Estimating the Photon-Number Distribution of Photonic Channels for Realistic Devices and Applications in Photonic Quantum Information Processing

Emilien Lavie,[1,*] Ignatius William Primaatmaja,[2] Wen Yu Kon,[1] Chao Wang,[1] and Charles Ci Wen Lim[1,2]

[1] *Department of Electrical & Computer Engineering, National University of Singapore, Singapore*
[2] *Centre for Quantum Technologies, National University of Singapore, Singapore*

(Received 1 March 2021; revised 7 May 2021; accepted 24 August 2021; published 10 September 2021)

Characterizing the input-output photon-number distribution of an unknown optical quantum channel is a worthwhile task for many applications in quantum information processing. Ideally, this would require deterministic photon-number sources and photon-number-resolving detectors, but these technologies are still work in progress. In this work, we propose a general method to rigorously bound the input-output photon-number distribution of an unknown optical channel using standard optical devices such as coherent light sources and non-photon-number-resolving detectors and homodyne detectors. To demonstrate the broad utility of our method, we consider the security analysis of practical quantum key distribution systems based on *calibrated* single-photon detectors and an experimental proposal to implement time-correlated single-photon counting technology using homodyne detectors instead of single-photon detectors.

DOI: 10.1103/PhysRevApplied.16.034020

I. INTRODUCTION

Quantum photonics is the art of using low-light optical signals to exchange and process information in the quantum regime [1,2]. Today, photonic systems represent one of the most promising platforms to implement quantum technology, with already several well-established applications ranging from quantum cryptography [3,4] and communications [5], to sensing and metrology [6–8], lithography [9], and imaging [10].

In the most general setting, one considers the preparation, transmission, and detection of optical signals. Here, the photonic channel of interest accepts an N-mode input state and returns an M-mode output state, which is then measured by a series of photon-counting devices. More formally, let $q(\vec{m}|\vec{n})$ be the probability of obtaining $\vec{m} = (m_1, m_2, \ldots, m_M)$ photons across the M output modes given $\vec{n} = (n_1, n_2, \ldots, n_N)$ photons are injected into the channel (see Fig. 1). Here, we note $q(\vec{m}|\vec{n})$ can be characterized independently of the channel's dynamics. That is, the knowledge of the channel is not needed to estimate $q(\vec{m}|\vec{n})$, i.e., we can treat the channel as a black box with N inputs and M outputs and sample accordingly. To keep the characterization as general as possible, we also allow cases in which the channel is not photon-number preserving. This can happen when the channel experiences loss and/or suffers from background noise. Correspondingly, if the channel is known to be photon-number preserving, then we have $\sum_{i=1}^{N} n_i = \sum_{j=1}^{M} m_j$.

In practice, the input-output photon-number distribution is central to a multitude of information-processing tasks. A good example is boson sampling—a type of nonuniversal quantum computation [11,12]. Here, a linear optical interferometer with N inputs and N outputs is considered, where the input is injected with a fixed number of single photons and the output measured with photon-counting devices. In Ref. [11], it was shown that $q(\vec{m}|\vec{n})$ evaluates directly the permanents of submatrices of the interferometer's matrix. On the other hand, solving such matrix permanents with a classical computer is known to be computationally hard.

Another example is quantum key distribution (QKD), particularly those using discrete variable encoding [13,14]. For such a communication system (connected by a quantum channel with one input and one output), the estimation of single-photon statistics is essential for protocol security. Take for instance $q(1|1)$, which quantifies how often the untrusted channel behaves as a true single-photon channel. Having this information strengthens the QKD security analysis by allowing one to assume that (1) the adversary forwards exactly one photon to the receiver and (2) the trusted detector noise and untrusted channel noise are separated. The former is especially powerful as it enables the

[*] emilien.lavie@u.nus.edu

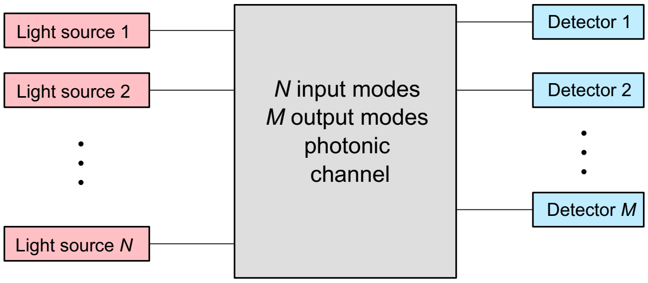

FIG. 1. Typical scheme for estimating the input-output photon-number distribution $q(\vec{m}|\vec{n})$ of a photonic channel. Each of the N input modes of the photonic channel is connected to a light source that supplies the input photons and each of the M output modes is connected to a detector that gives an outcome related to the number of photons leaving the photonic channel. Note that the sources and detectors considered here may include some form of active modulation devices, such as intensity modulators.

security analysis of practical QKD under the assumption of a qubit channel (it also applies generally to any qudit channel of interest and hence to high-dimensional QKD as well [15–17]).

As a final example, we consider time-correlated single-photon counting (TCSPC) [18,19], an optical waveform measurement technique that is widely used in fundamental physics research (e.g., ranging [20,21], imaging [22, 23], light-source characterization, and life sciences' experiments (e.g., fluorescence-lifetime imaging microscopy [24]). In this setting, the input and output optical modes of the channel are temporal modes corresponding to different time intervals. Here, we have $\sum_{i=1}^{N} n_i = 1$ and $\sum_{j=1}^{M} m_j \leq 1$ since only one photon is deployed in a single trial. In recent years, to improve the efficiency and speed of optical waveform measurement, the idea of using photon-number-resolving measurements has been proposed as well [25,26].

The input-output photon-number distribution can be easily estimated if one injects fixed photon-number states $|n_1\rangle|n_2\rangle \ldots |n_N\rangle$ into the channel and measure the output using photon-counting devices (which counts the number of photons in each output mode). However, this would require deterministic photon-number sources and photon-number-resolving detectors (PNRDs), which at the moment are still in development [1,2]. The more realistic options are probabilistic photon-number sources (e.g., coherent lasers) and non-photon-number-resolving detectors (e.g., threshold detectors and homodyne detectors); these optical devices are not only highly reliable and cost effective but also widely available.

To this end, it is natural to ask if one can use these standard optical devices to estimate the input-output photon-number distribution of an unknown photonic channel.

It is worthwhile to mention that the problem we are interested in can be seen as a special case of *coherent-state quantum process tomography* (CSQPT), which uses coherent states (probe states) and homodyne measurement to reconstruct the process matrix of an unknown optical channel [27–30]. Indeed, by looking at only the diagonal components of the process matrix, one can recover the photon-number distribution of the unknown channel. Since we are only interested in the photon-number distribution, the implementation can be significantly simplified, i.e., the probe states and local oscillators can come from independent laser sources, as we show later. Note that in the case of CSQPT, the relative phase between the probe states and the local oscillator has to be calibrated (needed to fully recover the underlying process matrix), which may be an issue in long-distance quantum-communication protocols such as QKD [31,32].

The problem of estimating the photon-number distribution of an unknown optical channel is not new and has been studied before in the field of QKD using threshold detectors. On the input side, *decoy-state method* has been proposed, which uses phase-randomized light pulses with different intensities to estimate single-photon statistics [33–35]. The method essentially entails solving a system of linear equations constrained by the different expected detection rates of the protocol. As such, there are two approaches towards solving the problem, namely one can do it analytically via Gaussian elimination [36,37] or numerically with linear programming [38,39]. The same principle can also be applied to threshold detectors to estimate the output photon-number distribution of the channel [40]. In this approach, called *detector-decoy method*, one randomly varies the detection efficiency with a variable optical attenuator or intensity modulator to generate a system of linear equations; likewise, these are constrained by the different detection rates effected by the variation of detection efficiency. Given that both decoy-state and detector-decoy methods are based on the same concept, it is thus natural to consider the combination of these two approaches. This direction was recently pursued by the authors of Ref. [41], who used the direct combination of decoy-state and detector-decoy methods to characterize multiphoton quantum-interference patterns. Alternatively, the authors of Ref. [42] used a source modulation along with PNRDs to characterize multiphoton quantum interference.

