Square Root Law for Covert Quantum Communication over Optical Channels

Evan J. D. Anderson
Wyant College of Optical Sciences
University of Arizona
Tucson, AZ, USA
ejdanderson@arizona.edu

Christopher K. Eyre
Dept. of Mathematics
Brigham Young University
Provo, UT, USA

Isabel M. Dailey
Dept. of Electrical and Computer Engineering
College of Engineering
University of Arizona
Tucson, AZ, USA

Filip Rozpędek
College of Information & Computer Sciences
University of Massachusetts Amherst
Amherst, MA, USA

Boulat A. Bash
Dept. of Electrical and Computer Engineering
College of Engineering
Wyant College of Optical Sciences
University of Arizona
Tucson, AZ, USA

***Abstract*—We explore covert communication of qubits over the lossy thermal-noise bosonic channel, which is a quantum-mechanical model of many practical channels, including optical. Covert communication ensures that an adversary is unable to detect the presence of transmissions, which are concealed in channel noise. We show a *square root law* (SRL) for quantum covert communication similar to that for classical: $\propto \sqrt{n}$ qubits can be transmitted covertly and reliably over n uses of an optical channel. Our achievability proof uses photonic dual-rail qubit encoding, which has been proposed for long-range repeater-based quantum communication and entanglement distribution. Our converse employs prior covert signal power limit results and adapts well-known methods to upper bound quantum capacity of optical channels. Finally, we believe that the gap between our lower and upper bounds for the number of reliable covert qubits can be mitigated by improving the quantum error correction codes and quantum channel capacity bounds.**

***Index Terms*—covert quantum communication, quantum communication, bosonic quantum channel**

I. Introduction

Covert, or low probability of detection/intercept (LPD/LPI) communication renders adversaries unaware of the presence of transmission between two or more parties. The last decade saw much exploration of the fundamental limits of covert communication over classical channels, with [1]–[4] leading to many follow-on works. However, the physics which underpins these channels is quantum. This motivated recent work on covert classical-quantum channels [5]–[9]. For all these channels, covert communication is fundamentally governed by the *square root law* (SRL) which limits communication that is both covert and reliable to $\propto \sqrt{n}$ bits over n channel uses. In this paper, we extend these results to quantum covert communication over lossy thermal-noise bosonic channels. Such channels model optical fiber, and free space communication in the optical, microwave, and radio-frequency regimes. Here, we study the achievability of quantum covert communication over such a channel utilizing dual-rail photonic qubits, as well as the converse using well-known upper bounds on the quantum capacity of a lossy thermal-noise bosonic channel.

Dual-rail qubits apply to many quantum information processing tasks. They are used in cluster-state generation [10], which, e.g., can enable one-way quantum computing. Additionally, the dual-rail encoding is convenient for entanglement distribution in quantum networks. Indeed, it was used to demonstrate a loophole-free Bell inequality violation [11], and to entangle trapped-ion qubits spatially separated by 230 m [12]. Furthermore, dual-rail qubits have been proposed to transmit quantum information over long-range repeater-based quantum networks [13]–[16]. The dual-rail encoding is also commonly used in quantum key distribution (QKD) [17], [18].

Covert quantum communication has been previously explored in the context of QKD [19]–[22]. Here, however, we take a direct approach and use dual-rail encoding to address quantum covert communication over the lossy thermal-noise bosonic channel. Specifically, we adapt the analysis from covert classical-quantum channels [5]–[9]. We believe that this approach extends naturally to other quantum encodings and channels. Analogous to the $\sqrt{n}$ scaling for bits in the classical-classical and classical-quantum channels, we find achievability of the SRL, where one can transmit reliably at least $\propto \sqrt{n}$ covert qubits with the dual-rail encoding over n uses of a lossy thermal-noise bosonic channel.

In the converse, we use the upper bound on the number of photons per mode that is covertly transmissible over a lossy thermal-noise bosonic channel [6]. Adapting the upper bound on the energy-constrained quantum capacity of lossy thermal-noise bosonic channel [23] shows that at most $\propto \sqrt{n}$ covert qubits can be reliably sent over n uses of this channel, matching the achievable lower bound scaling. However, the

This work was supported by the National Science Foundation under Grants No. CCF-2006679 and EEC-1941583.

gap between the achievability and the converse remains open.

The rest of this paper is organized as follows: in Section II we provide the mathematical preliminaries as well as the system and channel models. In Section III we describe the mathematical formalism underpinning covert communication and provide our results. Finally, we wrap up in Section IV with a discussion of our results and future research.

II. Preliminaries

A. Dual-rail Qubits

The dual-rail qubit is a well-known encoding of qubits into single photons in linear-optical quantum computing [24] and quantum communication [13]. With dual-rail encoding, a qubit is represented by the presence of a single photon in one of two optical modes. The logical states are physically represented using two-mode Fock (photon number) states: $|0\rangle_L = |01\rangle$ and $|1\rangle_L = |10\rangle$. The general logical qubit state $|\psi\rangle$ is then a superposition of the two states:

$$|\psi\rangle = \alpha|0\rangle_L + \beta|1\rangle_L = \alpha|01\rangle + \beta|10\rangle \tag{1}$$

and $\hat{\rho}_{\alpha,\beta} = |\psi\rangle\langle\psi|$ is the state's density operator with $\alpha, \beta \in \mathbb{C}$ normalized such that $|\alpha|^2 + |\beta|^2 = 1$.

We call our fundamental transmission unit a *round*. We transmit one qubit per round, occupying two optical modes.

B. System and Channel Model

Alice employs blocks of n two-mode rounds to encode each covert quantum message $|m\rangle$ using dual-rail qubits described in Section II-A and vacuum states $|00\rangle\langle 00|$. Thus, she employs a total of $2n$ optical modes. Utilizing the pre-shared classical secret as described in Section III, she either sends a dual-rail qubit or vacuum $|00\rangle\langle 00|$ through the lossy thermal-noise bosonic channel, as detailed in Fig. 1. The channel acts on each optical mode independently. Bob attempts to decode his received state utilizing the shared secret to obtain an estimate $|\check{m}\rangle$ of the message, while the adversary warden Willie tries to detect Alice's transmission.

