E}_{C_n,K,M}[b_1(X^n)|\mathcal{E}^c] \\ &= \mathbb{P}(\mathcal{E})B_{\text{max}}^{(1)} + \mathbb{P}(\mathcal{E}^c)B_1,\end{aligned} \quad (36)$$

where $B_{\text{max}}^{(1)} \triangleq \max_{x\in\mathcal{X}} b_1(x)$. From (35) the RHS of (36) tends to B_1 as n grows. Therefore,

$$\limsup_{n\to\infty} \mathbb{E}_{C_n,K,M,}[b_1(X^n)] \leq B_1. \quad (37)$$

Similarly, $\limsup_{n\to\infty} \mathbb{E}_{C_n,K,M,}[b_2(S^n)] \leq B_2$.

The region in Theorem 1 is derived by applying Fourier-Motzkin [40] to (26), (27), and (31). □

References

[1] A. B. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.

[2] P. H. Che, M. Bakshi, and S. Jaggi, "Reliable deniable communication: Hiding messages in noise," in *Proc. IEEE Int. Symp. on Info. Theory (ISIT)*, Istanbul, Turkey, Jul. 2013, pp. 2945–2949.

[3] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3493–3503, Jun. 2016.

[4] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2334–2354, May 2016.

[5] M. Tahmasbi and M. R. Bloch, "First- and second-order asymptotics in covert communication," *IEEE Trans. Inf. Theory*, vol. 65, no. 4, pp. 2190–2212, Apr. 2019.

[6] S.-H. Lee, L. Wang, A. Khisti, and G. W. Wornell, "Covert communication with channel-state information at the transmitter," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2310–2319, Sep. 2018.

[7] H. ZivariFard, M. R. Bloch, and A. Nosratinia, "Keyless covert communication in the presence of non-causal channel state information," in *Proc. IEEE Info. Theory Workshop (ITW)*, Visby, Sweden, Aug. 2019, pp. 1–5.

[8] ——, "Keyless covert communication via channel state information," *available at https://arxiv.org/abs/2003.03308*, Mar. 2020.

[9] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. Walkenhorst, "Achieving undetectable communication," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1195–1205, Oct. 2015.

[10] B. He, S. Yan, X. Zhou, and V. K. N. Lau, "On covert communication with noise uncertainty," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 941–944, Apr. 2017.

[11] T. V. Sobers, A. B. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Trans. Wireless Commun.*, vol. 16, no. 9, pp. 6193–6206, Sep. 2017.

[12] R. Soltani, D. Goeckel, D. Towsley, A. B. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7252–7267, Nov. 2018.

[13] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8517–8530, Dec. 2018.

[14] O. Shmuel, A. Cohen, O. Gurewitz, and A. Cohen, "Multi-antenna jamming in covert communication," in *Proc. IEEE Int. Symp. on Info. Theory (ISIT)*, Paris, France, Jul. 2019, pp. 987–991.

[15] Y.-K. Chia and A. El Gamal, "Wiretap channel with causal state information," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2838–2849, May 2012.

[16] Z. Goldfeld, P. Cuff, and H. H. Permuter, "Wiretap channels with random states non-causally available at the encoder," *IEEE Trans. Inf. Theory*, vol. 66, no. 3, pp. 1497–1519, Mar. 2020.

[17] T. S. Han and M. Sasaki, "Wiretap channels with causal state information: Strong secrecy," *IEEE Trans. Inf. Theory*, vol. 65, no. 10, pp. 6750–6765, Oct. 2019.

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

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

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

[21] Q. Zhang, M. Bakshi, and S. Jaggi, "Covert communication over adversarially jammed channels," in *Proc. IEEE Info. Theory Workshop (ITW)*, Guangzhou, China, Nov. 2018, pp. 1–5.

[22] E. C. van der Meulen, "A survey of multi-way channels in information theory: 1961-1976," *IEEE Trans. Inf. Theory*, vol. 23, no. 1, pp. 1–37, Jan. 1977.

[23] F. M. J. Willems and E. C. van der Meulen, "The discrete memoryless multiple-access channel with cribbing encoders," *IEEE Trans. Inf. Theory*, vol. 31, no. 3, pp. 313–327, May 1985.

[24] N. Helal, M. R. Bloch, and A. Nosratinia, "Cooperative resolvability and secrecy in the cribbing multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 66, no. 9, pp. 5429–5447, Sep. 2020.

[25] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[26] E. L. Lehmann and J. P. Romano, *Testing Statistical Hypotheses*. New York, NY, USA: Springer-Verlag, 2005.

[27] A. D. Wyner, "The common information of two dependent random variables," *IEEE Trans. Inf. Theory*, vol. 21, no. 2, pp. 163–179, Mar. 1975.

[28] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 752–772, May 1993.

[29] P. Cuff, "Distributed channel synthesis," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7071–7096, Nov. 2013.

[30] H. ZivariFard, M. R. Bloch, and A. Nosratinia, "One-sided channel resolvability in multiple access channel," *available at https://personal.utdallas.edu/~hxz163630/OneSidedResMAC.pdf*, Jan. 2021.

[31] M. H. Yassaee and M. R. Aref, "Multiple access wiretap channels with strong secrecy," in *Proc. IEEE Info. Theory Workshop (ITW)*, Dublin, Ireland, Sep. 2010, pp. 1–5.

[32] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[33] M. H. Yassaee, M. R. Aref, and A. A. Gohari, "A technique for deriving one-shot achievability results in network information theory," in *Proc. IEEE Int. Symp. on Info. Theory (ISIT)*, Istanbul, Turkey, Jul. 2013, pp. 1287–1291.

[34] S. Watanabe, S. Kuzuoka, and V. Y. F. Tan, "Nonasymptotic and second-order achievability bounds for coding with side-information," *IEEE Trans. Inf. Theory*, vol. 61, no. 4, pp. 1574–1605, Apr. 2015.

[35] I. Sason and S. Verdú, "f-divergence inequalities," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 5973–6006, Nov. 2016.

[36] Z. Goldfeld, G. Kramer, H. H. Permuter, and P. Cuff, "Strong secrecy for cooperative broadcast channels," *IEEE Trans. Inf. Theory*, vol. 63, no. 19, pp. 469–495, Jan. 2017.

[37] Y. Steinberg, "Resolvability theory for the multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 472–487, Mar. 1998.

[38] A. El Gamal and Y.-H. Kim, *Network Information Theory*, 1st ed. Cambridge, U.K: Cambridge University Press, 2012.

[39] E. C. Song, P. Cuff, and H. V. Poor, "A rate-distortion based secrecy system with side information at the decoders," in *Proc. 52th Annual Allerton Conference on Communication, Control, and Computing*, Monticello,IL, Sep. 2014, pp. 755–762.

[40] I. B. Gattegno, Z. Goldfeld, and H. H. Permuter, "Fourier-Motzkin elimination software for information theoretic inequalities," in *http://www.ee.bgu.ac.il/~fmeit/*, 2016.