Di Candia, Roberto; Jäntti, Riku; Duan, Ruifeng; Lietzén, Jari; Khalifa, Hany; Ruttik, Kalle

Quantum Backscatter Communication: A New Paradigm

Published in:
Proceedings of 2018 15th International Symposium on Wireless Communication Systems (ISWCS)

DOI:
10.1109/ISWCS.2018.8491095

Published: 01/01/2018

Document Version
Peer reviewed version

Please cite the original version:
Di Candia, R., Jäntti, R., Duan, R., Lietzén, J., Khalifa, H., & Ruttik, K. (2018). Quantum Backscatter Communication: A New Paradigm. In *Proceedings of 2018 15th International Symposium on Wireless Communication Systems (ISWCS)* (pp. 1-6). [8491095] (International Symposium on Wireless Communication Systems). IEEE. https://doi.org/10.1109/ISWCS.2018.8491095

Quantum Backscatter Communication: A New Paradigm

Roberto Di Candia*, Riku Jäntti†, Ruifeng Duan†, Jari Lietzén†, Hany Khalifa†, and Kalle Ruttik†
*Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany.
Email: rob.dicandia@gmail.com
†Department of Communications and Networking, Aalto University, Espoo, 02150 Finland.
Email: {riku.jantti; ruifeng.duan; jari.lietzen; hany.khalifa; kalle.ruttik}@aalto.fi

***Abstract*—In this paper, we propose a novel quantum backscatter communications (QBC) protocol, inspired by the quantum illumination (QI) concept. In the QBC paradigm, the transmitter generates entangled photon pairs. The signal photon is transmitted and the idler photon is kept at the receiver. The tag antenna communicates by performing the pulse amplitude modulation (PAM), binary phase shift keying (BPSK) or quadratic phase shift keying (QPSK) on the signal impinging at the antenna. Using the sum-frequency-generation receiver, our QBC protocol achieves a 6 dB error exponent gain for PAM and BPSK, and 3 dB gain for QPSK over its classical counterpart. Finally, we discuss the QI-enhanced secure backscatter communication.**

***Index Terms*—Quantum communication, backscatter communication, quantum illumination, error probability exponent**

I. Introduction

Backscatter of radio waves is a subject of active study since the development of radar in the 1930s, and the use of it for communications since 1948 [1]. Backscatter communication (BC) is widely used in radio frequency (RF) identification tags, and it bears close resemblance with the radar. Quantum radar [2] is a remote-sensing method based on quantum entanglement. Quantum illumination (QI) was introduced by S. Lloyd in 2008, which is a revolutionary photonic quantum sensing paradigm that enhances the sensitivity of photodetection in noisy and lossy environments with the idea of using entangled photons [3], [4]. The signal photon is transmitted from the antenna and interacts with the target. The idler, or ancilla, photon is kept at the receiver (RX). The detection is carried out using a joint measurement on the backscattered signal and the idler such that the quantum correlation between these two distills the signal from the noise. Later this scheme was extended to Gaussian states and it was found that in an optimal scenario of a two-mode squeezed vacuum state, one may obtain 6 dB of signal to noise ratio (SNR) improvement [5]. The application in the microwave regime was proposed afterwards, and it paved the way to a prototype of quantum radar [6].

The quantum radar has two merits over the classical radar: firstly, some target geometries become more visible in the quantum regime, and secondly, the sensitivity of the radar is enhanced beyond the limits of the classical radar [7]. Three detector schemes have been proposed for the QI-enhanced quantum radar. First, the simplest one is based on an optical parametric amplifier (PA) [8], [9], which amplifies intensity of signal light using nonlinear laser frequency conversion [10], and obtains only 3-dB SNR improvement. The second one is based on sum-frequency generation (SFG) [11], which is a second order nonlinear optical process generating a photo at a third frequency based on the annihilation of two input photons at two angular frequencies [12], and can achieve the full 6-dB improvement. Both detectors are coherent and require exact knowledge of the channel-induced phase offset. A modified SFG-RX for non-coherent detection has been proposed in [13] that achieves the same 3-dB improvement as OPA without the need to estimate the channel phase.

In addition, quantum communication is an emerging area of engineering that seeks to apply the non-classical, quantum, resources to enhance the performance of communication systems. Majority of the work in quantum communication has focused on, such as, quantum key distribution at optical frequencies [14], and quantum error correction coding [15]. The use of QI for quantum key distribution has been suggested in [16]. However, relatively little work in quantum communication has focused directly on wireless applications and even less in the field of wireless microwaves. The quantum-assisted wireless communication (QAWC) research seeks to apply quantum computers to enhance the digital base band processing at the RX [17], [18]. Recently, direct applications of quantum techniques to wireless communications have started to emerge. In [19], a multi-user-controlled bidirectional quantum-secure communication network protocol for transmitting qubits was proposed. Importantly, we have conducted the first work in [20] to consider the use of microwave quantum radar technology for wireless backscatter communication. Particularly, [20] has proposed to construct pre-coding and RX-beamforming beam-splitters such that the orthogonal eigen-channels can be accessed using quantum backscatter communication (QBC).