Consider a channel, $\mathcal{E}_{A\to BW}^{(\eta,\bar{n}_{\mathrm{B}})}$, in Fig. 1 that is described by a beamsplitter with transmittance $\eta \in [0, 1]$, two input modes (Alice and the environment), and two output modes (Bob and Willie). These modes are labeled by their modal annihilation operators $\hat{a}, \hat{e}, \hat{b}$, and $\hat{w}$ respectively. Their input-output modal relationships are:

$$\hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{e} \quad \text{and} \quad \hat{w} = \sqrt{1-\eta}\hat{a} - \sqrt{\eta}\hat{e}. \tag{2}$$

For the *lossy thermal-noise bosonic channel*, the input state of mode $\hat{e}$ is $\hat{\rho}_{\bar{n}_{\mathrm{B}}}$, a zero-mean thermal state with mean photon number $\bar{n}_{\mathrm{B}}$ expressed by the following sum over the diagonal elements in the Fock (photon number) basis $|k\rangle$:

$$\hat{\rho}_{\bar{n}_{\mathrm{B}}} \equiv \sum_{k=0}^{\infty} t_k(\bar{n}_{\mathrm{B}})|k\rangle\langle k|, \text{ where } t_k(\bar{n}_{\mathrm{B}}) = \frac{\bar{n}_{\mathrm{B}}^k}{(1+\bar{n}_{\mathrm{B}})^{k+1}}. \tag{3}$$

A *pure-loss* bosonic channel has $\bar{n}_{\mathrm{B}} = 0$ and mixes the input with vacuum rather than thermal noise. Finally, we note that the lossy thermal-noise bosonic channel belongs to a well-studied class of bosonic Gaussian channels [26].

C. Entanglement-Breaking Channel

An entanglement-breaking channel breaks entanglement between input quantum states at the channel's output. Entanglement is broken in a lossy thermal-noise bosonic channel if $\bar{n} > \kappa$ where $\bar{n} > 0$ is the mean photon number of the thermal noise added by the channel and κ is the fraction of the input photon number at the output [27]. In the following analysis, we assume that the Alice-to-Willie channel is naturally entanglement breaking, corresponding to $\eta\bar{n}_{\mathrm{B}} > 1 - \eta$, as is typical in optical communication systems. It is unknown whether the channel to the adversary must be entanglement breaking for covert quantum communication, and is a subject of ongoing investigation. However, if the physical channel does not break entanglement, Alice may introduce additional loss or noise after encoding to ensure entanglement is broken, per the following two lemmas:

Lemma 1: Entanglement is broken in the Alice-to-Willie channel by passing Alice's signal through a pure-loss channel with transmittance $\tau < \frac{\eta}{1-\eta}\bar{n}_{\mathrm{B}}$ prior to transmission, meeting the entanglement-breaking condition $\eta\bar{n}_{\mathrm{B}} > \tau(1-\eta)$.

Lemma 2: Entanglement is broken in the Alice-to-Willie channel by passing Alice's signal through a quantum-limited amplifier with gain coefficient $G_{\mathrm{eb}} = 2(1-\eta)/(2(1-\eta) - \eta\bar{n}'_{\mathrm{B}})$ and $\bar{n}'_{\mathrm{B}} > \frac{\eta}{1-\eta} - \bar{n}_{\mathrm{B}}$, followed by a pure loss channel with transmittance $\tau = 1/G_{\mathrm{eb}}$. This meets the entanglement-breaking condition $\eta(\bar{n}_{\mathrm{B}} + \bar{n}'_{\mathrm{B}}) > (1-\eta)$.

Proofs of both lemmas are in [28, Appendix A]. Enforcing the entanglement-breaking condition via either lemma reduces the number of qubits transmitted reliably and covertly without affecting the achievable SRL scaling. In Lemma 1 attenuation of Alice's signal breaks entanglement, while in Lemma 2 additional noise is used. Intuitively, Lemma 1 holds because a lossy thermal-noise bosonic channel decomposes into a pure-loss channel followed by a quantum-limited amplifier [29]–[31]. We combine the pure-loss component with Alice's additional pure-loss channel. The resulting transmittance is the fraction of Alice's input photon number delivered to Willie, while the amplifier gain determines the thermal noise added by the channel. Proof of Lemma 2 is not as intuitive.

III. Covert Communication

A. Covertness Analysis

Denote $\hat{\rho}_0^{W^n}$ and $\hat{\rho}_1^{W^n}$ as the respective states Willie observes when Alice is quiet or transmitting. Since two-mode vacuum $|00\rangle\langle 00|$ is input when Alice is quiet, $\hat{\rho}_0^{W^n} = \left(\hat{\rho}_0^W\right)^{\otimes n}$, where $\hat{\rho}_0^W = \hat{\rho}_{\eta\bar{n}_{\mathrm{B}}} \otimes \hat{\rho}_{\eta\bar{n}_{\mathrm{B}}}$ is a two-mode thermal product state [26]. Willie desires to determine if Alice and Bob are communicating; ergo, in n rounds (uses of the two-mode bosonic channel), he tries to distinguish between $\hat{\rho}_1^{W^n}$ and $\left(\hat{\rho}_0^W\right)^{\otimes n}$. The null and alternate hypotheses H_0 and H_1 correspond to Alice being quiet and transmitting, respectively. Willie collects all the photons that do not reach Bob, as shown in Fig. 1.

Willie can make two types of errors: a false alarm, where he decides that Alice is transmitting when she is not (choosing

