Sixto et al. *EPJ Quantum Technology* (2023) 10:53
https://doi.org/10.1140/epjqt/s40507-023-00210-0

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Secret key rate bounds for quantum key distribution with faulty active phase randomization

Xoel Sixto[1,2,3*], Guillermo Currás-Lorenzo[1,2,3,4], Kiyoshi Tamaki[4] and Marcos Curty[1,2,3]

*Correspondence:
xsixto@vqcc.uvigo.es
[1]Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain
[2]Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain
Full list of author information is available at the end of the article

Abstract

Decoy-state quantum key distribution (QKD) is undoubtedly the most efficient solution to handle multi-photon signals emitted by laser sources, and provides the same secret key rate scaling as ideal single-photon sources. It requires, however, that the phase of each emitted pulse is uniformly random. This might be difficult to guarantee in practice, due to inevitable device imperfections and/or the use of an external phase modulator for phase randomization in an active setup, which limits the possible selected phases to a finite set. Here, we investigate the security of decoy-state QKD when the phase is actively randomized by faulty devices, and show that this technique is quite robust to deviations from the ideal uniformly random scenario. For this, we combine a novel parameter estimation technique based on semi-definite programming, with the use of basis mismatched events, to tightly estimate the parameters that determine the achievable secret key rate. In doing so, we demonstrate that our analysis can significantly outperform previous results that address more restricted scenarios.

Keywords: Quantum key distribution; Decoy state; Phase randomization; Source imperfections

1 Introduction

Quantum key distribution (QKD) is a method for securely establishing symmetric cryptographic keys between two distant parties (so-called Alice and Bob) [1–3]. Its security is based on principles of quantum mechanics, such as the no-cloning theorem [4], which guarantee that any attempt by an eavesdropper (Eve) to learn information about the distributed key inevitably introduces detectable errors. Importantly, when combined with the one-time-pad encryption scheme [5], QKD provides information-theoretically secure communications.

The field of QKD has made much progress in recent years, both theoretically and experimentally, leading to the first deployments of metropolitan and intercity QKD networks [6–9]. Despite these remarkable achievements, there are still certain challenges that need to be overcome for the widespread adoption of this technology. One of these challenges is to close the existing security gap between theory and practice. This is so because QKD

security proofs, typically consider assumptions that the actual experimental implementations do not satisfy. Such discrepancies could create security loopholes or so-called side channels, which might be exploited by Eve to compromise the security of the generated key without being detected.

Indeed, practical QKD transmitters usually emit phase-randomized weak coherent pulses (PR-WCPs) generated by laser sources. These pulses might contain more than one photon prepared in the same quantum state. In this scenario, Eve is no longer limited by the no-cloning theorem, because multi-photon signals provide her with perfect copies of the signal photon. As a result, it can be shown that the secret key rate of the BB84 protocol [10] with PR-WCPs scales quadratically with the system's transmittance due to the photon-number-splitting (PNS) attack [11, 12]. This attack provides Eve with full information about the part of the key generated with the multi-photon pulses, without introducing any error.

To overcome this limitation, the most efficient solution today is undoubtedly the decoy-state method [13–15], in which Alice varies at random the intensity of the PR-WCPs that she sends to Bob. This allows them to better estimate the behavior of the quantum channel. Indeed, using the observed measurement statistics associated to different intensity settings, Alice and Bob can tightly estimate the yield and phase error rate of the single-photon pulses, from which the secret key is actually distilled. As a result, the decoy-state method delivers a secret key rate that scales linearly with the channel transmittance [13–16], matching the scaling achievable with ideal single-photon sources. This technique has been extensively demonstrated in multiple recent experiments [17–23], including satellite links [24, 25] and the use of photonic integrated circuits [26–29]. Also, decoy-state QKD setups are currently offered commercially by several companies [30–34], which highlights its importance.

Importantly, standard decoy-state security proofs assume perfect phase randomization, *i.e.*, that the phase, θ, of each generated WCP is uniformly random in $[0, 2\pi)$. That is, its probability density function (PDF), $g(\theta)$, should satisfy $g(\theta) = 1/2\pi$. However, none of the two main methods used today to generate PR-WCPs, namely passive and active, fulfill this condition exactly. In the passive scheme a technique known as gain-switching is used to effectively turn the laser on and off between pulses. However, in these configurations [20, 22, 23, 35–38], device imperfections can prevent the phases θ from being uniformly distributed. In the active scheme [26, 27, 39, 40], an external phase modulator is used to imprint one of N possible random values to the phase of each pulse, such that only a discrete number of phases is selected. Both scenarios violate a crucial assumption of the decoy-state technique.

The security of QKD with imperfect passive phase randomization has, under certain assumptions, been recently demonstrated in [41]. This analysis however, is not applicable to the numerous existing active setups that rely on an external phase modulator for phase randomization .[1] The security of the latter approach has been analyzed in [42] (see also [43]), but these works restrict themselves to the case in which the discrete random phases

[1] This is because the analysis in [41] requires that there is a known non-zero parameter q such that $g(\theta) \geq q$ for all $\theta \in [0, 2\pi)$. In the case of active phase randomization, only a discrete number of phases is selected, and therefore there might be many values $\theta \in [0, 2\pi)$ such that $g(\theta) = 0$.

are evenly distributed in $[0, 2\pi)$, *i.e.*, they assume that $g(\theta)$ satisfies

$$g(\theta) = \frac{1}{N}\sum_{k=0}^{N-1}\delta(\theta - \theta_k), \tag{1}$$

where $\delta(x)$ represents the Dirac delta function, and $\theta_k = 2\pi k/N$, with N being the total number of selected phases. Under this assumption, [42] shows that it is possible to approximate the secret key rate achievable in the ideal situation where $g(\theta) = 1/2\pi$, with around $N = 10$ random phases. While this result is remarkable, in practice, inevitable imperfections of the phase modulator and electronic noise might prevent the phases θ from being *exactly* evenly distributed, thus invalidating the application of the results presented in [42] to a real setup.

The main contributions of this paper are as follows. First, we introduce an analysis that can be applied in the more realistic and practical scenario in which $g(\theta)$ is an arbitrary PDF, due to imperfections in the active phase randomization process, and we provide asymptotic secret key rates for this general situation, thus filling an important gap in the literature.

Second, we show that this analysis can be applied in the scenario in which the PDF $g(\theta)$ is not fully characterized. This feature significantly simplifies the applicability of our results to a practical setup, where an accurate characterization of the PDF describing the phase might be challenging.

Third, we make a noteworthy finding regarding the utilization of basis mismatched events which are typically discarded in QKD security analyses, including that in [42]. The use of basis mismatched events is already known to provide a key-rate advantage in the presence of bit-and-basis encoding flaws [44] but here, we show that they can also be advantageous in the presence of imperfections due to a faulty phase randomization process. We believe that this additional result is highly nontrivial as intuitively the decoy state method has no relation with the state preparation flaw in encoding the bit information.

Fourth, when considering the ideal discrete-phase-randomization case described by Eq. (1), our analysis delivers considerably higher secret key rates than those provided by the seminal work in [42], or to put it in other words, it requires to spend fewer random bits for phase selection to achieve an equivalent performance.

As a side remark, we note that our results are also useful for other quantum communication schemes that go beyond QKD and employ laser sources, as they often rely on decoy-states with active phase randomization.

Finally, it is worth mentioning that, although, for simplicity, in our derivations we consider collective attacks, our analysis can be lifted to general attacks by applying the extension of the quantum de Finetti theorem [45] to infinitely-dimensional systems [46]. Because of this, the asymptotic key rates that we derive in this paper are also valid against general attacks.

The paper is organized as follows. In Sect. 2.1, we describe the quantum states emitted by Alice when θ follows an arbitrary PDF, $g(\theta)$. Then, in Sect. 2.2 we introduce the decoy-state protocol considered, together with its asymptotic secret key rate formula. Next, in Sect. 2.3, we present the parameter estimation technique based on SDP, as well as on the use of basis mismatched events, to calculate the different parameters required to evaluate the secret key rate. Then, in Sect. 3 we simulate the achievable secret key rate for various

functions $g(\theta)$ of practical interest, both for the cases in which this function is fully (or only partially) characterized. Section 4 concludes the paper with a summary. The paper includes as well some Appendixes with additional calculations.

2 Methods

2.1 Phase randomization with an arbitrary $g(\theta)$

In this section, we describe the quantum states emitted by Alice when each of them has a phase θ that follows an arbitrary PDF, $g(\theta)$.

In particular, a WCP of intensity μ and phase θ can be written in terms of the Fock basis as

$$\left|\sqrt{\mu}e^{i\theta}\right\rangle = e^{-\frac{\mu}{2}} \sum_{n=0}^{\infty} \frac{(\sqrt{\mu}e^{i\theta})^n}{\sqrt{n!}} |n\rangle, \tag{2}$$

where $|n\rangle$ represents a Fock state with n photons.

If Alice selects the phase θ of each generated signal independently and at random according to $g(\theta)$, its state is simply given by

$$\rho^{\mu}_{[g(\theta)]} = \int_0^{2\pi} g(\theta) \hat{P}\left(\left|\sqrt{\mu}e^{i\theta}\right\rangle\right) d\theta, \tag{3}$$

with $\hat{P}(|\phi\rangle) = |\phi\rangle\langle\phi|$.

Any quantum state can always be diagonalised in a certain orthonormal basis. For the states given by Eq. (3), we shall denote the elements of such basis by $|\psi_{n,\mu,g(\theta)}\rangle$, since, in general, they might depend on both the intensity μ and the function $g(\theta)$. Here, the subscript n simply identifies the different elements of the basis, which are not necessarily the Fock states. This means, in particular, that we can rewrite the states given by Eq. (3) as follows

$$\rho^{\mu}_{[g(\theta)]} = \sum_{n=0}^{\infty} p_{n|\mu,g(\theta)} \hat{P}\left(|\psi_{n,\mu,g(\theta)}\rangle\right), \tag{4}$$

where the coefficients $p_{n|\mu,g(\theta)} \geq 0$ satisfy $\sum_{n=0}^{\infty} p_{n|\mu,g(\theta)} = 1$. That is, these coefficients can be interpreted as the probability with which, in a certain time instance, Alice emits the state $|\psi_{n,\mu,g(\theta)}\rangle$, given that she chose the intensity μ and θ follows the PDF $g(\theta)$.

For instance, in the ideal scenario where $g(\theta)$ is uniformly random in $[0, 2\pi)$, the emitted signals are a Poisson mixture of Fock states given by

$$\rho^{\mu}_{[\frac{1}{2\pi}]} = \frac{1}{2\pi} \int_0^{2\pi} \hat{P}\left(\left|\sqrt{\mu}e^{i\theta}\right\rangle\right) d\theta = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} \hat{P}\left(|n\rangle\right), \tag{5}$$

i.e. $p_{n|\mu,1/2\pi} = e^{-\mu}\mu^n/(n!)$ and $|\psi_{n,\mu,1/2\pi}\rangle = |n\rangle$.

2.2 Protocol description and key generation rate

For concreteness, we shall assume that Alice and Bob implement a decoy-state BB84 scheme with three different intensity settings $\{s, \nu, \omega\}$ in each basis, with $s > \nu > \omega \geq 0$. Moreover, we consider that they generate secret key only from those events in which both

of them select the Z basis and Alice chooses the signal intensity setting s. This is the most typical configuration of the decoy-state BB84 protocol. We remark, however, that the analysis below could be straightforwardly adapted to other protocol configurations, or to other combinations of intensity settings.

In each round of the protocol, Alice probabilistically chooses a bit value $b \in \{0,1\}$ with probability $p_b = 1/2$, a basis $\alpha \in \{Z,X\}$ with probability p_α, an intensity value $\mu \in \{s,\nu,\omega\}$ with probability p_μ, and a random phase θ according to the PDF given by $g(\theta)$. Then, she generates a WCP of intensity μ and phase θ, $|\sqrt{\mu}e^{i\theta}\rangle$, and applies an operation that encodes her bit and basis choices b and α into the pulse. From Eve's perspective, these states are described by Eq. (4) due to her ignorance about the selected phase θ. On the receiving side, Bob measures each arriving signal using a basis $\alpha \in \{Z,X\}$, which he selects with probability p_α. We shall assume the basis independent detection efficiency condition throughout the paper. That is, the probability that Bob obtains a conclusive measurement outcome does not depend on his basis choice.

Once the quantum communication phase of the protocol ends, Alice and Bob broadcast (via an authenticated classical channel) both the intensity and basis settings selected for each detected signal. The results related to those detected signals in which both of them used the Z basis with intensity setting s constitute the sifted key. For the detected rounds in which Bob chose the X basis, Alice reveals her bit values b and Bob announces his corresponding measurement outcomes. This data is used for parameter estimation, *i.e.*, to determine the relevant quantities needed to evaluate the secret key rate formula. Finally, Alice and Bob apply error correction and privacy amplification to the sifted key to obtain a final secret key, following the standard post-processing procedure in QKD [1–3]. For a more detailed description of the protocol steps of a decoy-state BB84 scheme, we refer the reader to *e.g.* [16].