In this paper, we propose to use QI to enhance backscatter communications aiming at describing the QBC concept and analyzing its performance in terms of bit error rate (BER). The proposed QBC paradigm bears close resemblance to the quantum radar in a manner similar to BC being closely related to the classical radar. In the proposed QBC paradigm, the reader antennas are pointed toward a tag antenna that communicates by performing the pulse amplitude modulation (PAM), binary phase shift keying (BPSK) or quadratic phase shift keying (QPSK) on the signal. The RX is then able to discriminate the states of the idler-signal system after the

corresponding phase and amplitude modulation are performed by the tag. We compare the classical architecture, consisting in illuminating the antenna with classical light or microwave signal and performing heterodyne detection, with the quantum architecture using Gaussian entangled states as resources. We quantify the quality of the performance in a Bayesian setting by seeking the best scaling of the error probability (EP) averaged over the a priori probabilities of each symbol. In the PAM and BPSK cases, the quantum setting allows for up to 6 dB improvement in the EP exponent (EPE) [4]. This can be achieved by a slight modification of the Zhuang-RX (interchangeably called SFG-RX) proposed in [11], based on an SFG circuit, PAs, photon-counter and a feedback loop. Alternatively, a simpler circuit based only on parametric amplification and photon-counting can achieve a 3 dB gain [8], [9], which has been implemented in a laboratory environment in the optical regime [21]. We further show that only SFG-RX achieves a 3 dB gain in the QPSK case. At the end, we argue that the BPSK and QPSK schemes are useful for quantum cryptography, allowing for secure communication between the antenna and the RX.

A. States, Observables, and Quantum Harmonic Oscillator

In quantum mechanics, the *state of a system* can be represented by column vector $|\psi\rangle \in \mathbb{C}^{\infty}$, normalized as $\langle\psi|\psi\rangle = 1$. [1] *Observables* are Hermitian [2] operators $\hat{O} \in \mathbb{C}^{\infty\times\infty}$. The expectation value of the observable $\hat{O}$ on the state $|\psi\rangle$ is defined as $\langle\hat{O}\rangle_{\psi} \equiv \langle\psi|\hat{O}|\psi\rangle \in \mathbb{R}$. The *Hamiltonian of a system* is an operator $H \in \mathbb{C}^{\infty\times\infty}$, which rules the evolution of the state of the system via the Schrödinger's equation: $i\hbar\partial_t|\psi(t)\rangle = H|\psi(t)\rangle$, where $\hbar$ denotes the reduced Planck constant and $i = \sqrt{-1}$. These concepts can be easily generalized to bipartite systems by using the tensor product formalism. The joint state of two separate systems is represented by a vector $|\psi\rangle_{AB} \in \mathbb{C}^{\infty} \otimes \mathbb{C}^{\infty}$, where $\otimes$ denotes the tensor product and ${}_{AB}\langle\psi|\psi\rangle_{AB} = 1$. Observables in bipartite systems are Hermitian operators $\hat{O}_{AB} \in \mathbb{C}^{\infty\times\infty} \otimes \mathbb{C}^{\infty\times\infty}$. [3] A bipartite state $|\psi\rangle_{AB}$ is said to be *entangled* if it can not be decomposed as $|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\chi\rangle_B$. Entangled states show correlations between outcomes of measurements on the individual systems which are not reproducible in the classical systems, and they will be a key resources for the results in this paper.

In the low photon number regime, if the thermal fluctuations are negligible, the electromagnetic field behaves according to quantum electrodynamic theory. The free Hamiltonian of quantized electromagnetic field has the same form as the Hamiltonian of quantum harmonic oscillator $H = \hbar\omega\left(\hat{a}^{\dagger}\hat{a} + 1/2\right)$ with the annihilation operator $\hat{a}$ and the creation operator $\hat{a}^{\dagger}$. Their action on the basis defined by the eigenvectors $\{|n\rangle\}_{n=0}^{\infty}$ of the Hamiltonian H is $\hat{a}|n\rangle = \sqrt{n}|n-1\rangle$ and $\hat{a}^{\dagger}|n\rangle = \sqrt{n+1}|n+1\rangle$. Moreover, the commutation relation $[\hat{a}, \hat{a}^{\dagger}] = 1$ hold. The eigenstates of the operator $\hat{a}$ are referred to as coherent states, and we refer to them as classical states, because the statistics of their measurements resembles the one of the classical signals. The canonical position and momentum-like operators are given by $\hat{x} \equiv (\hat{a} + \hat{a}^{\dagger})/\sqrt{2}$ and $\hat{p} \equiv -i(\hat{a} - \hat{a}^{\dagger})/\sqrt{2}$ respectively.

B. Backscatter Communication

The BC consists in sending a signal to a tag, which chooses a symbol $(\sqrt{\eta}, \phi)$ belonging to alphabet $\mathcal{A}$ that defines a particular BC scheme, where $\sqrt{\eta}$ and ϕ denote the amplitude and the phase, respectively. In this work we consider the following BC schemes using PAM, BPSK, and QPSK modulation techniques:

$$\begin{aligned}
\mathcal{A}_{\mathsf{PAM}} &= \{(\sqrt{\eta_1}, 0), (\sqrt{\eta_2}, 0)\}\,,\\
\mathcal{A}_{\mathsf{BPSK}} &= \{(\sqrt{\eta}, 0), (\sqrt{\eta}, \pi)\}\,,\\
\mathcal{A}_{\mathsf{QPSK}} &= \{(\sqrt{\eta}, 0), (\sqrt{\eta}, \pi/2), (\sqrt{\eta}, \pi), (\sqrt{\eta}, 3\pi/2)\}\,.
\end{aligned}$$

In this framework, the QI setup previously studied in the literature corresponds to the PAM case with $\eta_1 = 0$, i.e., on-off keying modulation. In this paper, we consider the symmetric case, where all the symbols are chosen with equal *a priori* probability, and the performance of the BC scheme is quantified by the EP, defined as

$$P_{\mathsf{err}} = \frac{1}{|\mathcal{A}|}\sum_{(\eta,\phi)\in\mathcal{A}} \Pr\left[\bar{H}_{(\eta,\phi)}\middle|H_{(\eta,\phi)}\right], \tag{1}$$

where $|\mathcal{A}|$ is the size of $\mathcal{A}$ and $\Pr[\bar{H}|H]$ is the probability that, given the hypothesis H, we wrongly declare a different hypothesis. The EP P_{err} decays exponentially in both the classical and in the quantum case. We will show a quantum-RX decaying at a higher rate with respect the classical case.

