Two-way covert quantum communication in the microwave regime

Roberto Di Candia (rob.dicandia@gmail.com)
Aalto University
Hüseyin Yiğitler
Aalto University
Gheorghe Paraoanu
Aalto University
Riku Jäntti
Aalto University

Article

Keywords: Quantum communication, encryption techniques, microwave regime

Posted Date: October 23rd, 2020

DOI: https://doi.org/10.21203/rs.3.rs-93750/v1

Two-way covert quantum communication in the microwave regime

R. Di Candia,[1*] H. Yiğitler,[1] G. S. Paraoanu,[2] and R. Jäntti[1]

[1]Department of Communications and Networking, Aalto University, Espoo, 02150 Finland
[2]QTF Centre of Excellence, Department of Applied Physics,
Aalto University School of Science, FI-00076 AALTO, Finland

*To whom correspondence should be addressed; E-mail: roberto.dicandia@aalto.fi.

Quantum communication addresses the problem of exchanging information across macroscopic distances by employing encryption techniques based on quantum mechanical laws. Here, we advance a new paradigm for secure quantum communication by combining backscattering concepts with covert communication in the microwave regime. Our protocol allows communication between Alice, who uses *only* discrete phase modulations, and Bob, who has access to cryogenic microwave technology. Using notions of quantum channel discrimination and quantum metrology, we find the ultimate bounds for the receiver performance, proving that quantum correlations can enhance the signal-to-noise ratio by up to 6 dB. We show that security can be reached by covering the carrier signal through the presence of the thermal noise in the environment. We complement our information-theoretic results with a feasible experimental proposal in a circuit QED platform. This work makes a decisive step toward implementing secure quantum communication concepts in

the previously uncharted $1-10$ GHz frequency range, in the relevant scenario when the available power is severely constrained.

Introduction

It is well understood that the application of quantum mechanics to traditional technology-related problems may give a new twist to a number of fields. Quantum communication is a potential candidate for over-passing its classical counterpart in terms of information-theoretic security. By appropriately encoding the information in the degrees of freedom of quantum systems, a possible eavesdropping attack can be detected due to the sensitivity of the system to the measurement process. This simple reasoning has been at the basis of defining a number of quantum key distribution (QKD) protocols during the first quantum information era, such as BB84, E91 and B92. The defined protocols have been proven to be unconditionally secure provided that the transmitting channel has a low noise *(1)*. The same level of security would be impossible to reach even in the most sophisticated known classical architectures, which rely on the current impossibility of solving efficiently specific problems, such as prime number factorization or finding the solution of systems of multivariate equations *(2)*. This means that classical encryption techniques are not fundamentally secure: information considered to be safely stored *today* is not guaranteed to be so *tomorrow (3)*. Quantum communication aims to solve this long-term security problem at some infrastructure costs yet to be quantified.

From a theoretical point of view, there is a challenge in defining quantum communication protocols which are secure, efficient and practical at the same time. In this respect, optical systems have been considered for decades the main candidates for quantum communication, as thermal effects are negligible in this frequency range. For instance, QKD security proofs require level of noises which at room temperature are reachable only by frequencies at least in the Terahertz band *(4)*. In addition, entanglement can be distributed with minimal losses, allowing

for the implementation of a series of key long-distance quantum communication experiments, such as quantum teleportation, device-independent QKD, deterministic QKD, superdense coding, among others. The realization of these experiments have been mainly possible because of large efforts in improving photon-detection fidelities, single-photon generation, high-rate entanglement generation, and on-chip fabrication methods *(5)*. Despite these advances in optical technology for quantum communication, low-frequency systems, such as those operating in the microwave or radio wavelengths, have still advantages related to easier electronic design. In addition, microwave signals in the range 100 MHz – 10 GHz belong to the low-opacity window, therefore are particularly suitable for open-air communication applications. These factors also imply lower infrastructure costs for microwave-based communication with respect to the optical one. It is therefore compelling to investigate at the fundamental level whether secure open-air communication protocols are possible at larger wavelengths, with a long-term idea of reaching a network design integrating quantum and classical links, with minimal possible changes in the already existing infrastructure.

With the advent of circuit QED (cQED) as a promising platform for quantum computation, experimental and theoretical research has been focused on understanding the properties of microwave signals at the quantum level. If cooled down at 20 mK, thermal effects are suppressed and microwave electromagnetic fields with frequency above a few GHz show exemplary quantum effects, such as superposition, entanglement and squeezing below vacuum *(6)*. Lately, we have witnessed several experimental advances, which can be regarded as milestones for developing microwave quantum communication, such as improved Josephson parametric amplifiers (JPAs) *(7)*, microwave photodetectors *(8)* and bolometers *(9)*, generation of path-entanglement *(6,10)*, generation of multi-mode entangled states *(11,12)*, and remote state preparation *(13)*. The short-term promise in the field is to demonstrate the quantum teleportation *(14)* and the quantum illumination *(15,16)* protocols in the microwave regime *(17,18)*, which would

then enable real-life applications. Recent theoretical results in noisy quantum sensing and metrology show that preserving entanglement in an experiment is not a fundamental feature for reaching a quantum advantage *(19)*, paving the way for the implementation of open-air quantum microwave protocols.

This Article exploits recent results in quantum communication, quantum sensing and cQED in order to introduce a feasible secure *two-way* quantum communication protocol in the microwave regime. The protocol combines microwave quantum radar technology with covert communication. It consists in the secure exchange of information between a classical party (Alice) and a quantum party (Bob), who pre-share a secret. Bob sends a continuous-variable microwave signal to Alice, which encodes her message in the phase modulation according to a pre-agreed alphabet. The signal is then transmitted back to Bob and measured in order to discriminate between the different modulations (see Fig. 1). As Alice is performing uniquely passive operations at room temperature, she needs only classically available components. If seen from the energy-expenditure perspective, one can think of *one-* and *two-way* protocols as having fundamentally different features in quantum communication. In one-way protocols, Alice (the message transmitter) generates quantum states of some sort, while Bob (the message receiver) has access to some operations typically easy to implement, and a measurement device. Taking into account that even the simplest of the detection schemes, such as homodyne or heterodyne, requires amplifiers and signal generators, a non-negligible energy disposal for both Alice and Bob is required in order to implement any one-way protocol. Our two-way protocol, instead, puts all the challenging technological requirements at Bob's side. In addition, Alice's energy requirements are minimized, envisioning real-life applications in ultra-low power RF communications, Internet-of-Things, and Near Field Communication (NFC) based technology, among others. Our protocol brings in a significant advantage with respect to previous proposals *(20, 21)*, as it does not require active control at Alice side. We discuss both

the cases when the signal is in a coherent state and when it is correlated with an idler. The latter shows a gain of up to 6 dB in the signal-to-noise ratio (SNR) with respect to the former one, at some experimental cost in the preparation and the detection stages by Bob. The setup resembles the Gaussian quantum illumination protocol *(19)*, where a weak two-mode squeezed vacuum (TMSV) state is transmitted in a bright environment in order to detect the presence or absence of a low-reflectivity object in a region of space. Unlike radar applications, for which the quantum illumination paradigm is usually employed *(15,18)*, and where location, velocity and cross-section are unknown, our communicating setup can be thought to be applied with static antennas where all these properties are known and can be engineered. In the first part of the paper, we derive a general expression for the error probability, putting an emphasis on Gaussian states and Schrödinger's cat (SC) states *(22)*. We prove that 6 dB is indeed the maximal gain in the error probability exponent reachable by a quantum-correlated state over a coherent state receiver. This also solves an open problem in quantum illumination *(23)*. We show that our communication protocol is unconditionally secure by means of *covertness (24)*. In a covert quantum communication protocol the signal is hidden in the thermal noise unavoidably present in a room-temperature environment, so that Eve's detection probability collapses. The basic idea is therefore to protect unconditionally the message content by hiding its existence. This concept has a natural application in low-frequency spectrum communication. Security is achievable only if the generated signal is weak enough, so that cryogenic detection technology is needed at Bob's side. Here, we show the square-root-law for our two-way communication protocol, proving that the number of bits that can be sent over n channel usages scales as $O(\sqrt{n})$. Finally, we design an entanglement-assisted protocol based on SC states in a circuit QED (cQED) setup, which relies solely on Jaynes-Cumming interactions and qubit measurements. This shows the path for future experimental investigation of our concept.

The Setup

The two-way communication protocol is depicted in Fig. 2. Alice and Bob use $n = mM$ modes of the bosonic channel simultaneously in order to communicate m symbols. They use M modes to transmit a symbol ϕ taken from a discrete alphabet $\mathcal{A}$. We refer to each these M channel usages as a *slot*. In each slot, Bob generates M independent and identically distributed (i.i.d) signal modes $\{\hat{a}_S^{(k)}\}$ ($k = 1, \ldots, M$) with $N_S > 0$ average number of photons, and he sends the modes to Alice. The signal modes are possibly entangled with M idler modes $\{\hat{a}_I^{(k)}\}$, which are retained in the lab by Bob for the measurement stage. The signals are generated at a low enough temperature to consider the signal-idler (SI) state as pure. Although the results of this article are general, we emphasize the application in the microwave spectrum, specifically in the range of operating frequencies of a cQED setup, i.e. 1-10 GHz. In this range of frequencies, $T \simeq 20$ mK is required to avoid thermal fluctuations. We refer to the *idler-free* case when the idler is absent, or, equivalently, when the signal and the idler are uncorrelated. The signal modes are sent to Alice through a room-temperature channel ($T_B = 300$ K), which is modeled as a beamsplitter. Alice receives the modes $\{\hat{a}_S^{\prime(k)}\}$, with

$$\hat{a}_S^{\prime(k)} = \sqrt{\eta}\, \hat{a}_S^{(k)} + \sqrt{1-\eta}\, \hat{h}_{\leftarrow}^{(k)}. \tag{1}$$

Here, η is the power transmitting rate of the channel and $\{\hat{h}_{\leftarrow}^{(k)}\}$ are independent thermal modes with N_B average number of photons. The numerical value of N_B depends on the signal operating frequency ω_k as $N_B = (e^{\beta\hbar\omega_k} - 1)^{-1}$ with $\beta = (k_B T_B)^{-1}$, k_B being the Boltzmann constant. In the $1 - 10$ GHz spectrum this results to values of the order $N_B \sim 10^3$, therefore we will emphasize the $N_B \gg 1$ case. Alice modulates the phase of $\hat{a}_S^{\prime(k)}$ by $\tilde{\varphi}_k = \phi + \varphi_k$, with $\phi, \varphi_k \in \mathcal{A}$, generating the mode $e^{-i\tilde{\varphi}_k}\hat{a}_S^{\prime(k)}$. She then sends the signal back to Bob through the same channel. Here, ϕ embeds the symbol to be transmitted, while the phase-shift $e^{-i\varphi_k}$ is an encoding operation that Alice and Bob have secretly pre-shared. Bob receives the modes $\{\hat{a}_R^{(k)}\}$,

with

$$\hat{a}_R^{(k)} = \sqrt{\eta}\,(e^{-i\tilde{\varphi}_k}\hat{a}_S^{\prime(k)}) + \sqrt{1-\eta}\,\hat{h}_{\rightarrow}^{(k)}, \tag{2}$$

Here, $\{\hat{h}_{\rightarrow}^{(k)}\}$ are M independent thermal modes identical to $\{\hat{h}_{\leftarrow}^{(k)}\}$. We also assume that the modes $\{\hat{h}_{\leftarrow}^{(k)}\}$ and $\{\hat{h}_{\rightarrow}^{(k)}\}$ are independent. Bob applies the decoding transformation $e^{i\varphi_k}$ to the received mode $\hat{a}_R^{(k)}$. He then applies a discrimination strategy to the modes $\{e^{i\varphi_k}\hat{a}_R^{(k)}, \hat{a}_I^{(k)}\}$ for distinguishing between the different symbols in $\mathcal{A}$.

For a given symbol transmission ϕ, we denote with $\rho_{\eta,\phi}$ the density matrix of Bob's state at the receiver, i.e. the state of the system defined by the modes $\hat{a}_R^{(k)}$ and $\hat{a}_I^{(k)}$. As we are working in the i.i.d. assumption, $\rho_{\eta,\phi}$ does not depend on k. In the following, we work under the $\eta \ll 1$ assumption, corresponding to a very lossy thermal propagation channel. This is typically the case for open-air wave propagation. The number M has to be chosen to be large enough in order to give Bob the chance of discriminating between the possible phases in $\mathcal{A}$ with high confidence. The measurement discriminating between the symbols depends on the adopted SI system. We consider mainly the Binary-Phase-Shift-Keying (BPSK) alphabet, when $\mathcal{A} = \{0, \pi\}$. However, the results in this article can be extended to more complex alphabets. Different figures of merit can be used to quantify the performance of the optimal strategies to discriminate between the distinct modulations, depending on their a priori probabilities. Here, we discuss the case where all the modulations in the key have the same a priori probability of being realized, which is the most natural scenario for quantum communication.

The setup can be mapped to quantum illumination *(19)*, also referred to On-Off-Keying (OOK), where Alice modulates the amplitude of the signal. In fact, BPSK and OOK share the same optimal strategies in the $\eta \ll 1$ limit (see Material and Methods). In addition, BPSK performs better than OOK for given transmitting power, as the distance of the symbols in the phase-space is larger. A similar setup has been studied in the optical domain *(21)*. Here, a

phase-insensitive amplification by Alice is required in order to add thermal noise and ensure security with respect to a passive Eve. In the low-frequency spectrum, the thermal noise is naturally present in the environment, so that no amplification is needed and covertness can be ensured. Instead, in Ref. *(25)*, the authors discuss the advantage of using pre-shared entanglement between Alice and Bob for communication in noisy environment, finding that the number of covert bits that can be sent increases by a logarithmic factor with respect to the unentangled case. Although their setup falls in the one-way scenario, these results suggest that using quantum correlations should come with a logarithmic overhead in the capacity also in our case.

Results

Ultimate bounds for the receiver performance

We find the ultimate bounds on the receiver performance for the protocol described in Fig. 2. These results hold for SI systems in any quantum state. We set the encoding operation to the identity, i.e. we fix $\varphi_k = 0$. This is possible because both Alice and Bob have a pre-shared knowledge of φ_k, therefore this operation can be reversed by Bob. In the BPSK case, where the $\phi \in \{0, \pi\}$, our aim is to minimize the total error probability

$$p_{\text{err}} = \frac{1}{2}\left[\Pr\left(\phi = \pi | \phi = 0\right) + \Pr\left(\phi = 0 | \phi = \pi\right)\right], \tag{3}$$

where $\Pr\left(\phi = \pi | \phi = 0\right)$ is the probability of detecting a phase $\phi = \pi$ given that Alice has modulated the phase of the signal by $\phi = 0$, and a similar definition holds for $\Pr\left(\phi = 0 | \phi = \pi\right)$. The main strategies to achieve this can be classified in (i) *collective*, where the M modes are allowed to be measured together, and (ii) *local*, where the copies are measured separately, allowing classical communication between the measurements on the different copies. We consider the performance of a coherent state transmitter as reference for the correlated cases. In other contexts, such as in quantum illumination, coherent states transmitters are usually used as a

classical reference. This choice is done mainly for two reasons: 1) they achieve the optimal error probability in the idler-free case and 2) they describe faithfully coherent signals that can be generated with classical technology.

A. Collective strategies

The quantum Chernoff bound *(26)* provides an upper bound on the achievable error probability (EP) in the binary detection problem. Indeed, we have that $p_{\text{err}} \leq \frac{1}{2}e^{-\beta_\eta M}$, where $\beta_\eta = -\min_{s\in(0,1)} \log \text{Tr}\left(\rho_{\eta,0}^s \rho_{\eta,\pi}^{1-s}\right)$. This bound is tight for $M \gg 1$, and its exponent β_η can be used as figure of merit for quantifying the performance of the optimal discrimination protocol. Generally, one needs a collective measurement over all the M modes in order to saturate this bound. There are few exceptions to this statement, for instance, when either one of $\rho_{\eta,0}$ or $\rho_{\eta,\pi}$ is close enough to a pure state *(30)*, or for coherent state illumination in a bright environment.

In the following, we focus on computing analytically β_η up to the first relevant order in η, using a metric-based approach. As the the expansion of β_η to the first order of η is zero (see Material and Methods, Lemma 3), we can define the figure of merit for collective strategies as

$$\beta^{col} \equiv \lim_{\eta\to 0} \frac{\beta_\eta}{\eta^2}. \tag{4}$$

This metric provides us a framework for conducting comparative analysis between different transmitters. In addition, the found relations can be analytically computed, providing an insight on the scaling of the performance with respect to the system parameters. We are particularly interested in the $N_S \ll 1$ and $N_B \gg 1$ limits of β^{col}, where the protocol based on quantum correlations will present the maximal advantage with respect to a coherent state input with the same power. In addition, we will see that unconditional security by means of covertness can be ensured in this regime. In the following, for simplicity, we will refer to β^{col} as the quantum Chernoff bound (QCB). However, we stress that in the literature the QCB is generally referred

as β_η. The following results define the optimal receiver performances.

Theorem 1. [Ultimate receiver-EP bound: idler-free case] *Coherent states maximize β^{col} in the idler-free case. Its optimal value is*

$$\beta_{cl}^{col} = \frac{4N_S}{1+N_B}\frac{1}{\left(1+\sqrt{c_B}\right)^2}, \tag{5}$$

where $c_B = \frac{N_B}{1+N_B}$.

This is in agreement with the result of the standard quantum illumination protocol, up to a factor of four (see Material and Methods). We notice that $\beta_{cl}^{col} \simeq N_S/N_B$ in the $N_B \gg 1$ limit, which makes the comparison with the general correlated case easier.

Theorem 2. [Ultimate receiver-EP bound] $\beta^{col} \leq \min\{\frac{4N_S}{1+N_B}, \frac{2N_S+1}{1+N_B}\frac{1}{2\sqrt{c_B}}\}$.

The bound in Theorem 2 is tight for $N_S \ll 1$ and for $N_S, N_B \gg 1$. By a direct comparison with the bound in Theorem 2 and the QCB for coherent states, we see that the optimal gain with respect to the idler-free case is 6 dB, and the maximal advantage can be achieved when $N_B \gg 1$ and $N_S \ll 1$. No advantage can be detected in a vacuum environment ($N_B \ll 1$), which is the case of the optical systems. In addition, even in the $N_B \gg 1$ limit, the gain decreases with increasing number of signal photons N_S, achieving the same performance of a coherent state transmitter in the $N_S \gg 1$ limit. This makes the setup in Fig. 2 particularly relevant for studying entanglement-assisted low-frequency communication in very noisy environment. However, one must note that the advantage of using quantum correlations is kept when the environment is not bright, see Fig. 3a. For instance, a 4.6 dB maximal advantage can be achieved for $N_B \simeq 1$, implying that the advantage in using quantum correlations is not limited to the $N_B \gg 1$ case.