Here, based on the above ideas, we provide a systematic approach to analyze optical communication systems using a linear estimation of the photon-number statistics, extending the decoy-state, detector-decoy, and homodyne-based linear estimation methods. Our theoretical contributions are threefold: (1) the extension of Ref. [41] to homodyne detectors, (2) the security analysis of practical QKD systems based on *calibrated* single-photon detectors, and (3) an experimental proposal to implement TCSPC technology using homodyne detectors instead of single-photon detectors. Concerning the latter, there are two practical advantages in using homodyne detectors: (1) these detectors are typically much more cost effective than single-photon detectors and (2) no active intensity modulation is required to achieve the same effect as detector decoy. More generally, our extended approach with homodyne detectors provides a simpler and more cost-effective implementation path for applications that requires only the knowledge of $q(\vec{m}|\vec{n})$ instead of single-shot information (see the examples above). We also present two different methods to estimate the desired input-output photon-number probabilities: one based on Gaussian elimination and the other based on linear programming.

Additionally, we highlight that our work is focused on providing interval estimates on the photon-number statistics instead of point estimation. Indeed, our approach is essentially motivated by how parameters are estimated in QKD: there, it is imperative to provide reliable upper and lower bounds on parameters such as bit error rates and detection rates, which characterize the amount of key information leaked to the unknown channel. Therefore, the methods that we describe later include a guarantee on the statistical distance to the true value, unlike other estimation techniques such as maximum-likelihood [43] and least-squares estimation [44].

The paper is organized as follows. In Sec. II, we introduce a general channel model and the optical device models used in the estimation. Then in Sec. III, we present two methods for bounding the desired photon-number probabilities. Finally, in Sec. IV we show how our method can be used to analyze the security of practical QKD with calibrated detectors and TCSPC using homodyne detectors.

II. CHANNEL MODELING

In the following, we keep our analysis to a single-mode photonic channel (i.e., a channel with one input mode and one output mode); the generalization to multimode channels is straightforward. The starting point of our approach is the measurement function, $\{f(x,y)\}_{x,y}$, which characterizes the observed statistics depending on two designated control parameters x and y owned, respectively, by Alice (transmitter side) and Bob (receiver side). Here, the parameters are quantities used to test the unknown photonic channel. In the case of active schemes, they are random optical modulations operated by the users. In the case of passive schemes (e.g., passive decoy states [45–49] or homodyne detection as presented later in this paper), they are random variables whose outcomes are correlated to the behavior of the unknown channel.

In the most general setting, the measurement function is modeled by

$$f(x,y) = \sum_{n,m=0}^{\infty} \underbrace{p_n(x)}_{\text{transmitter}} \underbrace{q(m|n)}_{\text{channel}} \underbrace{r_m(y)}_{\text{receiver}}, \tag{1}$$

where $p_n(x)$ is the input photon-number distribution (representing correlations between a n-photon state transmission event and Alice's parameter x), $q(m|n)$ is the probability of the channel emitting m photons given it has received n photons, and $r_m(y)$ is the measurement response representing the correlation between a m-photon reception event and Bob's parameter y.

As mentioned above, our goal is to estimate certain elements of the unknown channel's input-output photon-number distribution, $q(m|n)$. To that end, we suppose the input photon-number distribution $p_n(x)$, the measurement response $r_m(y)$, and the measurement function $f(x,y)$ are fully characterized for any x and y. That is, we assume the user has complete knowledge of the underlying optical devices and has made enough measurements to accurately infer $f(x,y)$.

Similar to standard decoy-state method implementations, we use a phase-randomized coherent-wave laser to generate photon-number states at the channel's input. In this case, the light field entering the channel is described by a Poisson distribution of photon-number states

$$\rho_\mu = \sum_{n\geq 0} \frac{\mu^n e^{-\mu}}{n!} |n\rangle\langle n|, \tag{2}$$

where μ is the mean photon number of the field. The random input x is achieved by modulating the mean photon number with an intensity modulator. As such, the probability model of the source is fully characterized by x and given by

$$p_n(x) = \frac{x^n}{n!} e^{-x}. \tag{3}$$

For the measurement model, we can use either a threshold detector or a homodyne detector. In the former case, the detector only fires if some photons are detected. As such, there are only two possible outcomes, detection and no detection. Here, we consider only the no detection outcome since the detection outcome is simply the complement event. Following Ref. [40], the response of a practical threshold detector can be modeled using

$$r_m(y=\nu) = (1-p_{\rm DC})(1-\nu\,\eta_{\rm det})^m, \tag{4}$$

where $p_{\rm DC}$ is the probability of dark count, $\eta_{\rm det}$ is the single-photon efficiency of the detector, and ν is the transmission efficiency of the intensity modulator (placed in front of the detector) controlled by input y. We note that this model is general and applies to most of today's standard single-photon detection techniques, e.g., single-photon avalanche diodes (SPADs) and superconducting nanowire single-photon detectors (SNSPDs); see Ref. [50] for an overview of single-photon technology. This model is simple and might be inaccurate under specific operating conditions like fast repetition rate under which other effects like after pulses might appear. However, it is easy to replace the simple model used in Eq. (4) by a more refined model like the one suggested in Ref. [51] to account for such effects. For simplicity in this paper, we stick to the simple model to avoid unnecessary complication in the understanding of the underlying method.

In the case of homodyne detection, it does not count the number of photons in the incoming light field but rather gives an outcome whose probability density function is correlated to the number of photons [52]. This relation becomes more apparent when the local oscillator is phase randomized and the response of the detector when given m photons is given by [43,44]

$$r_m(y) = \sum_{k=0}^{m} \binom{m}{k} \frac{{\eta_{\mathrm{det}}}^k \left(1-\eta_{\mathrm{det}}\right)^{m-k}}{\sqrt{\pi}2^k k!} H_k^2(y) e^{-y^2}, \qquad (5)$$

where y is a real number and $\{H_k(y)\}_k$ are Hermite polynomials [53,54].

To estimate the desired photon-number distribution, several statistical methods can be employed, e.g., those based on linear estimation [55,56], least-squares estimation [44], and maximum likelihood [43].

Here, two observations are in order. Firstly, unlike threshold detectors, one can obtain any number of discrete outcomes by binning y—in practice, an analog-to-digital converter (ADC) is used. Secondly, notice that no additional intensity modulation is required here. This is because the response density function of a homodyne detector is sensitive to the range of y and hence one can optimize the binning function (i.e., the ADC) to assign different weights to different input photon-number states. Essentially, this is the same as the detector-decoy method, which assigns different detection probabilities to different photon-number states via the variation of the detection efficiency. Again here, the model we use in Eq. (5) is relatively simple and could be refined to include additional imperfection of realistic detectors like electronic noise [57].

III. METHODS

In most quantum-information-processing tasks, one is only interested in elements of $q(\vec{m}|\vec{n})$ that are small in the input photon number and output photon number. Additionally, the possible values for the controlled parameters x and y are limited to fixed sets $x \in \mathcal{X} := \{x_0, x_1, \ldots, x_{n_0}\}$ and $y \in \mathcal{Y} := \{y_0, y_1, \ldots, y_{m_0}\}$. We consider a practically relevant finite subset of $q(m|n)$ by focusing on $n \in \mathcal{N}_0 := \{0, 1, \ldots, n_0\}$ and $m \in \mathcal{M}_0 := \{0, 1, \ldots, m_0\}$. Our objective is to derive upper and lower bounds on a specific element or a linear combination of different elements from the set $\{q(m|n)\}_{n\in\mathcal{N}_0, m\in\mathcal{M}_0}$. As mentioned, this problem is essentially a linear optimization problem with constraints given by positivity, normalization, and the measurement distribution. More specifically, for positivity one has $q(m|n) \geq 0$ for any n and m, for subnormalization $\sum_{m=0}^{m_0} q(m|n) \leq 1$ for any n, and for measurement distribution

$$f(x,y) \geq \sum_{n=0}^{n_0} \sum_{m=0}^{m_0} p_n(x) q(m|n) r_m(y), \qquad (6)$$

for any x and y. In addition, one could also exploit the knowledge of characterized functions $p_n(x)$ and $r_m(y)$ to construct linear constraints like

$$0 \leq f(x,y) - \sum_{n=0}^{n_0} \sum_{m=0}^{m_0} p_n(x) q(m|n) r_m(y) \leq h(x,y), \qquad (7)$$

where $h(x,y)$ is some positive function depending on the optical devices used in the application. We provide some examples later in Sec. IV and more technical details in Appendix A. In the following, we present two methods to estimate the desired input-output photon-number statistics.

