New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

PAPER

Security of binary-modulated optical key distribution against quantum-enhanced coherent eavesdropping

Karol Łukanowski[1,*], **Michał Wójcik**[2], **Stefano Olivares**[3,4], **Konrad Banaszek**[1,2] and **Marcin Jarzyna**[1]

[1] Centre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, Banacha 2c, 02-097 Warsaw, Poland
[2] Faculty of Physics, University of Warsaw, Pasteura 5, 02-093 Warsaw, Poland
[3] Dipartimento di Fisica 'Aldo Pontremoli', Università degli Studi di Milano, via Celoria 16, I-20133 Milan, Italy
[4] Istituto Nazionale di Fisica Nucleare, Sezione di Milano, I-20133 Milan, Italy
[*] Author to whom any correspondence should be addressed.

E-mail: k.lukanowski@cent.uw.edu.pl, stefano.olivares@fisica.unimi.it, k.banaszek@uw.edu.pl and m.jarzyna@cent.uw.edu.pl

Keywords: optical key distribution, physical layer security, direct detection, coherent detection, quantum-enhanced measurements

OPEN ACCESS

RECEIVED
16 April 2026

REVISED
29 June 2026

ACCEPTED FOR PUBLICATION
14 July 2026

PUBLISHED
30 July 2026

Abstract

Optical key distribution protects the physical layer of communication links by taking advantage of the inherent noise present in the photodetection process. It allows for efficient generation of a shared random key between two distant users that is secure against passive eavesdropping and can be subsequently used for cryptographic purposes. Moreover, it can be straightforwardly implemented over standard intensity modulation and direct detection links, making it an attractive alternative to quantum key distribution. Here we present a comprehensive security analysis against more powerful eavesdroppers possessing the ability to perform either coherent detection, or even quantum-optimal measurements on the intercepted transmission.

1. Introduction

The physical layer of modern optical communication links remains largely unprotected from third party interference, with the bulk of security delegated to computational encryption in the higher layers of the network stack [1]. Due to the rising risk of hacking attacks against public key cryptosystems, either via improved classical methods or with the possible advent of large-scale quantum computing [2], more attention is directed towards procedures that provide additional safeguards to information transmission by taking advantage of the physics of the communication channel [3]. One such avenue is quantum key distribution (QKD), in which two distant devices (which we shall customarily call Alice and Bob) perform measurements on exchanged quantum states of light to obtain correlated sequences of bits [4]. Due to the no-cloning theorem for quantum states, with proper protocol engineering and digital post-processing, these sequences are assured to be unknown to potential third parties. When in possession of such shared secret sequences, Alice and Bob may equip their protocol with additional information-theoretic private key cryptography, or use them for fresh seeding of the security measures already in place, which strengthens their resilience. However, reliance on quantum phenomena makes QKD difficult to realize experimentally, especially in large-scale communication networks, as the technology required includes sophisticated techniques like single-photon or shot-noise-limited coherent detection and high-fidelity quantum state preparation. Moreover, inevitable signal attenuation and excess noise vastly limit the possible generation rates of quantum keys and the range of QKD links [5].

The recently proposed optical key distribution (OKD) protocol [6, 7] relaxes the technological requirements of QKD while offering the possibility of high-speed private key generation protected against passive eavesdropping, which currently is the most likely form of attack. The protocol can be readily implemented in standard intensity modulation & direct detection (DD) systems, as its security is derived only from the inherent randomness of the photodetection process. It is applicable both to optical fiber links [8] and free-space communication [9], and can be integrated with simultaneous standard data transmission [10, 11]. On the other hand, while QKD can in principle protect against

intercept-and-resend attacks, such as when a third party intercepts, measures, and resends the signal to the receiver device, OKD assumes that any potential third party (Eve) is at best a passive eavesdropper that may capture a part of the signal coming from Alice, but cannot modify the part that reaches Bob. This means that active eavesdropping such as source manipulation, detector blinding, or man-in-the-middle attacks, is not addressed in the present OKD security analysis. On the other hand, the passive eavesdropping model covers the most relevant current threats to communication security [8, 9, 12]. In the case of fiber communication, it includes the collection of light leakage by fiber bending or tapping into unused ports in a switch device [13]. In case of free-space optical communication, it includes the possibility of Eve collecting the signal that arrives outside of the area secured by Bob (e.g. for satellite or deep-space optical transmission, this could entail installing a rogue receiver telescope nearby and collecting the diffracted or scattered light).

In the previous theoretical study [7], OKD has been shown to guarantee positive key distribution rates if the eavesdropper Eve implements DD on the intercepted signals, same as Bob. Importantly, even if Eve captures the majority of the signal, this simply lowers the rate of key generation but does not preclude it, in contrast to wiretap channel coding [14]. In this work we show that in the asymptotic information-theoretic regime OKD allows for positive secret key generation rates even for the most general passive eavesdropper capabilities allowed by quantum theory. This paper is organized as follows. In section 2 we review the OKD protocol and previous results on the security against DD eavesdropping. Subsequently, we equip Eve with shot-noise-limited coherent detection capabilities in section 3, the ability to perform Helstrom measurements which minimize the probability of state discrimination error in section 4, and finally with optimal collective measurements that saturate the Holevo bound on accessible information in section 5. Section 6 summarizes the obtained results and concludes the paper. The main text analysis assumes that Bob and Eve measure signals of macroscopic strength, which allows us to approximate their outcome distributions as Gaussian. In the appendix we drop this assumption and treat numerically an exact model, which is shown to quickly converge to the approximate one with increasing signal strength.

2. DD eavesdropping

The goal of the OKD protocol is to establish between Alice and Bob a common sequence of random bits that are unknown to Eve. In each protocol round of binary-modulated OKD, Alice chooses randomly bit value $a \in \{0,1\}$, which constitutes an instance of her random variable A, and transmits to Bob a light pulse with one of two possible values of optical energy $n_a \in \{n_0, n_1\}$. The optical channel is characterized by transmission τ_{B}, with an additional side channel to Eve characterized by transmission τ_{E}. We assume that the light pulses received by Bob and Eve are of macroscopic strength, i.e. $\tau_{\mathrm{B}} n_a \gg 1$ and $\tau_{\mathrm{E}} n_a \gg 1$ for both values of a. In this regime the discrete Poissonian distribution of photocounts can be well approximated by a Gaussian distribution. Bob's and Eve's detected variables are then modeled by normally distributed continuous variables $k_{\mathrm{B}}|a \sim \mathcal{N}(\tau_{\mathrm{B}} n_a, \sigma^2_{\mathrm{B},a})$ and $k_{\mathrm{E}}|a \sim \mathcal{N}(\tau_{\mathrm{E}} n_a, \sigma^2_{\mathrm{E},a})$, where $\sigma^2_{\mathrm{B/E},a}$ denotes the variance of Bob's/Eve's outcome distribution given the value of a. Importantly, the energies n_0 and n_1 are chosen sufficiently close so that neither Bob nor Eve can unambiguously identify the value of each transmitted bit, due to the overlap of photocount distributions as depicted in figure 1. Because for large n_a the photocount outcome variance scales like n_a, due to the assumption of small $n_1 - n_0$ difference we further assume that photocount variance depends only on the average $\bar{n} = (n_0 + n_1)/2$ and has the same value for both a, $\sigma^2_{\mathrm{B/E},a} = \sigma^2_{\mathrm{B/E}}$. While this approximation results in greatly simplified key rate formulas, we further verify its validity in the appendix, where an exact model with a-dependent variances is shown numerically to quickly converge to the present one with equalized variances.

