Signaling for Covert Quantum Sensing

Mehrdad Tahmasbi
University of Amsterdam
Amsterdam, Netherlands
Email: m.tahmasbi@uva.nl

Boulat A. Bash, Saikat Guha
University of Arizona
Tucson, AZ, USA
Email: {boulat,saikat}@arizona.edu

Matthieu Bloch
Georgia Institute of Technology
Atlanta, GA, USA
Email: matthieu@gatech.edu

***Abstract*—Motivated by application to quantum radar and the known benefits of quantum illumination in the high-noise low-reflectance regime, we study the design of signaling schemes for covertly probing a distant target over a lossy and noisy bosonic channel. Specifically, we analyze the performance of *diffuse* and *sparse* signaling schemes, which achieve covertness by spreading a constant number of photons in many modes or in a few modes, respectively. We benchmark the performance against a converse bound that holds for arbitrary covert quantum illumination schemes. Numerical results suggest the superior performance of the diffuse signaling scheme, which we conjecture outperforms any other covert quantum illumination scheme.**

I. Introduction

Motivated by potential improvements in the performance of radar sensing, there has been much recent research on quantum illumination [1], [2]. The key premise of quantum illumination is to rely on a signal/idler entangled state, typically a photon pair obtained at the output of a spontaneous parametric down-conversion (SPDC) source, to illuminate a target with the signal and exploit the idler to analyze the reflected signal. In the regime of weak target reflectivity and high background noise, quantum illumination affords a factor of four improvement in the detection error probability exponent compared to a non-entangled coherent state based sensing [3]. This result is all the more surprising as entanglement is broken in the lossy noisy bosonic channel modeling the sensing, so that the returning and idler signals are not entangled. Notable recent results in quantum illumination include the proposal of realizable detectors [4]–[6] and a converse result placing limits on the best possible performance achievable using any quantum illumination system [7].

Concurrently, there has been a growing interest for the study of information-theoretic covertness in classical and quantum settings, defined as the ability to provably ensure a low probability of detection against an adversary deploying an optimal detector. In the context of reliable communication, results on covert communications have highlighted the existence of a square-root law [8] and led to the characterization of the covert capacity [8]–[11] for many channel models. In the context of sensing, the results most relevant to the present work are the covert sensing studies in [12], [13], which have considered the problem of estimating an unknown phase while preventing a quantum adversary from detecting the presence of the sensing. Undetectability is made possible by the presence of thermal noise impairing the detection of the adversary. The square-root law takes the form of a limit on the scaling of the mean-square phase estimation error, which scales as $\mathcal{O}(\frac{1}{\sqrt{n}})$ if n is the number of modes. Follow up work has analyzed covert sensing for classical [14] and classical-quantum channels [15], illustrating the usefulness of adaptivity through the characterization of detection error exponents and suggesting the potential benefits of entanglement in specific settings.

In the present work, we analyze the performance of covert quantum sensing schemes in the context of quantum illumination. Specifically, we consider the problem of detecting the presence of a target while escaping detection from an adversary. Our main results are the comparative performance analysis of two signaling schemes, which we call *diffuse* and *sparse* signaling, and the characterization of a converse bound on detection error probability limiting the performance of any covert quantum illumination scheme. As further detailed in the next sections, the diffuse and sparse schemes differ in how they achieve a low average photon number: the diffuse scheme spreads energy across all available modes while the sparse scheme concentrates a higher energy in a few modes. The latter scheme is relevant in that it might offer some experimental simplifications.

The rest of the paper is organized as follows. We introduce the formal model of covert quantum illumination in Section II. We analyze the performance of diffuse and sparse signaling in Section III and derive a converse bound in Section IV. We illustrate the results numerically in Section V.

II. Covert Quantum Illumination

Throughput the paper, the set $\{|x\rangle : x = 0, 1, \cdots\}$ denotes the basis of Fock states while $N \triangleq \sum_{x=0}^{\infty} |x\rangle\langle x|$ denotes the photon number operator. A lossy bosonic channel with excess noise n and transmissivity η is concisely denoted by $\mathcal{L}_{n,\eta}$.

