Capacity Theorems for Covert Bosonic Channels

Michael S. Bullock,* Christos N. Gagatsos,† Boulat A. Bash,*†
*Electrical and Computer Engineering Department, University of Arizona, Tucson, AZ
†College of Optical Sciences, University of Arizona, Tucson, AZ

***Abstract*—We study quantum-secure covert-communication over lossy thermal-noise bosonic channels, the quantum-mechanical model for many practical channels. We derive the expressions for the covert capacity of these channels: $L_{\textbf{no-EA}}$, when Alice and Bob share only a classical secret, and $L_{\textbf{EA}}$, when they benefit from entanglement assistance. Entanglement assistance alters the fundamental scaling law for covert communication. Instead of $L_{\textbf{no-EA}}\sqrt{n}-r_{\textbf{no-EA}}(n)$, $r_{\textbf{no-EA}}(n)=o(\sqrt{n})$, entanglement assistance allows $L_{\textbf{EA}}\sqrt{n}\log n - r_{\textbf{EA}}(n)$, $r_{\textbf{EA}}(n) = o(\sqrt{n}\log n)$, covert bits to be transmitted reliably over n channel uses. However, noise in entanglement storage erases the $\log n$ gain from our achievability; work on the matching converse is ongoing.**

I. Introduction

In contrast to standard information security methods (e.g., encryption, information-theoretic secrecy, and quantum key distribution (QKD)) that protect the transmission's content from unauthorized access, *covert* or *low probability of detection/intercept (LPD/LPI)* communication [2]–[4] prevents adversarial detection of transmissions in the first place. The covertness requirement constrains the transmission power averaged over the blocklength n to $\propto 1/\sqrt{n}$, where the power is either measured directly in watts [2], [3] and mean photon number [5], [6] output by a physical transmitter, or indirectly, as the frequency of non-zero symbol transmission over the discrete classical [7], [8] and quantum [9], [10] channels.

For many channels, including classical additive white Gaussian noise (AWGN) [2], [3], and discrete memoryless channels (DMCs) [7], [8], the power constraint prescribed by the covertness requirement imposes the *square root law* (SRL): no more than $L\sqrt{n}$ covert bits can be transmitted reliably in n channel uses. We call constant L the *covert capacity* of a channel, since it only depends on the channel parameters and captures a fundamental limit. Attempting to transmit more results in either detection by the adversary with high probability as $n\to\infty$, or unreliable transmission. Even though the Shannon capacity of such channels is zero (since $\lim_{n\to\infty}\frac{L\sqrt{n}}{n}=0$), the SRL allows reliable transmission of a significant number of covert bits for large n.

To date, the focus has been on classical covert communication. However, quantum mechanics governs the fundamental laws of nature, and quantum information theory is required to determine the ultimate limits of any communications system. Here we focus on the lossy thermal noise bosonic channel depicted in Fig. 1, called the bosonic channel for brevity, and formally described in Section II-A. The bosonic channel is a quantum-mechanical model of many practical channels (including optical, microwave, and radio frequency (RF)). This channel is parametrized by the power coupling (transmissivity) η between the transmitter Alice and the intended receiver Bob, and the mean photon number $\bar{n}_{\mathrm{B}}$ per mode injected by the thermal environment, where a single spatial-temporal-polarization mode is our fundamental transmission unit. We call a covert communication system *quantum secure* when it is robust against an adversary Willie who not only knows the transmission parameters (including the start time, center frequency, duration, and bandwidth), but also has access to all the transmitted photons that are not captured by Bob, as well as arbitrary quantum information processing resources (e.g., joint detection measurement, quantum memory, and quantum computing). While our approach is motivated by the security standards from the QKD literature, covertness demands a different set of assumptions. We require excess noise that is not under Willie's control (e.g., the unavoidable thermal noise from the blackbody radiation at the center wavelength of transmission and the receiver operating temperature). This assumption is not only well-grounded in practice, but also necessary for covertness, as the transmissions cannot be hidden from quantum-capable Willie that fully controls noise on the channel [5, Th. 1], [11]. Finally, we assume that Alice and Bob share a resource that is inaccessible by Willie. This enables covertness irrespective of channel conditions, as well as substantially increases the number of reliably-transmissible covert bits when the resource is an entangled quantum state.

In [6] we develop an expression for the maximum mean photon number $\bar{n}_{\mathrm{S}}$ that Alice can transmit under the aforemen-

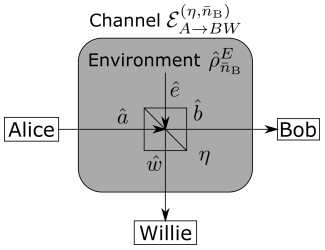

Fig. 1. Single-mode bosonic channel $\mathcal{E}^{(\eta,\bar{n}_{\mathrm{B}})}_{A\to BW}$ modeled by a beamsplitter with transmissivity η and an environment injecting a thermal state $\hat{\rho}_{\bar{n}_{\mathrm{B}}}$ with mean photon number $\bar{n}_{\mathrm{B}}$. $\hat{a}$, $\hat{e}$, $\hat{b}$, and $\hat{w}$ label input/output modal annihilation operators.

