applied sciences

MDPI

Article

Discrete-Modulation Continuous-Variable Quantum Key Distribution with Probabilistic Amplitude Shaping over a Linear Quantum Channel

Emanuele Parente [1,*], Michele N. Notarnicola [2], Stefano Olivares [3,4], Enrico Forestieri [1,5], Luca Potì [5] and Marco Secondini [1,5]

[1] Telecommunications, Computer Engineering, and Photonics (TeCIP) Institute, Scuola Superiore Sant'Anna, 56127 Pisa, Italy; enrico.forestieri@santannapisa.it (E.F.); marco.secondini@santannapisa.it (M.S.)
[2] Department of Optics, Palacký University, 779 00 Olomouc, Czech Republic; michelenicola.notarnicola@upol.cz
[3] Dipartimento di Fisica "Aldo Pontremoli", Università degli Studi di Milano, 20133 Milano, Italy; stefano.olivares@mi.infn.it
[4] Sezione di Milano, Istituto Nazionale di Fisica Nucleare, 20133 Milano, Italy
[5] National Laboratory of Photonic Networks, Consorzio Nazionale Interuniversitario per le Telecomunicazioni, 56124 Pisa, Italy; luca.poti@cnit.it
* Correspondence: emanuele.parente@santannapisa.it

Abstract

We propose a discrete-modulation continuous-variable quantum key distribution protocol based on coherent-state quadrature amplitude modulation combined with probabilistic amplitude shaping. Designed to overcome the practical limitations of Gaussian modulation schemes, the proposed protocol employs finite-energy shaped constellations and enables efficient implementation using standard telecom components while retaining compatibility with homodyne detection and reverse reconciliation. Assuming a linear quantum channel model, characterized by a linear input–output relation between quadratures, and considering collective attacks in the asymptotic regime, we evaluate the secret key rate, achievable transmission distance, optimal launch power, and excess noise tolerance for different constellation sizes, comparing the results with those of the benchmark GG02 protocol. Our results show that probabilistic shaping significantly enhances the performance of discrete-modulation schemes, allowing high-order constellations to closely approach the performance of GG02 in terms of secret key rate, transmission distance, optimal launch power, and excess noise tolerance while preserving practical implementability. By leveraging mature coherent optical communication technologies, the proposed approach provides a realistic pathway toward experimentally feasible high-rate continuous-variable quantum key distribution systems.

Keywords: continuous-variable quantum key distribution; unconditional security; quadrature amplitude modulation; probabilistic amplitude shaping; linear quantum channel

Academic Editor: Petros Nicopolitidis

Received: 21 May 2026
Revised: 24 June 2026
Accepted: 30 June 2026
Published: 3 July 2026

1. Introduction

Quantum key distribution (QKD) is the most prominent application of quantum cryptography and ensures the generation of a one-time pad secure key between two authenticated remote parties, Alice and Bob, despite the presence of a powerful adversary, Eve [1]. The importance of QKD over classical cryptography lies in its ability to offer

unconditional security, where no assumptions are made about the power of the adversary and whose strength is based only on the laws of quantum mechanics [2].

QKD protocols come in the equivalent entanglement-based (EB) or prepare-and-measure (PM) versions: in both cases a quantum channel along which the exchange of optical signals occurs and an authenticated classical channel for the reconciliation stage are required. Eve has the power to tamper the communication over the quantum channel and to only listen to the conversation over the classical one [3]. In particular, the latter needs to be authenticated so that the legitimate parties are sure they are actually talking to each other; this can be achieved by means of information-theoretically secure classical algorithms, so that the overall security of the protocol is not reduced [4]. The classical channel is considered error-free, so that all communication errors found during the post-processing stage are uniquely attributed to Eve's interference along the quantum channel. By exploiting quantum features such as non-orthogonality or entanglement, in fact, the exchanged quantum states cannot be discriminated without disturbing the system, nor can they be perfectly copied as a consequence of the no-cloning theorem [5,6]. In this way, Alice and Bob are not only able to detect the presence of an attacker, but are even able to estimate the amount of information an eavesdropper has acquired about the key, so that, whenever Eve's interference exceeds a certain threshold, the protocol can be aborted. Since only the key is transmitted during the entire process, no information leakage occurs in this circumstance [7,8].

Due to its low interaction with matter and its longer decoherence time, light is the most common and practical choice to transmit information in QKD realm. The distinction of two families of QKD protocols, i.e., discrete-variable (DV-QKD) and continuous-variable (CV-QKD) ones, reflects the possibility to encode information about the key into different degrees of freedom of light: the polarization (or time bin) of single photons (or weak coherent states) in the former case and the orthogonal quadratures of an optical field in the latter. Subsequently to the signal exchange, Alice and Bob get a raw key that they refine after several post-processing steps, during which they exchange classical side information to eventually agree on a secure common key [9].

Different aspects concur to assess the performance of a generic QKD protocol, i.e., the achievable distances, the rate at which the secure key is generated, the feasibility of its realization—including the costs of the employed devices—and the security level it provides [10]. Among the two classes mentioned above, CV-QKD protocols have shown rapid growth nowadays [11], primarily because they are able to circumvent the technological challenges of single-photon sources and detectors required for DV-QKD [12]. Specifically, CV-QKD protocols are well-suited for use with fiber-optic systems (showing high performance in metropolitan areas) and exploit coherent detection, namely homodyne or heterodyne (also referred to as phase diversity or double homodyne) detection, which offers the advantages of higher detection efficiency, higher secret key rate (SKR) at short distances, low implementation costs, and greater compatibility with state-of-the-art telecom equipment (they are easily integrable with photonic chips). Moreover, techniques such as wavelength division multiplexing can be implemented at room temperature using standard hardware [13–16].

The most well-known protocol in this category, currently used as a benchmark in CV-QKD, is GG02, introduced by Grosshans and Grangier in 2002 [17], which involves exploiting coherent states with random amplitude drawn from a Gaussian distribution that are sent through a noisy untrusted channel. The choice of Gaussian modulation (GM) is suggested as it achieves the Shannon capacity of a Gaussian channel between Alice and Bob, in the presence of coherent detection at the receiver [5,18]. Although the use of GM simplifies security proofs [1,13,19] it entails several practical difficulties: handling a

continuous modulation requires an infinite resolution of the digital-to-analog converter (DAC) at the transmitter and of the analog-to-digital converter (ADC) at the receiver, in addition to the requirement of an infinite extinction ratio of the modulator and an extreme computational burden for the random number source on the transmitter side. Furthermore, signal modulation with infinite peak power is theoretically required to generate a Gaussian distribution, which indeed has infinite support in phase space [12,20,21]. Then, the resulting lack of an efficient error-correction procedure at both high and low signal-to-noise ratio (SNR) limits the range and feasibility of this protocol [16].

A practical alternative to GM is offered by discrete-modulation formats, which are commonly used in digital communications and can be implemented using simple modulation schemes and readily available optical components [22]. An interesting choice is quadrature amplitude modulation (QAM), whose constellation points in phase space are arranged on a square lattice with finite support. This structure enables practical implementation using a finite-power laser and a nested Mach–Zehnder modulator [23]. QAM is widely employed in optical communications, as it offers high spectral efficiency with reasonable implementation complexity [24]. Its performance can be further enhanced by combining it with probabilistic amplitude shaping (PAS), where transmitted symbols are selected from the constellation with probabilities that depend on their energy, with the goal of maximizing the bit rate for a given mean energy per symbol [25]. Key advantages of PAS-QAM include its fine rate granularity and its ability to operate near Shannon capacity over the additive white Gaussian noise (AWGN) channel across a wide range of SNRs, using only standard binary error-correction codes and bit-wise soft decoders within a pragmatic bit-interleaved coded modulation (BICM) framework [26]. Owing to these properties and its simplicity, PAS-QAM has become a widely adopted modulation scheme for high-capacity fiber-optic communication systems [27–29].

Incorporating the advantages of PAS-QAM into a practical CV-QKD setup would represent a significant step toward the large-scale development of QKD systems based on mature technologies already deployed in current optical networks [30,31]. For instance, the feasibility of using binary codes and bit-wise soft decoders to implement an efficient reverse reconciliation protocol for CV-QKD with QAM modulation was recently demonstrated in [32]. However, such a change in the protocol should be supported by an accurate security analysis. In general, the security is closely linked to implementation-related vulnerabilities arising from deviations between theoretical models and practical realizations, which may open security loopholes for an adversary [33], leading to attacks such as wavelength attacks [34] and quantum hacking of homodyne detection [35]. Another fundamental challenge in establishing the security of CV-QKD protocols stems from the infinite-dimensional nature of the underlying Hilbert space, which prevents a complete state tomography; as a result, an exact characterization of the quantum state shared by Alice and Bob is not possible [1]. In fact, even though the individual pulses are Gaussian states, the average quantum state is non-Gaussian, so that the covariance matrix estimation performed during the channel evaluation stage is not sufficient to fully characterize it. However, in 2006 Navascues et al. [36] derived a lower bound on the SKR obtained by considering the Gaussian state associated with the same covariance matrix of the actual non-Gaussian state shared by Alice and Bob, providing a well-suited security framework for very large QAM constellations. Tighter bounds, also required for the investigation of a more realistic scenario of non-asymptotic key length exchange, can be found using convex optimization problems and, more precisely, semidefinite programming (SDP); however, these methods are numerically intensive and unsuitable for large-constellation-size cases [37,38]. Recently, Denys et al. [39] addressed this problem and introduced an explicit numerical bound for the asymptotic secret key rate computation of a coherent-state CV-

QKD protocol over an arbitrary quantum channel: their approach exploits a combination of Gaussian optimality arguments and semidefinite programming, and their results yield an explicit bound that is tight for QAM constellations with 64 or more symbols.

