2022 IEEE International Symposium on Information Theory (ISIT) | 978-1-6654-2159-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISIT50566.2022.9834682

# Covert Communication in the Presence of an Uninformed, Informed, and Coordinated 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

***Abstract*—This paper is eligible for the Jack Keil Wolf ISIT Student Paper Award. This paper investigates covert communication in the presence of a cooperative jammer. Covert communication refers to the inability of an adversary to distinguish data transmission from a so-called innocent symbol at the input. We consider three related problems: (1) a jammer without direct communication or coordination with the transmitter, (2) a jammer that cribs the output of the transmitter, and (3) a jammer that is able to coordinate with the transmitter via a secret key that is also shared with the legitimate receiver. For each model, we derive inner and outer bounds on the capacity region that are tight in some special cases. Unlike prior results in the literature, the jammer in our model does not have access to unlimited local randomness. In fact, uncovering the fundamental interplay between the covert communication rate, local randomness, and secret key rate, is one of the distinctions and contributions of the present work. In the context of a few specific channels, we calculate achievable covert rates to illuminate our results.**

## I. Introduction

Covert communication refers to reliable communication over a channel while requiring that an adversary called "warden," who observes a different channel output, remains unable to distinguish between data transmission and a so-called innocent symbol at the input [1]–[5]. In a single-transmitter Discrete Memoryless Channel (DMC), the number of covert bits that can be reliably communicated over $n$ channel transmissions scales at most as $O(\sqrt{n})$ [4].The search for positive covert rates has led to the study of channels whose Channel State Information (CSI) is known at some legitimate nodes but not the warden [6]–[8], or when the warden has uncertainty about the power of noise or interference [9]–[15]. Positive covert rates were demonstrated [11] over Additive White Gaussian Noise (AWGN) and standard block fading channels, albeit with unlimited local randomness at the jammer and without calculating the value of covert communication rate. In [15] the jammer has the benefit of a channel observation, senses the channel, and transmits when it estimates that the legitimate transmitter is silent. This work depends on the warden being limited to a power detector.

A broader class of contributions is also relevant to the present work. The problem of secret communication over DMCs with random states has been studied in [16]–[19]. Arbitrarily varying wiretap channels under strong and semantic secrecy criterion have been studied in [20]–[22] and covert communication over adversarially jammed channels has been studied in [23]. Multiple-Access Channel (MAC) with cribbing encoders was first studied by Willems and van der Meulen [24], [25] and channel resolvability and strong secrecy for a discrete memoryless MAC with cribbing has been studied in [26]. Also, discrete memoryless and Gaussian multiple-access wiretap channel are studied in [27].

We consider three related problems: (1) *blind jammer* where the jammer has no direct communication or coordination with the transmitter, (2) *informed jammer* where the jammer cribs the output of the transmitter, and (3) *coordinated jammer*, where the jammer is able to coordinate with the transmitter via a secret key that is also shared with the legitimate receiver. The second model is analyzed under the non-causal cribbing. For each model, we derive inner and outer bounds on the capacity region that are tight in some special cases. In each of the three problems mentioned above, we provide tight inner and outer bounds *if* unlimited local randomness is allowed. A key contribution of this work, however, is when local randomness is treated as a valuable resource; our work uncovers the fundamental interplay between covert transmission rates and the amount of local randomness that is needed to enable it. In the context of a few specific channels, we calculate achievable covert rates to illuminate our results.

Our work is distinct from the literature of covert communication with jamming in several ways. First, many works in the literature depend, essentially, on the covert codebook being unavailable to warden and/or an unlimited secret key being shared between legitimate parties. In our work, codebooks are public knowledge and all secret keys are quantified. Second, the literature thus far has only considered jammers that are unrestricted in their use of local randomness. Our work considers randomness as a valuable resource and explores the interplay of the amount of local randomness, the rate of the shared key, and the covert rates enabled by jamming. Third, some works in the literature restrict the warden to a power detector [12]–[14] while our work permits the warden to use a more capable statistical detector.