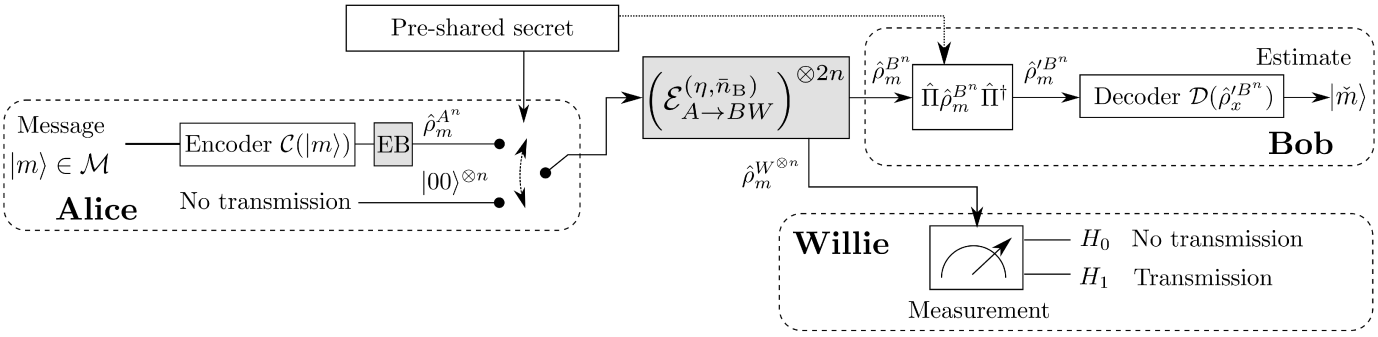

Fig. 1. Covert quantum communication over the lossy thermal-noise bosonic channel $\mathcal{E}_{A\to BW}^{(\eta,\bar{n}_B)}$. Alice and Bob employ a random coding scheme from [25, Secs. 23.3 and 24.4]. Transmission occurs with probability q in each of the n two-mode rounds. The rounds chosen for transmission constitute a pre-shared classical secret unknown to Willie. Alice chooses a quantum message $|m\rangle \in \mathcal{M}$. Alice employs additional noise or loss before transmitting to ensure that her channel to Willie is entanglement breaking. This is represented by the block labeled "EB." For each of the chosen rounds, Bob performs a probabilistic projection represented by operator $\hat{\Pi}$ to the dual-rail basis in (1). On failure, he replaces the state with a completely mixed state. He then decodes to obtain an estimate $|\check{m}\rangle$ of the original message. Willie tests between hypotheses H_0 and H_1 to determine if Alice is transmitting.

H_1 when H_0 is true), and a missed detection, where he decides that Alice is not transmitting when she is (choosing H_0 when H_1 is true). As is customary in the literature, we assume equal prior probabilities for the hypotheses $P(H_0) = P(H_1) = \frac{1}{2}$, though this is not a requirement. Thus, Willie's probability of error is: $P_e = \frac{P(H_0|H_1)+P(H_1|H_0)}{2}$.

Willie guessing randomly yields an ineffective detector with $P_e = \frac{1}{2}$. Hence, Alice's goal is to transmit so that P_e is as close to $\frac{1}{2}$ as possible. Formally, we call any system covert if, for large enough n and $\delta > 0$, $P_e \geq \frac{1}{2} - \delta$. With access to a quantum-optimal detector, Willie can achieve minimal $P_e = \frac{1}{2} - \frac{1}{4}\left\|\hat{\rho}_1^{W^n} - \left(\hat{\rho}_0^W\right)^{\otimes n}\right\|_1$ [25, Sec. 9.1.4], where $\|\hat{A}\|_1 \equiv \mathrm{tr}\left[\sqrt{\hat{A}^\dagger \hat{A}}\right]$ is the trace norm of $\hat{A}$ [25, Def. 9.1.1]. This implies our system is covert if $\frac{1}{4}\left\|\hat{\rho}_1^{W^n} - \left(\hat{\rho}_0^W\right)^{\otimes n}\right\|_1 \leq \delta$.

The trace distance is often mathematically unwieldy. Quantum relative entropy (QRE), $D\left(\hat{\rho}\|\hat{\sigma}\right) = \mathrm{tr}[\hat{\rho}\log\hat{\rho} - \hat{\rho}\log\hat{\sigma}]$, is commonly employed in covertness analysis [5]–[7], since it is additive over product states and upper bounds the trace distance via the quantum Pinsker's inequality [25, Th. 11.9.1]:

$$\frac{1}{4}\left\|\hat{\rho}_1^{W^n} - \left(\hat{\rho}_0^W\right)^{\otimes n}\right\|_1 \leq \sqrt{\frac{1}{8}D\left(\hat{\rho}_1^{W^n}\middle\|\left(\hat{\rho}_0^W\right)^{\otimes n}\right)}. \tag{4}$$

We employ the *right-hand side* (r.h.s.) of (4) rather than the left-hand side (l.h.s.) as our covertness criterion, as is common in both the classical [3], [4] and quantum [6]–[9] analyses. That is, we upper bound the r.h.s. of (4) by δ.

Alice and Bob ensure the covert communication by randomly selecting the transmission rounds they use via n flips of a biased coin, with the probability of heads q to be determined later. If the i^{th} flip is heads, then the i^{th} round is selected. The chosen dual-rail systems constitute the classical pre-shared secret in Fig. 1. A quantum error correction code (QECC) is used, with transmissions taking place only in the selected rounds. This procedure, channel parameters, value of q, the QECC, and the time of transmission are known to Willie.

As Willie's channel from Alice is entanglement breaking, the state he observes is a classical superposition of product states given by

$$\hat{\rho}_1^{W^n} = \sum_{|m\rangle\in\mathcal{M}} p\left(|m\rangle\right) \bigotimes_{i=1}^{n} \hat{\rho}_{1,i}^W(m), \tag{5}$$

where $\mathcal{M}$ is the set of messages, and $\sum_{|m\rangle\in\mathcal{M}} p\left(|m\rangle\right) = 1$. Furthermore,

$$\hat{\rho}_{1,i}^W(m) = (1-q)\hat{\rho}_0^W + q\hat{\rho}_{i,m}^W, \tag{6}$$

where $\hat{\rho}_{i,m}^W$ is Willie's two-mode state when Alice transmits a (possibly mixed) state with density matrix

$$\hat{\rho}_{i,m}^A = \begin{pmatrix} |\alpha(i,m)|^2 & \gamma(i,m) \\ \gamma^*(i,m) & |\beta(i,m)|^2 \end{pmatrix}, \tag{7}$$

in the logical basis with arbitrary coefficients $\alpha(i,m)$, $\beta(i,m)$, and $\gamma(i,m)$ depending on the QECC. Then, using (5) yields the following upper bound on the QRE in (4):

$$\begin{aligned} &D\left(\hat{\rho}_1^{W^n}\middle\|\left(\hat{\rho}_0^W\right)^{\otimes n}\right) \\ &\leq \sum_{|m\rangle\in\mathcal{M}} p\left(|m\rangle\right) D\left(\bigotimes_{i=1}^{n}\hat{\rho}_{1,i}^W(m)\middle\|\left(\hat{\rho}_0^W\right)^{\otimes n}\right) &(8)\\ &= \sum_{|m\rangle\in\mathcal{M}} p\left(|m\rangle\right) \sum_{i=1}^{n} D\left(\hat{\rho}_{1,i}^W(m)\middle\|\left(\hat{\rho}_0^W\right)^{\otimes n}\right) &(9)\\ &\leq \sum_{|m\rangle\in\mathcal{M}} p\left(|m\rangle\right) q^2 \sum_{i=1}^{n} D_{\chi^2}\left(\hat{\rho}_{i,m}^W\|\hat{\rho}_0^W\right), &(10)\end{aligned}$$

where (8) and (9) follow from the convexity [25, Corollary 11.9.2] and additivity [25, Ex. 11.8.7] properties of the QRE. Lastly, (10) is by [9, Lemma 1], where the quantum χ^2-divergence [32] between two states $\hat{\rho}$ and $\hat{\sigma}$ is:

$$D_{\chi^2}\left(\hat{\rho}\|\hat{\sigma}\right) = \mathrm{tr}\left[(\hat{\rho}-\hat{\sigma})^2\hat{\sigma}^{-1}\right] = \mathrm{tr}[\hat{\rho}^2\hat{\sigma}^{-1}] - 1, \tag{11}$$

with the second equality due to the cyclic property of the trace and the fact that the trace of a quantum state is unity. The following yields a bound on $D_{\chi^2}\left(\hat{\rho}_{i,m}^W\|\hat{\rho}_0^W\right)$:

