Quantum-noise limited communication with low probability of detection

Boulat A. Bash,[1] Saikat Guha,[2] Dennis Goeckel,[3] and Don Towsley[1]
[1]*School of Computer Science, University of Massachusetts, Amherst, Massachusetts, USA 01003,*
[2]*Quantum Information Processing Group, Raytheon BBN Technologies, Cambridge, Massachusetts, USA 02138,*
[3]*Electrical and Computer Engineering Department, University of Massachusetts, Amherst, Massachusetts, USA 01003*

We demonstrate the achievability of a square root limit on the amount of information transmitted reliably and with *low probability of detection* (LPD) over the single-mode lossy bosonic channel if either the eavesdropper's measurements or the channel itself is subject to the slightest amount of excess noise. Specifically, Alice can transmit $\mathcal{O}(\sqrt{n})$ bits to Bob over n channel uses such that Bob's average codeword error probability is upper-bounded by an arbitrarily small $\delta > 0$ while a passive eavesdropper, Warden Willie, who is assumed to be able to collect all the transmitted photons that do not reach Bob, has an average probability of detection error that is lower-bounded by $\frac{1}{2} - \epsilon$ for an arbitrarily small $\epsilon > 0$. We analyze the thermal noise and pure loss channels. The square root law holds for the thermal noise channel even if Willie employs a quantum-optimal measurement, while Bob is equipped with a standard coherent detection receiver. We also show that LPD communication is not possible on the pure loss channel. However, this result assumes Willie to possess an ideal receiver that is not subject to excess noise. If Willie is restricted to a practical receiver with a non-zero dark current, the square root law is achievable on the pure loss channel.

Typically wireless data transmission is secured from an eavesdropping third party by a cryptographic encryption protocol. However, there are real-life scenarios where encryption arouses suspicion and even theoretically robust encryption can be defeated by a determined adversary using a non-computational method such as side-channel analysis. Thus, protection from interception is often insufficient and the adversary's ability to even *detect the presence* of a transmission must be limited. This is known as *low probability of detection* (LPD) communication.

While practical LPD communication on radio frequency (RF) channels has been explored in the context of spread-spectrum communications [1, Part 5, Ch. 1], our recent work [2, 3] addressed the fundamental limits of LPD communication on an additive white Gaussian noise (AWGN) RF channel. However, free-space communication at optical frequencies offers significant advantages over RF, motivating the need to analyze the LPD communication capability of optical communication. Electromagnetic waves are quantum-mechanical and since modern high-sensitivity optical detection systems are limited by noise of quantum-mechanical origin, assessing the fundamental limits of LPD optical communication necessitates an explicit quantum analysis.

Refs. [2, 3] analyze the LPD communication on an AWGN channel. This corresponds to an optical channel where: (i) transmitter Alice uses ideal laser light to modulate her information, and (ii) both the adversary Warden Willie as well as the legitimate receiver Bob use coherent detection receivers. However, coherent detection receivers can be decidedly sub-optimal for both the intended receiver Bob and Warden Willie, and thus a more general analysis of LPD communication with no structural assumptions on Willie's receiver other than its realization being permissible by the laws of physics is desirable. The sub-optimality of coherent detection is particularly pronounced in the low photon number regime [4, 5], which is relevant to LPD communication. It is also preferable to show the possibility of LPD communication when Bob is equipped with a conventional (coherent detection or direct detection) optical receiver, while Willie remains quantum-powerful. Demonstrating how such is possible, even on a highly lossy and noisy channel, is our main contribution.

In this paper we provide the fundamental scaling limits for LPD communication on a lossy optical channel. We limit our analysis to pure input states since, by convexity, using mixed states as inputs can only deteriorate the performance (since that is equivalent to transmitting a randomly chosen pure state from an ensemble and discarding the knowledge of that choice). We consider two types of channels: the thermal noise and the pure loss channel. We show that if Willie has a thermal noise channel from Alice, then meaningful LPD communication between Alice and Bob is possible even if Willie is able to collect all the transmitted photons that do not reach Bob and employ an arbitrarily complex receiver measurement constrained only by the laws of quantum physics. On the other hand, if Willie has a pure loss channel from Alice, then there is a receiver he can employ that is capable of perfectly determining when Alice is *not* transmitting. Even though this receiver can err when Alice is transmitting, we show that Willie can utilize it to prevent LPD communication even when Bob is equipped with an optimal receiver. However, while Willie's receiver is theoretically conceivable, it has not been and is unlikely to be built. Practical receivers suffer from dark current due to a spontaneous emission process. We thus show that LPD communication is possible if Willie has a pure loss channel from Alice but is limited to a direct detection receiver with non-zero dark current.

In order to state the theorems that govern the LPD scaling laws, we denote Willie's average error probability $\mathbb{P}_e^{(w)} = \frac{\mathbb{P}_{FA}+\mathbb{P}_{MD}}{2}$, where $\mathbb{P}_{FA}$ is the probability that Willie raises a false alarm when Alice did not transmit and $\mathbb{P}_{MD}$ is the probability that Willie misses the detection of Alice's transmission. We say that Alice communicates to Bob *reliably* when Bob's average decoding error probability $\mathbb{P}_e^{(b)} \leq \delta$ for an arbitrary $\delta > 0$ given large enough n. We use asymptotic notation where $f(n) = \mathcal{O}(g(n))$ denotes an asymptotically tight upper bound on $f(n)$, and $f(n) = o(g(n))$ and $f(n) = \omega(g(n))$ denote upper and lower bounds, respectively, that are not asymp-

totically tight [6, Ch. 3.1].

First we present a theorem that establishes the achievability of the LPD communication when Willie's capabilities are limited only by the laws of quantum physics but his channel from Alice is subject to thermal noise.

Theorem 1 (Square root law for the thermal noise channel) *Suppose Willie has access to an arbitrarily complex receiver measurement as permissible by the laws of quantum physics and can capture all the photons transmitted by Alice. Let Willie's channel from Alice be subject to the noise from a thermal environment that injects $N_B > 0$ photons per channel use on average. Then Alice can lower-bound $\mathbb{P}_e^{(w)} \geq \frac{1}{2} - \epsilon$ for any $\epsilon > 0$ while reliably transmitting $\mathcal{O}(\sqrt{n})$ bits to Bob in n channel uses even if Bob only has access to a (sub-optimal) coherent detection receiver.*

Next we present a partial converse to Theorem 1. It is partial because Alice is restricted to using input states with bounded photon number variance. However, such restriction is not onerous since this restricted set subsumes all physically-realizable states of a bosonic mode (such as coherent states, squeezed states, number states, photon-subtracted squeezed vacuum, etc.). We show that, under this restriction, reliable transmission of $\omega(\sqrt{n})$ LPD bits to Bob in n channel uses is impossible.

Theorem 2 (Partial converse to Theorem 1) *Suppose Alice only uses quantum states with bounded photon number variance to communicate with Bob. Then, if she attempts to transmit $\omega(\sqrt{n})$ bits in n channel uses, as $n \to \infty$, she is either detected by Willie with arbitrarily low $\mathbb{P}_e^{(w)}$ or Bob cannot decode with arbitrarily low error probability.*

Now we show that LPD communication using *any* quantum state is impossible when Willie has a pure loss channel from Alice and is limited only by the laws of physics in his receiver measurement choice.

Theorem 3 (No LPD communication with quantum-powerful Willie on a pure loss channel) *Suppose Willie has a pure loss channel from Alice and is limited only by the laws of physics in his receiver measurement choice. Then Alice cannot reliably communicate to Bob using arbitrary pure states while limiting $\mathbb{P}_e^{(w)} \geq \epsilon$ for any $\epsilon > 0$ even if Bob employs a quantum-optimal receiver.*

While Theorem 3 seems to preclude Alice from using a pure loss channel for LPD communication, its proof requires Willie to build an ideal single photon direct detection receiver that detects vacuum perfectly. However, practical photon counting receivers are subject to "dark clicks", or photon detection events when no photons are impinging on the detector's active surface. We show that in this case LPD communication is possible.

Theorem 4 (Square root law when Willie experiences dark current) *Suppose that Willie has a pure loss channel from Alice but is limited to a receiver with a non-zero dark current. Then Alice can lower-bound $\mathbb{P}_e^{(w)} \geq \frac{1}{2} - \epsilon$ for any $\epsilon > 0$ while reliably transmitting $\mathcal{O}(\sqrt{n})$ bits to Bob in n channel uses.*

We start this letter by introducing our optical channel model and hypothesis testing. We then prove Theorems 1, 2, 3, and 4 in succession, and conclude the letter.