B. Quantum estimation strategies

An approach based on the quantum estimation of the amplitude modulation has been developed

in Ref. *(27)* in the quantum illumination context. This is less experimentally demanding than the collective strategy, as it does not require the interaction between the M copies of the received signal. However, it comes at some loss in the error exponent of the EP, quantified as at least 3 dB with respect to the optimal collective strategy. Here, we use the same concept in order to deal with the BPSK case. We address this approach as *local* strategy, as opposite of the collective strategies previously discussed. First, we notice that the received modes $\{\hat{a}_R^{(k)}\}$ can be expressed as

$$\hat{a}_R^{(k)} = \eta\, e^{-i\phi}\hat{a}_S^{(k)} + \sqrt{1-\eta^2}\,\hat{h}^{(k)}, \tag{6}$$

where $\hat{h}^{(k)} \equiv \sqrt{\frac{\eta}{1+\eta}}\; e^{-i\phi}\hat{h}_{\leftarrow}^{(k)} + \sqrt{\frac{1}{1+\eta}}\;\hat{h}_{\rightarrow}^{(k)}$ are thermal modes with N_B average number of photons. We can thus optimally estimate the parameter $\kappa \equiv \eta\, e^{-i\phi} \in \mathbb{R}$, obtaining a value κ_{est}, and deciding towards the hypothesis $[\phi = 0]$ if $\kappa_{est} > 0$ or the hypothesis $[\phi = \pi]$ if $\kappa_{est} < 0$. We refer to this strategy as "threshold discrimination strategy". The main figure of merit quantifying the quantum estimation performance is the quantum Fisher information (QFI), defined as *(28)*

$$F = \sum_{mn} \frac{|\langle\phi_m|d\rho|\phi_n\rangle|^2}{\lambda_m + \lambda_n}, \tag{7}$$

where $d\rho = (\partial_\kappa \rho_\kappa)_{|\kappa=0}$, with $\rho_\kappa \equiv \rho_{\eta.\phi}$, and λ_m is the eigenvalue of ρ_0 corresponding to the eigenstate $|\phi_m\rangle$. This is due to the Cramer-Rao bound, which asserts the limit of the achievable precision of an unbiased estimator $\hat{\kappa}$: $\Delta\hat{\kappa}^2 \geq 1/MF$. An estimator saturating the Cramer-Rao bound is given by the mean over the M single-copy measurements of the observable $\hat{O} = \hat{L}/F$, where $\hat{O} = \sum_{mn} \frac{\langle\phi_m|d\rho|\phi_n\rangle}{\lambda_m+\lambda_n}|\phi_m\rangle\langle\phi_n|$ is the symmetric logarithmic derivative computed at $\kappa = 0$. Due to the central limit theorem, the EP for the threshold discrimination strategy is $p_{\text{err}} \simeq 1 - \text{erf}\,(\eta\sqrt{FM/2}) \leq \frac{1}{2}e^{-\eta^2 FM/2}$ for $M \gg 1$. The previous discussion holds whenever one has an a priori knowledge of the neighborhood where κ belongs to (in our case $\kappa \ll 1$). If no assumptions of this sort can be made, generally the optimal strategy consists of a two-stage

adaptive protocol: use $M^{1/\delta}$ (with $\delta > 1$) copies to estimate the neighborhood and then use the rest of the copies to optimal estimate the parameter. This provides the same asymptotic performance as when the information on the neighborhood is provided. The same adaptive protocol can be used to generalize the ideas of this article to more complex alphabets, by first having a rough estimation of the phase ϕ, and then rotate the system in order to maximize the classical Fisher information *(29)*.

Similarly to the case of collective strategies, we will adopt the exponent of the EP to the first relevant order in η as figure of merit, i.e. $\beta^{loc} \equiv F/2$. We have the following bounds on the achievable EP decaying rate using quantum estimation methods.

Theorem 3. [Ultimate QFI bound] $\beta^{loc} \leq \min\{\frac{2N_S}{1+N_B}, \frac{2N_S+1}{1+N_B}\frac{1}{2\sqrt{c_B}}\}$.

Similarly to Theorem 2, the bound in Theorem 3 is tight for $N_S \ll 1$ and for $N_S, N_B \gg 1$. It follows that the maximal advantage with respect to the classical case is 3 dB in the EP exponent if we adopt a threshold discrimination strategy.

Theorem 4. [Ultimate QFI bound: idler-free case] *Coherent states maximize β^{loc} in the idler-free case. The optimal value is given by*

$$\beta_{cl}^{loc} = \frac{2N_S}{1+N_B}\frac{1}{1+c_B}, \tag{8}$$

where $c_B = \frac{N_B}{1+N_B}$. The optimal detector is homodyne.

This means that the optimal detector in the classical case can be implemented with local measurements in the $N_B \gtrsim 2$ regime, as in this case $\beta_{cl}^{loc} \simeq \beta_{cl}^{col}$. However, this is not anymore valid in the $N_B \lesssim 1$ regime, where collective measurements start to perform better, achieving $\beta_{cl}^{col} \simeq 2\beta_{cl}^{loc}$ in the $N_B \ll 1$ limit.

Examples

The aim of this section is to discuss two topical examples of transmitters whose optimal receiver saturates the ultimate bounds in the correlated case. In order to do so, we have derived explicit, general, formulas for the QCB in terms of the Schmidt values of the input state (see Material and Methods).

A. Two-mode squeezed vacuum state transmitter

We compute the ideal performance of entangled Gaussian states using the figures of merit β^{col} and β^{loc}. TMSV states are defined as

$$|\psi\rangle_{\text{TMSV}} = \sum_{n=0}^{\infty} \sqrt{\frac{N_S^n}{(1+N_S)^{1+n}}} |n\rangle_I |n\rangle_S, \tag{9}$$

where $\{|n\rangle\}_{n=0}^{\infty}$ is the Fock basis. They have been thoroughly studied in the context of QI because they are a good benchmark to show a quantum advantage and because they are experimentally easy to generate, regardless of the frequency regime. The performance for the optimal receiver of a TMSV state transmitter are given by

$$\beta^{col}_{\text{TMSV}} = \frac{4N_S}{1+N_B} \frac{1}{\left(1+\sqrt{c_S c_B}\right)^2} \tag{10}$$

$$\beta^{loc}_{\text{TMSV}} = \frac{2N_S}{1+N_B} \frac{1}{1+c_S c_B}, \tag{11}$$

where $c_S = \frac{N_S}{1+N_S}$ and $c_B = \frac{N_B}{1+N_B}$ (see Material and Methods). The optimal receiver for a threshold discrimination strategy consists in measuring in the eigenbasis of $\hat{a}_I \hat{a}_R + \hat{a}_I^\dagger \hat{a}_R^\dagger$. It is clear that TMSV states saturate the bound of Theorem 2 in the $N_S \ll 1$ limit. In addition, the advantage of using the optimal detector for TMSV states decays slowly with increasing N_S, making the protocol useful also for finite number of signal photons. The detectors achieving the maximal gain are known for both the collective (only for $N_S \ll 1$ *(30)*) and the local (for

any N_S *(31)*) cases. Generally, they involve photon-counting devices, which are yet to be developed in the microwave regime. A possible solution is the use optomechanical transducers into optical frequencies, where sensitive detectors are available *(17)*. However, current optomechanical transducers are still in infancy, as they suffer from low efficiencies and high thermal added noise. A different solution is to use a qubit as single-photon detector. This approach has the advantage of seamless integration with cQED platforms, as dispersive qubit measurements can be implemented already in the lab *(36)*. However, single-photon detection devices so far have achieved only a $70\ \%$ fidelity, making this approach currently unsuitable for practical applications. On a different note, the idler storage must be carefully considered in order to understand how quantum correlations can be useful in practice. In cQED, memory elements based on a coaxial $\lambda/4$ resonator with coherence time of nearly 1 ms have been demonstrated *(32)*. This corresponds to 300 Km of free-space propagation of light. Another promising alternative consists in transferring the idler bosonic degrees of freedom to the delay line based on surface acoustic waves *(33)*.

Assuming that an effective way of measuring the power of large bandwidth signals with few-photons sensitivity is available, then a Gaussian state protocol is arguably the best option for implementing the ideas presented this article. In fact, if we consider $N_S = 10^{-2}$, $N_B = 10^3$ and $\eta = 10^{-2}$ as typical parameter values, a time-bandwidth product $M = 10^8$ is needed for reaching low enough receiver error probabilities. The ability of generating large bandwidth Gaussian signals would reduce the time complexity of the protocol. Even though at the present stage Gaussian states remains the main solution for sensing and metrology in noisy regime, we discuss an alternative based on a promising quantum computing paradigm in cQED.

B. Schrödinger's cat state transmitter

We now discuss the performance of the protocol based on SC states, created by the interaction

of a qubit with a continuous-variable signal. It comes as no surprise that SC states show the same advantage of Gaussian states for $N_S \ll 1$, because in this limit the two states approximate each other. However, in the following we will see that the underlying physics is different. In fact, the proposed architecture will provide us with a digital way to store the idler in a cQED setup. The SC states that we consider are defined as

$$|\psi\rangle_{\rm SC} = \frac{1}{\sqrt{2}}\left[|+\rangle_I|\alpha\rangle_S + |-\rangle_I|-\alpha\rangle_S\right], \tag{12}$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|g\rangle \pm |e\rangle)$ are eigenstates of the Pauli operator $\hat{\sigma}_x$, $|\alpha\rangle$ is a coherent state with amplitude $\alpha > 0$ ($N_S = |\alpha|^2$), assumed to be real for simplicity. Of particular interest will be the case of $|\alpha| \ll 1$, that shows the maximal advantage with respect to the classical case. This state can be written in the Schmidt decomposition as

$$|\psi\rangle_{\rm SC} = \sqrt{\lambda_+}|g\rangle|\alpha_+\rangle + \sqrt{\lambda_-}|e\rangle|\alpha_-\rangle, \tag{13}$$

where $\lambda_\pm = \frac{1}{2}(1 \pm e^{-2N_S})$ and $|\alpha_\pm\rangle = \frac{1}{2\sqrt{\lambda_\pm}}[|\alpha\rangle \pm |-\alpha\rangle]$. The performance of the optimal receiver for a SC-state transmitter are given by

$$\beta_{\rm SC}^{col} = \frac{N_S}{1+N_B} f_{\rm SC}^{col}(N_S, N_B), \tag{14}$$

$$\beta_{\rm SC}^{loc} = \frac{N_S}{2+2N_B} f_{\rm SC}^{loc}(N_S, N_B), \tag{15}$$

where

$$f_{\rm SC}^{col} \overset{N_B \gg 1}{=} 1 - 2\sqrt{N_S} + O(N_S) \tag{16}$$

$$f_{\rm SC}^{loc} \overset{N_B \gg 1}{=} 1 - 2N_S + O(N_S^2). \tag{17}$$

The optimal threshold discrimination strategy in the $N_B \gg 1$ regime consists in measuring in the eigenbasis of the observable $\hat{O}_{opt} = \hat{\sigma}^-[\lambda_+\hat{a}_R + \lambda_-\hat{a}_R^\dagger] + c.c.$. The exact expressions of $f_{\rm SC}^{col}$ and $f_{\rm SC}^{loc}$ are given in the Material and Methods. A comparison with the TMSV state case is

shown in Fig. 3b. As expected, the maximal gain can be achieved for $N_S \ll 1$. In addition, the gain decays exponentially with increasing N_S. In fact, the observable $\hat{\sigma}_x(\hat{a}_R + \hat{a}_R^\dagger)$ is optimal for $N_S \gtrsim 1$, therefore the classical mixed state $\frac{1}{2}[|+\rangle_I\langle+| \otimes |\alpha\rangle_S\langle\alpha| + |-\rangle_I\langle-| \otimes |-\alpha\rangle_S\langle-\alpha|]$ performs the same as $|\psi\rangle_{\rm SC}$ in this regime. This loss of gain for finite N_S can be mitigated by considering states with larger Schmidt rank, i.e. $\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}|w_k\rangle_I|\alpha_k\rangle_S$, where $\alpha_k = \sqrt{N_S}e^{i\frac{2\pi k}{d}}$ and the idler is a d-level system with $\langle w_k|w_{k'}\rangle = \delta_{k,k'}$ *(27)*. This state can be implemented by letting several transmon qubits interacting with the same resonator. However, in this case the optimal detector is complicated and we will not consider it in the implementation discussion.

Covert quantum communication

We now discuss the possibility of performing secure quantum communication using the setup depicted in Fig. 2, by exploiting recent results about covert quantum communication *(24,35*. The basic idea is to protect the content of the message to be transmitted by covering the existence of the carrier in a given bandwidth and temporal frame. In this context, Eve's main task becomes to understand whether a message is being transmitted or not through the channel. Here, we provide bounds for Eve's detection probability depending on the receiver performance. The results of this Section holds for states which well approximates Gaussian states in the $N_S \ll 1$ limit. We prove that $\bar{m} = O(\sqrt{n})$ number of bits securely transmittable over n channel usages with an arbitrary small EP. We also show that quantum correlations can increase the bit transmission rate by a constant factor, depending on strategy adopted (i.e. collective or local).

A natural way of defining covertness consists in bounding from below the probability of detecting that communication between Alice and Bob is happening.

Definition 1. [Covertness criteria] *A communicating system is δ-covert over n channel usages if Eve's EP in discerning between the equally likely hypothesis of communication happening or not-happening is $P^{(\rm Eve)} \geq \frac{1}{2} - \delta$ for n large enough.*

Ideally, we would like to have δ as smaller as possible by still being able to communicate a finite number of bits. Generally, covert communication is possible because Eve does not have control at least to a part of the environmental channel *(24)*. This assumption is not radical, as in the low-frequency regime at room temperature there is an unavoidable noise dictated by the laws of physics. We assume that Bob's and Alice's places, where the state manipulation and the measurements are implemented, are sealed, and that the signals are sent directly to a room temperature environment where Eve may be placed. We also assume, for simplicity, that the part of the channel that Eve cannot control does not change while communication is in progress. The latter assumption can be relaxed by analyzing more general fading communication channel models, where the amplitude losses and/or the signal phases are random variables *(36)*. In addition, we provide Alice with the capability of implementing *truly* random phase modulations on her signal on the alphabet $\mathcal{A}$. This is an important requirement for ensuring covertness in the two-way setup.

Alice and Bob use $n = mM$ modes of the bosonic channel simultaneously. They use M modes to transmit a symbol taken from a discrete alphabet $\mathcal{A}$. In addition, they use a publicly available codebook $\mathcal{C}$ that maps $\bar{m}$-bit input blocks to m-symbol codewords from $\mathcal{A}^m$, with $\bar{m} < m$, by generating $2^{\bar{m}}$ codeword sequences, i.e. $\mathcal{C} = \{a_k \in \mathcal{A}^m\}_{k=1}^{2^{\bar{m}}}$. The codebook is built in the way that the codewords, when the transmission is corrupted by the channel, are distinguishable from each other with high probability. This induces a natural way of defining when communication is reliable.

Definition 2. [Reliability criteria] *A communicating protocol is ϵ-reliable if the decoding error probability averaged over the codebook is bounded by ϵ, i.e. when $\frac{1}{|\mathcal{C}|}\sum_{a_k\in\mathcal{C}}\sum_{a_j\in\mathcal{C}\setminus\{a_k\}} P(a_j|a_k) \leq \epsilon$ for n large enough.*

We focus primarily to the BPSK case, corresponding to $\mathcal{A} = \{0, \pi\}$, keeping in mind that the concept can be generalised to more complex constellations. Each symbol transmission is

done by performing the two-way protocol described in the Fig. 2. We define the on-setting, corresponding to the case when the communication is happening, and the off-setting, when no information is exchanged between Alice and Bob. In other words, we consider the on-setting when Alice and Bob applies the protocol with $N_S > 0$, while the off-setting is when $N_S = 0$. We consider a passive eavesdropper, able to catch all the modes that are lost in the Bob-Alice path, denoted with the $\leftarrow$ subscript, and Alice-Bob path, denoted with the $\rightarrow$ subscript. For a given slot, Eve gets the modes

$$\hat{w}_{\leftarrow}^{(k)} = -\sqrt{1-\eta}\,\hat{a}_S^{(k)} + \sqrt{\eta}\,\hat{h}_{\leftarrow}^{(k)} \tag{18}$$

$$\hat{w}_{\rightarrow}^{(k)} = -\sqrt{1-\eta}\,e^{-i\tilde{\varphi}_k}\hat{a}_S^{\prime(k)} + \sqrt{\eta}\,\hat{h}_{\rightarrow}^{(k)}, \tag{19}$$

for $k = 1, \ldots, M$. Here, $\{N_S > 0,\ \tilde{\varphi}_k = \varphi_k + \phi\}$ defines the on-setting, while $\{N_S = 0,\ \tilde{\varphi}_k = \varphi_k\}$ is the off-setting. The goal is to let the on and the off settings the least distinguishable possible. This is possible only in the $N_S \ll 1$ limit, as in this case Eve's mode in both settings approximate each other. This is due to the fact that both $\varphi_k + \phi$ and φ_k are distributed uniformly at random in the alphabet $\mathcal{A}$. The inclusion of the random sequence of phase-shifts by Alice is a crucial requirement for the covertness proof, as otherwise Eve would have enough resources to uncover the communication by detecting the phase ϕ in a given slot. However, she can still detect if communication is happening by detecting the changes in power of each path, and their correlations. As all the $\hat{a}_S^{(k)}$ are i.i.d., Eve's quantum state does not depend on k and on which symbol is being transmitted.

Lemma 1. [Covertness achievability] *Let $N_S > 0$ be the average number of signal photons in the on-setting. Let the signal density matrix be $\rho_S = \sum_{j=0}^{\infty} N_S^j \sigma_j$, where*

$$\sigma_0 = |0\rangle\langle 0| \tag{20}$$

$$\sigma_1 = |1\rangle\langle 1| - |0\rangle\langle 0| \tag{21}$$

$$\sigma_2 = c(|2\rangle\langle 2| - 2|1\rangle\langle 1| + |0\rangle\langle 0|), \tag{22}$$

with $0 \leq c \leq 1$. *Then, the communication between Alice and Bob is* δ*-covert over* n *channel usages, provided that* $N_S \leq \frac{4\sqrt{\eta^2 N_B(1+\eta^2 N_B)}}{(1-\eta^2)^2}\frac{\delta}{\sqrt{n}}$.