In the ideal scenario where $g(\theta) = 1/2\pi$, Alice's state preparation process is equivalent to emitting Fock states $|n\rangle$ with a Poisson distribution of mean equal to the intensity setting μ selected, as shown by Eq. (5). In this situation, both the single-photon and vacuum pulses with the intensity setting s contribute to secret bits [47]. The multi-photon signals are insecure due to the PNS attack. Similarly, when θ follows an arbitrary PDF, $g(\theta)$, and Alice chooses the intensity setting μ, from Eq. (4) we have that her state preparation process is equivalent to generating pure states $|\psi_{n,\mu,g(\theta)}\rangle$ with probability $p_{n|\mu,g(\theta)}$. The closer the function $g(\theta)$ is to a uniform distribution, the closer the signals (probabilities) $|\psi_{n,\mu,g(\theta)}\rangle$ ($p_{n|\mu,g(\theta)}$) are to the Fock states $|n\rangle$ (probabilities $e^{-\mu}\mu^n/n!$). In this scenario, Alice and Bob can in principle distill secret bits from any $|\psi_{n,\mu,g(\theta)}\rangle$ with $\mu = s$, though the main contribution would mainly arise from those with indexes $n = 0,1$, which are the ones closer to vacuum and single-photon pulses. These are the contributions that we consider below. Indeed, for the examples studied in Sect. 3, we have tested numerically that the improvement in key rate that can be obtained when considering $n > 1$ is negligible.

This means that, in this imperfect state preparation scenario, the asymptotic secret key rate formula for the decoy-state BB84 protocol considered can be written as [15, 47, 48]

$$\begin{aligned} R &\geq p_Z^2 p_s \left\{ \sum_{n=0}^{\infty} p_{n|s,g(\theta)} Y^Z_{n,s,g(\theta)} \left[1 - h(e_{n,s,g(\theta)})\right] - f Q^Z_{s,g(\theta)} h\left(E^Z_{s,g(\theta)}\right) \right\} \\ &\geq p_Z^2 p_s \left\{ \sum_{n=0}^{1} p^{\mathrm{L}}_{n|s,g(\theta)} Y^{Z,\mathrm{L}}_{n,s,g(\theta)} \left[1 - h\left(e^{\mathrm{U}}_{n,s,g(\theta)}\right)\right] - f Q^Z_{s,g(\theta)} h\left(E^Z_{s,g(\theta)}\right) \right\}, \end{aligned} \tag{6}$$

where $Y^Z_{n,s,g(\theta)}$ denotes the yield associated to the state $|\psi_{n,s,g(\theta)}\rangle$ encoded (and measured) in the Z basis, *i.e.*, the probability that Bob observes a detection click in his measurement apparatus conditioned on Alice and Bob selecting the Z basis and Alice preparing the state $|\psi_{n,s,g(\theta)}\rangle$; the parameter $e_{n,s,g(\theta)}$ represents the phase error rate of these latter signals; $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function; the quantity f is the efficiency of the error correction protocol; $Q^Z_{s,g(\theta)}$ is the overall gain of the signals emitted conditioned on Alice selecting the intensity s and Alice and Bob choosing the Z basis, *i.e.*, the probability that Bob observes a detection click conditioned on Alice sending him such signals; and $E^Z_{s,g(\theta)}$ is the overall quantum bit error rate (QBER) associated to these latter signals. Moreover, in Eq. (6), the superscript L (U) refers to a (an) lower (upper) bound.

The quantities $Q^Z_{s,g(\theta)}$ and $E^Z_{s,g(\theta)}$ are directly observed in the experiment. In principle, the probabilities $p_{n|s,g(\theta)}$ could also be known, and depend on the state preparation process. However, in practice it might be difficult to find their value analytically. Instead, in the next section we present a simple method to obtain a lower bound, $p^{\mathrm{L}}_{n|s,g(\theta)}$, on these quantities. There, we also explain how to estimate the parameters $Y^{Z,\mathrm{L}}_{n,s,g(\theta)}$ and $e^{\mathrm{U}}_{n,s,g(\theta)}$, with $n = 0, 1$, which are needed to evaluate Eq. (6).

2.3 Parameter estimation

The parameter estimation procedure presented here is an adaptation of the one very recently introduced in [41] in the context of phase correlations in a passive randomization setup. For simplicity, below we introduce the main results and refer the reader to Appendixes A and B for the detailed derivations.

2.3.1 Lower bound on the yields $Y^Z_{n,s,g(\theta)}$

In Appendix A it is shown that a lower bound on the yields $Y^Z_{n,s,g(\theta)}$ can be obtained by solving the following SDP:[2]

$$\begin{aligned} &\min_{J_Z} \ \mathrm{Tr}\big[\hat{P}\big(|\psi_{n,s,g(\theta)}\rangle\big)J_Z\big] \\ &\text{subject to } \ \mathrm{Tr}\big[\rho^{\mu}_{[g(\theta)]}J_Z\big] = Q^Z_{\mu,g(\theta)}, \quad \forall \mu \in \{s,\nu,\omega\} \\ &\qquad 0 \le J_Z \le \mathbb{I}. \end{aligned} \tag{7}$$

The states $|\psi_{n,s,g(\theta)}\rangle$ and $\rho^{\mu}_{[g(\theta)]}$ are known in principle but inaccessible and depend on the intensity setting selected by Alice and on the function $g(\theta)$. Also, as already mentioned, the gains $Q^Z_{\mu,g(\theta)}$ are directly observed experimentally in a realization of the protocol. That is, the only unknown in Eq. (7) is the positive semi-definite operator J_Z over which the minimization takes place. Let J^*_Z denote the solution to the SDP given by Eq. (7). Then, we find that

$$Y^Z_{n,s,g(\theta)} \ge \mathrm{Tr}\big[\hat{P}\big(|\psi_{n,s,g(\theta)}\rangle\big)J^*_Z\big] := Y^{Z,\mathrm{L}}_{n,s,g(\theta)}. \tag{8}$$

[2] From this point on, if we have two operators, say A and B by $A \le B$ we mean that $B - A \ge 0$, *i.e.* that $B - A$ is a positive semi-definite operator.

2.3.2 *Upper bound on the phase-error rates* $e_{n,s,g(\theta)}$

The phase-error rates, $e_{n,s,g(\theta)}$, are defined by means of a virtual protocol [49]. For this, we shall consider the standard assumption in which the efficiency of Bob's measurement is independent of his basis choice. Then, for those rounds in which both Alice and Bob select the Z basis and Alice generates the n-th eigenstate $|\psi_{n,s,g(\theta)}\rangle$, we can equivalently describe her state preparation process as follows. First, she prepares the following bipartite entangled state

$$\left|\Psi^{Z}_{n,s,g(\theta)}\right\rangle = \frac{1}{\sqrt{2}}\left(|0_Z\rangle_A \hat{V}_{0_Z} + |1_Z\rangle_A \hat{V}_{1_Z}\right)|\psi_{n,s,g(\theta)}\rangle, \tag{9}$$

where $\hat{V}_{b_\alpha}$, with $b = 0, 1$ and $\alpha \in \{Z, X\}$, denotes the encoding operation corresponding to the α basis and the bit value b. Although our analysis is valid for any $\{\hat{V}_{b_\alpha}\}$, for simplicity, in our simulations, we assume that these operators, are ideal BB84 encoding operators, given by $\hat{V}_{0_Z}|n\rangle = |n\rangle|0\rangle$, $\hat{V}_{1_Z}|n\rangle = |0\rangle|n\rangle$,

$$\begin{aligned}
\hat{V}_{0_X}|n\rangle &= \sum_k \frac{1}{\sqrt{2^n}}\sqrt{\binom{n}{k}}|k\rangle|n-k\rangle, \\
\hat{V}_{1_X}|n\rangle &= \sum_k (-1)^k \frac{1}{\sqrt{2^n}}\sqrt{\binom{n}{k}}|k\rangle|n-k\rangle.
\end{aligned} \tag{10}$$

We note that these operators are independent of the physical degree of freedom used for the encoding. For example, in a time-bin encoding setup, the first ket would represent the early time bin, and the second ket would represent the late time bin; while in a polarization-encoding setup, the first ket would represent the horizontally-polarized mode, and the second ket would represent the vertically-polarized mode.

Next, she measures her ancilla system A in Eq. (9) in the orthonormal basis $\{|0_Z\rangle, |1_Z\rangle\}$ to learn the bit value encoded, and sends the other system to Bob, who measures it in the Z basis.

In this situation, the phase-error rate $e_{n,s,g(\theta)}$ corresponds to the bit error rate that Alice and Bob would observe if Alice (Bob) instead performed an X basis measurement on the ancilla system A (arriving signal). If Alice performs a X basis measurement on her system A, this is equivalent to emitting the states

$$\left|\lambda^{\text{virtual}}_{\Delta,n,s,g(\theta)}\right\rangle \propto \left|\bar{\lambda}^{\text{virtual}}_{\Delta,n,s,g(\theta)}\right\rangle = {}_A\langle\Delta_X|\Psi^{Z}_{n,s,g(\theta)}\rangle = \frac{1}{2}\left[\hat{V}_{0_Z} + (-1)^{\Delta}\hat{V}_{1_Z}\right]|\psi_{n,s,g(\theta)}\rangle, \tag{11}$$

with probability $p^{\text{virtual}}_{\Delta,n,s,g(\theta)} = \||\bar{\lambda}^{\text{virtual}}_{\Delta,n,s,g(\theta)}\rangle\|^2$, where $\Delta \in \{0, 1\}$ and $|\Delta_X\rangle = [|0_Z\rangle + (-1)^{\Delta}|1_Z\rangle]/\sqrt{2}$. Let $Y^{(\Delta\oplus 1)_X,\text{virtual}}_{\Delta,n,s,g(\theta)}$ denote the probability that Bob obtains the measurement outcome $(\Delta \oplus 1)_X$ when he performs an X basis measurement on the arriving signal conditioned on Alice emitting the state $|\lambda^{\text{virtual}}_{\Delta,n,s,g(\theta)}\rangle$. That is, this event corresponds to a phase error. Then, the phase error rate $e_{n,s,g(\theta)}$ can be written as

$$e_{n,s,g(\theta)} = \frac{1}{Y^{Z}_{n,s,g(\theta)}}\sum_{\Delta=0}^{1} p^{\text{virtual}}_{\Delta,n,s,g(\theta)} Y^{(\Delta\oplus 1)_X,\text{virtual}}_{\Delta,n,s,g(\theta)}. \tag{12}$$

In Appendix A, it is shown that an upper bound on the quantity $p^{\text{virtual}}_{\Delta,n,s,g(\theta)} Y^{(\Delta\oplus 1)_X,\text{virtual}}_{\Delta,n,s,g(\theta)}$ can be obtained by solving the following SDP:

$$\begin{aligned} \max_{L_{(\Delta\oplus 1)_X}} \quad & \text{Tr}\big[\hat{P}\big(|\bar{\lambda}^{\text{virtual}}_{\Delta,n,s,g(\theta)}\rangle\big) L_{(\Delta\oplus 1)_X}\big] \\ \text{subject to} \quad & \text{Tr}\big[\hat{V}_{b_\alpha}\rho^{\mu}_{[g(\theta)]}\hat{V}^{\dagger}_{b_\alpha} L_{(\Delta\oplus 1)_X}\big] = Q^{(\Delta\oplus 1)_X}_{\mu,g(\theta),b_\alpha}, \\ & \forall \mu \in \{s,\nu,\omega\}, \forall b \in \{0,1\}, \forall \alpha \in \{Z,X\} \\ & 0 \le L_{(\Delta\oplus 1)_X} \le \mathbb{I}, \end{aligned} \tag{13}$$

where $\rho^{\mu}_{[g(\theta)]}$ is given by Eq. (4), and $Q^{(\Delta\oplus 1)_X}_{\mu,g(\theta),b_\alpha}$ denotes the probability that Bob observes the result $(\Delta\oplus 1)_X$ with his X basis measurement given that Alice chose the intensity setting μ, the basis α, the bit value b, and the phases θ follow the PDF $g(\theta)$. We note that Eq. (13) includes constraints provided by basis mismatched events [44] in which Alice prepares the signals in the Z basis and Bob measures them in the X basis, which may result in a tighter estimation. This is because, in general, $|\lambda^{\text{virtual}}_{\Delta,n,s,g(\theta)}\rangle \neq \hat{V}_{\Delta_X}|\psi_{n,s,g(\theta)}\rangle$, and $\hat{P}(|\lambda^{\text{virtual}}_{\Delta,n,s,g(\theta)}\rangle)$ may be better approximated by an operator-form linear combination of both Z-encoded and X-encoded states, rather than just the latter.