In this work, we propose a QAM-based CV-QKD protocol implemented over a linear quantum channel that competently models transmission through common optical fibers, and study the achievable rates, achievable distances and maximum tolerable noise in the case of collective attacks, reverse reconciliation schemes, infinite key sizes, and homodyne detection, and in the distance range 0.5–300 km. Within the established asymptotic security framework based on collective attacks and Gaussian optimality arguments, we apply probabilistic amplitude shaping (PAS-) to QAM-based CV-QKD systems and optimize the shaping parameter for different constellation sizes, comparing the resulting performance with that of uniform (U-) QAM and the GG02 benchmark protocol. We then compare the SKR obtained under this scheme with the wiretap channel model outlined in [40], where Eve is assumed to implement a beam-splitting attack, and highlight the advantages, in terms of performance, adduced by the use of the PAS technique in a CV-QKD protocol with QAM modulation and coherent states.

2. Materials and Methods

2.1. Proposed Protocol

With reference to Figure 1, we now describe the PM version of our discrete-modulated (DM) protocol and consider the asymptotic limit at which an infinite number of symbols is transmitted.

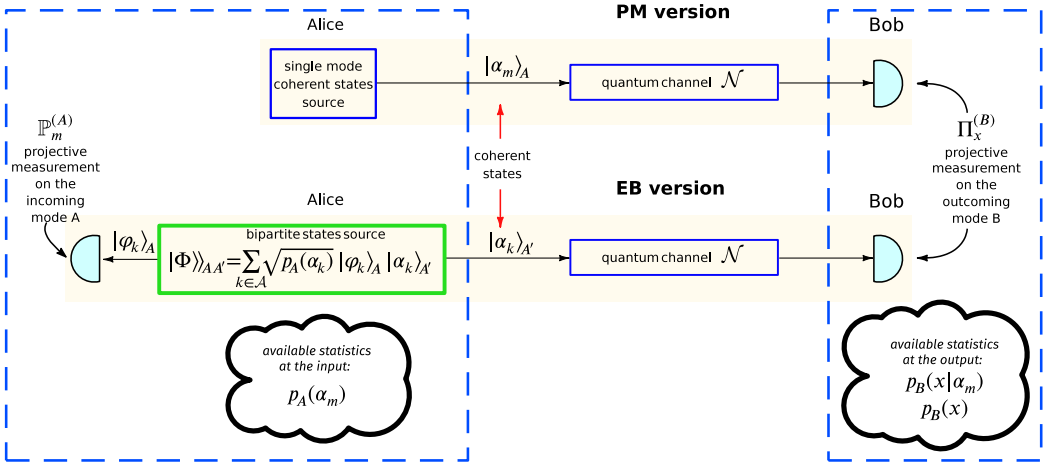

Figure 1. Prepare-and-measure version (**top**) and entanglement-based version (**bottom**) of our discrete-modulated protocol.

Alice (A) encodes a pair of classical variables (x_A, y_A) in a set of displaced single-mode coherent states $|x_A + iy_A\rangle$, where $x_A, y_A \in \mathbb{R}$ are generated according to a discrete-valued probability distribution. Then, Alice sends these states to Bob (B) through a quantum channel under control of Eve (E). On the receiver side, Bob performs quantum homodyne detection, measuring at random one of the two orthogonal quadratures q or p, which satisfy the commutation relation $[q, p] = 2i\sigma_0^2$, where σ_0^2 is the shot-noise variance; here we adopt shot-noise units (SNUs), that is, we set $\sigma_0^2 = 1$. The information about the measured quadrature is subsequently revealed during the classical post-processing stage. This sifting step only identifies which quadrature was measured for each transmitted coherent state and does not involve discarding any homodyne outcomes. Due to the symmetry of the constellation, the statistics associated with the q and p quadratures are equivalent. Therefore, without loss of generality, we restrict the security analysis and

SKR evaluation to the case where Bob measures the quadrature q. In the following, Bob's measurement is described by the projector $\Pi_x^B = |x\rangle\langle x|$, which is a Gaussian measurement experimentally implemented through homodyne detection.

In this work, we are interested in the transmission of signals via a fiber-optic link; this medium is characterized by the transmittance parameter T, which reflects the amount of losses caused by random scattering of the light passing through it and which depends exponentially on the length d of the communication link according to $T = 10^{-\eta d/10}$, where $\eta = 0.2\,\mathrm{dB/km}$ is the attenuation coefficient at the optical wavelength of 1550 nm [3]. Beyond losses, the noise also affects the reliability of communication, and its impact is quantified by the excess noise parameter ξ. In our analysis, we assume that the quantum signal transmission and detection may be affected by the presence of noise, and that the quantum channel is linear. A linear quantum channel represents a class of channels that also includes the category of Gaussian channels [1,5]. In fact, this channel is characterized by the input–output relations for the quadrature operators in the Heisenberg picture [11]:

$$q_B = \sqrt{T}\, q_{A'} + q_b \quad \text{and} \quad p_B = \sqrt{T}\, p_{A'} + p_b, \tag{1}$$

where q_b and p_b represent the quadrature operators of some additional noise modes, assumed to be uncorrelated with the input quadratures $q_{A'}$ and $p_{A'}$ (the input signal) and characterized by the first two order moments

$$\begin{cases} \langle q_b \rangle = \langle p_b \rangle = 0\,, \\ \langle q_b^2 \rangle = \langle p_b^2 \rangle = 1 - T + \xi T\,. \end{cases} \tag{2}$$

After the signal exchange, Alice and Bob perform a post-processing stage in which they share some side information through a classical authenticated channel to agree on a secret common key. Specifically, they first perform a parameter estimation operation, where they estimate both the experimental parameters T and ξ describing the channel and the amount of information Eve may have acquired so far; then, a reconciliation step for error correction—which can be either direct (DR) or reverse (RR), depending on whether the information on the key bits is shared by Alice or Bob respectively—and, finally, a privacy amplification process where they extract from the raw key a shorter secret key, eliminating any possible information gained by the eavesdropper [9,10]. Here we adopt a RR scheme, which is more advantageous, since it overcomes the 3 dB limit problem of the DR scheme [4,10,13].

Finally, to ensure a higher level of security to our protocol, we consider the untrusted-device scenario—where Eve has access to both the channel and Bob's apparatus—and the case of collective attacks, which are the most powerful in the asymptotic limit of an infinitely long key. In the collective attack picture, Eve performs an independent and identically distributed (i.i.d.) attack on all signals by making these interact with a set of separable ancilla states, stores each of these ancillae in a quantum memory and jointly measures them at the end of post-processing. In this way, Eve can take advantage of both signal transmissions and the public information Alice and Bob have shared along the classical channel during post-processing.

2.2. Alice's Modulation

During the modulation stage, Alice generates pairs of quadrature values (x_A, y_A) representing the coordinates of a uniform square M-ary QAM constellation in classical phase space. Each quadrature component is selected from the one-dimensional alphabet $\Lambda = \{n\Delta \mid n = -(N-1)/2, \ldots, (N-1)/2\}$ that contains $N = 2^k$ points, with $k \in \mathbb{N}$ and $\Delta \in \mathbb{R}$, the latter being called the scaling factor or the symbol spacing. The two-

dimensional QAM constellation is then defined as $\mathcal{A} = \Lambda \times \Lambda$ and therefore contains $M = N^2$ constellation points. Thereafter, Alice maps the $M = N^2$ constellation points of $\mathcal{A}$ in quantum phase space [41] by encoding each couple (x_A, y_A) into the corresponding coherent state $|x_A + iy_A\rangle$. In particular, the distance between neighbouring points in the classical phase space is equal to Δ; in turn, as a consequence of the expectation values of the quadrature operators over a generic coherent state $|\alpha\rangle$ [13]

$$\langle q \rangle_\alpha = 2\sigma_0 Re(\alpha) \qquad \text{and} \qquad \langle p \rangle_\alpha = 2\sigma_0 Im(\alpha), \tag{3}$$

we find that, in quantum phase space, the QAM symbols are still arranged in a square lattice, but they appear centered at $(2\sigma_0 x_A\,, 2\sigma_0 y_A)$ and spaced by $2\sigma_0\Delta$ (see Figure 2).