The rest of this paper is organized as follows. In Section II, we describe a bistatic QI-enhanced quantum backscatter system. Section III introduces the quantum receivers and discusses quantum protocols, and we then compare the performance of classical and quantum receivers. We discuss in Sec. IV the possibility of using QI to enhance the secure backscatter communication. Finally, Section IV concludes the paper.

II. System model

The quantum backscatter system shown in Fig. 1 enhances the feature of a classical QBC using entangled photons. In the classical case, the transmitter (TX) transmits an unmodulated carrier backscattered from the tag to the RX. The carrier is modeled in quantum mechanics as a coherent state $|\alpha\rangle_S = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\sqrt{\alpha^n/n!}\,|n\rangle$, where α is a parameter related to the mean number of signal photons.

[1] We use the bra-ket notation. The scalar product between two states $|\phi\rangle$ and $|\psi\rangle$ is denoted by $\langle\phi|\psi\rangle \equiv \sum_i \phi_i^*\psi_i$, where * denotes complex conjugate of a number. The operators $\hat{A} \in \mathbb{C}^{\infty\times\infty}$ apply only on the right so that $\langle\phi|\hat{A}|\psi\rangle = \sum_i \phi_i^*(\hat{A}\psi)_i = [\sum_i \psi_i^*(\hat{A}^{\dagger}\phi)_i]^* = \langle\psi|\hat{A}^{\dagger}|\phi\rangle^*$, where † is an adjoint operator.

[2] Despite non-Hermitian operators, i.e., $\hat{A} \neq \hat{A}^{\dagger}$, do not represent measurable quantities, it is useful to formally define their expectation values on the state $|\psi\rangle$ as $\langle\hat{A}\rangle_{\psi} \equiv \langle\psi|\hat{A}|\psi\rangle \in \mathbb{C}$.

[3] Observables of individual systems are operators $\hat{O}_A \otimes \mathbb{I}$ and $\mathbb{I} \otimes \hat{O}_B$, and are usually denoted simply as $\hat{O}_A$ and $\hat{O}_B$. Here $\mathbb{I}$ is the identity operator.

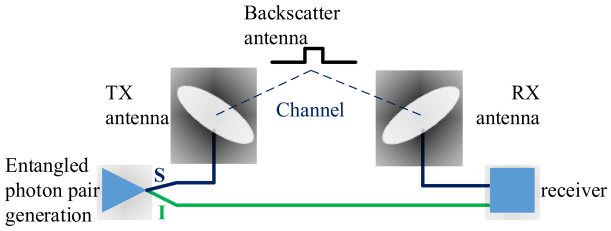

Fig. 1. An illustration of bistatic QI-enhanced QBC systems.

In the QI setup, the entangled signal-idler (S-I) photon pairs are first generated at the TX. The S-photon is transmitted and backscattered from a tag antenna. The idler is kept at the RX to be measured jointly with the backscattered signal. The RX uses both the received S-photon from the RX antenna and the I-photon. The system in Fig. 1 is bistatic[4], meaning that the transmitter and the RX are separated in space. We consider a source able to continuously generate S-I photon pairs in the radio frequency regime in a two-mode squeezed state (TMSS)

$$|\psi\rangle_{SI} = \sum_{n=0}^{\infty} \sqrt{N_S^n/(N_S+1)^{n+1}}\, |n\rangle_S |n\rangle_I,$$

where N_S is the average number of photons of both the signal and the idler [4], [8], [9], [11]. The joint probability distribution of the quadratures of the TMSS is a Gaussian with zero mean value, hence the state is well defined by its covariance matrix. Indeed, if $\hat{a}_S$ and $\hat{a}_I$ represent the modes of the signal and the idler, respectively, then we have that $\langle \hat{a}_S^\dagger \hat{a}_S \rangle = \langle \hat{a}_I^\dagger \hat{a}_I \rangle = N_S$, $\langle \hat{a}_S \hat{a}_I \rangle = \sqrt{N_S(N_S+1)}$ and $\langle \hat{a}_S^\dagger \hat{a}_I \rangle = 0$.

We model the quantum channel with a low-reflectivity beam splitter, whose inputs are the signal and a thermal state modeling the effect of the environment. This is described with the unitary operator

$$B_{\eta,\phi} = \exp\left[\sin^{-1}(\sqrt{\eta})\left(\hat{a}_S^\dagger \hat{a}_Z e^{-i\phi} - \hat{a}_S \hat{a}_Z^\dagger e^{i\phi}\right)\right],$$

where ϕ is the phase shift, and η is the round-trip transmissivity (RTT) of the channel. Here, the environmental thermal mode $\hat{a}_Z$ is a Gaussian mode. The number of thermal photons $N_Z = (e^{\hbar\omega/k_B T} - 1)^{-1}$, where T is the environment temperature and k_B the Bolzmann constant. Both the impact of the propagation path loss and the tag antenna are included in the effective parameters $\eta \ll 1$ and ϕ. The input-output relations of the beam splitter read

$$\hat{a}_R \equiv B_{\eta,\phi}^\dagger \hat{a}_S B_{\eta,\phi} = \sqrt{\eta} e^{-i\phi} \hat{a}_S + \sqrt{1-\eta}\hat{a}_Z, \quad (2)$$

$$\hat{a}_Y \equiv B_{\eta,\phi}^\dagger \hat{a}_Z B_{\eta,\phi} = -\sqrt{\eta} e^{i\phi} \hat{a}_Z + \sqrt{1-\eta}\hat{a}_S, \quad (3)$$

where $\hat{a}_R$ is the received mode, and $\hat{a}_Y$ corresponds to modes that are not received and can thus be ignored.