Importantly, the states $|\bar{\lambda}^{\text{virtual}}_{\Delta,n,s,g(\theta)}\rangle$ and $\rho^{\mu}_{[g(\theta)]}$, as well as the operators $\hat{V}_{b_\alpha}$, are known and depend on Alice's state preparation process. The gains $Q^{(\Delta\oplus 1)_X}_{\mu,g(\theta),b_\alpha}$ are directly observed in a realization of the protocol. That is, the only unknown in Eq. (13) is the positive semi-definite operator L over which the maximization takes place.

Let $L^{*}_{(\Delta\oplus 1)_X}$ denote the solution to the SDP given by Eq. (13). Then, we have that

$$p^{\text{virtual}}_{\Delta,n,s,g(\theta)} Y^{(\Delta\oplus 1)_X,\text{virtual}}_{\Delta,n,s,g(\theta)} \le \text{Tr}\big[\hat{P}\big(|\bar{\lambda}^{\text{virtual}}_{\Delta,n,s,g(\theta)}\rangle\big) L^{*}_{(\Delta\oplus 1)_X}\big]. \tag{14}$$

That is,

$$e_{n,s,g(\theta)} \le \frac{1}{Y^{Z,\text{L}}_{n,s,g(\theta)}} \sum_{\Delta=0}^{1} \text{Tr}\big[\hat{P}\big(|\bar{\lambda}^{\text{virtual}}_{\Delta,n,s,g(\theta)}\rangle\big) L^{*}_{(\Delta\oplus 1)_X}\big] := e^{\text{U}}_{n,s,g(\theta)}. \tag{15}$$

2.3.3 *Solving Eqs.* (7)–(13) *numerically*

Solving numerically the SDPs presented above is difficult for two main reasons. Firstly, they are infinitely dimensional, because the states $\rho^{\mu}_{[g(\theta)]}$ are infinite-dimensional. Secondly, this also renders the calculation of the eigendecomposition of $\rho^{\mu}_{[g(\theta)]}$ given by Eq. (4) a difficult task. To overcome these two limitations, we follow a technique recently introduced in [50] (see also [51]), which consists in projecting the states $\rho^{\mu}_{[g(\theta)]}$ onto a finite-dimensional subspace that contains up to M photons. We shall denote the projected states as

$$\rho^{\mu}_{[g(\theta)],M} = \frac{\Pi_M \rho^{\mu}_{[g(\theta)]} \Pi_M}{\text{Tr}[\Pi_M \rho^{\mu}_{[g(\theta)]} \Pi_M]}, \tag{16}$$

where $\Pi_M = \sum_{n=0}^{M} |n\rangle\langle n|$ denotes the projector onto the M-photon subspace, being $|n\rangle$ a Fock state. In doing so, now the eigendecomposition of $\rho^{\mu}_{[g(\theta)],M}$ can be easily obtained numerically. For later convenience, we will denote the eigendecomposition of the numerator

of the right hand side of Eq. (16) as

$$\Pi_M \rho^{\mu}_{[g(\theta)]} \Pi_M = \sum_{n=0}^{M} q_{n|\mu,g(\theta)} \hat{P}\big(|\varphi_{n,\mu,g(\theta)}\rangle\big). \tag{17}$$

Importantly, this technique also allows to transform the infinite-dimensional SDPs given by Eqs. (7)–(13) onto finite-dimensional SDPs that can be solved numerically. The resulting SDPs and their derivation are provided in Appendix B.

2.3.4 Lower bound on the probabilities $p_{n|s,g(\theta)}$

As explained in the previous subsection, because the states $\rho^{\mu}_{[g(\theta)]}$ are infinite-dimensional, it might be difficult to calculate their eigendecomposition, and thus the probabilities $p_{n|s,g(\theta)}$. Instead, here we provide a lower bound on these probabilities based on the eigendecomposition given by Eq. (17). In particular, in Appendix B it is shown that

$$p_{n|s,g(\theta)} \geq q_{n|s,g(\theta)} - \epsilon_s := p^{\mathrm{L}}_{n|s,g(\theta)} \tag{18}$$

with $\epsilon_s = 2\sqrt{1 - \mathrm{Tr}[\Pi_M \rho^{s}_{[g(\theta)]} \Pi_M]}$.

3 Results

In this section, we now evaluate the secret key rate obtainable for various examples of functions $g(\theta)$. For illustration purposes, we consider three main scenarios, depending on whether or not the function $g(\theta)$ is fully characterized. Also, for the simulations, we consider a simple channel model whose transmission efficiency is given by $10^{-\frac{\gamma}{10}}$, where γ (measured in dB) represents the overall system loss, *i.e.*, it also includes the effect of the finite detection efficiency of Bob's detectors. Moreover, for simplicity, we disregard any misalignment effect, and assume that the only source of errors are the dark counts of Bob's detectors, whose probability is set to $p_d = 10^{-8}$ [23, 52]. In addition, as already mentioned, we consider that the BB84 encoding operators are ideal even though the analysis presented here is applicable if this condition is not met, and we take an error correction efficiency $f = 1.16$.

To obtain the bounds $Y^{Z,\mathrm{L}}_{n,s,g(\theta)}$ and $e^{\mathrm{U}}_{n,s,g(\theta)}$ we use the finite-dimensional versions of the SDPs above, which are presented in Appendix B. Note that, the resulting secret key rate is an increasing function of M. However, the time required to numerically solve such SDPs grows rapidly with this parameter. For this reason, we have set a sufficiently large M so that an increase in this parameter would result in a negligible improvement of the secret key rate as tested numerically. The effect that the parameter M has in the secret key rate, is studied in Appendix D.

3.1 Fully-characterized $g(\theta)$

Here, we consider the scenario in which the function $g(\theta)$ is completely characterized, and we evaluate two specific examples of practical interest. The first example corresponds to the scenario given by Eq. (1), which has been considered in [42], while the second example can be interpreted as a noisy version of the first one.

3.1.1 Ideal discrete phase randomization

The results are shown in Fig. 1 for different values of the total number of random phases N selected by Alice. In particular, the solid lines in the figure have been obtained using the parameter estimation procedure presented in Sect. 2.3 based on SDP and the use of basis mismatched events. If we discard these latter events, the obtainable key rate decreases, as illustrated by the dashed-dot lines. Finally, the dotted lines correspond to the analysis in [42]. For completeness, this latter approach is summarized in Appendix E. In the first two cases, for simplicity, we set the intensity settings to the possibly sub-optimal values $\omega = 0$, $\nu = s/5$ and we optimize s as a function of the overall system loss γ, while in the later case we set $\omega = 0$ and optimize both ν and s as a function of γ (which provides the optimal solution for this approach). Importantly, despite this fact, Fig. 1 shows that the use of SDP and basis mismatched events significantly improve the secret key rate when compared to the results in [42]. Furthermore, we find that the improvement of using basis mismatched events is more advantageous when N is small. Indeed, when $N \geq 5$, this enhancement in performance is almost negligible. This is expected as basis mismatched events do not improve the estimation in the case of ideal continuous phase randomization, *i.e.*, in the limit $N \to \infty$. On the other hand, when N is small, the eigenstates $|\psi_{n,s,g(\theta)}\rangle$ for $n = 0, 1$ deviate more from a perfect Fock state, meaning that the virtual states $|\lambda^{\text{virtual}}_{\Delta,n,s,g(\theta)}\rangle$ deviate more from the X-encoded states $\hat{V}_{\Delta_X}|\psi_{n,s,g(\theta)}\rangle$ and thus basis mismatched events provide a tighter estimation.

Note that, as shown in Fig. 2, when $N \geq 6$, the improvement in the secret key rate that can be obtained by further increasing the value of N decelerates. Hence, it seems that a value of around $N = 8$ might be a good practical compromise, as this configuration requires only three random bits per pulse to select the random phase. As in the previous figure, here we set the intensities to $\{s, s/5, 0\}$ and optimize s as a function of the overall system loss to simplify the numerics. This is done for both the ideal PR-WCP scenario and for the different values of N to ensure a fear comparison between both scenarios.

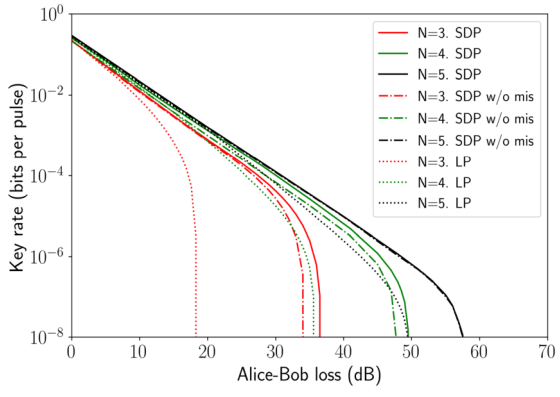

Figure 1 Secret key rate in logarithmic scale versus the overall system loss for the ideal discrete phase-randomization scenario given by Eq. (1), as a function of the total number of random phases N selected by Alice. The solid lines correspond to the parameter estimation procedure based on SDP and basis mismatched events considered in this work, while the dashed-dotted lines represent the same procedure overlooking basis mismatched events. Finally, the dotted lines correspond to the analysis in [42] using linear programming

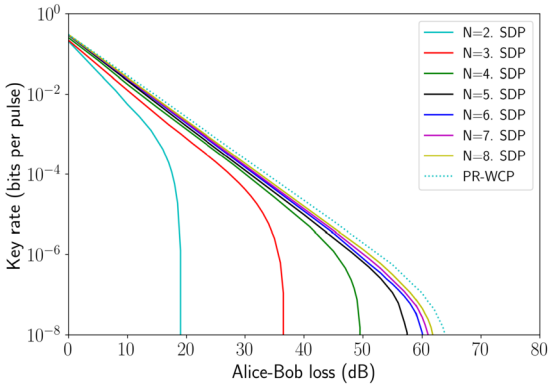

Figure 2 Secret key rate in logarithmic scale versus the overall system loss for the ideal discrete phase-randomization scenario given by Eq. (1), as a function of the total number of random phases N selected by Alice, when Alice and Bob employ the parameter estimation procedure based on SDP and basis mismatched events considered in this work. Remarkably, as shown in the figure, only eight random phases are enough to deliver a secret key rate already quite close to the ideal scenario of perfect PR-WCPs, where the phase of each pulse is uniformly random in $[0, 2\pi)$

3.1.2 Noisy discrete phase randomization

Here we consider the situation in which the actual phase encoded by Alice in each emitted pulse follows a certain PDF around the selected discrete value $\theta_k = 2\pi k/N$. This might happen due to device imperfections of the phase modulator or the electronics that control it. For concreteness and illustration purposes, we shall assume that this PDF is a truncated Gaussian distribution, though we remark that our analysis can be applied to any given distribution. A truncated Gaussian distribution has the form

$$f(\theta;\theta_k,\sigma_k,\lambda_k,\Lambda_k) = \frac{\phi(\theta;\theta_k,\sigma_k^2)}{\Phi(\Lambda_k;\theta_k,\sigma_k^2) - \Phi(\lambda_k;\theta_k,\sigma_k^2)}, \tag{19}$$

when the phase θ is in the interval $\lambda_k < \theta < \Lambda_k$, and zero otherwise. The functions $\phi(x;\gamma,\sigma^2)$ and $\Phi(x;\gamma,\sigma^2)$ in Eq. (19) are, respectively, given by

$$\begin{aligned} \phi(x;y,z) &= \frac{1}{\sqrt{2\pi z}} e^{-\frac{(x-y)^2}{2z}}, \\ \Phi(x;y,z) &= \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi z}} e^{-\frac{(t-y)^2}{2z}}\, dt. \end{aligned} \tag{20}$$

That is, in this scenario the function $g(\theta)$ has the following form

$$g(\theta) = \frac{1}{N}\sum_{k=0}^{N-1} f(\theta;\theta_k,\sigma_k,\lambda_k,\Lambda_k) \tag{21}$$

for certain parameters θ_k, σ_k, λ_k and Λ_k.