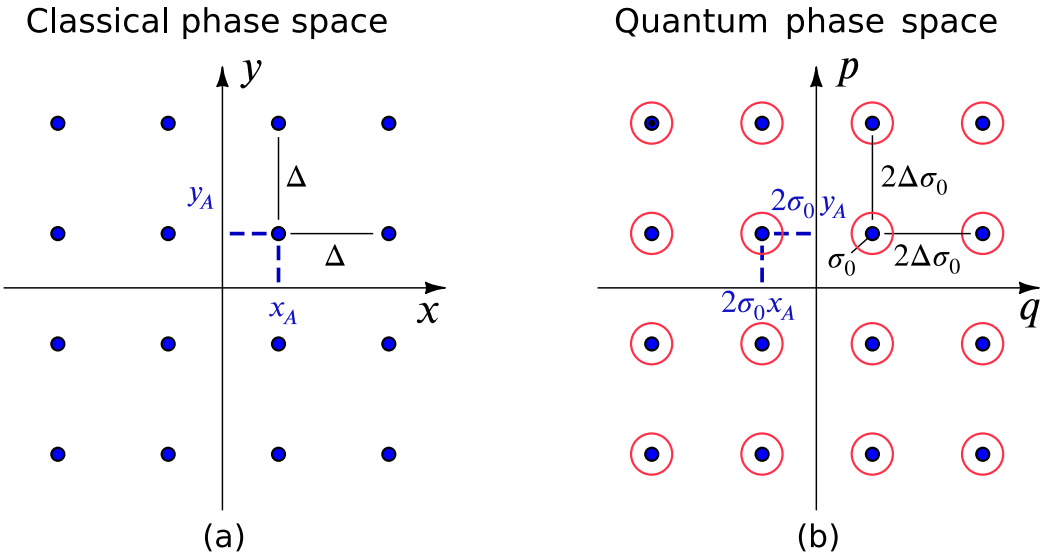

Figure 2. 16QAM constellation in (**a**) classical and (**b**) quantum phase space; the symbols are spaced by Δ and centered at (x_A, y_A) in the former case, and spaced by 2Δ and placed in $(2\sigma_0 x_A, 2\sigma_0 y_A)$ in the latter.

The value of Δ is related to the average energy of the constellation, here expressed in terms of the average number of photons

$$\bar{n} = \sum_{\mathbf{z} \in \mathcal{A}} p_A(\mathbf{z})\ ||\mathbf{z}||^2, \tag{4}$$

where $p_A(\mathbf{z})$ is the input mass probability governing the extraction of the quadrature component $\mathbf{z} = (x_A, y_A) \in \mathcal{A}$. One trivial choice for $p_A(\mathbf{z})$ is the uniform distribution; further, compared to other modulation formats that still require coherent detection such as phase shift keying (PSK), QAM-based systems can be enriched by the use of the PAS technique. The combination of QAM and PAS offers a way to improve the bit rate of the communication with fixed launch power. In particular, using the maximum entropy principle [42] or variational calculus [43] one can find that Maxwell–Boltzmann (MB) distribution is the one that maximizes the Shannon entropy for a fixed average energy of a discrete constellation (and hence for a certain power usage), being able to provide the ultimate shaping gain of 1.53 dB [44]. The MB distribution can be written as

$$\mathcal{M}_\beta(\mathbf{z}) = \frac{e^{-\beta\,||\mathbf{z}||^2}}{\sum_{\mathbf{z}} e^{-\beta\,||\mathbf{z}||^2}}\quad , \tag{5}$$

where β is a shaping parameter: when $\beta \to 0$ we get a uniform distribution, while for $\beta \gg 1$, a general M-QAM reduces to a QPSK format, since the extraction of the outer points of the constellation is ruled out [25].

In this work we compare the performance of our protocol considering both uniform and non-uniform signaling (that is, PAS using the MB distribution) of quantum states. In the uniform case, i.e., $p_A(\mathbf{z}) = 1/M$, the constellation is characterized by a single parameter, the spacing Δ between the symbols, which is completely specified by the choice of the average number of photons $\bar{n}$: given the latter, Δ can be easily found by inverting (4). Instead, when the a priori probabilities follow the MB distribution (5), the modulation is characterized by two parameters, the spacing Δ and the shaping parameter β. These two degrees of freedom are constrained by the desired average number of photons $\bar{n}$: for any fixed β, the corresponding value of Δ can be obtained via (4). The optimal value of β is then determined by maximizing the SKR (see next Section 2.3), according to the numerical procedure described in [26].

2.3. Secret Key Rate Calculation

The asymptotic SKR is a fundamental metric to assess the performance and security of a CV-QKD protocol. Although the assumption of an infinitely long signal exchange is not realistic, it provides an upper bound on the achievable SKR and simplifies the theoretical security analysis [21].

For collective attacks with the RR scheme, the SKR is bounded from below by the Devetak–Winter formula [9]

$$SKR \geq \zeta I_{AB} - \chi_{BE}, \tag{6}$$

where I_{AB} is the mutual information shared by Alice and Bob, χ_{BE} is the Holevo information (HI) between Bob and Eve, and $\zeta \in [0, 1]$ is the reconciliation efficiency. In particular, this parameter takes into account an imperfect error correction performed by Alice and Bob and then limits the classical amount of information that they can extract. In this regard, modern information reconciliation techniques for CV-QKD, including multilevel coding with multistage decoding [45] and multidimensional (MD) reconciliation based on multi-edge LDPC codes [46], can achieve reconciliation efficiencies close to unity. Recent reviews of CV-QKD systems confirm that reconciliation efficiencies around 95% are routinely considered achievable with state-of-the-art error-correction schemes [11,33]. Therefore, throughout this work, we adopt the realistic value $\zeta = 0.95$. On the other hand, the HI term is not affected by ζ since Eve's power is assumed not to be limited by current technology [16].

2.3.1. Mutual Information

The mutual information I_{AB} measures the average information content exchanged between Alice and Bob [2]. In order to compute this term, we consider the PM scheme described in Section 2.1. For each use of the channel, Alice prepares the coherent state $|x_A + iy_A\rangle$ and sends it through the quantum channel; at the output, according to our convention, Bob measures the quadrature q and obtains the outcome x_B. Given the linearity of the channel, equivalent to an AWGN picture, the random variables are described by the general input–output relation $x_B = 2\sigma_0\sqrt{T}x_A + n$, where the noise n is normally distributed $\mathcal{N}(0, \sigma^2_\xi)$; in our case, x_A, n and hence x_B are real numbers. For a generic M-ary modulation alphabet, the mutual information can then be expressed as [47]

$$I_{AB} = \sum_{x_A} \int dx_B \; p_A(x_A) p_{B|A}(x_B|x_A) \log_2 \frac{p_{B|A}(x_B|x_A)}{\sum_{x'_A} p_A(x'_A) p_{B|A}(x_B|x'_A)}, \tag{7}$$

where $p_A(x_A)$ is the a priori probability of the classical symbol x_A and $p_{B|A}(x_B|x_A)$ is the transition probability relating the input and the output of the AWGN channel

$$p_{B|A}(x_B|x_A) = \frac{1}{\sqrt{2\pi\sigma_\xi^2}} \exp\left(-\frac{(x_B - 2\sigma_0\sqrt{T}x_A)^2}{2\sigma_\xi^2}\right), \tag{8}$$

where the value of the variance $\sigma_\xi^2 = \sigma_0^2(1 + T\xi)$ in (8) quantifies the impact of noise on the signal received at the channel output.

2.3.2. Holevo Information

The Holevo information term χ_{BE} quantifies the maximum amount of information about Bob's measurement outcomes that Eve can obtain in the reverse reconciliation scenario [11]. An accurate determination of this quantity is essential for the security analysis of our CV-QKD protocol.

To facilitate the analysis, we exploit the equivalence between the PM and EB descriptions of QKD protocols [13], and focus on the latter, which offers a more tractable theoretical framework. If in the PM scheme Alice prepares the coherent states $\{|\alpha_k\rangle, p_A(\alpha_k)\}$, where $k = (x_A, y_A) \in \mathcal{A}$ and $\mathcal{A}$ represents the alphabet of our QAM constellation, with the latter described by the density operator $\rho = \sum_k p_A(\alpha_k)|\alpha_k\rangle\langle\alpha_k|$, in the EB scheme Alice actually produces a set of a bipartite entangled states $|\Phi\rangle\rangle_{AA'}$ in the two modes A and A' [38,48]

$$|\Phi\rangle\rangle_{AA'} = \sum_{k\in\mathcal{A}} \sqrt{p_A(\alpha_k)}\ |\varphi_k\rangle_A|\alpha_k\rangle_{A'}, \tag{9}$$

where $\{|\varphi_k\rangle_A\}_{k\in\mathcal{A}}$ forms an orthonormal basis in mode A on which Alice, in order to determine which state to send to Bob, performs a local measurement described by POVM $\{\Pi_k^A = |\varphi_k\rangle_A\langle\varphi_k|\}_{k\in\mathcal{A}}$. This causes the state $|\alpha_k\rangle_{A'}$ on the other mode A' to be projected onto a coherent state with the corresponding probability $p_A(\alpha_k)$.