Lemma 3: When Alice transmits an arbitrary quantum state with the following density operator in the logical basis

$$\hat{\rho}^A = \begin{pmatrix} |\alpha|^2 & \gamma \\ \gamma^* & |\beta|^2 \end{pmatrix} \tag{12}$$

that is encoded in dual-rail qubit basis, the corresponding output at Willie $\hat{\rho}^W$ satisfies:

$$D_{\chi^2}\left(\hat{\rho}^W \middle\| \left(\hat{\rho}_0^W\right)^{\otimes 2}\right) \leq \frac{(1-\eta)^2}{\eta\bar{n}_{\mathrm{B}}(1+\eta\bar{n}_{\mathrm{B}})}. \tag{13}$$

Here we provide a proof sketch, with the full proof deferred to [28, Appendix B].

Proof (sketch): Our first challenge is to determine $\hat{\rho}^W$. First, we find its density-operator representation. The anti-normally ordered characteristic function completely defines a quantum state $\hat{\rho}$, and, for a two-mode state, is given by:

$$\chi_A^{\hat{\rho}}(\zeta_1,\zeta_2) = \mathrm{tr}\left[\hat{\rho} e^{-\zeta_1^*\hat{a}_1} e^{\zeta_1\hat{a}_1^\dagger} e^{-\zeta_2^*\hat{a}_2} e^{\zeta_2\hat{a}_2^\dagger}\right], \tag{14}$$

where $\zeta_i \in \mathbb{C}$ and $\hat{a}_i, \hat{a}_i^\dagger$ are modal annihilation and creation operators for $i = 1, 2$ [26]. Using the expression for $\hat{w}$ in (2),

$$\begin{aligned}\chi_A^{\hat{\rho}^W}(\zeta_1,\zeta_2) = \chi_A^{\hat{\rho}^A}\left(\sqrt{1-\eta}\zeta_1, \sqrt{1-\eta}\zeta_2\right) \\ \times \chi_A^{\hat{\rho}^E}\left(\sqrt{\eta}\zeta_1, \sqrt{\eta}\zeta_2\right),\end{aligned} \tag{15}$$

where $\chi_A^{\hat{\rho}^A}(\cdot)$ and $\chi_A^{\hat{\rho}^E}(\cdot)$ are the characteristic functions for Alice's input state (12) and the thermal state. The expression for $\chi_A^{\hat{\rho}^E}(\cdot)$ is well known [33, Sec. 7.4.3.2]. $\chi_A^{\hat{\rho}^A}(\cdot)$ is derived by using (12) in (14) and expanding the exponentials:

$$\begin{aligned}\chi_A^{\hat{\rho}^W}(\zeta_1,\zeta_2) = e^{-(1+\eta\bar{n}_{\mathrm{B}})(|\zeta_1|^2+|\zeta_2|^2)}\left[1-(1-\eta)\left(|\alpha|^2||\zeta_2|^2\right.\right. \\ \left.\left.+|\beta|^2|\zeta_1|^2+\gamma\zeta_1\zeta_2^*+\gamma^*\zeta_1^*\zeta_2\right)\right].\end{aligned} \tag{16}$$

A quantum state $\hat{\rho}^W$ and its characteristic function $\chi_A^{\hat{\rho}^W}(\cdot)$ are related via the operator Fourier transform [26]:

$$\hat{\rho}^W = \iint \frac{d^2\zeta_1}{\pi}\frac{d^2\zeta_2}{\pi}\chi_A^{\hat{\rho}^W} e^{\zeta_2\hat{w}_2^\dagger} e^{\zeta_1\hat{w}_1^\dagger} e^{-\zeta_1^*\hat{w}_1} e^{-\zeta_2^*\hat{w}_2}, \tag{17}$$

where the integrals are over the complex planes for ζ_1 and ζ_2. This allows $\hat{\rho}^W$ to be expressed in the Fock basis with the elements $p_{f,g,f',g'} = \langle fg|\hat{\rho}^W|f'g'\rangle$ for $f, g, f', g' \in \mathbb{N}_0$.

The integrals in (17) are evaluated in polar coordinates with expansions of the exponentials that include annihilation and creation operators. Details are deferred to [28, Appendix B]. Due to the orthogonality of Fock states for the $|\alpha|^2$ and $|\beta|^2$ contributions, the only non-zero terms occur when $f = f'$ and $g = g'$, defining the main diagonal of the density operator. The γ-contribution terms are non-zero when $f' = f+1$ and $g' = g-1$ from an off-by-one exponential in integration over the corresponding polar coordinates. The γ^*-contributions follow similarly for $f' = f-1$ and $g' = g+1$. The Fourier transform in (17) yields:

$$\begin{aligned}\hat{\rho}^W = \sum_{g=0}^{\infty}\sum_{f=0}^{\infty}\left(|\alpha|^2 W_1(f,g) + |\beta|^2 W_1(g,f)\right)|fg\rangle\langle fg| \\ + \gamma W_2(g,f)|fg\rangle\langle f+1, g-1| \\ + \gamma^* W_2(f,g)|fg\rangle\langle f-1, g+1|\end{aligned} \tag{18}$$

where

$$\begin{aligned}W_1(f,g) &= \left(\frac{(\eta\bar{n}_{\mathrm{B}})^g}{(1+\eta\bar{n}_{\mathrm{B}})^{g+1}} - \frac{(1-\eta)(\eta\bar{n}_{\mathrm{B}}-g)(\eta\bar{n}_{\mathrm{B}})^{g-1}}{(1+\eta\bar{n}_{\mathrm{B}})^{g+2}}\right) \\ &\quad \times \frac{(\eta\bar{n}_{\mathrm{B}})^f}{(1+\eta\bar{n}_{\mathrm{B}})^{f+1}}, \\ W_2(f,g) &= \frac{(1-\eta)(\eta\bar{n}_{\mathrm{B}})^{g+f-1}}{(1+\eta\bar{n}_{\mathrm{B}})^{g+f+3}}\sqrt{f(g+1)}.\end{aligned} \tag{19}$$

Thus, $\hat{\rho}^W$ is a tri-diagonal operator as it is defined by $|fg\rangle\langle fg|$, $|fg\rangle\langle f-1, g+1|$, and $|fg\rangle\langle f+1, g-1|$. We obtain $(\hat{\rho}^W)^2$ by assigning each diagonal to operators $\hat{A}$, $\hat{B}$, $\hat{C}$ and computing $(\hat{\rho}^W)^2 = \left(\hat{A}+\hat{B}+\hat{C}\right)^2$.