I. PREREQUISITES

Channel model—Consider a single spatial mode free space optical channel, where each channel use corresponds to one signaling interval that carries one modulation symbol. We focus on single-mode quasi-monochromatic propagation, since our results readily generalize to multiple spatial modes (near-field link) and/or a wideband channel with appropriate power-allocation across spatial modes and frequencies [7]. For simplicity of exposition we limit our analysis to vacuum propagation, i.e., we do not address the effect of atmospheric turbulence. The Heisenberg-picture input-output relationship of the single-mode bosonic channel is captured by a 'beamsplitter' relationship, $\hat{b} = \sqrt{\eta}\,\hat{a} + \sqrt{1-\eta}\,\hat{e}$, where $\hat{a}$ and $\hat{b}$ are modal annihilation operators of the input and output modes respectively, and $\eta \in [0,1]$ is the power transmissivity, the fraction of power Alice puts in the input mode that couples into Bob's aperture. Classically, a power attenuation is captured by the relationship $b = \sqrt{\eta}\,a$, where a and b are complex field amplitudes of the input and output mode functions. The quantum description of the channel requires the 'environment' mode $\hat{e}$ in order to preserve the commutator brackets, i.e., $\left[\hat{b}, \hat{b}^\dagger\right] = 1$, which translates to preserving the Heisenberg uncertainty relationship of quantum mechanics. For the pure loss channel, the environment mode $\hat{e}$ is in a *vacuum* state, i.e., $\hat{\rho}^E = |0\rangle\langle 0|^E$. The vacuum state captures the minimum amount of noise that must be injected when 'nothing happens' other than pure power attenuation. For a thermal noise channel, $\hat{e}$ is in a thermal state with mean photon number $N_B > 0$, i.e. $\hat{\rho}^E = \hat{\sigma}^T(N_B)$ where $\hat{\sigma}^T(N_B)$ is a mixture of coherent states weighted by a Gaussian distribution:

$$\hat{\sigma}^T(\bar{n}) = \sum_{i=0}^{\infty} \frac{\bar{n}^i}{(1+\bar{n})^{1+i}} |i\rangle\langle i|^E = \int_{\mathbb{C}} \frac{e^{-\frac{|\alpha|^2}{\bar{n}}}}{\pi\bar{n}} |\alpha\rangle\langle\alpha|^E \mathrm{d}^2\alpha. \tag{1}$$

The mean number of photons injected by the thermal environment is $N_B \approx \pi 10^6 \lambda^3 N_\lambda / \hbar\omega^2$, where N_λ is the background spectral radiance (in W/m^2 sr-μm) [8]. A typical daytime value $N_\lambda \approx 10$ W/m^2 sr-μm at $\lambda = 1.55\mu$m leads to $N_B \approx 10^{-6}$ photons/mode. For $N_B = 0$, the thermal noise channel reduces to the pure loss channel.

Hypothesis Testing—Willie collects part of the transmitted light during the transmission of Alice's n modulation symbols and performs a hypothesis test on whether Alice transmitted or not. Willie's null hypothesis H_0 is that Alice does not transmit, and thus he observes vacuum plus noise photons, injected either by a thermal environment or due to dark current generated by a spontaneous emission process in his own measurement apparatus. His alternate hypothesis H_1 is that Alice transmits.

II. THERMAL NOISE CHANNEL ($N_B > 0$)

We begin by providing a constructive proof of achievability of $\mathcal{O}(\sqrt{n})$ LPD bits in n channel uses: we describe Alice and Bob's communication system and prove that Willie's average probability of detection error is lower-bounded arbitrarily close to $\frac{1}{2}$, while Bob's average probability of codeword decoding error is upper-bounded arbitrarily close to zero.

Proof. *(Theorem 1). Construction:* Let Alice use a zero-mean isotropic Gaussian-distributed coherent state input $\{p(\alpha), |\alpha\rangle\}$, where $\alpha \in \mathbb{C}$, $p(\alpha) = e^{-|\alpha|^2/\bar{n}}/\pi\bar{n}$ with mean photon number per symbol $\bar{n} = \int_{\mathbb{C}} |\alpha|^2 p(\alpha) \mathrm{d}^2\alpha$. Alice encodes M-bit blocks of input into codewords of length n symbols at the rate $R = M/n$ bits/symbol by generating 2^{nR} codewords $\{\bigotimes_{i=1}^{n} |\alpha_i\rangle_k\}_{k=1}^{2^{nR}}$, each according to $p(\bigotimes_{i=1}^{n} |\alpha_i\rangle) = \prod_{i=1}^{n} p(\alpha_i)$, where $\bigotimes_{i=1}^{n} |\alpha_i\rangle = |\alpha_1 \dots \alpha_n\rangle$ is an n-mode tensor-product coherent state. The codebook is used only once to send a single message and is kept secret from Willie, though he knows how it is constructed.[18]

Analysis (Willie): Suppose that Willie captures all of Alice's transmitted energy that does not reach Bob's receiver. This is a fairly strong assumption for a line-of-sight diffraction-limited far-field optical link. Since Willie does not have access to Alice's codebook, the n-channel use average quantum states at Willie's receiver under the two hypotheses are given respectively by the density operators,

$$\hat{\rho}_0^{\otimes n} = \left(\sum_{i=0}^{\infty} \frac{(\eta N_B)^i}{(1+\eta N_B)^{1+i}} |i\rangle \langle i| \right)^{\otimes n}, \text{ and} \tag{2}$$

$$\hat{\rho}_1^{\otimes n} = \left(\sum_{i=0}^{\infty} \frac{((1-\eta)\bar{n} + \eta N_B)^i}{(1+(1-\eta)\bar{n} + \eta N_B)^{1+i}} |i\rangle \langle i| \right)^{\otimes n}. \tag{3}$$

The quantum-limited minimum average probability of error in discriminating the n-copy states $\hat{\rho}_0^{\otimes n}$ and $\hat{\rho}_1^{\otimes n}$ is:

$$\mathbb{P}_{e,\min}^{(w)} = \frac{1}{2}\left[1 - \frac{1}{2}\|\hat{\rho}_1^{\otimes n} - \hat{\rho}_0^{\otimes n}\|_1\right], \tag{4}$$

where $\|\hat{\rho} - \hat{\sigma}\|_1$ is the *trace distance* between states $\hat{\rho}$ and $\hat{\sigma}$. We can lower-bound[19] $\mathbb{P}_{e,\min}^{(w)}$ using quantum Pinsker's Inequality [9, Th. 11.9.2]:

$$\|\hat{\rho} - \hat{\sigma}\|_1 \leq \sqrt{2D(\hat{\rho}\|\hat{\sigma})}, \tag{5}$$

where $D(\hat{\rho}\|\hat{\sigma}) \equiv \mathrm{Tr}\{\hat{\rho}(\ln(\hat{\rho}) - \log(\hat{\sigma}))\}$ is the quantum relative entropy (QRE) between states $\hat{\rho}$ and $\hat{\sigma}$. We thus have:

$$\mathbb{P}_e^{(w)} \geq \mathbb{P}_{e,\min}^{(w)} \geq \frac{1}{2} - \sqrt{\frac{1}{8} D(\hat{\rho}_0^{\otimes n}\|\hat{\rho}_1^{\otimes n})}. \tag{6}$$

Since QRE is additive for tensor product states, $D(\hat{\rho}_0^{\otimes n}\|\hat{\rho}_1^{\otimes n}) = nD(\hat{\rho}_0\|\hat{\rho}_1)$. Since $\hat{\rho}_0$ and $\hat{\rho}_1$ are diagonal in the photon-number basis, the QRE is:

$$D(\hat{\rho}_0\|\hat{\rho}_1) = \eta N_B \ln \frac{(1+(1-\eta)\bar{n}+\eta N_B)\eta N_B}{((1-\eta)\bar{n}+\eta N_B)(1+\eta N_B)} + \\ + \ln \frac{1+(1-\eta)\bar{n}+\eta N_B}{1+\eta N_B}. \tag{7}$$

The details of the derivation of (7) are given in the Supplement. The first two terms of the Taylor series expansion of (7) around $\bar{n} = 0$ are zero and the fourth term is negative. Thus, using Taylor's Theorem we can upper-bound (7) by the third term as follows:

$$D(\hat{\rho}_0\|\hat{\rho}_1) \leq \frac{(1-\eta)^2\bar{n}^2}{2\eta N_B(1+\eta N_B)}. \tag{8}$$

Therefore, setting

$$\bar{n} = \frac{4\epsilon\sqrt{\eta N_B(1+\eta N_B)}}{\sqrt{n}(1-\eta)} \tag{9}$$

ensures that Willie's error probability is lower-bounded by $\mathbb{P}_e^{(w)} \geq \frac{1}{2} - \epsilon$ over n optical channel uses by Alice.