Thereafter, she sends the state $|\alpha_k\rangle_{A'}$ to Bob over the quantum channel, the latter described by a completely positive (CP) quantum map $\mathcal{N}_{A'\to B}$; the bipartite state ρ_{AB} shared by Alice and Bob is then

$$\rho_{AB} = (\mathbb{I}_A \otimes \mathcal{N}_{A'\to B})[\ |\Phi\rangle\rangle_{AA'}\langle\langle\Phi|\ ], \tag{10}$$

where $\mathbb{I}_A$ is the identity channel acting on the states collected at Alice's side and $(\mathbb{I}_A \otimes \mathcal{N}_{A'\to B})$ is a completely positive trace-preserving (CPTP) map. The conditional state Bob receives after Alice's projective measurement is

$$\rho_{B|\alpha_k} = \frac{1}{p_A(\alpha_k)} \mathrm{Tr}_A\left[\rho_{AB}\ (\Pi_k^A \otimes \mathbb{I}_B)\right]. \tag{11}$$

If Alice has sent the state $|\alpha_k\rangle = |x_A + iy_A\rangle$, for Bob performing a homodyne detection and measuring the quadrature q with POVM $\Pi_x^B = |x\rangle\langle x|$, the conditional distribution of Bob's measurement outcome x_B is given by

$$p_{B|A}(x_B|x_A) = \mathrm{Tr}_A\left[\rho_{AB}\ |\varphi_k\rangle\langle\varphi_k|_A \otimes \Pi_x^B\right], \tag{12}$$

and the corresponding marginal distribution of Bob's outcome is

$$p_B(x_B) = \sum_m p_{B|A}(x_B|x_A)p_A(x_A). \tag{13}$$

Unfortunately, these available statistics—namely, $p_A(x_A)$, $p_{B|A}(x_B|x_A)$, and $p_B(x_B)$—are not sufficient for the proper parties to uniquely characterize the underlying untrusted quantum channel, and this lack of complete information plays in favor of Eve. In fact, the eavesdropper can exploit the non-uniqueness of the noisy maps $\mathcal{N}$ that yield the same input–output statistics by selecting and implementing the unitary dilation of the quantum channel that maximizes her accessible information while remaining consistent with the statistics observed by Alice and Bob, and hence without being noticed. For the purpose of unconditional security, we consider Eve to perform a purification attack; then, the Devetak–Winter formula can be re-written as [37]

$$\mathrm{SKR} = \zeta I_{AB} - \sup_{\mathcal{U}_{A' \to BE} \in S} \chi_{BE}, \tag{14}$$

where the supremum is taken over all isometric quantum channels controlled by Eve and belonging to the set S compatible with the channel statistics obtained by Alice and Bob during the parameter estimation phase of the PM version of the protocol. In the case of the purification attack here considered, Eve holds a tripartite isolated system ABE that is described by the pure state $|\psi\rangle_{ABE}$ and of which she controls the unitary dilation additional modes of the noisy CP map $\mathcal{N}$. The density matrices ρ_{AB} and ρ_E can be found from $|\psi\rangle_{ABE}$ by tracing the modes E and AB, respectively.

Now, the HI term corresponds to [9]

$$\chi_{BE} = S(E) - S(E|B), \tag{15}$$

where $S(E)$ is the von Neumann entropy of Eve's state ρ_E accessible to Eve for collective measurements, and $S(E|B)$ is the von Neumann entropy conditional to the same state after Bob's measurement (a homodyne projection in our case). However, in a purification attack scenario the state ρ_{AB} provides the same entropic calculations of ρ_E, i.e., $S(E) = S(AB)$ and $S(E|B) = S(A|B)$, so that

$$\chi_{BE} = S(E) - S(E|B) = S(AB) - S(A|B). \tag{16}$$

This implies that χ_{BE} can be directly computed from the bipartite state ρ_{AB} shared between Alice and Bob [1,9,13].

Given this consideration, we provide the security analysis by invoking the "optimality of Gaussian attacks" theorem [36,49,50], which bounds the HI in (16) as $\chi_{BE} < \chi_{BE}^{(\mathrm{G})}$, where $\chi_{BE}^{(\mathrm{G})}$ is the HI associated with the Gaussian state $\rho_{AB}^{(\mathrm{G})}$ with the same covariance matrix Γ_{AB} of ρ_{AB}. Up to local operations, Γ_{AB} is expressed as

$$\Gamma_{AB} = \begin{pmatrix} V\mathbb{I}_2 & Z\sigma_z \\ Z\sigma_z & W\mathbb{I}_2 \end{pmatrix} = \begin{pmatrix} \gamma_A & \gamma_C \\ \gamma_C & \gamma_B \end{pmatrix}, \tag{17}$$

where $\mathbb{I}_2 = \mathrm{diag}(1,1)$ is the identity matrix and $\sigma_z = \mathrm{diag}(1,-1)$ the Pauli matrix, V is the variance at Alice's side (of mode A) and W the one at Bob's side, and Z is the correlation term. At this point, the von Neumann entropy of the joint state $\rho_{AB}^{(\mathrm{G})}$ can be obtained as [37,41]

$$S(\rho_{AB}) = g\left(\frac{d_1 - 1}{2}\right) + g\left(\frac{d_2 - 1}{2}\right), \tag{18}$$

where $d_{1,2}$ are the symplectic eigenvalues of Γ_{AB} satisfying the constraint $d_{1,2} \geq 1$, namely

$$d_{1,2} = \sqrt{(\Delta \pm \sqrt{\Delta^2 - 4I_4})/2}, \tag{19}$$

and

$$g(x) = (x+1)\log_2(x+1) - x\log_2 x, \tag{20}$$

while $\Delta = I_1 + I_2 + 2I_3$, and

$$\begin{aligned} I_1 &= \det(\gamma_A), \quad I_2 = \det(\gamma_B), \\ I_3 &= \det(\gamma_C), \quad I_4 = \det(\Gamma_{AB}). \end{aligned} \tag{21}$$

The conditional entropy $S(\rho^{(G)}_{A|B})$, instead, can be computed as $S(\rho^{(G)}_{A|B}) = g(d_3)$ [48] with

$$d_3 = \det(\gamma_A - \gamma_C(\gamma_B + \gamma_M)^{-1}\gamma_C^T), \tag{22}$$

and γ_M is the 2×2 covariance matrix associated with homodyne detection [51]:

$$\gamma_M = \lim_{\lambda\to 0}\begin{pmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{pmatrix}. \tag{23}$$

In practical implementations of CV-QKD, while Alice's variance $V = 1 + 2\bar{n}$ is known by the modulation stage, Bob's variance W is determined via measurements (the transmittance and excess noise values are accessible after the parameter estimation stage), so the only unknown is the cross term Z, which needs nonlocal bipartite measurements to be directly evaluated [11].

In this regard, the hypothesis of a linear quantum channel solves the problem and provides an exact evaluation of Z and then of the covariance matrix under a purification attack. The linearity of the channel ensures that the covariance matrix Γ_{AB} of the state shared by Alice and Bob can be expressed as a function of the covariance matrix $\Gamma_{AA'}$ of the bipartite state $|\Phi\rangle\rangle_{AA'}$ generated by Alice, which reads

$$\Gamma_{AA'} = \begin{pmatrix} V\mathbb{I}_2 & Z_{AA'}\,\sigma_z \\ Z_{AA'}\,\sigma_z & V\mathbb{I}_2 \end{pmatrix}, \tag{24}$$

in which

$$Z_{AA'} = \frac{1}{2}\,{}_{AA'}\langle\langle\Phi|(q_A q_{A'} - p_A p_{A'})|\Phi\rangle\rangle_{AA'}. \tag{25}$$

In order to find Z, we use the Schmidt decomposition of the bipartite entangled state $|\Phi\rangle\rangle_{AA'}$ [39]:

$$|\Phi\rangle\rangle_{AA'} = \left((\rho_A^*)^{1/2} \otimes \mathbb{I}\right)|EPR\rangle\rangle_{AA'}\,, \tag{26}$$

with $|EPR\rangle\rangle = \sum_{n=0}^{\infty}|n_A\rangle|n_{A'}\rangle$, the two-mode squeezed vacuum state with infinite squeezing and $\{|n\rangle_A\}_{n=0}^{\infty}$, $\{|n\rangle_{A'}\}_{n=0}^{\infty}$, the Fock basis for the modes A and A'. Straightforward calculations lead to

$$\begin{aligned} Z_{AA'} &= \sum_{mn}\left\langle mm\right|[\rho_A^{1/2}\otimes\mathbb{I}_2](a_A a_{A'})[(\rho_A^*)^{1/2}\otimes\mathbb{I}_2]\left|nn\right\rangle + h.c. \\ &= \sum_{mn}\left\langle m\right|\rho_A^{1/2}a_A(\rho_A^*)^{1/2}\left|n\right\rangle\langle m|a_{A'}|n\rangle + h.c., \end{aligned} \tag{27}$$

where $\langle m|a_{A'}|n\rangle = \sqrt{n}\,\delta_{m,n-1}$ so that

$$\begin{aligned} Z_{AA'} &= \sqrt{n}\sum_{n}\left\langle n-1\right|\rho_A^{1/2}a_A(\rho_A^*)^{1/2}\left|n\right\rangle + h.c. \\ &= \left\langle n\right|a_A^\dagger\,\rho_A^{1/2}\,a_A\,(\rho_A^*)^{1/2}\left|n\right\rangle + h.c., \end{aligned} \tag{28}$$

and

$$Z_{AA'} = 2\,\mathrm{Tr}[\rho_A^{1/2}\, a\, \rho_A^{1/2}\, a^\dagger]. \tag{29}$$