CNG acknowledges the Office of Naval Research (ONR) MURI program on Optical Computing under grant no. N00014-14-1-0505. MSB and BAB were sponsored by the Army Research Office under Grant Number W911NF-19-1-0412. This material is based upon work supported in part by the National Science Foundation under Grant No. CCF-2006679. The authors also acknowledge General Dynamics Mission Systems for supporting this research.
The results with full proofs (except Section III-D) were published in [1].

tioned quantum-secure covertness conditions. Here, we rigorously examine the coding limits under the resulting constraint.

Our main contribution is the analysis of the covert communication system depicted in Fig. 2 and formally described in Sec. II-B, with and without an entangled resource state shared by Alice and Bob. Since entanglement assistance gain manifests only when $\bar{n}_{\mathrm{S}} \to 0$ and $\bar{n}_{\mathrm{B}} > 0$, we expect it to benefit covert communication. We find that, while entanglement assistance alters the fundamental scaling law of covert communication, the gain is fragile:

1) We show that without entanglement assistance, the SRL has a standard form: $M_{\text{no-EA}} = L_{\text{no-EA}}\sqrt{n} - r_{\text{no-EA}}(n)$, $r_{\text{no-EA}}(n) = o(\sqrt{n})$, covert bits transmissible reliably over n channel uses.[1] Our second-order bound is similar to classical [13]: $M_{\text{no-EA}} \geq L_{\text{no-EA}}\delta\sqrt{n} + K_{\text{no-EA}}\Phi^{-1}(\epsilon)n^{1/4} + O(n^{n/8})$, where ϵ is the average decoding error probability and $\Phi^{-1}(x)$ is the inverse-Gaussian cumulative distribution function.
2) We show that with entanglement assistance, the scaling law becomes $M_{\text{EA}} = L_{\text{EA}}\sqrt{n}\log n - r_{\text{EA}}(n)$, $r_{\text{EA}}(n) = o(\sqrt{n}\log n)$. We derive the expression for the optimal constant L_{EA} and the second-order bound.[2]
3) We analyze the impact of loss and noise in entanglement storage and find that, while loss only reduces the entanglement-assisted capacity L_{EA}, noise erases the $\log n$ scaling gain in our achievability proof. We defer the matching converse to future work.

Next, we present the mathematical prerequisites, including the channel and system models, the formal definitions of covertness and reliability, and the bounds we need. We state results in Sec. III, deferring the formal proofs to [1]. We conclude with the discussion of future work in Sec. IV.

II. Prerequisites

A. Channel model

We focus on a single-mode lossy thermal noise bosonic channel $\mathcal{E}_{A\to BW}^{(\eta,\bar{n}_{\mathrm{B}})}$ in Fig. 1. It quantum-mechanically describes the transmission of a single (spatio-temporal-polarization) mode of the electromagnetic field at a given transmission wavelength (such as optical or microwave) over linear loss and additive Gaussian noise (such as noise stemming from blackbody radiation). Here, we introduce the bosonic channel briefly, deferring the details to [14]. The attenuation in the Alice-to-Bob channel is modeled by a beamsplitter with transmissivity (fractional power coupling) η. The input-output relationship between the bosonic modal annihilation operators of the beamsplitter, $\hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{e}$, requires the "environment" mode $\hat{e}$ to ensure that the commutator $\left[\hat{b}, \hat{b}^\dagger\right] = 1$, and to preserve the Heisenberg uncertainty law of quantum mechanics. On the contrary, classical power attenuation is described by $b = \sqrt{\eta}a$, where a and b are complex amplitudes of input and output mode functions. Bob captures a fraction η of Alice's transmitted photons, while Willie has access to the remaining $1-\eta$ fraction. We model noise by mode $\hat{e}$ being in a zero-mean thermal state $\hat{\rho}_{\bar{n}_{\mathrm{B}}}$ which injects mean $\bar{n}_{\mathrm{B}}$ photons per mode.

B. System model

The covert communication framework is depicted in Fig. 2. Our fundamental transmission unit is the field mode described above. We assume a discrete-time model with $n = 2TW$ modes available to Alice and Bob. TW is the number of orthogonal temporal modes, which is the product of the transmission duration T (in seconds) and the optical bandwidth W (in Hz) of the source around its center frequency, and the factor of two corresponds to the use of both orthogonal polarizations. The orthogonality of the available modes results in the bosonic channel $\mathcal{E}_{A\to BW}^{(\eta,\bar{n}_{\mathrm{B}})}$ being memoryless. Alice and Bob have access to a bipartite resource state $\hat{\rho}^{S^mR^m}$ occupying m systems S at Alice and R at Bob. Correlations between parts of $\hat{\rho}^{S^mR^m}$ in systems S and R can either be classical or quantum, resulting in either a classical-quantum or an entangled state $\hat{\rho}^{S^mR^m}$. The latter allows entanglement-assisted communication.