In the Supplemental Material we also prove the converse of Lemma 1. Lemma 1 can be directly applied to a TMSV state transmitter, which corresponds to $c = 1$. It can be also applied to coherent state and SC state transmitters, if we allow Bob to perform random phase modulations. In fact, let $|\alpha_k\rangle$ with $\alpha = |\alpha|e^{-ik\pi/4}$ be a coherent state, then $\rho_S = \frac{1}{8}\sum_{k=0}^{7}|\alpha_k\rangle\langle\alpha_k|$ respects the conditions of Lemma 1 with $c = 1/2$. Bob's phase modulation at the transmission can be reversed at the receiver level due to the linearity of the communicating channel. We also notice that a Gaussian thermal state at Bob's side is not needed in order to ensure covertness, meaning that complex Gaussian modulations of Bob's signal are not needed. We can rely instead on discrete phase modulations, which are experimentally easier to generate and they require less memory complexity.

We have provided an upper bound on the average transmitting power N_S, which need to scale as $1/\sqrt{n}$ in order to keep the communication covert over n channel usages. Typical transmitter operates at constant photon number per mode, and the requirement of N_S decaying with the inverse of $\sqrt{n}$ can be quite restrictive. This constraint can be relaxed by defining a *probabilistic* version of the protocol, which makes use only of a fraction $\tau \leq \frac{4\eta^2 N_B}{N_S}\frac{\delta}{\sqrt{n}}$ of the n available modes in the *on*-setting *(35)*, see Fig. 4. In each of these modes, the transmitting power N_S is kept constant and small.

Lemma 1, together with a random-coding argument (see Material and Methods), implies that the square-root-law is achievable by our two-way setup.

Theorem 5. [Square-root law: two-way setup] *Let Alice and Bob share a publicly available codebook and a secret random sequence of length* n. *Then, they can communicate* $\bar{m} = \frac{2}{\log 2}c_B\beta\delta\eta^4\sqrt{n} + \log_2\epsilon$ *bits over* n *channel usages by keeping the system* δ*-covert and the communication* ϵ*-reliable, provided that Bob has access to a signal generator satisfying the*

assumption of Lemma 1. Here, β is a constant that depends on the detector: $\beta = 4$ ($\beta = 2$) for the TMSV state and SC state transmitters with the optimal collective (local) receiver, and $\beta = 1$ for the coherent state transmitter with a homodyne receiver.

Summarizing, Alice and Bob need to agree secretly on the following information prior the communication: (i) A secret random sequence corresponding to the random phase-shifts by Alice. This information requires $O(n \log |\mathcal{A}|)$ bits of pre-shared knowledge, or $O(\sqrt{n} \log |\mathcal{A}|)$ in the probabilistic version. (ii) In the probabilistic version, the information needed to specify the modes which are used in the on-setting. This requires $O(\sqrt{n} \log n)$ bits of shared secret.

It is clear that there is at least a logarithmic overhead of number of pre-shared bits with respect to the transmitted ones, if we want to ensure covertness. In order to mitigate this problem, one can define a protocol based on pseudo-random generating functions *(37)*. Indeed, if Alice and Bob pre-share a pseudo-random generating function $f : \{0,1\}^l \to \{0,1\}^{p(l)}$, where $l \in \mathbb{N}$ and $l = o(p(l))$ for $l \gg 1$, then it is possible to communicate more bits than the pre-shared ones. Widely used Advanced Encryption Standard and the Secure Hashing Algorithm have outputs that are exponentially larger than their seeds while still retaining computational indistinguishability from true randomness *(37)*. This is therefore a practical tool for for covert quantum key distribution protocols, where one wants to covertly expand a pre-shared key, keeping in mind that the security of the protocol is bounded by the security of the pseudo-random function f.

Circuit-QED Implementation

The ideas introduced in this paper can be easily implemented using coherent states properly modulated, as described in the previous section, and heterodyne measurement. While this scheme does not achieve any of the ultimate bounds for the receiver, it is the most practical way of realizing the protocol. If one is allowed to implement certain entangling operations at the transmitting and receiver level, then larger key rates are achievable. In this context, optimal

schemes for the Gaussian state receiver have been thoroughly studied in the literature. Instead, a receiver for the SC state transmitter is still missing. In this Section, we fill this gap by introducing an implementation in a circuit QED setup for a SC state based transmitter and receiver. We show that Jaynes-Cumming (JC) operations and qubit measurements are sufficient to fully implement the protocol. This is a big advantage with respect to the Gaussian state receiver, which requires photo-detectors. We also provide an analysis of how the decoherence affects the protocol based on quantum correlations. The discussion will be mostly at the model level. However, it is noteworthy to observe that all the operations described in the following have been proved in cQED since fifteen years, with increasing enhancements of fidelity for the gate implementation and state storage.

A. Schrödinger's cat state preparation

The SC state defined in Eq. (12) can be prepared in a circuit QED setup as described in the following. Consider the JC Hamiltonian

$$\hat{H} = \hat{H}_0^{(\omega_r,\omega_q)} + \hat{H}_{JC}^{g}, \tag{23}$$

where $\hat{H}_0^{(\omega_r,\omega_q)} = \hbar\omega_r \hat{a}^\dagger \hat{a} + \frac{\hbar\omega_q}{2}\hat{\sigma}_z$, with $\hat{\sigma}_z = |e\rangle\langle e| - |g\rangle\langle g|$, and $\hat{H}_{JC}^{g} = \hbar g(\hat{\sigma}^+ \hat{a} + \hat{\sigma}^- \hat{a}^\dagger)$. Here, ω_r and ω_q are the frequency of the resonator and the qubit respectively, and g is the coupling between these two systems. We also define the detuning $\Delta = \omega_r - \omega_q$ and $\Gamma = \max\{\kappa, 1/T_1, 1/T_2\}$, where κ is the cavity decay rate, and T_1 and T_2 are the qubit decaying and dephasing times respectively (see Supplemental Material). In the dispersive regime, where $\Delta \gg g$, one can apply perturbation theory to the first order of the parameter g/Δ, finding the effective Hamiltonian

$$\hat{H}_{SDR} = \hat{H}_0^{(\omega_r,\omega_q+\chi)} + \hbar\chi\hat{\sigma}_z\hat{a}^\dagger\hat{a}, \tag{24}$$

where $\chi = g^2/\Delta$ *(38)*. We assume that $\chi \gg \Gamma$, which is known as the *strong-dispersive regime* (SDR). In this way, any losses of the bosonic mode and the qubit are negligible during

the implementation of the gate, as long as the operating time will be sufficiently short. The preparation protocol is based on the fact that the Hamiltonian H_{SDR} is a conditional phase-shift on the resonator, with the qubit acting as the control. To put this easier in evidence, we will work in a rotating frame defined by the free Hamiltonian $\hat{H}_0^{(\omega_r,\omega_q+\chi)}$. The Hamiltonian in the rotating frame is $\chi\sigma_z\hat{a}^\dagger\hat{a}$. The preparation protocol consists in the following steps, assuming an initial qubit-resonator state $|g\rangle|0\rangle$ (see Fig. 5).

Step 1 Apply a $\pi/2$ $\hat{\sigma}_y$-pulse to the qubit in the ground state, and drive the resonator at frequency ω_r with a signal calibrated such that the coherent state $|-i\alpha\rangle$ is prepared.

Step 2 Let the qubit and the resonator interact for a time $t_\chi = \frac{\pi}{2\chi}$. This results in a conditional phase shift on the cavity state by the operator $|g\rangle\langle g| \otimes \exp(i\pi\hat{a}^\dagger\hat{a}/2) + |e\rangle\langle e| \otimes \exp(-i\pi\hat{a}^\dagger\hat{a}/2)$, Its action on the state prepared at Step 1 can be understood as a uniform counterclockwise rotation by an angle $\pi/2$ of the coherent state, followed by the application of the photon parity operator $\exp(-i\pi\hat{a}^\dagger\hat{a})$ if the qubit is excited. The state after this step is $\frac{1}{\sqrt{2}}\left[|g\rangle|\alpha\rangle + |e\rangle|-\alpha\rangle\right]$.

Step 3 Apply a $\pi/2$ $\hat{\sigma}_y$-pulse to the qubit. The state after this step is $\frac{1}{\sqrt{2}}\left[|+\rangle|\alpha\rangle + |-\rangle|-\alpha\rangle\right]$.

In order to implement Step 1 and Step 3 we would need to decouple the qubit and the resonator: this can be achieved either by a tunable coupler or by further detuning the qubit. Also we have considered here the ideal situation when all the operations can be realized with high fidelity, which is a good approximation in the strong regime *(22)*. The main remaining source of errors is due to the spurious thermal contribution present in the cryogenic environment prior to the preparation stage. This will be the object of a later on discussion.

B. Receiver for the entanglement-assisted protocol

For the implementation of the optimal observable $\hat{O}_{opt}$ we will make use of the JC Hamiltonian defined in Eq. (23) in the *strong-resonant* regime, i.e. when $\omega_q = \omega_r$ and $g \gg \Gamma$. The qubit-resonator system evolution under a time $t_g = \tau/g$ corresponds to applying the gate $\hat{U}_\tau = e^{-\tau[\hat{a}_R^\dagger \hat{\sigma}^- - \hat{a}_R \hat{\sigma}^+]}$ up to a known phase shift $e^{-i\hat{H}_0 t_g/\hbar}$, as $[\hat{H}_0^{(\omega_q,\omega_q)}, \hat{H}_{JC}^g] = 0$. The observable $\hat{O}_{opt}$ can be implemented in an approximately in the following way, see Fig. 6.

Step 1 Perform a squeezing operation $\hat{S}(r)$ on the reflected mode $\hat{a}_R$, with squeezing parameter $r = -\operatorname{arcsinh}\lambda_-$ *(44)*. This generates the mode $\hat{a}'_R = \lambda_+ \hat{a}_R + \lambda_- \hat{a}_R^\dagger$.

Step 2 Apply a $\pi/2$ $\hat{\sigma}_x$-pulse to the qubit state. This switches $\hat{\sigma}^-$ with $\hat{\sigma}^+$.

Step 3 Let the qubit-signal system interact with the JC Hamiltonian in the strong-resonant regime for a time $t_g = \tau/g$, with a small enough τ. This generates the transformation

$$\hat{V}^\dagger |e\rangle\langle e| V = |g\rangle\langle g| + \tau \hat{O}_{opt} + o(\tau), \tag{25}$$

where $V = \hat{U}_\tau \hat{S}(r)\hat{\sigma}_x$.

Step 4 Measure the qubit in the basis $\{|g\rangle\langle g|, |e\rangle\langle e|\}$.

If τ is low enough, this protocol approximates the measurement in the low-energy eigenspace of $\hat{O}_{opt} = \hat{\sigma}^-[\lambda_+ \hat{a}_R + \lambda_- \hat{a}_R^\dagger] + c.c.$, which, in $N_S \ll 1$ regime, is the relevant part of the Hilbert space. Let us define $\hat{O}_\tau = V|e\rangle\langle e|V^\dagger$. The threshold discrimination protocol consists in repeating the steps 1-3 M times, collecting the results $\{o_i\}_{i=1}^M$. Here, $o_i = 1$ (or 0) is the measurement outcome corresponding to the projection on the state $|g\rangle$ (or $|e\rangle$). We then calculate the relative frequency $\frac{1}{M}\sum_{i=1}^M o_i$, which corresponds to the expected value of the observable $\hat{O}_\tau$ on the [qubit]-[reflected signal] system state. We use the result to discriminate between the two hypothesis: $\langle \hat{O}_\tau \rangle_{\phi=0} = \lambda_+ + \tau\eta\sqrt{N_S}(1 + e^{-4N_S}) + o(\tau)$ and

$\langle \hat{O}_\tau \rangle_{\phi=\pi} = \lambda_+ - \tau\eta\sqrt{N_S}(1+e^{-4N_S}) + o(\tau)$. We choose the τ value in order to maximize the SNR $Q_{\hat{O}_\tau}$ for the observable $\hat{O}_\tau$, defined as

$$Q_{\hat{O}_\tau} \equiv \frac{(\langle \hat{O}_\tau \rangle_{\rho_{\eta,\pi}} - \langle \hat{O}_\tau \rangle_{\rho_{\eta,0}})^2}{\Delta \hat{O}_\tau^2}, \tag{26}$$

where $\Delta \hat{O}_\tau^2 = \frac{1}{4}\left[\sqrt{\Delta \hat{O}^2_{\tau,\phi=\pi}} + \sqrt{\Delta \hat{O}^2_{\tau,\phi=0}}\right]^2$. is the variance of the observable $\hat{O}_\tau$ averaged over the states $\rho_{\eta,\phi=\pi}$ and $\rho_{\eta,\phi=0}$. The SNR is related to the EP of a threshold discrimination strategy as $p_{\rm err} \sim \exp\left[-\frac{\bar{Q}_{\hat{O}_\tau} M}{8}\right]$ for $M \gg 1$. Any value $N_S/N_B \ll \tau^2 \ll 1/N_B$ is good for approximating the optimal SNR in the $N_B \gg 1$, $N_S \ll 1$ regime (see Supplemental Material). For, instance, if we choose $\tau^2 = N_S/\sqrt{N_B} \equiv \tau^{*2}$, we obtain

$$\frac{Q_{\hat{O}_{\tau^*}}}{Q_{\hat{O}_{opt}}} \simeq 1 - \frac{1}{\sqrt{N_B}} + 4N_S. \tag{27}$$

Lastly, interfacing a signal with $N_B \sim 10^3$ number of photons with a low-temperature environment is challenging. An initial attenuation is needed, making the protocol less efficient in terms of the SNR. An attenuation can be modeled with the beamsplitter input-output relations $\hat{a}_{R,att} = \sqrt{\eta_{att}}\,\hat{a}_R + \sqrt{1-\eta_{att}}\,\hat{v}$, where η_{att} is a power attenuator and v is a bosonic mode assumed to be in a vacuum state. This can be achieved with cryogenic microwave attenuators. The measurement protocol is applied to the mode $\hat{a}_{R,att}$, resulting in a rescaled SNR: $Q^{att}_{O_{\tau^*}}/Q_{O_{\tau^*}} \simeq \frac{\eta_{att}N_B}{1+\eta_{att}N_B}$ in the $N_S \ll 1$ limit, This means that the performance is not affected as long as $\eta_{att}N_B$ is kept large enough.

C. Effects of decoherence on the performance

In the discussed scheme, the main source of inefficiency is given by the spurious thermal contribution present in the cryogenic environment prior to the preparation stage. In addition, while any sort of signal dissipation after the state preparation is already included in the model in an effective way, the idler decoherence must be characterized and bounded in order to understand

the actual performance of the protocol in practical scenarios. Let us first discuss how the protocol is affected by the initial thermal noise. We assume a Markovian environment at temperature T, whose Lindblad master equation is $\partial_t \rho = [\mathcal{L}_D^q + \mathcal{L}_D^r]\rho$. Here,

$$\mathcal{L}_D^q/\hbar = \frac{\gamma}{2}\mathcal{D}[\hat{\sigma}_z] + \Gamma_\uparrow \mathcal{D}[\hat{\sigma}^+] + \Gamma_\downarrow \mathcal{D}[\hat{\sigma}^-], \tag{28}$$

models the qubit decoherence, and

$$\mathcal{L}_D^r/\hbar = \kappa(1+N_T)\mathcal{D}[\hat{a}] + \kappa N_T \mathcal{D}[\hat{a}^\dagger], \tag{29}$$

with $N_T = (e^{\beta\hbar\omega_r} - 1)^{-1}$ and $\beta = (k_B T)^{-1}$, is the resonator dissipation in an environment at temperature T. The Lindblad operators act on a general qubit-resonator state ρ as $\mathcal{D}[\hat{L}]\rho = \hat{L}\rho\hat{L}^\dagger - \frac{1}{2}\{\hat{L}^\dagger\hat{L}, \rho\}$. In addition, the relations $a_g \equiv \frac{\Gamma_\downarrow}{\Gamma_\downarrow+\Gamma_\uparrow} = (1+e^{-\beta\hbar\omega_q})^{-1}$ and $a_e \equiv \frac{\Gamma_\uparrow}{\Gamma_\downarrow+\Gamma_\uparrow} = e^{-\beta\hbar\omega_q}$ hold for a qubit in an environment at temperature T. In a $T \simeq 20$ mK environment we have that $\beta\hbar\omega_{r,q} \gg 1$ for $\omega_{r,q} \sim 1-10$ GHz, therefore decoherence and dissipations in principle should not play a role in the performance evaluation. However, small thermal contributions can be relevant in the low-photons regime, and their effects on the SNR need to be quantified. We assume the initial qubit-resonator state to be the steady state of the Lindblad master equation, i.e. $\rho_q \otimes \rho_r$ with $\rho_q = a_g|g\rangle\langle g| + a_e|e\rangle\langle e|$ and $\rho_r = \frac{1}{1+N_T}\sum_{n=0}^{\infty}\left(\frac{N_T}{1+N_T}\right)^n |n\rangle\langle n|$. By applying the state preparation protocol, we obtain the state $\rho_{\text{noisy}} = \frac{1}{2}\sum_{k,k'\in\{+,-\}}[a_g + kk'a_e]|k\rangle\langle k'| \otimes D(k\alpha)\rho_r D(k'\alpha)$, where $D(\beta)$ is a displacement operator. This implies a rescaling of the optimal SNR for fixed transmitting power, given by $Q^{\text{noisy}}_{\hat{O}_{opt}}/Q_{\hat{O}_{opt}} = \frac{(a_g-a_e)^2}{1+c^{-1}}$, where we have set $|\alpha|^2 = cN_T$. We notice that for $c \leq [2(a_g-a_e)^2-1]^{-1}$ we cannot have any quantum advantage. This sets an upper limit to the amount of thermal noise tolerable before losing all the advantage with respect to a coherent-state transmitter. The initial thermal contribution can be experimentally characterized in several ways. For instance, recently a primary thermometry for propagating microwaves with sensitiv-

ity of 4×10^{-4} photons/$\sqrt{\text{Hz}}$ and a bandwidth of 40 MHz has been developed *(39)*. A similar analysis can be performed for the TMSV state case, obtaining comparable results.