## II. Preliminaries

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

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.

978-1-6654-2159-1/22/$31.00 ©2022 IEEE

$P_X(x)$ we write $P(x)$. 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 $\mathbb{V}(P,Q) \triangleq \frac{1}{2}\sum_x |P(x) - Q(x)|$. Throughout the paper, $\log$ denotes the base 2 logarithm. $\mathbb{H}_P$ and $\mathbb{I}_P$ indicates that an entropy or a mutual information term is calculated with respect to a Probability Mass Function (PMF) $P$. For brevity, we sometimes omit the subscripts in the entropy and mutual information terms if they are clear from the context. Also, the convex hull of the set $\mathcal{A}$ is denoted by $\text{conv}(\mathcal{A})$. The set of $\epsilon-$strongly jointly typical sequences of length $n$, according to $P_X$, is denoted by $\mathcal{T}_\epsilon^{(n)}(P_X)$.

## III. Problem Definition

Consider a discrete memoryless $(\mathcal{X}, \mathcal{S}, \mathcal{Y}, \mathcal{Z}, W_{Y,Z|X,S})$, which consists of channel input alphabet $\mathcal{X}$ at the transmitter, channel input alphabet $\mathcal{S}$ at the jammer, channel output alphabet $\mathcal{Y}$ at the receiver, and channel output alphabet $\mathcal{Z}$ at the warden. All alphabets are finite.

Let $x_0 \in \mathcal{X}$ be the innocent symbol which will be sent over the channel by the transmitter when no communication takes place. When the transmitter sends $x_0^n \in \mathcal{X}^n$, unlike other jamming problems, here the jammer transmits a non-independent and identically distributed (i.i.d.) *coded* sequence $S^n$. Therefore, the distribution induced at the output of the channel when no communication takes place, denoted by $\Upsilon_{Z^n}$, is not necessarily i.i.d. The first reason that we use a coded jammer instead of a jammer that transmits i.i.d. sequences is that random numbers are a precious resource in practice, and we want to use this resource as little as possible. The second reason that we use a coded jammer is that it enables us to *design* the jammer's codebook in such a way that it helps the transmitter to communicate both covertly and reliably.

Here we consider three different jamming models. In the first model, the transmitter and the receiver are assumed to have access to a rate limited and uniformly distributed shared secret key $K \in \mathcal{K}$, this helps the transmitter to communicate with the receiver covertly even when the receiver's channel is noisier than the warden's channel. Nevertheless, the existence of this secret key is not crucial in our analysis, and one can extend our results by removing the shared secret key between the transmitter and the receiver. In this problem, we assume that there is a secret key with negligible rate between the transmitter and jammer, and therefore they can coordinate, however we show that our result also recovers the results when there is no secret key shared between the jammer and the transmitter.

In the second jamming model, the jammer and the receiver are assumed to have access to a rate limited and uniformly distributed shared secret key $K \in \mathcal{K}$, this helps the receiver to cancel the interference caused by the randomness that the jammer interpolates into the channel. Similar to the previous models, the existence of this secret key is not crucial in our analysis. Here, the transmitter's channel input is assumed to be available non-causally at the jammer so that the jammer can coordinate its channel input according to the transmitter's channel input. The transmitter does not have access to any source of local randomness, but the jammer uses a rate limited source of local randomness, which is shared with the receiver.