The rate of key generation K attainable from the raw data held by Alice and Bob after completing the protocol is upper bounded by the Csiszár–Körner theorem valid for individual attacks [16],

$$\begin{aligned}\mathsf{K} &= \max\{I(B;A) - I(B;E),\, 0\} \\ &= \max\{H(B|E) - H(B|A), 0\},\end{aligned} \tag{1}$$

expressed either as the difference of mutual information between Alice's and Bob's variables $I(B;A)$ and between Bob's and Eve's $I(B;E)$, or the difference of respective conditional Shannon entropies $H(B|E)$ and $H(B|A)$. Note that this bound is an information-theoretic expression valid in the asymptotic regime of the number of protocol rounds and neglects finite-size corrections [17] as well as other detrimental factors that may limit the key rate achievable in practice, such as imperfect key reconciliation efficiency between Alice and Bob [18].

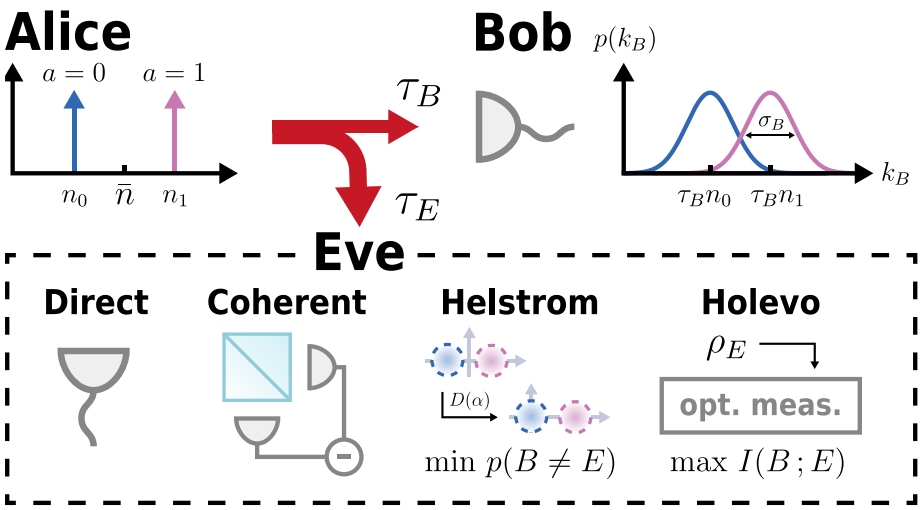

Figure 1. Schematic view of the OKD protocol and different eavesdropping scenarios considered in this work. In binary-modulated OKD, Alice prepares one of two macroscopic pulses of similar energy values n_0 and n_1. She transmits them to Bob via a channel with transmission τ_B. Bob implements direct detection and records normally distributed outputs k_B. The eavesdropper Eve passively captures fraction τ_E of Alice's signal. In the article, four strategies of Eve are considered: direct detection (section 2), coherent detection (section 3), error-minimizing Helstrom measurements (section 4, here pictured in reference to the Helstrom-achieving displacement receivers [15]), and optimal measurements saturating the Holevo bound for accessible information (section 5).

To calculate the key rate it is convenient to first shift and rescale Bob's and Eve's variables,

$$y_B = (k_B - \tau_B \bar{n})/\sigma_B, \quad y_E = (k_E - \tau_E \bar{n})/\sigma_E, \tag{2}$$

where $\bar{n} = (n_0 + n_1)/2$. We then find the distributions of y_B and y_E conditioned on A:

$$y_B|a \sim \mathcal{N}\left((-1)^{1-a}\,\delta_B, 1\right), \quad y_E|a \sim \mathcal{N}\left((-1)^{1-a}\,\delta_E, 1\right), \tag{3}$$

where

$$\delta_B = \frac{\tau_B (n_1 - n_0)}{2\sigma_B}, \quad \delta_E = \frac{\tau_E (n_1 - n_0)}{2\sigma_E}. \tag{4}$$

The conditional entropy $H(B|A)$ can be simply obtained as the differential entropy of a standard normal distribution,

$$H(B|A) = \frac{1}{2}\log_2(2\pi e). \tag{5}$$

The calculation of $H(B|E)$ is more involved due to the need to condition Bob's variable on Eve's knowledge. In general,

$$H(B|E) = -\int_{\mathbb{R}^2} \mathrm{d}y_E\, \mathrm{d}y_B\, p(y_B, y_E) \log_2 p(y_B|y_E), \tag{6}$$

where $p(y_B, y_E)$ is the joint probability distribution of Bob's and Eve's variables and $p(y_B|y_E)$ is the probability distribution of Bob's variable conditioned on Eve's. For y_B and y_E defined according to equation (2), the integral in equation (6) can be simplified to

$$H(B|E) = \frac{1}{2}\log_2(2\pi e) + \delta_B^2 \log_2 e - \int_{\mathbb{R}^2} \mathrm{d}y_E\, \mathrm{d}y_B\, p(y_B, y_E) \log_2 \frac{\cosh(\delta_E y_E + \delta_B y_B)}{\cosh(\delta_E y_E)} \tag{7}$$

with

$$p(y_B, y_E) = \frac{1}{4\pi}\left[\exp\left(-\frac{(y_B + \delta_B)^2 + (y_E + \delta_E)^2}{2}\right) + \exp\left(-\frac{(y_B - \delta_B)^2 + (y_E - \delta_E)^2}{2}\right)\right]. \tag{8}$$

Introducing the *eavesdropper's advantage* parameter

$$\mathscr{E} = \left(\frac{\tau_{\mathrm{E}}/\sigma_{\mathrm{E}}}{\tau_{\mathrm{B}}/\sigma_{\mathrm{B}}}\right)^2, \tag{9}$$

one may relate

$$\delta_{\mathrm{E}}/\delta_{\mathrm{B}} = \sqrt{\mathscr{E}}. \tag{10}$$

Therefore, one may express the key rate in equation (1) as a function only of the eavesdropper's advantage $\mathscr{E}$, which is defined by the channel parameters, and either the δ_{B} or the δ_{E} parameter, which depend on n_1 and n_0 and thus are determined by Alice's choice of modulation. Thus, the maximal attainable key rate results from the optimization of equation (1) over δ_{B} (or equivalently δ_{E}) and is then seen to be a function of $\mathscr{E}$ only. From the security point of view, the worst-case scenario occurs when Eve's detection is shot-noise-limited, $\sigma_{\mathrm{E}}^2 = \tau_{\mathrm{E}}\bar{n}$, so that $\delta_{\mathrm{E}} = \sqrt{\tau_{\mathrm{E}}}(n_1 - n_0)/(2\sqrt{\bar{n}})$. On the other hand, for Bob the variance can be decomposed as $\sigma_{\mathrm{B}}^2 = \tau_{\mathrm{B}}\bar{n} + \sigma_{\mathrm{B,ex}}^2$ with the first term corresponding to shot noise and the second to any additional source of noise. Note that due to the macroscopic pulse strength assumption, we may use the same variance value for both the 0 and 1 pulses that depends only on the average $\bar{n}$. Taking the above into account, the eavesdropper's advantage can be written as

$$\mathscr{E} = \frac{\tau_{\mathrm{E}}}{\tau_{\mathrm{B}}}\left(1 + \frac{\sigma_{\mathrm{B,ex}}^2}{\tau_{\mathrm{B}}\bar{n}}\right) \tag{11}$$

and automatically accommodates increased values of Bob's noise.