In the limit when the standard deviations $\sigma_k \to 0\ \forall k$, Eq. (21) converges to the PDF given by Eq. (1), because in that regime each truncated Gaussian distribution approaches the Dirac delta function. On the other hand, when $\sigma_k \to \infty$, and given that the concatenation of the truncation intervals defined by λ_k and Λ_k allow the phase to take any value within the range of $[0, 2\pi)$ but do not overlap each other, Eq. (21) converges to the PDF of a

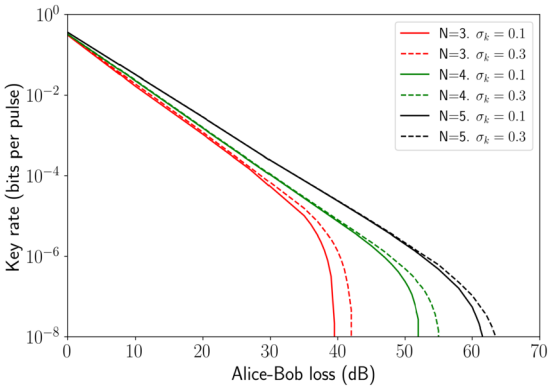

Figure 3 Secret key rate in logarithmic scale versus the overall system loss when $g(\theta)$ follows the PDF given by Eq. (21), as a function of the total number of random phases N selected by Alice, and for two different values of the standard deviations σ_k, which are assumed to be equal for all k

uniform distribution in $[0, 2\pi)$. Importantly, this means that the achievable secret key rate will increase with higher values of σ_k, or, to put it in other words, when the uncertainty about the phase actually imprinted by Alice on each of her prepared signals increases, given that $g(\theta)$ is completely characterized.

The simulation results are shown in Fig. 3, which presents a comparison between the achievable secret key rate for two different values of the standard deviations σ_k, which, for simplicity, are assumed to be equal for all k. As expected, the larger the value of σ_k is, the higher the resulting secret key rate, regardless of the number N of random phases selected by Alice, though the improvement is more relevant when N is small. For simplicity and due to the lack of experimental data, Fig. 3 assumes that $\lambda_k = \theta_k - 3\sigma_k$ and $\Lambda_k = \theta_k + 3\sigma_k$. Moreover, like in the previous example, we set $\omega = 0$, $\nu = s/5$ and we optimize s as a function of the overall system loss.

3.2 Partially-characterized $g(\theta)$

Here, we now consider the scenario in which only partial information about the function $g(\theta)$ is known. In particular, and for illustration purposes, we shall assume that the actual phase encoded by Alice in each emitted pulse could be any phase within a certain interval around the selected discrete value $\theta_k = 2\pi k/N$, but its precise PDF $g(\theta)$ is unknown. Precisely, let $\delta_{\max}$ denote the maximum possible deviation between the actual selected phase θ_k and the actual imprinted phase, which we shall denote by $\hat{\theta}_k$. That is, we assume that the actual imprinted phase lies in the interval $\hat{\theta}_k \in [\theta_k - \delta_{\max}, \theta_k + \delta_{\max}]$, and we conservatively take the combination of values $\hat{\theta}_k$ for all k that minimizes the secret key rate following the analysis presented in Appendix C.

The results are illustrated in Fig. 4, as a function of the total number of phases N selected by Alice and the value of the maximum deviation $\delta_{\max}$. Like in the previous examples, for simplicity, we fix $\omega = 0$, $\nu = s/5$ and we optimize s as a function of the overall system loss. As expected, the larger the value of $\delta_{\max}$ is, the lower the resulting secret key rate.

Also, from Fig. 4 we see that for higher values of $\delta_{\max}$, the secret key rate becomes less sensitive to the parameter N. Indeed, when $\delta_{\max} = 10^{-1}$, the achievable secret key rate for the cases $N = 3, 4, 5$ essentially overlap each other, which is the left-most curve. This seems to be due to the fact that a significant increase in $\delta_{\max}$ allows in principle for some phases

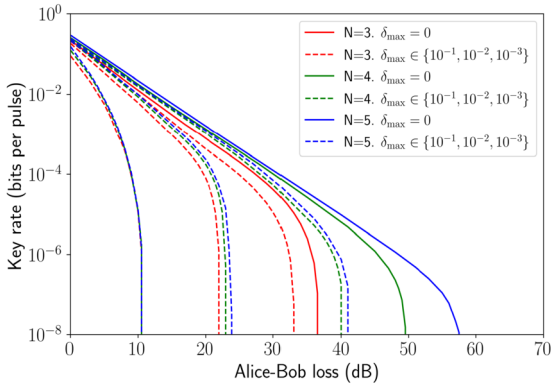

Figure 4 Secret key rate in logarithmic scale versus the overall system loss when the phases lie in the intervals $\theta_k \pm \delta_{\max}$ and the function $g(\theta)$ is unknown, as a function of the total number of random phases N selected by Alice and the value of $\delta_{\max}$

to lie close to each other, or even become identical if this parameter is large enough. Under this situation, the increase of N does not help to improve the performance, as the effective randomness remains almost the same.

4 Conclusion

In this paper we have considered the security of decoy-state quantum key distribution (QKD) when the phase of each generated signal is not uniformly random, as requested by the theory, but follows an arbitrary, continuous or discrete, probability density function (PDF). This might happen due to the presence of device imperfections in the phase-randomization process, and/or due to the use of an external phase modulator to imprint the random phases on the generated pulses, which limits the possible selected phases to a finite set.

Our analysis combines a novel parameter estimation technique, based on semi-definite programming, with the use of basis mismatched events, to tightly estimate the relevant parameters that are needed to evaluate the achievable secret key rate. In doing so, we have shown that decoy-state QKD is rather robust to faulty phase-randomization, particularly when the PDF that governs the random phases is well-characterized. Moreover, our results significantly outperform those of previous works while being also more general, in the sense that they can handle more realistic and practical scenarios.

This work might be relevant as well to other quantum communication protocols beyond QKD that use laser sources and decoy states.

Appendix A: Derivation of the SDPs given by Eqs. (7)–(13)

In this Appendix, we follow a similar approach to the one in [41] to derive the infinite-dimensional SDPs presented in Eqs. (7)–(13) of the main text, under the assumption of collective attacks. We recall that these infinite-dimensional SDP's cannot be solved numerically and a further dimension-reduction step is needed (see Appendix B).

Let Ω denote a quantum channel (or the action of Eve) that acts independently on each optical pulse emitted by Alice. Also, let us assume that in a certain round, Bob measures the incoming signal with a positive operator valued measure (POVM) that contains the

element Π. In this scenario, the probability that Bob obtains the outcome associated with the element Π given that Alice sends him a quantum state σ can be expressed as

$$\mathrm{Tr}\big[\Omega(\sigma)\Pi\big] = \mathrm{Tr}\left(\sum_k A_k \sigma A_k^\dagger \Pi\right) = \mathrm{Tr}\left(\sigma \sum_k A_k^\dagger \Pi A_k\right) = \mathrm{Tr}(\sigma H), \tag{A.1}$$

where $\Omega(\sigma)$ represents the action of Ω on σ, $\{A_k\}$ denotes the set of Kraus operators corresponding to the operator-sum representation of the channel Ω, and

$$0 \leq H = \sum_k A_k^\dagger \Pi A_k \leq \sum_k A_k^\dagger A_k = \mathbb{I}. \tag{A.2}$$

Bob measures the incoming signals in either the Z or the X basis. Let us denote the POVM elements corresponding to each of these two measurements by $\{\Pi_{0_Z}, \Pi_{1_Z}, \Pi_f\}$ and $\{\Pi_{0_X}, \Pi_{1_X}, \Pi_f\}$, respectively. That is, Π_{b_α} represents the POVM element associated to the outcome b in the basis α, with $\alpha \in \{Z, X\}$, and Π_f represents the POVM element associated to an inconclusive outcome. Note that here we are implicitly considering the basis-independent detection efficiency assumption, which means that the POVM element Π_f is equal for both basis. Let $\Pi_d = \mathbb{I} - \Pi_f = \Pi_{0_Z} + \Pi_{1_Z} = \Pi_{0_X} + \Pi_{1_X}$ denote the operator associated to a conclusive outcome at Bob's side. Then, after substituting in Eq. (A.1) the state σ with Alice's emitted state when she chooses the Z basis,

$$\rho^{\mu,Z}_{[g(\theta)]} = \frac{1}{2}\hat{V}_{0_Z}\rho^{\mu}_{[g(\theta)]}\hat{V}_{0_Z}^\dagger + \frac{1}{2}\hat{V}_{1_Z}\rho^{\mu}_{[g(\theta)]}\hat{V}_{1_Z}^\dagger, \tag{A.3}$$

and the operator Π with Π_d, we obtain

$$Q^Z_{\mu,g(\theta)} = \mathrm{Tr}\big[\Omega\big(\rho^{\mu,Z}_{[g(\theta)]}\big)\Pi_d\big] = \mathrm{Tr}\big[\rho^{\mu,Z}_{[g(\theta)]}H\big] = \mathrm{Tr}\big[\rho^{\mu}_{[g(\theta)]}J_Z\big], \tag{A.4}$$

with $H = \sum_k A_k^\dagger \Pi_d A_k$, and the operator J_Z satisfying

$$0 \leq J_Z = \frac{1}{2}\big(\hat{V}_{0_Z}^\dagger H \hat{V}_{0_Z} + \hat{V}_{1_Z}^\dagger H \hat{V}_{1_Z}\big) \leq \mathbb{I}. \tag{A.5}$$

Finally, by taking into account that the yield associated to the states $|\psi_{n,s,g(\theta)}\rangle$ encoded in the Z basis is given by

$$Y^Z_{n,s,g(\theta)} = \mathrm{Tr}\big\{\Omega\big[\hat{P}\big(\big|\psi^Z_{n,s,g(\theta)}\big\rangle\big)\big]\Pi_d\big\} = \mathrm{Tr}\big[\hat{P}(|\psi_{n,s,g(\theta)}\rangle)J_Z\big], \tag{A.6}$$

with

$$\hat{P}\big(\big|\psi^Z_{n,s,g(\theta)}\big\rangle\big) = \frac{1}{2}\hat{V}_{0_Z}\hat{P}\big(|\psi_{n,s,g(\theta)}\rangle\big)\hat{V}_{0_Z}^\dagger + \frac{1}{2}\hat{V}_{1_Z}\hat{P}\big(|\psi_{n,s,g(\theta)}\rangle\big)\hat{V}_{1_Z}^\dagger, \tag{A.7}$$

we obtain the SDP presented in Eq. (7).

Regarding the SDP given by Eq. (13) to estimate the phase error rate, we note that the numerator of Eq. (12), can be expressed as

$$\begin{aligned} &p^{\mathrm{virtual}}_{\Delta,n,s,g(\theta)} Y^{(\Delta\oplus 1)_X,\mathrm{virtual}}_{\Delta,n,s,g(\theta)} \\ &\quad = p^{\mathrm{virtual}}_{\Delta,n,s,g(\theta)}\,\mathrm{Tr}\big\{\Omega\big[\hat{P}\big(\big|\lambda^{\mathrm{virtual}}_{\Delta,n,s,g(\theta)}\big\rangle\big)\big]\Pi_{(\Delta\oplus 1)_X}\big\} \end{aligned}$$

$$= \mathrm{Tr}\Big[\hat{P}\Big(\big|\bar{\lambda}^{\mathrm{virtual}}_{\Delta,n,s,g(\theta)}\big\rangle\Big)L_{(\Delta\oplus 1)_X}\Big], \tag{A.8}$$

where $0 \leq L_{(\Delta\oplus 1)_X} = \sum_k A_k^\dagger \Pi_{(\Delta\oplus 1)_X} A_k \leq \mathbb{I}$ according to Eq. (A.1), and $|\bar{\lambda}^{\mathrm{virtual}}_{\Delta,n,s,g(\theta)}\rangle = \sqrt{p^{\mathrm{virtual}}_{\Delta,n,s,g(\theta)}}|\lambda^{\mathrm{virtual}}_{\Delta,n,s,g(\theta)}\rangle$.

By using again Eq. (A.1), we have that the gains $Q^{(\Delta\oplus 1)_X}_{\mu,g(\theta),b_\alpha}$ can be expressed as

$$Q^{(\Delta\oplus 1)_X}_{\mu,g(\theta),b_\alpha} = \mathrm{Tr}\Big[\hat{V}_{b_\alpha}\rho^{\mu}_{[g(\theta)]}\hat{V}^\dagger_{b_\alpha}L_{(\Delta\oplus 1)_X}\Big]. \tag{A.9}$$

Putting it all together, we find that the SDP presented in Eq. (13) of the main text, provides an upper bound on $p^{\mathrm{virtual}}_{\Delta,n,s,g(\theta)}Y^{(\Delta\oplus 1)_X,\mathrm{virtual}}_{\Delta,n,s,g(\theta)}$.

Appendix B: Finite-dimensional SDPs when $g(\theta)$ is fully characterized

B.1 Lower bound on the yields $Y^Z_{n,s,g(\theta)}$

In this Appendix, we show how to obtain a finite-dimensional relaxation of the SDP given by Eq. (7) to find a lower bound on the yields $Y^Z_{n,s,g(\theta)}$. For this, we follow again the approach presented in [41, 50]. The key idea is rather simple: instead of considering the infinite-dimensional state $\rho^{\mu}_{[g(\theta)]}$ given by Eq. (4), we employ a projection $\rho^{\mu}_{[g(\theta)],M}$ of this state onto a finite-dimensional subspace with up to M photons (see Eq. (16)), and then we relax the original constraints of the SDP accordingly.