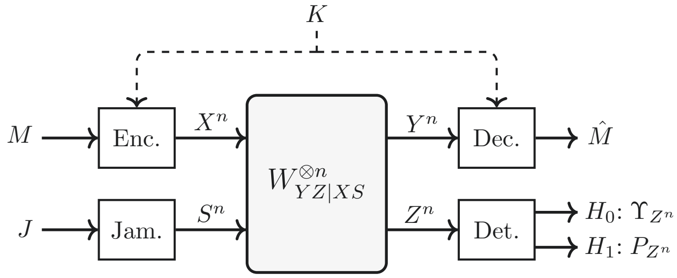

Fig. 1. Covert communication with a blind jammer

In the third jamming model, the transmitter, the receiver, and the jammer are assumed to have access to a rate limited and uniformly distributed shared secret key $K \in \mathcal{K}$. This helps the transmitter to coordinate its channel input according to the jammer's channel input, and it also helps the receiver to cancel the interference caused by the jammer's channel input. In this problem, the transmitter and the jammer do not have access to any source of local randomness.

The code is assumed known to all parties, and the objective is to design a code that is both reliable and covert. Reliable means that the average probability of error $P_e^{(n)} = \mathbb{P}(\hat{M} \neq M)$ vanishes when $n \to \infty$. Covert means that the warden cannot determine whether communication is happening (hypothesis $H_1$) or not (hypothesis $H_0$). Specifically, the probabilities of false alarm $\alpha_n$ (warden deciding $H_1$ when $H_0$ is true) and missed detection $\beta_n$ (warden deciding $H_0$ when $H_1$ is true) satisfy $\alpha_n + \beta_n = 1$ for an uninformed warden making random decisions. When the channel carries communication, the warden's channel output distribution is $P_{Z^n}$ and when the channel does not carry communication, the warden's channel output distribution is $\Upsilon_{Z^n}$ and the optimal hypothesis test by the warden satisfies $\alpha_n + \beta_n \geq 1 - \sqrt{\mathbb{D}(P_{Z^n}||\Upsilon_{Z^n})}$ [28]. Therefore, we define a code as covert if $\mathbb{D}(P_{Z^n}||\Upsilon_{Z^n})$ vanishes when $n \to \infty$. We assume that $\text{supp}(\Upsilon_Z) = \mathcal{Z}$ for otherwise $\mathbb{D}(P_{Z^n}||\Upsilon_{Z^n})$ diverges.

A rate $R$ is achievable if there exists a sequence of reliable and covert codes, and the covert capacity is the supremum of all achievable covert rates.

## IV. Blind Jamming

In this section, we study a scenario in which a transmitter wishes to communicate a message $M \in \mathcal{M}$ covertly with a receiver while there is a friendly jammer in the environment. Here, the transmitter and the receiver are assumed to have access to a rate limited and uniformly distributed shared secret key $K \in \mathcal{K}$, this helps the transmitter to communicate covertly with the receiver when the warden has a better channel than the receiver. But, one can simply extend our results to the case that there is no shared secret key between the transmitter and the receiver. In this problem, unlike the jamming problems studied so far, the jammer has a limited source of local randomness. We study this problem when the jammer and the transmitter share a secret key of negligible rate, and therefore the transmitter and the jammer can coordinate and as a result the jammer knows in which blocks communication is happening. But our results can be reduced to a case that there is no shared secret key of negligible rate between the transmitter and the jammer.

**Theorem 1.** *Let*

$$\mathcal{A} = \left\{ \begin{array}{l} (R, R_K) \geq 0 : \exists \big(P_{S_1XYZ}, \Upsilon_{S_2ZY}\big) \in \mathcal{D} : \\ R < \mathbb{I}_P(X;Y) \\ R_K > \mathbb{I}_P(X;Z) - \mathbb{I}_P(X;Y) \\ R_J > \max\big\{\mathbb{I}_P(S_1;Z), \mathbb{I}_\Upsilon(S_2;Z)\big\} \\ R_K + R_J > \mathbb{I}_P(X, S_1; Z) - \mathbb{I}_P(X;Y) \end{array} \right\}, \tag{1a}$$