Now, the density operator for the two-mode thermal state $\left(\hat{\rho}_0^W\right)^{\otimes 2}$ received by Willie when Alice is silent is [26]:

$$\left(\hat{\rho}_0^W\right)^{\otimes 2} = \sum_{f=0}^{\infty}\sum_{g=0}^{\infty} t_g(\eta\bar{n}_{\mathrm{B}}) t_f(\eta\bar{n}_{\mathrm{B}})|fg\rangle\langle fg|, \tag{20}$$

where $t_f(\eta\bar{n}_{\mathrm{B}})$ and $t_g(\eta\bar{n}_{\mathrm{B}})$ are defined in (3). Since (20) is a diagonal operator, its inverse is also diagonal. Calculating $D_{\chi^2}\left(\hat{\rho}^W \middle\| \left(\hat{\rho}_0^W\right)^{\otimes 2}\right) = \mathrm{tr}\left[(\hat{\rho}^W)^2\left((\hat{\rho}_0^W)^{-1}\right)^{\otimes 2}\right] - 1$ reduces to multiplying the diagonal elements of $(\hat{\rho}^W)^2$ and $\left((\hat{\rho}_0^W)^{-1}\right)^{\otimes 2}$, and summing the results. This yields:

$$\begin{aligned}\mathrm{tr}\left[(\hat{\rho}^W)^2\left((\hat{\rho}_0^W)^{-1}\right)^{\otimes 2}\right] = \left[\left((1-\eta)^2+\eta\bar{n}_{\mathrm{B}}(1+\eta\bar{n}_{\mathrm{B}})\right)\right. \\ \times\left(|\alpha|^4+|\beta|^4\right)+2\left(|\alpha|^2|\beta|^2\eta\bar{n}_{\mathrm{B}}(1+\eta\bar{n}_{\mathrm{B}})\right. \\ \left.\left.+(1-\eta)^2|\gamma|^4\right)\right]/(\eta\bar{n}_{\mathrm{B}}(1+\eta\bar{n}_{\mathrm{B}})).\end{aligned} \tag{21}$$

A pure-state logical qubit input with $|\gamma| = |\alpha\beta|$ maximizes (21), yielding the lemma. ∎

Lemma 3 upper-bounds $D_{\chi^2}\left(\hat{\rho}_{i,m}^W \middle\| \hat{\rho}_0^W\right)$ independently of α, β, and γ. Combining it with (4) and (10) yields:

$$\sqrt{\frac{1}{8}D\left(\hat{\rho}_1^{W^n} || \left(\hat{\rho}_0^W\right)^{\otimes n}\right)} \leq \frac{q(1-\eta)\sqrt{n}}{2\sqrt{2\eta\bar{n}_{\mathrm{B}}(1+\eta\bar{n}_{\mathrm{B}})}}. \tag{22}$$

Therefore, the covertness requirement is maintained if $q \leq \frac{2c_{\mathrm{cov}}\delta}{\sqrt{n}}$, where the covertness constant is:

$$c_{\mathrm{cov}} = \frac{\sqrt{2\eta\bar{n}_{\mathrm{B}}(1+\eta\bar{n}_{\mathrm{B}})}}{(1-\eta)}. \tag{23}$$

Note that we employ the same constant c_{cov} as in [6, Eq. (2)].

B. Reliability Analysis and Achievability

Let $M(n)$ be the number of qubits transmitted covertly in n channel uses. Denote by $[x]^+ = \max(x, 0)$. The following theorem characterizes the lower bound on $E[M(n)]$, where the expectation is over the biased random coin flips used to select the dual-rail systems in Section III-A:

Theorem 1 (Achievability): $E[M(n)] \geq 2\sqrt{n}c_{\mathrm{cov}}R\delta$ qubits can be transmitted reliably and covertly over n uses of the lossy thermal-noise bosonic channel, where c_{cov} is in (23), and δ is the covertness constraint. $R \geq [1-H(\vec{p})]^+$ is the constant achievable rate of reliable qubit transmission per round, where $\vec{p} = \left[1-\frac{3p}{4}, \frac{p}{4}, \frac{p}{4}, \frac{p}{4}\right]$, $p = 1-\frac{\eta}{(1+(1-\eta)\bar{n}_{\mathrm{B}})^4}$, and $H(\vec{p}) = -\sum_{p_i\in\vec{p}} p_i\log(p_i)$ is the Shannon entropy.

Proof: Alice and Bob pre-share a secret, determining the rounds to be used for transmission. Alice employs a random code from [25, Secs. 23.3 and 24.4] to encode the message. The expected number of rounds selected is $qn = 2c_{\rm cov}\delta\sqrt{n}$, per Section III-A.

Bob projects the two-mode systems in each of the selected rounds into the subspace spanned by the dual-rail basis states in (1). The probability of projection failure is $p_{\rm fail} = 1 - \langle 01|\hat{\rho}^B|01\rangle + \langle 10|\hat{\rho}^B|10\rangle = 1 - \frac{2\bar{n}_{\rm B}(1+\bar{n}_{\rm B})(1-\eta)^2+\eta}{(1+(1-\eta)\bar{n}_{\rm B})^4}$ where $\hat{\rho}^B$ is described by (18) with η swapped for $1-\eta$ and vice versa, and arbitrary α, β, and γ. When the projection is unsuccessful, Bob replaces the state with the maximally mixed state $\frac{\hat{\pi}}{2}$. This mimics a depolarizing channel $\hat{\rho}^B \to \hat{\rho}^B_{\rm proj} = (1-p_{\rm fail})\hat{\rho}^B + p_{\rm fail}\frac{\hat{\pi}}{2}$ parameterized by $p_{\rm fail}$.