[4]We assume that the I-photons are available for the RX without losses. In mono-static case, the idler photon is directly available at the RX. In the bistatic case, it would need to be transmitted over a cable to the RX. In practice this transmission will cause losses which will reduce the system gain.

Depending on the transmit and receive antenna gains G_t and G_r of the reader, distance from the transmitter to the tag R_t, the communication frequency ω, and the distance from tag to RX R_r, the RTT η can be represented as:

$$\eta = \frac{G_r G_t \mathsf{c}^2 \sigma_Q}{(16\pi\omega^2 R_t^2 R_r^2)},$$

where c denotes the speed of light. The parameter $\sigma_Q = \langle \hat{I}_s \rangle / \langle \hat{I}_i \rangle$ is the Quantum Radar Cross Section (QRCS) [7], where $\langle \hat{I}_s \rangle$ denotes the intensity measured by a detector after a photon is reflected by atoms on the target surface, the tag antenna in our case, and $\langle \hat{I}_i \rangle$ is the incident intensity calculated assuming the target to act as a photon detector. The phase shift of the channel ϕ depends on the communication distance $R = R_t + R_r$ and the phase shift caused by the tag $\phi = 2\pi R/\mathsf{c} + \varphi$. A large number of mode pairs M are needed in order to perform the quadrature sampling detection (QSD) at the RX. The available number of mode pairs $M = WT_s$ depends on the phase matching bandwidth W and the tag symbol duration T_s assumed to be small compared to the channel coherence time.

III. Performance Analysis

A. Classical receiver

In the base-line classical case (referred to as C-RX), i.e. without using QI technique, the carrier is a Gaussian mode in a coherent state with an average number of photons N_S. Heterodyne detection is then performed on each of the M copies of the received mode $\hat{a}_R$ defined in (2). Heterodyne detection is modeled in the quantum formalism as a $50:50$ beam splitter with outputs $\hat{a}_1 = (\hat{a}_R + \hat{a}_V)/\sqrt{2}$ and $\hat{a}_2 = (\hat{a}_R - \hat{a}_V)/\sqrt{2}$, where $\hat{a}_V$ is a complex Gaussian noise with variances $\langle \hat{x}_V^2 \rangle = \langle \hat{p}_V^2 \rangle = 1/2$. Let us introduce the complex envelope $\hat{S} \equiv (\hat{x}_1 + i\hat{p}_2)/\sqrt{N_S}$ with mean value $\langle \hat{S} \rangle = \sqrt{\eta} e^{-i\phi}$, given that $\langle \hat{x}_1 \rangle = \sqrt{\eta N_S}\cos(\phi)$ and $\langle \hat{p}_2 \rangle = -\sqrt{\eta N_S}\sin(\phi)$. If we measure $M \gg 1$ times both $\hat{x}_1$ and $\hat{p}_2$, we can estimate the mean value of the complex envelope with the sample mean $\bar{S} \equiv \sum_{i=1}^{M} S_i/M$. Finally, we declare the symbol $\{\sqrt{\tilde{\eta}}, \tilde{\phi}\} = \text{argmin}_{\{\sqrt{\tau},\varphi\}\in\mathcal{A}_L} \left|\bar{S} - \sqrt{\tau} e^{-i\varphi}\right|$, and the protocol succeeds if $\{\sqrt{\tilde{\eta}}, \tilde{\phi}\} = \{\sqrt{\eta}, \phi\}$. In the classical setup, regardless the BC scheme used, it is well-known that the EP P_{err}^c is lower-bounded by [9]

$$P_{\mathsf{err}}^c \geq \frac{1}{2|\mathcal{A}|}\text{erfc}\left(\sqrt{\frac{\min_{\tilde{k}\neq k} d_{k\tilde{k}}^2 N_S M}{4N_Z}}\right) \sim e^{-\frac{\min_{\tilde{k}\neq k} d_{k\tilde{k}}^2 N_S M}{4N_Z}}, \quad (4)$$

where $d_{k\tilde{k}} \equiv |\sqrt{\eta_k} e^{-i\phi_k} - \sqrt{\eta_{\tilde{k}}} e^{-i\phi_{\tilde{k}}}|$ and the minimum is taken over the elements of $\mathcal{A}$. This provides the asymptotic behaviour of the classical EP. For the considered BC schemes we have that: $|\mathcal{A}_{\mathsf{PAM}}| = 2$ and $d_{k\tilde{k}}^2 = |\sqrt{\eta_2} - \sqrt{\eta_1}|^2 \equiv d_{\mathsf{PAM}}^2$ for PAM; $|\mathcal{A}_{\mathsf{BPSK}}| = 2$ and $d_{k\tilde{k}}^2 = 4\eta \equiv d_{\mathsf{BPSK}}^2$ for BPSK; $|\mathcal{A}_{\mathsf{QPSK}}| = 4$ and $\min_{\tilde{k}\neq k} d_{k\tilde{k}}^2 = 2\eta \equiv d_{\mathsf{QPSK}}^2$ for QPSK.