*where,*

$$\mathcal{D} \triangleq \left\{ \begin{array}{l} \big(P_{S_1XYZ}, \Upsilon_{S_2ZY}\big) : \\ P_{S_1XYZ} = P_{S_1}P_X W_{YZ|XS} \\ \Upsilon_{S_2YZ} = P_{S_2} W_{YZ|S, X=x_0} \\ P_Z = \Upsilon_Z \end{array} \right\}. \tag{1b}$$

*The covert capacity of the DMC $W_{YZ|XS}$ with a blind jammer is lower-bounded as*

$$C_{\text{BJ}} \supseteq \operatorname{conv}(\mathcal{A}). \tag{2}$$

The proof for Theorem 1 is based on channel resolvability, the details of the proof are available in [29, Appendix D].

**Remark 1.** *According to Theorem 1, the transmitter and the receiver can communicate covertly if the covert constraint $P_Z = \Upsilon_Z$ holds, if the warden has a better channel the rate of the secret key between the transmitter and the receiver is big enough to compensate for that, and if the sum rate of the message, the shared key, and the jammer's local randomness are big enough to induce i.i.d. distribution on the warden's output.*

**Remark 2.** *The region in Theorem 1 reduces to the case that there is no shared secret key between the transmitter and the jammer if we set $S_1 = S_2$. Also, if we set $S_1 = \emptyset$, the region in Theorem 1 reduces to the region with a strategy proposed in [11], [15], which is similar to the stealth communication introduced in [30] because instead of the jammer the transmitter itself can transmit random signals for the no-communication mode. In [29, Example 3] we show that this strategy can be suboptimal in the context of an example. This is partly because, for this strategy, the superposition property of the wireless channels does not exist.*

We now provide an upper bound on the covert capacity when a friendly jammer is present. Note that in the problem described above, the jammer is using a limited source of local randomness with rate $R_J$. To derive the upper bound, we use the fact that the covert capacity when the jammer uses an unlimited source of local randomness is not less than the covert capacity when the jammer uses a limited source of local randomness. Hence, we derive an upper bound on the covert capacity when the jammer uses an unlimited source of local randomness, by transmitting an i.i.d. sequence according to some distribution $P_{S_1}$ when communication is not happening and transmitting another i.i.d. sequence according to $P_{S_2}$ when communication is happening, and therefore this upper bound is also an upper bound on the covert capacity when the jammer uses a limited amount of local randomness. In this case, the distribution induced on the warden's observation when communication is not happening is $Q_0^{\otimes n}$, where $Q_0(\cdot) = \sum_{s\in\mathcal{S}} P_{S_1}(s_1) W_{Z|X=x_0,S}(\cdot|x_0, s)$.

**Theorem 2.** *Let*

$$\mathcal{A} = \left\{ \begin{array}{l} (R, R_K) \geq 0 : \exists P_{S_2XYZ} \in \mathcal{D} : \\ R \leq \mathbb{I}(X;Y) \\ R_K \geq \mathbb{I}(X;Z) - \mathbb{I}(X;Y) \end{array} \right\}, \tag{3a}$$

*where,*

$$\mathcal{D} \triangleq \left\{ \begin{array}{l} P_{S_2XYZ} : \\ P_{S_2XYZ} = P_{S_2}P_X W_{YZ|XS} \\ P_Z = Q_0 \end{array} \right\}. \tag{3b}$$

*The covert capacity of the DMC $W_{YZ|XS}$ with a blind jammer is upper-bounded as*

$$C_{\text{BJ}} \subseteq \operatorname{conv}(\mathcal{A}). \tag{4}$$

The details of the proof are available in [29, Appendix B].

**Remark 3.** *The achievability scheme in Theorem 1 meets the upper bound in Theorem 2 when the jammer has an unlimited source of local randomness and transmits an i.i.d. sequence with some distribution $P_{S_1}$ when communication is not happening and transmits an i.i.d. sequence with some distribution $P_{S_2}$ when communication is happening.*

*Example (Noiseless Binary Additive Channel):* Consider a scenario in which the channel inputs and outputs are all binary, the innocent symbol $x_0 = 0$, and the channel rules are $Y = Z = X \oplus S$.