Eventually, the covariance matrix reads [39]

$$\Gamma_{AB} = \begin{pmatrix} V\mathbb{I}_2 & \sqrt{T}\, Z_{AA'}\sigma_z \\ \sqrt{T}\, Z_{AA'}\sigma_z & TV_B\mathbb{I}_2 \end{pmatrix}, \tag{30}$$

where

$$V_B = V + \chi \quad , \quad \chi = \frac{1-T}{T} + \xi. \tag{31}$$

3. Results and Discussion

The performance of the proposed CV-QKD protocol, which employs QAM modulation combined with PAS, is evaluated by comparing it against two baselines: (i) QAM with uniform distribution, and (ii) the benchmark GG02 protocol, which uses GM. Specifically, we will analyze and compare the maximum achievable SKRs, the maximum transmission distances, and the maximum tolerable excess noise across these schemes. Moreover, for the same protocols, we will investigate the optimal launch power and the power range over which a positive SKR can be achieved, both expressed in terms of photons per symbol on Alice's side. It should be emphasized that, as already pointed out in Section 2.1, each channel use corresponds to the transmission of a single coherent state and yields one homodyne outcome, independently of the randomly selected quadrature. Hence, in contrast to standard DV-QKD protocols such as BB84, where basis mismatch leads to sifting losses, every channel use contributes one usable measurement result for key generation. Accordingly, the SKR and all derived figures of merit are expressed in bits per channel use, equivalently interpreted as bits per transmitted coherent state or per homodyne outcome, and no factor 1/2 associated with quadrature selection is required. We also note that the security analysis is carried out within an asymptotic collective-attack framework.

3.1. Maximum Achievable SKR

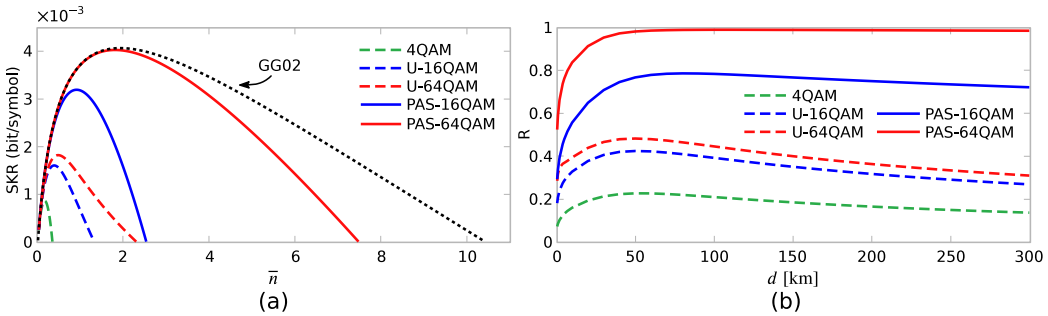

Figure 3. (**a**) SKR for GG02 and for 4QAM, 16QAM, 64QAM with uniform and non-uniform input signaling in terms of the number of photons on Alice's side at 100 km in the case of collective attacks, homodyne detection, reverse reconciliation and no excess noise; (**b**) corresponding values of R in the range 0.5–300 km.

We begin by addressing the noiseless scenario ($\xi = 0$). Figure 3 (left) shows the SKR as a function of the average number of photons $\bar{n}$ at Alice's side for GG02 and for 4, 16 and 64QAM with uniform (U) distribution or PAS, at a fixed distance of 100 km. As expected, different constellations yield different SKR performance. Firstly, 4QAM, equivalent to QPSK, achieves the lowest SKR peak at a very low $\bar{n}$, after which the SKR quickly decays to zero. The SKR peak and the support of the SKR curve in the photon number domain can be increased by increasing the cardinality of the constellation. However, with uniform

signaling the improvement is quite limited, with little gain achieved by U-64QAM over U-16QAM, and a large gap with respect to the SKR peak achievable by GG02; on the other hand, PAS provides a significant performance improvement and allows us to better exploit alphabets with higher cardinality. PAS-16QAM largely outperforms both U-16QAM and U-64QAM, and PAS-64QAM provides a further improvement, closing the gap with GG02.

It is particularly interesting to explore how the maximum SKR varies with the transmission distance and verify if the relative behavior of the various protocols changes. For each distance, we define SKR_{max} as the peak of the SKR curve over the launch power, and introduce the dimensionless parameter R:

$$\mathrm{R} = \frac{\mathrm{SKR}_{\mathrm{max}}}{\mathrm{SKR}_{\mathrm{max}}^{\mathrm{GM}}} \tag{32}$$

defined as the ratio between the $\mathrm{SKR}_{\mathrm{max}}$ value obtained for a given protocol, and that obtained for the GG02 protocol. This provides a measure of efficiency of a given protocol compared to GG02.

This efficiency parameter is reported in Figure 3 on the right. Compared to uniform signaling, PAS significantly improves the efficiency of the protocol and mitigates the decay of R at long distances, where channel loss dominates. The improvement is more pronounced for QAM constellations with higher cardinality due to the larger flexibility in shaping the input distribution. For example, PAS-64QAM reaches 95% of the GG02 performance beyond 40 km, while PAS-16QAM is already sufficient to reach almost 70% at the same distance, outperforming both U-16QAM and U-64QAM, whose efficiency never exceeds 50%. In summary, PAS not only improves the SKR of QAM-based protocols, but also allows high-cardinality constellations like 64QAM to closely approach the performance of GG02, making practical protocols based on discrete modulations more competitive in terms of maximum achievable SKR.

We now turn our attention to the role of excess noise, which—along with losses—affects performance in realistic scenarios. We fix the cardinality of the constellation (64QAM) and study the evolution of $\mathrm{SKR}_{\mathrm{max}}$ with distance for increasing excess noise levels $\xi \in \{0.01, 0.03, 0.05\}$ (in SNU). In experimentally reported fiber-based CV-QKD systems [52–54], excess noise values typically range from a few 10^{-3} SNU to a few 10^{-2} SNU, depending on the system architecture, transmission conditions, and hardware implementation [33]. The values considered in this work are representative of realistic operating scenarios, ranging from well-optimized and carefully calibrated setups to more challenging conditions in which excess noise may be increased by phase fluctuations, modulation imperfections, detector non-idealities, Raman scattering from co-propagating classical channels, and other implementation-dependent noise sources [13,55].

As shown in Figure 4 (left), the $\mathrm{SKR}_{\mathrm{max}}$ decays more rapidly with distance as ξ increases, dropping to zero at progressively shorter distances. However, PAS still provides an effective solution, significantly slowing down the decay rate and extending the maximum distance compared to uniform signaling.

This resilience is also reflected in the behavior of the relative efficiency R, shown in Figure 4 (right). At short distances, R is constrained by the constellation cardinality M, which limits the entropy of the source to $\log_2 M$. Interestingly, in this regime, an increase in the excess noise level ξ reduces the gap between discrete modulations and GG02. This is reflected by the moderate increase in R with ξ for uniform signaling, and a slightly more pronounced increase for PAS.

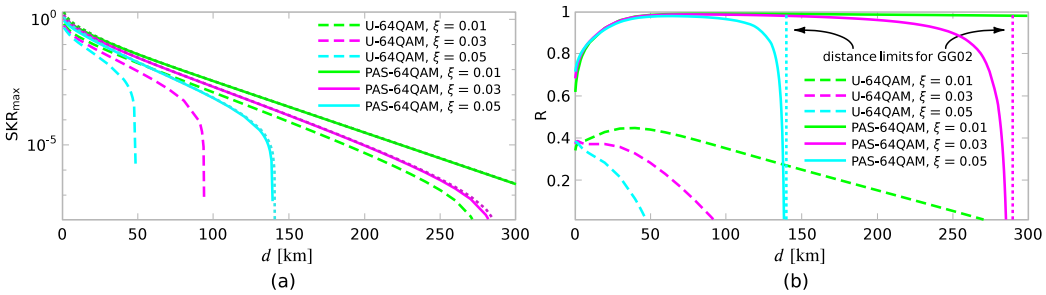

Figure 4. (**a**) Maxima of SKR for the 64QAM with uniform and non-uniform input signaling in the range 0.5–300 km for different excess noise values ξ. GG02 curves are shown as dotted lines and are hardly distinguishable, as they are almost completely superimposed on the corresponding PAS curves. (**b**) Corresponding values of R in the same range of distances and excess noise values; the dotted lines show the maximum achievable distances of GG02 for $\xi = 0.03$ (magenta) and $\xi = 0.05$ (light blue).

In general, PAS provides a substantial gain over uniform signaling at all noise levels. While shaped signaling cannot fully bridge the gap with GG02 at short distances—due to the aforementioned entropy limitation—it performs increasingly well in the medium-distance regime, where R approaches 1. In this regime, excess noise generally reduces the efficiency of discrete modulations relative to GG02. However, the advantage of PAS over uniform signaling becomes increasingly pronounced as the excess noise level rises, with the efficiency parameter R remaining close to 1 across a broad range of distances and noise levels. In fact, PAS-64QAM achieves almost the same distance limit as GG02, with its efficiency relative to GG02 only beginning to decline a few kilometers before that limit.