We begin by briefly introducing some helpful results for this purpose. The first one is a direct consequence of the Cauchy-Schwarz inequality in Hilbert spaces [53, 54], which allows to relate the quantities $\mathrm{Tr}[\sigma H]$ and $\mathrm{Tr}[\rho H]$, with $0 \leq H \leq \mathbb{I}$, as a function of the fidelity between the states σ and ρ,

$$F(\rho,\sigma) = \mathrm{Tr}[\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}]^2. \tag{B.1}$$

In particular, it states that

$$G_-\big(\mathrm{Tr}[\rho H], F(\sigma,\rho)\big) \leq \mathrm{Tr}[\sigma H] \leq G_+\big(\mathrm{Tr}[\rho H], F(\sigma,\rho)\big), \tag{B.2}$$

with the functions $G_\pm(y,z)$ being defined as

$$G_-(y,z) = \begin{cases} g_-(y,z) & \text{if } y > 1-z, \\ 0 & \text{otherwise,} \end{cases} \tag{B.3}$$

and

$$G_+(y,z) = \begin{cases} g_+(y,z) & \text{if } y < z, \\ 1 & \text{otherwise,} \end{cases} \tag{B.4}$$

with $g_\pm(y,z) = y + (1-z)(1-2y) \pm 2\sqrt{z(1-z)y(1-y)}$.

The remaining results we use, *i.e.* Eqs. (B.5)–(B.6)–(B.7)–(B.8) below, have been derived in [41, 50, 55]. In particular, we have that

$$\begin{aligned} F\big(\rho^{\mu}_{[g(\theta)]}, \rho^{\mu}_{[g(\theta)],M}\big) &= \mathrm{Tr}\big[\Pi_M \rho^{\mu}_{[g(\theta)]} \Pi_M\big] \\ &= \sum_{n=0}^{M} q_{n|\mu,g(\theta)} := F^{\mathrm{proj}}_{\mu,g(\theta)}, \end{aligned} \tag{B.5}$$

where the coefficients $q_{n|s,g(\theta)}$ are given in Eq. (17). Also, we have that the quantities $|p_{n|\mu,g(\theta)} - q_{n|\mu,g(\theta)}|$ can be upper bounded as

$$\begin{aligned} |p_{n|\mu,g(\theta)} - q_{n|\mu,g(\theta)}| &\leq 2\sqrt{1 - \mathrm{Tr}\big[\Pi_M \rho^{\mu}_{[g(\theta)]} \Pi_M\big]} \\ &= 2\sqrt{1 - F^{\mathrm{proj}}_{\mu,g(\theta)}} =: \epsilon_\mu. \end{aligned} \tag{B.6}$$

Finally, the fidelity $F(\hat{P}(|\varphi_{n,\mu,g(\theta)}\rangle), \hat{P}(|\psi_{n,\mu,g(\theta)}\rangle)) = |\langle\varphi_{n,\mu,g(\theta)}|\psi_{n,\mu,g(\theta)}\rangle|^2$ satisfies

$$F\big(\hat{P}\big(|\varphi_{n,\mu,g(\theta)}\rangle\big), \hat{P}\big(|\psi_{n,\mu,g(\theta)}\rangle\big)\big) \geq 1 - \left(\frac{\epsilon_\mu}{\delta_{n,\mu}}\right)^2 := F^{\mathrm{vec}}_{n,\mu,g(\theta)}, \tag{B.7}$$

with

$$\begin{aligned} \delta_{0,\mu} &= q_{0|\mu,g(\theta)} - q_{1|\mu,g(\theta)} - \epsilon_\mu \\ \delta_{n,\mu} &= \min\{q_{n-1|\mu,g(\theta)} - q_{n|\mu,g(\theta)} - \epsilon_\mu, q_{n|\mu,g(\theta)} - q_{n+1|\mu,g(\theta)} - \epsilon_\mu\}. \end{aligned} \tag{B.8}$$

Then, from Eqs. (8)–(B.2)–(B.7) we have that

$$Y^{Z,\mathrm{L}}_{n,s,g(\theta)} = \mathrm{Tr}\big[\hat{P}(|\psi_{n,s,g(\theta)}\rangle) J^*_Z\big] \geq G_-\big(\mathrm{Tr}\big[\hat{P}(|\varphi_{n,s,g(\theta)}\rangle) J^*_Z\big], F^{\mathrm{vec}}_{n,s,g(\theta)}\big), \tag{B.9}$$

where J^*_Z is the solution to the SDP presented in Eq. (7), and we have used the fact that G_- is increasing with respect to its second argument. Since $G_-(y,z)$ is decreasing with respect to its first argument, one can lower bound Eq. (B.9) by finding a lower bound on its first argument.

From Eq. (B.2), we have that

$$G_-\big(Q^Z_{\mu,g(\theta)}, F^{\mathrm{proj}}_{\mu,g(\theta)}\big) \leq \mathrm{Tr}\big[\rho^{\mu}_{[g(\theta)],M} J_Z\big] \leq G_+\big(Q^Z_{\mu,g(\theta)}, F^{\mathrm{proj}}_{\mu,g(\theta)}\big), \tag{B.10}$$

with the operator J_Z defined in Eq. (7). Here, since the states $\rho^{\mu}_{[g(\theta)],M}$ are finite dimensional, the calculation of $\mathrm{Tr}[\rho^{\mu}_{[g(\theta)],M} J_Z]$ can be restricted to operators J_Z that act on their finite subspace. Putting it all together, we find that a lower bound on $Y^Z_{n,s,g(\theta)}$ can be obtained by solving the following finite-dimensional SDP program

$$\begin{aligned} &\min_{J_Z} \ \mathrm{Tr}\big[\hat{P}(|\varphi_{n,s,g(\theta)}\rangle) J_Z\big] \\ &\text{subject to} \ \ G_-\big(Q^Z_{\mu,g(\theta)}, F^{\mathrm{proj}}_{\mu,g(\theta)}\big) \leq \mathrm{Tr}\big[\rho^{\mu}_{[g(\theta)],M} J_Z\big] \\ &\qquad\qquad \leq G_+\big(Q^Z_{\mu,g(\theta)}, F^{\mathrm{proj}}_{\mu,g(\theta)}\big), \quad \forall \mu \in \{s, \nu, \omega\} \\ &\qquad 0 \leq J_Z \leq \mathbb{I}. \end{aligned} \tag{B.11}$$

That is, we have that

$$\mathrm{Tr}\big[\hat{P}\big(|\varphi_{n,s,g(\theta)}\rangle\big)J_Z^*\big] \geq \mathrm{Tr}\big[\hat{P}\big(|\varphi_{n,s,g(\theta)}\rangle\big)J_Z^{**}\big], \tag{B.12}$$

with J_Z^{**} being the solution to the SDP in Eq. (B.11), and J_Z^* the solution to Eq. (7). This holds because the constrains in Eq. (B.11) are looser than those in Eq. (7).

Finally, by combining Eq. (B.9) with Eq. (B.12) we have that

$$Y_{n,s,g(\theta)}^{Z,\mathrm{L}} \geq G_-\big(\mathrm{Tr}\big[\hat{P}\big(|\varphi_{n,s,g(\theta)}\rangle\big)J_Z^{**}\big], F_{n,s,g(\theta)}^{\mathrm{vec}}\big) := \tilde{Y}_{n,s,g(\theta)}^{Z,\mathrm{L}}. \tag{B.13}$$

The lower bound $\tilde{Y}_{n,s,g(\theta)}^{Z,\mathrm{L}}$ is the one we use in our simulations in Sect. 3.1.

B.2 Upper bound on the phase-error rates $e_{n,s,g(\theta)}$

In this Appendix, we show how to estimate an upper bound on $e_{n,s,g(\theta)}$ by using a finite-dimensional SDP. To do so, let us also define the operator

$$M_{\mathrm{ph}} := |0_X\rangle\langle 0_X| \otimes L_{1_X}^* + |1_X\rangle\langle 1_X| \otimes L_{0_X}^*, \tag{B.14}$$

where $L_{(\Delta\oplus 1)_X}^*$ denotes the solution to the SDP given by Eq. (13), so that

$$\begin{aligned}&\sum_{\Delta=0}^{1} p_{\Delta,n,s,g(\theta)}^{\mathrm{virtual}} Y_{\Delta,n,s,g(\theta)}^{(\Delta\oplus 1)_X,\mathrm{virtual}} \\ &\quad\leq \sum_{\Delta=0}^{1} \mathrm{Tr}\big[\hat{P}\big(\big|\bar{\lambda}_{\Delta,n,s,g(\theta)}^{\mathrm{virtual}}\big\rangle\big)L_{(\Delta\oplus 1)_X}^*\big] = \mathrm{Tr}\big[\hat{P}\big(\big|\Psi_{n,s,g(\theta)}^{Z}\big\rangle\big)M_{\mathrm{ph}}\big].\end{aligned} \tag{B.15}$$

Now, let us define the finite-dimensional state

$$\big|\Psi_{n,s,g(\theta)}^{Z,M}\big\rangle = \frac{1}{\sqrt{2}}\big(|0_Z\rangle_A \hat{V}_{0_Z} + |1_Z\rangle_A \hat{V}_{1_Z}\big)|\varphi_{n,s,g(\theta)}\rangle, \tag{B.16}$$

and the unnormalized states $|\bar{\lambda}_{\Delta,n,s,g(\theta)}^{\mathrm{virtual},M}\rangle$ as

$$\big|\bar{\lambda}_{\Delta,n,s,g(\theta)}^{\mathrm{virtual},M}\big\rangle = {}_A\big\langle\Delta_X\big|\Psi_{n,s,g(\theta)}^{Z,M}\big\rangle = \frac{1}{2}\big[\hat{V}_{0_Z} + (-1)^{\Delta}\hat{V}_{1_Z}\big]|\varphi_{n,s,g(\theta)}\rangle. \tag{B.17}$$

Then, we have that

$$\big|\big\langle\Psi_{n,s,g(\theta)}^{Z,M}\big|\Psi_{n,s,g(\theta)}^{Z}\big\rangle\big|^2 = \big|\langle\varphi_{n,s,g(\theta)}|\psi_{n,s,g(\theta)}\rangle\big|^2 \geq F_{n,s,g(\theta)}^{\mathrm{vec}}, \tag{B.18}$$

where we have used Eq. (B.7) and the fact that $\hat{V}_{0Z}^{\dagger}\hat{V}_{0Z} = \hat{V}_{1Z}^{\dagger}\hat{V}_{1Z} = \mathbb{I}$. Now, by applying the Cauchy-Schwarz constraint given by Eq. (B.2), and taking into account the fact that $G_+(y,z)$ is a decreasing function with respect to its second argument, we find that

$$\mathrm{Tr}\big[\hat{P}\big(\big|\Psi_{n,s,g(\theta)}^{Z}\big\rangle\big)M_{\mathrm{ph}}\big] \leq G_+\big(\mathrm{Tr}\big[\hat{P}\big(\big|\Psi_{n,s,g(\theta)}^{Z,M}\big\rangle\big)M_{\mathrm{ph}}\big], F_{n,s,g(\theta)}^{\mathrm{vec}}\big). \tag{B.19}$$

Importantly, since $G_+(y,z)$ is an increasing function with respect to its first argument, one can upper bound the previous equation by finding an upper bound on its first argument. Moreover, since the states $|\Psi_{n,s,g(\theta)}^{Z,M}\rangle$ are finite dimensional, one can restrict the

optimization search to operators L that act on the corresponding finite subspace. In particular, we have that

$$\begin{aligned}&\mathrm{Tr}\big[\hat{P}\big(\big|\Psi^{Z,M}_{n,s,g(\theta)}\big\rangle\big)M_{\mathrm{ph}}\big]\\&=\sum_{\Delta=0}^{1}\mathrm{Tr}\big[\hat{P}\big(\big|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,g(\theta)}\big\rangle\big)L^{*}_{(\Delta\oplus 1)_X}\big]\leq\sum_{\Delta=0}^{1}\mathrm{Tr}\big[\hat{P}\big(\big|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,g(\theta)}\big\rangle\big)L^{**}_{(\Delta\oplus 1)_X}\big],\end{aligned}\tag{B.20}$$

where $L^{**}_{(\Delta\oplus 1)_X}$ is the solution to the finite-dimensional SDP presented below.