**Proposition 1.** *The covert capacity for the example described above is lower-bounded as,*

$$C_{\text{BJ}} \supseteq \operatorname{conv} \left\{ \begin{array}{l} (R, R_K, R_J) : \alpha \in [0\!:\!0.5] \\ R < \mathbb{H}_b(\alpha),\ R_K > 0,\ R_J > \mathbb{H}_b(\alpha) \end{array} \right\}. \tag{5}$$

*Proof.* We now show that the region provided in Theorem 1 reduces to the region in Proposition 1. Without loss of generality, let the channel input $X$ be a Bernoulli random variable with parameter $\alpha \in [0\!:\!0.5]$, the jammer's channel input $S_1$ be a Bernoulli random variable with parameter $\beta \in [0\!:\!0.5]$, and the jammer's channel input $S_2$ be a Bernoulli random variable with parameter $\eta \in [0\!:\!0.5]$. The covertness constraint $P_Z = \Upsilon_Z$ implies that,

$$\begin{aligned} P_Z(z=0) &= \mathbb{P}(x=0, s_1=0) + \mathbb{P}(x=1, s_1=1) \\ &= \alpha\beta + (1-\alpha)(1-\beta), \end{aligned} \tag{6}$$

$$\Upsilon_Z(z=0) = \mathbb{P}(s_2=0) = \eta. \tag{7}$$

By choosing $\beta = 0$, the covertness constraint $P_Z = \Upsilon_Z$, reduces to $\eta = \alpha$. We now have,

$$\begin{aligned}
\mathbb{I}_P(X;Y) &\overset{(a)}{=} \mathbb{I}_P(X;Z) = \mathbb{H}_P(Y) - \mathbb{H}_P(Y|X)\\
&= \mathbb{H}_P(X \oplus S_1) - \mathbb{H}_P(X \oplus S_1|X)\\
&= \mathbb{H}_P(X) = \mathbb{H}_b(\alpha), && (8)\\
\mathbb{I}_P(S_1;Z) &= 0, && (9)\\
\mathbb{I}_\Upsilon(S_2;Z) &= \mathbb{H}_\Upsilon(Z) - \mathbb{H}_\Upsilon(Z|S_2)\\
&= \mathbb{H}_\Upsilon(x_0 \oplus S_2) - \mathbb{H}_\Upsilon(x_0 \oplus S_2|S_2)\\
&= \mathbb{H}_\Upsilon(S_2) = \mathbb{H}_b(\alpha), && (10)
\end{aligned}$$

$$\mathbb{I}_P(X,S_1;Z) - \mathbb{I}_P(X;Y) \overset{(b)}{=} \mathbb{I}_P(S_1;Z|X) = 0, \tag{11}$$

where $(a)$ and $(b)$ follow since in this example $Y = Z$. □

## V. Informed Jammer

In this section, we study a problem in which to transmit the covert message, denoted by $M \in \mathcal{M}$, the jammer and the receiver are assumed to share a rate limited and uniformly distributed shared secret key $K \in \mathcal{K}$, this helps the receiver to cancel the interference caused by the randomness that the jammer interpolates into the channel. Here, the transmitter's channel input is assumed to be available non-causally at the jammer thereby the jammer can coordinate its channel input according to the transmitter's channel input. The transmitter does not use any source of local randomness, but the jammer uses a limited amount of local randomness, which is shared with the receiver as a shared secret key. This problem setup is illustrated in Fig. 2. The problems that the transmitter's output is available strictly-causally, or causally at the jammer is available in [29].