Analysis (Bob): Suppose Bob uses a coherent detection receiver. A homodyne receiver, which is more efficient than a heterodyne receiver in the low photon number regime [4], induces an AWGN channel with noise power $\sigma_b^2 = \frac{2(1-\eta)N_B+1}{4\eta}$. Since Alice uses Gaussian modulation with symbol power $\bar{n}$ defined in (9), we can upper-bound $\mathbb{P}_e^{(b)}$ as follows [2, Eq. (7)]:

$$\mathbb{P}_e^{(b)} \leq \delta = 2^{B_{\text{hom}}(n,\epsilon,\delta) - \frac{n}{2}\log_2\left(1+\bar{n}/2\sigma_{b,\text{hom}}^2\right)}. \tag{10}$$

Substituting the expression for $\bar{n}$ from (9) and σ_b^2, and solving for the maximum number of bits $B_{\text{hom}}(n,\epsilon,\delta)$ that can be transmitted from Alice to Bob in n channel uses, we obtain:

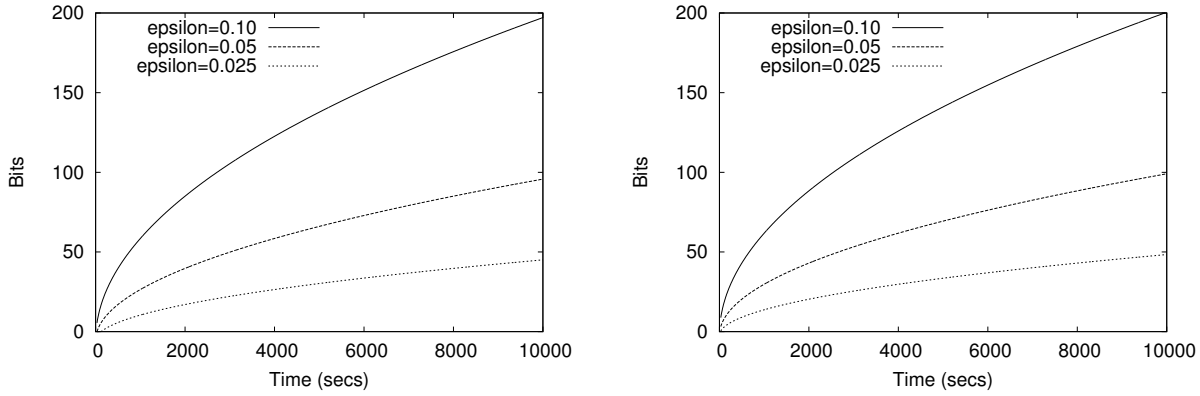
$$B_{\text{hom}}(n,\epsilon,\delta) = C_d(\delta) + \sqrt{n}C_c(\epsilon,\eta,N_B) + \mathcal{O}(1), \tag{11}$$

where $C_d(\delta) = \log_2 \delta$ is the 'cost' of upper-bounding Bob's decoding error probability by $\mathbb{P}_e^{(b)} \leq \delta$, and $C_c(\epsilon,\eta,N_B) = \frac{\epsilon\sqrt{\eta N_B(1+\eta N_B)}}{(1-\eta)} \times \frac{4\eta}{2(1-\eta)N_B+1}$ is the cost of lower-bounding Willie's probability of detection by $\mathbb{P}_{e,\min}^{(w)} \geq \frac{1}{2} - \epsilon$. ■

Remark. Eq. (11) illustrates that while the cost of reducing Bob's decoding error has an additive impact that is insignificant at large enough n, the cost of limiting Willie's detection capabilities is multiplicative and proportional to ϵ. We plot $B_{\text{hom}}(n,\epsilon,\delta)$ using transmissivity $\eta = 0.1$ for various values of ϵ and δ on Figure 1, illustrating the square root law and that the probability of decoding error imposed on Bob has insignificant impact, while the tolerance of being detected by Willie greatly affects the amount of information that can be covertly transmitted. The small number of bits that can be sent across the channel (200 bits in 10,000 seconds, or roughly 2 hours 45 minutes, with $\epsilon = 0.1$) is likely due to the very conservative assumptions we make on Willie's capability.

III. PARTIAL CONVERSE TO THEOREM 1

Here Alice's objective is to transmit a message W_k that is $M = \omega(\sqrt{n})$ bits long to Bob at the rate $R = M/n$ bits/channel use using a codeword containing n pure states with arbitrarily small probability of decoding error as n gets



(a) $\delta = 0.01$ (b) $\delta = 0.10$

FIG. 1: $B_{\text{hom}}(n, \epsilon, \delta)$ plotted for $\eta = 0.1$ and several values of ϵ and δ. Here $N_B = 10^{-6}$ and each modulation symbol duration is 100ps. Figures clearly illustrate that while the choice of δ is hardly noticeable, choice of ϵ has a significant multiplicative impact on the number of covert bits that can be sent across the channel.

large, while limiting Willie's ability to detect her transmission. For an upper bound on the reduction in entropy, the messages are chosen equiprobably. We now show that if Alice violates the square root law by attempting to transmit $\omega(\sqrt{n})$ bits in n channel uses, as $n \to \infty$, she is either detected by Willie with arbitrarily low $\mathbb{P}_e^{(w)}$ or Bob's probability of decoding error is lower-bounded by a positive constant. We restrict Alice to transmitting only the states with bounded photon number variance, that is, for any state $|\psi\rangle = \sum_{k=0}^{\infty} b_k |k\rangle$ that Alice uses, we require that $\sum_{k=0}^{\infty} k^2 |b_k|^2 \leq \sigma_{UB}^2 < \infty$. While we note that all practical states meet this requirement, in the future we would like generalize this result to arbitrary pure states.

Willie uses a simple heterodyne receiver to detect Alice's transmissions. We demonstrate that this is enough to detect with arbitrarily small error probability as $n \to \infty$ those codewords with mean photon number per symbol $\bar{n} = \omega(1/\sqrt{n})$. We then use Fano's inequality to show that when Alice attempts to transmit $\omega(\sqrt{n})$ bits of information, while preventing the upper bound on the error probability of Willie's heterodyne receiver from being arbitrarily close to zero, Bob suffers non-zero decoding error probability.

Proof. *(Theorem 2).* Suppose Alice uses a codebook $\{\Omega_u^A, u = 1, \ldots, 2^{nR}\}$, where a state $\Omega_u^A = \bigotimes_{i=1}^{n} \hat{\rho}_i^A(u)$ encodes message W_u out of M possible messages, with $\hat{\rho}_i^A(u) = |\psi_i(u)\rangle \langle\psi_i(u)|$ and $|\psi_i(u)\rangle = \sum_{k=0}^{\nu_i(u)} b_k^{(i)}(u) |k\rangle$ where $\nu_i(u)$ can, in principle, be infinite. First we analyze Willie's detector and assume that an arbitrary message W_a was transmitted. At each channel use, Willie observes an output state $\hat{\rho}_i^W(a)$ of a thermal noise channel from Alice, where the channel is described by a beamsplitter relationship $\hat{w} = \sqrt{\gamma}\hat{a} + \sqrt{1-\gamma}\hat{e}$ with $\hat{a}$ and $\hat{e}$ being the input and environment modes and $0 < \gamma \leq 1 - \eta$. We subsume any subunity detection efficiency of Willie's heterodyne receiver in γ. Then Willie's hypothesis test reduces to choosing between the states,

$$\hat{\rho}_0^{\otimes n} = \left(\sum_{i=0}^{\infty} \frac{((1-\gamma)N_B)^i}{(1+(1-\gamma)N_B)^{1+i}} |i\rangle \langle i| \right)^{\otimes n}, \text{ and} \quad (12)$$

$$\hat{\rho}_1^{\otimes n} = \bigotimes_{i=1}^{n} \hat{\rho}_i^W(a) \quad (13)$$

where $\hat{\rho}_i^W(a)$ is the output state of a thermal noise channel with transmissivity γ corresponding to an input state $\hat{\rho}_i^A(a)$.

Willie uses a heterodyne receiver and only considers the squared magnitude of the complex output of this receiver (thus discarding the in-phase component of his readings). After collecting a sequence of n such observations of his channel from Alice $\{|y_1|^2, \ldots, |y_n|^2\}$, Willie compares their average $S = \frac{1}{n}\sum_{i=1}^{n} |y_i|^2$ to a threshold. The probability distribution for the test statistic S depends on which hypothesis is true: we denote by $\mathbb{P}_0$ the distribution when H_0 holds with Alice not transmitting, and $\mathbb{P}_1^{(a)}$ when H_1 holds with Alice transmitting message W_a. We first show that Willie's error probabilities $\mathbb{P}_{FA}$ and $\mathbb{P}_{MD}$ can be bounded for this receiver given Alice's codeword parameters. Then we show that if Alice uses a codebook that makes this bound fail, Bob cannot decode her transmissions without error even with an quantum-optimal receiver.

The statistics of heterodyne receiver measurements are given by the Husimi Q representation $Q(\alpha) = \frac{1}{\pi} \langle\alpha| \hat{\rho} |\alpha\rangle$ of the received quantum state $\hat{\rho}$. If the null hypothesis is true and Alice is not transmitting, then Willie observes a sequence of attenuated thermal states, each with mean photon number $(1-\gamma)N_B$. Each squared magnitude of the heterodyne receiver reading is independently and identically distributed (i.i.d.) and the Q-function of the attenuated thermal state is $Q^T(\alpha) = \frac{1}{\pi(1+N_B)} e^{-|\alpha|^2/(1+N_B)}$. Therefore, under the null hypothesis, $\mathbb{E}[S] = 1 + (1-\gamma)N_B$ and $\text{Var}[S] = \frac{(1+(1-\gamma)N_B)^2}{n}$. Since the test statistic S should be close to $1 + (1-\gamma)N_B$ when Alice is not transmitting, Willie

picks a threshold t and compares S to $1+(1-\gamma)N_B+t$. Using the Chebyshev's inequality, we can upper bound the probability of the false alarm as follows:

$$\mathbb{P}_{FA} = \mathbb{P}_0(S \geq 1+(1-\gamma)N_B+t) \tag{14}$$
$$\leq \mathbb{P}_0(|S-(1+(1-\gamma)N_B)| \geq t) \tag{15}$$
$$\leq \frac{(1+(1-\gamma)N_B)^2}{nt^2} \tag{16}$$

Thus, to obtain desired $\mathbb{P}^*_{FA}$, Willie sets $t = \frac{d}{\sqrt{n}}$, where $d = \frac{1+(1-\gamma)N_B}{\sqrt{\mathbb{P}^*_{FA}}}$. Note that the threshold decreases with more observations.