An approximate expression for the key rate is derived in [7] by expanding the integrand in equation (7) in the limit of $\mathscr{E} \gg 1$, indicating a strong advantage for Eve, which results in

$$\mathsf{K}^{\mathrm{DD}}(\mathscr{E} \gg 1) \approx \gamma \cdot \frac{\log_2 e}{2\mathscr{E}}, \tag{12}$$

where

$$\gamma = \max_{\delta \geqslant 0}\left\{\delta^2\left[2 - \int_{\mathbb{R}} \mathrm{d}t \, \frac{\mathrm{e}^{-(t-\delta)^2/2}}{\sqrt{2\pi}} \, \frac{\sinh(2\delta t) + 1}{\cosh^2(\delta t)}\right]\right\} \tag{13}$$

can be evaluated numerically to equal $\gamma \approx 0.4795$. Both the key rate values obtained by numerically optimizing the difference of equations (5) and (7) over δ_{B}, as well as the approximate expression (12) for strong eavesdropping, are depicted in figure 2 as functions of the eavesdropper's advantage $\mathscr{E}$.

3. Coherent detection eavesdropping

In the second quantization picture, the light pulses sent by Alice can be described by coherent states $\left|\sqrt{n_a}\mathrm{e}^{\mathrm{i}\phi_a}\right\rangle$, where $\sqrt{n_a}$ signifies the amplitude and ϕ_a the phase. Phase-insensitive DD performed by Bob on such states yields the photocount statistics discussed in the previous section, which in the macroscopic signal strength regime can be described by the variable y_B defined in equation (3). If, however, Eve possesses coherent detection capabilities, she may try to distinguish between the two states by measuring their optical phase-dependent quadratures instead of only the intensity, as a difference in phase increases the phase-space distance between the two states. From the point of view of Alice, it is therefore sensible to randomize the phase ϕ_a for every pulse. This requirement has been recognized as important for QKD security [19, 20] and can be mitigated, for instance, with a phase modulator driven by quantum random number generation [21] or gain-switched laser diodes [22]. Phase-randomized coherent states are characterized only by the photon number distribution identical to that of section 2, in which case coherent detection does not offer any advantage over DD and the security analysis therein remains applicable. On the other hand, if the phase of Alice's pulses is fixed, for example when they are carved with an electro-optic modulator from a narrowband continuous-wave laser output, it is important to ensure that in each individual transmission the choice of signal strength is uncorrelated with the phase, $\phi_0 = \phi_1$, so that the latter does not carry any information about the value of the variable A. In the pessimistic scenario in which Eve has the ability to sync to the pulses' phase, one may simply set $\phi_a = 0$ in the analysis and formulate her task as distinguishing between two coherent states $\left|\sqrt{\tau_{\mathrm{E}}n_0}\right\rangle$ and $\left|\sqrt{\tau_{\mathrm{E}}n_1}\right\rangle$

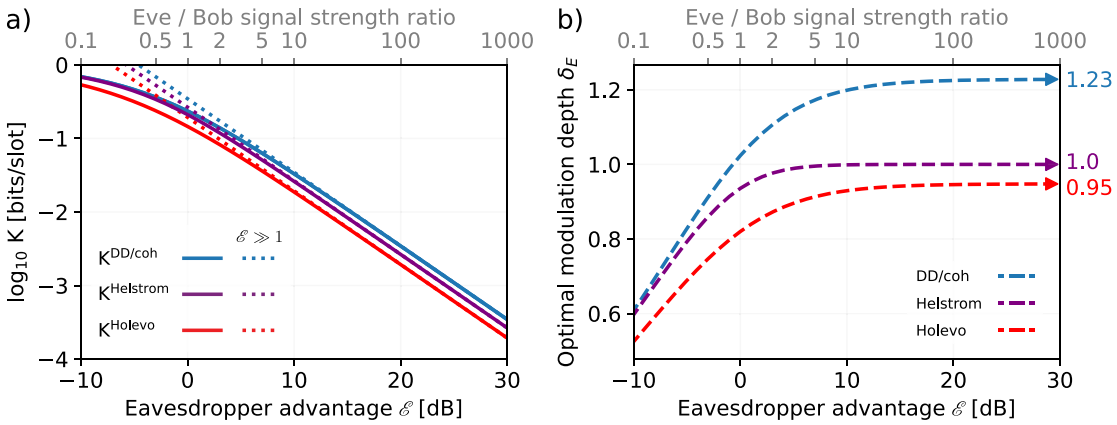

Figure 2. (a) Key generation rates as a function of the eavesdropper's advantage $\mathscr{E}$ for the case of passive eavesdropping with: direct/coherent detection (blue, sections 2 & 3); optimal state discrimination via Helstrom measurements (purple, section 4); optimal measurements saturating the Holevo bound (red, section 5). Dotted lines indicate approximations derived in text for the strong eavesdropping limit, $\mathscr{E} \gg 1$. The upper axis indicates the ratio of Eve's and Bob's signal strength if Bob's detection is shot-noise limited, in which case $\mathscr{E} = \tau_E/\tau_B$ according to equation (11). (b) Values of the modulation depth δ_E that maximize the key rate for the three considered passive eavesdropping scenarios as a function of the eavesdropper's advantage. Arrows indicate the optimal values that maximize the corresponding asymptotic key rate expressions in equations (12), (25) and (38).

in each protocol round. Then, if Eve performs shot-noise-limited homodyne detection of the amplitude quadrature, she obtains a result q_E distributed according to [23]

$$q_E|a \sim \mathcal{N}\left(\sqrt{2\tau_E n_a}, 1/2\right). \tag{14}$$

Following section 2, one may define an equivalent rescaled variable

$$y_E^{\mathrm{coh}} = \left(q_E - \sqrt{2\tau_E}\overline{\alpha}\right)/\sqrt{1/2} \tag{15}$$

with $\overline{\alpha} = (\sqrt{n_0} + \sqrt{n_1})/2$. Note that the factor $(\sqrt{1/2})^{-1}$ follows from the standard deviation of the conditional distribution. When conditioned on A, Eve's variable is seen to have a similar form to equation (3),

$$y_E^{\mathrm{coh}}|a \sim \mathcal{N}\left((-1)^{1-a}\,\delta_E^{\mathrm{coh}}, 1\right), \tag{16}$$

but with a different modulation depth given by

$$\delta_E^{\mathrm{coh}} = \sqrt{\tau_E}\left(\sqrt{n_1} - \sqrt{n_0}\right), \tag{17}$$