The main source of losses appears in the traveling phase of the protocol. Here, the idler must be preserved coherently in order to profit from the initial quantum correlations. In fact, it is easy to see that under the lossy dynamics described in Eq. (28), we have that

$$\frac{Q^{dec}_{\hat{O}_{opt}}}{Q_{\hat{O}_{opt}}} = e^{-2\frac{t}{T_2}}, \tag{30}$$

where $Q^{dec}_{\hat{O}_{opt}}$ is the SNR for the protocol applied to the state $\rho^{dec} = e^{t\mathcal{L}^q_D/\hbar}[|\psi\rangle_{\text{SC}}\langle\psi|]$, $T_2 = \gamma + \frac{\Gamma_\uparrow+\Gamma_\downarrow}{2}$, t is the traveling time, and we have discarded any initial thermal contributions (see Material and Methods). This means that the protocol must be performed in a time well below the dephasing time of the qubit. Nowadays, qubits with 100 μs lifetime can be realized, corresponding to 30 km freespace propagation of light. An alternative would be the storage in high-Q Nb resonators. Presently, internal quality factors can reach above 1 milion, which at 5 GHz frequencies it corresponds to a decay time of $2/5$ ms. Other options include highly coherent two-level systems formed in the junctions of qubits and high-frequency piezo-mechanical modes.

Digital methods based on error correction have been widely studied in the context of quantum computing. There are principally two approaches to tackle the decoherence problem with a digital approach. We may encode the idler into a logical qubit since the beginning, and perform the protocol in the logical Hilbert space. This is always doable in principle, and one may make a statement that an efficient cQED error-correction code implementation will be soon reached in the context of quantum computing *(40)*. However, this approach is generally costy, as it requires the simultaneous control of several qubits. An alternative consists in exploiting the possibility of transfer the qubit information to the infinite degrees of freedom of a bosonic resonator field via a Jaynes-Cumming interaction *(41)*. This approach requires only one resonator to store the

idler, making the syndrome detection and error correction tasks easier to realize, because dissipation would be the main source of noise at $T \simeq 20$ mK. These so-called cat codes are at the basis of one of the most promising quantum computing architectures, and they have been experimentally demonstrated. Theoretically, one may reach substantial fidelity improvements over the uncorrected protocol for given time, with millisecond lifetime instead of hundred of microseconds of a bare transmon qubit *(41)*. In principle, this approach should be better than using the Fock states of a resonator as a qubit. However, further experimental research is needed in this context, as the lifetime of the cat-qubit implemented in a recent experiment has been only 1.1 larger than an uncorrected qubit encoded in the Fock basis of a resonator *(42)*.

Discussion

We have developed, for the first time, the theory for performing a secure two-way quantum communication protocol in the low-frequency regime, in the scenario where the message sender has a severe bound in the energy. This concept has a natural application in a number of fields, ranging from ultra-low-power RF communications and NFC-based technology to Internet-of-Things. While the results of this article are quite general, we have focused mainly on the $1 - 10$ GHz spectrum, where cQED platforms have been highly developed in the late decades. We have proved the ultimate bounds for the optimal receivers, finding that a quantum correlated detector can be at most a factor of four better in terms of SNR. We have proved the square-root law for covert communication in our two-way setup, showing that $O(\sqrt{n})$ bits can be covertly and reliably transmitted by using the channel n times. Finally, we have provided the ingredients for performing a cQED based experiment, using Schrödinger's cat states as resource. On the conceptual level, the results of this paper provide the foundation of a low-power microwave quantum communication theory. While this is a challenging task, due to the amount of noise that the related systems exhibit at room temperature, a positive output would arguably pave the

way for building quantum communication systems with lower infrastructural costs than those arising in optical-fiber based implementations.

Material and Methods

Notations

We introduce the following notations, useful for the discussion of the technical results.

- *Fock basis*, indicated with latin alphabet kets (or bra): $\{|k\rangle\}_{k=0}^{\infty}$;
- *Coherent states* with amplitude $\alpha \in \mathbb{C}$, indicated with greek alphabet kets (or bra): $|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{k=0}^{\infty} \frac{\alpha^k}{\sqrt{k!}} |k\rangle$;
- *Thermal States* with N_B average photon numbers: $\rho_B = \sum_k \tau_k |k\rangle\langle k|$, where $\tau_k = \frac{1}{1+N_B} \left(\frac{N_B}{1+N_B}\right)^k$;
- *General signal-idler state* of r Schmidt-rank: $|\psi\rangle_{SI} = \sum_{k=0}^{r} \sqrt{p_k} |v_k\rangle_I |w_k\rangle_S$. The signal mode is indicated by $\hat{a}_S$ and we use indistinctively the notation $|v\rangle|w\rangle$ and $|v, w\rangle$. The Schmidt rank r differentiates between the entangled ($r > 1$) and the idler-free ($r = 1$) cases;
- *Constants*: $c_B = \frac{N_B}{1+N_B}$ and $c_S = \frac{N_S}{1+N_S}$.

Receiver Error Probability

Here, we discuss the results based on the calculation of the Chernoff bounds and the quantum Fisher information (QFI) relative to Bob's receiver. In the following, as Bob and Alice are sharing φ_k values, we can set it to zero.

1. Equivalence between OOK and BPSK

In the $\eta \ll 1$ limit, we can map the problem of discriminating between different ϕ to the quantum illumination (QI) setup, where Alice decides to modulate the amplitude between $\eta = 0$ and $\eta = \bar{\eta}$, leaving the phase unchanged ($\phi = 0$). This is usually referred as On-Off-Keying (OOK). We first notice that the received modes $\{\hat{a}_R^{(k)}\}$ can be expressed as

$$\hat{a}_R^{(k)} = \eta\, (e^{-i\phi}\hat{a}_S^{(k)}) + \sqrt{1-\eta^2}\, \hat{h}^{(k)}, \tag{31}$$

where $\hat{h}^{(k)} \equiv \sqrt{\frac{\eta}{1+\eta}}\, e^{-i\phi}\hat{h}_{\leftarrow}^{(k)} + \sqrt{\frac{1}{1+\eta}}\, \hat{h}_{\rightarrow}^{(k)}$ are thermal modes with N_B average number of photons. This means that if $|\psi\rangle_{SI}\langle\psi|$ is the state of the SI system, then the final Bob's state is $\rho_{\eta,\phi} = \mathrm{Tr}_E\left[\hat{B}_\eta \hat{U}_\phi |\psi\rangle_{SI}\langle\psi| \otimes \rho_B \hat{U}_\phi^\dagger \hat{B}_\eta^\dagger\right]$, where $\hat{B}_\eta = \exp\left[\arccos\eta(\hat{a}_S^\dagger \hat{h} - \hat{a}_S \hat{h}^\dagger)\right]$ is a beam-splitter operation and $\hat{U}_\phi = e^{-i\phi\hat{n}_S}$ is a phase-shift operation. We can now prove the equivalence between OOK and BPSK.

Lemma 2. [Equivalence of OOK and BPSK] *In the $\eta \ll 1$ limit, the BPSK and OOK optimal strategies are the same for both the local and the collective cases. The BPSK performs as an OOK with $\bar{\eta} = 2\eta$.*

Proof. We have that $\rho_{\eta,0} = \rho_B - \eta d\rho + o(\eta)$, $\rho_{\eta,\pi} = \rho_B + \eta d\rho + o(\eta)$ for $\eta \ll 1$, where $d\rho = \mathrm{Tr}_S\left[\hat{a}_S^\dagger \hat{h} - \hat{a}_S \hat{h}^\dagger, |\psi\rangle_{SI}\langle\psi| \otimes \rho_B\right]$. Therefore, we have that $\rho_{\eta,0}^{\otimes n} = \rho_B^{\otimes n} - \eta d\sigma + o(\eta)$ and $\rho_{\eta,\pi}^{\otimes n} = \rho_B^{\otimes n} + \eta d\sigma + o(\eta)$, with $d\sigma = \sum_{i=1}^n \rho_B^{\otimes j-1} \otimes d\rho \otimes \rho_B^{\otimes n-j}$. This means that $(\rho_{\eta,\pi}^{\otimes n} - \rho_{\eta,0}^{\otimes n}) = (\rho_{0,0}^{\otimes n} - \rho_{2\eta,0}^{\otimes n}) + o(\eta)$. Therefore, BPSK performs as an OOK with $\bar{\eta} = 2\eta$ in the $\eta \ll 1$ limit, and their optimal measurement setups - being local or collective - are the same. □

2. Quantum Chernoff bound and quantum Fisher information: general formulas

We can now analyze the OOK case to state the general formulas for the quantum Chernoff bound and quantum Fisher information for the BPSK case. In the following, we denote $\rho_\eta \equiv \rho_{\eta,\phi=0}$.

Lemma 3. [Chernoff bound for QI (OOK)] *Given* $\rho_\eta = Tr_E\left(\hat{B}_\eta|\psi\rangle_{SI}\langle\psi|\otimes\rho_B\hat{B}_\eta^\dagger\right)$, *with* $\hat{B}_\eta = \exp\left[\arccos\sqrt{\eta}(\hat{a}_S^\dagger\hat{h} - \hat{a}_S\hat{h}^\dagger)\right]$. *Then, the optimal error probability in the task of distinguishing between* ρ_0 *and* $\rho_{\bar{\eta}}$ *is* $p_{\text{err}} \sim \frac{1}{2}e^{-MC(\rho_0,\rho_{\bar{\eta}})}$ *for* $M \gg 1$, *where*

$$\frac{C(\rho_0,\rho_{\bar{\eta}})}{\bar{\eta}^2} = \frac{1}{1+N_B}\sum_{k,k'}\frac{p_k p_{k'}}{\left[\sqrt{p_{k'}}+\sqrt{p_k}\sqrt{c_B}\right]^2}|\langle w_{k'}|a_S|w_k\rangle|^2 + o(1), \tag{32}$$

for $\bar{\eta} \ll 1$.

Proof. See Supplemental Material. □

Lemma 4. [Quantum Fisher information for QI (OOK)] *Given* ρ_η *as in Lemma 3. Then, the quantum Fisher information for estimating the parameter* η *in the* $\eta \ll 1$ *neighborhood is*

$$F = \frac{4}{1+N_B}\sum_{k,k'}\frac{p_k p_{k'}}{p_{k'}+p_k c_B}|\langle w_{k'}|a_S|w_k\rangle|^2. \tag{33}$$

Proof. See Supplemental Material. □

3. Ultimate error probability bounds

Proof of Theorem 1. We apply Lemma 3 with $\bar{\eta} = 2\eta$ (see Lemma 2) to the simple case of Schmidt-rank one, finding that $\beta_{cl}^{loc} = \frac{4|\langle w|a_S|w\rangle|^2}{1+N_B}\frac{1}{(1+\sqrt{c_B})^2}$. Then, by applying the Hölder's inequality, we find that $|\langle w|a_S|w\rangle|^2 \leq \||a_S|w\rangle\|_2^2 = N_S$, which is saturated by $|w\rangle = |\alpha\rangle$. □

Proof of Theorem 2. By applying the inequality $\frac{p_{k'}}{\left[\sqrt{p_{k'}}+\sqrt{p_k}\sqrt{c_B}\right]^2} \leq 1$ to Eq. (32) with $\bar{\eta} = 2\eta$ (see Lemma 2), we obtain $\beta^{col} \leq \frac{4}{1+N_B}\sum_{k,k'} p_k\langle w_k|a_S^\dagger|w_{k'}\rangle\langle w_{k'}|a_S|w_k\rangle$. By using the completeness relation $\sum_{k'}|w_{k'}\rangle\langle w_{k'}| = \mathbb{I}$ - which can be assumed by adding zero probability terms to the sum - and by noticing that $N_S = \sum_k p_k\langle w_k|a_S^\dagger a_S|w_k\rangle$, we conclude that $\beta^{col} \leq \frac{4N_S}{1+N_S}$. By applying the inequality of arithmetic and geometric means $\frac{p_k p_{k'}}{[\sqrt{p_{k'}}+\sqrt{p_k}c_B]^2} \leq \frac{\sqrt{p_k p_{k'}}}{4\sqrt{c_B}} \leq \frac{p_k+p_{k'}}{8\sqrt{c_B}}$, and by using the completeness relation, we find the second inequality $\beta^{col} \leq \frac{2N_S+1}{1+N_B}\frac{1}{2\sqrt{c_B}}$. Moreover, no mixed state can do better, as in this case the bound can be applied to its purification. □

Proof of Theorem 3. This is done similarly as in the proof of Theorem 2, with the inequalities $\frac{p_{k'}}{p_{k'}+p_\alpha c_B} \leq 1$ and $\frac{p_k p_{k'}}{p_{k'}+p_k c_B} \leq \frac{p_k+p_{k'}}{4\sqrt{c_B}}$ applied to Eq. (33). Also in this case no mixed state can do better, by applying the bound to the purified state. □

Proof of Theorem 4. By applying Lemma 4 with $\bar{\eta} = 2\eta$ (seel Lemma 2) to the Schmidt-rank one case, we find that $\beta_{cl}^{loc} = \frac{2|\langle w|a_S|w\rangle|^2}{1+N_B}\frac{1}{1+c_B}$, which is maximal for $|w\rangle = |\alpha\rangle$ (see the proof of Theorem 1). Homodyne is optimal as one can directly see by checking that the signal-to-noise ratio $\langle\hat{x}\rangle^2_{\rho_{\bar{\eta}}}/\langle\hat{x}^2\rangle_{\rho_0}$ saturates the QFI, and by using Lemma 2. □

4. Examples

QCB and QFI of TMSV states: This is done by setting $p_k = \frac{1}{1+N_S}c_S^k$ and $|w_k\rangle = |k\rangle$ (Fock state with k photons) into the Eq. (32), where we set $\bar{\eta} = 2\eta$, and Eq. (33). It results in a sum of a geometric series and its first derivative, that can be cast as written in the Theorem statement. Similarly, the optimal observable for the threshold discrimination strategy is found by computing $\sum_{kk'nn'} \frac{\langle k',n'|d\rho|k,n\rangle}{p_{k'}\tau_{n'}+p_k\tau_n}|k',n'\rangle\langle k,n|$ *(32).*

QCB and QFI of SC states: This is done by applying Lemma 3 and 4 to the Schmidt decomposition of the SC state given in Eq. (13) of the main text, i.e. $|\psi\rangle_{\rm SC} = \sqrt{\lambda_+}|g\rangle|\alpha_+\rangle + \sqrt{\lambda_-}|e\rangle|\alpha_-\rangle$. We then use Lemma 2 to bring the result to the BPSK. The result is

$$\beta_{\rm SC}^{col} = \frac{4N_S}{1+N_B} f_{\rm SC}^{col}(N_S,N_B) \tag{34}$$

$$\beta_{\rm SC}^{loc} = \frac{2N_S}{1+N_B} f_{\rm SC}^{loc}(N_S,N_B) \tag{35}$$

with

$$f_{\rm SC}^{col}(N_S,N_B) = \frac{\lambda_+^2}{\left(\sqrt{\lambda_+}+\sqrt{\lambda_-}\sqrt{c_B}\right)^2} + \frac{\lambda_-^2}{\left(\sqrt{\lambda_-}+\sqrt{\lambda_+}\sqrt{c_B}\right)^2}, \tag{36}$$

$$f_{\rm SC}^{loc}(N_S,N_B) = \frac{\lambda_+^2}{\lambda_+ + \lambda_- c_B} + \frac{\lambda_-^2}{\lambda_- + \lambda_+ c_B}. \tag{37}$$

In the $N_B \gg 1$ limit, these quantities approximate to

$$f_{\rm SC}^{col} \overset{N_B\gg 1}{=} \frac{1+e^{-4N_S}}{2+2\sqrt{1-e^{-4N_S}}} = 1-2\sqrt{N_S}+O(N_S), \tag{38}$$

$$f_{\rm SC}^{loc} \overset{N_B\gg 1}{=} \frac{1+e^{-4N_S}}{2} = 1-2N_S+O(N_S^2), \tag{39}$$

where we have used that $\lambda_\pm = \frac{1}{2}[1 \pm e^{-2N_S}]$. The optimal local observable can be found by computing

$$\hat{O}_{opt} = \sum_{kk'\in\{g,e\};\, nn'\in[0,\infty]} \frac{\langle k',n'|d\rho|k,n\rangle}{p_{k'}\tau_{n'}+p_k\tau_n}|k',n'\rangle\langle k,n|, \tag{40}$$

where $p_e = \lambda_-$ and $p_g = \lambda_+$. Alternatively, one can directly compute the SNR of $\hat{O}_{opt}$ and see that it saturates the QFI in the $N_B \gg 1$ limit.

Covert Quantum Communication

Here, we provide the technical details present in the discussion about covert communication. We denote Eve's quantum state when Alice applies a phase modulation $\tilde{\varphi}$ as $\rho_{\tilde{\varphi}}^{(N_S)}$. $N_S > 0$ corresponds to the *on*-setting, while $N_S = 0$ is the *off*-setting. We drop any k superscript and subscript, as we are in the i.i.d assumptions. In addition, we introduce the beamsplitter unitary operator $\hat{B}_{12} = \exp\left[\frac{\theta}{2}(\hat{a}_1\hat{a}_2^\dagger - \hat{a}_1^\dagger\hat{a}_2)\right]$, where $\theta = 2\arccos\sqrt{\eta}$. Let us introduce

$$\mathcal{E}_{\tilde{\varphi}}[\sigma] = \mathrm{Tr}_S\left[\hat{B}_{\rightarrow,S}e^{-i\tilde{\varphi}\hat{n}_S}\hat{B}_{\leftarrow,S}(\rho_B\otimes\rho_B\otimes\sigma)\hat{B}_{\leftarrow,S}^\dagger e^{i\tilde{\varphi}\hat{n}_S}B_{\rightarrow,S}^\dagger\right] \tag{41}$$

$$= e^{-i\tilde{\varphi}\hat{n}_\rightarrow}\mathrm{Tr}_S\left[\hat{B}_{\rightarrow,S}\hat{B}_{\leftarrow,S}(\rho_B\otimes\rho_B\otimes\sigma)\hat{B}_{\leftarrow,S}^\dagger B_{\rightarrow,S}^\dagger\right]e^{i\tilde{\varphi}\hat{n}_\rightarrow}, \tag{42}$$

where $\sigma = \sum_{k,k'} c_{kk'}|k\rangle_S\langle k'|$, Tr_S denotes the partial trace on the signal mode, and the equality is due to the phase-invariance of the thermal state. The latter is evident at seeing the input-output relations in Eqs. (18)-(19) of the main text. Let us denote by $\rho^{(N_S)} = \frac{1}{|\mathcal{A}|}\sum_{\tilde{\varphi}\in\mathcal{A}}\rho_{\tilde{\varphi}}^{(N_S)}$, where $\rho_{\tilde{\varphi}}^{(N_S)} = \mathcal{E}_{\tilde{\varphi}}[\rho_S]$. Here, we denote the phase shift at Alice as $\tilde{\varphi}$, which is $\varphi+\phi$ or φ depending if we are in the *on* or *off* setting respectively. In both cases, $\tilde{\varphi}$ is distributed uniformly at random in $\mathcal{A}$.