Now, when Alice transmits a codeword $\Omega_a^A = \bigotimes_{i=1}^n \hat{\rho}_i^A(a)$, Willie receives the output state $\bigotimes_{i=1}^n \hat{\rho}_i^W(a)$ of the thermal noise channel with transmissivity γ. Since the output state is a tensor product, the heterodyne detector readings are independent but not identical. The expected squared magnitude of each reading is:

$$\mathbb{E}[|y_i|^2] = \int_{\mathbb{C}} |\alpha|^2 Q^W_{|\psi_i(a)\rangle}(\alpha) d^2\alpha \tag{17}$$
$$= 1+(1-\gamma)N_B+\gamma\bar{n}_i(a) \tag{18}$$

where $\bar{n}_i(a) = \sum_{k=0}^{\nu_i(a)} k b_k^{(i)}(a)$ denotes the mean photon number of state $\hat{\rho}_i^A(a)$ and $Q^W_{|\psi_i(a)\rangle}(\alpha)$ is the Q representation of $\hat{\rho}_i^W(a)$. Similarly, the variance is:

$$\mathrm{Var}[|y_i|^2] = \gamma^2\sigma_i^2(a) + c_1\bar{n}_i(a) + c_2 \tag{19}$$

where $\sigma_i^2(a) = \mu_i^{(2)}(a) - (\bar{n}_i(a))^2$ denotes the photon number variance of $\hat{\rho}_i^A(a)$, and $c_1 = 2\gamma((2+N_B)(1-\gamma)-1)$, $c_2 = (1+(1-\gamma)N_B)^2$. To obtain $Q^W_{|\psi_i(a)\rangle}(\alpha)$, we convolve [20] the Q representation of the thermal environment $Q^T(\alpha)$ with that of the input state $|\psi_i(a)\rangle$,

$$Q^A_{|\psi_i(a)\rangle}(\alpha) = \frac{1}{\pi}\sum_{k=0}^{\nu_i(a)}\sum_{l=0}^{\nu_i(a)} b_k^{(i)}(a)\left(b_l^{(i)}(a)\right)^* \frac{(\alpha^*)^k\alpha^l}{\sqrt{k!l!}} e^{-|\alpha|^2}, \tag{20}$$

using [10, Eq. (2.17)], with the details of the derivation of (18) and (19) in the supplement. Since the photon number variance of $\hat{\rho}_i^A(a)$ is bounded by σ_{UB}^2, we have $\sigma_i^2(a) \leq \sigma_{UB}^2$. Denoting the average photon number of the codeword Ω_a by $\bar{n}(a) = \frac{1}{n}\sum_{i=1}^n \bar{n}_i(a)$, the probability of missing the detection of codeword Ω_a can thus be bounded using Chebyshev's inequality as follows:

$$\mathbb{P}^{(a)}_{MD} = \mathbb{P}^{(a)}_1(S < 1+(1-\gamma)N_B+t) \tag{21}$$
$$\leq \mathbb{P}^{(a)}_1(|S-1-(1-\gamma)N_B-\gamma\bar{n}(a)| \geq \gamma\bar{n}(a)-t) \tag{22}$$
$$\leq \frac{\sum_{i=1}^n \gamma^2\sigma_i^2(a)+c_1\bar{n}_i(a)+c_2}{n^2\left(\gamma\bar{n}(a)-t\right)^2} \tag{23}$$
$$\leq \frac{\gamma\sigma_{UB}^2+c_1\bar{n}(a)}{\left(\gamma\sqrt{n}\bar{n}(a)-d\right)^2} \tag{24}$$

If the average photon number $\bar{n}(a) = \omega(1/\sqrt{n})$, $\lim_{n\to\infty}\mathbb{P}^{(a)}_{MD} = 0$. Thus, given enough observations, Willie can detect Alice's codewords that have the average photon number $\bar{n}(a) = \omega(1/\sqrt{n})$ with arbitrarily low probability of error $\mathbb{P}_e^{(w)}$. Note that not only is Willie oblivious to any details about Alice's codebook construction, but he also only needs a simple heterodyne detector to detect Alice.

Now, only when the transmitted codeword has average photon number $\bar{n}_{\mathcal{U}} = \mathcal{O}(1/\sqrt{n})$, the upper bound in (24) fails to approach zero as $n\to\infty$. In other words, if Alice wants to lower-bound $\mathbb{P}_e^{(w)}$, her codebook must contain a positive fraction κ of such low photon number codewords. Denote the subset of messages that have codewords with the average photon number $\bar{n}_{\mathcal{U}} = \mathcal{O}(1/\sqrt{n})$ by $\mathcal{U}$. Let's examine Bob's probability of decoding error $\mathbb{P}_e^{(b)}$. Denote by $E_{a\to k}$ the event that a transmitted message W_a is decoded as $W_k \neq W_a$. Since the messages are equiprobable, the average probability of error for the codebook containing only the codewords in $\mathcal{U}$ is as follows:

$$\mathbb{P}_e^{(b)}(\mathcal{U}) = \frac{1}{|\mathcal{U}|}\sum_{W_a\in\mathcal{U}} \mathbb{P}\left(\cup_{W_k\in\mathcal{U}\setminus\{W_a\}} E_{a\to k}\right), \tag{25}$$

where $|\cdot|$ is the set cardinality operator. The probability of Bob's decoding error is lower-bounded by $\mathbb{P}_e^{(b)} \geq \kappa\mathbb{P}_e^{(b)}(\mathcal{U})$, since the equality holds only when Bob errorlessly receives messages that are not in $\mathcal{U}$ and knows when the messages from $\mathcal{U}$ are sent (in other words, the equality holds with the set of messages on which decoder can err is reduced to $\mathcal{U}$). The probability that a message is sent from $\mathcal{U}$ is κ, which means that if Alice's coding rate is R, then there are $\kappa 2^{nR}$ messages in $\mathcal{U}$. Denote by $W_a \in \mathcal{U}$ the message transmitted by Alice, and by $\hat{W}_a$ Bob's decoding of W_a. Then, since each message is equiprobable,

$$\log_2\kappa + nR = H(W_a) \tag{26}$$
$$= I(W_a;\hat{W}_a) + H(W_a|\hat{W}_a) \tag{27}$$
$$\leq I(W_a;\hat{W}_a) + 1 + (\log_2\kappa+nR)\mathbb{P}_e^{(b)}(\mathcal{U}) \tag{28}$$
$$\leq \chi(\{\frac{1}{|\mathcal{U}|};\Omega_u^A\}) + 1 + (\log_2\kappa+nR)\mathbb{P}_e^{(b)}(\mathcal{U}) \tag{29}$$

where (27) is from the definition of mutual information, (28) is due to classical Fano's inequality [11, Eq. (9.37)], and (29) is the Holevo's bound $I(X;Y) \leq \chi(\{p_i,\hat{\rho}_i\})$, with $\chi(\{p_i,\hat{\rho}_i\})$ being the Holevo information for a channel with input alphabet X, $\{p_i,\hat{\rho}_i\}$ the priors and the modulating states, and Y the resulting output alphabet (assuming a POVM $\{\Pi_j\}$) [12]. Since the Holevo information of a single-mode bosonic channel with mean photon number constraint is maximized by a coherent state ensemble with a zero-mean circularly-symmetric Gaussian distribution [4], we have:

$$\log_2\kappa + nR \leq \chi\left((\hat{\rho}^B)^{\otimes n}\right) + 1 + (\log_2\kappa+nR)\mathbb{P}_e^{(b)}(\mathcal{U}) \tag{30}$$

where $\hat{\rho}^B = \hat{\sigma}^T(\eta\bar{n}_{\mathcal{U}})$, with $\hat{\sigma}^T(\bar{n})$ defined in (1). Now, $\chi(\hat{\rho}^B) = H(\hat{\rho}^B)$ since coherent states are pure, and $\chi\left((\hat{\rho}^B)^{\otimes n}\right) = n\left(\log_2(1+\eta\bar{n}_{\mathcal{U}}) + \eta\bar{n}_{\mathcal{U}}\log_2\left(1+\frac{1}{\eta\bar{n}_{\mathcal{U}}}\right)\right)$ is due to the additivity of the Holevo information across the modes of the bosonic channels. This implies:

$$\mathbb{P}_e^{(b)}(\mathcal{U}) \geq 1 - \frac{\log_2(1+\eta\bar{n}_{\mathcal{U}}) + \eta\bar{n}_{\mathcal{U}}\log_2\left(1+\frac{1}{\eta\bar{n}_{\mathcal{U}}}\right) + \frac{1}{n}}{\frac{\log_2\kappa}{n} + R} \tag{31}$$

Since Alice transmits $\omega(\sqrt{n})$ bits in n channel uses, her rate is $R = \omega(1/\sqrt{n})$ bits/symbol. However, $\bar{n}_{\mathcal{U}} = \mathcal{O}(1/\sqrt{n})$, and, as $n \to \infty$, $\mathbb{P}_e^{(b)}(\mathcal{U})$ is bounded away from zero. Since $\kappa > 0$, $\mathbb{P}_e^{(b)}$ is also bounded away from zero when Alice tries to transmit $\omega(\sqrt{n})$ bits in n channel uses while beating Willie's heterodyne receiver. ■

IV. PURE LOSS CHANNEL ($N_B = 0$) WITH QUANTUM-POWERFUL WILLIE

Now we prove that Alice and Bob cannot hide their communication from Willie if Willie has a pure loss channel from Alice and a choice of a receiver restricted only by the laws of quantum physics. First, we let Willie pick a receiver that does not necessarily capture all the transmitted energy that does not reach Bob's receiver. Alice uses an arbitrary pure state codebook. While Willie is oblivious to its structure, we show that Alice must constrain her codewords to limit the detection capability of Willie's particular receiver. We then show that this constraint prevents Bob from decoding Alice's transmissions without error, proving the theorem.