calculated here as half of the difference between the peaks of $p(y_E^{\mathrm{coh}}|n_0)$ and $p(y_E^{\mathrm{coh}}|n_1)$. Therefore, the joint distribution $p(y_B, y_E^{\mathrm{coh}})$ also assumes the same form as in equation (8) and leads to the same expression for the key rate, the only difference being that now Eve's modulation depth is δ_E^{coh} instead of δ_E. However, the two can be related by

$$\delta_E^{\mathrm{coh}} = \delta_E \frac{\sqrt{2\left(n_0 + n_1\right)}}{\sqrt{n_0} + \sqrt{n_1}} = \delta_E\left[1 + \frac{1}{32}\left(\frac{\Delta n}{\bar{n}}\right)^2 + \mathcal{O}\left(\left(\frac{\Delta n}{\bar{n}}\right)^4\right)\right] \tag{18}$$

with $\Delta n := n_1 - n_0$. Because we already assumed the input energy to be large $\bar{n} \gg 1$ and $n_0 \approx n_1$, to a good approximation we have $\delta_E^{\mathrm{coh}} \approx \delta_E$, which means that the key rate calculations for DD eavesdropping are reproduced exactly with coherent eavesdropping and one obtains to a good approximation $\mathsf{K}^{\mathrm{coh}} = \mathsf{K}^{\mathrm{DD}}$. Thus, OKD retains the same level of security against coherent detection as against DD, provided that Alice does not encode any information in the phase quadrature.

The equivalence should in fact be expected since for states aligned across the $\phi_a = 0$ axis in phase space, DD effectively measures q_E^2. For large signal strengths the negative tail of the Gaussian distribution in equation (14) is negligible and Eve observes only positive quadrature values which she can equivalently infer from DD results by taking a square root without any sign ambiguity, meaning both types of measurements provide the same information.

4. Eavesdropping based on minimum-error state discrimination

The natural next question is whether there are better ways for Eve to distinguish between the states $\left|\sqrt{\tau_E n_a}\right\rangle$. Indeed, in quantum detection and estimation theory the strategy characterized by the lowest probability of error in discriminating between two quantum states is given by the Helstrom measurement [24].

For the specific case of two coherent states $|\alpha_a\rangle = \left|\sqrt{\tau_E n_a}\right\rangle$, $a \in \{0,1\}$, this measurement can be performed with the Dolinar receiver [15] and yields the minimum discrimination error probability

$$P_{\rm err} = \frac{1}{2}\left(1 - \sqrt{1 - |\langle\alpha_0|\alpha_1\rangle|^2}\right) = \frac{1}{2}\left[1 - \sqrt{1 - {\rm e}^{-\left(\delta_E^{\rm coh}\right)^2}}\right], \tag{19}$$

where $\left|\left\langle\sqrt{\tau_E n_0}\middle|\sqrt{\tau_E n_1}\right\rangle\right|^2 = {\rm e}^{-\tau_E\left(\sqrt{n_1}-\sqrt{n_0}\right)^2}$ and we used equation (17).

Let us now focus on the calculation of the key rate. When conditioned on $A = a$, the results of Bob, y_B, and Eve, m_E, are uncorrelated, and the corresponding joint probability distribution reads $p(a, y_B, m_E) = p(a)\,p(y_B|a)\,p(m_E|a)$ where $p(a) = 1/2$ and $p(y_B|a)$ is still given by equation (3). If Eve implements the Helstrom measurement with outcome $m_E \in \{0,1\}$, we can write

$$p\left(m_E|a\right) = \begin{cases} 1 - P_{\rm err} & m_E = a \\ P_{\rm err} & m_E \neq a \end{cases} \tag{20}$$

and we can easily retrieve the conditional probability

$$p\left(y_B, m_E\right) = \frac{1}{2}\sum_a p\left(y_B|a\right)\,p\left(m_E|a\right). \tag{21}$$

Eve's outcome being discrete, the expression for the conditional entropy now reads

$$H(B|E) = -\frac{1}{2}\sum_{m_E}\int_{\mathbb{R}} {\rm d}y_B\, p\left(y_B|m_E\right)\log_2 p\left(y_B|m_E\right), \tag{22}$$

where we used $p(y_B, m_E) = p(y_B|m_E)p(m_E)$ and $p(m_E) = 1/2$. The explicit analytical expression of equation (22) is complicated and results in a lengthy integral which is not analytically solvable. However, to obtain a closed-form approximate result, one may again enforce the limit of large eavesdropper's advantage, $\mathscr{E} \gg 1$ or, equivalently, $\delta_B \ll 1$ due to equation (10). If one expands the probabilities up to second order in δ_B, equation (22) reduces to

$$H(B|E) = \frac{1}{2\ln 2}\int_{\mathbb{R}} {\rm d}y_B\,\frac{{\rm e}^{-y_B^2/2}}{\sqrt{2\pi}}\left\{\left(y_B^2 + \ln 2\pi\right) + \delta_B^2\,\frac{y_B^4 + y_B^2\left[\ln 2\pi - 5 + 2\,{\rm e}^{-\left(\delta_E^{\rm coh}\right)^2}\right] + 2 - \ln 2\pi}{2}\right\} \tag{23}$$

and can now be evaluated analytically. By combining the result with equation (5) and plugging $\delta_B = \delta_E^{\rm coh}/\sqrt{\mathscr{E}}$, the key rate in equation (1) for the case of Eve performing optimal Helstrom measurements greatly simplifies to

$$\mathsf{K}^{\rm Helstrom}\left(\delta_E^{\rm coh}, \mathscr{E} \gg 1\right) = \frac{\log_2 e}{2\mathscr{E}}\cdot {\delta_E^{\rm coh}}^2 {\rm e}^{-\left(\delta_E^{\rm coh}\right)^2}. \tag{24}$$

The expression in equation (24) can now be maximized over $\delta_E^{\rm coh}$, which is equivalent to Alice choosing optimal values of energy n_0 and n_1 for the light pulses. This gives us a rather elegant result for the key rate secure against passive eavesdropping that depends only on $\mathscr{E}$:

$$\mathsf{K}^{\rm Helstrom}\left(\mathscr{E} \gg 1\right) \approx \frac{1}{e}\cdot\frac{\log_2 e}{2\mathscr{E}}. \tag{25}$$

Note that the key rate in equation (25) exhibits the same scaling with $\mathscr{E}$ as for direct/coherent detection in equation (12) but with a lower multiplicative factor due to the Helstrom measurement allowing for better state discrimination by Eve. Both the full numerical solution and approximate analytical key rate values are plotted in figure 2.