3.2. Launch Power

A key design parameter in QKD systems is the launch power—typically expressed as the average number of photons per symbol $\bar{n}$ on Alice's side—which must be optimized to ensure secure operation at a given distance and noise level. Figure 5 reports, as a function of distance, the optimal launch power $\bar{n}_{\max}$ (solid lines) that maximizes the SKR, along with the operating power range (shaded areas), defined by the minimum and maximum $\bar{n}$ values (dotted lines) for which the SKR remains positive. The left and right panels correspond to 16QAM and 64QAM formats, respectively, with the GG02 reference shown in all plots. The top, middle, and bottom panels represent different levels of excess noise. For each distance, the corresponding power value on Bob's side is equal to $T(\bar{n} + \xi/2)$.

The GG02 protocol starts, at short distances (where channel losses are negligible), with a high optimal launch power (exceeding 100 photons per symbol) and a wide operating power range. As the distance increases, the optimal launch power initially decreases rapidly and then stabilizes at an almost constant value. At the same time, the power operating range gradually narrows around the optimal power, and eventually collapses when the protocol reaches its maximum transmission distance, which depends on the excess noise level. Discrete modulations exhibit a qualitatively similar trend, but with some relevant differences. First, the optimal launch power starts from much lower values at zero distance due to the entropy limitation of finite-size constellations. Additionally, both the power operating range and maximum achievable distance are generally reduced compared to GG02. These limitations are particularly evident for uniform signaling, with minimal improvement when moving from 16QAM to 64QAM. By contrast, the higher efficiency of PAS is reflected in both a higher optimal launch power and a broader operating range relative to uniform signaling. Notably, except for the first 70 km—where the entropy constraint of the constellation still limits the performance—PAS-64QAM closely follows

the behavior of GG02, with practically the same optimal launch power, operating power range, and maximum distance.

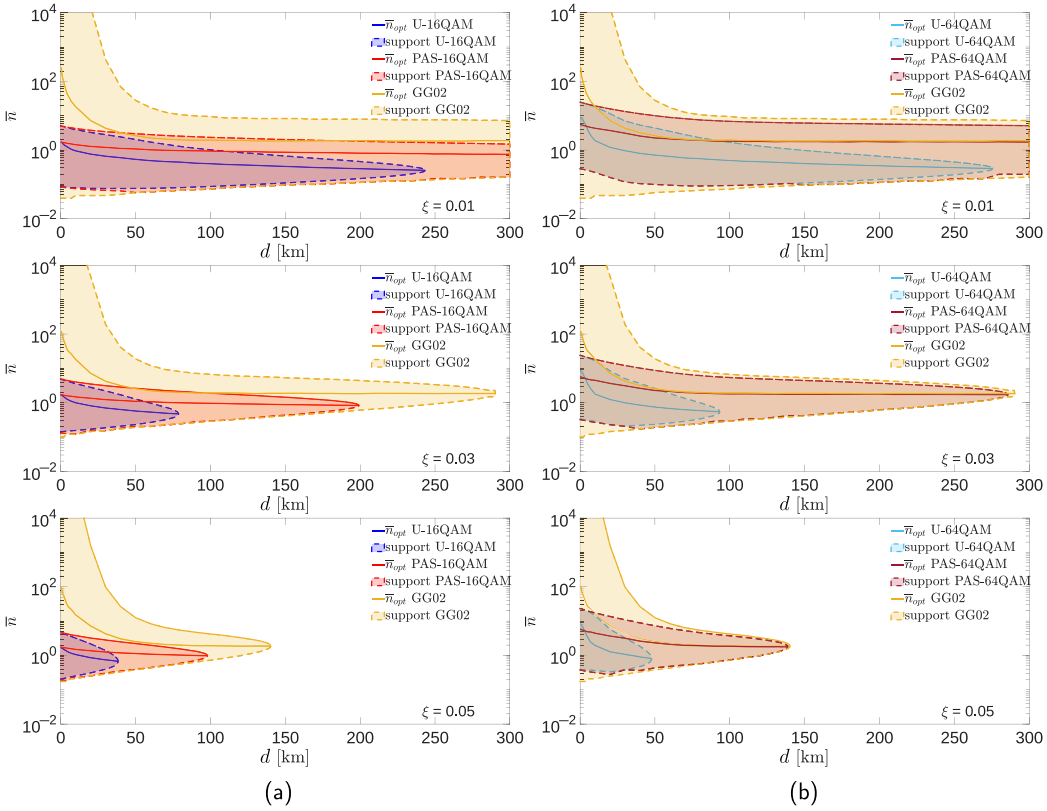

Figure 5. $\bar{n}_{\max}$ and mean number of photons supporting SKR curves at Alice's side for (**a**) 16QAM and (**b**) 64QAM with both uniform and non-uniform signaling and with respect to the GG02 case at different excess noise values (from top to bottom $\xi = 0.01, 0.03, 0.05$).

3.3. Maximum Tolerable Excess Noise

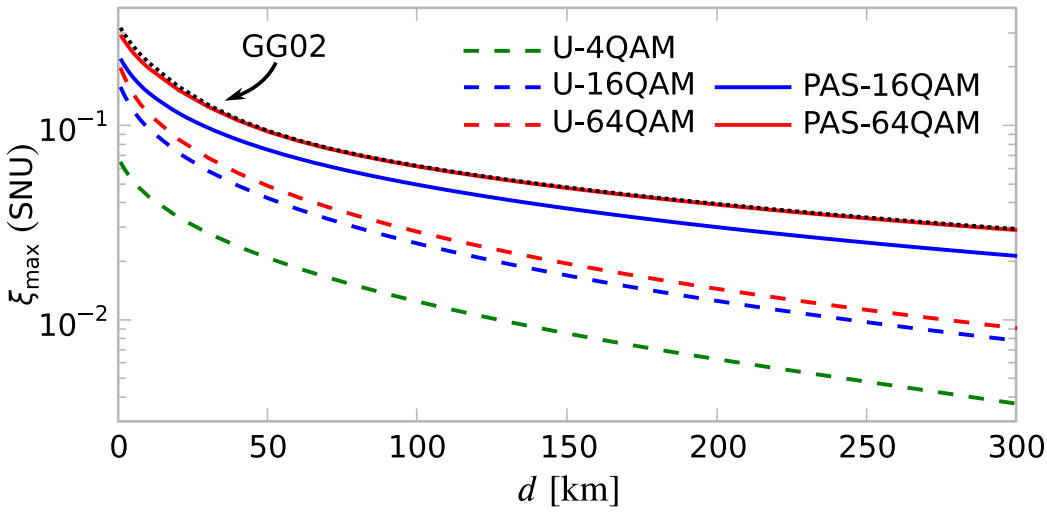

Figure 6. Tolerable excess noise ξ_{max} for collective attacks, homodyne detection and reverse reconciliation in the range 0.5–300 km for 4QAM, 16QAM, 64QAM with uniform and non-uniform signaling and for the GG02 protocol.

We now assess the noise resilience of the proposed protocol by analyzing the maximum excess noise that can be tolerated as a function of the transmission distance. We define the maximum tolerable excess noise as the highest value of ξ for which the SKR remains

positive. Figure 6 compares this quantity for the GG02 protocol and for QAM-based protocols with uniform or shaped input distributions.

Consistent with the trends observed in previous Sections 3.1 and 3.2, we find that the maximum tolerable excess noise increases with the cardinality M of the constellation and decreases with transmission distance. This behavior reflects the opposing trends of the two terms in the SKR expression (14): while the HI term increases with noise, the MI term decreases with both noise and distance. As expected, uniform QAM is substantially less resilient to excess noise than GG02. However, PAS significantly improves the robustness of QAM-based protocols. Notably, at long distances, PAS-16QAM more than doubles the noise tolerance compared to both uniform 16QAM and 64QAM. Moreover, PAS-64QAM can tolerate nearly the same level of excess noise as GG02 at all distances beyond 40 km.

3.4. Wiretap Quantum Channel vs. Linear Quantum Channel

An efficient evaluation of a generic protocol must take into account the level of security it guarantees, the performance it provides, and the feasibility of its implementation. Regarding the latter two, we have discussed above how our protocol is easily compatible with the classical telecommunication techniques currently exploited and what achievable rates, distances and noise resilience we can expect from it. Its security, instead, was untangled in the estimation of the HI term, where we assumed Eve is able to purify the system introducing additional modes that she can control.

In the following, we compare the results we have found here with those we obtained in our previous work [40], in which we dealt with a QAM-based CV-QKD scheme, but under the different scenario of a wiretap quantum channel, where Eve is limited to a beam-splitting attack. Although the wiretap channel represents much more restrictive eavesdropping, a comparison between these two channel models can shed light on the role of the probabilistic shaping technique in a generic CV-QKD system with QAM modulation of the input symbols. It is therefore interesting to understand how the wiretap (w) and the linear quantum channel (ℓ) hypotheses, characterized by different security levels, influence the performance of the same CV-QKD protocol and how the probabilistic shaping technique behaves as a resource in these different contexts. In particular, since we are interested in the advantages in the rate of communication (SKR), we explore these features only in a noiseless framework.