The specific model used to analyze covert quantum illumination is illustrated in Fig. 1. A transmitter, Alice, aims at detecting whether a distant target exists while avoiding detection from a monitoring adversary, Willie. To sense the target, Alice prepares a signal-reference state $|\phi\rangle_{I^nS^n}$ to be transmitted over n modes (such as n signal/idler pairs resulting from an SPDC source) and transmits the signal $|\phi_{S^n}\rangle$ while retaining the reference $|\phi_{I^n}\rangle$ in a quantum memory to assist detection. Covertness is measured with respect to

M. R. Bloch is supported in part by National Science Foundation (NSF) grant FET-1910859. B. A. Bash and Saikat Guha are supported in part by NSF grant CCF-2045530 and NSF grant EEC-1941583.

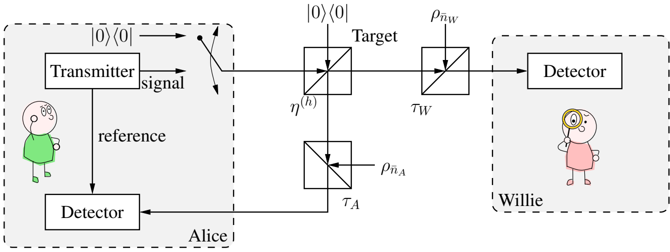

Fig. 1. Covert quantum illumination model.

the situation in which Alice does not transmit any signal, which corresponds to transmitting the vacuum state $|0\rangle\langle 0|$ over n modes. We model the distant target by a beam-splitter with transmissivity $\eta^{(h)}$, where $h \in \{0,1\}$ depending on the absence ($h = 0$) or presence ($h = 1$) of a target. In the absence of the target, $\eta^{(0)} \triangleq 1$, while in the presence of the target, $\eta^{(1)} \triangleq \eta_t < 1$. Alice's signal is sent to one input port while the other input port is in the vacuum state $|0\rangle\langle 0|$. One output port of the target is fed back to Alice through a lossy bosonic channel $\mathcal{L}_{\overline{n}_A,\tau_A}$ while the other output port is accessed by Willie through another lossy bosonic channel $\mathcal{L}_{\overline{n}_W,\tau_W}$. This effectively assumes that all signals not reflected back to Alice are potentially detected by Willie. The effective channels to Alice and Willie are $\mathcal{L}_{\overline{n}_A(1-\tau_A),(1-\eta^{(h)})\tau_A}$ and $\mathcal{L}_{\overline{n}_W(1-\tau_W),\eta^{(h)}\tau_W}$, respectively.

Alice's objective is to detect the presence or absence of the target. Formally, under hypothesis $h \in \{0,1\}$, Alice obtains the state

$$\rho^{(h)}_{I^nR^n} \triangleq (\mathrm{id}_{I^n} \otimes \mathcal{L}_{\overline{n}_A(1-\tau_A),(1-\eta^{(h)})\tau_A})(\phi_{I^nS^n}) \tag{1}$$

after transmission and performs a joint measurement on the return signal and reference to decide on the value of h. Assuming the target is equally likely to be present or not, the estimation error is defined as the minimum sum of the probabilities of false alarm and missed detection $P_e \triangleq \frac{P_{\mathrm{FA}}+P_{\mathrm{MD}}}{2}$. The optimal value of P_e is known as the Helstrom limit.

Concurrently, Willie's objective is to detect the presence or absence of Alice's sensing signal. Specifically, Willie, who knows the state $|\phi\rangle_{I^nA^b}$ prepared by Alice and the presence of absence of the target $h \in \{0,1\}$, receives the state

$$\rho^{(h)}_{W^n} \triangleq \mathrm{tr}_{I^n}\left((\mathrm{id}_{I^n} \otimes \mathcal{L}_{\overline{n}_W(1-\tau_W),\eta^{(h)}\tau_W})(\phi_{I^nS^n})\right), \tag{2}$$

based of which he attempts to detect whether Alice transmitted ϕ_{A^n} or was silent, corresponding to transmitting $|0\rangle\langle 0|^{\otimes n}$. The detectability of Alice's activity by Willie is measured through the quantum relative entropy

$$\max_{h=0,1} \mathbb{D}\left(\rho^{(h)}_{W^n} \| (\rho^{(h)}_0)^{\otimes n}\right). \tag{3}$$

where

$$\rho^{(h)}_0 \triangleq \mathcal{L}_{\overline{n}_W(1-\tau_W),\eta^{(h)}\tau_W}(|0\rangle\langle 0|). \tag{4}$$

A small value of the quantum relative entropy ensures that Willie's best detection is not much better than a guess that ignores his received signals, effectively ensuring covertness.