**Theorem 3.** *Let*

$$\mathcal{A} = \left\{\begin{array}{l}(R,R_K) \geq 0 : \exists\big(P_{S_1XYZ}, \Upsilon_{S_2YZ}\big) \in \mathcal{D} :\\ R < \min\big\{\mathbb{I}_P(X,S_1;Y), \mathbb{H}_P(X)\big\}\\ R_K > \max\big\{\mathbb{I}_P(X,S_1;Z)\\ \quad - \min\big\{\mathbb{I}_P(X,S_1;Y), \mathbb{H}_P(X)\big\}, \mathbb{I}_\Upsilon(S_2;Z)\big\}\end{array}\right\}, \tag{12a}$$

*where*

$$\mathcal{D} = \left\{\begin{array}{l}\big(P_{S_1XYZ}, \Upsilon_{S_2YZ}\big) :\\ P_{S_1XYZ} = P_X P_{S_1|X} W_{YZ|XS}\\ \Upsilon_{S_2YZ} = P_{S_2} W_{YZ|X=x_0,S}\\ \min\big\{\mathbb{I}_P(X,S_1;Y), \mathbb{H}_P(X)\big\} > \mathbb{I}_P(X;Z)\\ P_Z = \Upsilon_Z\end{array}\right\}. \tag{12b}$$

*The covert capacity of the DMC $W_{YZ|XS}$ when the transmitter's channel input is available non-causally at the jammer is lower bounded by*

$$C_{\text{IJ-NC}} \supseteq \text{conv}(\mathcal{A}). \tag{13}$$

Theorem 3 is proved in [29, Appendix O].

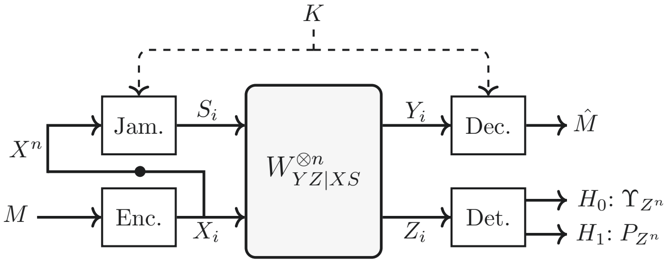

Fig. 2. Covert communication with an informed jamming

Similar to the upper bound provided in the previous section, we provide an upper bound on the covert capacity when the jammer has an unlimited source of local randomness and transmits an i.i.d. sequence, according to some distribution $P_{S_2}$, when the transmitter is not communicating with the receiver and transmits a sequence from its codebook otherwise. In this case, the distribution induced on the warden's observation is $Q_0^{\otimes n}$ where $Q_0(\cdot) = \sum_{s_2 \in \mathcal{S}_2} P_{S_2}(s_2) W_{Z|X=x_0,S}(\cdot|x_0,s_2)$.

**Theorem 4.** *Let*

$$\mathcal{A} = \left\{\begin{array}{l}(R,R_K) \geq 0 : \exists P_{XSYZ} \in \mathcal{D} :\\ R \leq \min\{\mathbb{I}(X,S;Y), \mathbb{H}(X)\}\\ R_K \geq \mathbb{I}(X,S;Z) - \min\{\mathbb{I}(X,S;Y), \mathbb{H}(X)\}\end{array}\right\}, \tag{14a}$$

*where*

$$\mathcal{D} = \left\{\begin{array}{l}P_{XSYZ} :\\ P_{XSYZ} = P_X P_{S|X} W_{YZ|XS}\\ \min\{\mathbb{I}(X,S;Y), \mathbb{H}(X)\} \geq \mathbb{I}(X;Z)\\ P_Z = Q_0\end{array}\right\}. \tag{14b}$$

*The covert capacity of the DMC $W_{YZ|XS}$ when the transmitter's channel input is available non-causally at the jammer is upper bounded by*

$$C_{\text{IJ-NC}} \subseteq \text{conv}(\mathcal{A}). \tag{15}$$

Theorem 3 is proved in [29, Appendix P].