5. Collective eavesdropping

From the point of view of Eve, minimizing the key rate K in equation (1) entails maximizing her correlation with Bob's outcomes, quantified by the mutual information $I(B;E)$. Quantum theory provides a theoretical upper bound to this value given by the Holevo quantity $\chi(B;E)$ [23, 25], resulting in a generalized key rate expression

$$\mathsf{K}^{\text{Holevo}} = \max\left\{I(A;B) - \chi\left(B;E\right),\, 0\right\}. \tag{26}$$

On the one hand, here the mutual information $I(A;B)$ between Alice and Bob can be expressed as [7]

$$I(A;B) = \delta_{\text{B}}^2 \log_2 e - \int_{\mathbb{R}} \mathrm{d}t \frac{\mathrm{e}^{-(t-\delta_{\text{B}})^2/2}}{\sqrt{2\pi}} \log_2\left[\cosh\left(\delta_{\text{B}} t\right)\right], \tag{27}$$

where δ_B has been introduced in the previous sections. On the other hand, the Holevo quantity $\chi(B;E)$ between Bob and Eve quantifies the maximal amount of information that Eve can learn about Bob's classical variable B from the received quantum states, optimized over all possible quantum operations that she can perform. This includes collective attacks in which she may store the collected states in a quantum memory and measure them jointly later, which can in theory give her more information than individual round-by-round measurements [26]. The Holevo quantity is defined as

$$\chi\left(B;E\right) = S\left[\rho_{\text{E}}\right] - \int_{\mathbb{R}} \mathrm{d}y_{\text{B}}\, p\left(y_{\text{B}}\right) S\left[\rho_{\text{E}|\text{B}=y_{\text{B}}}\right], \tag{28}$$

where $S[\rho] = -\mathrm{Tr}\left(\rho \log_2 \rho\right)$ is the von Neumann entropy of a quantum state ρ,

$$\rho_{\text{E}} = \frac{1}{2}\sum_a \left|\sqrt{\tau_{\text{E}} n_a}\right\rangle \left\langle\sqrt{\tau_{\text{E}} n_a}\right|_{\text{E}}, \tag{29}$$

is the overall state received by Eve, which is a mixture of two coherent states, whereas $\rho_{\text{E}|\text{B}=y_{\text{B}}}$ is her state conditioned on Bob's outcome y_{B}.

In order to calculate $\chi(B;E)$ we start from the tripartite state after Alice's transmission, that, since we are in the presence of coherent states, can be written as [27]

$$\rho_{\text{ABE}}^{(\text{in})} = \frac{1}{2}\sum_a \rho_a^{(\text{A})} \otimes \rho_a^{(\text{B})} \otimes \rho_a^{(\text{E})}, \tag{30}$$

where $\rho_a^{(K)} = \left|\sqrt{\tau_K n_a}\right\rangle \left\langle\sqrt{\tau_K n_a}\right|_K$ is the state received by $K \in \{B,E\}$ given the input signal $\rho_a^{(A)} = |a\rangle\langle a|_A$, with $a \in \{0,1\}$ as usual. After Bob performs DD, the state transforms to

$$\rho_{\text{ABE}} = \frac{1}{2}\sum_a \rho_a^{(\text{A})} \otimes \rho_{\text{B}|\text{A}=a} \otimes \rho_a^{(\text{E})}, \tag{31}$$

where his part is now a classical mixture of outcomes y_{B} distributed according to equation (2) and denoted by orthogonal states $|y_{\text{B}}\rangle$,

$$\rho_{\text{B}|\text{A}=a} = \int_{\mathbb{R}} \mathrm{d}y_{\text{B}} \frac{\mathrm{e}^{-[y_{\text{B}}+(-1)^a\delta_{\text{B}}]^2/2}}{\sqrt{2\pi}} \left|y_{\text{B}}\right\rangle \left\langle y_{\text{B}}\right|. \tag{32}$$

Thereafter, we have the following joint state of Bob and Eve

$$\rho_{\text{BE}} = \mathrm{Tr}_{\text{A}}\left(\rho_{\text{ABE}}\right) = \int_{\mathbb{R}} \mathrm{d}y_{\text{B}}\, p\left(y_{\text{B}}\right) \left|y_{\text{B}}\right\rangle \left\langle y_{\text{B}}\right| \otimes \rho_{\text{E}|\text{B}=y_{\text{B}}}, \tag{33}$$

where

$$p\left(y_{\text{B}}\right) = \frac{1}{2}\sum_a \frac{\mathrm{e}^{-[y_{\text{B}}+(-1)^a\delta_{\text{B}}]^2/2}}{\sqrt{2\pi}} \tag{34}$$

and

$$\rho_{\text{E}|\text{B}=y_{\text{B}}} = \frac{\sum_a \mathrm{e}^{-[y_{\text{B}}+(-1)^a\delta_{\text{B}}]^2/2} \rho_a^{(E)}}{\sum_a \mathrm{e}^{-[y_{\text{B}}+(-1)^a\delta_{\text{B}}]^2/2}}. \tag{35}$$

In summary, both ρ_{E} and $\rho_{\mathrm{E}|\mathrm{B}=y_{\mathrm{B}}}$ appearing in equation (28) are mixtures of two coherent states. Since the von Neumann entropy of a general mixture of two coherent states $\rho = p\,|\alpha\rangle\langle\alpha| + (1-p)\,|\beta\rangle\langle\beta|$ is given by

$$S[\rho] = h\left[\frac{1-\sqrt{1-4p(1-p)\left(1-|\langle\alpha|\beta\rangle|^2\right)}}{2}\right], \tag{36}$$

where $h[x] = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function, one can straightforwardly calculate the entropies $S[\rho_{\mathrm{E}}]$ and $S[\rho_{\mathrm{E}|\mathrm{B}=y_{\mathrm{B}}}]$ in equation (28).

Given $I(A;B)$ and $\chi(B;E)$, the key rate expression can now be optimized numerically; nevertheless, one may again determine an approximate expression valid for strong eavesdropping by expanding the integrands up to second order in δ_{B} and optimizing over δ_{E}. The result, depicted in figure 2, is seen to follow the same scaling with $\mathscr{E}$ as in the previous cases of sections 2–4,

$$\mathsf{K}^{\mathrm{Holevo}}\left(\mathscr{E} \gg 1\right) \approx \chi \cdot \frac{\log_2 e}{2\mathscr{E}}, \tag{37}$$

with

$$\chi = \max_{\delta \geqslant 0}\left\{\delta^2\left[1 - 2\coth^{-1}\left(\mathrm{e}^{\delta^2/2}\right)\sinh\left(\delta^2/2\right)\right]\right\} \approx 0.2683. \tag{38}$$

Crucially, the key rate is further reduced by a multiplicative factor when compared to direct/coherent detection and the Helstrom measurement, but the scaling with $\mathscr{E}$ still remains the same.

6. Discussion

We have analyzed the asymptotic information-theoretic key generation rates attainable by OKD, assuming the regime of macroscopic signal strengths and Gaussian photocount statistics, in the presence of a malicious passive eavesdropper with general capabilities. These include coherent eavesdropping with homodyne detection, shown to be equivalent to the DD scenario, and generalized quantum strategies: the Helstrom measurement minimizing the state discrimination error probability and measurements saturating the ultimate Holevo bound on accessible information. In both of the quantum-enhanced cases the attainable key rate values are reduced, but only by multiplicative factors compared to direct and coherent detection, while following the same asymptotic scaling with a parameter quantifying the eavesdropper's advantage. In conclusion, granting the passive eavesdropper enhanced quantum capabilities does not prohibit secure key distribution between the honest parties using the OKD protocol. Remarkably, the crucial restriction of passive eavesdropping imposed on Eve in OKD is enough to provide strong security guarantees, even if she is allowed to perform arbitrary quantum operations on her intercepted signal.