The problem of covert quantum illumination consists in characterizing the minimum value of P_e subject to an upper bound $\delta > 0$ on the quantum relative entropy in (3). It will be convenient to introduce the covert estimation error exponent defined as $\lim_{n\to\infty} -\frac{1}{\sqrt{n\delta}} \log P_e$, which we shall see is only a function of the channel parameters and does not depend on the block length n or the relative entropy bound δ.

Remark 1. *The model of Fig. 1 corresponds to a situation in which the amplitude and phase of the target are known, and therefore does not capture the full challenges of radar sensing. A natural extension of the model is to consider the presence of a Rayleigh-faded target as in [6] but is outside the scope of the present work.*

III. Covert Signaling for Quantum Illumination

We now derive the estimation error of two explicit signaling schemes, which we refer to as *diffuse* and *sparse* signaling.

A. Performance of Diffuse Signaling

For diffuse signalling, Alice prepares n independent EPR pairs $|\phi\rangle_{I^nS^n} \triangleq |\mathrm{EPR}\rangle_{\mathrm{IS}}(\overline{n}_S)^{\otimes n}$ where

$$|\mathrm{EPR}\rangle_{\mathrm{IS}}(\overline{n}_S) \triangleq \sum_{x=0}^{\infty} \sqrt{\frac{\overline{n}_S{}^x}{(1+\overline{n}_S)^{x+1}}}|x\rangle_I |x\rangle_S. \tag{5}$$

and transmits ϕ_{S^n} over the channel. The signaling is called diffuse because every one of the n modes contains energy but, as we shall see shortly, the mean photon number $\overline{n}_S$ must vanish with n to satisfy the covertness constraint. We denote by $\rho^{(h)}_{IR}(\overline{n}_S) \triangleq (\mathrm{id}_I \otimes \mathcal{L}_{\overline{n}_A(1-\tau_A),(1-\eta^{(h)})\tau_A})(|\mathrm{EPR}\rangle\langle\mathrm{EPR}|(\overline{n}_S))$ the state received by Alice under hypothesis h. We similarly define $\rho^{(h)}_W(\overline{n}_S)$ as the received state by Willie under hypothesis h. The optimal estimation error is then [3]

$$\begin{aligned}\exp&\left(-n\overline{n}_S \max_{s\in[0,1]} \Phi(s,\overline{n}_S)\right)\\ &= \exp\left(-n\left(\overline{n}_S \max_{s\in[0,1]} \Psi(s) + O(\overline{n}_S{}^2)\right)\right)\end{aligned} \tag{6}$$

where

$$\Phi(s,\overline{n}_S) \triangleq -\log\left(\left(\rho^{(0)}_{IR}(\overline{n}_S)\right)^s \left(\rho^{(1)}_{IR}(\overline{n}_S)\right)^{1-s}\right) \tag{7}$$

$$\Psi(s) \triangleq \frac{\partial\Phi}{\partial\overline{n}_S}(s,0). \tag{8}$$

$\Psi(s)$ can be evaluated numerically using a symplectic decomposition. For a single mode, the quantum relative entropy is

$$\begin{aligned}\max_{h=0,1} &\mathbb{D}\left(\rho^{(h)}_W(\overline{n}_S)\|\rho^{(h)}_W(0)\right)\\ &= \max_{h=0,1}\left(\eta^{(h)}\tau_W\overline{n}_S + (1-\tau_W)\overline{n}_W\right)\\ &\times \log\frac{\left(\eta^{(h)}\tau_W\overline{n}_S + (1-\tau_W)\overline{n}_W\right)(1+(1-\tau_W)\overline{n}_W)}{\left(\eta^{(h)}\tau_W\overline{n}_S + (1-\tau_W)\overline{n}_W + 1\right)(1-\tau_W)\overline{n}_W}\\ &+ \log\frac{1+(1-\tau_W)\overline{n}_W}{\eta^{(h)}\tau_W\overline{n}_S + (1-\tau_W)\overline{n}_W + 1}\end{aligned}$$

$$= \frac{(\tau_W \overline{n}_S)^2}{2(1-\tau_W)\overline{n}_W(1+(1-\tau_W)\overline{n}_W)} + O(\overline{n}_S{}^3). \quad (9)$$