Proof. *(Theorem 3).* Suppose Alice uses a codebook where a state $\Omega_u^A = \bigotimes_{i=1}^n \hat{\rho}_i^A(u)$ encodes message W_u out of M possible messages, with $\hat{\rho}_i^A(u) = |\psi_i(u)\rangle\langle\psi_i(u)|$ and $|\psi_i(u)\rangle = \sum_{k=0}^{\nu_i(u)} a_k^{(i)}(u)|k\rangle$ where $\nu_i(u)$ can, in principle, be infinite. First we analyze Willie's detector and assume that an arbitrary message W_a was transmitted. Willie captures a fraction of the transmitted energy, γ, where $0 < \gamma \leq 1-\eta$. Then Willie's hypothesis test reduces to choosing between the states,

$$\hat{\rho}_0^{\otimes n} = |0\rangle\langle 0|^{\otimes n}, \text{ and} \tag{32}$$

$$\hat{\rho}_1^{\otimes n} = \bigotimes_{i=1}^n \hat{\rho}_i^W(a) \tag{33}$$

where $\hat{\rho}_i^W(a)$ is the output state of a pure loss channel with transmissivity γ corresponding to an input state $\hat{\rho}_i^A(a)$. Let Willie use an ideal single photon sensitive direct detection receiver given by positive operator-valued measure (POVM) $\left\{|0\rangle\langle 0|, \sum_{j=1}^\infty |j\rangle\langle j|\right\}^{\otimes n}$ over all n channel uses. Then Willie's probability of error is

$$\mathbb{P}_e^{(w)}(a) = \frac{1}{2}\prod_{i=1}^n \langle 0|\hat{\rho}_i^W(a)|0\rangle. \tag{34}$$

Note that the error is entirely due to the missed codeword detections, as Willie's receiver detects vacuum perfectly and never raises a false alarm.

The diagonal elements of $\hat{\rho}_i^W(a)$ expressed in the photon number basis are as follows (see Supplement for derivation):

$$\langle s|\hat{\rho}_i^W(a)|s\rangle = \sum_{k=0}^{\nu_i(a)} \left|a_k^{(i)}(a)\right|^2 \binom{k}{s}(1-\gamma)^{k-s}\gamma^s \tag{35}$$

Therefore,

$$\langle 0|\hat{\rho}_i^W(a)|0\rangle = \sum_{k=0}^{\nu_i(a)} \left|a_k^{(i)}(a)\right|^2 (1-\gamma)^k \tag{36}$$

$$\leq \left|a_0^{(i)}(a)\right| + (1-\left|a_0^{(i)}(a)\right|^2)(1-\gamma) \tag{37}$$

$$= 1-\gamma\left(1-\left|a_0^{(i)}(a)\right|^2\right) \tag{38}$$

Thus, substituting (38) into (34) and using the Taylor series expansion of $\log(1-x)$ yields:

$$\mathbb{P}_e^{(w)} \leq \frac{1}{2}\exp\left[-\gamma\sum_{i=1}^n\left(1-\left|a_0^{(i)}\right|^2\right)\right], \tag{39}$$

implying that Alice must set $\sum_{i=1}^n\left(1-\left|a_0^{(i)}(a)\right|^2\right) = c_a$, with c_a a constant, for every codeword in her codebook with a positive probability of being transmitted. Next we show that the codewords constructed this way are "too close" to one another to allow reliable communication.

Let's analyze Bob's receiver. Denote by p_u the *a priori* probability that W_u is transmitted. Then, given that W_u is transmitted, the probability of the decoding error is the probability of the union of events $\cup_{v=0,v\neq u}^n E_v$, where E_v is the event that the received state is decoded as $\hat{W} = W_v$, $v \neq u$. Let Bob choose a POVM $\{\Lambda_j\}$ that minimizes the average probability of error:

$$\mathbb{P}_e^{(b)} = \inf_{\{\Lambda_j\}}\sum_{u=1}^M p_u\mathbb{P}\left(\cup_{v=0,v\neq u}^n E_v|W_u \text{ sent}\right) \tag{40}$$

Now, any scheme used to transmit a positive number of bits has to have at least two messages with positive prior transmission probabilities. Thus, let's pick a pair of messages $\{W_r, W_s\}$ from Alice's codebook with a positive prior probabilities $\{p_r > 0, p_s > 0\}$ of transmission. Then we have:

$$\mathbb{P}_e^{(b)} \geq p_r\mathbb{P}\left(E_s|W_r \text{ sent}\right) + p_s\mathbb{P}\left(E_r|W_s \text{ sent}\right) \tag{41}$$

$$= (p_r+p_s)\mathbb{P}_e^{r\leftrightarrow s} \tag{42}$$

The lower bound in (41) is due to the exclusion of a non-negative elements from the sum in (40), as well as the events E_r and E_s being contained in the unions $\cup_{v=0,v\neq r}^n E_v$ and $\cup_{v=0,v\neq s}^n E_v$, respectively. In (42) we reduced the analytically intractable problem of discriminating between many states in (40) to a quantum binary hypothesis test, since $\mathbb{P}_e^{r\leftrightarrow s} \equiv$

$\frac{p_r}{p_r+p_s}\mathbb{P}\left(E_s|W_r \text{ sent}\right) + \frac{p_s}{p_r+p_s}\mathbb{P}\left(E_r|W_s \text{ sent}\right)$ is Bob's average probability of error in a scenario where Alice only sends messages W_r and W_s with priors proportional to p_r and p_s. We note that the probabilities are with respect to the POVM $\{\Lambda_j\}$ that minimizes (40) over the entire codebook, and thus may be suboptimal for a test between W_r and W_s.

Recall that Alice transmits messages by sending codewords through a single mode lossy bosonic channel. The lower bound on the probability of error in discriminating two received states can be obtained by lower-bounding the probability of error in discriminating two codewords *before* they are sent (this is equivalent to Bob having a channel from Alice with unity transmissivity). Since the codewords are tensor products of pure states, we can apply the Helstrom bound [13, Eq. 2.34] for discriminating pure states as follows:

$$\mathbb{P}_e^{r\leftrightarrow s} \geq \frac{\left(1-\sqrt{1-\frac{4p_rp_s}{(p_r+p_s)^2}\prod_{i=1}^{n}\left|\langle\psi_i(r)|\psi_i(s)\rangle\right|^2}\right)}{2} \tag{43}$$

Lower bounding $\prod_{i=1}^{n}\left|\langle\psi_i(r)|\psi_i(s)\rangle\right|^2$ yields the lower bound on (43). Now, $\prod_{i=1}^{n}\left|\langle\psi_i(r)|\psi_i(s)\rangle\right|^2$ is the fidelity $F(\Omega_r^A,\Omega_s^A)$ between the pure state codewords Ω_r^A and Ω_s^A, which can be represented using the trace distance as follows:

$$F(\Omega_r^A,\Omega_s^A) = 1-\frac{1}{4}\|\Omega_r^A-\Omega_s^A\|_1^2 \tag{44}$$

$$\geq 1-\frac{(\|\Omega_r^A-\Omega_0\|_1+\|\Omega_s^A-\Omega_0\|_1)^2}{4} \tag{45}$$

where $\Omega_0 = |0\rangle\langle 0|^{\otimes n}$ is the vacuum codeword and (45) is due to the triangle inequality for trace distance. To lower bound (45), we can upper bound the respective trace distances between codewords and vacuum using fidelity as follows:

$$\|\Omega_r^A-\Omega_0\|_1 \leq \sqrt{1-\prod_{i=1}^{n}\left|\langle 0|\psi_i(r)\rangle\right|^2} \tag{46}$$

$$= \sqrt{1-e^{\sum_{i=1}^{n}\log(1-(1-|\langle 0|\psi_i(r)\rangle|^2))}} \tag{47}$$

$$\leq \sqrt{1-e^{-(c_r+\mathcal{O}(c_r^2))}} \tag{48}$$

where (48) follows from the Taylor series expansion of $\log(1-x)$, the fact that $|\langle 0|\psi_i(r)\rangle|^2) = \left|a_0^{(i)}(r)\right|^2$, the fact that Alice has to set $\sum_{i=1}^{n}\left(1-\left|a_0^{(i)}(r)\right|^2\right) = c_r$ for some constant c_r to avoid detection by Willie, and that the square of the sum is greater than the sum of the squares when the sequence contains only non-negative numbers. Analogously,

$$\|\Omega_s^A-\Omega_0\|_1 \leq \sqrt{1-e^{-(c_s+\mathcal{O}(c_s^2))}}. \tag{49}$$

Combining (42), (43), (45), (48) and (49) yields:

$$\mathbb{P}_e^{(b)} \geq \frac{p_r+p_s}{2}\left(1-\sqrt{1-\frac{4p_rp_s}{(p_r+p_s)^2}\left(1-\frac{1}{4}\left(\sqrt{1-e^{-(c_r+\mathcal{O}(c_r^2))}}+\sqrt{1-e^{-(c_s+\mathcal{O}(c_s^2))}}\right)^2\right)}\right) \tag{50}$$

Therefore, by (50), the probability of error is bounded away from zero as the codeword length $n\to\infty$ and reliable covert communication is not possible using pure states when Willie has a pure loss channel from Alice and ability to construct an ideal single photon sensitive direct detection receiver. ■

We have shown above that there exists a quantum measurement that Willie can employ to prevent Alice from covertly using a pure loss channel. However, Alice's situation is not completely hopeless, since the ideal direct detection is nearly impossible to realize in practice.