C. Coding and reliability

Alice desires to transmit one of 2^M equally-likely M-bit messages $x \in \{1, \ldots, 2^M\}$ covertly to Bob using n available modes of the bosonic channel $\mathcal{E}_{A\to BW}^{(\eta,\bar{n}_{\mathrm{B}})}$ and her share of the resource state $\hat{\rho}^{S^mR^m}$. Her encoder is a set of encoding channels $\left\{\mathcal{M}_{S^m\to A^n}^{(x)}\right\}$. Alice encodes message x by acting on m systems S of $\hat{\rho}^{S^mR^m}$ with $\mathcal{M}_{S^m\to A^n}^{(x)}$, transforming $\hat{\rho}^{S^mR^m}$ to $\hat{\rho}_x^{A^nR^m} = \mathcal{M}_{S^m\to A^n}^{(x)}(\hat{\rho}^{S^mR^m})$. Transmission of the resulting n systems A over n uses of $\mathcal{E}_{A\to BW}^{(\eta,\bar{n}_{\mathrm{B}})}$ results in Bob receiving the state $\hat{\rho}_x^{B^nR^m} = \mathrm{Tr}_{W^n}\left[\left[\mathcal{E}_{A\to BW}^{(\eta,\bar{n}_{\mathrm{B}})}\right]^{\otimes n}\left(\mathcal{M}_{S^m\to A^n}^{(x)}(\hat{\rho}^{S^mR^m})\right)\right]$, where $\hat{\rho}^A = \mathrm{Tr}_B\left[\hat{\rho}^{AB}\right]$ denotes the partial trace over system B. Bob decodes x by applying a positive operator-valued measure (POVM) $\left\{\Lambda_{B^nR^m}^{(x)}\right\}$ to $\hat{\rho}_x^{B^nR^m}$. Denoting by X and $\check{X}$ the respective random variables corresponding to Alice's message and Bob's estimate of it, the average decoding error probability is:

$$P_{\mathrm{e}} = \frac{1}{2^M}\sum_{x=1}^{2^M} P(\check{X} \neq x | X = x), \tag{1}$$

where $P(\check{X} \neq x|X = x) = \mathrm{Tr}\left[\left(\hat{I} - \Lambda_{B^nR^m}^{(x)}\right)\hat{\rho}_x^{B^nR^m}\right]$. We call the communication system *reliable* if, for any $\epsilon \in (0,1)$, there exists n large enough with a corresponding resource state $\hat{\rho}^{S^mR^m}$, encoder $\left\{\mathcal{M}_{S^m\to A^n}^{(x)}\right\}$, and decoder POVM $\left\{\Lambda_{B^nR^m}^{(x)}\right\}$, such that $P_{\mathrm{e}} \leq \epsilon$.

[1] We denote by $f(n) = O(g(n))$ an asymptotic upper bound on $f(n)$ (i.e. there exist constants $m, n_0 > 0$ such that $0 \leq f(n) \leq mg(n)$ for all $n \geq n_0$) and by $f(n) = o(g(n))$ an upper bound on $f(n)$ that is not asymptotically tight (i.e. for any constant $m > 0$, there exists constant $n_0 > 0$ such that $0 \leq f(n) < mg(n)$ for all $n \geq n_0$) [12, Ch. 3.1].

[2] Our fundamental information unit is a bit and $\log x$ indicates the binary logarithm, while $\ln x$ is the natural logarithm.

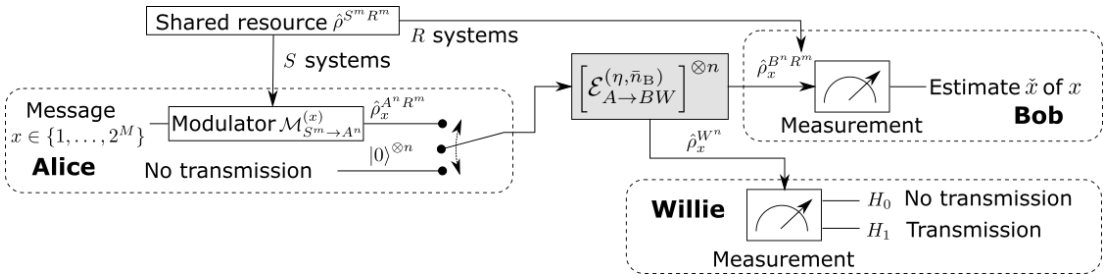

Fig. 2. Covert communication over the bosonic channel. Alice has a bosonic channel, depicted in Fig. 1, to receiver Bob and adversary Willie. Alice and Bob share a bipartite resource state $\hat{\rho}^{S^m R^m}$ that is inaccessible by Willie and may or may not be entangled. Alice uses her share of $\hat{\rho}^{S^m R^m}$ in S systems to encode message x with blocklength n code, and chooses whether to transmit it using $\mathcal{E}^{(\eta,\bar{n}_B)}_{A\to BW}$ n times. Willie observes his channel from Alice to determine whether she is quiet (null hypothesis H_0) or not (alternate hypothesis H_1). A covert communication system must ensure that any detector Willie uses is close to ineffective (i.e., a random guess between the hypotheses), while allowing Bob to reliably decode the message (if one is transmitted).