Linear programming method: Let $q(m^*|n^*)$ be the quantity of interest to which an upper bound is desired, then the linear programming (LP) problem is

$$\begin{aligned}
\text{maximise} \quad & q(m^*|n^*) \\
\text{subject to} \quad & 0 \leq q(m|n) \leq 1, \ \forall\, n \leq n_c, \ m \leq m_c \\
& \sum_{m=0}^{m_c} q(m|n) \leq 1, \ \forall n \leq n_c \\
& \sum_{n=0}^{n_c} \sum_{m=0}^{m_c} p_n(x) q(m|n) r_m(y) \\
& \leq f(x,y), \ \forall\, x, y \\
& \sum_{n=0}^{n_c} \sum_{m=0}^{m_c} p_n(x) q(m|n) r_m(y) \\
& \geq f(x,y) - h(x,y), \ \forall\, x, y.
\end{aligned} \qquad (8)$$

Evidently, the idea behind LP is to use the various constraints on $q(m|n)$ or some linear combination of them to provide bounds for the possible values of $q(m|n)$. Also, since the optimization is numerical, it is useful to first narrow down to a set of m and n of interest, which can be done via the truncation of both m and n up till some suitable choice of $m_c \geq m_0$ and $n_c \geq n_0$. Notably, LP is performed by first defining a feasible region where the set of input-output distribution $\{q(m|n)\}_{m\le m_c,n\le n_c}$ satisfies the constraints. One can then maximize (respectively, minimize) the desired probability $q(m^*|n^*)$ over the feasible region to obtain the upper (respectively, lower) bound on $q(m^*|n^*)$.

Analytical method: The basic idea of the second method is to leverage the complete knowledge of the characterized devices to estimate $q(m^*|n^*)$ without using any cutoff condition $n \le n_c$ or $m \le m_c$. To that end, we consider a linear combination of the measurement function [see Eq. (1)] over a finite set of evaluation points in $\mathcal{X}$ and $\mathcal{Y}$. This gives us a real-valued quantity Λ, which is defined as

$$\begin{aligned}\Lambda &:= \sum_{i=0}^{n_0}\sum_{j=0}^{m_0}\alpha_i\beta_j f(x_i,y_j)\\ &= \sum_{n,m\ge 0} q(m|n)\sum_{i=0}^{n_0}\alpha_i p_n(x_i)\sum_{j=0}^{m_0}\beta_j r_m(y_j),\end{aligned} \tag{9}$$

where coefficients $\{\alpha_i\}_{i=0}^{n_0}$ and $\{\beta_j\}_{j=0}^{m_0}$ are real numbers. Also, we write

$$u_n := \sum_{i=0}^{n_0}\alpha_i p_n(x_i), \quad v_m := \sum_{j=0}^{m_0}\beta_j r_m(y_j), \tag{10}$$

to capture the summation over all the considered evaluation points.

Here, we want to get Λ as close as possible to $q(m^*|n^*)$. To do that, we set $u_n = \delta_{n,n^*}$ and $v_m = \delta_{m,m^*}$ for all values of $n \in \mathcal{N}_0$ and $m \in \mathcal{M}_0$, where $\delta_{a,b}$ is the Kronecker δ function, and solve for α_i and β_j. In essence, this step requires solving two systems of linear equations, namely one for the source device,

$$\underbrace{\begin{bmatrix} p_0(x_0) & p_0(x_1) & \dots & p_0(x_{n_0})\\ p_1(x_0) & p_1(x_1) & \dots & p_1(x_{n_0})\\ \vdots & \vdots & \ddots & \vdots\\ p_{n_0}(x_0) & p_{n_0}(x_1) & \dots & p_{n_0}(x_{n_0})\end{bmatrix}}_{\text{Input photon-number distribution}} \begin{bmatrix}\alpha_0\\ \alpha_1\\ \vdots\\ \alpha_{n_0}\end{bmatrix} = \begin{bmatrix}\delta_{0,n^*}\\ \delta_{1,n^*}\\ \vdots\\ \delta_{n_0,n^*}\end{bmatrix}, \tag{11}$$

and one for the measurement device,

$$\underbrace{\begin{bmatrix} r_0(y_0) & \dots & r_0(y_{m_0})\\ r_1(y_0) & \dots & r_1(y_{m_0})\\ \vdots & \ddots & \vdots\\ r_{m_0}(y_0) & \dots & r_{m_0}(y_{m_0})\end{bmatrix}}_{\text{Detection response function}} \begin{bmatrix}\beta_0\\ \beta_1\\ \vdots\\ \beta_{m_0}\end{bmatrix} = \begin{bmatrix}\delta_{0,m^*}\\ \delta_{1,m^*}\\ \vdots\\ \delta_{m_0,m^*}\end{bmatrix}. \tag{12}$$

Notice that this step does not require the knowledge of $f(x_i,y_j)$ and hence can be seen as part of the calibration process prior to characterizing the channel.

Solving Eqs. (11) and (12) hence gives

$$\begin{aligned}\Lambda = q(m^*|n^*) + \sum_{n\ge n_0+1} q(m^*|n)u_n + \sum_{m\ge m_0+1} q(m|n^*)v_m\\ + \sum_{n\ge n_0+1}\sum_{m\ge m_0+1} q(m|n)u_n v_m.\end{aligned} \tag{13}$$

As one can see, Λ is now expressed in terms of the desired quantity, $q(m^*|n^*)$, and some other irrelevant terms that emanate from higher photon-number contributions, i.e., those from $n \ge n_0 + 1$ and $m \ge m_0 + 1$. In Appendix A, we show that these terms can be rigorously bounded by using known information of the optical devices. This in turn provides upper and lower bounds on $q(m^*|n^*)$. More concretely, the idea is to establish bounds on u_n and v_m using the characterized input photon-number distribution and detection-response function. Therefore, these bounds are specific to the types of light sources and detectors used in the setup; in Appendix A, we provide standard bounds for common optical devices such as phase-randomized lasers, threshold detectors, and homodyne detectors with phase-randomized local oscillators. We also note that these bounds can be made arbitrarily tight by selecting large enough n_0 and m_0 values. Indeed, a key condition is to ensure that the derived bounds on the extra terms in Eq. (13) are small when compared to $q(m^*|n^*)$; and this can be achieved by using bigger values of n_0 and m_0.

This linear method is conceptually similar to early papers in homodyne tomography using *pattern functions* to recompute photon-number statistics [55,56]. They considered the use of pattern functions $M_n(x)$ such that

$$p_n = \int_{-\infty}^{+\infty} M_n(x)f(x)dx. \tag{14}$$

Indeed, there is an obvious similarity with our method when using only one input mode:

$$\Lambda = \sum_{i=0}^{n_0}\alpha_i f(x_i), \tag{15}$$

and Λ is a good approximation of p_n up to some deviation we can bound. Our computation in Eq. (15) can be seen as a discretized version of Eq. (14). The main benefit is that it can be generalized easily beyond homodyne tomography, for instance using threshold detectors or other light sources, and as such may provide a unified understanding of photon-number probability estimation.

IV. APPLICATIONS

We present here two applications to illustrate the utility of our framework. In the first application, we consider the security of practical prepare-and-measure QKD with realistic photon sources and single-photon detectors. More specifically, we show how to rigorously bound the single-photon channel security of the protocol. In the second application, we show how to use our framework to enable TCSPC with homodyne detection instead of single-photon detection.

A. Prepare-and-measure QKD with single-photon channel security

As a first application of our method, we analyze the asymptotic security analysis of discrete-variable QKD protocols based on practical optical devices such as lasers and threshold detectors. Here, we consider the celebrated Bennett-Brassard 1984 (BB84) protocol [13] and the six-state protocol [58,59]. These two protocols are formulated as *qubit* protocols, i.e., the preparation, evolution and measurement can be described in a Hilbert space of dimension 2 [14].

In practice, however, most QKD systems use weak coherent laser sources and threshold detectors [14] to implement qubit states and measurements. This is because, as mentioned above, deterministic single-photon sources and PNRDs are not yet available and weak coherent laser sources and threshold detectors are the closest one can get to achieving qubit states and measurements in practice (at least with regards to cost and practicality). However, one critical drawback is that there are some fundamental differences between the qubit models (assumed in the protocol) and these optical devices. Some of these differences are irreconcilable and hence cannot be applied to qubit protocols, while some may lead to implementation loopholes such as photon-number splitting attacks [60,61].