Furthermore, this projection allows one to treat the lossy thermal-noise channel as a depolarizing channel acting on $\hat{\rho}^B_{\rm proj}$ and parameterized by $p' = \frac{2(1-\eta)^2\bar{n}_{\rm B}(1+\bar{n}_{\rm B})}{\eta+2(1-\eta)^2\bar{n}_{\rm B}(1+\bar{n}_{\rm B})}$ [34, Appendix B]. Then Bob's state, $\hat{\rho}'^B$, prior to decoding is given by $\hat{\rho}^B_{\rm proj} \to \hat{\rho}'^B = (1-p')\hat{\rho}^B_{\rm proj} + p'\frac{\hat{\pi}}{2}$, where

$$\hat{\rho}'^B = (1-p')\left((1-p_{\rm fail})\hat{\rho}^B + p_{\rm fail}\frac{\hat{\pi}}{2}\right) + p'\frac{\hat{\pi}}{2} \tag{24}$$

$$= (1-p')(1-p_{\rm fail})\hat{\rho}^B + (p' + (1-p')p_{\rm fail})\frac{\hat{\pi}}{2} \tag{25}$$

$$= (1-p)\hat{\rho}^B + p\frac{\hat{\pi}}{2}, \tag{26}$$

with $p = p' + (1-p')p_{\rm fail} = 1 - \frac{\eta}{(1+(1-\eta)\bar{n}_{\rm B})^4}$ in (26). Thus, in each round, Bob's state is equivalent to Alice's state transmitted through a depolarizing channel parameterized by p. This channel is a Pauli channel parameterized by $\vec{p} = \left[1-\frac{3p}{4}, \frac{p}{4}, \frac{p}{4}, \frac{p}{4}\right]$ [25, Ex. 4.7.4]. We complete the proof using the hashing bound [25, Sec. 24.6.3]. ∎

The following remarks are in order:

1) Entanglement-breaking condition: If the Alice-to-Willie channel is not naturally entanglement breaking, Alice may use Lemmas 1 or 2 to break it. Using Lemma 1 replaces $(1-\eta)$ with $\tau(1-\eta)$ in the expressions for $c_{\rm cov}$ and η by $1-\tau(1-\eta)$ in R. Using Lemma 2 replaces $\bar{n}_{\rm B}$ with $\bar{n}_{\rm B} + \bar{n}'_{\rm B}$ in $c_{\rm cov}$ and $\bar{n}_{\rm B} + \bar{n}''_{\rm B}$ in R where $\bar{n}''_{\rm B} = \frac{2(1-1/G)\eta}{1-\eta}$.

2) Use of auxiliary covert classical channel: Suppose that Alice and Bob have a covert full-duplex classical communication link. Let Alice prepare Bell states, sending one qubit of each state to Bob using the dual-rail basis on the rounds selected for transmission. Bob's projection of his received state to the smaller dual-rail subspace in (1) is probabilistic, with outcomes known to Bob. Bob communicates to Alice the indices of successful rounds over the covert classical full-duplex link, allowing hashing-based entanglement distillation [35] on these rounds. Alice can then teleport qubits to Bob using this distributed entanglement and the covert classical link, achieving $R' = (1-p_{\rm fail})\left(1 - H(\vec{p'})\right)$ where $\vec{p'} = \left[1-\frac{3p'}{4}, \frac{p'}{4}, \frac{p'}{4}, \frac{p'}{4}\right]$ and p' is the same as that in the proof of Theorem 1. The resulting expected number of reliably-transmissible covert qubits is plotted in Fig. 2. The average number of classical bits that need to be covertly exchanged is $\propto \sqrt{n}$, making this scheme feasible under certain channel conditions. However, we defer the characterization of covert classical communication link requirements to future work.

3) Potential improvement of the bound on R without classical communication: When Bob fails to project a state to the basis defined by (1), he replaces it with a maximally mixed state. Hence, instead of an erasure error, it is treated as a random Pauli error and Bob throws away useful information that may aid in decoding. Indeed, it is known that any stabilizer code can correct up to twice as many erasure errors as Pauli errors [36, Sec. III.A]. Although the use of random codes and their analytical achievable rate R has only been established for Pauli errors, the rates for large codes correcting erasure errors (such as the tree code [37]) can be computed numerically.

Finally, here, we restrict encoding to the finite-dimensional subspace spanned by dual-rail basis in (1). Bosonic codes may improve the rate R, as they take advantage of the entire infinite-dimensional space. However, the covertness requirement may diminish this advantage. For example, ideal Gottesman-Kitaev-Preskill (GKP) states require infinite energy, conflicting with covertness. Nevertheless, the trade-off should be studied.

C. Converse

The following provides an upper bound on $M(n)$:

Theorem 2 (Converse): $M(n) \le 2nC$ where

$$C = \left[g\left(\frac{(G+1)\bar{n}_{\rm S} + \bar{G}}{2}\right) - g\left(\frac{\bar{G}(1+\bar{n}_{\rm S})}{2}\right)\right]^+, \tag{27}$$

with $g(x) \equiv (1+x)\log(1+x) - x\log(x)$, $G = \frac{\eta}{\eta-(1-\eta)\bar{n}_{\rm B}/2}$, $\bar{G} = G - 1$, and the mean photon number of Alice's input state for $c_{\rm cov}$ defined in (23) is constrained by $\bar{n}_{\rm S} \le \frac{2c_{\rm cov}\delta}{\sqrt{n}}$.

Proof: In Theorem 1, we use the total of $2n$ modes of lossy thermal-noise bosonic channel, since we transmit dual-rail qubits. Hence, we employ the standard arguments from [25, Sec. 24.5] to obtain $M(n) \le C'_{2n}$, where C'_{2n} is the channel quantum capacity (regularized coherent information) over these $2n$ uses. Any lossy thermal-noise channel with transmittance η and mean thermal photon number $\bar{n}_{\rm B}$ can be decomposed into a quantum-limited amplifier with gain coefficient $G = \frac{\eta}{\eta-(1-\eta)\bar{n}_{\rm B}/2}$ followed by a pure-loss channel with transmittance $\eta' = \eta/G$ [29], [30]. Discarding one of these channels and applying the data-processing inequality upper bounds $C'_{2n} \le C_{2n}$, where C_{2n} is the quantum capacity of the remaining channel over $2n$ uses. Since both pure-loss and pure-input quantum-limited amplifier channels are degradable [38], their coherent information is additive, and $C_{2n} = 2nC$, where C is the single-channel-use quantum capacity. Usually, the amplifier channel is discarded (see, e.g., [23, Th. 16]), since the resulting bound is tighter unless $\bar{n}_{\rm S} \to 0$. Here, due to constraint on $\bar{n}_{\rm S}$, we obtain a tighter bound by discarding the pure-loss[1] channel: C in (27) is an upper bound on the quantum capacity of the amplifier channel

[1]Discarding the amplifier instead yields a poor bound that is $\propto \sqrt{n}\log(n)$.

with gain G assisted by the arbitrary local operations and classical communication (LOCC) [39, Eqs. (115), (172)] [40].