Likewise, the constraints in Eq. (13) can be relaxed by using essentially the same techniques discussed in Appendix B.1. In doing so, we find that an upper bound on $\mathrm{Tr}[\hat{P}(|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,g(\theta)}\rangle)L_{(\Delta\oplus 1)_X}]$ can be found by solving the following SDP

$$\begin{aligned}&\max_{L_{(\Delta\oplus 1)_X}}\ \mathrm{Tr}\big[\hat{P}\big(\big|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,g(\theta)}\big\rangle\big)L_{(\Delta\oplus 1)_X}\big]\\&\text{subject to}\ \ G_{-}\big(Q^{(\Delta\oplus 1)_X}_{\mu,g(\theta),b_\alpha},F^{\mathrm{proj}}_{\mu,g(\theta)}\big)\leq\mathrm{Tr}\big[\hat{V}_{b_\alpha}\rho^{\mu}_{[g(\theta)],\mathrm{M}}\hat{V}^{\dagger}_{b_\alpha}L_{(\Delta\oplus 1)_X}\big]\\&\qquad\qquad\leq G_{+}\big(Q^{(\Delta\oplus 1)_X}_{\mu,g(\theta),b_\alpha},F^{\mathrm{proj}}_{\mu,g(\theta)}\big),\\&\qquad\forall\mu\in\{s,\nu,\omega\},\forall b\in\{0,1\},\forall\alpha\in\{Z,X\}\\&\qquad 0\leq L_{(\Delta\oplus 1)_X}\leq\mathbb{I},\end{aligned}\tag{B.21}$$

where $F^{\mathrm{proj}}_{\mu,g(\theta)}$ is given by Eq. (B.5).

Let $L^{**}_{(\Delta\oplus 1)_X,}$ denote the operator that maximizes the SDP given by Eq. (B.21), then

$$e_{n,s,g(\theta)}\leq\frac{1}{\tilde{Y}^{Z,\mathrm{L}}_{n,s,g(\theta)}}G_{+}\left(\sum_{\Delta=0}^{1}\mathrm{Tr}\big[\hat{P}\big(\big|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,g(\theta)}\big\rangle\big)L^{**}_{(\Delta\oplus 1)_X}\big],F^{\mathrm{vec}}_{n,s,g(\theta)}\right):=\tilde{e}^{\mathrm{U}}_{n,s,g(\theta)}.$$

This is the upper bound that we use in our simulations in Sect. 3.1.

Appendix C: Finite-dimensional SDPs when $g(\theta)$ is partially characterized

Here, we consider the scenario studied in Sect. 3.2, *i.e.*, when the actual imprinted phases lies in certain intervals $\hat{\theta}_k\in[\theta_k-\delta_{\max},\theta_k+\delta_{\max}]$, with $\theta_k=2\pi k/N$, and the exact form of $g(\theta)$ is unknown.

A direct solution to this case could be found as follows. First, one defines a dense grid with p discrete values within each interval, and then one follows essentially the approach in Sect. 3.1.1 for each possible combination of these discrete phases from the different intervals. The secret key rate would then correspond to the worst case scenario, *i.e.*, the one that minimizes it among all possible combinations. The main drawback of this approach is, however, that the number of SDPs that needs to be solved grows very rapidly, as $\propto p^N$.

Instead, here we introduce a much simpler approach based on a modified version of the SDPs presented in Eqs. (B.11)–(B.21). In particular, let $f(\theta)$ denote the PDF associated to the ideal discrete phase randomization scenario given by Eq. (1), and let $\rho^{\mu}_{[f(\theta)],M}$ be the finite-dimensional state obtained by projecting $\rho^{\mu}_{[f(\theta)]}$ onto the subspace that contains up to M photons. Also, let $\rho^{\mu}_{[g(\theta)]}$ denote the state actually emitted by Alice in the scenario described above, *i.e.*, when $g(\theta)$ is partially characterized. Then, we can bound the fidelity

between $\rho^{\mu}_{[g(\theta)]}$ and $\rho^{\mu}_{[f(\theta)],M}$ by means of the Bures distance, which is defined as [56]

$$d_B(\rho,\sigma)^2 = 2\big[1-\sqrt{F(\rho,\sigma)}\big], \tag{C.1}$$

for any state ρ and σ. This distance satisfies the triangle inequality [56], which means that

$$\begin{aligned}\sqrt{F\big(\rho^{\mu}_{[g(\theta)]},\rho^{\mu}_{[f(\theta)],M}\big)} &= 1-\frac{1}{2}d_B\big(\rho^{\mu}_{[g(\theta)]},\rho^{\mu}_{[f(\theta)],M}\big)^2\\ &\geq 1-\frac{1}{2}\big[d_B\big(\rho^{\mu}_{[f(\theta)]},\rho^{\mu}_{[f(\theta)],M}\big)\\ &\quad + d_B\big(\rho^{\mu}_{[g(\theta)]},\rho^{\mu}_{[f(\theta)]}\big)\big]^2.\end{aligned} \tag{C.2}$$

We now compute the fidelities that correspond to the Bures distances $d_B(\rho^{\mu}_{[f(\theta)]},\rho^{\mu}_{[f(\theta)],M})$ and $d_B(\rho^{\mu}_{[g(\theta)]},\rho^{\mu}_{[f(\theta)]})$ so that, via Eq. (C.1), we can obtain the necessary fidelity bound with Eq. (C.2).

In particular, from Eq. (B.5), we have that $F(\rho^{\mu}_{[f(\theta)]},\rho^{\mu}_{[f(\theta)],M}) = F^{\text{proj}}_{\mu,f(\theta)}$. The fidelity $F(\rho^{\mu}_{g(\theta)},\rho^{\mu}_{[f(\theta)]})$, on the other hand, can be computed by considering the following purifications of the states $\rho^{\mu}_{[f(\theta)]}$ and $\rho^{\mu}_{[g(\theta)]}$, respectively,

$$\begin{aligned}\big|\psi^{\mu,N}_{[f(\theta)]}\big\rangle &= \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}|k\rangle\big|\sqrt{\mu}e^{2\pi ki/N}\big\rangle,\\ \big|\psi^{\mu,N}_{[g(\theta)]}\big\rangle &= \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}e^{i\phi_k}|k\rangle\big|\sqrt{\mu}e^{i(2\pi k/N+\delta_k)}\big\rangle.\end{aligned} \tag{C.3}$$

We find, therefore, that

$$\begin{aligned}F\big(\rho^{\mu}_{[g(\theta)]},\rho^{\mu}_{[f(\theta)]}\big) &\geq \big|\big\langle\psi^{\mu,N}_{[f(\theta)]}|\psi^{\mu,N}_{[g(\theta)]}\big\rangle\big|^2\\ &= \left|\sum_{k=0}^{N-1}\frac{1}{N}\big\langle\sqrt{\mu}e^{2\pi ki/N}|\sqrt{\mu}e^{i(2\pi k/N+\delta_k)}\big\rangle\right|^2\\ &\geq \left|\sum_{k=0}^{N-1}\frac{1}{N}\big\langle\sqrt{\mu}e^{2\pi ki/N}|\sqrt{\mu}e^{i(2\pi k/N+\delta_{\max})}\big\rangle\right|^2\\ &= \big|\big\langle\sqrt{\mu}|\sqrt{\mu}e^{i\delta_{\max}}\big\rangle\big|^2,\end{aligned} \tag{C.4}$$

where in the first inequality we have used the fact that the states on the right hand side are a purification of those on the left hand side; in the first equality we have taken into account that the phases ϕ_k in Eq. (C.3) can be chosen so that they cancel the phase of the inner product, and in the second inequality we have used the fact that $|\delta_k| \leq \delta_{\max}\ \forall k$.

Since the function $g(\theta)$ is unknown, we do not have access to the exact form of the eigenvectors $|\varphi_{n,s,[g(\theta)]}\rangle$ of $\rho^{s}_{[g(\theta)],M}$ which are needed to solve the relevant finite-dimensional SDP, but we can lower bound the value of $\text{Tr}[\hat{P}(|\varphi_{n,s,[g(\theta)]}\rangle)J_Z]$, with $0 \leq J_Z \leq \mathbb{I}$, by employing the Cauchy-Schwartz constraint presented in Eq. (B.2). Precisely, we have that

$$\text{Tr}\big[\hat{P}\big(|\varphi_{n,s,[g(\theta)]}\rangle\big)J_Z\big] \geq G_-\big(\text{Tr}\big[\hat{P}\big(|\varphi_{n,s,[f(\theta)]}\rangle\big)J_Z\big], F\big(|\varphi_{n,s,[g(\theta)]}\rangle,|\varphi_{n,s,[f(\theta)]}\rangle\big)\big), \tag{C.5}$$

where $|\varphi_{n,s,[f(\theta)]}\rangle$ are the eigenvectors of $\rho^{s}_{[f(\theta)],M}$, and the value of $F(|\varphi_{n,s,[g(\theta)]}\rangle, |\varphi_{n,s,[f(\theta)]}\rangle)$ is calcuated numerically as explained below.

With these considerations, we can now find a lower bound on the yields $Y^{Z}_{n,s,g(\theta)}$. For this, we first solve the following optimization problem to find the operator J^{**}_{z} that minimizes its objective function

$$\begin{aligned} &\min_{J_Z} \ \mathrm{Tr}\big[\hat{P}\big(|\varphi_{n,s,[f(\theta)]}\rangle\big)J_Z\big] \\ &\text{subject to } G_{-}\big(Q^{Z}_{\mu,g(\theta)}, F\big(\rho^{\mu}_{[g(\theta)]}, \rho^{\mu}_{[f(\theta)],M}\big)\big) \\ &\qquad \leq \mathrm{Tr}\big[\rho^{\mu}_{[f(\theta)],M} J_Z\big] \leq G_{+}\big(Q^{Z}_{\mu,g(\theta)}, F\big(\rho^{\mu}_{[g(\theta)]}, \rho^{\mu}_{[f(\theta)],M}\big)\big), \\ &\qquad 0 \leq J_Z \leq \mathbb{I}. \end{aligned} \tag{C.6}$$

Following Eq. (C.5), we now define

$$\hat{Y}^{Z,\mathrm{L}}_{n,s,g(\theta)} := G_{-}\big(\mathrm{Tr}\big[\hat{P}\big(|\varphi_{n,s,[f(\theta)]}\rangle\big)J^{**}_{Z}\big], F\big(|\varphi_{n,s,[g(\theta)]}\rangle, |\varphi_{n,s,[f(\theta)]}\rangle\big)\big). \tag{C.7}$$

Finally, by using the arguments introduced in Appendix B.1, we obtain that a lower bound on $Y^{Z}_{n,s,g(\theta)}$ is given by

$$Y^{Z}_{n,s,g(\theta)} \geq G_{-}\big(\hat{Y}^{Z,\mathrm{L}}_{n,s,g(\theta)}, F^{\mathrm{vec}}_{n,s,g(\theta)}\big) := \tilde{Y}^{Z,\mathrm{L}}_{n,s,g(\theta)}. \tag{C.8}$$

Note that, since we do not know which values of $\hat{\theta}_k$ result in the set of states $|\varphi_{n,s,[g(\theta)]}\rangle$ that minimizes the key rate, we find the worst case scenario numerically. To do so, we implement a Montecarlo simulation by considering a dense grid of values in $\theta_k \pm \delta_{\max}$ for every k and we find the combination of $\hat{\theta}_k$ that minimizes Eq. (C.8) (which includes the fidelity in Eq. (C.7)). This allow us to find the desired lower bound with arbitrary precision. Also, note that the number of SDPs that need to be solved grows very rapidly in the case of the direct solution mentioned at the beginning of this section. With this approach, this problem has been circumvented by reducing it to a simple calculation of the fidelities, which makes it computationally much faster, despite possibly providing looser bounds.

Regarding the estimation of an upper bound on the phase error rate, we follow the same procedure described in Appendix B.2. In doing so, we first solve the following finite-dimensional SDP,

$$\begin{aligned} &\max_{L_{(\Delta\oplus 1)_X}} \ \mathrm{Tr}\big[\hat{P}\big(\big|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,[f(\theta)]}\big\rangle\big)L_{(\Delta\oplus 1)_X}\big] \\ &\text{subject to } G_{-}\big(Q^{(\Delta\oplus 1)_X}_{\mu,b_\alpha}, F\big(\rho^{\mu}_{[g(\theta)]}, \rho^{\mu}_{[f(\theta)],M}\big)\big) \\ &\qquad \leq \mathrm{Tr}\big[\hat{V}_{b_\alpha}\rho^{\mu}_{[f(\theta)],M}\hat{V}^{\dagger}_{b_\alpha} L_{(\Delta\oplus 1)_X}\big] \leq G_{+}\big(Q^{(\Delta\oplus 1)_X}_{\mu,b_\alpha}, F\big(\rho^{\mu}_{[g(\theta)]}, \rho^{\mu}_{[f(\theta)],M}\big)\big), \\ &\qquad 0 \leq L_{(\Delta\oplus 1)_X} \leq \mathbb{I}, \end{aligned} \tag{C.9}$$

where $Q^{(\Delta\oplus 1)_X}_{\mu,b_\alpha}$ represents the observed rate at which Bob obtains the result $(\Delta\oplus 1)_X$ conditioned on Alice choosing the intensity setting μ, the basis α, the bit value b and Bob choosing the X basis. Now, similarly to Eq. (C.7), we define

$$\hat{e}^{\mathrm{U}}_{n,s,g(\theta)} := \sum_{\Delta=0}^{1} G_{+}\big(\mathrm{Tr}\big[\hat{P}\big(\big|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,[f(\theta)]}\big\rangle\big)L^{**}_{(\Delta\oplus 1)_X}\big], F\big(\big|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,[f(\theta)]}\big\rangle, \big|\bar{\lambda}^{\mathrm{virtual},M}_{\Delta,n,s,[g(\theta)]}\big\rangle\big)\big), \tag{C.10}$$

where $L^{**}_{(\Delta\oplus 1)_X}$ is the solution to Eq. (C.9). This way, we obtain that the phase error rate $e_{n,s,g(\theta)}$ is upper bounded by

$$e_{n,s,g(\theta)} \leq \frac{G_+(\hat{e}^{\mathrm{U}}_{n,s,g(\theta)}, F^{\mathrm{vec}}_{n,s,g(\theta)})}{\tilde{Y}^{Z,\mathrm{L}}_{n,s,g(\theta)}} := \tilde{e}^{\mathrm{U}}_{n,s,g(\theta)}, \tag{C.11}$$

where again, we use the combination of $\hat{\theta}_k$ that maximizes Eq. (C.11) to obtain the relevant upper bound.