It is interesting to note that in the regime of strong eavesdropping, $\mathscr{E} \gg 1$, we found the same scaling $1/\mathscr{E}$ for all the considered strategies of Eve, with more powerful quantum eavesdropping resulting only in lower multiplicative prefactors in the key rate formulas. Intuitively, this may result from the following interplay. First of all, the passive eavesdropping model and the use of coherent states as information carriers result in limited correlation between Bob's and Eve's outcomes given the value of a, as although Eve can improve her state discrimination power, she cannot influence the random result obtained by Bob. Second of all, we observe in all the cases that it is optimal for Alice to choose a modulation depth on the order of $\delta_{\mathrm{E}} \approx 1$, equivalent to the phase space separation of Eve's received coherent states. In this regime, quantum-enhanced measurements are not expected to qualitatively change Eve's distinguishability, in contrast to the limit of vanishing state separation where they offer a fundamental advantage over classical detection [23]. To further elucidate this phenomenon, more research into the interplay of quantum and classical protocols is needed.

There are multiple other interesting directions to explore in relation to this work. While this is a fundamental study of the protocol limits under quantum passive eavesdropping, it would be interesting to see how practical considerations such as finite-size effects, limited reconciliation efficiency, or the use of hard decoding [7] would influence the attainable key rates. In terms of phase control discussed in the section on coherent eavesdropping, one could study the effect of imperfect phase randomization of Alice's states or information leakage through a residual correlation between phase and signal strength. One could also consider the use of quantum signals by Alice, such as displaced squeezed

states, or other photon-number-resolving-based strategies for Eve like the weak-field homodyne detection [28]. Finally, equipping Bob with quantum-enhanced capabilities could improve the attainable rates, but would move the protocol away from its attractive simplicity and integrability with modern communications infrastructure.

Acknowledgments

The authors would like to thank Mateusz Kucharczyk, Patryk Urban, and Mateusz Borkowski for insightful discussions.

Data availability statement

The data that support the findings of this study are available upon reasonable request from the authors. The data comprises solutions to equations which are stated in the text and thus easily reproducible by other researchers.

Funding

This work was supported by the Polish Ministry of Education and Science under the 'Quantum strategies in communication through noisy optical channels' Project No. PN/01/0204/2022 carried out within the 'Pearls of Science' program. The "Quantum Optical Technologies" (FENG.02.01-IP.05-0017/23) project is carried out within the Measure 2.1 International Research Agendas programme of the Foundation for Polish Science, co-financed by the European Union under the European Funds for Smart Economy 2021-2027 (FENG).

Appendix. Validation of approximations and small signal strength behavior

In the main text we derived compact key rate expressions owing to the assumption of macroscopic pulse intensities measured by Bob's and Eve's detectors, $\tau_{\mathrm{B/E}}\, n_a \gg 1$, which allowed us to approximate the Poissonian statistics of photodetection with normal distributions. Moreover, we constricted Alice's modulation depth to be small, meaning that her two transmitted signal strengths are similar, $n_0 \approx n_1$, in order to prevent unambiguous detection of the bit value by Bob and Eve. This and the fact that photocount variance generally scales proportionally with the signal strength prompted another simplifying approximation in which we set the same variance value for both the 0 and 1 pulse as a function of $\bar{n} = (n_0 + n_1)/2$ only. To assess the validity of these simplifications, in this appendix we compare the main text results with an exact numerical treatment. By doing so, we also show how the key rates behave in the regime of small signal strengths. Below we first explain the necessary changes to the main text derivations if one were to drop the above approximations. Next we plot the comparison of approximated and exact calculations and show that the two converge quickly with increasing signal strength.

The protocol structure remains the same: in each OKD round Alice transmits one of two coherent states with an average number of photons $n_a \in \{n_0, n_1\}$ and equal probability $p(a) = 1/2$, after which Bob performs DD of the received pulses attenuated by transmission τ_{B}. At the shot noise level his number of photocounts k_{B} is then distributed according to a Poisson distribution with mean $\tau_{\mathrm{B}} n_a$ dependent on the value of a. One may consider Bob's detection to be noisy and have his outcome be a sum of signal and noise random variables. A natural choice is to model the latter also as an independent Poisson process with mean $\sigma^2_{\mathrm{B,ex}}$, which is characteristic of DD in the presence of dark counts or thermal radiation. As a result, Bob's exact outcome is distributed as $k^{\mathrm{P}}_{\mathrm{B}}|a \sim \mathrm{Pois}(\tau_{\mathrm{B}} n_a + \sigma^2_{\mathrm{B,ex}})$ and its probability mass function reads

$$p\left(k^{\mathrm{P}}_{\mathrm{B}}|a\right) = \frac{\exp\left(-\tau_{\mathrm{B}} n_a - \sigma^2_{\mathrm{B,ex}}\right) \cdot \left[\tau_{\mathrm{B}} n_a + \sigma^2_{\mathrm{B,ex}}\right]^{k^{\mathrm{P}}_{\mathrm{B}}}}{k^{\mathrm{P}}_{\mathrm{B}}!} \tag{39}$$

with both the mean and variance equal to $\tau_{\mathrm{B}} n_a + \sigma^2_{\mathrm{B,ex}}$. Depending on the chosen scenario, other forms of contributing noise could also be considered here, which would necessitate a different form of Bob's

outcome distribution. Note that in the main text, excess noise was modeled simply by adding a factor $\sigma^2_{\mathrm{B,ex}}$ to the Gaussian outcome variance.

Apart from Alice and Bob, the protocol assumes the presence of a passive eavesdropper Eve measuring pulses attenuated by transmission τ_{E}, who we have equipped in the main text with increasingly enhanced detection capabilities. As is customary in security analysis, Eve's detection has no excess noise to cover for the worst-case scenario. If she performs DD, her exact outcome is now $k^{\mathrm{P}}_{\mathrm{E}} \sim \mathrm{Pois}(\tau_{\mathrm{E}} n_a)$, i.e. a shot-noise limited Poisson random variable with mean and variance dependent on a. If Eve performs coherent detection as in section 3 or minimum-error state discrimination as in section 4, her outcome distributions in equations (14) and (20) do not change, as we did not need to enforce any approximation for these cases. Finally, if Eve is equipped with collective eavesdropping as in section 5, in the derivation one needs to replace Bob's conditional state in equation (32) with

$$\rho_{\mathrm{B}|\mathrm{A}=a} = \sum_{k^{\mathrm{P}}_{\mathrm{B}}=0}^{\infty} p\left(k^{\mathrm{P}}_{\mathrm{B}}|a\right) |k^{\mathrm{P}}_{\mathrm{B}}\rangle \langle k^{\mathrm{P}}_{\mathrm{B}}| \tag{40}$$

and update the following expressions of section 5 accordingly.