Fortunately, for most qubit protocols (including BB84), the gap between theory and practice can be mitigated using innovative techniques such as the decoy-state method [33–35] and squashing [62–65]. In the case of the former, assuming that the prepared optical signals are diagonal in the photon-number basis, Eve's attacks can be categorized according to the emitted photon numbers. This allows us to focus on the single-photon component of emitted optical signal and hence view the states prepared by Alice as qubits. On the other hand, squashing models provide an elegant method to map the actual full (infinite-dimensional) mode measurement onto a finite-dimensional Hilbert space followed by the ideal measurement. In the case of the BB84 protocol, a squashing model exists and hence one could assume qubit models for Bob's measurements in practice.

Therefore, using the decoy-state method together with a squashing model, one can derive statistical bounds on the single-photon error rates of the BB84 protocol and hence compute its secret key rate. However, this approach is quite restrictive and does not apply readily to other qubit protocols. For instance, it has been shown that squashing does not immediately apply to the six-state protocol [63,66]; on the other hand, it has been shown that by relaxing certain statistical constraints, it is possible to define squashing maps for a wide range of finite-dimensional protocols [65].

By contrast, our method allows us to analyze any qubit (more generally, any higher dimension) protocol [15–17] without using a squashing model. Assuming that Alice and Bob prepare and receive a single photon defined across two orthogonal optical modes, the states and measurements can be described by qubit states and qubit measurements, respectively. Our method allows us to bound the probability of Bob receiving a single photon (just before the measurement) when Alice prepares and sends a single photon as well as the corresponding error rate in each basis.

Roughly speaking, our method provides three practical advantages over existing methods. Firstly, since we consider only secret key contributions from events in which Alice prepares a single photon and Bob receives a single photon, we can directly use any security proof technique for qubit models without applying any squashing model. As such, our method can be applied to most practical QKD systems under the condition that these systems randomly vary their detection efficiency as specified by the detector-decoy method. Secondly, since squashing models typically require mapping double-detection events to random outcomes [63,66], applying a squashing model would likely introduce some additional errors from the detector background noise. On top of that, squashing also does not differentiate between clicks due to true single-photon detections and empty detections, which may also introduce additional errors. Hence, our method, which can rigorously bound the true channel error rates, could give an enhanced bound on the secret key rate especially in the high-loss regime where the dark-count rate is not negligible. Finally, as mentioned, our method allows us to analyze the security of the protocol based on single-photon channel security. To appreciate this feature better, we comparatively note that when using the decoy-state method combined with a squashing model, one actually evaluates the security of the channel together with the detector noise, which is normally trusted. In this case, the single-photon error rates include the trusted detector noise. By contrast, our method allows the rigorous separation of channel noise and detector noise and thus provides a concise method to derive lower bounds on the secret key rate in the calibrated detector setting; in fact, the security of QKD with calibrated devices is known to be an open problem [14].

We now demonstrate how our method can be applied to the security analyses of practical QKD systems. We emphasize that our method can be used for most discrete-variable protocols, but as concrete examples, we apply only our method to the BB84 and six-state protocol. To that end, we introduce some notations that we use in this subsection only. We denote the basis choice of Alice and Bob by x and y, respectively. x and y are randomly chosen from the set $\mathcal{X}$ and $\mathcal{Y}$, respectively, where $\mathcal{X} = \mathcal{Y} = \{X, Z\}$ for BB84 and $\mathcal{X} = \mathcal{Y} = \{X, Y, Z\}$ for the six-state protocol. The symbol value encoded by Alice is denoted by $a \in \mathcal{A}$ and Bob's detection pattern is denoted by $b \in \mathcal{B}$. For both the BB84 and six-state protocol, $a \in \{0, 1\}$ and $b = b_0b_1$ is a two-bit string where b_i indicates whether the detector in mode i clicks (we have $b_i = 0$ when the detector in mode i does not click and $b_i = 1$ when the detector clicks). Based on b, Bob would then map the observed click pattern into the decoded symbol or he could choose to discard inconclusive events (such as no-click or double-click events). Finally, we denote Alice's intensity setting by μ and Bob's detection efficiency by η (composed of η_0 for detector 0 and η_1 for detector 1), which are chosen randomly in each round. We now focus our attention on the case where $|\mathcal{A}| = 2$, i.e., the protocol uses binary symbols. The generalization to a higher-dimensional protocol is straightforward.

In a typical discrete-variable protocol, Alice would randomly choose a basis x and bit value a. She would then choose an intensity setting μ and then prepare a phase-randomised coherent state in the corresponding mode. For phase-randomized coherent source, the emitted photon number n would follow a Poisson distribution with mean μ. Similarly, Bob randomly chooses a basis choice y as well as detection efficiency setting η and he obtains the outcome b. In the parameter estimation step, Alice and Bob can estimate the following conditional probabilities (for all possible combination of parameters):

$$f^{\{xyab\}}(\mu, \eta) = \Pr(b|x, y, a, \mu, \eta). \tag{16}$$

This function can be expanded as

$$f^{\{xyab\}}(\mu, \eta) = \sum_{n\geq 0} p_n(\mu) \underbrace{\sum_{k,l\geq 0} q^{\{xya\}}(kl|n) r_k^{\{b_0\}}(\eta_0) r_l^{\{b_1\}}(\eta_1)}_{Y_n^{\{xyab\}}}, \tag{17}$$

where $p_n(\mu)$ is the probability of the source emitting n photons [defined in Eq. (3)] while $q^{\{xya\}}(kl|n)$ is the probability of k photons arriving in mode 0 and l photons arriving in mode 1 given that the source emitted n photons, Alice chooses the basis x and bit value a and Bob chooses measurement basis y. $r_k^{\{b_0\}}(\eta_0)$ denotes the probability of the detector in mode 0 clicking ($b_0 = 1$) or not ($b_0 = 0$), given that k photons arrived in that mode and $r_l^{\{b_1\}}(\eta_1)$ is defined similarly. Note that the probability of a threshold detector not clicking is given in Eq. (4).

As such, Eq. (17) represents the conditional probability as a product of different system elements (transmitter, channel and receiver) in the form given in Eq. (1). The parameters x, y, a, and b are considered as fixed parameters when estimating the input-output photon-number distribution. Here, we remark that these parameters serve only as a means for Alice and Bob to organize their measurement data, i.e., they categorize the input-output photon-number distributions according to x, y, a, and b. Of note, the input-output photon-number distributions have to be independent of these parameters: this is needed to ensure that the single-photon channel behavior is *basis independent*. In other words, Eve's attacks on the quantum channel have to be independent of Alice's and Bob's basis choices [62]. In addition to this, we also need that the input-output photon-number distributions are independent of μ and η. In practice, these conditions can be reasonably enforced by using phase-randomized coherent lasers and photon-counting detectors, which is the case in our consideration.

Notice that the n-photon yield, which is denoted by $Y_n^{\{xyab\}}$ here, is the usual quantity of interest in decoy-state QKD [34]. More precisely, in Ref. [34], the authors considered events in which Alice and Bob choose the same basis, i.e., $x = y$, and the cases in which Bob observes at least one click. They also average the yield over Alice's bit value a. Hence, the n-photon yield is the probability of observing a click given that Alice's laser emits n photons. Clearly this would depend on both the channel and the trusted detectors, which are located in Bob's lab. In contrast, our method bounds the probability of k and l photons arriving at Bob's measurement device given that n photons are prepared by Alice. This would depend only on the behavior of the channel and not on the detectors.