To ensure that the quantum relative entropy does not exceed $\delta > 0$ over n modes, the mean photon number should be chosen to satisfy

$$\overline{n}_S \lesssim \sqrt{\frac{2\delta(1-\tau_W)\overline{n}_W(1+(1-\tau_W)\overline{n}_W)}{n\tau_W^2}}, \quad (10)$$

where the inequality ignores terms in $\mathcal{O}(\frac{1}{n})$. The resulting covert estimation error exponent is then

$$\sqrt{\frac{2(1-\tau_W)\overline{n}_W(1+(1-\tau_W)\overline{n}_W)}{\tau_W^2}} \max_{s\in[0,1]} \Psi(s). \quad (11)$$

B. Performance of Sparse Signaling

For sparse signalling, Alice prepares $n\alpha_n$ ($\alpha_n < 1$) independent EPR pairs that she transmits in randomly selected modes out of n. The signaling is called sparse because we shall see that the fraction α_n of modes containing a signal is vanishing when the mean photon number of each signal mode does not vanish. The sparse signaling scheme offers experimental advantages over the diffuse scheme, although we shall see that this comes at a performance cost.

Formally, let us fix $\overline{n}_S$ independent of n and a vanishing sequence $\{\alpha_n\}_{n\geq 1}$ of non-negative numbers. Let P_n be Bernoulli(α_n). For $\zeta > 0$, define the set

$$\mathcal{A} \triangleq \{x^n \in \{0,1\}^n : \alpha_n(1+\zeta) \geq \frac{1}{n}\sum_{i=1}^{n} x_i \geq \alpha_n(1-\zeta)\}, \quad (12)$$

which contains the length n binary sequences whose normalized weight is close to α_n, and define

$$P_{X^n}(x^n) \triangleq \begin{cases} \frac{P_n^{\otimes n}(x^n)}{P_n^{\otimes n}(\mathcal{A})} & x^n \in \mathcal{A}, \\ 0 & x^n \notin \mathcal{A}. \end{cases} \quad (13)$$

We need to expurgate "atypical" sequences to avoid compromising the error exponent. Alice samples X^n according to P_{X^n}, and in mode i, prepares an independent EPR pair $|\text{EPR}\rangle_{\text{IS}}(\overline{n}_S X_i)$ and transmits the S sub-system over the channel. Following the calculations of [14], we upper-bound the estimation error by

$$\exp\left(-n\alpha_n(1-\zeta)(\Phi(s,\overline{n}_S)+o(1))\right). \quad (14)$$

Further following [14], we upper bound the quantum relative entropy under hypothesis h for $\overline{n}_S$ small enough as

$$\mathbb{D}\left(\rho_{W^n}^{(h)} \| \left(\rho_0^{(h)}\right)^{\otimes n}\right) \quad (15)$$

$$\leq n\mathbb{D}\left(\alpha_n\rho_W^{(h)}(\overline{n}_S) + (1-\alpha_n)\rho_0^{(h)} \| \rho_0^{(h)}\right) + o(1) \quad (16)$$

$$\leq \frac{1}{2}\alpha_n^2\chi_2(\rho_W^{(h)}(\overline{n}_S)\|\rho_0^{(h)}) + o(1) \quad (17)$$

$$= \frac{\alpha_n^2}{2}\frac{(\eta^{(h)}\tau_W\overline{n}_S)^2}{((1-\tau_W)\overline{n}_W)^2 + (1-\tau_W)\overline{n}_W - (\eta^{(h)}\tau_W\overline{n}_S)^2} + o(1), \quad (18)$$

where $\chi_2(\rho\|\sigma) \triangleq \text{tr}\left(\rho^2\sigma^{-1}\right) - 1$. To ensure that the quantum relative entropy does not exceed $\delta > 0$ over n modes, the fraction α_n of EPR pairs must then satisfy

$$\alpha_n \lesssim \sqrt{\frac{2\delta\left((1-\tau_W)\overline{n}_W)^2 + (1-\tau_W)\overline{n}_W\right)}{n(\tau_W\overline{n}_S)^2} - 1}, \quad (19)$$

where the inequality ignores again terms in $\mathcal{O}(\frac{1}{n})$. Therefore, the resulting covert estimation error exponent is

$$\sqrt{2\left(((1-\tau_W)\overline{n}_W)^2 + (1-\tau_W)\overline{n}_W - (\eta^{(h)}\tau_W\overline{n}_S)^2\right)} \frac{\Phi(s,\overline{n}_S)}{\tau_W\overline{n}_S}. \quad (20)$$

Note that in the limit of $\overline{n}_S \to 0$, Eq. (20) tends to Eq. (11).