Proof of Lemma 1. We have that $P^{(\mathrm{Eve})} = \frac{1}{2}\left[1 - \frac{1}{2}\|{\rho^{(N_S)}}^{\otimes n} - {\rho^{(0)}}^{\otimes n}\|_1\right]$ *(30)*. As done in Ref. *(24)*, we can simplify the calculation by using the Pinsker's inequality, i.e. $\|\rho_a - \rho_b\|_1 \leq \sqrt{2D(\rho_a, \rho_b)}$ for any states ρ_a and ρ_b, where $D(\rho_a, \rho_b) = -\mathrm{Tr}\ \rho_a \ln \rho_b + \mathrm{Tr}\, \rho_a \ln \rho_a$ is the quantum relative entropy between ρ_a and ρ_b. This provides the bound

$$P^{(\mathrm{Eve})} \geq \frac{1}{2} - \sqrt{\frac{1}{8} D({\rho^{(0)}}^{\otimes n}, {\rho^{(N_S)}}^{\otimes n})}, \tag{43}$$

meaning that

$$D({\rho^{(0)}}^{\otimes n}, {\rho^{(N_S)}}^{\otimes n}) \leq 8\delta^2 \tag{44}$$

ensures that $P^{(\mathrm{Eve})} \geq \frac{1}{2} - \delta$ over n modes. We use that the quantum relative entropy is additive for tensor product, i.e. $D({\rho^{(0)}}^{\otimes n}, {\rho^{(N_S)}}^{\otimes n}) = nD(\rho^{(0)}, \rho^{(N_S)})$ to reduce the calculation to the single channel-usage case.

- **TMSV case:** We have that

$$\begin{aligned} D_{\mathrm{Gauss}} &= D(\rho^{(0)}, \rho^{(N_S)}) && (45)\\ &\leq \frac{1}{|\mathcal{A}|} \sum_{\tilde{\varphi} \in \mathcal{A}} D(\rho^{(0)}_{\tilde{\varphi}}, \rho^{(N_S)}_{\tilde{\varphi}}) && (46)\\ &= D(\rho^{(0)}_{\tilde{\varphi}=0}, \rho^{(N_S)}_{\tilde{\varphi}=0}), && (47) \end{aligned}$$

  where we have used the joint convexity property of the relative entropy, and that the $D(U\rho U^\dagger, U\sigma U^\dagger) = D(\rho, \sigma)$ for any unitary U and states ρ and σ, together with Eq. (42). The resulting quantity can be readily computed using Gaussian state quantum information tools (see Supplemental Material). The expansion to the third order in N_S gives

$$\begin{aligned} D(\rho^{(N_S)}_{\tilde{\varphi}=0}, \rho^{(0)}_{\tilde{\varphi}=0}) &= \frac{(1-\eta^2)^2}{2N_B\eta^2(1+N_B\eta^2)} N_S^2 + aN_S^3 + o(N_S^3) && (48)\\ &\leq \frac{(1-\eta^2)^2}{2N_B\eta^2(1+N_B\eta^2)} N_S^2 && (49) \end{aligned}$$

  where $a < 0$ has allowed us to use the Taylor's remainder theorem.

- **General case:** We extend the result to signal states of the form $\rho_S = \sum_{j=0}^{\infty} N_S^j \sigma_j$, where

$$\sigma_0 = |0\rangle\langle 0| \tag{50}$$

$$\sigma_1 = |1\rangle\langle 1| - |0\rangle\langle 0| \tag{51}$$

$$\sigma_2 = c(|2\rangle\langle 2| - 2|1\rangle\langle 1| + |0\rangle\langle 0|), \tag{52}$$

with $0 \leq c \leq 1$. This set of states includes the Gaussian state case ($c = 1$). In addition, for $N_S \ll 1$ these states well approximate Gaussian states. Let us consider the Taylor expansion for the logarithm of a matrix

$$\log(A + tB) = \log(A) + t \int_0^{\infty} \frac{1}{A+z} B \frac{1}{A+z} dz - t^2 \int_0^{\infty} \frac{1}{A+z} B \frac{1}{A+z} B \frac{1}{A+z} dz + t^3 \int_0^{\infty} \frac{1}{A+z} B \frac{1}{A+z} B \frac{1}{A+z} B \frac{1}{A+z} dz + +o(t^3). \tag{53}$$

If we set $A = \rho^{(0)}$, $B = \frac{\rho^{(N_S)} - \rho^{(0)}}{N_S}$ and $t = N_S$, we obtain

$$D_c(\rho^{(0)}, \rho^{(N_S)}) = b_0 + b_1 N_S^2 + b_2 N_S^3 + c b_3 N_S^3 + o(N_S^3), \tag{54}$$

where

$$b_0 = -\text{Tr}\left(\rho^{(N_S)} - \rho^{(0)}\right) \int_0^{\infty} \frac{1}{\rho^{(0)}+z} \rho^{(0)} \frac{1}{\rho^{(0)}+z} dz \tag{55}$$

$$b_1 = \text{Tr}\,\rho^{(0)} \int_0^{\infty} \frac{1}{\rho^{(0)}+z} \rho_1 \frac{1}{\rho^{(0)}+z} \rho_1 \frac{1}{\rho^{(0)}+z} dz \tag{56}$$

$$b_2 = -\text{Tr}\,\rho^{(0)} \int_0^{\infty} \frac{1}{\rho^{(0)}+z} \rho_1 \frac{1}{\rho^{(0)}+z} \rho_1 \frac{1}{\rho^{(0)}+z} \rho_1 \frac{1}{\rho^{(0)}+z} dz \tag{57}$$

$$b_3 = \text{Tr}\,\rho^{(0)} \int_0^{\infty} \left[\frac{1}{\rho^{(0)}+z} \rho_1 \frac{1}{\rho^{(0)}+z} \rho_2 \frac{1}{\rho^{(0)}+z} + \frac{1}{\rho^{(0)}+z} \rho_2 \frac{1}{\rho^{(0)}+z} \rho_1 \frac{1}{\rho^{(0)}+z} \right] dz, \tag{58}$$

and we have introduced $\rho_k = \frac{1}{|\mathcal{A}|} \sum_{\tilde{\varphi} \in \mathcal{A}} \mathcal{E}_{\tilde{\varphi}}[\sigma_k]$. First, we notice that $b_0 = 0$, given that $\int_0^{\infty} \frac{s}{(s+z)^2} dz = 1$ and $\rho^{(N_S)} - \rho^{(0)}$ is traceless. Next, we prove that $b_2 \leq 0$. Let use define

$A_z = \frac{\sqrt{\rho^{(0)}}}{\rho^{(0)}+z}\rho_1\frac{\sqrt{\rho^{(0)}}}{\rho^{(0)}+z}$ and $B_z = \frac{\rho^{(0)}+z}{\rho^{(0)}}$. We have that

$$b_2 = -\text{Tr}\int_0^\infty (A_z B_z)^2 A_z dz \tag{59}$$

$$\leq -\text{Tr}\int_0^\infty A_z dz \tag{60}$$

$$= 0, \tag{61}$$

where we have used that $(A_z B_z)^2 \geq 0$ and that ρ_1 is traceless.

We can now bound D_c regardless of the sign of b_3, by using Eq. (49), as $c = 1$ includes the Gaussian case. In fact, assume that $b_3 \geq 0$, then $D_c = D_{\text{Gauss}} + (c-1)b_3 N_S^3 + o(N_S^3)$. We can use Eq. (49) and the Taylor's remainder theorem to conclude that $D_{0\leq c\leq 1} \leq \frac{(1-\eta^2)^2 N_S^2}{2N_B\eta^2(1+N_B\eta^2)}$. Assume that $b_3 < 0$, then we have that $D_c \leq b_1 N_S^2$ by the Taylor's remainder theorem. In addition, we have that the bound $D_{\text{Gauss}} = b_1 N_S^2 + O(N_S^3) \leq \frac{(1-\eta^2)^2 N_S^2}{2N_B\eta^2(1+N_B\eta^2)}$ holds for any $N_S > 0$, which implies that $b_1 \leq \frac{(1-\eta^2)^2}{2N_B\eta^2(1+N_B\eta^2)}$.

Therefore, if we choose $N_S \leq \frac{\sqrt[4]{N_B\eta^2(1+N_B\eta^2)\delta}}{(1-\eta^2)^2\sqrt{n}}$, then we have that $P^{(\text{Eve})} \geq \frac{1}{2} - \delta$ over n channel usages. □

Lemma 1 implies the square-root law, provided that Alice and Bob share a codebook. Notice that the error probability of reading one wrong bit is

$$P_{\text{err}} = 1 - (1 - p_{\text{err}})^m \leq m p_{\text{err}} \tag{62}$$

where p_{err} is the single-bit receiver error probability. This automatically means that a number $m = O(\sqrt{n}/\log n)$ bits are reliably transmissible. In fact, we have that $p_{\text{err}} \leq \frac{1}{2}\exp\left(-M\beta\eta^2\frac{N_S}{1+N_B}\right)$ for M large enough. Here, $\beta = 4$ for the TMSV state and SC state transmitters with the optimal collective receiver, $\beta = 2$ for the TMSV state and SC state transmitter with the optimal local receiver, and $\beta = 1$ for the coherent state transmitter with a homodyne detector receiver. By

setting $N_S = \frac{4\sqrt{N_B\eta^2(1+N_B\eta^2)}\delta}{(1-\eta^2)^2\sqrt{n}}$, with $n = mM$, we get

$$P_{\text{err}} \leq \frac{m}{2} \exp\left(-4c_B\beta\delta\eta^4\frac{\sqrt{n}}{m}\right), \tag{63}$$

where $c_B = \frac{N_B}{1+N_B}$. By setting $m = \frac{A\sqrt{n}}{\log\frac{A}{\epsilon}\log\sqrt{n}}$ with $A = 4\delta\eta^4 c_B\beta$, we have that $P_{\text{err}} \leq \frac{\epsilon}{\log\frac{A}{\epsilon}\log\sqrt{n}} \leq \epsilon$, for small enough ϵ.

We can use the results in Refs. *(24,43)* for AWGN channels in order to get a better scaling for the decoding error probability. This is Theorem 5 of the main text.

Proof of Theorem 5. Let us define $\sigma^2_\beta = \frac{1+N_B}{2\beta\eta^2 M}$. In the optimal local protocol case, the induced AWGN channel for $M \gg 1$ has a variance $\sigma^2_{\beta=2}$. For the coherent state case, the induced AWGN channel for any M has a variance $\sigma^2_{\beta=1}$. In the optimal collective protocol case, we can induce a AWGN channel by dividing M into $K \gg 1$ slots of M/K samples each, and apply the optimal collective protocol on each of the K slots. This provides the same asymptotic performance for the receiver as long as $M/K \gg 1$. The resulting AWGN channel has $\sigma^2_{\beta=4}$ variance. In all cases, we can use Equation (9) of Ref. *(43)* to upper bound the error probability for transmitting $\bar{m}$ bits over m modes in a AWGN channel using a random Gaussian codebook, as

$$P_{\text{err}} \leq 2^{\bar{m}-\frac{m}{2}\log_2\left(1+\frac{N_S}{2\sigma^2_\beta}\right)} \equiv P, \tag{64}$$

where $c_B = \frac{N_B}{1+N_B}$. By setting $N_S = \frac{4\sqrt{N_B\eta^2(1+N_B\eta^2)}\delta}{(1-\eta^2)^2\sqrt{n}}$ and $M = \frac{n}{m}$, we get

$$\log_2 P \simeq \bar{m} - \frac{m}{2\log 2}\frac{N_S}{2\sigma^2_\beta} \tag{65}$$

$$= \bar{m} - \frac{m}{2\log 2}\frac{4\sqrt{N_B\eta^2(1+N_B\eta^2)}\delta}{(1-\eta^2)^2\sqrt{n}}\frac{\beta\eta^2 n/m}{1+N_B} \tag{66}$$

$$\leq \bar{m} - \frac{2}{\log 2}c_B\beta\delta\eta^4\sqrt{n}. \tag{67}$$

By setting $\bar{m} = \frac{2}{\log 2} c_B \beta \delta \eta^4 \sqrt{n} + \log_2 \epsilon$, we get that $P \leq \epsilon$. As this calculation holds for a random codebook, it implies that there exists a specific codebook achieving this performance. This concludes the proof. □

Effects of the qubit decoherence on the SNR

Here, we show how the decoherence affects the qubit measurements. We are assuming a Markovian noise described by the Lindblad operator $\mathcal{L}_D/\hbar = \frac{\gamma}{2}\mathcal{D}[\hat{\sigma}_z] + \Gamma_\uparrow \mathcal{D}[\hat{\sigma}^+] + \Gamma_\downarrow \mathcal{D}[\hat{\sigma}^-]$, where $\mathcal{D}[\hat{L}]\rho = (\hat{L}\rho\hat{L}^\dagger - \frac{1}{2}\{\hat{L}^\dagger\hat{L}, \rho\})$. We have that

$$e^{t\mathcal{L}_D^\dagger}\hat{\sigma}^- = e^{-t/T_2}\hat{\sigma}^- \tag{68}$$

where $\mathcal{L}_D^\dagger$ is the dual of $\mathcal{L}_D$, and $T_2 = \left(\gamma + \frac{\Gamma_\uparrow + \Gamma_\downarrow}{2}\right)^{-1}$ (see Supplemental Material). As $\hat{O}_{opt} = \sigma^-(\lambda_+\hat{a} + \lambda_-\hat{a}^\dagger) + c.c.$ is linear in $\hat{\sigma}^-$ and σ^+, we have that $Q^{dec}_{\hat{O}_{opt}}/Q_{\hat{O}_{opt}} = e^{-2t/T_2}$, which is Eq. (30) of the main text.

References and Notes

1. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck et al., "Advances in Quantum Criptography", (2019), arXiv:1906.01645 [quant-ph].

2. D. J. Bernstein and T. Lange, "Post-quantum cryptography", Nature vol. **549**, pp. 188?194 (2017).

3. M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?", IEEE Security & Privacy, vol. **16**, no. 5, pp. 38-41, September/October (2018).

4. C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-variable quantum key distribution using thermal states", Phys. Rev. A **86**, 022318 (2012).

5. J. Wang, F. Sciarrino, A. Laing, and M. J. Thompson, "Integrated photonic quantum technologies", Nat. Photonics 1-12 (2019).

6. E. P. Menzel, R. Di Candia, F. Deppe, P. Eder, L. Zhong, M. Ihmig et al., "Path-entanglement of Continuous-Variable Quantum Microwaves", Phys. Rev. Lett. **109**, 250502 (2012).

7. L. Zhong, E. P. Menzel, R. Di Candia, P. Eder, M. Ihmig, A. Baust et al., "Squeezing with a flux-driven Josephson parametric amplifier", New J. of Phys. **15**, 125013 (2013).

8. J.-C. Besse, S. Gasparinetti, M. C. Collodo, T. Walter, P. Kurpiers, M. Pechal, C. Eichler, and A. Wallraff, "Single-Shot Quantum Nondemolition Detection of Individual Itinerant Microwave Photons", Phys. Rev. X **8**, 021003 (2018).

9. R. Kokkoniemi, J. Govenius, V. Vesterinen, R. E. Lake, A. M. Gunyho, K. Y. Tan et al., "Nanobolometer with Ultralow Noise Equivalent Power", Comm. Phys. Vol. 2, no. 124 (2019).

10. K. G. Fedorov, S. Pogorzalek, U. Las Heras, M. Sanz, P. Yard, P. Eder et al.,"Finite-time quantum entanglement in propagating squeezed microwaves", Sci. Rep. **8**, 6416 (2018).

11. P. Lähteenmäki, G. S. Paraoanu, J. Hassel, and P. J. Hakonen, "Coherence and multimode correlations from vacuum fluctuations in a microwave superconducting cavity", Nat. Comm. **7**, 12548 (2016).

12. C. W. Sandbo Chang, M. Simoen, J. Aumentado, C. Sabin, P. Forn-Diaz, A. M. Vadiraj, F. Quijandria, G. Johansson, I. Fuentes, and C. M. Wilson, "Generating Multimode Entangled Microwaves with a Superconducting Parametric Cavity", Phys. Rev. Applied **10**, 044019 (2018).

13. S. Pogorzalek, K. G. Fedorov, M. Xu, A. Parra-Rodriguez, M. Sanz, M. Fischer, E. Xie, K. Inomata, Y. Nakamura, E. Solano, A. Marx, F. Deppe, and R. Gross, "Secure quantum remote state preparation of squeezed microwave states", Nature Comm. **10**, 2604 (2019).

14. R. Di Candia, K. G. Fedorov, L. Zhong, S. Felicetti, E. P. Menzel, M. Sanz, F. Deppe, A .Marx, R. Gross, and E. Solano , "Quantum teleportation of propagating quantum microwaves", EPJ Quantum Technology **2**, 25 (2015).

15. S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola, "Microwave Quantum Illumination", Phys. Rev. Lett. **114**, 080503 (2015).

16. U. Las Heras, R. Di Candia, K. G. Fedorov, F. Deppe, M. Sanz, and E. Solano, "Quantum Illumination Unveils Cloaking", Sci. Rep. **7**, 9333 (2017).

17. S. Barzanjeh, S. Pirandola, D. Vitali, and J. M. Fink, "Microwave quantum illumination using a digital receiver", Science Advances Vol. 6, no. 19, eabb0451 (2020).

18. C. W. Sandbo Chang, A. M. Vadiraj, J. Bourassa, B. Balaji, and C. M. Wilson, "Quantum-enhanced noise radar", Appl. Phys. Lett. **114**, 112601 (2019).

19. 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", Phys. Rev. Lett. **101**, 253601 (2008).

20. S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, "Continuous-variable quantum cryptography using two-way quantum communication", Nat. Phys. **4**, 726?730 (2008).

21. J. H. Shapiro, "Defeating passive eavesdropping with quantum illumination", Phys. Rev. A **80**, 022320 (2009).

22. C. Wang, Y. Y. Gao, P. Reinhold, R. W. Heeres, N. Ofek, K. Chou et al., "A Schrödinger cat living in two boxes", Science **352**, 1087 (2016).

23. J. H. Shapiro, "The Quantum Illumination Story", (2019), arXiv:1910.12277 [quant-ph].

24. 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. Comm. **6**, 8626 (2015).