The bounds $\tilde{Y}^{Z,L}_{n,s,g(\theta)}$ and $\tilde{e}^{\mathrm{U}}_{n,s,g(\theta)}$ are used in the simulations presented in Sect. 3.2.

As shown in Fig. 4, higher values of $\delta_{\max}$ result in an almost negligible impact of the parameter N on the secret key rate, as explained in the main text.

Appendix D: Influence of the parameter M in the secret key rate

As stated in the main text, the secret key rate is an increasing function of the size of the finite dimensional SDP, denoted by M. However, the computational time for solving these SDPs significantly increases with higher values of M. In this Appendix we briefly explore how the size of the SDP impacts the secret key rate. Figure 5 displays the secret key rate for a case involving 8 random phases, showcasing changes as M varies. It is evident from the figure that selecting a small $M < 8$ results in a considerable drop in performance. Nevertheless, when $M > 8$ the key rate appears to saturate and the improvement that we can get by enlarging M is negligible. Hence, in the figures presented in the main text, for each N, we choose an M such that, further increases offer only marginal improvements in the secret key rate. This leads us to select different M values depending on N, as less random phases require smaller SDPs to fulfill the condition above.

Appendix E: Parameter estimation procedure based on linear programming

For completeness, in this Appendix we summarize the parameter estimation technique presented in [42], using linear programming, to evaluate the case of perfect discrete phase randomization for the protocol described in Sect. 2.2.

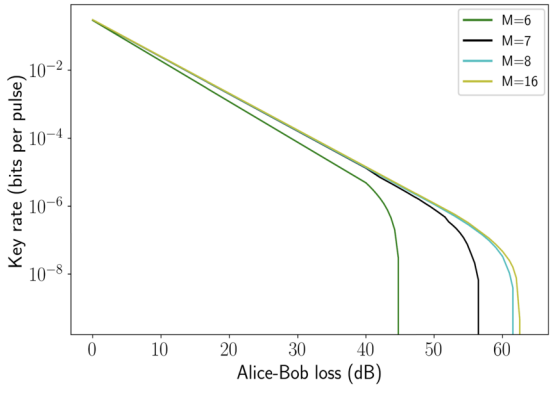

Figure 5 Secret key rate as a function of the size of the SDP, represented by the parameter M when the number of random phases is fixed to $N = 8$. As one can see, selecting a small M causes a significant drop in performance. Increasing M requires exponentially more time to solve the SDPs

In particular, given that the PDF follows Eq. (1), which we will denote as $f(\theta)$ as in the previous Appendix and $N \geq 1$, a purification of Alice's emitted states can be expressed as

$$\left|\psi^{\mu,N}_{[f(\theta)]}\right\rangle = \sum_{k=0}^{N-1} |k\rangle_A \left|\sqrt{\mu} e^{2k\pi i/N}\right\rangle = \sum_{j=0}^{N-1} |j\rangle_A \left|\beta^{\mu}_{j}\right\rangle, \tag{E.1}$$

where the second equality corresponds to the Schmidt decomposition. Note that in Eq. (E.1) we consider unnormalized states, which we will do throughout this Appendix for convenience. The states $|j\rangle_A$ can be interpreted as a quantum coin with N random outputs, while the states $|\beta^{\mu}_{j}\rangle$ are given by

$$\left|\beta^{\mu}_{j}\right\rangle = \sum_{k=0}^{N-1} e^{-2kj\pi i/N} \left|e^{2k\pi i/N}\sqrt{\mu}\right\rangle. \tag{E.2}$$

By using Eq. (2), these latter states can be rewritten as

$$\left|\beta^{\mu}_{j}\right\rangle = \sum_{l=0}^{\infty} \frac{(\sqrt{\mu})^{lN+j}}{\sqrt{(lN+j)!}} |lN+j\rangle. \tag{E.3}$$

Indeed, it is easy to show that when N is large, $|\beta^{\mu}_{j}\rangle$ approaches a Fock state with j photons.

If Alice measures her ancilla system A from the state $|\psi^{\mu,N}_{[f(\theta)]}\rangle$ in the basis $\{|j\rangle_A\}$, she obtains the result j with probability P^{μ}_{j} given by

$$P^{\mu}_{j} = \frac{\langle \beta^{\mu}_{j} \mid \beta^{\mu}_{j} \rangle}{\sum_{j=0}^{N-1} \langle \beta^{\mu}_{j} \mid \beta^{\mu}_{j} \rangle} \tag{E.4}$$

$$= \sum_{l=0}^{\infty} \frac{\mu^{lN+j} e^{-\mu}}{(lN+j)!}. \tag{E.5}$$

Ref. [42] employs the Gottesman, Lo, Lütkenhaus and Preskill (GLLP) security analysis [48], which needs to determine the basis dependence Δ^{μ}_{j} of the source, which is closely related to the fidelity F^{μ}_{j} between the states in the X and Z basis. Precisely, let us define

$$\Delta^{\mu}_{j} = \frac{1 - F^{\mu}_{j}}{2Y^{Z}_{j,\mu,f(\theta)}}, \tag{E.6}$$

where $Y^{Z}_{j,\mu,f(\theta)}$ refers to the yield that corresponds to the states $|\beta^{\mu}_{j}\rangle$ encoded in the Z basis, and the fidelity F^{μ}_{j} can be bounded by

$$F^{\mu}_{j} \geq \left| \frac{\sum_{l=0}^{\infty} \frac{\mu^{lN+j}}{(lN+j)!} 2^{-\frac{lN+j}{2}} \left(\cos\frac{lN+j}{4}\pi + \sin\frac{lN+j}{4}\pi\right)}{\sum_{l=0}^{\infty} \frac{\mu^{lN+j}}{(lN+j)!}} \right|. \tag{E.7}$$

Moreover, since $|\beta_j^\mu\rangle \neq |\beta_j^\gamma\rangle$ when $\mu \neq \gamma$, one can relate the yields and bit error rates associated to different intensity settings as follows [48]

$$\begin{aligned} &|Y_{j,\mu,f(\theta)} - Y_{j,\gamma,f(\theta)}| \leq \sqrt{1 - F_{\mu\gamma}^2}, \\ &\left|e^b_{j,\mu,f(\theta)} Y_{j,\mu,f(\theta)} - e^b_{j,\gamma,f(\theta)} Y_{j,\gamma,f(\theta)}\right| \leq \sqrt{1 - F_{\mu\gamma}^2}, \end{aligned} \tag{E.8}$$

where $e^b_{j,\mu,f(\theta)}$ denotes the bit error rate corresponding to the states $|\beta_j^\mu\rangle$, *i.e.*, the probability that Alice and Bob obtain different results when they use the same basis and Alice emits the state $|\beta_j^\mu\rangle$. The parameter $F_{\mu\gamma}$, on the other hand, is given by

$$F_{\mu\gamma} := \frac{\sum_{l=0}^{\infty} \frac{(\mu\gamma)^{lN/2}}{(lN)!}}{\sqrt{\sum_{l=0}^{\infty} \frac{\mu^{lN}}{(lN)!} \sum_{l=0}^{\infty} \frac{\gamma^{lN}}{(lN)!}}}. \tag{E.9}$$

The phase error rate $e_{j,\mu,g(\theta)}$ in the Z basis can be upper bounded by means of the bit error rate $e^b_{j,\mu,g(\theta)}$ in the X basis and the basis dependence parameter Δ_j^μ as [53]

$$\begin{aligned} e_{j,\mu,f(\theta)} \leq\ & e^{b,X}_{j,\mu,f(\theta)} + 4\Delta_j^\mu \left(1 - \Delta_j^\mu\right)\left(1 - 2e^{b,X}_{j,\mu,f(\theta)}\right) \\ & + 4\left(1 - 2\Delta_j^\mu\right)\sqrt{\Delta_j^\mu \left(1 - \Delta_j^\mu\right) e^{b,X}_{j,\mu,f(\theta)}\left(1 - e^{b,X}_{j,\mu,f(\theta)}\right)}, \end{aligned} \tag{E.10}$$

where we have included the superscript X in the bit error rate to emphasize that it refers to that in the X basis.

Putting it all together, we have that a lower bound on the yields $Y^Z_{j,s,f(\theta)}$ encoded in the Z basis can be estimated with the following linear program

$$\begin{aligned} &\min\ Y^Z_{j,s,f(\theta)} \\ &\text{subject to } \left|Y^Z_{j,\mu,f(\theta)} - Y^Z_{j,\gamma,f(\theta)}\right| \leq \sqrt{1 - F_{\mu\gamma}^2}, \\ &\qquad \forall \mu, \gamma \in \{s, \nu, \omega\}, \mu \neq \gamma, \\ &\qquad Q^Z_{\mu,f(\theta)} = \sum_{j=0}^{N-1} P_j^\mu Y^Z_{j,\mu,f(\theta)}, \quad \forall \mu \in \{s, \nu, \omega\}. \end{aligned} \tag{E.11}$$

Similarly, an upper bound on the bit error rate $e^{b,X}_{j,\mu,g(\theta)}$ can be calculated with the following linear program

$$\begin{aligned} &\max\ \xi^X_{j,s,f(\theta)} \\ &\text{subject to } \left|\xi^X_{j,\mu,f(\theta)} - \xi^X_{j,\gamma,f(\theta)}\right| \leq \sqrt{1 - F_{\mu\gamma}^2}, \\ &\qquad \forall \mu, \gamma \in \{s, \nu, \omega\}, \mu \neq \gamma, \\ &\qquad E^X_{\mu,f(\theta)} Q^X_{\mu,f(\theta)} = \sum_{j=0}^{N-1} P_j^\mu \xi^X_{j,\mu,f(\theta)}, \quad \forall \mu \in \{s, \nu, \omega\}, \end{aligned} \tag{E.12}$$

where $\xi^X_{j,s,f(\theta)} = e^{b,X}_{j,s,f(\theta)} Y^X_{j,s,f(\theta)}$. In particular, let $\xi^{X*}_{j,s,f(\theta)}$ denote the solution to the linear program above, then we have that

$$e^{b,X}_{j,s,f(\theta)} \leq \frac{\xi^{X*}_{j,s,f(\theta)}}{Y^{X,\mathrm{L}}_{j,s,f(\theta)}} := e^{b,X,\mathrm{U}}_{j,s,f(\theta)}, \tag{E.13}$$

where $Y^{X,\mathrm{L}}_{j,s,f(\theta)}$ represents a lower bound on the yield $Y^X_{j,s,f(\theta)}$ in the X basis. This quantity can be calculated with the linear program given by Eq. (E.11) by simply replacing the superscript Z with X.

Finally, one can calculate the phase error rate $e_{j,\mu,f(\theta)}$ in the Z basis by means of Eq. (E.10), after replacing $e^{b,X}_{j,\mu,f(\theta)}$ with its upper bound and Δ^{μ}_{j} with the upper bound obtained after replacing a lower bound for the yield in Eq. (E.6). Importantly, with this approach there is no need to make a projection onto a finite dimensional subspace. This means that when evaluating the secret key rate formula given by Eq. (6), the probabilities $p^{L}_{n|s,f(\theta)}$ are directly given by P^{μ}_{j} as defined in Eq. (E.4).