B. Quantum receiver

In the quantum case, different symbols correspond to different quantum states at the RX. Therefore, the task reduces to find a measurement discriminating with the least number of measurements, between the quantum states which are the possible outputs of the considered QBC scheme. A practical requirement consists in finding an experimentally feasible circuit achieving the optimal measurement. The optimal decision rule for discriminating between two equally likely quantum states ρ_0 and ρ_1 was found by Helstrom [22]. It consists in measuring the operators E_0, E_1, with $E_0 + E_1 = \mathbb{I}$, where E_1 is the projection on the range of the positive part of $\rho_1 - \rho_0$. The corresponding optimal EP is $P_H = (1 - \|\rho_0 - \rho_1\|_1)/2$. In the multiple copies case, where we need to discriminate between the two states $\rho_0^{\otimes M}$ and $\rho_1^{\otimes M}$, with $M \gg 1$, the computation of the optimal probability and the corresponding measurement can be substantially challenging. An upper bound on the EP is provided by the *quantum Chernoff bound* (QCB) [23], stating that $P_H \leq e^{-M\xi_{QCB}}$, where $\xi_{QCB} = -\log\left(\min_{0\leq s\leq 1} \mathrm{Tr}\left(\rho_0^s \rho_1^{1-s}\right)\right)$. This bound is asymptotically tight, i.e. $P_H \sim e^{-M\xi_{QCB}}$ for $M \gg 1$.

In the QI setup, the QCB has been computed for PAM case in [4], showing a 6 dB gain over the best classical strategy. Recently, a measurement saturating the Helstrom EP has been obtained in [11]. It applies an SFG to the modes at the RX, allowing to map the problem to the discrimination between two coherent states, where the Dolinar RX is known to be optimal for this task [24]. A suboptimal RX, achieving a 3 dB gain and consisting in a PA and photon-counting, has been proposed in [8] and implemented in [21]. The performance loss is accompanied with a benefit in the experimental feasibility, as the latter RX involves only two-mode interactions in contrast to three-mode interactions needed in the SFG-RX. We show how these RXs achieve a gain in QBCs.

PA-receiver: It consists in the measurement of the observable $\hat{O}_{PA} = \hat{a}_I \hat{a}_R + \hat{a}_I^\dagger \hat{a}_R^\dagger$, with mean value $\langle \hat{O}_{PA} \rangle = \sqrt{\eta N_S(N_S+1)}\cos(\phi)$ and variance[5] $\langle O_{PA}^2 \rangle - \langle \hat{O}_{PA} \rangle^2 \approx N_Z$. This is implemented with the help of a PA, whose input-output relations are

$$\hat{c} = \sqrt{G}\hat{a}_I + \sqrt{G-1}\hat{a}_R^\dagger \quad \text{and} \quad \hat{d} = \sqrt{G}\hat{a}_R + \sqrt{G-1}\hat{a}_I^\dagger. \tag{5}$$

If we choose $G = 1 + \varepsilon^2$, with $N_S/N_Z \ll \varepsilon^2 \ll 1/N_Z$ [8], then the photon-number operator approximates $\hat{O}_{PA}$:

$$\hat{c}^\dagger \hat{c} = G\,\hat{a}_I^\dagger \hat{a}_I + (G-1)\,\hat{a}_R \hat{a}_R^\dagger + \sqrt{G(G-1)}\,\hat{O}_{PA} \approx \varepsilon\,\hat{O}_{PA}, \tag{6}$$

where we have used that $\varepsilon^2 \ll 1/N_Z$ and $\langle \hat{a}_I^\dagger \hat{a}_I \rangle = N_S \ll 1$ in order to conclude that $G\,\hat{a}_I^\dagger \hat{a}_I + (G-1)\,\hat{a}_R \hat{a}_R^\dagger \approx 0$. A threshold strategy can be easily defined, showing a 3 dB advantage of the QBC over BC in the PAM and BPSK cases, where $|\langle \hat{O}_{PA} \rangle|$ is maximal. Indeed, if we consider the sample mean $\bar{O}_{PA} = \sum_{k=1}^M O_{PA}^k/M$, where O_{PA}^k is the measurement outcome of the k-th copy, we declare the symbol $\{\bar{\eta}, \bar{\phi}\} = \mathrm{argmin}_{\{\sqrt{\eta},\phi\}\in\mathcal{A}} \left|\bar{O}_{PA} - \sqrt{\eta}e^{-i\phi}\right|$. It was shown in [8], [9], with a Cramer-Chernoff theorem based argument, that

$$P_{\mathsf{err}}^{PA} \leq e^{-d^2_{\mathsf{PAM(BPSK)}} N_S M/2N_Z}. \tag{7}$$

The EPE is twice the one found in (4), which corresponds to a 3 dB gain. However, the PA receiver does not provide any gain in the QPSK scheme since the symbols are not aligned.