V. PURE LOSS CHANNEL ($N_B = 0$) WITH WILLIE LIMITED BY PRACTICAL RECEIVER

Let us reconsider the pure loss channel but assume that Willie's photon counting receiver registers a Poisson dark count process with rate λ_d. On each symbol interval (channel use) of τ seconds, the probability of a dark count at Willie's receiver $p_d \approx \lambda_d\tau$. For instance, $p_d = 10^{-7}$ for a typical superconducting nanowire detector with 100 counts/sec dark count rate and 1 ns time slots. The constructive structure of the proof below is similar to that of Theorem 1.

Proof. *(Theorem 4).* Let Alice use a coherent state on-off keying (OOK) modulation $\{\pi_i, S_i = |\psi_i\rangle\langle\psi_i|\}$, $i = 1, 2$, where $\pi_1 = 1-q$, $\pi_2 = q$, $|\psi_1\rangle = |0\rangle$, $|\psi_2\rangle = |\alpha\rangle$. When Alice transmits $|\alpha\rangle$, Bob receives $|\sqrt{\eta}\alpha\rangle$. Alice and Bob generate a random codebook with each codeword symbol chosen i.i.d. from the above binary OOK constellation. Since the codebook is kept secret from Willie, Willie observes a sequence of n i.i.d. Bernoulli random variables $\{X_i\}$, $1 \leq i \leq n$, where X_i denotes the output of Willie's receiver on the i^{th} observation. When Alice is not transmitting (i.e., when H_0 is true), the distribution of X_i is $\mathbb{P}_0 = \text{Bernoulli}(p_d)$. When Alice is transmitting a codeword (i.e. when H_1 is true), it is $\mathbb{P}_1 = \text{Bernoulli}(p_d + q(1-p_d)(1-e^{-(1-\eta)|\alpha|^2}))$ since, as in the proof of Theorem 1, Willie captures all of the transmitted energy that does not reach Bob's receiver and

$|\langle\sqrt{1-\eta}\alpha|0\rangle|^2 = e^{-(1-\eta)|\alpha|^2}$.

Willie's hypothesis test here is classical and we can thus use the classical relative entropy (CRE) as we do for the AWGN channel in [2, 3] to lower-bound $\mathbb{P}_e^{(w)}$. CRE is given by $\mathcal{D}(\mathbb{P}_0\|\mathbb{P}_1) = \sum_{x\in\mathcal{X}} p_0(x)\log\frac{p_0(x)}{p_1(x)}$ where $p_0(x)$ and $p_1(x)$ are the respective densities of $\mathbb{P}_0$ and $\mathbb{P}_1$, and $\mathcal{X}$ is the support of $p_1(x)$. CRE is additive for independent distributions, and lower-bounds $\mathbb{P}_e^{(w)} \geq \frac{1}{2} - \sqrt{\frac{n}{8}\mathcal{D}(\mathbb{P}_0\|\mathbb{P}_1)}$. The Taylor series expansion of $\mathcal{D}(\mathbb{P}_0\|\mathbb{P}_1)$ around $|\alpha|^2 = 0$ yields (via Taylor's Theorem) the following upper bound:

$$\mathcal{D}(\mathbb{P}_0\|\mathbb{P}_1) \leq \frac{(1-p_d)(q(1-\eta)|\alpha|^2)^2}{2p_d} \tag{51}$$

Thus, to ensure that $\mathbb{P}_e^{(w)} \geq \frac{1}{2} - \epsilon$, Alice can set her average symbol power to

$$\bar{n} = q|\alpha|^2 = \frac{4\epsilon}{\sqrt{n}(1-\eta)}\sqrt{\frac{p_d}{1-p_d}} \tag{52}$$

This allows Alice to transmit $\mathcal{O}(\sqrt{n})$ covert bits reliably to Bob if he also uses a direct detection receiver. The details of the reliability proof are available in the Supplement. ■

Theorems 1 and 4 suggest that some form of noise in the adversary's measurements, however small, is essential in making LPD communication possible, as LPD communication masquerades as noise. The nature of the noise appears to be immaterial. It can come from the thermal environment, be Johnson noise, or be generated locally at the adversary's receiver as dark current due to a spontaneous emission process.

Essentially, Alice takes advantage of Willie's measurement noise by transmitting messages, which, when mixed with noise, closely resemble the noise that Willie expects to see on his channel when Alice is quiet. Bob also has to deal with noise in his measurements while decoding, but he has a crucial advantage over Willie: his knowledge of the codebook allows him to reduce the size of his search space, allowing him to compare only the codewords to their received noisy versions.

VI. CONCLUSION

We demonstrated that, provided Willie experiences noise in his measurements (either due to thermal noise in the channel or excess local noise in his receiver), Alice can transmit $\mathcal{O}(\sqrt{n})$ bits in n channel uses to Bob such that Bob's average decoding error probability approaches zero as n gets large while Willie's average probability of detection error is lower-bounded arbitrarily close to $\frac{1}{2}$. Surprisingly, this scaling law holds even if Willie obtains a quantum-optimal joint-detection measurement over n channel uses and Alice's transmissions are subject to thermal noise on the channel. We also showed that in the absence of any excess noise in Willie's measurements (i.e., on a pure loss channel and an ideal detector for Willie), reliable LPD communication is not possible.

The full converses of Theorems 1 and 4 are open problems that we plan on tackling in the future work.

[1] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook* (McGraw-Hill, 1994), revised ed., ISBN 9780070576292.

[2] B. A. Bash, D. Goeckel, and D. Towsley, IEEE Journal on Selected Areas in Communications **31**, 1921 (2013).

[3] B. A. Bash, D. Goeckel, and D. Towsley, in *Proc. of IEEE International Symposium on Information Theory (ISIT)* (Cambridge, MA, 2012).

[4] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, Phys. Rev. Lett. **92**, 027902 (2004).

[5] S. Guha, Phys. Rev. Lett. **106**, 240502 (2011).

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

[7] J. H. Shapiro, S. Guha, and B. I. Erkmen, Journal of Optical Networking **4**, 501 (2005).

[8] N. Kopeika and J. Bordogna, Proc. of the IEEE **58**, 1571 (1970), ISSN 0018-9219.

[9] M. M. Wilde, *From Classical to Quantum Shannon Theory*, arXiv:1106.1445 (2011).

[10] M. S. Kim and N. Imoto, Phys. Rev. A **52**, 2401 (1995).

[11] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (John Wiley & Sons, Hoboken, NJ, 2002), 2nd ed.

[12] A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).

[13] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, Inc., New York, 1976).

[14] C. E. Shannon, Bell System Technical Journal **28**, 656 (1949).

[15] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography* (CRC Press, Inc., Boca Raton, FL, USA, 1996), 1st ed., ISBN 0849385237.

[16] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products* (Elsevier Academic Press, 2007), 7th ed.

[17] R. G. Gallager, *Information Theory and Reliable Communication* (John Wiley and Sons, Inc., New York, 1968).

[18] Conceptually, the codebook is similar to a one-time pad [14] and the shared secret requirement follows 'best practices' in security system design where the security of the system depends only on the secret key [15].

[19] Since $\hat{\rho}_0$ and $\hat{\rho}_1$ are diagonal in the number basis, Willie's quantum-optimal measurement to discriminate $\hat{\rho}_0^{\otimes n}$ and $\hat{\rho}_1^{\otimes n}$ is an ideal photon number resolving direct detection receiver with POVM elements given by the photon number operators $\{|i\rangle\langle i|\}$, $i \in \{0, 1, \ldots\}$. We can derive $\mathbb{P}_{e,\min}^{(w)}$ exactly, however, Pinsker's Inequality is simple and sufficient for the bound we need.

[20] Since the Q representation is not a probability distribution but a quasiprobability, the standard convolution law for the probability distributions does not apply. Given the beamsplitter relationship $\hat{w} = \sqrt{\gamma}\hat{a} + \sqrt{1-\gamma}\hat{e}$ between the input modes a and b, and the output mode w, the Husimi Q function $Q_w(\alpha) = \frac{1}{1-\gamma}\int_{\mathbb{C}} Q_a(\beta)Q_b\left(\frac{\alpha-\sqrt{\gamma}\beta}{\sqrt{1-\gamma}}\right)d^2\beta$ [10, Eq. (2.17)].