C. On the Optimality of the Diffuse Scheme

The sparse signaling offers potential experimental benefits, chiefly by using EPR pairs parsimoniously; however, we posit that this comes at a performance cost. While we could not establish this result formally, we show next that the result is true if the following conjecture holds.

Conjecture 1. *$\Phi(s,\overline{n}_S)$ defined in (7) is concave in $\overline{n}_S$ for all $s \in [0,1]$.*

We explored the validity of the conjecture numerically and could not find evidence of the contrary. In the remainder of the section, we assume that the conjecture holds.

Suppose that Alice samples X^n in $\mathbb{R}_+^n$ from an arbitrary distribution P_{X^n}. She then prepares $|\phi\rangle_{I^nS^n} \triangleq |\text{EPR}\rangle_{\text{IS}}(X_1) \otimes \cdots \otimes |\text{EPR}\rangle_{\text{IS}}(X_n)$ and transmits ϕ_{S^n} over the channel, which corresponds to varying the mean photon number in each pair according to the realization of X^n. For a specific realization $X^n = x^n$, the Chernoff bound and Jensen's inequality imply that the estimation error is at least

$$\exp\left(-\sup_{s\in[0,1]}\sum_{i=1}^{n}\Phi(s,x_i)\right) \overset{(a)}{\geq} \exp\left(-n\sup_{s\in[0,1]}\Phi(s,\overline{x})\right) \quad (21)$$

for $\overline{x} \triangleq \frac{1}{n}\sum_{i=1}^{n} x_i$, where (a) holds if Conjecture 1 is true. We now provide a bound on the mean photon number transmitted by Alice given a covertness constraint.

Lemma 1. *Let Alice prepare an arbitrary initial state $|\phi\rangle_{I^nS^n}$ such that*

$$\max_{h=0,1}\mathbb{D}\left(\rho_{W^n}^{(h)} \| \left(\rho_0^{(h)}\right)^{\otimes n}\right) \leq \delta. \quad (22)$$

We then have

$$\mathcal{N}_S \triangleq \sum_{i=1}^{n}\text{tr}\left(\phi_{A_i}N\right) \quad (23)$$

$$\leq \sqrt{n\delta}f(\overline{n}_W,\tau_W) + o(\sqrt{n}), \quad (24)$$

where

$$f(\overline{n}_W,\tau_W) \triangleq \frac{\sqrt{(2((1-\tau_W)\overline{n}_W)^2 + 2(1-\tau_W)\overline{n}_W)}}{\tau_W}. \quad (25)$$

Note that Lemma 1 holds regardless of the conjecture.

Proof. The proof is largely borrowed from [16] and is inspired by the characterization of the covert capacity in [10], [17]. We first single-letterize the covertness condition and use the result that thermal states maximize the entropy for a given mean photon number. The details of the proof are as follows. Note that

$$\mathbb{D}\left(\rho_{W^n} \| \left(\rho_0^{(h)}\right)^{\otimes n}\right) \tag{26}$$

$$= -H(\rho_{W^n}) - \operatorname{tr}\left(\rho_{W^n} \log\left(\left(\rho_0^{(h)}\right)^{\otimes n}\right)\right) \tag{27}$$

$$= -H(\rho_{W^n}) - \sum_{i=1}^{n} \operatorname{tr}\left(\rho_{W_i} \log \rho_0^{(h)}\right) \tag{28}$$

$$\geq \sum_{i=1}^{n} \left(-H(\rho_{W_i}) - \operatorname{tr}\left(\rho_{W_i} \log \rho_0^{(h)}\right)\right) \tag{29}$$

$$= \sum_{i=1}^{n} \mathbb{D}\left(\rho_{W_i} \| \rho_0^{(h)}\right) \tag{30}$$

$$= n\mathbb{D}\left(\frac{1}{n}\sum_{i=1}^{n} \rho_{W_i} \| \rho_0^{(h)}\right). \tag{31}$$