SFG-RX: It maps the problem to the one of discriminating between coherent states [11]. The SFG circuit is described by the interaction Hamiltonian

$$H_I = \hbar g \sum_{m=1}^M \left(\hat{b}^\dagger \hat{a}_{R_m} \hat{a}_{I_m} + \hat{b}\hat{a}_{R_m}^\dagger \hat{a}_{I_m}^\dagger\right),$$

where $\{\hat{a}_{R_m}, \hat{a}_{I_m}\}_{m=1}^M$ are the modes corresponding to the different copies of the RX and the idler, $\hat{b}$ is initially in the vacuum state, and g is the coupling parameter. If we assume the low-brightness conditions $n_R(t) \equiv \langle \hat{a}_{R_m}^\dagger \hat{a}_{R_m} \rangle_t \ll 1$, $n_I(t) \equiv \langle \hat{a}_{I_m}^\dagger \hat{a}_{I_m} \rangle_t \ll 1$ and $|C(t)|^2 \equiv |\langle \hat{a}_{S_m} \hat{a}_{R_m} \rangle_t|^2 \ll 1$, then one can solve the dynamics in the qubit approximation, finding that the mode $\hat{b}$ is in a coherent state mixed with a weak thermal noise [11]:

$$\begin{aligned}
C(t) &= C(0)\cos(\sqrt{M}gt), \\
n_R(t) &= n_R(0), \quad n_I(t) = n_I(0), \\
b(t) &= -i\sqrt{M}C(0)\sin(\sqrt{M}gt), \\
n_b(t) &= [M|C(0)|^2 + n_I(0)n_R(0)]\sin^2(\sqrt{M}gt),
\end{aligned}$$

where $n_I(0)n_R(0)$ term in the last equation is the aforementioned thermal noise contribution. If we let evolve the circuit for a time $t_l = l\pi/2\sqrt{M}g$, with l positive odd integer, then the correlations between the RX modes $C(t)$ disappears in favour of the coherent state amplitude $b(t)$. This results in the following input-output relations:

$$\hat{a}_{R_m}(t_l) = \sqrt{1+|C(0)|^2}\,\hat{a}_{R_m}(0) - C(0)\,\hat{a}_{I_m}^\dagger, \tag{8}$$

$$\hat{a}_{I_m}(t_l) = \sqrt{1+|C(0)|^2}\,\hat{a}_{I_m}(0) - C(0)\,\hat{a}_{R_m}^\dagger. \tag{9}$$

Notice that $n_R(0) \simeq N_Z \gg 1$, which lets the low-brightness condition fall. This issue is solved by sending the modes $\hat{a}_{R_m}$ to a low-transmissivity beam splitter, obtaining

$$\begin{aligned}
\hat{a}_{R_m,1}^{(1)} &= \sqrt{\tau}\,\hat{a}_{R_m} + \sqrt{1-\tau}\,\hat{v}_m^{(1)}, \quad \text{and} \\
\hat{a}_{R_m,2}^{(1)} &= \sqrt{1-\tau}\,\hat{a}_{R_m} - \sqrt{\tau}\,\hat{v}_m^{(1)},
\end{aligned}$$

where $\hat{v}_m^{(1)}$ is a vacuum mode and $\tau N_Z \ll 1$. We then send $\hat{a}_{R_m,1}^{(1)}$ and $\hat{a}_{I_m}^{(1)} = \hat{a}_{I_m}$ as inputs of the SFG circuit, which generates the mode $\hat{b}^{(1)}$ in a coherent state $|\sqrt{\tau M}C(0)\rangle$ and the outputs $\{\hat{a'}_{R_m}^{(1)}, \hat{a'}_{I_m}^{(1)}\}$ according to Eqs. (8)-(9). We mix the mode $\hat{a'}_{R_m}^{(1)}$ with $\hat{a}_{R_m,2}^{(1)}$, obtaining

$$\begin{aligned}
\hat{a}_E^{(1)} &= \sqrt{\tau}\,\hat{a}_{R_m,2}^{(1)} + \sqrt{1-\tau}\,\hat{a'}_{R_m}^{(1)}, \\
\hat{a}_R^{(1)} &= \sqrt{\tau}\,\hat{a'}_{R_m}^{(1)} - \sqrt{1-\tau}\,\hat{a}_{R_m,2}^{(1)}.
\end{aligned}$$

We iterate this process K times, by sending as input of the SFG the modes $\hat{a}_{R_m,1}^{(k)} = \sqrt{\tau}\,\hat{a}_{R_m}^{(k-1)} + \sqrt{1-\tau}\,\hat{v}_m^{(k)}$ and

[5] It has been approximated in the $\eta \ll 1, N_S \ll 1, N_Z \gg 1$ limits.

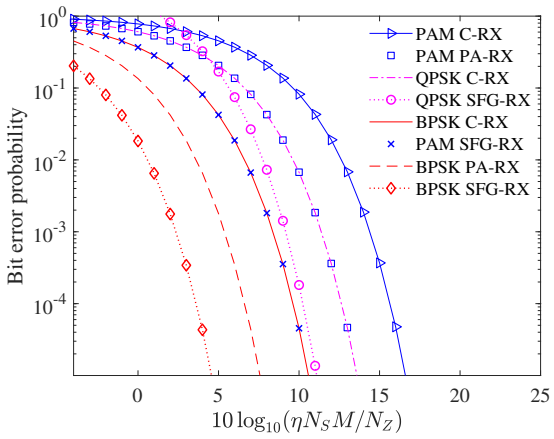

Fig. 2. Bit error probability for PAM, BPSK and QPSK for Heterodyne-RX in (4), PA-RX in (7) and SFG-RX in (9a)-(9c) as a function of $\eta N_s M/N_Z$.