Funding
This work was supported by Cisco Systems Inc., the Galician Regional Government (consolidation of Research Units: AtlantTIC), the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through the grant No. PID2020-118178RB-C21, MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1) and the Galician Regional Government with own funding through the "Planes Complementarios de I + D + I con las Comunidades Autónomas" in Quantum Communication, the European Union's Horizon Europe Framework Programme under the Marie Skłodowska-Curie Grant No. 101072637 (Project QSI) and the project "Quantum Security Networks Partnership" (QSNP, grant agreement No 101114043). X.S. acknowledges support from an FPI predoctoral scholarship granted by the Spanish Ministry of Science and Innovation. G.C.-L. acknowledges support from JSPS Postdoctoral Fellowships for Research in Japan. K.T. acknowledges support from JSPS KAKENHI Grant Number JP18H05237.

Abbreviations
QKD, quantum key distribution; GLLP, Gottesman, Lo, Lütkenhaus and Preskill; SDP, Semidefinite programming; LP, linear programming; PR-WCP, phase-randomized weak coherent pulse; PDF, probability density function.

Data availability
Not applicable.

Code availability
The code is available upon request from the authors.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
All authors consent to the publication of this manuscript.

Competing interests
The authors declare no competing interests.

Author contributions
M.C. identified the need for the research project, and all authors conceived the fundamental idea behind the parameter estimation technique. X.S. performed the calculations and the numerical simulations with inputs from G.C.-L. X.S. wrote the manuscript, and all authors contributed towards improving it and checking the validity of the results.

Author details
[1]Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain. [2]Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain. [3]atlanTTic Research Center, University of Vigo, Vigo E-36310, Spain. [4]Faculty of Engineering, University of Toyama, Gofuku 3190, Toyama 930-8555, Japan.

Received: 26 September 2023 Accepted: 5 December 2023 Published online: 15 December 2023

References

1. Xu F, Ma X, Zhang Q, Lo HK, Pan JW. Secure quantum key distribution with realistic devices. Rev Mod Phys. 2020;92:025002. https://doi.org/10.1103/RevModPhys.92.025002.
2. Pirandola S, Andersen UL, Banchi L, Berta M, Bunandar D, Colbeck R et al. Advances in quantum cryptography. Adv Opt Photonics. 2020;12(4):1012. https://doi.org/10.1364/aop.361502.
3. Lo HK, Curty M, Tamaki K. Secure quantum key distribution. Nat Photonics. 2014;8(8):595–604. https://doi.org/10.1038/nphoton.2014.149.
4. Wootters WK, Zurek WH. A single quantum cannot be cloned. Nature. 1982;299:802–3. https://doi.org/10.1038/299802a0.
5. Vernam GS. Cipher printing telegraph systems for secret wire and radio telegraphic communications. Trans Am Inst Electr Eng. 1926;XLV:295–301. https://doi.org/10.1109/T-AIEE.1926.5061224.
6. Sasaki M, Fujiwara M, Ishizuka H, Klaus W, Wakui K, Takeoka M et al. Field test of quantum key distribution in the Tokyo QKD network. Opt Express. 2011;19(11):10387. https://doi.org/10.1364/oe.19.010387.
7. Stucki D, Legré M, Buntschu F, Clausen B, Felber N, Gisin N et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. New J Phys. 2011;13(12):123001. https://doi.org/10.1088/1367-2630/13/12/123001.
8. Dynes JF, Wonfor A, Tam WWS, Sharpe AW, Takahashi R, Lucamarini M et al. Cambridge quantum network. npj Quantum Inf. 2019;5(1):101. https://doi.org/10.1038/s41534-019-0221-4.
9. Chen YA, Zhang Q, Chen TY, Cai WQ, Liao SK, Zhang J et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature. 2021;589:214–9. https://doi.org/10.1038/s41586-020-03093-8.
10. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE international conference on computers, systems, and signal processing. 1984. p. 175–9.
11. Huttner B, Imoto N, Gisin N, Mor T. Quantum cryptography with coherent states. Phys Rev A. 1995;51:1863–9. https://doi.org/10.1103/PhysRevA.51.1863.
12. Brassard G, Lütkenhaus N, Mor T, Sanders BC. Limitations on practical quantum cryptography. Phys Rev Lett. 2000;85:1330. https://doi.org/10.1103/PhysRevLett.85.1330.
13. Hwang WY. Quantum key distribution with high loss: toward global secure communication. Phys Rev Lett. 2003;91(5):057901. https://doi.org/10.1103/physrevlett.91.057901.
14. Wang XB. Beating the photon-number-splitting attack in practical quantum cryptography. Phys Rev Lett. 2005;94(23):230503. https://doi.org/10.1103/physrevlett.94.230503.
15. Lo HK, Ma X, Decoy CK. State quantum key distribution. Phys Rev Lett. 2005;94(23):230504. https://doi.org/10.1103/physrevlett.94.230504.
16. Lim CCW, Curty M, Walenta N, Xu F, Concise ZH. Security bounds for practical decoy-state quantum key distribution. Phys Rev A. 2014;89:022307. https://doi.org/10.1103/physreva.89.022307.
17. Zhao Y, Qi B, Ma X, Lo HK, Qian L. Experimental quantum key distribution with decoy states. Phys Rev Lett. 2006;96:70502. https://doi.org/10.1103/PhysRevLett.96.070502.
18. Rosenberg D, Harrington JW, Rice PR, Hiskett PA, Peterson CG, Hughes RJ et al. Long-distance decoy-state quantum key distribution in optical fiber. Phys Rev Lett. 2007;98:10503. https://doi.org/10.1103/physrevlett.98.010503.
19. Schmitt-Manderbach T, Weier H, Fürst M, Ursin R, Tiefenbacher F, Scheidl T et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. Phys Rev Lett. 2007;98:10504. https://doi.org/10.1103/PhysRevLett.98.010504.
20. Liu Y, Chen TY, Wang J, Cai WQ, Wan X, Chen LK et al. Decoy-state quantum key distribution with polarized photons over 200 km. Opt Express. 2010;18:8587–94. https://doi.org/10.1364/OE.18.008587.
21. Fröhlich B, Lucamarini M, Dynes JF, Comandar LC, Tam WWS, Plews A et al. Long-distance quantum key distribution secure against coherent attacks. Optica. 2017;4(1):163–7. https://doi.org/10.1364/OPTICA.4.000163.
22. Yuan Z, Murakami A, Kujiraoka M, Lucamarini M, Tanizawa Y, Sato H et al. 10-Mb/s quantum key distribution. J Lightwave Technol. 2018;36:3427–33. https://doi.org/10.1109/jlt.2018.2843136.
23. Boaron A, Boso G, Rusca D, Vulliez C, Autebert C, Caloz M et al. Secure quantum key distribution over 421 km of optical fiber. Phys Rev Lett. 2018;121:190502. https://doi.org/10.1103/PhysRevLett.121.190502.
24. Liao SK, Cai WQ, Liu WY, Zhang L, Li Y, Ren JG et al. Satellite-to-ground quantum key distribution. Nature. 2017;549(7670):43–7. https://doi.org/10.1038/nature23655.
25. Liao SK, Cai WQ, Handsteiner J, Liu B, Yin J, Zhang L et al. Satellite-relayed intercontinental quantum network. Phys Rev Lett. 2018;120:030501. https://doi.org/10.1103/PhysRevLett.120.030501.
26. Sibson P, Erven C, Godfrey M, Miki S, Yamashita T, Fujiwara M et al. Chip-based quantum key distribution. Nat Commun. 2017;8:13984. https://doi.org/10.1038/ncomms13984.
27. Bunandar D, Lentine A, Lee C, Cai H, Long CM, Boynton N et al. Metropolitan quantum key distribution with silicon photonics. Phys Rev X. 2018;8:021009. https://doi.org/10.1103/PhysRevX.8.021009.
28. Paraïso TK, De Marco I, Roger T, Marangon DG, Dynes JF, Lucamarini M et al. A modulator-free quantum key distribution transmitter chip. npj Quantum Inf. 2019;5:42. https://doi.org/10.1038/s41534-019-0158-7.
29. Marco ID, Woodward RI, Roberts GL, Paraïso TK, Roger T, Sanzaro M et al. Real-time operation of a multi-rate, multi-protocol quantum key distribution transmitter. Optica. 2021;8(6):911–5. https://doi.org/10.1364/OPTICA.423517.
30. ID Quantique SA. https://www.idquantique.com/.
31. Toshiba Europe Limited. https://www.global.toshiba/ww/products-solutions/security-ict/qkd.html.
32. QuantumCTek Co., Ltd. http://www.quantum-info.com/English/.
33. ThinkQuantum S.R.L. https://www.thinkquantum.com.
34. Quantum Telecommunications Italy S.R.L. https://www.qticompany.com.
35. Yuan ZL, Sharpe AW, Shields AJ. Unconditionally secure one-way quantum key distribution using decoy pulses. Appl Phys Lett. 2007;90:011118. https://doi.org/10.1063/1.2430685.
36. Dixon AR, Yuan ZL, Dynes JF, Sharpe AW, Shields AJ. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. Opt Express. 2008;16:18790. https://doi.org/10.1364/OE.16.018790.
37. Lucamarini M, Patel KA, Dynes JF, Fröhlich B, Sharpe AW, Dixon AR et al. Efficient decoy-state quantum key distribution with quantified security. Opt Express. 2013;21:21. https://doi.org/10.1364/oe.21.024550.

38. Valivarthi R, Zhou Q, John C, Marsili F, Verma VB, Shaw MD et al. A cost-effective measurement-device-independent quantum key distribution system for quantum networks. Quantum Sci Technol. 2017. 2:04LT01. https://doi.org/10.1088/2058-9565/aa8790.
39. Zhao Y, Qi B, Lo HK. Experimental quantum key distribution with active phase randomization. Appl Phys Lett. 2007;90(4):044106. https://doi.org/10.1063/1.2432296.
40. Sun SH, Liang LM. Experimental demonstration of an active phase randomization and monitor module for quantum key distribution. Appl Phys Lett. 2012;101:071107. https://doi.org/10.1063/1.4746402.
41. Currás-Lorenzo G, Tamaki K, Curty M. Security of decoy-state quantum key distribution with imperfect phase randomization. Preprint. 2022. arXiv:2210.08183.
42. Cao Z, Zhang Z, Lo HK, Ma X. Discrete-phase-randomized coherent state source and its application in quantum key distribution. New J Phys. 2015;17(5):053014. https://doi.org/10.1088/1367-2630/17/5/053014.
43. Currás-Lorenzo G, Wooltorton L, Twin-Field RM. Quantum key distribution with fully discrete phase randomization. Phys Rev Appl. 2021;15:014016. https://doi.org/10.1103/PhysRevApplied.15.014016.
44. Tamaki K, Curty M, Kato G, Lo HK, Azuma K. Loss-tolerant quantum cryptography with imperfect sources. Phys Rev A. 2014;90:052314. https://doi.org/10.1103/PhysRevA.90.052314.
45. Renner R, Cirac JI. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. Phys Rev Lett. 2009;102:110504. https://doi.org/10.1103/PhysRevLett.102.110504.
46. Renner R. Symmetry of large physical systems implies independence of subsystems. Nat Phys. 2007;3(9):645–9. https://doi.org/10.1038/nphys684.
47. Lo HK. Getting something out of nothing. Quantum Inf Comput. 2005;5:413–8. https://doi.org/10.26421/QIC5.45-10.
48. Gottesman D, Lo HK, Lütkenhaus N, Preskill J. Security of quantum key distribution with imperfect devices. Quantum Inf Comput. 2004;4:325–60. https://doi.org/10.26421/QIC4.5-1.
49. Koashi M. Simple security proof of quantum key distribution based on complementarity. New J Phys. 2009;8:045018. https://doi.org/10.1088/1367-2630/11/4/045018.
50. Shlok N. Decoy-state quantum key distribution with arbitrary phase mixtures and phase correlations.
51. Upadhyaya T, Himbeeck T, Lin J, Lütkenhaus N. Dimension reduction in quantum key distribution for continuous- and discrete-variable protocols. PRX Quantum. 2021;2:020325. https://doi.org/10.1103/PRXQuantum.2.020325.
52. Yin HL, Chen TY, Yu ZW, Liu H, You LX, Zhou YH et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys Rev Lett. 2016;117:190501. https://doi.org/10.1103/PhysRevLett.117.190501.
53. Lo HK, Preskill J. Security of quantum key distribution using weak coherent states with nonrandom phases. Quantum Inf Comput. 2007;8:431–58. https://doi.org/10.26421/QIC7.5-6-2.
54. Pereira M, Kate G, Mizutani A, Curty M, Tamaki K. Quantum key distribution with correlated sources. Sci Adv. 2020;6:eaaz4487. https://doi.org/10.1126/sciadv.aaz4487.
55. Winter A. Coding theorem and strong converse for quantum channels. IEEE Trans Inf Theory. 1999;45(7):2481–5. https://doi.org/10.1109/18.796385.
56. Farenick D, Bures RM. Contractive channels on operator algebras. NY J Math. 2017;23:1369–93.

Publisher's Note