The energy-constrained capacity is required, as bounding the QRE on the r.h.s. of (4) limits Alice's input state mean photon number $\bar{n}_{\mathrm{S}}$ per [6, Thm. 1]. While this result[2] is applied to the classical-quantum capacity in [6], the theorem is general for any quantum state. ■

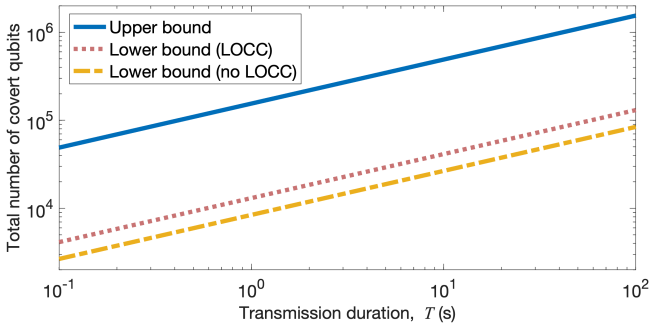

Fig. 2. Log-log plot for upper (solid blue line) and lower (dot-dashed red line) bounds given by Theorem 2 and Theorem 1 respectively for the total number of covert bits reliably transferred vs time in seconds. The orange dotted line is the lower bound discussed in remark 2 of Section III-B enabled by a two-way classical communication link. Here, transmittance $\eta = 0.9$, the mean thermal photon number $\bar{n}_{\mathrm{B}} = 0.12$, and the covertness parameter $\delta = 0.05$.

Taylor series expansion of (27) around $\bar{n}_{\mathrm{S}} = 0$ yields the SRL scaling of the upper bound in Theorem 2, matching that of the lower bound in Theorem 1. However, a multiplicative gap exists between these bounds, as shown in Fig. 2, where we set the channel transmittance to $\eta = 0.9$, and $\bar{n}_{\mathrm{B}} = 0.12$. These parameters ensure that the Alice-to-Willie channel is entanglement breaking. Furthermore, we employ a modulation frequency of 100 MHz or 10^8 modes/second with a covertness criterion of $\delta = 0.05$. We suspect the looseness of the upper bound is due to the data processing argument, insofar as we disregard the pure-loss channel in the decomposition of the original channel. Indeed, a tighter bound may exist. However, deriving such a bound remains a difficult open problem as it requires analysis of the regularized coherent information of the channel [25, Th. 24.3.1] [41].

IV. Conclusion and Discussion

We develop an achievable lower bound on the expected number $E[M(n)]$ of qubits that are covertly and reliably transmissible using dual-rail qubit encoding over the lossy thermal-noise bosonic channel (we defer removing the expectation to future work). We also provide a converse. Although we specifically address quantum communication rather than QKD, we expect our work to provide insight into the open questions in covert QKD [19]–[22].

While both the upper and lower bounds in the converse and the achievability scale $\propto \sqrt{n}$, the gap between them is fairly large. This motivates improvement of the QECC capabilities and the upper bounds of the quantum capacity of the lossy thermal-noise bosonic channel, as noted in Sections III-B and III-C. Furthermore, in our achievability analysis, we require that the Alice-to-Willie channel is entanglement breaking to simplify the mathematics. While Lemmas 1 and 2 may be employed to ensure this condition, for atmospheric models such as MODTRAN [42], $R = 0$ in Theorem 1. However, using classical covert channel can yield $R > 0$. Further investigation of the necessity of entanglement-breaking condition is needed. Other covertness criteria, including bounding the trace norm on the l.h.s. of (4) directly (as done in [43] for classical-quantum channels), also need to be studied.

Practical aspects of achieving covert quantum communication have to be considered. Our covertness scheme requires a substantial number of classical pre-shared secret bits; resolvability techniques from [3], [9] should be adapted to reduce this burden. Additionally, here we assume that quantum states are generated for transmission on demand. However, quantum processes are inherently random. This stochasticity needs to be included in the calculation of channel use selection probability q. Moreover, although randomness in state generation is generally considered an undesired characteristic of quantum information processing, here it might be exploited. For example, the quasi-probabilistic nature of heralded entangled photonic Einstein-Podolsky-Rosen (EPR) pair generation [44] could be used to select a random subset of channel uses.

Finally, the framework provided in this manuscript can be applied to other qubit encodings and quantum channels. Encodings such as single-rail and GKP are enticing candidates due to their prevalence in the literature and error-correcting properties of the latter. In fact, it has been shown [45] that GKP qubits allow reliable quantum communication rates that differ only by a constant factor from the known upper bound on the quantum capacity of the pure-loss bosonic channel and perform well in the lossy thermal-noise bosonic channel setting. However, their energy requirements negatively impact covertness. Indeed, practical codes enabling a physical realization of covert quantum communication should be investigated.

Acknowledgement

The authors benefited from discussions with Christos Gagatsos, Brian Smith, Ryan Camacho, Michael Bullock, Narayanan Rengaswamy, Kenneth Goodenough, and Saikat Guha.

[2]There is a typo in the short paragraph between Criterion 2 and Eq. (4) in [6]: $\delta = \sqrt{\delta_{\mathrm{QRE}}}$ should be $\sqrt{8}\delta = \sqrt{\delta_{\mathrm{QRE}}}$. We apply this correction in deriving the constraint on $\bar{n}_{\mathrm{S}}$ in the statement of Theorem 2.

REFERENCES

[1] 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.

[2] B. A. 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.

[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] 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] 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.

[8] 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.

[9] M. S. Bullock, A. Sheikholeslami, M. Tahmasbi, R. C. Macdonald, S. Guha, and B. A. Bash, "Covert Communication over Classical-Quantum Channels," arXiv:1601.06826v7 [quant-ph], Jul. 2023.

[10] P. Thomas, L. Ruscio, O. Morin, and G. Rempe, "Efficient generation of entangled multiphoton graph states from a single atom," *Nature*, vol. 608, no. 7924, pp. 677–681, Aug. 2022.

[11] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres," *Nature*, vol. 526, no. 7575, pp. 682–686, Oct. 2015.

[12] V. Krutyanskiy, M. Galli, V. Krcmarsky, S. Baier, D. A. Fioretto, Y. Pu, A. Mazloom, P. Sekatski, M. Canteri, M. Teller, J. Schupp, J. Bate, M. Meraner, N. Sangouard, B. P. Lanyon, and T. E. Northup, "Entanglement of trapped-ion qubits separated by 230 meters," *Phys. Rev. Lett.*, vol. 130, p. 050803, Feb 2023.