25. H. Shi, Z. Zhang, and Q. Zhuang, "Practical Route to Entanglement-Assisted Communication Over Noisy Bosonic Channels", Phys. Rev. Appl. **13**, 034029 (2020).

26. J. Calsamiglia, R. Muñoz-Tapia, Ll. Masanes, A. Acin, and E. Bagan, "Quantum Chernoff bound as a measure of distinguishability between density matrices: Application to qubit and Gaussian states", Phys. Rev. A **77**, 032311 (2008).

27. M. Sanz, U. Las Heras, J. J. Garcia-Ripoll, E. Solano, and R. Di Candia, "Quantum Estimation Methods for Quantum Illumination", Phys. Rev. Lett. **118**, 070803 (2017).

28. M. Paris, "Quantum Estimation for Quantum Technology", Int. J. Quant. Inf. **7**, 125 (2009).

29. H. Shi, Z. Zhang, and Q. Zhuang, "Practical Route to Entanglement-Assisted Communication Over Noisy Bosonic Channels", Phys. Rev. Appl. **13**, 034029 (2020).

30. Q. Zhuang, Z. Zhang, and J. H. Shapiro, "Optimum Mixed-State Discrimination for Noisy Entanglement-Enhanced Sensing", Phys. Rev. Lett. **118**, 040801 (2017).

31. S. Guha and B. I. Erkmen, "Gaussian-state quantum-illumination receivers for target detection", Phys. Rev. A **80**, 052310 (2009).

32. R. Dassonneville, T. Ramos, V. Milchakov, L. Planat, É. Dumur, F. Foroughi, J. Puertas, S. Leger, K. Bharadwaj, J. Delaforce, C. Naud, W. Hasch-Guichard, J. J. García-Ripoll, N. Roch, and O. Buisson, "Fast High-Fidelity Quantum Nondemolition Qubit Readout via a Nonperturbative Cross-Kerr Coupling", Phys. Rev. X **10**, 011045 (2020).

33. M. Reagor, W. Pfaff, C. Axline, R. W. Heeres, N. Ofek, K. Sliwa et al., "Quantum memory with millisecond coherence in circuit QED", Phys. Rev. B **94**, 014506 (2016).

34. M. K. Ekström, T. Aref, A. Ask, G. Andersson, B. Suri, H. Sanada, G. Johansson, and P. Delsing, "Towards phonon routing: Controlling propagating acoustic waves in the quantum regime", New J. Phys. **21**, 123013 (2019).

35. M. S. Bullock, C. N. Gagatsos, S. Guha, and Boulat A. Bash, "Fundamental limits of quantum-secure covert communication over bosonic channels", IEEE Journal on Selected Areas in Communications, vol. 38, no. 3, pp. 471-482 (2020).

36. Q. Zhuang, Z. Zhang, and J. H. Shapiro, "Quantum illumination for enhanced detection of Rayleigh-fading targets", Phys. Rev. A **96**, 020302(R)(2017).

37. J. M. Arrazola and R. Amiri, "Secret-key expansion from covert communication", Phys. Rev. A **97**, 022325 (2018).

38. M. Boissonneault, J. M. Gambetta, and A. Blais, "Dispersive regime of circuit QED: Photon-dependent qubit dephasing and relaxation rates", Phys. Rev. A **79**, 013819 (2009).

39. M. Scigliuzzo, A. Bengtsson, J.-C. Besse, A. Wallraff, P. Delsing, and S. Gasparinetti., "Primary thermometry of propagating microwaves in the quantum regime", (2020), arXiv:2003.13522 [quant-ph].

40. F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandra, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Yuezhen Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, "Quantum supremacy using a programmable superconducting processor", Nature vol. **574**, pp. 505?510 (2019).

41. Z. Leghtas, G. Kirchmair, B. Vlastakis, R. J. Schoelkopf, M. H. Devoret, and M. Mirrahimi, "Hardware-Efficient Autonomous Quantum Memory Protection" , Phys. Rev. Lett. **111**, 120501 (2013).

42. N. Ofek, A. Petrenko, R. Heeres, P. Reinhold, Z. Leghtas, B. Vlastakis, Y. Liu, L. Frunzio, S. M. Girvin, L. Jiang, M. Mirrahimi, M. H. Devoret, and R. J. Schoelkopf, "Extending the lifetime of a quantum bit with error correction in superconducting circuits", Nature **536**, 441 (2016).

43. B. A. 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 (2013).

44. The squeezing operation on the mode $\hat{a}_R$ is defined as $\hat{S}(\xi) = \exp\left(-\frac{\xi^2}{2}\hat{a}_R^{\dagger 2} + \frac{\xi^{*2}}{2}\hat{a}_R^2\right)$, where $\xi = re^{-i\phi}$ is the squeezing parameter.

Acknowledgements

The authors thank Sergey N. Filippov, Giuseppe Vitagliano, Göran Johansson, and Stefano Pirandola for useful discussions.

Funding: The authors acknowledge support from Academy of Finland (grants nos. 319578, 312296, and 328193). RDC acknowledges support from the Marie Skłodowska Curie fellowship number 891517 (MSC-IF Green-MIQUEC). GSP acknowledges the EU's Horizon 2020 research and innovation programme (grant agreement no. 862644, FET Open QUARTET), as well as the support of the Scientific Advisory Board for Defence (Finland) and Saab.

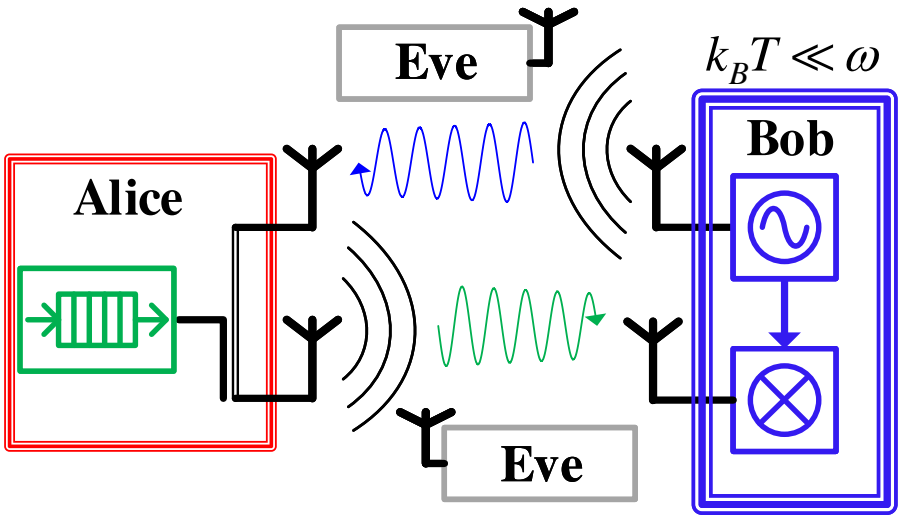

Figure 1: **Sketch of the two-way quantum communication protocol.** Bob sends a signal to Alice, who embeds the message by phase modulation. The signal is then sent back to Bob, who retrieve the information via a suitable measurement. Bob may use quantum correlations in order to increase the signal-to-noise ratio. A passive Eve is able to collect the photons lost in both paths, but she does not have access to Bob and Alice labs.

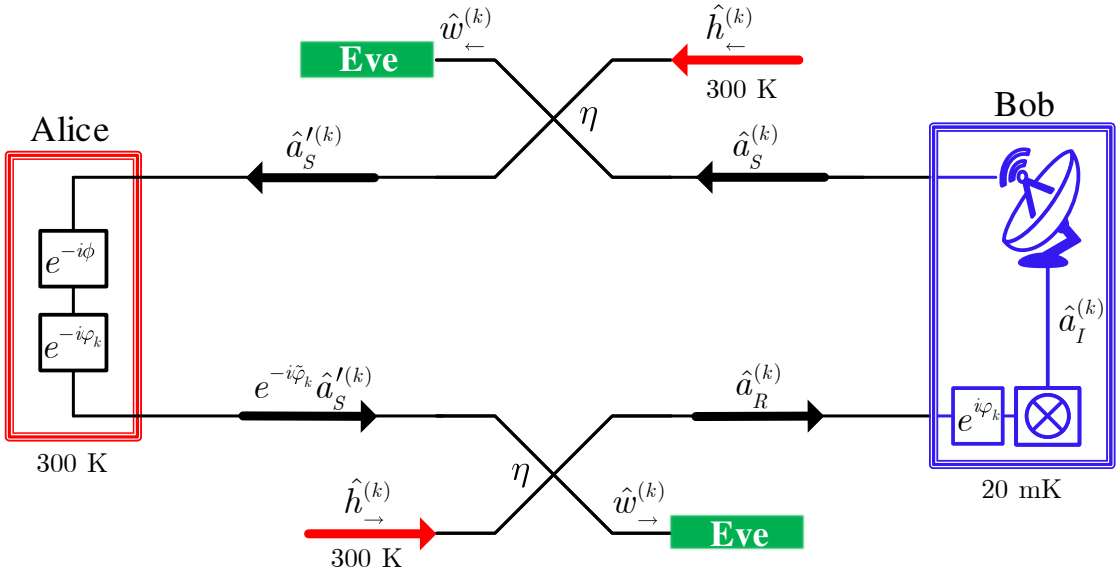

Figure 2: **Setup for the two-way covert quantum communication through a bright bosonic channel.** A signal microwave mode $\hat{a}^{(k)}_S$, possibly entangled with an idler mode $\hat{a}^{(k)}_I$, is generated by Bob. The idler mode is stored in the lab, while the signal is sent through a noisy channel to Alice, who receive the noisy modes $a'^{(k)}_S$. Alice modulates the phase of the signal by $\tilde{\varphi}_k = \phi + \varphi_k$, where ϕ and φ_k belong to a pre-agreed discrete alphabet $\mathcal{A}$. Here, ϕ embeds the information to be sent, while $e^{-i\varphi_k}$ is an encoding operator. The value of φ_k is taken uniformly at random in $\mathcal{A}$, and it is known only to Alice and Bob. The signal is then scattered back to Bob, who decodes it by applying a phase modulation $e^{i\varphi_k}$. This process is repeated M times ($k = 1, \ldots, M$), for each symbol transmission. Bob performs a measurement on the modes $\{e^{i\varphi_k}\hat{a}^{(k)}_R, \hat{a}^{(k)}_I\}$ in order to discriminate between the possible values ϕ. Eve performs a collective measurement on the modes $\{\hat{w}^{(k)}_{\leftarrow}, w^{(k)}_{\rightarrow}\}$ in order to understand whether Alice and Bob are communicating. If the average power of the signal modes is $O(\eta^2 N_B/\sqrt{n})$, then Alice and Bob are able to use covertly n channel modes. This allows to transmit $O(\sqrt{n})$ number of bits in a secure way. In the $1 - 10$ GHz band, Bob's signals are generated at 20 mK in order to suppress the thermal contribution and comply with the covertness conditions.

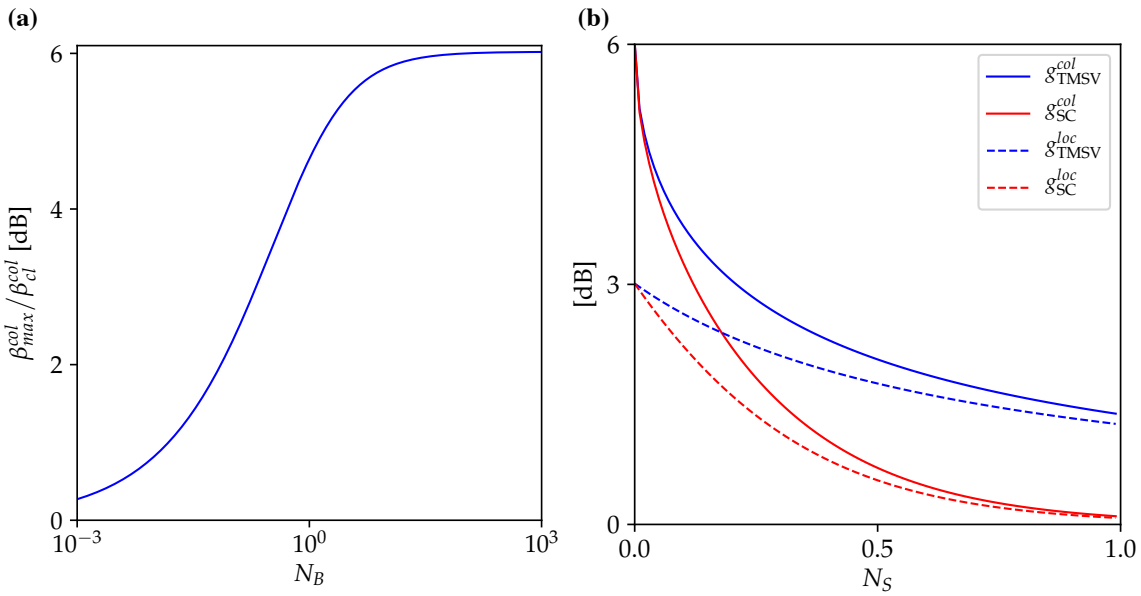

Figure 3: **Performance of the quantum correlated protocol with respect to the idler-free case. (a)** Maximal achievable gain of the Chernoff bound of the quantum correlated case (denoted as β^{col}_{max}) with respect to the idler-free case (β^{col}_{cl}), depending on the average number of thermal photons in the environment N_B. For instance, for $N_B = 1$, the maximal gain is about 4.6 dB and it is reached in the $N_S \ll 1$ limit. **(b)** Comparison of the optimal receiver performance for Gaussian states and Schrödinger's cat states with respect to the idler-free case, in the $N_B \gg 1$ limit. The performance is quantified in terms of the error probability decaying exponent. Indeed, the quantities $g^{col}_{\mathrm{TMSV,SC}} = \beta^{col}_{\mathrm{TMSV,SC}}/\beta^{col}_{cl}$ and $g^{loc}_{\mathrm{TMSV,SC}} = \beta^{loc}_{\mathrm{TMSV,SC}}/\beta^{loc}_{cl}$ are plotted for $N_B \gg 1$. The graphics shows how the advantage in using quantum correlations decays with the transmitting power N_S. Gaussian states perform better than Schrödinger's cat states for finite N_S.

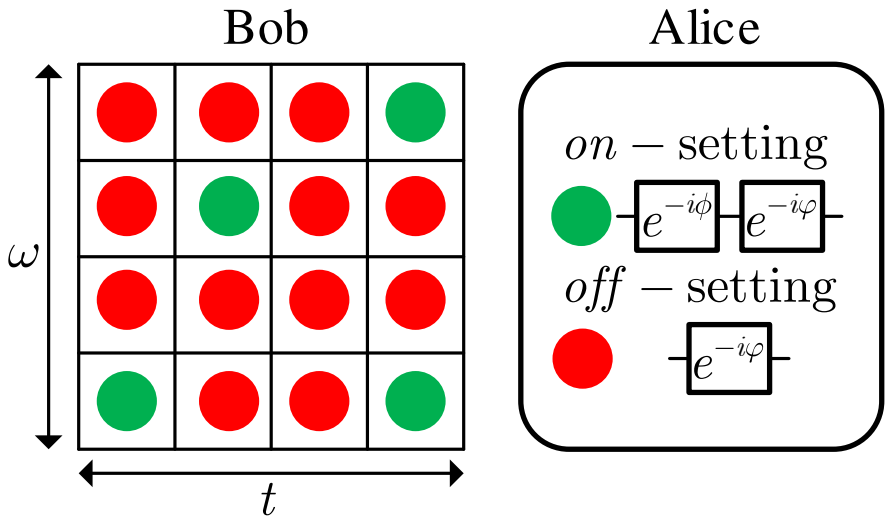

Figure 4: **Probabilistic version of the two-way covert quantum communication protocol.** Alice and Bob secretly choose to communicate only in the fraction of the temporal and frequency modes at their disposal. In the on-setting (green dots), Alice performs a phase modulation $e^{-i(\phi+\varphi)}$, where $\phi \in \mathcal{A}$ is the symbol that Alice wants to transmit and φ is taken uniformly at random in $\mathcal{A}$. The phase φ is secretly known to both Alice and Bob. In the off-setting (red dots), Alice performs a phase modulation $e^{-i\varphi}$, where φ is taken uniformly at random in $\mathcal{A}$.

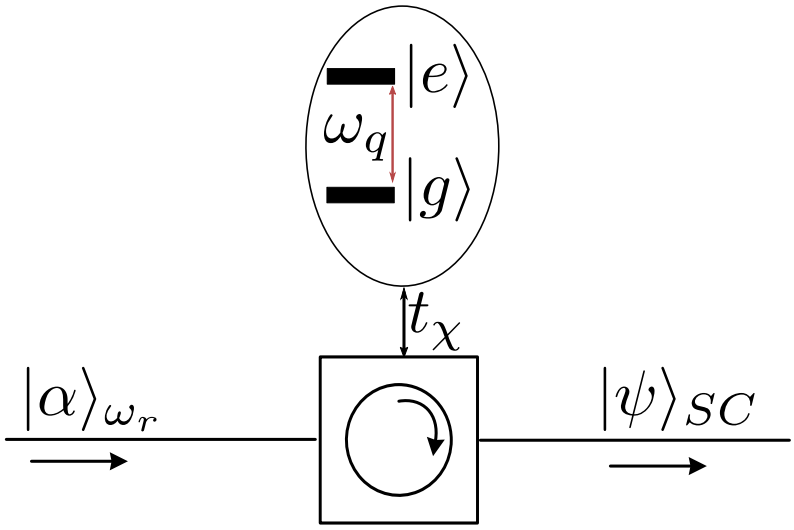

Figure 5: **Scheme for the preparation of the Schrödinger's cat state.** A resonator with central frequency ω_r is driven with a coherent signal, displacing the state of the cavity to $|-i\alpha\rangle$. A transmon qubit with frequency ω_q is initialized in a state $|+\rangle = \frac{|e\rangle+|g\rangle}{\sqrt{2}}$. A conditional phase shift is then applied. This is implemented by letting the resonator and qubit interact in the strong dispersive regime for a time $t_\chi = \pi/2\chi$, where $\chi = g^2/\Delta$ is the effective coupling. Here, g is the coupling strength of the qubit-resonator system, $\Delta = \omega_r - \omega_q$ and $g/\Delta \ll 1$. Finally, a $\pi/2$ $\hat{\sigma}_y$-pulse is applied to the qubit. Feasible parameters are $\omega_r = 5$ GHz, $\omega_q = \omega_r + \Delta$ with $\Delta = 20$ Mhz, and $g = 100$ Khz.