**Remark 4.** *Similar to Remark 3, the achievability scheme in Theorem 3 meets the upper bound in Theorem 4 if the jammer has unlimited source of local randomness. In this case, the jammer transmits an i.i.d. sequence when the transmitter is not communicating with the receiver and transmits a sequence from its codebook when communication is happening.*

*Example (Binary Multiplicative-Additive Channel):* Consider a channel in which $X, Y, Z$, and $S$ are all binary and the innocent symbol is $x_0 = 0$, the transmitter's output is available non-causally or causally at the jammer, and the law of the channel is as follows,

$$Y = X \otimes S, \qquad Z = X \oplus S. \tag{16}$$

**Proposition 2.** *The covert capacity of the DMC described above is*

$$C_{\text{IJ-NC}} = C_{\text{IJ-C}} = \Big\{(R,R_K) : R \leq 1,\ R_K \geq 0\Big\}. \tag{17}$$

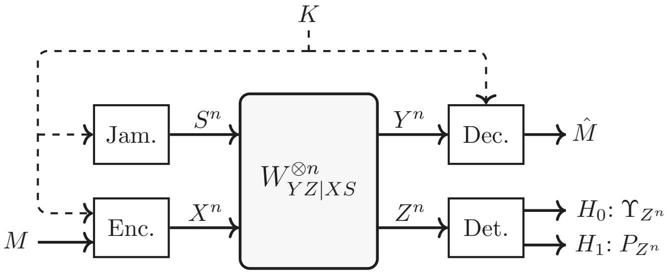

Fig. 3. Covert communication with a shared secret key

Intuitively speaking, to satisfy the condition $P_Z = \Upsilon_Z$ the jammer can choose $S_1 = X$ therefore $Y = X$ and $Z = 0$ and the transmitter can communicate with rate $\max_{P_X} \mathbb{H}(X) = 1$ with the receiver. The proof for Proposition 2 is similar to that of Proposition 1, the details of the proof are available in [29, Section VIII].

## VI. Coordinated Jammer

Now we study a problem in which there is a rate limited and uniformly distributed shared secret key $K \in \mathcal{K}$ between the legitimate terminals (i.e., the transmitter, the receiver, and the jammer), this helps the transmitter to coordinate its channel input according to the jammer's channel input, and it also helps the receiver to cancel the interference caused by the jammer's channel input. In this problem, the transmitter and the jammer do not have access to any source of local randomness.

**Theorem 5.** *Let*

$$\mathcal{A} = \left\{ \begin{array}{l} (R, R_K) \geq 0 : \left(P_{S_1XYZ}, \Upsilon_{S_2ZY}\right) \in \mathcal{D} : \\ R < \mathbb{I}_P(X;Y|S_1) \\ R_K > \max\{\mathbb{I}_P(X, S_1; Z) \\ \quad -\mathbb{I}_P(X;Y|S_1), \mathbb{I}_P(S_1;Z), \mathbb{I}_\Upsilon(S_2;Z)\} \end{array} \right\}, \tag{18a}$$

*where*

$$\mathcal{D} = \left\{ \begin{array}{l} \left(P_{S_1XYZ}, \Upsilon_{S_2ZY}\right) : \\ P_{S_1XYZ} = P_{S_1}P_{X|S_1}W_{YZ|XS_1} \\ \Upsilon_{S_2ZY} = P_{S_2}W_{YZ|X=x_0,S_2} \\ P_Z = \Upsilon_Z \end{array} \right\}. \tag{18b}$$

*The covert capacity of the DMC $W_{YZ|XS}$ when there is a shared key between all the legitimate terminals is lower bounded as*

$$C_{\text{FK}} \supseteq \text{conv}(\mathcal{A}). \tag{19}$$

The proof for Theorem 5 is based on superposition coding and channel resolvability, the details of the proof are available in [29, Appendix E].