D. Quantum-secure covertness

As is standard in information theory of covert communication, we assume that Willie cannot access $\hat{\rho}^{S^m R^m}$, although he knows how it is generated. To be *quantum secure*, a covert communication system has to prevent the detection of Alice's transmission by Willie, who has access to all transmitted photons that are not received by Bob and arbitrary quantum resources. Thus, the quantum state $\hat{\rho}_1^{W^n} = \sum_{x=1}^{2^M} \frac{1}{2^M} \mathrm{Tr}_{B^n R^m} \left[\left[\mathcal{E}^{(\eta,\bar{n}_B)}_{A\to BW}\right]^{\otimes n} \left(\mathcal{M}^{(x)}_{S^m \to A^n}(\hat{\rho}^{S^m R^m})\right)\right]$, observed by Willie when Alice is transmitting, has to be sufficiently similar to the product thermal state $\hat{\rho}^{\otimes n}_{\eta\bar{n}_B}$ that describes the noise observed when she is not. We call a system *covert* if, for any $\delta > 0$ and n large enough, $D\left(\hat{\rho}_1^{W^n} \| \hat{\rho}^{\otimes n}_{\eta\bar{n}_B}\right) \leq \frac{\delta}{\log e}$. Arbitrarily small $\delta > 0$ implies that the performance of a quantum-optimal detection scheme is arbitrarily close to that of a random coin flip through quantum Pinsker's inequality [15, Th. 10.8.1]. The properties of both classical and quantum relative entropy are highly attractive for mathematical proofs, and were used to analyze covert communication [2]–[10]. We discuss the significance of the quantum relative entropy in [6, Sec. II.B]. The maximum mean photon number per mode $\bar{n}_S$ that Alice can transmit under the covertness constraint is [6]:

$$\bar{n}_S = \frac{\sqrt{\delta} c_{\mathrm{cov}}}{\sqrt{n}}, \tag{2}$$

where $c_{\mathrm{cov}} = \frac{\sqrt{2\eta\bar{n}_B(1+\eta\bar{n}_B)}}{1-\eta}$. When the exact values for the environment mean photon number per mode $\bar{n}_B$ and the transmissivity η are unknown, Planck's law [16] and the diffraction-limited propagation model [17] provide a useful lower bound. Coherent-state modulation using the continuous-valued complex Gaussian distribution [5, Th. 2] and practical QPSK scheme [6, Th. 2] achieve (2).

While quantum resources, such as entanglement shared between Alice and Bob, or quantum states lacking a semi-classical description (e.g., squeezed light) do not improve signal covertness, the quantum methodology allows covertness without assumptions of adversary's limits, other than the laws of physics. However, the square root scaling in (2) holds even when Willie uses readily-available devices such as noisy photon counters [5, Th. 5], with a constant larger than c_{cov}. Nevertheless, here we show that quantum resources—specifically, entanglement assistance—allow the transmission of significantly more covert bits. Next, we discuss the finite blocklength capacity bounds that we use in our proofs.

E. Finite blocklength capacity bounds for bosonic channels

One can obtain the converses for covert communication using the standard channel coding theorems. However, covertness introduces the dependence of the mean photon number per mode $\bar{n}_S$ on the blocklength n in (2). This complicates both classical and quantum achievability proofs by rendering invalid the conditions for employing standard results such as the asymptotic equipartition property. We use a lower bound on the second-order coding rate for infinite-dimensional states that is based on the new quantum union bound [18].

Define quantum relative entropy $D(\hat{\rho}\|\hat{\sigma})$ between states $\hat{\rho}$ and $\hat{\sigma}$, and its second and fourth central moments as follows:

$$D(\hat{\rho}\|\hat{\sigma}) = \mathrm{Tr}\left[\hat{\rho}\log\hat{\rho} - \hat{\rho}\log\hat{\sigma}\right] \tag{3}$$

$$V(\hat{\rho}\|\hat{\sigma}) = \mathrm{Tr}\left[\hat{\rho}\left|\log\hat{\rho} - \log\hat{\sigma} - D(\hat{\rho}\|\hat{\sigma})\right|^2\right] \tag{4}$$

$$Q(\hat{\rho}\|\hat{\sigma}) = \mathrm{Tr}\left[\hat{\rho}\left|\log\hat{\rho} - \log\hat{\sigma} - D(\hat{\rho}\|\hat{\sigma})\right|^4\right], \tag{5}$$

where $V(\hat{\rho}\|\hat{\sigma})$ is quantum relative entropy variance. The finite blocklength capacity of a memoryless classical-quantum channel described in Sec. II-B is characterized as follows:

Lemma 1: Suppose that the channel from Alice to Bob is memoryless, such that over n uses $\mathcal{N}_{A^n\to B^n} = (\mathcal{N}_{A\to B})^{\otimes n}$. There exists a coding scheme that employs a shared resource state $\rho^{S^m R^m}$ to transmit M bits over n uses of $\mathcal{N}_{A\to B}$ with arbitrary decoding error probability ϵ for a sufficiently large n and m, such that:

$$M \geq nD\left(\hat{\rho}^{BR}\middle\|\hat{\rho}^B\otimes\hat{\rho}^R\right) + \sqrt{nV\left(\hat{\rho}^{BR}\middle\|\hat{\rho}^B\otimes\hat{\rho}^R\right)}\Phi^{-1}(\epsilon) - C_n,$$

where $C_n = \frac{C_{B\text{-}E}}{\sqrt{2\pi}}\frac{\left[Q(\hat{\rho}^{BR}\|\hat{\rho}^B\otimes\hat{\rho}^R)\right]^{3/4}}{V\left(\hat{\rho}^{BR}\|\hat{\rho}^B\otimes\hat{\rho}^R\right)} + \frac{\sqrt{V\left(\hat{\rho}^{BR}\|\hat{\rho}^B\otimes\hat{\rho}^R\right)}}{\sqrt{2\pi}} + \log(4\epsilon n)$, *$C_{B\text{-}E}$ is the Berry-Esseen constant satisfying* $0.40973 \leq C_{B\text{-}E} \leq 0.4784$, *$\hat{\rho}^{BR}$ is Bob's marginal state for the output of a single channel use, and $\Phi^{-1}(x)$ is the inverse-Gaussian distribution function.*

The proof of Lemma 1 in [1] adapts [18]. In contrast to [18], we do not absorb the remainder terms of C_n in asymptotic

notation. This is to capture the dependence of $\bar{n}_S$ on n imposed by the covertness constraint (2).

III. Results

A. Covert channel capacity

In information theory, the channel capacity $C = \liminf_{n\to\infty} \frac{M}{n}$ is measured in bits per channel use, where M is the total number of reliably-transmissible bits in n channel uses. On the other hand, the power constraint (2) imposed by covert communication implies that $M = o(n)$ and that the capacity of the covert channel is zero. Inspired by [8], we regularize the number of covert bits that are transmitted reliably without entanglement assistance by $\sqrt{n}$ and with entanglement assistance $\sqrt{n}\log n$, instead of n. This approach allows us to state Definitions 1 and 2 of covert channel capacity and derive the results that follow. As in [8], we also normalize the capacity by the covertness parameter δ.

B. Covert communication without entanglement assistance

We define the capacity of covert communication over the bosonic channel when Alice and Bob do not have access to a shared entanglement source as follows:

Definition 1. *The capacity of covert communication without entanglement assistance is:*

$$L_{\text{no-EA}} \triangleq \liminf_{n\to\infty} \frac{M_{\text{no-EA}}}{\sqrt{\delta n}}, \tag{6}$$

where $M_{\text{no-EA}}$ is the number of covert bits that are reliably transmissible in n channel uses (modes), and δ parametrizes the desired covertness.

The following theorem provides the expression for $L_{\text{no-EA}}$:

Theorem 1. *The covert capacity of the bosonic channel without entanglement assistance is $L_{\text{no-EA}} = c_{\text{cov}} c_{\text{rel,no-EA}}$, where c_{cov} is defined below* (2) *and $c_{\text{rel,no-EA}} = \eta \log\left(1 + \frac{1}{(1-\eta)\bar{n}_B}\right)$.*

In order to prove Theorem 1, we prove the following lemma:

Lemma 2: There exists a sequence of codes with covertness parameter δ, blocklength n, size 2^M, average error probability ϵ, and $K_{\text{no-EA}} = \sqrt{c_{\text{cov}}\sqrt{\delta}(1+2(1-\eta)\bar{n}_B)c_{\text{rel,no-EA}}}$ such that:

$$M_{\text{no-EA}} \geq L_{\text{no-EA}}\sqrt{\delta n} + K_{\text{no-EA}}\Phi^{-1}(\epsilon)n^{1/4} + O\left(n^{1/8}\right). \tag{7}$$