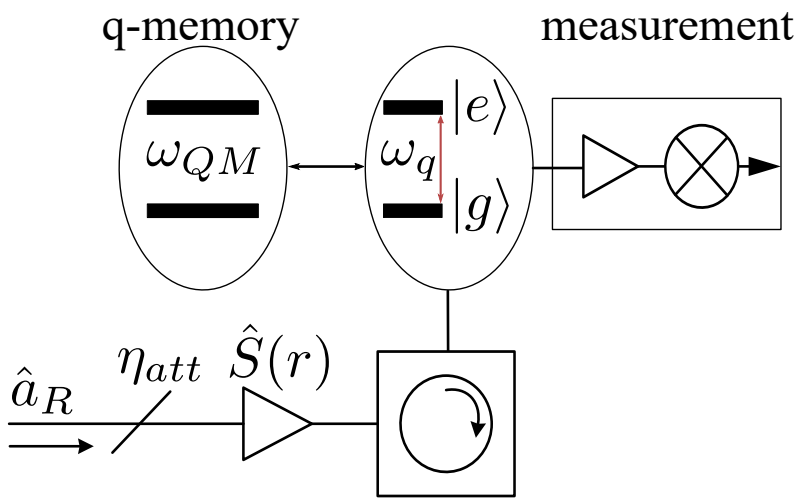

Figure 6: **Scheme for the implementation of the observable optimizing the quantum Fisher information.** During the signal transmission, which happens at frequency ω_r, the qubit state is transferred to a quantum memory. The qubit frequency is then tuned to $\omega_q = \omega_r$. Here the quantum memory is a resonator at frequency ω_{QM}, interacting dispersively with the qubit. This allows the implementation of the cat code. The state is transferred back to the qubit for the measurement stage. The received signal $\hat{a}_R$ is attenuated. A squeezing operation is then applied using a JPA in the degenerate mode. The output interacts with the qubit in the resonant regime. Finally, the qubit is measured in the $\{|g\rangle\langle g|, |e\rangle\langle e|\}$ basis.

Supplemental Material

S1: General formulas for the quantum Chernoff bound and the quantum Fisher information

Here, we prove Lemma 3 and Lemma 4 stated in Material and Methods.

Proof of Lemma 3. This can be done by performing a Taylor expansion of the quantum Chernoff bound, as in Calsamiglia et al. *(1)*. We have that $C(\rho_0,\rho_{\bar\eta}) = -\min_{s\in[0,1]}\log \mathrm{Tr}(\rho_0^s\rho_{\bar\eta}^{1-s})$. Considering the Taylor expansion around $\bar\eta=0$, $\rho_{\bar\eta}=\rho_0+\bar\eta d\rho+o(\bar\eta)$, then

$$C(\rho_0,\rho_{\bar\eta}) = \frac{\bar\eta^2}{2}\sum_{kk'nn'}\frac{|\langle v_k,n|d\rho|v_{k'}n'\rangle|^2}{[\sqrt{p_k\tau_n}+\sqrt{p_{k'}\tau_{n'}}]^2}+o(\bar\eta^2) \tag{69}$$

$$= \bar\eta^2\beta^{col}+o(\bar\eta^2), \tag{70}$$

see Equation (47) of Ref. *(1)*. The task reduces in computing Eq. (70) with $d\rho = \mathrm{Tr}_S[\hat a_S^\dagger\hat h - \hat a_S\hat h^\dagger, |\psi\rangle_{SI}\langle\psi|\otimes\rho_B]$. First, we notice that

$$\langle v_k,n|d\rho|v_{k'}n'\rangle = (\tau_{n'}-\tau_n)[\langle w_{k'}|\hat a_S^\dagger|w_k\rangle\sqrt{n+1}\delta_{n',n+1} - \langle w_{k'}|\hat a_S|w_k\rangle\sqrt{n'+1}\delta_{n,n'+1}]. \tag{71}$$

We have that

$$\beta^{col} = \frac{1}{2}\sum_{kk'nn'}\frac{|\langle v_k,n|\sum_{jj'}\sqrt{p_jp_{j'}}|v_j\rangle\langle v_{j'}|\otimes[\langle w_{j'}|\hat a_S^\dagger|w_j\rangle\hat h - \langle w_{j'}|s|w_j\rangle\hat h^\dagger,\rho_B]|v_{k'},n'\rangle|^2}{[\sqrt{p_k\tau_n}+\sqrt{p_{k'}\tau_{n'}}]^2} \tag{72}$$

$$= \frac{1}{2}\sum_{kk'nn'}\frac{p_kp_{k'}|\langle w_{k'}|\hat a_S^\dagger|w_k\rangle(\tau_{n'}-\tau_n)\sqrt{n+1}\delta_{n',n+1} - \langle w_{k'}|\hat a_S|w_k\rangle(\tau_{n'}-\tau_n)\sqrt{n'+1}\delta_{n,n'+1}|^2}{[\sqrt{p_k\tau_n}+\sqrt{p_{k'}\tau_{n'}}]^2} \tag{73}$$

$$= \frac{1}{2}\sum_{kk'nn'}\frac{p_kp_{k'}(\tau_{n'}-\tau_n)^2}{[\sqrt{p_k\tau_n}+\sqrt{p_{k'}\tau_{n'}}]^2}\left[|\langle w_{k'}|\hat a_S^\dagger|w_k\rangle|^2(n+1)\delta_{n',n+1}+|\langle w_{k'}|s|w_k\rangle|^2(n'+1)\delta_{n,n'+1}\right] \tag{74}$$

$$= \frac{1}{2}\sum_{kk'n}(n+1)p_kp_{k'}[\tau_{n+1}-\tau_n]^2\left[\frac{|\langle w_{k'}|\hat a_S^\dagger|w_k\rangle|^2}{[\sqrt{p_k\tau_n}+\sqrt{p_{k'}\tau_{n'}}]^2}+\frac{|\langle w_{k'}|\hat a_S|w_k\rangle|^2}{[\sqrt{p_k\tau_n}+\sqrt{p_{k'}\tau_{n'}}]^2}\right], \tag{75}$$

where in the last line we have summed on the n' index. We now use that the last sum is symmetric under the exchange of k and k' and that $\tau_n/\tau_{n-1} = \frac{N_B}{1+N_B}$:

$$\beta^{col} = \sum_{kk'n}(n+1)p_k p_{k'}[\tau_{n+1}-\tau_n]^2 \frac{|\langle w_{k'}|\hat{a}_S|w_k\rangle|^2}{[\sqrt{p_k\tau_n}+\sqrt{p_{k'}\tau_{n'}}]^2}) \tag{76}$$

$$= \sum_{kk'n}(n+1)\tau_n p_k p_{k'}\left[1-\frac{\tau_{n+1}}{\tau_n}\right]^2 \frac{|\langle w_{k'}|\hat{a}_S|w_k\rangle|^2}{\left[\sqrt{p_{k'}}+\sqrt{p_k}\sqrt{\frac{\tau_{n+1}}{\tau_n}}\right]^2} \tag{77}$$

$$= \frac{1}{1+N_B}\sum_{kk'} \frac{p_k p_{k'}|\langle w_{k'}|\hat{a}_S|w_k\rangle|^2}{\left[\sqrt{p_{k'}}+\sqrt{p_k}\sqrt{\frac{N_B}{1+N_B}}\right]^2}. \tag{78}$$

□

Proof of Lemma 4. The QFI is given by *(2)*

$$F = 2\sum_{kk'nn'} \frac{|\langle v_k, n|d\rho|v_{k'}n'\rangle|^2}{p_k\tau_n + p_{k'}\tau_{n'}}, \tag{79}$$

where $d\rho = \mathrm{Tr}_S[\hat{a}_S^\dagger \hat{h} - \hat{a}_S\hat{h}^\dagger, |\psi\rangle_{SI}\langle\psi| \otimes \rho_B]$. The calculation is similar as in Lemma 3. □

S2: Relative entropy of Gaussian states

Here, we provide the relative entropy calculation for TMSV which has been used in the proof of Lemma 1 of the main text. Let us define the vector $\vec{r} = (\hat{x}_\leftarrow, \hat{p}_\leftarrow, \hat{x}_\rightarrow, \hat{p}_\rightarrow)^T$, where $\hat{x}_l = \frac{\hat{a}_l + \hat{a}_l^\dagger}{\sqrt{2}}$ and $\hat{p}_l = \frac{\hat{a}_l - \hat{a}_l^\dagger}{\sqrt{2}i}$ ($l \in \{\leftarrow, \rightarrow\}$). For a zero-mean Gaussian state ρ, the covariance matrix is defined as $\Sigma_{ij} = \mathrm{Tr}\left(\{\hat{r}_j, \hat{r}_k\}\rho\right)$. The covariance matrix of the Gaussian state $\rho_{\tilde{\varphi}}^{(N_S)}$ is

$$\Sigma_{\tilde{\varphi}}^{(N_S)} = 2 \times \begin{bmatrix} A & 0 & -B\cos\tilde{\varphi} & B\sin\tilde{\varphi} \\ 0 & A & -B\sin\tilde{\varphi} & -B\cos\tilde{\varphi} \\ -B\cos\tilde{\varphi} & -B\sin\tilde{\varphi} & C & 0 \\ B\sin\tilde{\varphi} & -B\cos\tilde{\varphi} & 0 & C \end{bmatrix} \tag{80}$$

where $A = \frac{1}{2} + \eta N_B + (1-\eta)N_S$, $B = (1-\eta)\sqrt{\eta}(N_B - N_S)$, and $C = \frac{1}{2} + [(1-\eta)^2 + \eta]N_B + (1-\eta)\eta N_S$. For zero-mean Gaussian states, we have that

$$D(\rho_{\tilde{\varphi}}^{(0)}, \rho_{\tilde{\varphi}}^{(N_S)}) = \frac{1}{2}\left[\log\frac{\det[\Sigma_{\tilde{\varphi}}^{(N_S)} + i\Omega]}{\det[\Sigma_{\tilde{\varphi}}^{(0)} + i\Omega]} + \frac{1}{2}\mathrm{Tr}\left[\Sigma_{\tilde{\varphi}}^{(0)}(H_{\tilde{\varphi}}^{(N_S)} - H_{\tilde{\varphi}}^{(0)})\right]\right], \tag{81}$$

where $\Omega = -i\mathbb{I}_2 \otimes \sigma_y$ is the symplectic form and $H_{\tilde{\varphi}}^{(N_S)} = 2\,\text{arccoth}(i\Omega\Sigma_{\tilde{\varphi}}^{(N_S)})i\Omega$ is the Hamiltonian matrix, given that $\rho_{\tilde{\varphi}}^{(N_S)}$ is a faithful Gaussian state *(3,4)*. Eq. (81) has been computed using Mathematica, finding

$$\begin{aligned} D(\rho_{\tilde{\varphi}}^{(0)}, \rho_{\tilde{\varphi}}^{(N_S)}) = &- (1 + 2N_B\eta^2 + 2N_S(1-\eta^2)) \left[\text{arccoth}(1 + 2N_B\eta^2)\right. \\ &\left. -\text{arccoth}(1 + 2N_S + 2(N_B - N_S)\eta^2)\right] \\ &+ \frac{1}{2}\log \frac{N_B\eta^2(1+N_B\eta^2)}{N_S(1+N_S) + (N_B - N_S)(1+2N_S)\eta^2 + (N_B - N_S)^2\eta^4}, \end{aligned} \tag{82}$$

which does not depend on $\tilde{\varphi}$.

S3: Converse lemma

Here, we prove that the bound found in Lemma 1 of the main text is tight. This is usually referred as *converse*.

Lemma 5. [Converse] $D(\rho^{(N_S)^{\otimes n}}, \rho^{(0)^{\otimes n}}) \leq 8\delta^2$ *implies that* $N_S \leq \frac{4\sqrt{\eta^2 N_B(1+\eta^2 N_B)}}{(1-\eta^2)^2}\frac{\delta}{\sqrt{n}}$.

Proof. Let us consider Eve's modes $\hat{w}_{\leftarrow}^{(k)}$ and $\hat{w}_{\rightarrow}^{(k)}$, $k = 1, \ldots, n$. Let us these modes be the output of a black-box which has the knowledge of the individual realizations of $\tilde{\varphi}_k$. The black-box acts as a beamsplitter, generating the modes

$$\hat{w}_1^{(k)} = \sqrt{\frac{\eta}{1+\eta}}\,\hat{w}_{\rightarrow}^{(k)} + \sqrt{\frac{1}{1+\eta}}\,e^{-i\tilde{\varphi}_k}\,\hat{w}_{\leftarrow}^{(k)} \tag{83}$$

$$\hat{w}_2^{(k)} = -\sqrt{\frac{1}{1+\eta}}\,e^{i\tilde{\varphi}_k}\,\hat{w}_{\rightarrow}^{(k)} + \sqrt{\frac{\eta}{1+\eta}}\,\hat{w}_{\leftarrow}^{(k)}. \tag{84}$$

We then trace-out the modes $\hat{w}_2^{(k)}$. Notice that

$$\hat{w}_1^{(k)} = -\sqrt{1-\eta^2}\,e^{-i\tilde{\varphi}_k}\,\hat{a}_S^{(k)} + \eta\,\hat{h}^{(k)}, \tag{85}$$

where $\hat{h}^{(k)} = \sqrt{\frac{\eta}{1+\eta}}\,\hat{h}_{\rightarrow}^{(k)} + \sqrt{\frac{1}{1+\eta}}\,e^{-i\tilde{\varphi}_k}\,\hat{h}_{\leftarrow}^{(k)}$ is in a thermal state with N_B average number of photons, regardless of the value of $\tilde{\varphi}_k$. As Eve does not have the knowledge of the phase $\tilde{\varphi}_k$ and

$\hat{a}_S^{(k)}$ are i.i.d., the state of the modes $\hat{w}_1^{(k)}$ does not depend on k. Let us denote its density matrix as $\sigma^{(N_S)}$. Here, $N_S = 0$ in the *off*-setting and $N_S > 0$ in the *on*-setting. We have that

$$D(\rho^{(0)^{\otimes n}}, \rho^{(N_S)^{\otimes n}}) \geq D(\sigma^{(0)^{\otimes n}}, \sigma^{(N_S)^{\otimes n}}), \tag{86}$$

which comes from the monotonicity of the quantum relative entropy under CPTP maps. This reduces the calculation to the one-way case. Following the proof of Theorem 1 in Ref. *(5)*, we find that

$$D(\sigma^{(0)^{\otimes n}}, \sigma^{(N_S)^{\otimes n}}) \geq \frac{n(1-\eta^2)N_S^2}{2\eta^2 N_B(1+\eta^2 N_B)} + o(N_S^2). \tag{87}$$

Solving for N_S ends the proof. □

S4: SNR of the SC state receiver

Here, we quantify the performance of the circuit QED implementation of $\hat{O}_\tau$ in terms of the signal-to-noise ratio.

Taylor expansion of $\hat{O}_\tau$: We first expand $\hat{U}_\tau^\dagger |e\rangle\langle e| \hat{U}_\tau$ with respect to the parameter τ:

$$\begin{aligned}\hat{U}_\tau^\dagger |e\rangle\langle e| \hat{U}_\tau = |e\rangle\langle e| + \tau \left[\hat{a}_R^\dagger \hat{\sigma}^- - \hat{a}_R \hat{\sigma}^+, |e\rangle\langle e|\right] \\ + \frac{\tau^2}{2!}\left[\hat{a}_R^\dagger \hat{\sigma}^- - \hat{a}_R \hat{\sigma}^+, [\hat{a}_R^\dagger \hat{\sigma}^- - \hat{a}_R \hat{\sigma}^+, |e\rangle\langle e|]\right] + o(\tau^2).\end{aligned} \tag{88}$$

We have that

$$\left[\hat{a}_R^\dagger \sigma^- - \hat{a}_R \hat{\sigma}^+, |e\rangle\langle e|\right] = \hat{a}_R^\dagger \hat{\sigma}^- + \hat{a}_R \hat{\sigma}^+ \equiv \hat{E}_1 \tag{89}$$

and

$$[\hat{a}_R^\dagger \hat{\sigma}^- - \hat{a}_R \hat{\sigma}^+, \hat{E}_1] = 2[\hat{a}_R^\dagger \hat{\sigma}^-, \hat{a}_R \hat{\sigma}^+] = -2|e\rangle\langle e| - 2\hat{\sigma}_z \hat{a}_R^\dagger \hat{a}_R \tag{90}$$

where $\sigma_z = |e\rangle\langle e| - |g\rangle\langle g|$ and we have used that $[\hat{\sigma}^-, \hat{\sigma}^+] = -\hat{\sigma}_z$. By applying the unitary evolution $\hat{S}(r)\hat{\sigma}_x$ to each of the terms, and using the relations $\hat{\sigma}_x \hat{\sigma}^\pm \hat{\sigma}_x = \hat{\sigma}^\mp$, $\hat{\sigma}_x \hat{\sigma}_z \hat{\sigma}_x = -\hat{\sigma}_z$

and $\hat{S}(r)^\dagger \hat{a}_R \hat{S}(r) = \hat{a}'_R$, we obtain

$$\hat{O}_\tau = |g\rangle\langle g| + \tau \hat{O}_{opt} + \tau^2 \hat{A} + o(\tau^2), \tag{91}$$

where $\hat{A} = -|g\rangle\langle g| + \hat{\sigma}_z \hat{a}'^\dagger_R \hat{a}'_R$. This holds for $\tau^2 \langle \hat{A} \rangle_{\rho_{\eta,\phi=0,\pi}} \ll 1$. In the $N_S \ll 1$, $N_B \gg 1$ regime, this means roughly $\tau^2 \ll 1/N_B$.