Supplementary material

1. Derivation of (7)

Quantum relative entropy $D(\rho\|\sigma) \equiv \mathrm{Tr}\{\rho(\ln(\rho) - \log(\sigma))\} = -\mathrm{Tr}\{\rho(\ln(\sigma))\} - H(\rho)$, where $H(\rho)$ is the von Neumann entropy of the state ρ. Both ρ_0 and ρ_1 are diagonal in the photon-number basis, which greatly simplifies the calculation of the QRE. First, let's calculate $-H(\rho_0)$:

$$\begin{aligned}
-H(\rho_0) &= \mathrm{Tr}\left[\left(\sum_{n=0}^{\infty} \frac{(\eta N_B)^n}{(1+\eta N_B)^{1+n}} |n\rangle\langle n|\right)\left(\sum_{n=0}^{\infty} \ln \frac{(\eta N_B)^n}{(1+\eta N_B)^{1+n}} |n\rangle\langle n|\right)\right] \\
&= \sum_{n=0}^{\infty} \frac{(\eta N_B)^n}{(1+\eta N_B)^{1+n}} \ln \frac{(\eta N_B)^n}{(1+\eta N_B)^{1+n}} \qquad (53) \\
&= \frac{1}{1+\eta N_B} \ln \frac{1}{1+\eta N_B} \sum_{n=0}^{\infty} \left(\frac{\eta N_B}{1+\eta N_B}\right)^n + \\
&\quad + \ln \frac{\eta N_B}{1+\eta N_B} \sum_{n=0}^{\infty} n \frac{1}{1+\eta N_B} \left(\frac{\eta N_B}{1+\eta N_B}\right)^n \qquad (54) \\
&= \ln \frac{1}{1+\eta N_B} + \eta N_B \ln \frac{\eta N_B}{1+\eta N_B} \qquad (55)
\end{aligned}$$

where (55) is due to geometric series $\sum_{n=0}^{\infty}\left(\frac{\eta N_B}{1+\eta N_B}\right)^n = \left(1 - \frac{\eta N_B}{1+\eta N_B}\right)^{-1}$ and $\sum_{n=0}^{\infty} n \frac{1}{1+\eta N_B}\left(\frac{\eta N_B}{1+\eta N_B}\right)^n = \eta N_B$ being the expression for the mean of geometrically distributed random variable $X \sim \mathrm{Geom}\left(\frac{1}{1+\eta N_B}\right)$. We can compute $-\mathrm{Tr}[\rho_0 \ln(\rho_1)]$ using similar techniques:

$$\begin{aligned}
-\mathrm{Tr}[\rho_0 \ln(\rho_1)] &= -\sum_{n=0}^{\infty} \frac{(\eta N_B)^n}{(1+\eta N_B)^{1+n}} \ln \frac{((1-\eta)\bar{n} + \eta N_B)^n}{(1+(1-\eta)\bar{n}+\eta N_B)^{1+n}} \qquad (56) \\
&= -\frac{1}{1+\eta N_B} \ln \frac{1}{1+(1-\eta)\bar{n}+\eta N_B} \sum_{n=0}^{\infty} \left(\frac{\eta N_B}{1+\eta N_B}\right)^n - \\
&\quad - \ln \frac{(1-\eta)\bar{n}+\eta N_B}{1+(1-\eta)\bar{n}+\eta N_B} \sum_{n=0}^{\infty} n \frac{1}{1+\eta N_B} \cdot \left(\frac{\eta N_B}{1+\eta N_B}\right)^n \qquad (57) \\
&= -\ln \frac{1}{1+(1-\eta)\bar{n}+\eta N_B} - \eta N_B \ln \frac{(1-\eta)\bar{n}+\eta N_B}{1+(1-\eta)\bar{n}+\eta N_B} \qquad (58)
\end{aligned}$$

2. Derivation of (18) and (19)

To obtain (18) and (19) we need the Q representation of the output state observed by Willie $\hat{\rho}_i^W(a)$. Given the beamsplitter relationship $\hat{w} = \sqrt{\gamma}\hat{a} + \sqrt{1-\gamma}\hat{e}$ between the input modes a and b, and the output mode w, the Husimi Q function $Q_w(\alpha) = \frac{1}{1-\gamma}\int_{\mathbb{C}} Q_a(\beta) Q_b\left(\frac{\alpha - \sqrt{\gamma}\beta}{\sqrt{1-\gamma}}\right) d^2\beta$ [10, Eq. (2.17)]. One of our input modes is the thermal environment $\hat{\rho}^E$ with the Q representation

$$Q^T(\alpha) = \frac{1}{\pi(1+N_B)} e^{-|\alpha|^2/(1+N_B)}. \qquad (59)$$

The other input mode is Alice's input state $\hat{\rho}_i^A(a) = |\psi_i(a)\rangle\langle\psi_i(a)|$ with the Q representation

$$Q^A_{|\psi_i(a)\rangle}(\alpha) = \frac{1}{\pi} \sum_{k=0}^{\nu_i(a)} \sum_{l=0}^{\nu_i(a)} b_k^{(i)}(a) \left(b_l^{(i)}(a)\right)^* \frac{(\alpha^*)^k \alpha^l}{\sqrt{k!l!}} e^{-|\alpha|^2}, \qquad (60)$$

Using [10, Eq. (2.17)], we have:

$$Q^W_{|\psi_i(a)\rangle}(\alpha) = \frac{1}{(1+N_B)(1-\gamma)\pi^2}\int_{\mathbb{C}} e^{-\frac{|\alpha-\sqrt{\gamma}\beta|^2}{(1-\gamma)(1+N_B)}-|\beta|^2}\left(\sum_{k=0}^{\nu_i(a)}\frac{|b_k^{(i)}(a)|^2|\beta|^{2k}}{k!}+\sum_{k=0}^{\nu_i(a)}\sum_{l=0,l\neq k}^{\nu_i(a)}\frac{b_k^{(i)}(a)(b_l^{(i)}(a))^*(\beta^*)^k\beta^l}{\sqrt{k!l!}}\right)d^2\beta \tag{61}$$

$$= \sum_{k=0}^{\nu_i(a)}\frac{|b_k^{(i)}(a)|^2}{(1+N_B)(1-\gamma)\pi^2 k!}\int_0^\infty\int_0^{2\pi} e^{-\frac{r_\alpha^2+\gamma r_\beta^2-2\sqrt{\gamma}r_\alpha r_\beta\cos(\theta_\alpha-\theta_\beta)}{(1-\gamma)(1+N_B)}-r_\beta^2}r_\beta^{2k+1}d\theta_\beta dr_\beta + \sum_{k=0}^{\nu_i(a)}\sum_{l=0,l\neq k}^{\nu_i(a)}\frac{b_k^{(i)}(a)(b_l^{(i)}(a))^*}{(1+N_B)(1-\gamma)\pi^2\sqrt{k!l!}}\int_0^\infty\int_0^{2\pi} e^{-\frac{r_\alpha^2+\gamma r_\beta^2-2\sqrt{\gamma}r_\alpha r_\beta\cos(\theta_\alpha-\theta_\beta)}{(1-\gamma)(1+N_B)}-r_\beta^2}r_\beta^{k+l+1}e^{j(l-k)\theta_\beta}d\theta_\beta dr_\beta \tag{62}$$

$$= \sum_{k=0}^{\nu_i(a)}\frac{2|b_k^{(i)}(a)|^2}{(1+N_B)(1-\gamma)\pi k!}\int_0^\infty e^{-\frac{r_\alpha^2+(1+(1-\gamma)N_B)r_\beta^2}{(1-\gamma)(1+N_B)}}I_0\left(\frac{2\sqrt{\gamma}r_\alpha r_\beta}{(1-\gamma)(1+N_B)}\right)r_\beta^{2k+1}dr_\beta + \sum_{k=0}^{\nu_i(a)}\sum_{l=0,l\neq k}^{\nu_i(a)}\frac{2b_k^{(i)}(a)(b_l^{(i)}(a))^*}{(1+N_B)(1-\gamma)\pi\sqrt{k!l!}}\int_0^\infty e^{-\frac{r_\alpha^2+(1+(1-\gamma)N_B)r_\beta^2}{(1-\gamma)(1+N_B)}}I_{l-k}\left(\frac{2\sqrt{\gamma}r_\alpha r_\beta}{(1-\gamma)(1+N_B)}\right)r_\beta^{k+l+1}e^{j(l-k)\theta_\alpha}dr_\beta \tag{63}$$

where in (62) we substituted the polar form of complex variables $\alpha = r_\alpha e^{j\theta_\alpha}$ and $\beta = r_\beta e^{j\theta_\beta}$ as well as changed the order of integration and summation. The latter is justified by Tonelli's theorem, as Q-functions are positive. (63) is due to the integral-based definition of the modified Bessel function of the first kind $I_n(z) = \frac{1}{\pi}\int_0^\pi e^{z\cos\theta}\cos(n\theta)d\theta$.