$\hat{a}_{I_m}^{(k)} = \hat{a'}_{I_m}^{(k-1)}$. This generates, as output, the $\hat{b}^{(k)}$ modes in a coherent state $|\sqrt{\tau M}C(0)[1-\tau(1+N_Z)]^k\rangle$ embedded in a thermal environment with $N_S N_Z \ll 1$ average number of photons, and the $\hat{a}_E^{(k)}$ modes in an thermal state with mean number of photons $n_E^{(k)} = n_b^{(k)} = \tau M|C(0)|^2[1-\tau(1+N_Z)]^{2k}$. The number of cycles K is chosen such that $\sum_{k=1}^{K} n_b^{(k)} / \sum_{k=1}^{\infty} n_b^{(k)} = 1-\varepsilon$, for some $\varepsilon \ll 1$.[6] As the mean number of photons $n_E^{(k)}$ and $n_b^{(k)}$ are both zero for $C(0) = 0$, one can test the different hypothesis by simply applying a two-mode squeezing operation (TMSO) before the SFG circuit. The latter allows to displace to zero the phase-sensitive correlations of one of the hypothesis.[7] We discuss the performance in the different QBC schemes in the $N_Z \gg 1$, $N_S \ll 1$, $\tau N_Z \ll 1$, $\varepsilon \ll 1$ limit.

a) PAM: The SFG-RX achieves a 6 dB gain in the EPE with respect the classical BC. We can simply apply a TMSO before the SFG, in order to have $n_E^{(k)} = n_b^{(k)} = 0$ for the hypothesis $(\sqrt{\eta_1}, 0)$. One can simply measure the total number of photons $\sum_{k=1}^{K}(\hat{n}_b^{(k)} + \hat{n}_E^{(k)})$ and declare the aforementioned hypothesis if no photons are counted, obtaining the EP bound in (9a).

b) BPSK: The same can be done here, by applying a TMSO before the SFG, in order to have $n_E^{(k)} = n_b^{(k)} = 0$ for the hypothesis $(\sqrt{\eta}, \pi)$. Then, we proceed like in the PAM case, achieving an EP given in (9b), which corresponds to a 6 dB gain in the SNR with respect the classical case.

c) QPSK: The task is equivalent to discriminate between the coherent states $|e^{i\phi}\sqrt{\sum_{k=1}^{K}(n_b^{(k)} + n_E^{(k)})}\rangle$, with $\phi \in \{0, \pi/2, \pi, 3\pi/2\}$, where the TMSOs have the role of the displacements. This can be done following Bayesian strategies, like in the Dolinar-RX [24]. In alternative, we can simply test the different hypothesis by applying TMSOs, and discarding them as soon as one photon is detected [25], achieving the same 3 dB gain in the SNR as in the Dolinar-RX, see in (9c). This is in contrast with the PA-RX, which does not provide any gain in this case.

$$P_{\text{err}}^{\text{PAM}} \leq e^{-d_{\text{PAM}}^2 N_S M/N_Z}, \tag{9a}$$

$$P_{\text{err}}^{\text{BPSK}} \leq e^{-4\sum_{k=1}^{K}(n_b^{(k)}+n_E^{(k)})} \simeq e^{-d_{\text{BPSK}}^2 N_S M/N_Z}, \tag{9b}$$

$$P_{\text{err}}^{\text{QPSK}} \leq 4e^{-\sum_{k=1}^{K}(n_b^{(k)}+n_E^{(k)})} \simeq 4e^{-d_{\text{QPSK}}^2 N_S M/2N_Z}. \tag{9c}$$

Figure 2 illustrates the bit error probability (or interchangeably bit error rate) performance of Heterodyne, PA and SFG RXs for PAM, BPSK and QPSK modulations. In PAM, we have assumed that $\eta_2 = \eta$ and $\eta_1 = 0$ corresponding to on-off-keying (OOK). The plots verify the results addressed in our analysis. For PAM and BPSK, the PA-RX and SGF-RX provide a 3 dB and a 6 dB EPE gain over the classical RX, respectively. For QPSK, only the SGF-RX provides a 3 dB EPE gain over the classical RX.

IV. QI-SECURED BACKSCATTER COMMUNICATION

This section discusses the possibility of using QI to enhance the secure backscatter communication.

The use of QI can provide a factor 4 gain in the error exponent for the communication link (referred to as Bob-Alice) between the backscatter device Bob and the transceiver Alice compared to the link (referred to as Bob-Eve) between Bob and the eavesdropping RX Eve. This is because the QI is not available on the Bob-Eve link. In order for Eve to compensate this, Eve would need to use higher-gain antennas than that which Alice uses or be closer to Bob. Further, in order to increase the security that is to make the life of active eavesdropper more complicated, Alice can apply random phase shift to both the signal and idler paths. In case of BPSK, Eve would need to estimate this random phase shift before decoding the message from Bob such that the security of Bob-Alice link is enhanced.

The system is vulnerable to active Eavesdropping attack where Eve illuminates Bob's antenna with its own signal. Eve's signal will cause interference at Alice's RX and can be detected. Adding a power detector to Bob would also be utilized to detect Eve, but in practice this would mean that a fraction of the power impinging at it's antenna would need to be fed to the detector thus reducing σ_Q (and thus η). For instance, $50-50$ power divider at Bob's antenna would reduce the error exponent by factor 2 so that in case of PA-RX would negate the gain achieved by using QI.

V. CONCLUSIONS

We proposed to use the quantum radar technology to enhance the performance of backscatter communication systems. Especially, we the use of quantum illumination to enhance the system performance. The proposed QBC concept was verified to be within the reach of engineering applications such that in the PAM and BPSK cases, the quantum setting allows for a 6 dB advantage in the error probability exponent while

[6] As a further technical remark, in the Chernoff bound regime we have $M|C(0)|^2 \gg 1$. Therefore, in order to apply the qubit approximation, we need to divide the M signal-idler pair of modes in $M/\tilde{K}$ subsets, such that $\tilde{K}|C(0)|^2 \ll 1$, and apply the RX to the $\tilde{K}$ pair of modes at a time [11].