SNR estimation: We compute the SNR up to the second order in τ, obtaining

$$Q_{\hat{O}_\tau} \simeq \frac{\tau^2 (\langle \hat{O}_{opt} \rangle_{\rho_{\eta,\phi=0}} - \langle \hat{O}_{opt} \rangle_{\rho_{\eta,\phi=\pi}})^2}{(\lambda_+ - \lambda_+^2) + \tau^2 [\Delta \hat{O}^2_{opt} - 2\langle |g\rangle\langle g| (\mathbb{I} + \hat{a}'^\dagger_R \hat{a}'_R) \rangle_{\rho_{\eta,\phi=0}} - 2\lambda_+^2 \langle \hat{A} \rangle^2_{\rho_{\eta,\phi=0}}]} \tag{92}$$

$$= Q_{\hat{O}_{opt}} \left[\frac{\tau^2}{a + \tau^2 (1+b)} \right], \tag{93}$$

where $\Delta \hat{O}^2_{opt} = \langle \hat{O}^2_{opt} \rangle_{\rho_{\eta=0}} - \langle \hat{O}_{opt} \rangle^2_{\rho_{\eta=0}}$, $a = (\lambda_+ - \lambda_+^2)/\Delta \hat{O}^2_{opt}$ and $b = -[2\lambda_+^2 \langle \hat{A} \rangle^2_{\rho_{\eta,\phi=0}} + 2\langle |g\rangle\langle g| (\mathbb{I} + \hat{a}'^\dagger_R \hat{a}'_R) \rangle_{\rho_{\eta,\phi=0}}]/\Delta \hat{O}^2_{opt}$. Here, we have used the approximation $\langle \hat{O}^2_{opt} \rangle_{\rho_{\eta=0}} - \langle \hat{O}_{opt} \rangle^2_{\rho_{\eta=0}} \simeq \langle \hat{O}^2_{opt} \rangle_{\rho_{\eta,\phi}} - \langle \hat{O}_{opt} \rangle^2_{\rho_{\eta,\phi}}$ holding for any value of ϕ in the $\eta \ll 1$ limit. In the $N_S \ll 1$ and $N_B \gg 1$ regime, we have that $a \simeq N_S/N_B$, and $b \simeq -4N_S$. If $\tau^2 \gg \frac{a}{1-b}$, then the SNR of $\hat{O}_\tau$ is close to the optimal one. In the $N_B \gg 1$ regime, this happens whenever $\tau^2 \gg N_S/N_B$. Therefore, any value $N_S/N_B \ll \tau \ll 1/N_B$ approximates $\hat{O}_\tau$ to the optimal observable. For instance, by setting $\tau^2 = N_S/\sqrt{N_B} = \tau^{*2}$, we have that

$$\frac{Q_{\hat{O}_{\tau^*}}}{Q_{\hat{O}_{opt}}} \simeq 1 - \frac{a}{\tau^2} - b \tag{94}$$

$$\simeq 1 - \frac{1}{\sqrt{N_B}} + 4N_S. \tag{95}$$

S5: Qubit decoherence

Here, we show how the decoherence affects the qubit measurements. We are assuming a Markovian noise described by the Lindblad operator $\mathcal{L}_D/\hbar = \frac{\gamma}{2}\mathcal{D}[\hat{\sigma}_z] + \Gamma_\uparrow \mathcal{D}[\hat{\sigma}^+] + \Gamma_\downarrow \mathcal{D}[\hat{\sigma}^-]$, where $\mathcal{D}[\hat{L}]\rho = (\hat{L}\rho\hat{L}^\dagger - \frac{1}{2}\{\hat{L}^\dagger \hat{L}, \rho\})$. In order to do so, we solve the equation $\partial_t \hat{O} = \mathcal{L}^\dagger_D \hat{O}$ for different $\hat{O}$ defining a basis in the qubit Hilbert space, with $\mathcal{L}^\dagger_D$ being the dual of $\mathcal{L}_D$. The linearity of the time-translation operator allows us to find the solution for general qubit observables.

Lemma 6. *We have that*

$$e^{t\mathcal{L}_D^\dagger}\hat{\sigma}^- = e^{-\left[\gamma+\frac{\Gamma_\uparrow+\Gamma_\downarrow}{2}\right]t}\hat{\sigma}^- \tag{96}$$

$$e^{t\mathcal{L}_D^\dagger}\hat{\sigma}_z = e^{-(\Gamma_\uparrow+\Gamma_\downarrow)t}\hat{\sigma}_z + \left[1-e^{-(\Gamma_\uparrow+\Gamma_\downarrow)t}\right]\frac{\Gamma_\uparrow-\Gamma_\downarrow}{\Gamma_\uparrow+\Gamma_\downarrow}\mathbb{I}. \tag{97}$$

Proof. The relations can be derived by simply checking the action of the decoherence generators on the operator of interest. Notice that $\mathcal{L}_D^\dagger = \frac{\gamma}{2}\mathcal{D}[\hat{\sigma}_z]^\dagger + \Gamma_\uparrow\mathcal{D}[\hat{\sigma}^+]^\dagger + \Gamma_\downarrow\mathcal{D}[\hat{\sigma}^-]^\dagger$, where $\mathcal{D}[\hat{L}]^\dagger\hat{O} = \hat{L}^\dagger\hat{O}\hat{L} - \frac{1}{2}\{\hat{L}^\dagger\hat{L},\hat{O}\}$. We have that

$$\mathcal{D}[\hat{\sigma}_z]^\dagger\hat{\sigma}^- = -2\hat{\sigma}^- \tag{98}$$

$$\mathcal{D}[\hat{\sigma}^+]^\dagger\hat{\sigma}^- = -\frac{\hat{\sigma}^-}{2} \tag{99}$$

$$\mathcal{D}[\hat{\sigma}^-]^\dagger\hat{\sigma}^- = -\frac{\hat{\sigma}^-}{2}, \tag{100}$$

from which Eq. (96) follows trivially using $e^{t\mathcal{L}_D^\dagger} = \sum_{k=0}^\infty \frac{t^k\mathcal{L}_D^{\dagger k}}{k!}$. We have that

$$\mathcal{D}[\hat{\sigma}_z]^\dagger\hat{\sigma}_z = 0 \tag{101}$$

$$\mathcal{D}[\hat{\sigma}^+]^\dagger\hat{\sigma}_z = 2|g\rangle\langle g| \tag{102}$$

$$\mathcal{D}[\hat{\sigma}^-]^\dagger\hat{\sigma}_z = -2|e\rangle\langle e|, \tag{103}$$

from which it follows that $\mathcal{L}_D^\dagger\hat{\sigma}_z = -(\Gamma_\uparrow+\Gamma_\downarrow)\hat{\sigma}_z + (\Gamma_\uparrow-\Gamma_\downarrow)\mathbb{I}$. By using that $\mathcal{L}_D^\dagger\mathbb{I} = 0$, we infer that $\mathcal{L}_D^{\dagger k}\hat{\sigma}_z = (-1)^k(\Gamma_\uparrow+\Gamma_\downarrow)^k\hat{\sigma}_z + (-1)^{k-1}(\Gamma_\uparrow+\Gamma_\downarrow)^{k-1}(\Gamma_\uparrow-\Gamma_\downarrow)\mathbb{I}$, $k = 1,2,\ldots$ Eq. (97) follows trivially. □

Therefore, we have that $T_1 = (\Gamma_\uparrow+\Gamma_\downarrow)^{-1}$ and $T_2 = \left(\gamma+\frac{\Gamma_\uparrow+\Gamma_\downarrow}{2}\right)^{-1}$.

References

1. J. Calsamiglia, R. Muñoz-Tapia, Ll. Masanes, A. Acin, and E. Bagan, "Quantum Chernoff bound as a measure of distinguishability between density matrices: Application to qubit and Gaussian states", Phys. Rev. A **77**, 032311 (2008).

2. M. Paris, "Quantum Estimation for Quantum Technology", Int. J. Quant. Inf. **7**, 125 (2009).

3. S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications", Nat. Comm. **8**, 15043 (2017).

4. K. P. Seshadreesan, L. Lami, and M. M. Wilde, "Renyi relative entropies of quantum Gaussian states", J. of Math. Phys. **59**, 072204 (2018).

5. M. S. Bullock, C. N. Gagatsos, S. Guha, and Boulat A. Bash, "Fundamental limits of quantum-secure covert communication over bosonic channels", IEEE Journal on Selected Areas in Communications, vol. 38, no. 3, pp. 471-482 (2020).

Figures

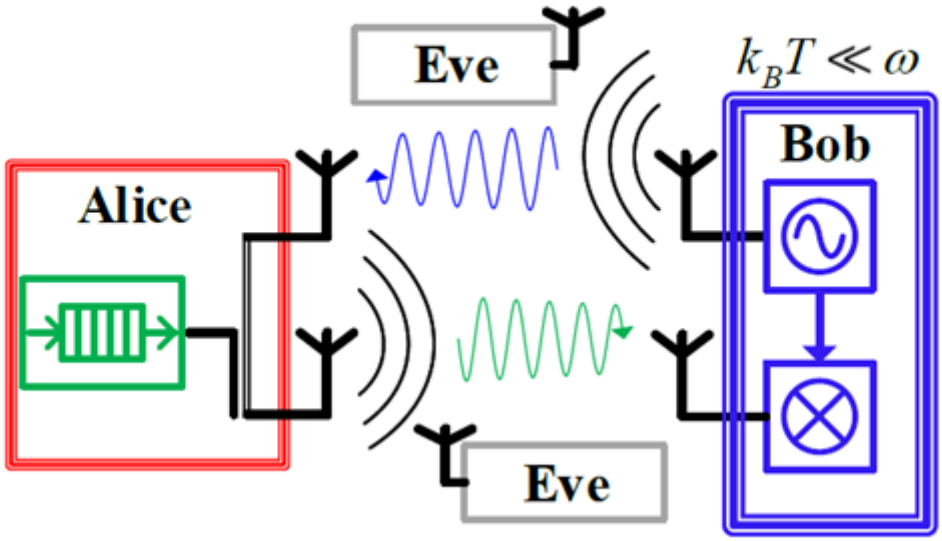

Figure 1

Sketch of the two-way quantum communication protocol. Bob sends a signal to Alice, who embeds the message by phase modulation. The signal is then sent back to Bob, who retrieve the information via a suitable measurement. Bob may use quantum correlations in order to increase the signal-to-noise ratio. A passive Eve is able to collect the photons lost in both paths, but she does not have access to Bob and Alice labs.

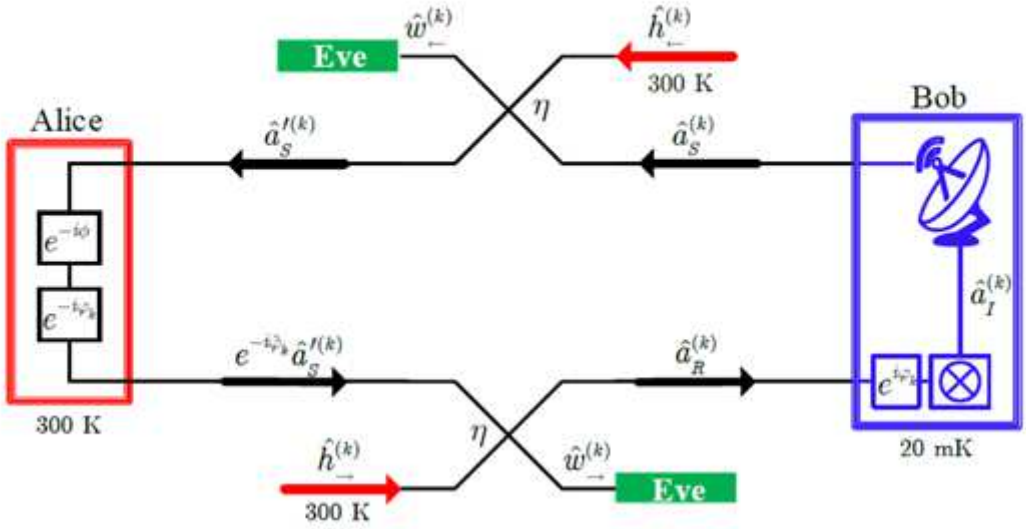

Figure 2

Setup for the two-way covert quantum communication through a bright bosonic channel.

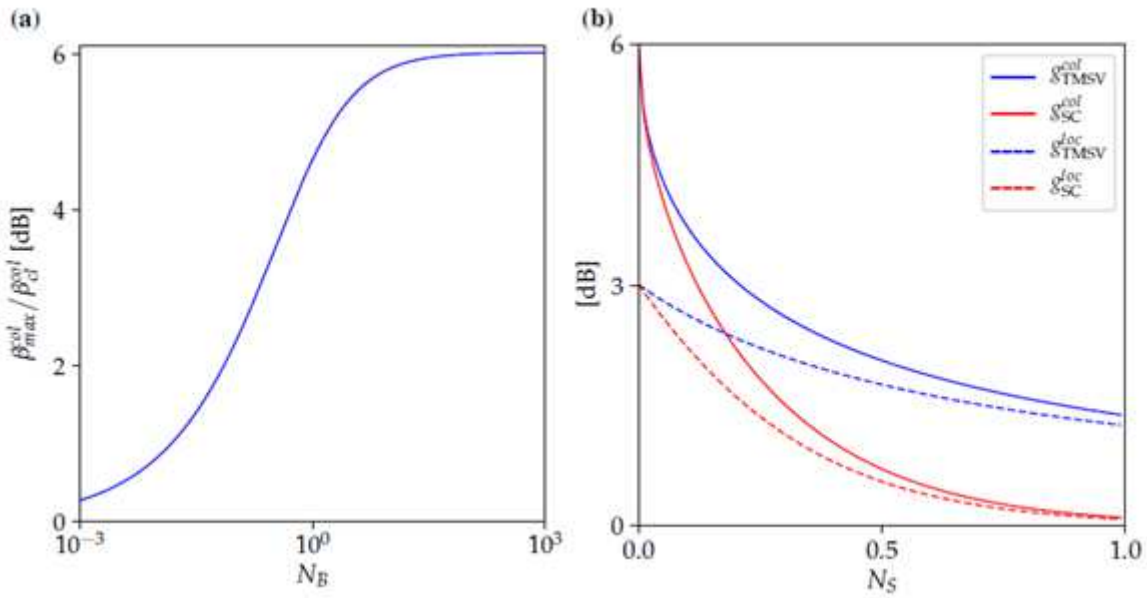

Figure 3

Performance of the quantum correlated protocol with respect to the idler-free case.

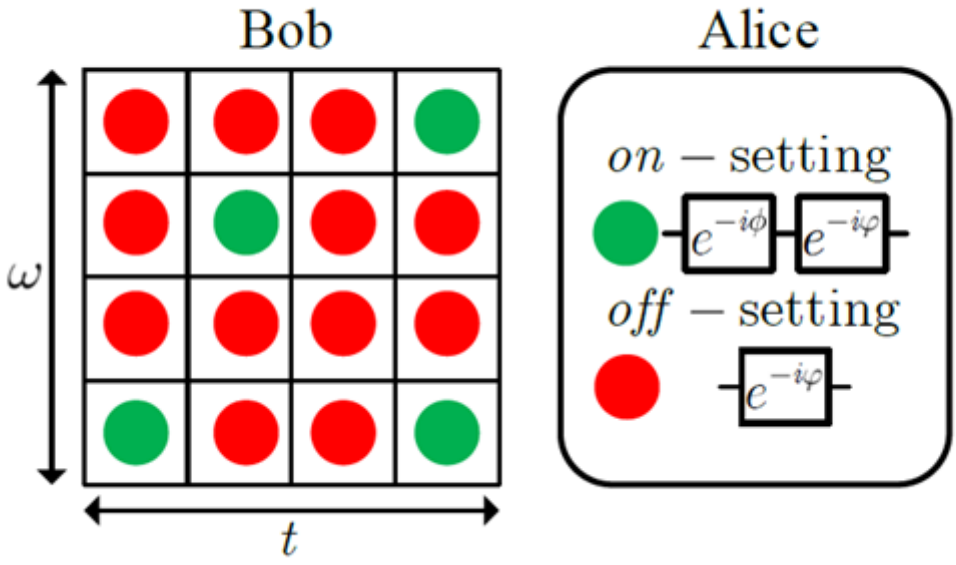

Figure 4

Probabilistic version of the two-way covert quantum communication protocol.

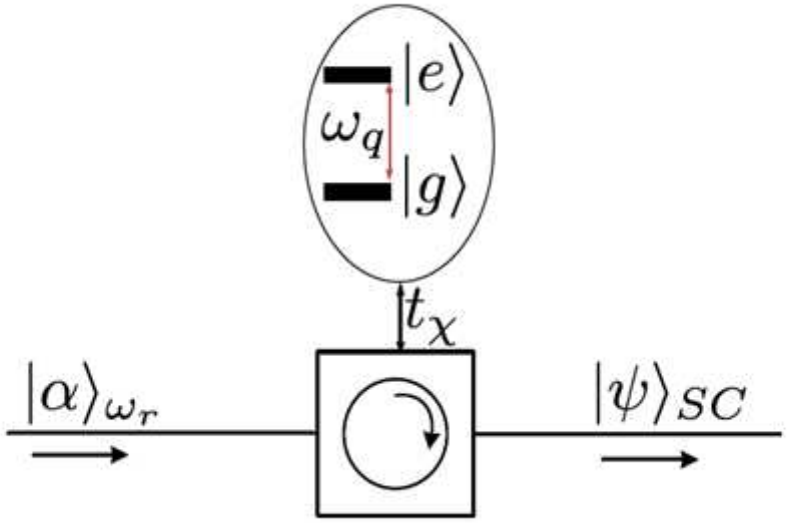

Figure 5

Scheme for the preparation of the Schr¨odinger's cat state.

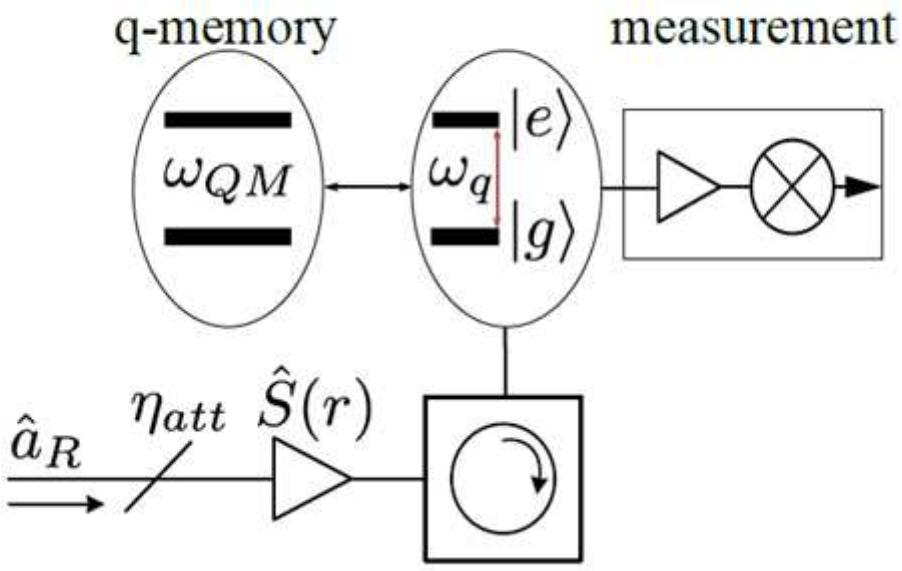

Figure 6

Scheme for the implementation of the observable optimizing the quantum Fisher information.