[13] S. Takeda, T. Mizuta, M. Fuwa, P. van Loock, and A. Furusawa, "Deterministic quantum teleportation of photonic quantum bits by a hybrid technique," *Nature*, vol. 500, no. 7462, pp. 315–318, Aug. 2013.

[14] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, "Rate-loss analysis of an efficient quantum repeater architecture," *Phys. Rev. A*, vol. 92, p. 022357, Aug 2015.

[15] P. Dhara, D. Englund, and S. Guha, "Entangling quantum memories via heralded photonic bell measurement," *Phys. Rev. Res.*, vol. 5, p. 033149, Sep 2023.

[16] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, "Quantum repeaters: From quantum networks to the quantum internet," *Rev. Mod. Phys.*, vol. 95, p. 045006, Dec 2023.

[17] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep. 2009.

[18] T. Honjo, S. W. Nam, H. Takesue, Q. Zhang, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, B. Baek, R. Hadfield, S. Miki, M. Fujiwara, M. Sasaki, Z. Wang, K. Inoue, and Y. Yamamoto, "Long-distance entanglement-based quantum key distribution over optical fiber," *Opt. Express*, vol. 16, no. 23, pp. 19 118–19 126, Nov 2008.

[19] J. M. Arrazola and V. Scarani, "Covert Quantum Communication," *Phys. Rev. Lett.*, vol. 117, no. 25, p. 250503, Dec. 2016.

[20] 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.

[21] ——, "Toward undetectable quantum key distribution over bosonic channels," *IEEE J. Sel. Areas Inf. Theory*, vol. 1, no. 2, pp. 585–598, 2020.

[22] ——, "Covert and secret key expansion over quantum channels under collective attacks," *IEEE Trans. Inf. Theory*, vol. 66, no. 11, pp. 7113–7131, Nov. 2020.

[23] K. Sharma, M. M. Wilde, S. Adhikari, and M. Takeoka, "Bounding the energy-constrained quantum and private capacities of phase-insensitive bosonic Gaussian channels," *New J. Phys.*, vol. 20, no. 6, p. 063025, Jun. 2018.

[24] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature*, vol. 409, no. 6816, pp. 46–52, Jan. 2001.

[25] M. Wilde, *Quantum Information Theory*, 2nd ed. Cambridge University Press, 2016.

[26] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, pp. 621–669, May 2012.

[27] A. S. Holevo, "Entanglement-breaking channels in infinite dimensions," *Probl. Inf. Transm.*, vol. 44, no. 3, pp. 171–184, Sep. 2008.

[28] E. J. D. Anderson, C. K. Eyre, I. M. Dailey, F. Rozpędek, and B. A. Bash, "Covert quantum communication over optical channels," arXiv:2401.06764 [quant-ph], 2024.

[29] R. García-Patrón, C. Navarrete-Benlloch, S. Lloyd, J. H. Shapiro, and N. J. Cerf, "Majorization theory approach to the gaussian channel minimum entropy conjecture," *Phys. Rev. Lett.*, vol. 108, p. 110505, Mar 2012.

[30] F. Caruso, V. Giovannetti, and A. S. Holevo, "One-mode bosonic gaussian channels: a full weak-degradability classification," *New J. Phys.*, vol. 8, no. 12, p. 310, dec 2006.

[31] M. Rosati, A. Mari, and V. Giovannetti, "Narrow Bounds for the Quantum Capacity of Thermal Attenuators," *Nature Communications*, vol. 9, no. 1, p. 4339, Oct. 2018.

[32] K. Temme, M. J. Kastoryano, M. Ruskai, M. M. Wolf, and F. Verstraete, "The χ^2-divergence and mixing times of quantum Markov processes," *J. Math. Phys.*, vol. 51, no. 12, p. 122201, 2010.

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

[34] S. P. Kish, P. Gleeson, P. K. Lam, and S. M. Assad, "Comparison of discrete variable and continuous variable quantum key distribution protocols with phase noise in the thermal-loss channel," arXiv:2206.13724 [quant-ph], 2023.

[35] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A*, vol. 54, pp. 3824–3851, Nov 1996.

[36] M. Grassl, T. Beth, and T. Pellizzari, "Codes for the Quantum Erasure Channel," *Physical Review A*, vol. 56, no. 1, pp. 33–38, Jul. 1997.

[37] M. Varnava, D. E. Browne, and T. Rudolph, "Loss Tolerance in One-Way Quantum Computation via Counterfactual Error Correction," *Physical Review Letters*, vol. 97, no. 12, p. 120501, Sep. 2006.

[38] F. Caruso and V. Giovannetti, "Degradability of bosonic gaussian channels," *Phys. Rev. A*, vol. 74, p. 062307, Dec 2006.

[39] N. Davis, M. E. Shirokov, and M. M. Wilde, "Energy-constrained two-way assisted private and quantum capacities of quantum channels," *Phys. Rev. A*, vol. 97, p. 062310, Jun 2018.

[40] K. Goodenough, D. Elkouss, and S. Wehner, "Assessing the performance of quantum repeaters for all phase-insensitive gaussian bosonic channels," *New Journal of Physics*, vol. 18, no. 6, p. 063005, jun 2016.

[41] S. Khatri, K. Sharma, and M. M. Wilde, "Information-theoretic aspects of the generalized amplitude-damping channel," *Phys. Rev. A*, vol. 102, p. 012401, Jul 2020.

[42] A. Berk, G. P. Anderson, P. K. Acharya, L. S. Bernstein, L. Muratov, J. Lee, M. Fox, S. M. Adler-Golden, J. H. Chetwynd, Jr., M. L. Hoke, R. B. Lockwood, J. A. Gardner, T. W. Cooley, C. C. Borel, P. E. Lewis, and E. P. Shettle, "MODTRAN5: 2006 update," in *Proc. SPIE*, vol. 6233, 2006, pp. 62 331F–62 331F–8.

[43] S.-Y. Wang, T. Erdoğan, and M. Bloch, "Towards a Characterization of the Covert Capacity of Bosonic Channels under Trace Distance," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Jun. 2022, pp. 318–323.

[44] K. C. Chen, P. Dhara, M. Heuck, Y. Lee, W. Dai, S. Guha, and D. Englund, "Zero-added-loss entangled-photon multiplexing for ground- and space-based quantum networks," *Phys. Rev. Appl.*, vol. 19, p. 054029, May 2023.

[45] K. Noh, V. V. Albert, and L. Jiang, "Quantum capacity bounds of gaussian thermal loss channels and achievable rates with Gottesman-Kitaev-Preskill codes," *IEEE Trans. Inf. Theory*, vol. 65, no. 4, pp. 2563–2582, 2019.