To analyze the security of the BB84 and six-state protocol, the quantity of interest is $q^{\{xya\}}(kl|n)$ when $n = 1$ and $k + l = 1$, i.e., the probability of the channel outputting a single photon given that a single photon enters the channel. In this case, the conventional security proofs [67,68] that rely on the qubit models can be directly applied without the need for a squashing model [62,63,65]. For all values of x, y, a, it is possible to use either method of Sec. III to deduce $\{q^{\{xya\}}(10|1), q^{\{xya\}}(01|1)\}$ once $f^{\{xyab\}}(\mu, \eta)$ is obtained from the parameter estimation step of the protocol. The single-photon error rates are just functions of $\{q^{\{xya\}}(10|1), q^{\{xya\}}(01|1)\}$; for example, the single-photon error rate given that Alice and Bob have chosen the same basis (i.e., $x = y$) is given by

$$e_{x=y} = \frac{\sum_a \Pr(a) q^{\{xya\}}(a, a \oplus 1|1) \left(1 - r_a^{\{0\}}(\eta_0) r_{a\oplus 1}^{\{0\}}(\eta_1)\right)}{p_{\text{det}}^{x=y}}, \tag{18}$$

where the qubit detection probability is

$$p_{\text{det}}^{x=y} = \sum_a \sum_{k+l=1} \Pr(a) q^{\{xya\}}(k, l|1) \left(1 - r_k^{\{0\}}(\eta_0) r_l^{\{0\}}(\eta_1)\right). \tag{19}$$

Once the single-photon error rates are determined, the secret key rate can be easily computed. Here, we present the bound on the secret key rate while we defer the detailed security analysis of the six-state protocol to Appendix B. In the asymptotic limit and under the assumption of collective attacks, the secret key rate K of BB84 and six-state protocols is given by

$$\begin{aligned} K \geq\ & p_0(\mu)q(00|0)\left[1 - r_0^{\{0\}}(\eta_0)r_0^{\{0\}}(\eta_1)\right] \\ & + p_1(\mu)p_{\text{det}}^{x=y=Z}H(A|E) - Q(\mu,\eta)h_2\left[E(\mu,\eta)\right], \end{aligned} \tag{20}$$

where $H(A|E)$ is single-photon conditional entropy given Eve's quantum side information; $h_2(\cdot)$ denotes the binary entropy function. $Q(\mu,\eta)$ and $E(\mu,\eta)$ is the observed gain and quantum bit error rate when Alice and Bob choose intensity μ and detection efficiency η, respectively. Hence, the first term is the contribution due to the events in which Alice prepares vacuum state. Since no quantum information is leaked whenever Alice prepares the vacuum state, all the detected events due to the transmission of vacuum states are secure. The second term is the single-photon contribution and the third term is the leakage due to error correction assuming that the error-correcting code saturates the Shannon limit. Using $\{e_X, e_Y, e_Z\}$ as shorthand for the single-photon error rate in the respective basis, the single-photon conditional entropy $H(A|E)$ for the BB84 protocol and the six-state protocol is given by

$$H(A|E) = \begin{cases} 1 - h_2(e_X) & \text{(BB84)} \\ 1 + h_2(e_Z) - H(\lambda) & \text{(six-state)} \end{cases}. \tag{21}$$

Here, $\lambda = (\lambda_0, \lambda_1, \lambda_2, \lambda_3)$ is a real vector containing the unique solution to the following simultaneous equations:

$$\begin{aligned} \lambda_0 + \lambda_1 &= 1 - e_Z, \\ \lambda_0 + \lambda_2 &= 1 - e_X, \\ \lambda_0 + \lambda_3 &= 1 - e_Y, \\ \lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 &= 1, \end{aligned} \tag{22}$$

and $H(\lambda)$ is the corresponding Shannon entropy. Therefore, by substituting the appropriate $H(A|E)$ to Eq. (20), we obtain the bound on the secret key rate of the corresponding protocol.

We present the simulated secret key rates in Fig. 2 assuming standard SPAD parameters. Here, we compare against the asymptotic secret rate based on the standard decoy-state method [36]. As mentioned above, the key difference is that our method directly evaluates the single-photon channel security whereas the standard decoy-state method would include the detectors' background noise (dark counts). Indeed, in Fig. 3, we see that the single-photon error rate of our method does not include the detectors' dark counts in the channel error rate and hence our proposed upper bound on the error rate remains close to the exact value while that based on Ref. [36] is dominated by the dark-count noise in the high-loss regime.

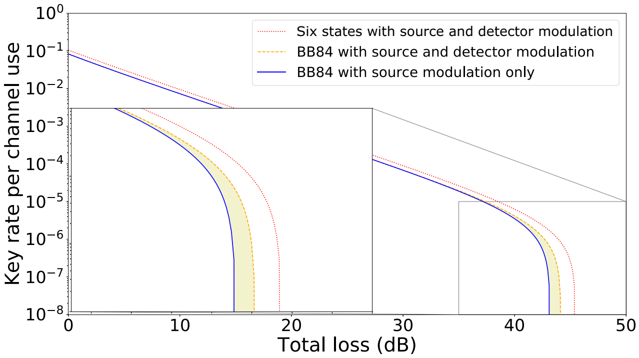

FIG. 2. We simulate the achievable secure key rate with two avalanche photodiode detectors, each one featuring a dark-count rate of 10^{-6} and a fixed channel error rate of 5% in all bases (depolarizing channel). The secure key rate in the source and detector modulation case is $K \geq p_0(\mu)q_{00|0}\left[1 - r_0^{(0)}(\eta_0)r_0^{(0)}(\eta_1)\right] + p_1(\mu)p_{\text{det}}^{x=y=0}H(A|E) - Q(\mu,\eta)h_2\left[E(\mu,\eta)\right]$ where $H(A|E)$ is the conditional entropy on Alice's key bit given Eve's side information for a qubit protocol. For BB84, we have $H(A|E) \geq 1 - h_2(e_X)$, for six states we have $H(A|E) \geq 1 - \left[H(\lambda) - h_2(e_Z)\right]$. To recompute the single-photon statistics, we use three intensity levels: $10^{-3}, 10^{-2}, 0.5$ and four efficiency levels per detector: $0.94, 0.96, 0.98, 1$. See more details in Appendix B.

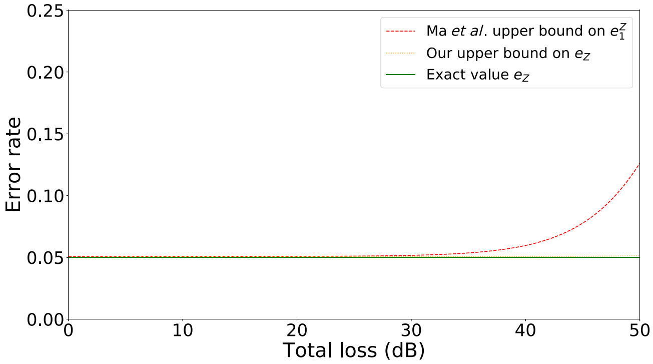

FIG. 3. We compare the exact channel error rate value used for the simulation (5% here) to the upper bound provided by our proposed analytical method and the one proposed in Ref. [36]. The definition in Ref. [36] is including the noise from the detector dark counts while our is only considering the noise on the channel. As a result, the definition of Ref. [36] is increasing while ours is staying close to the exact value in the high-loss regime, hence a slight improvement in distance for the key rate. Note that this improvement is only affecting privacy amplification, since the noise due to dark counts still has to be corrected in the error-correction step.

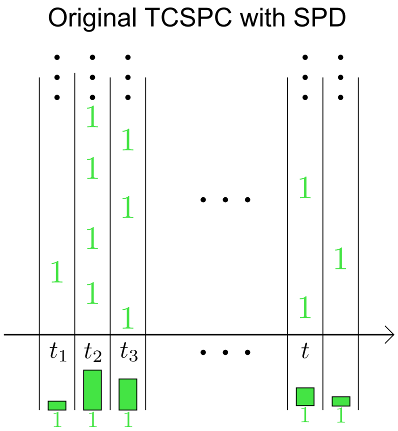

FIG. 4. The original TCSPC concept is based on the recording of single-photon detection events and construction of the corresponding histogram as shown above. As a result, there is an implicit postselection of the conclusive outcomes. That is, the experiment is repeated until the bin with the maximum number of events reaches a certain level. The histogram is then normalized to derive the probability of having a detection event in a particular bin $t \in \mathcal{T}$ given that there was a conclusive outcome C, i.e., $\Pr(t|C)$. Nevertheless, due to the dead time effect, the recorded probability is not exactly the one aforementioned, but rather the probability of observing a detection in a bin and not recording any detection before. When the counting rate is low, the two probabilities are close though [24].

B. Time-correlated single-photon counting with homodyne detection

Here we propose TCSPC with homodyne detection instead of single-photon detection. There are significant practical benefits in doing so; largely one could reduce the implementation cost and footprint of TCSPC through integrated photonics platforms. The basic idea of TCSPC is to measure the single-photon emission time profile in the nanosecond time scale, e.g., fluorescence decays of excited samples [24]. The current method achieves this via the small time resolution (hundreds of picoseconds) of single-photon detectors (SPDs; e.g., photomultiplier tubes, microchannel plates, SPADs) to measure the time difference between a reference “start” signal and a “stop” signal triggered by a single-photon emission event [18,19]. As such, by using a pulsed laser the intensity profile can be sampled repeatedly and a histogram of photon arrivals per time bin over the intended time domain can be constructed; assuming the probability of multiphoton emission is negligible. This concept is depicted in Fig. 4.