In a lossy (noiseless) wiretap channel scenario, Eve cannot alter the nature of the quantum signals: in fact, she can only collect the fraction of signals that has been lost during propagation; as a consequence, the channel in Eve's hands can be pictured as a beam splitter, whose output ports deliver the fraction T of signals to Bob and the stolen fraction $1 - T$ to Eve [56,57]. In the linear noiseless quantum channel framework, the shot-noise is still the only resource that can be exploited by Eve to hide her interaction with the system, but Eve's actions are only constrained to preserve Alice and Bob's statistics without being limited to Gaussian attacks, so that the attacker has more freedom in choosing the dilation map that allows her to maximize the knowledge on the system.

As already seen, a good figure of merit for the evaluation of the achievable rate compared to that of the GG02 protocol is the parameter R; in Figure 7 we compared this quantity obtained for each model and for both 16QAM (left side) and 64QAM (right side). From a general point of view, the linear quantum framework (ℓ) provides worse results than the wiretap one in terms of maximum rate. We can, in fact, notice how the curves related to the uniform signaling in (w) are very close to those obtained from a MB shaping of the input probabilities in (ℓ): for example, U-16QAM (w) (blue dotted line) is able to outperform the PAS-16QAM obtained in (ℓ) (red solid line). However, this feature does not

occur in the 64QAM case: unlike before, here a larger statistical set contributes to a better effect of the PAS technique on the achievable rate of the key distribution.

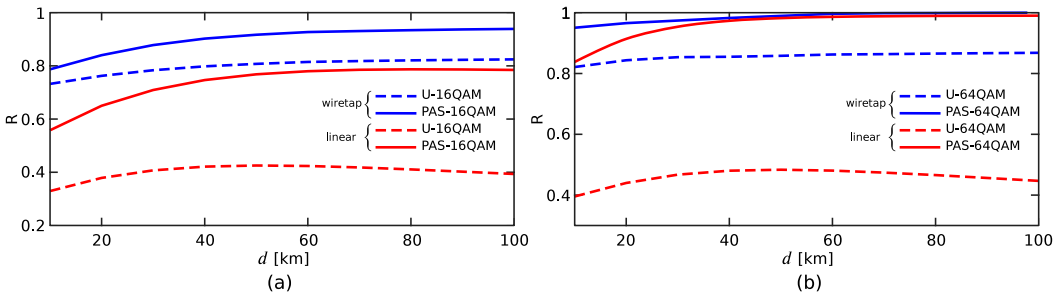

Figure 7. The parameter R for collective attacks, homodyne detection and reverse reconciliation in the range 10–100 km for (**a**) 16QAM and (**b**) 64QAM for a wiretap quantum channel and a linear quantum channel with no excess noise.

Therefore, we can say that the increased level of security provided by the linear quantum channel framework generally comes at the cost of reduced performance. However, even if the values of R in (ℓ) are noticeably lower than those in (w) for uniform signaling, shaping is still able to increase the system performance in the long distance regime, reducing the gap with GG02. It is important to note that the percentage increase in the rate is, proportionately, even larger for (ℓ) than for (w); in particular, it can be easily seen that the performance of the PAS-64QAM (ℓ) is almost equal to that of the PAS-64QAM (w) after a distance of 40 km.

4. Conclusions

In this work, we have investigated a QAM-based CV-QKD system with uniform and non-uniform signaling (PAS technique using a Maxwell–Boltzmann distribution) within the framework of homodyne detection and the asymptotic regime of infinite key length. We focused on collective attacks, which are the most powerful class of attacks in the asymptotic limit, and adopted the reverse reconciliation scheme since it enables longer communication distances between the legitimate parties. In particular, we studied the system under a linear quantum channel model, which provides a simple and effective description of the propagation of quantum signals in an optical fiber link and is commonly adopted in practical CV-QKD experiments. In this context, the "linear channel" assumption refers to an effective linear input–output relation between quadrature operators in the Heisenberg picture. During parameter estimation, a fraction of the exchanged data is publicly disclosed and used to assess the consistency of the observed statistics with a linear channel model. Under this model, we analyzed the system behavior against the purification attack, which represents the most powerful strategy available to Eve. Using the GG02 protocol as a benchmark, we evaluated the system performance in terms of achievable secret key rates and maximum transmission distances for different levels of excess noise, and assessed its robustness against noise.

We found that the combination of QAM modulation and PAS based on the Maxwell–Boltzmann distribution consistently outperforms the corresponding uniform distribution protocol for all the distances and excess noise values considered in this work. In particular, PAS-64QAM proved to be an effective and practical solution to closely approach the performance of the GG02 protocol, especially in the long-distance regime. Indeed, beyond approximately 40 km, PAS-64QAM achieves nearly the same secure key rates and exhibits the same excess noise tolerance compared to the ideal GG02 protocol. Furthermore, PAS significantly enhances the performance of QAM-based schemes at any distance, with the

simpler PAS-16QAM outperforming the more complex uniform 64QAM and showing increased robustness to excess noise.

Moreover, we analyzed the impact of PAS under different assumptions on Eve's capabilities. To this end, we have compared the results obtained for a noiseless linear quantum channel model with those corresponding to a lossy wiretap channel scenario, in which Eve is limited to accessing only the fraction of losses introduced by imperfections in the optical fiber link. In general, we observed that the use of discrete modulation assisted by a uniform probability of input symbols leads to lower achievable key rates in a noiseless linear quantum channel compared to the lossy wiretap model. Nevertheless, within the noiseless linear quantum channel framework, PAS not only provides an effective means to mitigate this performance degradation, but also yields a higher percentage gain in terms of secure key rates compared to the lossy wiretap model. These features are particularly evident from the observed good agreement between the maximum secure key rates obtained under the two channel models for PAS-64QAM in the long-distance regime.

To provide a more complete assessment of the security of our protocol, we conclude by highlighting several limitations of the present analysis that may affect both the security and performance of the proposed DM CV-QKD scheme in practical scenarios and, then, motivate future investigations. First, during parameter estimation, Alice and Bob reconstruct only the first and second statistical moments of the measurement data and verify their consistency with the assumed linear channel model. However, the covariance matrix alone does not provide a complete characterization of a non-Gaussian protocol like the one we analyzed and therefore does not allow one to exclude more general nonlinear or non-Gaussian transformations that reproduce the same second-order statistics while affecting higher-order moments, whose treatment is outside the scope of the present work. Second, from a practical perspective, real optical fibers may exhibit nonlinear propagation effects, such as the above mentioned Kerr-induced self-phase modulation [58–60], especially in high-power regimes or ultra-long-haul transmission scenarios. Also in this case, such effects can lead to deviations from the assumed linear input–output relations for quadrature operators and are therefore not captured by standard covariance-matrix-based parameter estimation. Third, the present analysis is restricted to the asymptotic regime of infinitely long key exchanges. In practical implementations, however, finite-size effects reduce the accuracy of parameter estimation, affect excess noise estimation, and ultimately reduce the achievable secret key rate and transmission distance. Therefore, the security guarantees reported in this work should be interpreted within the established asymptotic security framework for linear quantum channels under collective attacks. Overall, this work provides a systematic performance comparison of PAS-QAM CV-QKD protocols against uniform modulation and the GG02 benchmark, highlighting the benefits of probabilistic shaping while clearly delineating the scope of the underlying security assumptions. Future work will address finite-size security analysis and the inclusion of nonlinear channel effects.