[7] [11] applies also two TMSO after the SFG circuit. This allows to have in every cycle $n_E^{(k)} = n_b^{(k)}$, and both $n_E^{(k)}$ and $n_b^{(k)}$ homogeneous functions of the phase-sensitive correlations of the hypothesis that we are testing.

in the QPSK scheme a 3 dB gain can be achieved using the SFG-RX. Finally, we would like to notice that in any scheme involving only phase modulation, as in the BPSK and QPSK protocols, the quantum setting allows for secure communication by means of quantum cryptography in a way similar to optical systems [16].

REFERENCES

[1] H. Stockman, "Communication by means of reflected power," *Proc. IRE*, vol. 36, no. 10, pp. 1196–1204, Oct. 1948.

[2] E. H. Allen and M. Karageorgis, "Radar system and methods using entangled quantum particles," US Patent 7,375,802 B2, May, 2008.

[3] S. Lloyd, "Enhanced sensitivity of photodetection via quantum illumination," *Science*, vol. 321, no. 5895, pp. 1463–1465, 2008.

[4] 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.*, vol. 101, p. 253601, 2008.

[5] G. De Palma and J. Borregaard, "The ultimate precision of quantum illumination," *arXiv preprint arXiv:1802.02158*, 2018.

[6] S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola, "Microwave quantum illumination," *Phys. Rev. Lett.*, vol. 114, no. 8, p. 080503, 2015.

[7] K. Liu, H. Xiao, H. Fan, and Q. Fu, "Analysis of quantum radar cross section and its influence on target detection performance," *IEEE Photon. Technol. Lett.*, vol. 26, no. 11, pp. 1146–1149, 2014.

[8] S. Guha, "Receiver design to harness quantum illumination advantage," in *Proc. IEEE Int. Symp. Inf. Theory*, 2009, pp. 963–967.

[9] M. Sanz, U. Las Heras, J. J. García-Ripoll, E. Solano, and R. Di Candia, "Quantum estimation methods for quantum illumination," *Phys. Rev. Lett.*, vol. 118, p. 070803, Feb. 2017.

[10] G. Pan, R. Xiao, and L. Zhou, "Entanglement of coupled optomechanical systems improved by optical parametric amplifiers," *Internat J. Theoret. Phys.*, vol. 55, no. 8, pp. 3697–3705, Aug. 2016.

[11] Q. Zhuang, Z. Zhang, and J. H. Shapiro, "Optimum mixed-state discrimination for noisy entanglement-enhanced sensing," *Phys. Rev. Lett.*, vol. 118, p. 040801, Jan. 2017.

[12] R. Boyd, *Nonlinear Optics*. New York, NY, USA: Academic Press, 2008.

[13] Q. Zhuang, Z. Zhang, and J. H. Shapiro, "Quantum illumination for enhanced detection of Rayleigh-fading targets," *Physical Review A*, vol. 96, no. 2, p. 020302, 2017.

[14] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, no. 8, p. 595, 2014.

[15] P. Botsinis, Z. Babar, D. Alanis, D. Chandra, H. Nguyen, S. X. Ng, and L. Hanzo, "Quantum error correction protects quantum search algorithms against decoherence," *Scientific reports*, vol. 6, p. 38095, 2016.

[16] J. H. Shapiro, Z. Zhang, and F. N. C. Wong, "Secure communication via quantum illumination," *Quantum Information Processing*, vol. 13, no. 10, pp. 2171–2193, Oct. 2014.

[17] P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design," *IEEE access*, vol. 1, pp. 94–122, 2013.

[18] P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, "Quantum-aided multi-user transmission in non-orthogonal multiple access systems," *IEEE Access*, vol. 4, pp. 7402–7424, 2016.

[19] Z. Z. Li, G. Xu, X. B. Chen, X. Sun, and Y. X. Yang, "Multi-user quantum wireless network communication based on multi-qubit GHZ state," *IEEE Commun. Lett.*, vol. 20, no. 12, Dec. 2016.

[20] R. Jäntti, R. Di Candia, R. Duan, and K. Ruttik, "Multiantenna quantum backscatter communications," in *2017 IEEE Globecom Workshops (GC Wkshps)*, Dec. 2017, pp. 1–6.

[21] Z. Zhang, S. Mouradian, F. N. Wong, and J. H. Shapiro, "Entanglement-enhanced sensing in a lossy and noisy environment," *Phys. Rev. Lett.*, vol. 114, no. 11, p. 110506, 2015.

[22] C. W. Helstrom, *Quantum Detection and Estimation Theory*. New York, NY, USA: Academic Press, 1976.

[23] K. M. R. Audenaert, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, L. Masanes, A. Acin, and V. F., "Discriminating states: The quantum Chernoff bound," *Phys. Rev. Lett.*, vol. 98, p. 160501, 2007.

[24] S. J. Dolinar, "An optimum receiver for the binary coherent state quantum channel," *Res. Lab. Electron. MIT Quarterly Progress Rep.*, vol. 111, pp. 115–120, 1973.

[25] S. J. van Enk, "Unambiguous state discrimination of coherent states with linear optics: Application to quantum cryptography," *Phys. Rev. A*, vol. 66, p. 042313, 2002.