However, SPDs typically suffer from finite recovery time (or dead time); consequently, the detector becomes inactive for a period of time after a first detection event (hundreds of nanoseconds to dozens of microseconds [50, 69]). As such, any optical signal arriving during this time window will not be detected and this problem tends to bias the measurement results towards earlier detection events. This is a well-known issue called *pulse pile up* [70]. In practice, to mitigate this problem, a popular approach is to keep the multiphoton emissions low and the counting rate below 2%–5% or lower [70], e.g., by restricting the excitation power. In this case, nothing is detected most of the time and once in a while a unique photon is detected and recorded. This common approach of limiting the excitation power solves the multiphoton emission issue but leads to a longer acquisition time.

Yet, TCSPC is not making full use of the single-shot information of a photon being detected or not at a particular time window; it extracts only the average count rate for each time window. This suggests that other forms of detection technology could be used instead, for instance, homodyne detection. Indeed, this possibility has already been discussed in Ref. [71]: the authors therein described a linear method to compute the moments of an unknown probability distribution using the moments of the outcome function obtained experimentally. Our proposal with homodyne detection essentially follows this idea: that we can recover the photon-number statistics with phase-randomized homodyne detection. To help fix ideas, in the following we first briefly describe an ideal version based on PNRDs. We then provide a proof-of-concept simulation of the homodyne TCSPC technique.

1. TCSPC with perfect photon-number-resolving detection

It is useful to first consider an intermediate ideal TCSPC protocol to illustrate the main ideas of our homodyne-based protocol. Here, we assume a perfect PNRD is used to measure the photons’ arrival time. By perfect, we mean that the detector has zero dead time, perfect detection efficiency, and able to tell how many photons are detected in a given time window. Mathematically, the outcome of the protocol is described by a sequence of time-ordered random variables, $Y^{\{t\}} \in \mathbb{N}$, where each random variable counts the number of photons in the time bin $t \in T$ as shown in Fig. 5. Evidently, this ideal TCSPC protocol can recover the original TCSPC protocol’s information by keeping only the events in which $Y^{\{t\}} \geq 1$. We also highlight that there will be the same number of events recorded (regardless of the value of $Y^{\{t\}}$) in each time bin. As a result, the probability of recording an event in a certain time window is $\Pr(t) = 1/|\mathcal{T}|$.

In the limit of many repetitions, the data from $Y^{\{t\}}$ allows computation of the probability of detection of n photons in the time bin t:

$$q_n^{\{t\}} = \Pr(Y^{\{t\}} = n). \tag{23}$$

We label C a conclusive event; it is the set of photon-number values leading to a conclusive outcome, here all values $n \geq 1$. We further denote the probability of a

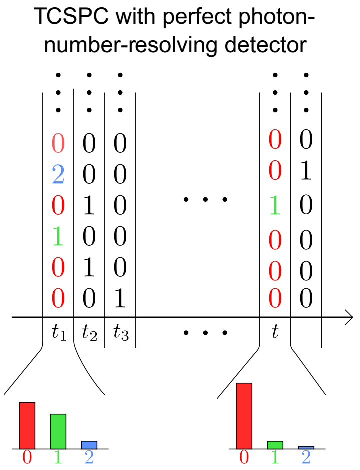

FIG. 5. We consider here an ideal version of TCSPC where perfect PNRDs are used to record the exact number of incoming photons in each time bin. We label $Y^{\{t\}} \in \mathbb{N}$ the corresponding random variable for each time bin. After enough events have been recorded, it is possible to estimate the photon-number probability distribution at each time bin. By keeping only the single-photon events, it is easy to recover the same TCSPC information as in Fig. 4.

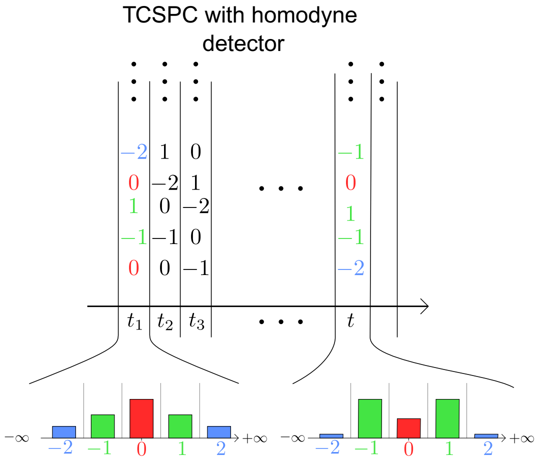

FIG. 6. We consider here a practical implementation of TCSPC using a binned homodyne detector. We label $X^{\{t\}} \in \mathcal{X}$ the corresponding random variable for each time bin. After enough events have been recorded, it is possible to estimate the measurement PDF at each time bin. Then from this information, we show that it is possible to recompute the same photon-number distribution as in Fig. 5.

conclusive event within a time window:

$$q^{\{t\}} = \Pr(C|t) = \sum_{n\in C} q_n^{\{t\}}. \tag{24}$$

From this information only, it is possible to recompute the same probability as in the original version of TCSPC using the uniformity of T and Bayes' rule:

$$\Pr(t|C) = \frac{\Pr(C|t)\Pr(t)}{\sum_{t'}\Pr(C|t')\Pr(t')} = \frac{q^{\{t\}}}{\sum_{t'} q^{\{t'\}}}. \tag{25}$$

2. Homodyne TCSPC

We now replace the perfect PNRD in the ideal version described above by a homodyne detector that sequentially measures all the time bins one after the other, up to the time resolution and speed of the ADC. In this case, the homodyne detector gives a continuous outcome, which is also binned depending on the ADC resolution. We label $\mathcal{X}$ the set of bins. Now the sequence of random variables $Y^{\{t\}} \in \mathbb{N}$ is replaced by $X^{\{t\}} \in \mathcal{X}$ as drawn in Fig. 6.

In the limit of many repetitions and small bins in $\mathcal{X}$, we can recompute the probability density function (PDF) of every time bin, which is assumed to have the following structure:

$$f^{\{t\}}(x) = \sum_{n\geq 0} q_n^{\{t\}} A_n(x), \tag{26}$$

with $A_n(x)$ representing the homodyne measurement response as we define in Sec. II Eq. (5). It is also possible to consider a binned version for f by using the binned version of $A_n(x)$ accordingly. Due to the structure of the detector, $f^{\{t\}}(x)$ is even, i.e., $f^{\{t\}}(-x) = f^{\{t\}}(x)$, hence we can simply consider only the positive region, i.e., $x \geq 0$. The $q_n^{\{t\}}$ in Eq. (26) are defined in Eq. (23) and represent the contribution to the outcome due to n photons on the detector. From the value of $f^{\{t\}}(x)$ at each $x \in \mathcal{X}$, the direct application of Sec. III allows us to recompute a reasonably good estimation of the weights $q_n^{\{t\}}$ in front of the $A_n(x)$ in Eq. (26) for the low photon-number events. Then recomputing the probability distribution as in the original TCSPC can be done with Eq. (25).

We consider a simple physical experimental model to highlight the feasibility of our homodyne TCSPC. Here, we consider the intensity profile of a fluorescence decay after a δ excitation happening at $t_0 = 50$ ns. Following Ref. [72] and assuming an exponential decay for the intensity profile, the photon-number distribution is

$$q_n^{\{t\}} = \frac{\exp\left[-E(t)\right]E(t)^n}{n!}, \tag{27}$$

where $E(t)$ is the energy arriving on the detector for $t \geq t_0$

$$E(t) = \int_t^{t+T} \alpha P(u)du = \alpha \exp\left(-\frac{t-t_0}{\tau}\right) \times \left[1 - \exp\left(-\frac{T}{\tau}\right)\right], \tag{28}$$

and $T = 5$ ns is the time-bin duration, $\tau = 100$ ns is the decay time, $\alpha = 0.9$ is a coefficient including the excitation power and the detector sensitivity. Then, the measurement

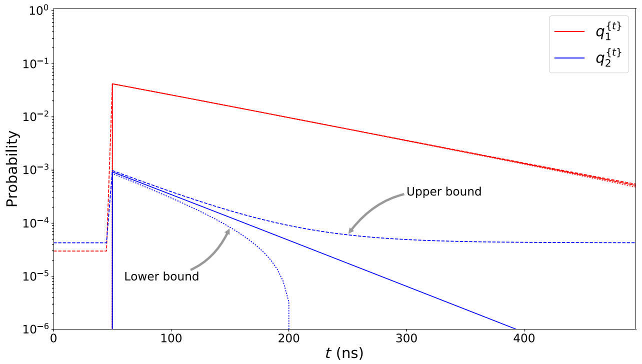

FIG. 7. Simulation of an exponential decay intensity profile that can be reconstructed using homodyne detection only. The upper (dashed line) and lower (dotted line) bound on the probability of one photon emission are very close to the exact value (solid line) using our method while the bounds on the probability of two photon emission are looser due to the inability of the method to recover very low values. This simulation is using 16 bins evenly spaced in the range [0, 5] for the real outcome given by the homodyne detector.