We now provide an upper bound on the covert capacity when there is a shared secret key between the legitimate terminals. Note that in the problem described above the jammer is using a limited amount of randomness with rate $R_K$, which is shared between all the legitimate terminals, and therefore the legitimate terminals can coordinate that is the jammer and the receiver know in which blocks the transmitter is communicating with the receiver. Similar to the Theorem 2, we derive an upper bound for the case that the jammer uses an unlimited amount of randomness when the transmitter is not communicating with the receiver. In this case, the distribution induced on the warden's observation when communication is not happening is $Q_0^{\otimes n}$, where $Q_0(\cdot) = \sum_{s \in \mathcal{S}} P_S(s) W_{Z|X=x_0,S}(\cdot|x_0, s)$.

**Theorem 6.** *Let*

$$\mathcal{A} = \left\{ \begin{array}{l} (R, R_K) \geq 0 : \exists P_{SXYZ} \in \mathcal{D} : \\ R \leq \mathbb{I}(X;Y|S) \\ R_K \geq \max\{\mathbb{I}(X, S; Z) - \mathbb{I}(X;Y|S), \mathbb{I}(S;Z)\} \end{array} \right\}, \tag{20a}$$

*where*

$$\mathcal{D} = \left\{ \begin{array}{l} P_{SXYZ} : \\ P_{SXYZ} = P_S P_{X|S} W_{YZ|XS} \\ P_Z = Q_0 \end{array} \right\}. \tag{20b}$$

*The covert capacity of the DMC $W_{YZ|XS}$ when there is a shared key between all the legitimate terminals is upper bounded by*

$$C_{\text{FK}} \subseteq \text{conv}(\mathcal{A}). \tag{21}$$

Theorem 3 is proved in [29, Appendix F].

**Remark 5.** *One can show that when the jammer has unlimited source of local randomness and transmits an i.i.d. sequence when the transmitter is not communicating with the receiver and transmits a sequence from its codebook when communication is happening, the achievability scheme in Theorem 5 meets the upper bound in Theorem 6.*

*Example (Noiseless Binary Additive Channel):* Consider a scenario in which the channel inputs and outputs are all binary, the innocent channel input symbol $x_0 = 0$, and the channel rules are as follows,

$$Y = Z = X \oplus S. \tag{22}$$

**Proposition 3.** *The covert capacity for the example described above is lower bounded as,*

$$C_{\text{FK}} \supseteq \text{conv} \left\{ \begin{array}{l} (R, R_K) : \alpha, \beta, \eta \in (0 : 0.5) \\ R < (\alpha + \beta)\mathbb{H}_b\left(\frac{\alpha}{\alpha+\beta}\right) \\ \qquad +(1 - \alpha - \beta)\mathbb{H}_b\left(\frac{\eta}{1-\alpha-\beta}\right) \\ R_K > \mathbb{H}_b(\alpha + \eta) \end{array} \right\}. \tag{23}$$

The proof for Proposition 3 is similar to that of Proposition 1, the details of the proof are available in [29, Section IV].

**Remark 6.** *Intuitively speaking, in this channel, since the transmitter has access to the jammer's channel input through the shared key it chooses the channel input $X^n$ such that after it adds up with the jammer's channel input the results look like it has been generated according to $P_S$. The receiver can recover $X^n$ since it has access to $S^n$ through the shared secret key, but the warden cannot distinguish its output from $S^n$.*

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

[4] 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.

[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] W. Xiong, Y. Yao, X. Fu, and S. Li, "Covert communication with cognitive jammer," *IEEE Commun. Lett.*, vol. 9, no. 10, pp. 1753–1757, Oct. 2020.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

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

[29] H. ZivariFard, M. R. Bloch, and A. Nosratinia, "Covert communication via cooperative jamming," *available at https://personal.utdallas.edu/∼hxz163630/Cooperative_Covert.pdf*, Feb. 2021.

[30] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," in *Proc. IEEE Int. Symp. on Info. Theory (ISIT)*, HI, USA, Jul. 2014, pp. 601–605.