Without the opportunity for simplification of the formulas through approximations, one has to express the key generation rates as functions of the exact outcome probability distributions and calculate them numerically. For the sake of completeness, let us list the full expressions to be used. For individual attacks in equation (1) one now takes

$$H(B|A) = -\sum_a p(a) \left(\sum_{k^{\mathrm{P}}_{\mathrm{B}}=0}^{\infty} p\left(k^{\mathrm{P}}_{\mathrm{B}}|a\right) \log_2 p\left(k^{\mathrm{P}}_{\mathrm{B}}|a\right) \right) \tag{41}$$

and, if Eve performs DD,

$$H(B|E) = -\sum_{k^{\mathrm{P}}_{\mathrm{E}},k^{\mathrm{P}}_{\mathrm{B}}=0}^{\infty} p\left(k^{\mathrm{P}}_{\mathrm{B}},k^{\mathrm{P}}_{\mathrm{E}}\right) \log_2 \frac{p\left(k^{\mathrm{P}}_{\mathrm{B}},k^{\mathrm{P}}_{\mathrm{E}}\right)}{p\left(k^{\mathrm{P}}_{\mathrm{E}}\right)} \tag{42}$$

with $p(k^{\mathrm{P}}_{\mathrm{B}},k^{\mathrm{P}}_{\mathrm{E}}) = \sum_a p(a)p(k^{\mathrm{P}}_{\mathrm{B}}|a)p(k^{\mathrm{P}}_{\mathrm{E}}|a)$ and $p(k^{\mathrm{P}}_{\mathrm{E}}) = \sum_a p(a)p(k^{\mathrm{P}}_{\mathrm{E}}|a)$. If Eve performs the Helstrom measurement, her outcome is still discrete but now has two values $m_{\mathrm{E}} \in \{0,1\}$ distributed as in equation (20) and one needs to substitute $k^{\mathrm{P}}_{\mathrm{E}}$ for m_{E} in the above formula. For Eve with coherent detection capabilities, her outcome is continuous and her conditional probability $p(y^{\mathrm{coh}}_{\mathrm{E}}|a)$ is given by equation (16), in which case

$$H(B|E) = -\sum_{k^{\mathrm{P}}_{\mathrm{B}}=0}^{\infty} \int_{\mathbb{R}} \mathrm{d}y^{\mathrm{coh}}_{\mathrm{E}}\, p\left(k^{\mathrm{P}}_{\mathrm{B}},y^{\mathrm{coh}}_{\mathrm{E}}\right) \log_2 \frac{p\left(k^{\mathrm{P}}_{\mathrm{B}},y^{\mathrm{coh}}_{\mathrm{E}}\right)}{p\left(y^{\mathrm{coh}}_{\mathrm{E}}\right)} \tag{43}$$

with $p(k^{\mathrm{P}}_{\mathrm{B}},y^{\mathrm{coh}}_{\mathrm{E}}) = \sum_a p(a)p(k^{\mathrm{P}}_{\mathrm{B}}|a)p(y^{\mathrm{coh}}_{\mathrm{E}}|a)$ and $p(y^{\mathrm{coh}}_{\mathrm{E}}) = \sum_a p(a)p(y^{\mathrm{coh}}_{\mathrm{E}}|a)$. Finally, for collective attacks in equation (26) one resorts to the full expression

$$I(A;B) = \sum_a \sum_{k^{\mathrm{P}}_{\mathrm{B}}=0}^{\infty} p\left(a,k^{\mathrm{P}}_{\mathrm{B}}\right) \log_2 \left(\frac{p\left(a,k^{\mathrm{P}}_{\mathrm{B}}\right)}{p(a)\,p\left(k^{\mathrm{P}}_{\mathrm{B}}\right)} \right) \tag{44}$$

with $p(a,k^{\mathrm{P}}_{\mathrm{B}}) = p(a)p(k^{\mathrm{P}}_{\mathrm{B}}|a)$ and $p(k_{\mathrm{B}}) = \sum_a p(a,k^{\mathrm{P}}_{\mathrm{B}})$, while the calculation of $\chi(B;E)$ proceeds again as a difference of two von Neuman entropies of coherent state mixtures, only with Bob's exact outcome probability distribution $p(k^{\mathrm{P}}_{\mathrm{B}}|a)$ used in place of the approximated Gaussian one.

The lack of approximations makes life harder in two ways. First of all, exact calculations of the above expressions call for infinite sums and integrals to be computed. To circumvent that, we proceed each time by calculating these numerically with a high enough upper limit and precision that raising them further does not influence the results anymore. Second of all, while previously key rate expressions were derived as functions of a single eavesdropper's advantage parameter $\mathscr{E}$, now they are functions of individual parameters including transmissions τ_{B}, τ_{E}, excess noise $\sigma^2_{\mathrm{B,ex}}$, and transmitted pulse intensities n_0 and n_1.

Figure 3 plots the attainable key generation rates K secure against passive eavesdropping as a function of Bob's average signal strength $\tau_{\mathrm{B}}\bar{n}$ for four representative cases of either Eve highly attenuated with respect to Bob, $\tau_{\mathrm{E}}/\tau_{\mathrm{B}} = 0.1$, or Bob with respect to Eve, $\tau_{\mathrm{E}}/\tau_{\mathrm{B}} = 10$, and either nonzero excess noise in

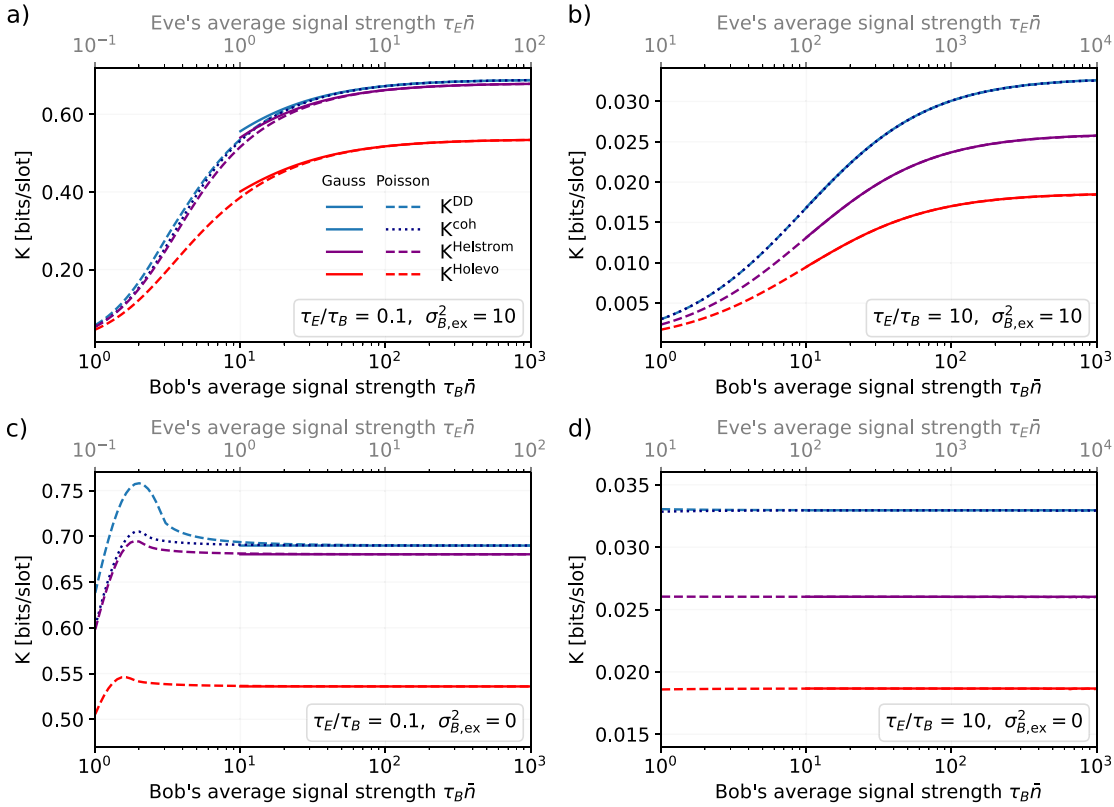

Figure 3. Comparison of key generation rates of the model derived in the main text under macroscopic pulse strength and small modulation depth approximations (solid lines) with an exact model delineated in the appendix (dashed and dotted lines) for select representative cases of the τ_E/τ_B ratio and excess noise $\sigma^2_{B,ex}$.