PDF is computed according to Eq. (26) and a direct application of Sec. III allows us to compute upper and lower bounds on the single- and two-photon emission probabilities. Here, we use 16 bins evenly spaced over the range [0, 5] and apply the analytical method presented in Sec. III to obtain the results shown in Fig. 7. The bounds on the single-photon emission probability are very close to the exact value for any time considered in our simulation while the bounds for the two-photon emission probability are less tight due to its lower value that cannot be estimated well via our method. This is due to the finite value of the extra terms in Eq. (13) as discussed in Sec. III. One way to tighten this bound would be to consider more bins for the PDF.

V. CONCLUSION

In this paper, we show the possibility of using realistic light sources and detectors to recompute relevant information about the input-output photon-number distribution of any unknown channel. We describe a simple linear framework to model characterized sources, detectors, and any multimode unknown channel. Then, we present two computational methods to derive upper and lower bounds on the input-output photon-number distribution. Such information can be used for various applications in quantum optics and quantum information processing. To that end, we highlight two applications: the single-photon channel security of practical QKD and TCSPC with homodyne detection. For example, the application to QKD shows that this framework is a bridge between practical implementations and theoretical qubit security proofs. Here, it is useful to mention that even though we present only one class of qubit protocols and an associated security proof, other finite-dimensional QKD protocols can also be proven secure in the same fashion, such as the reference-frame-independent [73], loss-tolerant [74] and tomography-based [75,76] protocols. We can also highlight that the single-photon detectors could possibly be replaced by homodyne detectors in certain schemes [77]. The TCSPC example also suggests that this technology could possibly be deployed with homodyne detection for more cost-effective implementations. Therefore, many applications relying on TCSPC as a module could potentially be upgraded to use a homodyne TCSPC instead. For instance, we can think of applications based on time-of-flight measurement [78] such as ranging [20,21] and low light imaging [22,23].

ACKNOWLEDGMENTS

We acknowledge funding support from the National Research Foundation of Singapore (NRF) Fellowship Grant (No. NRFF11-2019-0001) and NRF Quantum Engineering Programme 1.0 Grant (No. QEP-P2) and the Centre for Quantum Technologies.

APPENDIX A: BOUND DERIVATION

The goal of this section is to show that the estimate given in Eq. (13) approximates well the quantity of interest $q(m^*|n^*)$. We give practical bounds on the extra terms. First we describe the general strategy and arguments that we use regardless of the actual hardware under use, and then we give the explicit bounds for a laser source, a threshold detector and a homodyne detector.

We recall a few notations:

$$f(x,y) = \sum_{n,m\geq 0} p_n(x)q(m|n)r_m(y), \tag{A1}$$

$$\Lambda = \sum_{i=0}^{n_0}\sum_{j=0}^{m_0}\alpha_i\beta_j f(x_i,y_j) = \sum_{n,m\geq 0} q(m|n)u_n v_m, \tag{A2}$$

$$u_n = \sum_i \alpha_i p_n(x_i), \tag{A3}$$

$$v_m = \sum_j \beta_j r_m(y_j). \tag{A4}$$

Let us define the residuals:

$$\begin{aligned} R_{n_0} &= \sum_{n\geq n_0+1} q(m^*|n)u_n,\\ R_{m_0} &= \sum_{m\geq m_0+1} q(m|n^*)v_m,\\ R_{n_0m_0} &= \sum_{n\geq n_0+1}\sum_{m\geq m_0+1} q(m|n)u_n v_m. \end{aligned} \tag{A5}$$

1. General strategy

The general strategy is to compute upper and lower bounds on these individual residuals to obtain bounds on $R = R_{n_0} + R_{m_0} + R_{n_0 m_0} = \Lambda - q(m^*|n^*)$. We highlight below a few general remarks that are useful for the subsequent derivation.

1. The sequences u_n and v_m depend, respectively, on n_0 and m_0, since it is the number of terms in the summation. The values of α and β also depend on n_0 and m_0. Hence one has to be careful when considering n_0 or $m_0 \to +\infty$.
2. The series u_n has a finite zeroth moment ($\sum_{n\geq 0} u_n < +\infty$) and first moment ($\sum_{n\geq 0} n u_n < +\infty$). That is because it is related to the probability distribution of a source with finite energy.
3. The series v_m does not have a finite zeroth moment in general since it is related to a conditional probability. However, the sequence is always bounded.
4. $\forall n, m \geq 0 : 0 \leq q(m|n) \leq 1$.
5. The series $q(m|n)$ has a finite zeroth moment in m for all n: $\sum_{m\geq 0} q(m|n) = 1$.
6. The series $q(m|n)$ does not have a finite zeroth moment in n in general.

a. Bound on R_{n_0}

The best we can do for bounding R_{n_0} is to bound $q(m^*|n)$ by $+1$ or -1 depending on the sign of u_n. Let us denote

$$u_n^{\oplus} = \max(0, u_n) \geq 0, \tag{A6}$$

$$u_n^{\ominus} = \min(0, u_n) \leq 0. \tag{A7}$$

Then the bound is related to the remainder of the convergent series $u_n^{\oplus}$ and $u_n^{\ominus}$:

$$\sum_{n\geq n_0+1} u_n^{\ominus} \leq R_{n_0} \leq \sum_{n\geq n_0+1} u_n^{\oplus}. \tag{A8}$$

b. Bound on R_{m_0}

For this one, we need to combine the series $q(m|n)$ and v_m together since the former is convergent in m while the latter is not. Similarly, let us denote

$$v_m^{\oplus} = \max(0, v_m) \geq 0, \tag{A9}$$

$$v_m^{\ominus} = \min(0, v_m) \leq 0. \tag{A10}$$

Additionally we assume that the sequence $v_m^{\oplus}$ is nonincreasing for $m \geq m_0 + 1$ and similarly, $v_m^{\ominus}$ is nondecreasing for $m \geq m_0 + 1$. If it is not the case, we assume that we can find an upper (lower) bound on $v_m^{\oplus}$ ($v_m^{\ominus}$) that satisfies this property, and we use it instead. This assumption helps computation of an upper bound and lower bound on v_m by simply considering the first element:

$$\max_{m\geq m_0+1} v_m = v_{m_0+1}^{\oplus}, \tag{A11}$$

$$\min_{m\geq m_0+1} v_m = v_{m_0+1}^{\ominus}. \tag{A12}$$

In that case, we can derive the following bound:

$$v_{m_0+1}^{\ominus} \sum_{m\geq m_0+1} q_{m|n^*} \leq R_{m_0} \leq v_{m_0+1}^{\oplus} \sum_{m\geq m_0+1} q_{m|n^*}. \tag{A13}$$

We can see that this bound depends on our ability to find a good bound on

$$\tilde{q} = \sum_{m\geq m_0+1} q_{m|n^*} = 1 - \sum_{m=0}^{m_0} q_{m|n^*}. \tag{A14}$$

As a first approximation, we can use $\tilde{q} \leq 1$. It is possible to start from this rough estimate to obtain a valid upper and lower bounds on a few $q(m|n^*)$ in the range $m \in \{0 \ldots m_0\}$ and then use this information to update the bound on $\tilde{q}$. After a few iterations of this procedure, the bounds on R_{m_0} usually become of the same order of magnitude as those on R_{n_0}. Alternatively, it is also possible to analyze some geometric arithmetic sequence to compute the limit after many iterations.

c. Bound on $R_{n_0 m_0}$

This bound is easy to compute since we do not have much information anyway. The best we can do is to bound $\sum_{m\geq m_0+1} q_{m|n}$ by 1.

$$\begin{aligned} |R_{n_0 m_0}| &\leq \sum_{n\geq n_0+1} |u_n| \, \|v\|_\infty \\ &\leq \sum_{n\geq n_0+1} \max(u_{n_0+1}^{\oplus}, -u_{n_0+1}^{\ominus}) \max(v_{m_0+1}^{\oplus}, -v_{m_0+1}^{\ominus}). \end{aligned} \tag{A15}$$

The reader can notice that the bound on $R_{n_0 m_0}$ is roughly the product of the previous bounds on R_{n_0} and R_{m_0}, and hence it is small in practice, and the main contribution comes from the residuals related to source only R_{n_0} and detector only R_{m_0}. Similar to the previous cases, it is also possible to consider quantities like $\left(u_n v_m\right)^{\oplus}$ to refine $R_{n_0 m_0}$ but the improvement is limited.