Proof sketch (full proof in [1]): We use a position-based code [18] constructed from a coherent-state QPSK alphabet, and apply Lemma 1. Since the closed-form expressions for $D\left(\hat{\rho}^{BR}\middle\|\hat{\rho}^B\otimes\hat{\rho}^R\right)$ and $V\left(\hat{\rho}^{BR}\middle\|\hat{\rho}^B\otimes\hat{\rho}^R\right)$ are unknown, we obtain $L_{\text{no-EA}}$ and $K_{\text{no-EA}}$ from their Taylor series expansions at $\bar{n}_S = 0$. We then show that $Q\left(\hat{\rho}^{BR}\middle\|\hat{\rho}^B\otimes\hat{\rho}^R\right) = O(\bar{n}_S)$, substitute $\bar{n}_S$ from (2), and observe that $\frac{\left[Q(\hat{\rho}^{BR}\|\hat{\rho}^B\otimes\hat{\rho}^R)\right]^{3/4}}{V\left(\hat{\rho}^{BR}\middle\|\hat{\rho}^B\otimes\hat{\rho}^R\right)} = O\left(n^{1/8}\right)$ dominates the remainder C_n in Lemma 1. ∎

Proof sketch for Theorem 1 (full proof in [1]): Dividing both sides of (7) by $\sqrt{n\delta}$ and taking the limit yields the achievability. The converse uses standard arguments involving Fano's inequality and the Holevo bound [19, Th. 12.1], [20]. The latter upper-bounds the mutual information between random variables $X^{(n)}$ and $\check{X}^{(n)}$ corresponding to Alice's message and Bob's decoding of it by the Holevo capacity $C_\chi(\bar{n}_S;\eta,\bar{n}_B) = g(\eta\bar{n}_S + (1-\eta)\bar{n}_B) - g((1-\eta)\bar{n}_B)$ of the bosonic channel from Alice to Bob $\mathcal{E}_{A\to B}^{(\eta,\bar{n}_B)}$ [21] with

$$g(x) \equiv (1+x)\log(1+x) - x\log x. \tag{8}$$

Expanding the Taylor series of $C_\chi(\bar{n}_S;\eta,\bar{n}_B)$ around $\bar{n}_S = 0$, dividing by $\sqrt{n\delta}$, and taking the limit completes the proof. ∎

C. Entanglement-assisted covert communication

Entanglement assistance increases the communication channel capacity [22], [23]. However, in most practical settings (including optical communication where noise level is low $\bar{n}_B \ll 1$ and microwave/RF communication where signal power is high $\bar{n}_S \gg 1$), the gain over the Holevo capacity without entanglement assistance is at most a factor of two. The only scenario with a significant gain is when $\bar{n}_S \to 0$ while $\bar{n}_B > 0$ [24, App. A]. This is precisely the covert communication setting. In fact, entanglement assistance alters the fundamental square root scaling law for covert communication, changing the normalization from $\sqrt{n}$ to $\sqrt{n}\log n$:

Definition 2. *The capacity of covert communication with entanglement assistance is:*

$$L_{\text{EA}} \triangleq \liminf_{n\to\infty} \frac{M_{\text{EA}}}{\sqrt{\delta n}\log n}, \tag{9}$$

where M_{EA} is the number of covert bits that are reliably transmissible in n channel uses (modes), and δ parametrizes the desired covertness.

The following theorem provides the expression for L_{EA}:

Theorem 2. *The covert capacity of the bosonic channel with entanglement assistance is $L_{\text{EA}} = c_{\text{cov}} c_{\text{rel,EA}}$, where c_{cov} is defined below* (2) *and $c_{\text{rel,EA}} = \frac{\eta}{2(1+(1-\eta)\bar{n}_B)}$.*

Thus, while quantum resources such as shared entanglement and joint detection receivers do not affect $\bar{n}_S$, they dramatically impact the amount of information that can be covertly conveyed. As in the proof of Theorem 1, in order to prove Theorem 2, we prove the following lemma:

Lemma 3: There exists a sequence of codes with covertness parameter δ, blocklength n, size 2^M, average error probability ϵ, and $K_{\text{EA}} = \sqrt{c_{\text{cov}}\sqrt{\delta}c_{\text{rel,EA}}}$ such that:

$$M_{\text{EA}} \geq L_{\text{EA}}\sqrt{\delta n}\log n + K_{\text{EA}}\Phi^{-1}(\epsilon)n^{1/4}\log n + O\left(n^{1/8}\log n\right). \tag{10}$$