Let us define

$$\overline{\rho} \triangleq \frac{1}{n}\sum_{i=1}^{n} \rho_{W_i}, \tag{32}$$

for which we have

$$\operatorname{tr}(N\overline{\rho}) = \eta^{(h)}\tau_W \frac{\mathcal{N}_S}{n} + (1-\tau_W)\overline{n}_W. \tag{33}$$

We then have

$$\mathbb{D}\left(\overline{\rho} \| \rho_0^{(h)}\right) = -H(\overline{\rho}) - \operatorname{tr}\left(\overline{\rho} \log(\rho_0^{(h)})\right) \tag{34}$$

Furthermore,

$$\operatorname{tr}\left(\overline{\rho} \log(\rho_0^{(h)})\right) \tag{35}$$

$$= \operatorname{tr}\left(\overline{\rho} \log\left(\sum_{x=0}^{\infty} \frac{((1-\tau_W)\overline{n}_W)^x}{((1-\tau_W)\overline{n}_W+1)^{x+1}} |x\rangle\langle x|\right)\right) \tag{36}$$

$$= \operatorname{tr}\left(\overline{\rho}\left(\log\left(\frac{(1-\tau_W)\overline{n}_W}{(1-\tau_W)\overline{n}_W+1}\right) N + \log \frac{1}{(1-\tau_W)\overline{n}_W+1}\mathbf{1}\right)\right) \tag{37}$$

$$= \log\left(\frac{(1-\tau_W)\overline{n}_W}{(1-\tau_W)\overline{n}_W+1}\right) \operatorname{tr}(N\overline{\rho}) + \log \frac{1}{(1-\tau_W)\overline{n}_W+1}. \tag{38}$$

For a given mean photon number, thermal states maximize the entropy [18]. Therefore,

$$-H(\overline{\rho}) \geq -\left(\operatorname{tr}(N\overline{\rho})+1\right)\log\left(\operatorname{tr}(N\overline{\rho})+1\right) + \operatorname{tr}(N\overline{\rho})\log\left(\operatorname{tr}(N\overline{\rho})\right). \tag{39}$$

We thus have

$$\begin{aligned}
&\mathbb{D}\left(\overline{\rho} \| \rho_0^{(h)}\right) \\
&= -\left(\operatorname{tr}(N\overline{\rho})+1\right)\log\left(\operatorname{tr}(N\overline{\rho})+1\right) + \operatorname{tr}(N\overline{\rho})\log\left(\operatorname{tr}(N\overline{\rho})\right) \\
&\qquad - \log\left(\frac{(1-\tau_W)\overline{n}_W}{(1-\tau_W)\overline{n}_W+1}\right)\operatorname{tr}(N\overline{\rho}) \\
&\qquad - \log \frac{1}{(1-\tau_W)\overline{n}_W+1} \\
&= \frac{\left(\eta^{(h)}\tau_W \frac{\mathcal{N}_S}{n}\right)^2}{2((1-\tau_W)\overline{n}_W)^2 + 2(1-\tau_W)\overline{n}_W} + \mathcal{O}\left(\left(\frac{\mathcal{N}_S}{n}\right)^3\right).
\end{aligned} \tag{40}$$

We finally obtain

$$\mathcal{N}_S \leq \frac{\sqrt{n\delta\left(2((1-\tau_W)\overline{n}_W)^2 + 2(1-\tau_W)\overline{n}_W\right)}}{\eta^{(h)}\tau_W} + o(\sqrt{n}). \tag{41}$$

$\square$

Applying Lemma 1, to the specific protocol, we obtain that

$$\mathbb{E}_{P_{X^n}}\left[\frac{1}{n}\sum_{i=1}^{n} X_i\right] \leq \frac{1}{\sqrt{n}}\left(\sqrt{\delta} f(\overline{n}_W, \tau_W) + o(1)\right) \tag{42}$$

when

$$\max_{h=0,1} \mathbb{D}\left(\rho_{W^n}^{(h)} \| \left(\rho_0^{(h)}\right)^{\otimes n}\right) \leq \delta. \tag{43}$$