We obtain the expected squared magnitude of heterodyne detector reading when Alice transmits $\hat{\rho}_i^A(a)$ using (63):

$$\mathbb{E}[|y_i|^2] = \int_{\mathbb{C}}|\alpha|^2 Q^W_{|\psi_i(a)\rangle}(\alpha)d^2\alpha \tag{64}$$

$$= \int_0^\infty\int_0^{2\pi} r_\alpha^3 Q^W_{|\psi_i(a)\rangle}(r_\alpha e^{j\theta_\alpha})d\theta_\alpha dr_\alpha \tag{65}$$

$$= \sum_{k=0}^{\nu_i(a)}|b_k^{(i)}(a)|^2(1+(1-\gamma)N_B+\gamma k) \tag{66}$$

$$= 1+(1-\gamma)N_B+\gamma\bar{n}_i(a). \tag{67}$$

When evaluating (65) we note that the second (double) summation in (63) is zero because $\int_0^{2\pi}e^{j(l-k)\theta_\alpha}d\theta_\alpha = 0$ when $l\neq k$. Thus, we only need to integrate the first summation in (63). We substitute the summation-based definition of the modified Bessel function of the first kind $I_0(z) = \sum_{m=0}^\infty\frac{(z/2)^{2m}}{(m!)^2}$ and change in the order of summation and integration, using Tonelli's theorem to justify the latter step since the arguments in summations are non-negative. The the integrals with respect to r_α and r_β take a form with the following solution [16, Eq. (3.326.2)]: $\int_0^\infty x^m e^{-cx^n}dx = \frac{\Gamma(\kappa)}{nc^\kappa}$ where $\kappa = (m+1)/n$. Finally, to arrive at (66) we use the identity $\sum_{m=0}^\infty\frac{r^m(m+n)!}{m!} = n!\sum_{m=0}^\infty r^m\binom{m+n}{m} = \frac{n!}{(1-r)^{n+1}}$ which is valid for any r satisfying $0\leq r<1$ as is our case.

Similarly, the second moment of the square magnitude of heterodyne detector reading when Alice transmits $\hat{\rho}_i^A(a)$ is obtained as follows:

$$\mathbb{E}[|y_i|^4] = \int_{\mathbb{C}}|\alpha|^4 Q^W_{|\psi_i(a)\rangle}(\alpha)d^2\alpha \tag{68}$$

$$= \int_0^\infty\int_0^{2\pi} r_\alpha^5 Q^W_{|\psi_i(a)\rangle}(r_\alpha e^{j\theta_\alpha})d\theta_\alpha dr_\alpha \tag{69}$$

$$= \sum_{k=0}^{\nu_i(a)}|b_k^{(i)}(a)|^2(\gamma^2k^2+2(1+(1-\gamma)N_B)^2+4\gamma(1-\gamma)(1+N_B)k) \tag{70}$$

$$= \gamma^2\mu_i^{(2)}(a)+2(1+(1-\gamma)N_B)^2+4\gamma(1-\gamma)(1+N_B)\bar{n}_i(a) \tag{71}$$

where $\mu_i^{(2)}(a) = \sum_{k=0}^{\nu_i(a)} k^2 |b_k^{(i)}(a)|^2$. The variance of the squared magnitude of heterodyne detector reading when Alice transmits $\hat{\rho}_i^A(a)$ is then:

$$\mathrm{Var}[|y_i|^2] = \gamma^2 \sigma_i^2(a) + c_1 \bar{n}_i(a) + c_2 \tag{72}$$

where $\sigma_i^2(a) = \mu_i^{(2)}(a) - (\bar{n}_i(a))^2$ denotes the photon number variance of $\hat{\rho}_i^A(a)$, and $c_1 = 2\gamma((2+N_B)(1-\gamma)-1)$, $c_2 = (1+(1-\gamma)N_B)^2$.

3. Derivation of (35)

A beamsplitter can be described as a unitary transformation U_{BS} from two input modes to two output modes. In our scenario, the inputs are Alice's input state $\hat{\rho}^A = |\psi\rangle^A {}^A\langle\psi|$ and vacuum environment $\hat{\rho}^E = |0\rangle^E {}^E\langle 0|$. The outputs are Willie's output state $\hat{\rho}^W$ and Bob's output state $\hat{\rho}^B$. First, suppose Alice transmits a number state $|\psi\rangle^A = |k\rangle^A$. Then the inputs and outputs of a beamsplitter with transmissivity γ are related as follows:

$$U_{BS} |k\rangle^A |0\rangle^E = \sum_{m=0}^{k} \sqrt{\binom{k}{m} \gamma^m (1-\gamma)^{k-m}} |m\rangle^W |k-m\rangle^B . \tag{73}$$

Now suppose that Alice transmits an arbitrary pure state expressed in the number basis as follows: $|\psi\rangle^A = \sum_{k=0}^{\infty} a_k |k\rangle^A$. Since U_{BS} is a linear transformation,

$$U_{BS} \left(\sum_{k=0}^{\infty} a_k |k\rangle^A \right) |0\rangle^E = \sum_{k=0}^{\infty} a_k \sum_{m=0}^{k} \sqrt{\binom{k}{m} \gamma^m (1-\gamma)^{k-m}} |m\rangle^W |k-m\rangle^B \equiv |\psi\rangle^{WB} \tag{74}$$

with the output state $\hat{\rho}^{WB} = |\psi\rangle^{WB\,WB}\langle\psi|$. However, we desire only Willie's output state $\hat{\rho}^W$, which we obtain using the partial trace over the Bob's output state:

$$\hat{\rho}^W = \mathrm{Tr}_B \left[|\psi\rangle^{WB\,WB}\langle\psi| \right] \tag{75}$$

$$= \sum_{n=0}^{\infty} {}^B\langle n|\psi\rangle^{WB\,WB}\langle\psi|n\rangle^B \tag{76}$$

where

$${}^B\langle n|\psi\rangle^{WB} = \sum_{k=0}^{\infty} a_k \sum_{m=0}^{k} \sqrt{\binom{k}{m} \gamma^m (1-\gamma)^{k-m}} |m\rangle^{W\,B}\langle n|k-m\rangle^B \tag{77}$$

$$= \sum_{k=0}^{\infty} a_k \sqrt{\binom{k}{n} \gamma^{k-n} (1-\gamma)^n} |k-n\rangle^W \tag{78}$$

with (78) due to the orthonormality of number states. Thus,

$$\langle s| \hat{\rho}^W |s\rangle = \sum_{n=0}^{\infty} |a_n|^2 \binom{n}{s} \gamma^s (1-\gamma)^{n-s} \tag{79}$$

where we use the convention that $\binom{a}{b} = 0$ when $a < b$.

4. Reliability of LPD Communication Using OOK Modulation

Dark current in Bob's receiver induces a binary asymmetric channel (BAC) between Alice and Bob depicted in Figure 2. Since the channel between Alice and Bob is a classical *discrete memoryless channel* (DMC), by [17, Th. 5.6.1] and the discussion that follows it in [17], Bob's average probability of decoding error $\mathbb{P}_e^{(b)}$ can be upper-bounded as follows:

$$\mathbb{P}_e^{(b)} \leq e^{-n(E_0(s)-sR)}, \tag{80}$$

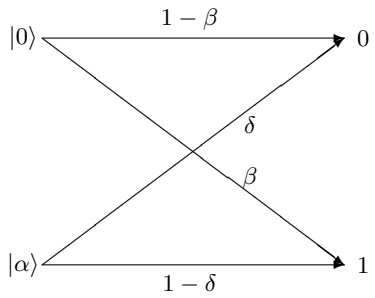


FIG. 2: The binary asymmetric channel between Alice and Bob. Input probabilities are $p(|0\rangle) = 1-q$ and $p(|\alpha\rangle) = q$. Transition probabilities are $\delta = e^{-\eta|\alpha|^2}(1-p_b)$ and $\beta = p_b$.

where n is the size of the codeword, p_b is Bob's receiver dark click probability, R is the coding rate, $0 \leq s \leq 1$, and $E_0(s)$ is defined as follows:

$$E_0(s) = -\ln\left[(1-p_b)\left(1-q\left(1-e^{-\frac{\eta|\alpha|^2}{1+s}}\right)\right)^{1+s} + \left((1-q)p_b^{1/(1+s)} + q\left(1-(1-p_b)e^{-\eta|\alpha|^2}\right)^{1/(1+s)}\right)^{1+s}\right] \tag{81}$$

However, the Taylor series expansion around $|\alpha|^2 = 0$ has a zero first-order term:

$$E_0(s) = \frac{(1-q)q(1-p_b)s\eta^2|\alpha|^4}{2p_b(1+s)} + \mathcal{O}(|\alpha|^6) \tag{82}$$

Therefore, Alice and Bob have to set their per-symbol mean photon number $|\alpha|^2 = \omega(1/\sqrt{n})$ to upper-bound Bob's probability of decoding error by an arbitrary $\delta > 0$. However, recall that to prevent the detection by Willie, they must set the mean photon number $\bar{n} = q|\alpha|^2$ to (52). Thus, using a method similar to the one described in [2, App. A], they can construct a covert codebook in two stages. First, Alice and Bob randomly select the symbol periods that they will use for their transmission by flipping a biased coin n times and selecting the i^{th} symbol period with probability $c/\sqrt{n} < 1$ for some constant c. Denote the number of selected symbol periods by τ and note that mean $\bar{\tau} = c\sqrt{n}$. Second, set

$$|\alpha|^2 = \frac{4\epsilon n}{\tau\sqrt{n}(1-\eta)}\sqrt{\frac{p_d}{1-p_d}} \tag{83}$$

and generate the codebook with codewords of length τ on the selected τ symbol periods. Since the symbol location selection is independent of both the symbol and the channel noise, the analysis leading to (51) applies. Covert communication criterion (52) is satisfied, and $|\alpha|^2 = \omega(1/\sqrt{n})$ with high probability, ensuring reliable transmission of $\mathcal{O}(\sqrt{n})$ covert bits from Alice to Bob.