Proof sketch (full proof in [1]): We follow the steps in the proof of Lemma 2, however, here we construct the code from two-mode squeezed vacuum (TMSV) states. To obtain the constants in (10), we expand $D\left(\hat{\rho}^{BR}\middle\|\hat{\rho}^B\otimes\hat{\rho}^R\right)$ and $V\left(\hat{\rho}^{BR}\middle\|\hat{\rho}^B\otimes\hat{\rho}^R\right)$ around $\bar{n}_S = 0$. We employ the

symplectic matrix formalism to derive the expression for $V\left(\hat{\rho}^{BR}\middle\|\hat{\rho}^{B}\otimes\hat{\rho}^{R}\right)$ [1, Appendix II-B] and use [23]:

$$D\left(\hat{\rho}^{BR}\middle\|\hat{\rho}^{B}\otimes\hat{\rho}^{R}\right) = g(\bar{n}_{\mathrm{S}}) + g(\eta\bar{n}_{\mathrm{S}} + (1-\eta)\bar{n}_{\mathrm{B}}) - g(A_{+}) - g(A_{-}), \quad (11)$$

with $g(x)$ defined in (8), $A_{\pm} = \frac{B-1\pm(1-\eta)(\bar{n}_{\mathrm{B}}-\bar{n}_{\mathrm{S}})}{2}$, and $B = \sqrt{(\bar{n}_{\mathrm{S}}+1+\eta\bar{n}_{\mathrm{S}}+(1-\eta)\bar{n}_{\mathrm{B}})^2 - 4\eta\bar{n}_{\mathrm{S}}(\bar{n}_{\mathrm{S}}+1)}$. ■

Proof sketch for Theorem 2 (full proof in [1]): Proof follows that of Theorem 1 with $D\left(\hat{\rho}^{BR}\middle\|\hat{\rho}^{B}\otimes\hat{\rho}^{R}\right)$ in (11). ■

D. Impact of noise on the resource state

Consider entanglement-assisted communication where R systems are not preserved perfectly. Let the TMSV idler modes retained by Bob be degraded by the lossy thermal-noise bosonic channel $\mathcal{E}_{R\to R'}^{(\eta_{\mathrm{i}},\bar{n}_{\mathrm{B_i}})}$ modeling storage in an optical delay loop. Lemma 1 still governs the finite blocklength capacity:

$$D\left(\hat{\rho}^{BR'}\middle\|\hat{\rho}^{B}\otimes\hat{\rho}^{R'}\right) = g(\eta_{\mathrm{i}}\bar{n}_{\mathrm{S}} + (1-\eta_{\mathrm{i}})\bar{n}_{\mathrm{B_i}}) - g\left(A'_{+}\right) + g(\eta\bar{n}_{\mathrm{S}} + (1-\eta)\bar{n}_{\mathrm{B}}) - g\left(A'_{-}\right), \quad (12)$$

where $A'_{\pm} = \frac{B'-1\pm((1-\eta)(\bar{n}_{\mathrm{B}}-\bar{n}_{\mathrm{S}})-(1-\eta_{\mathrm{i}})(\bar{n}_{\mathrm{B_i}}-\bar{n}_{\mathrm{S}}))}{2}$ and $B' = \sqrt{(1+(1-\eta)\bar{n}_{\mathrm{B}}+(1-\eta_{\mathrm{i}})\bar{n}_{\mathrm{B_i}}+(\eta+\eta_{\mathrm{i}})\bar{n}_{\mathrm{B}})^2 - 4\eta\eta_{\mathrm{i}}\bar{n}_{\mathrm{S}}(1+\bar{n}_{\mathrm{S}})}$. By inspection, $\eta_{\mathrm{i}} < 1$ with $\bar{n}_{\mathrm{B_i}} = 0$ only reduces L_{EA}. However, for $\bar{n}_{\mathrm{B_i}} > 0$, the Taylor series expansion of (12) around $\bar{n}_{\mathrm{S}} = 0$ yields $D\left(\hat{\rho}^{BR'}\middle\|\hat{\rho}^{B}\otimes\hat{\rho}^{R'}\right) = \bar{n}_{\mathrm{S}}c_{\mathrm{rel,noisyEA}} + O(\bar{n}_{\mathrm{S}}^2)$ where

$$c_{\mathrm{rel,noisyEA}} = \frac{\eta\eta_{\mathrm{i}}\left(\log\left(1+\frac{1}{(1-\eta)\bar{n}_{\mathrm{B}}}\right)+\log\left(1+\frac{1}{(1-\eta_{\mathrm{i}})\bar{n}_{\mathrm{B_i}}}\right)\right)}{1+(1-\eta)\bar{n}_{\mathrm{B}}+(1-\eta_{\mathrm{i}})\bar{n}_{\mathrm{B_i}}}. \quad (13)$$

Adapting [1, Appendix II-B] we get $V\left(\hat{\rho}^{BR'}\middle\|\hat{\rho}^{B}\otimes\hat{\rho}^{R'}\right) = O(\bar{n}_{\mathrm{S}})$. Substituting $\bar{n}_{\mathrm{S}}$ from (2) yields the number of covert bits reliably transmissible in n modes:

$$M_{\mathrm{noisyEA}} \geq c_{\mathrm{cov}}c_{\mathrm{rel,noisyEA}}\sqrt{\delta n} - O(n^{1/4}). \quad (14)$$

This demonstrates the fragility of entanglement-assisted communication: even though the constant $c_{\mathrm{rel,noisyEA}}$ can be large for η_{i} and $\bar{n}_{\mathrm{B_i}}$ small, the $\log n$ scaling gain is lost. Optimization over Gaussian input states and application of the Holevo-Werner theorem [25] is a promising path to show an upper bound matching (14); this work is ongoing.