By Markov's inequality, we have

$$\begin{aligned}
&\mathbb{P}_{P_{X^n}}\left(\frac{1}{n}\sum_{i=1}^{n} X_i \leq \frac{n}{(n-1)\sqrt{n}}\left(\sqrt{\delta} f(\overline{n}_W, \tau_W) + o(1)\right)\right) \\
&= \mathbb{P}_{P_{X^n}}\left(\frac{1}{n}\sum_{i=1}^{n} X_i \leq \frac{1}{\sqrt{n}}\left(\sqrt{\delta} f(\overline{n}_W, \tau_W) + o(1)\right)\right)
\end{aligned} \tag{44}$$

$$\geq \frac{1}{n} \tag{45}$$

Since $\Phi(s,x)$ is non-decreasing in x, we can lower-bound the estimation error by

$$\mathbb{E}_{P_{X^n}}\left[\exp\left(-n \sup_{s\in[0,1]} \Phi\left(s, \frac{1}{n}\sum_{i=1}^{n} X_i\right)\right)\right] \tag{46}$$

$$\geq \frac{1}{n}\exp\left(-n \sup_{s\in[0,1]} \Phi\left(s, \frac{1}{\sqrt{n}}\left(\sqrt{\delta} f(\overline{n}_W, \tau_W) + o(1)\right)\right)\right) \tag{47}$$

$$= \frac{1}{n}\exp\left(-\sqrt{n\delta} f(\overline{n}_W, \tau_W) \sup_{s\in[0,1]} \Psi(s) + o(\sqrt{n})\right), \tag{48}$$

where $\Psi(s)$ is defined in (8). Therefore, the achievable exponent is less than (11), showing the suboptimality of any scheme other than the diffuse signaling scheme.[1]

[1] A similar result was derived in [19] in the context of covert communications.

IV. CONVERSE BOUND

We now derive a fundamental limit on the detection error of any covert quantum illumination scheme. The approach leverages a very recent bound established for standard quantum illumination [7] and adapts it to account for the covertness constraint.

Theorem 2. *Any achievable exponent is less than*

$$-\ln\left(1-\frac{(1-\eta_t)\tau_A}{1+\overline{n}_A(1-\tau_A)}\right)f(\overline{n}_W,\tau_W), \tag{49}$$

where $f(\overline{n}_W,\tau_W)$ *is defined in Lemma 1.*

Proof. Alice prepares the state $|\phi\rangle_{I^nS^n}$ and transmits ϕ_{A^n} over the channel. By [7, Eq. (13)], we have

$$P_e \geq \frac{1}{2}\exp\left(\ln\left(1-\frac{(1-\eta_t)\tau_A}{1+\overline{n}_A(1-\tau_A)}\right)\mathcal{N}_S\right) \tag{50}$$

where

$$\mathcal{N}_S \triangleq \sum_{i=1}^{n}\operatorname{tr}\left(\phi_{A_i}N\right) \tag{51}$$

and N is number operator. Using the bound on $\mathcal{N}_S$ from Lemma 1 completes the proof. □

V. NUMERICAL ILLUSTRATION

We conclude the paper with a numerical illustration of the covert estimation error exponents obtained for the diffuse signaling scheme, the sparse signaling scheme, and the converse bound. Fig. 2 illustrates the exponents obtained for $\overline{n}_S = 0.5$, $\eta_t = 0.3$, $\tau_W = \tau_A = 0.3$, as a function of the noise parameter $\overline{n}_W = \overline{n}_A$. The diffuse signaling scheme achieves close to optimal performance while the sparse signaling scheme suffers from more than a factor of two loss.

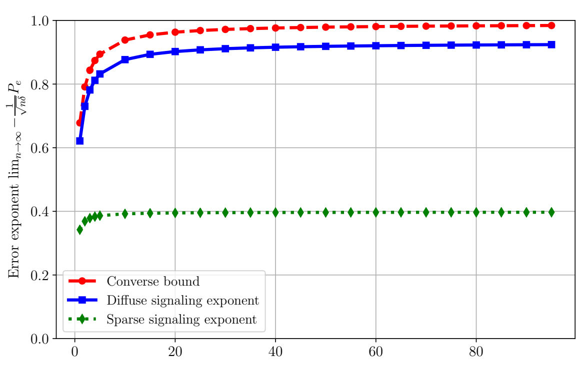

Fig. 2. Comparison of covert estimation error exponents for diffuse and sparse signaling schemes. See text for parameter values.