Bob's measurement, $\sigma^2_{B,ex} = 10$, or noiseless DD, $\sigma^2_{B,ex} = 0$. The exact values of key generation rates calculated according to the prescription in this appendix are plotted with dashed and dotted lines, where for each $\tau_B\bar{n}$, the values of $\tau_B n_0$ and $\tau_E n_1$ are optimized for highest K. Additionally, the approximate key rate formulas derived in the main text under the macroscopic pulse strength and small modulation depth assumptions are plotted with solid lines from $\tau_B\bar{n} = 10$ onwards, as from roughly this value one can generally start to approximate Poissonian distributions with Gaussians. In this case, for each $\tau_B\bar{n}$ and the values of τ_E/τ_B and $\sigma^2_{B,ex}$ we calculate $\mathscr{E}$ according to equation (11) and plot the key rates derived as functions of $\mathscr{E}$ in section 2 through 5. In subfigures (a) and (b) the nonzero excess-noise-related penalty to $\mathscr{E}$ in equation (11) ranges from high to small throughout the plotted range. In the noiseless case of subfigures (c) and (d), $\mathscr{E}$ no longer depends on $\tau_B\bar{n}$, which results in constant values for the solid Gaussian lines.

The exact and approximate values are seen to closely coincide with each other already very well at medium photon numbers, $\tau_{B/E}\bar{n} \approx 10$, and reach excellent agreement with increasing $\tau_B\bar{n}$. This validates the main text assumptions and shows that the key rate formulas derived therein are quite general and fully applicable. In addition to showing that, the plot elucidates the small signal strength behavior of OKD with enhanced passive eavesdropping. Crucially, if a constant value of excess noise is present, it is seen that key rates generally increase with signal strength due to the corresponding decrease of the eavesdropper's advantage $\mathscr{E}$, which is at its lowest when shot noise dominates over excess noise in Bob's measurement.

ORCID iDs

Karol Łukanowski 0000-0001-7460-3363
Michał Wójcik 0009-0005-6872-9476
Stefano Olivares 0000-0002-9251-0731
Konrad Banaszek 0000-0002-5389-6897
Marcin Jarzyna 0000-0001-9989-1648

References

[1] Stallings W 2020 *Cryptography and Network Security: Principles and Practice* 8th edn (Pearson Education)
[2] Shor P W 1997 *SIAM J. Comp.* **26** 1484–509
[3] Banaszek K, Kucharczyk M, Łukanowski K and Jarzyna M 2025 Quantum-safe physical layer security in optical networks *25th Anniversary Int. Conf. on Transparent Optical Networks (ICTON)* (IEEE) pp 1–4
[4] Pirandola S, Andersen U L, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C and Ottaviani C 2020 *Adv. Opt. Photonics* **12** 1012–236
[5] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 15043
[6] Ikuta T and Inoue K 2016 *New J. Phys.* **18** 013018
[7] Banaszek K, Jachura M, Kolenderski P and Lasota M 2021 *Opt. Express* **29** 43091
[8] Jachura M, Szlachetka J, Kucharczyk M, Jarzyna M, Kolenderski P, Turkiewicz J P and Banaszek K 2024 Simultaneous IM/DD data transmission and high-rate secret key distribution over a single C-band channel *Optical Fiber Communication Conf. (OFC) 2024* (Optica Publishing Group) p W1H.6
[9] Czerwinski A, Lasota M, Jarzyna M, Kucharczyk M, Jachura M and Banaszek K 2026 *IEEE J. Sel. Top. Quantum Electron.* **32** 1–13
[10] Jachura M, Lasota M, Kolenderski P and Banaszek K 2023 Modelling concurrent IM/DD key distribution and data transmission over an optical LEO-to-ground link *Int. Conf. on Space Optics–ICSO 2022* vol 12777 (SPIE) pp 568–74
[11] Łukanowski K, Kucharczyk M, Jachura M, Jarzyna M and Banaszek K 2025 Physical layer security for photon-starved communication links *Int. Conf. on Space Optics — ICSO 2024* F Bernard, N Karafolas, P Kubik and K Minoglou (SPIE) p 237
[12] Kucharczyk M, Turkiewicz J P, Kowalik K, Stabrawa A, Urban P and Banaszek K 2026 Securing physical layer of access networks with optical key distribution *31st Optoelectronics And Communications Conf. (OECC), Session Tu3a* (paper Tu3A-1)
[13] Karlsson S, Lin R, Wosinska L and Monti P 2022 Eavesdropping G.652 vs. G.657 fibres: a performance comparison 2022 *Int. Conf. on Optical Network Design and Modeling (ONDM)* (IEEE) pp 1–3
[14] Bloch M and Barros J 2011 *Physical-Layer Security: From Information Theory to Security Engineering* (Cambridge University Press)
[15] Dolinar S J 1973 *MIT Research Laboratory of Electronics Quarterly Progress Report* vol 111 pp 115–20
[16] Cover T M and Thomas J A 2005 *Elements of Information Theory* (Wiley)
[17] Portmann C and Renner R 2022 *Rev. Mod. Phys.* **94** 1539–0756
[18] Elkouss D, Martínez Mateo J and Martin V 2010 *Quantum Inf. Comput.* **11** 226–38
[19] Lo H K and Preskill J 2007 *Quantum Inf. Comput.* **7** 431–58
[20] Currás-Lorenzo G, Nahar S, Lütkenhaus N, Tamaki K and Curty M 2023 *Quantum Sci. Technol.* **9** 015025
[21] Zhao Y, Qi B and Lo H K 2007 *Appl. Phys. Lett.* **90** 2432296
[22] Lo Y S, Brzosko A H, Smith P R, Woodward R I, Marangon D G, Dynes J F, Juárez S, Paraïso T K, Stevenson R M and Shields A J 2026 Phase-randomized laser pulse generation at 10 GHz for quantum photonic applications (arXiv:2601.04031)
[23] Banaszek K, Kunz L, Jachura M and Jarzyna M 2020 *J. Lightwave Technol.* **38** 2741–54
[24] Helstrom C W 1969 *J. Stat. Phys.* **1** 231–52
[25] Holevo A S 1973 *Probl. Inf. Transm.* **9** 177–83
[26] Preskill J 2004 Lecture notes for physics 219: quantum computation, Chapter 10. Quantum Shannon Theory (available at: www.preskill.caltech.edu/ph219/)
[27] Olivares S 2021 *Phys. Lett. A* **418** 127720
[28] Notarnicola M N and Olivares S 2025 *IEEE J. Sel. Areas Commun.* **43** 1524–35