Author Contributions: Conceptualization: all; methodology: M.N.N., S.O. and M.S.; formal analysis: E.P. and M.N.N.; software: E.P.; writing—original draft preparation: E.P.; writing—review and editing: all; supervision: S.O., E.F., L.P. and M.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the PNRR MUR project PE0000023-NQSTI, and by the National Operational Programme on Research and Innovation 2014–2020—FSE REACT EU "Azione IV.5 Dottorati su tematiche Green" (DM 1061/2021).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, 621–669.
2. Maurer, U. Information-theoretic cryptography. In *Proceedings of the Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 1999; pp. 47–65.
3. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301.
4. Martin, V.; Martinez-Mateo, J.; Peev, M. Introduction to quantum key distribution. *Wiley Encycl. Electr. Electron. Eng.* **2017**, *1*, 1–17.
5. Cariolaro, G. *Quantum Communications Systems*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 281–359.
6. Braunstein, S.L.; Van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513–577.
7. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145.
8. Dušek, M.; Lütkenhaus, N.; Hendrych, M. Quantum cryptography. *Prog. Opt.* **2006**, *49*, 381–454.
9. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **2020**, *12*, 1012–1236.
10. Wolf, R. *Quantum Key Distribution*; Springer: Berlin/Heidelberg, Germany, 2021.
11. Zhang, Y.; Bian, Y.; Li, Z.; Yu, S.; Guo, H. Continuous-variable quantum key distribution system: Past, present, and future. *Appl. Phys. Rev.* **2024**, *11*, 011318.
12. Kaur, E.; Guha, S.; Wilde, M.M. Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. *Phys. Rev.* **2021**, *103*, 012412.
13. Laudenbach, F.; Pacher, C.; Fung, C.H.F.; Poppe, A.; Peev, M.; Schrenk, B.; Hentschel, M.; Walther, P.; Hübel, H. Continuous-variable quantum key distribution with Gaussian modulation—The theory of practical implementations. *Adv. Quantum Technol.* **2018**, *1*, 1800011.
14. Abushgra, A.A. Variations of QKD protocols based on conventional system measurements: A literature review. *Cryptography* **2022**, *6*, 12.
15. Lupo, C.; Ouyang, Y. Quantum key distribution with nonideal heterodyne detection: Composable security of discrete-modulation continuous-variable protocols. *PRX Quantum* **2022**, *3*, 010341.
16. Leverrier, A.; Grangier, P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.* **2009**, *102*, 180504.
17. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902.
18. Holevo, A.S.; Giovannetti, V. Quantum channels and their entropic characteristics. *Rep. Prog. Phys.* **2012**, *75*, 046001.
19. Cerf, N.J.; Leuchs, G.; Polzik, E.S. *Quantum Information with Continuous Variables of Atoms and Light*; World Scientific: Singapore, 2007.
20. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E.; Leverrier, A. Analysis of imperfections in practical continuous-variable quantum key distribution. *Phys. Rev. A—At. Mol. Opt. Phys.* **2012**, *86*, 032309.
21. Diamanti, E.; Leverrier, A. Distributing secret keys with quantum continuous variables: Principle, security and implementations. *Entropy* **2015**, *17*, 6072–6092.
22. Djordjevic, I.B. On the discretized Gaussian modulation (DGM)-based continuous variable-QKD. *IEEE Access* **2019**, *7*, 65342–65346.
23. Proakis, J.; Salehi, M. *Digital Communications*, 4th ed.; McGraw-Hill: New York, NY, USA, 2001.
24. Winzer, P.J. High-spectral-efficiency optical modulation formats. *J. Light. Technol.* **2012**, *30*, 3824–3835.
25. Kschischang, F.R.; Pasupathy, S. Optimal nonuniform signaling for Gaussian channels. *IEEE Trans. Inf. Theory* **1993**, *39*, 913–929.
26. Böcherer, G.; Steiner, F.; Schulte, P. Bandwidth efficient and rate-matched low-density parity-check coded modulation. *IEEE Trans. Commun.* **2015**, *63*, 4651–4665.
27. Buchali, F.; Steiner, F.; Böcherer, G.; Schmalen, L.; Schulte, P.; Idler, W. Rate adaptation and reach increase by probabilistically shaped 64-QAM: An experimental demonstration. *J. Light. Technol.* **2015**, *34*, 1599–1609.
28. Fehenberger, T. Information rates of probabilistically shaped coded modulation for a multi-span fiber-optic communication system with 64QAM. *Opt. Commun.* **2018**, *409*, 2–6.
29. Fehenberger, T.; Alvarado, A.; Böcherer, G.; Hanik, N. On probabilistic shaping of quadrature amplitude modulation for the nonlinear fiber channel. *J. Light. Technol.* **2016**, *34*, 5063–5073.

30. Fan-Yuan, G.J.; Xie, W.X.; He, D.Y.; Huang, X.J.; Wang, S.; Yin, Z.Q.; Chen, W.; Li, Q.; Mao, H.K.; Zhang, G.W.; et al. High-rate quantum key distribution with compact state preparation and detection. *Proc. Natl. Acad. Sci. USA* **2026**, *123*, e2521590123.
31. Lu, F.Y.; Wang, Z.H.; Zhou, Y.; Fan, Y.X.; Wang, S.; Yin, Z.Q.; Li, J.; He, D.Y.; Wang, F.X.; Chen, W.; et al. Fully heterogeneous prepare-and-measure quantum network for the next stage of quantum internet. *Nat. Commun.* **2025**, *16*, 11487.
32. Origlia, M.; Secondini, M. Soft Reverse Reconciliation for Discrete Modulations. In Proceedings of the 2025 14th International ITG Conference on Systems, Communications and Coding (SCC), Karlsruhe, Germany, 10–13 March 2025; IEEE: New York, NY, USA, 2025; pp. 1–6.
33. Usenko, V.C.; Acín, A.; Alléaume, R.; Andersen, U.L.; Diamanti, E.; Gehring, T.; Hajomer, A.A.; Kanitschar, F.; Pacher, C.; Pirandola, S.; et al. Continuous-variable quantum communication. *Rev. Mod. Phys.* **2026**, *98*, 015003.
34. Huang, J.Z.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Li, H.W.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A—At. Mol. Opt. Phys.* **2013**, *87*, 062329.
35. Huang, J.Z.; Kunz-Jacques, S.; Jouguet, P.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking on quantum key distribution using homodyne detection. *Phys. Rev. A* **2014**, *89*, 032304.
36. Navascués, M.; Grosshans, F.; Acin, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502.
37. Ghorai, S.; Grangier, P.; Diamanti, E.; Leverrier, A. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Phys. Rev. X* **2019**, *9*, 021059.
38. Lin, J.; Upadhyaya, T.; Lütkenhaus, N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Phys. Rev. X* **2019**, *9*, 041064.
39. Denys, A.; Brown, P.; Leverrier, A. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum* **2021**, *5*, 540.
40. Notarnicola, M.N.; Olivares, S.; Forestieri, E.; Parente, E.; Potì, L.; Secondini, M. Probabilistic amplitude shaping for continuous-variable quantum key distribution with discrete modulation over a wiretap channel. *IEEE Trans. Commun.* **2023**, *72*, 375–386.
41. Olivares, S. Quantum optics in the phase space: A tutorial on Gaussian states. *Eur. Phys. J. Spec. Top.* **2012**, *203*, 3–24.
42. Cover, T.M. *Elements of Information Theory*; John Wiley & Sons: Hoboken, NJ, USA, 1999.
43. Forney, G.D.; Wei, L.F. Multidimensional constellations. I. Introduction, figures of merit, and generalized cross constellations. *IEEE J. Sel. Areas Commun.* **1989**, *7*, 877–892.
44. Forney, G.; Gallager, R.; Lang, G.; Longstaff, F.; Qureshi, S. Efficient modulation for band-limited channels. *IEEE J. Sel. Areas Commun.* **1984**, *2*, 632–647.
45. Wen, X.; Li, Q.; Mao, H.; Wen, X.; Chen, N. An improved slice reconciliation protocol for continuous-variable quantum key distribution. *Entropy* **2021**, *23*, 1317.
46. Mani, H.; Gehring, T.; Grabenweger, P.; Ömer, B.; Pacher, C.; Andersen, U.L. Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution. *Phys. Rev. A* **2021**, *103*, 062419.
47. Secondini, M. Information capacity of optical channels. In *Optical Fiber Telecommunications VII*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 867–920.
48. Notarnicola, M.N. Quantum communications in continuous variable systems. *Int. J. Quantum Inf.* **2025**, *23*, 2550003.
49. García-Patrón, R.; Cerf, N.J. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503.
50. Leverrier, A. Theoretical Study of Continuous-Variable Quantum Key Distribution. Ph.D. Thesis, Télécom ParisTech, Palaiseau, France, 2009.
51. Ferraro, A.; Olivares, S.; Paris, M.G. Gaussian states in continuous variable quantum information. *arXiv* **2005**, arXiv:quant-ph/0503237.
52. Hajomer, A.A.; Bruynsteen, C.; Derkach, I.; Jain, N.; Bomhals, A.; Bastiaens, S.; Andersen, U.L.; Yin, X.; Gehring, T. Continuous-variable quantum key distribution at 10 gbaud using an integrated photonic-electronic receiver. *Optica* **2024**, *11*, 1197–1204.
53. Wang, N.; Du, S.; Liu, W.; Wang, X.; Li, Y.; Peng, K. Long-distance continuous-variable quantum key distribution with entangled states. *Phys. Rev. Appl.* **2018**, *10*, 064028.
54. Roumestan, F.; Ghazisaeidi, A.; Renaudier, J.; Vidarte, L.T.; Leverrier, A.; Diamanti, E.; Grangier, P. Experimental demonstration of discrete modulation formats for continuous variable quantum key distribution. *arXiv* **2022**, arXiv:2207.11702.
55. Birhanu, S.L.; Ghadimi, M.; Hai, Y.; Seeling, P.; Bassoli, R.; Fitzek, F.H. A Survey of Continuous Variable Quantum Key Distribution in Quantum Communication. *IEEE Access* **2025**, *13*, 166027–166061.
56. Sych, D.; Leuchs, G. Coherent state quantum key distribution with multi letter phase-shift keying. *New J. Phys.* **2010**, *12*, 053019.
57. Pan, Z.; Seshadreesan, K.P.; Clark, W.; Adcock, M.R.; Djordjevic, I.B.; Shapiro, J.H.; Guha, S. Secret-key distillation across a quantum wiretap channel under restricted eavesdropping. *Phys. Rev. Appl.* **2020**, *14*, 024044.
58. Kunz, L.; Paris, M.G.; Banaszek, K. Noisy propagation of coherent states in a lossy Kerr medium. *J. Opt. Soc. Am. B* **2018**, *35*, 214–222.

59. Stobińska, M.; Milburn, G.; Wódkiewicz, K. Wigner function evolution of quantum states in the presence of self-Kerr interaction. *Phys. Rev. A—At. Mol. Opt. Phys.* **2008**, *78*, 013810.
60. Rossi, M.A.; Albarelli, F.; Paris, M.G. Enhanced estimation of loss in the presence of Kerr nonlinearity. *Phys. Rev. A* **2016**, *93*, 053805.