VI. DISCUSSION AND FUTURE WORK

We studied two schemes for covert quantum sensing: sparse and diffuse signaling. While sparse signaling may be experimentally more feasible, we show that given a conjecture, which we checked numerically, the diffuse signaling has optimal performance over a large class of schemes. We also established an upper bound on the performance of any covert quantum sensing strategy. For future work, beyond investigating the validity of the conjecture, one can explore the benefits of quantum error correction codes for covert quantum sensing (e.g., see [20], [21]).

REFERENCES

[1] S. Pirandola, B. R. Bardhan, T. Gehring, C. Weedbrook, and S. Lloyd, "Advances in photonic quantum sensing," *Nature Photonics*, vol. 12, no. 12, p. 724–733, Nov. 2018.

[2] J. H. Shapiro, "The quantum illumination story," *IEEE Aerospace and Electronic Systems Magazine*, vol. 35, no. 4, pp. 8–20, Apr. 2020.

[3] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, "Quantum illumination with Gaussian states," *Physical Review Letters*, vol. 101, no. 25, Dec. 2008.

[4] S. Guha and B. I. Erkmen, "Gaussian-state quantum-illumination receivers for target detection," *Physical Review A*, vol. 80, no. 5, p. 052310, Nov. 2009.

[5] Q. Zhuang, Z. Zhang, and J. H. Shapiro, "Optimum mixed-state discrimination for noisy entanglement-enhanced sensing," *Physical Review Letters*, vol. 118, no. 4, p. 040801, Jan. 2017.

[6] ——, "Quantum illumination for enhanced detection of rayleigh-fading targets," *Physical Review A*, vol. 96, no. 2, p. 020302, Aug. 2017.

[7] R. Nair and M. Gu, "Fundamental limits of quantum illumination," *Optica*, vol. 7, no. 7, p. 771, Jul. 2020.

[8] B. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.

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

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

[11] M. Tahmasbi and M. R. Bloch, "First and second order asymptotics in covert communication," *IEEE Transactions on Information Theory*, vol. 65, no. 4, pp. 2190 –2212, Apr. 2019.

[12] B. A. Bash, C. N. Gagatsos, A. Datta, and S. Guha, "Fundamental limits of quantum-secure covert optical sensing," in *Proc. of IEEE International Symposium on Information Theory*, Aachen, Germany, Jun. 2017, pp. 3210–3214.

[13] C. N. Gagatsos, B. A. Bash, A. Datta, Z. Zhang, and S. Guha, "Covert sensing using floodlight illumination," *Physical Review A*, vol. 99, p. 062321, Jun. 2019.

[14] M. Tahmasbi and M. R. Bloch, "Active covert sensing," in *Proc. of IEEE International Symposium on Information Theory*, Los Angeles, CA, Jun. 2020, pp. 840–845.

[15] ——, "On covert quantum sensing and the benefits of entanglement," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 352–365, March 2021.

[16] M. S. Bullock, C. N. Gagatsos, S. Guha, and B. A. Bash, "Fundamental limits of quantum-secure covert communication over bosonic channels," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 3, p. 471–482, Mar. 2020.

[17] L. Wang, "Optimal throughput for covert communication over a classical-quantum channel," in *Proc. of IEEE Information Theory Workshop*, Sep. 2016, p. 364–368.

[18] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Reviews of Modern Physics*, vol. 84, no. 2, p. 621–669, May 2012.

[19] S. Yan, B. He, X. Zhou, Y. Cong, and A. L. Swindlehurst, "Delay-intolerant covert communications with either fixed or random transmit power," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, p. 129–140, Jan. 2019.

[20] S. Zhou, M. Zhang, J. Preskill, and L. Jiang, "Achieving the heisenberg limit in quantum metrology using quantum error correction," *Nature Communications*, vol. 9, no. 1, p. 78, Dec. 2018.

[21] D. Layden, S. Zhou, P. Cappellaro, and L. Jiang, "Ancilla-free quantum error correction codes for quantum metrology," *Phys. Rev. Lett.*, vol. 122, p. 040502, Jan. 2019.