IV. Conclusion

We derived the quantum-secure covert capacity for the bosonic channel with and without entanglement assistance, closing an important gap from [6]. Surprisingly, entanglement assistance alters the fundamental scaling law for covert communication from $O(\sqrt{n})$ to $O(\sqrt{n}\log n)$ covert bits reliably transmissible in n channel uses. However, noise eliminates this gain in our achievability proof. In the follow-on work, we will address the matching converse as well as the shared resource state size, the entanglement-assisted receiver design [24] for covert communication, and the possible relationship of the scaling law for entanglement-assisted covert communication to a corner case in classical and non-entanglement assisted classical-quantum covert communication.

References

[1] C. N. Gagatsos, M. S. Bullock, and B. A. Bash, "Covert capacity of bosonic channels," *IEEE J. Sel. Areas Inf. Theory*, vol. 1, pp. 555–567, 2020.

[2] B. A. Bash, D. Goeckel, and D. Towsley, "Square root law for communication with low probability of detection on AWGN channels," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Cambridge, MA, Jul. 2012.

[3] ——, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Select. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, 2013.

[4] B. A. Bash, D. Goeckel, S. Guha, and D. Towsley, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Commun. Mag.*, vol. 53, no. 12, 2015.

[5] B. A. Bash, A. H. Gheorghe, M. Patel, J. L. Habif, D. Goeckel, D. Towsley, and S. Guha, "Quantum-secure covert communication on bosonic channels," *Nat. Commun.*, vol. 6, Oct. 2015.

[6] M. S. Bullock, C. N. Gagatsos, S. Guha, and B. A. Bash, "Fundamental limits of quantum-secure covert communication over bosonic channels," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 471–482, Mar. 2020.

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

[8] 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.

[9] A. Sheikholeslami, B. A. Bash, D. Towsley, D. Goeckel, and S. Guha, "Covert communication over classical-quantum channels," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Barcelona, Spain, Jul. 2016, arXiv:1601.06826 [quant-ph].

[10] L. Wang, "Optimal throughput for covert communication over a classical-quantum channel," in *Proc. Inform. Theory Workshop (ITW)*, Cambridge, UK, Sep. 2016, pp. 364–368, arXiv:1603.05823 [cs.IT].

[11] M. Tahmasbi and M. R. Bloch, "Framework for covert and secret key expansion over classical-quantum channels," *Phys. Rev. A*, vol. 99, p. 052329, May 2019.

[12] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, 2nd ed. Cambridge, Massachusetts: MIT Press, 2001.

[13] 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.

[14] M. Orszag, *Quantum Optics*, 3rd ed. Berlin, Germany: Springer, 2016.

[15] M. Wilde, *Quantum Information Theory*, 2nd ed. Cambridge University Press, 2016, arXiv:1106.1445v7.

[16] N. Kopeika and J. Bordogna, "Background noise in optical communication systems," *Proc. of the IEEE*, vol. 58, no. 10, pp. 1571–1577, Oct. 1970.

[17] J. H. Shapiro, S. Guha, and B. I. Erkmen, "Ultimate channel capacity of free-space optical communications," *IEEE J. Opt. Netw.*, vol. 4, no. 8, pp. 501–516, Aug. 2005.

[18] S. K. Oskouei, S. Mancini, and M. M. Wilde, "Union bound for quantum information processing," *Proc. Roy. Soc. A*, vol. 475, no. 2221, p. 20180612, 2019.

[19] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. New York, NY, USA: Cambridge University Press, 2000.

[20] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," *Problems Inf. Transmiss.*, vol. 9, pp. 177–183, 1973.

[21] V. Giovannetti, R. García-Patrón, N. Cerf, and A. Holevo, "Ultimate classical communication rates of quantum optical channels," *Nat. Photon.*, vol. 8, no. 10, pp. 796–800, 2014.

[22] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse shannon theorem," *IEEE Trans. Inform. Theory*, vol. 48, no. 10, pp. 2637–2655, Oct. 2002.

[23] V. Giovannetti, S. Lloyd, L. Maccone, and P. W. Shor, "Broadband channel capacities," *Phys. Rev. A*, vol. 68, p. 062323, Dec. 2003.

[24] S. Guha, Q. Zhuang, and B. A. Bash, "Infinite-fold enhancement in communications capacity using pre-shared entanglement," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Jun. 2020, arXiv:2001.03934 [quant-ph].

[25] A. S. Holevo and R. F. Werner, "Evaluating capacities of bosonic gaussian channels," *Phys. Rev. A*, vol. 63, p. 032312, Feb 2001.