2. Phase-randomized laser

We consider here a Poisson distribution for the source $p_n(x) = e^{-x}(x^n/n!)$, and $n_0 + 1$ evaluation points $0 \leq x_0 < x_1 < \cdots < x_{n_0} \leq x_{\max}$ with $x_{\max} \leq n_0$.

We notice that $p_n(x)$ is nonincreasing in n when n is larger than $x_{\max}$. It is useful to keep the sign in α otherwise the bound quickly becomes loose, therefore it is not satisfactory to simply bound α by its 1-norm or positive or negative part. However, due to the simple expression of $p_n(x)$, it is easy to check that u_n has a constant sign. Indeed, we find that $u_n \underset{n\to+\infty}{\sim} \alpha_{n_0} p_n(x_{n_0})$ so for n large enough, the sign of u_n is given by the sign of α_{n_0}. For the first few n before that property is satisfied, it is possible to numerically check a finite number of values to establish a correct upper and lower bound. For the rest, we can take

$$u_n^{\oplus} = u_n \text{ and } u_n^{\ominus} = 0, \text{ if } u_{n_0+1} \geq 0, \tag{A16}$$

$$u_n^{\oplus} = 0 \text{ and } u_n^{\ominus} = u_n, \text{ if } u_{n_0+1} < 0. \tag{A17}$$

In our examples, the sign is always constant and depending on the parity of $n^* - n_0$, similar to what Ref. [37] reported for decoy states with their bounds X_n and Z_n alternatively being lower or upper bound.

3. Threshold detectors

We consider $r_m(y) = (1-y)^m$ and $m_0 + 1$ evaluation points $y_0 \dots y_{m_0}$. We denote $\tilde{y}_j = 1 - y_j$ and assume $0 \leq \tilde{y}_0 < \cdots < \tilde{y}_{m_0} \leq \tilde{y}_{\max}$ with $\tilde{y}_{\max}$ small enough. In other words, the y_j are in a range $[1-\tilde{y}_{\max}; 1]$.

We first notice that $r_m(y)$ is nonincreasing in m for any y. We also have the following property:

$$r_{m+1}(y) = (1-y) r_m(y), \tag{A18}$$

from which we find that v_m is decreasing if it is positive and increasing if it is negative. Similar to the laser case, we find $v_m \underset{m\to+\infty}{\sim} \beta_{m_0} r_m(y_{m_0})$ where y_{m_0} is the lowest value for y. Therefore the sign of v_m is given by the sign of β_{m_0} for m large enough, then by monotonicity we find that the sign is constant for all m.

Therefore similar to the laser case, we take

$$v_m^{\oplus} = v_m \text{ and } v_m^{\ominus} = 0 \text{ if } v_{m_0+1} \geq 0, \tag{A19}$$

$$v_m^{\oplus} = 0 \text{ and } v_m^{\ominus} = v_m \text{ if } v_{m_0+1} < 0. \tag{A20}$$

4. Homodyne detectors

We use a homodyne detector at the receiver. The detection function is as follows [43,44]:

$$r_m(y) = A_m(y) = \sum_{k=0}^{m} \binom{m}{k} \eta^k (1-\eta)^{m-k} |a_k(y)|^2, \tag{A21}$$

which is a binomial mixture of Hermite functions $a_m(y)$ defined by the following recursion [44]:

$$a_{-1}(y) = 0, \tag{A22}$$

$$a_0(y) = \pi^{-(1/4)} \exp\left(-\frac{y^2}{2}\right), \tag{A23}$$

$$a_{m+1}(y) = \left(\frac{2}{m+1}\right)^{(1/2)} y a_m(y) - \left(\frac{m}{m+1}\right)^{(1/2)} a_{m-1}(y). \tag{A24}$$

Since the functions $A_m(y)$ are even, we can assume without loss of generality that the outcome y is non-negative. We further assume that $y \in [0; y_{\max}]$. This is motivated by the finite range of the ADC that will restrict the maximum observable value for the outcome.

We recall a few useful properties of $a_m(y)$ [53,54,79]:

$$\sqrt{2m} a_m(y) = y a_{m-1}(y) - a'_{m-1}(y), \tag{A25}$$

$$a'_m(y) = y a_{m-1}(y) - \sqrt{2m} a_m(y). \tag{A26}$$

We define two functions for m large enough to ensure $2m - y_{\max}^2 > 0$:

$$g_m(y) = a_m(y)^2 + \frac{a'_m(y)^2}{2m+1-y^2}, \tag{A27}$$

$$h_m(y) = a_m(y)^2 + \frac{a'_m(y)^2}{2m-y^2}, \tag{A28}$$

$g_m(y)$ was defined by Szego in Ref. [80] to prove Sonin's theorem for Hermite functions. More specifically for our purpose, $g_m(y)$ is nondecreasing in y.

We can show using Eqs. (A25) and (A26) that $h_m(y)$ also satisfies [79]

$$h_m(y) = a_{m-1}(y)^2 + \frac{a'_{m-1}(y)^2}{2m-y^2}, \tag{A29}$$

and then $g_{m+1}(y) \leq h_{m+1}(y) \leq g_m(y) \leq h_m(y)$, and hence $g_m(y)$ is nonincreasing in m. Evidently, we also have $a_m(y)^2 \leq g_m(y)$.

We define as usual

$$v_m = \sum_{j=0}^{m_0} \beta_j A_m(y_j). \tag{A30}$$

On the interval of interest, the functions $A_m(y)$ are oscillating between 0 and some local maxima. More precisely, the plot of $|a_m|$ has $m+1$ "bumps" before quickly decreasing to zero. When the detector efficiency is lower than 1, the oscillations are attenuated for the first few local extrema, and the last bump remains predominant. As a result, the series v_m is also oscillating somehow, and it is difficult to analyze.

To simplify the analysis, we use an upper bound defined as follows for m large enough to ensure $2m + 1 - y_{\max}^2 > 0$:

$$G_m(y) = \sum_{k=0}^{m} \binom{m}{k} \eta^k \big(1-\eta\big)^{m-k} g_k(y). \tag{A31}$$

Then it is sufficient to take:

$$v_m^{\oplus} = \sum_{j=0}^{m)} \max(0, \beta_j) G_m(y_j), \tag{A32}$$

$$v_m^{\ominus} = \sum_{j=0}^{m)} \min(0, \beta_j) G_m(y_j). \tag{A33}$$

APPENDIX B: SINGLE-PHOTON CHANNEL SECURITY OF QKD

We consider a binary six-state protocol where the key basis is given by the Z basis (also denoted basis 0) and the test bases are given by the X basis and Y basis (denoted, respectively, 1 and 2). The protocol operates as follows:

1. **Preparation**: Alice randomly chooses a bit value $a \in \mathcal{A} = \{0, 1\}$ uniformly $[\Pr(a = 0) = \Pr(a = 1) = \frac{1}{2}]$ and basis $x \in \mathcal{X} = \{0, 1, 2\}$ with probability $\Pr(x)$. She also randomly selects the intensity $\mu \in M$ with probability $\Pr(\mu)$. The set M has three intensity levels, and we assume that only the rounds where the highest intensity is chosen can be used to generate raw key bits. The other rounds are used for channel estimation only. In the simulation, we use $M = \{10^{-3}, 10^{-2}, 0.5\}$. She would then prepare phase-randomized coherent state with the chosen intensity μ to imprint her bit choice a in basis x on all photons in the pulse.
2. **Measurement**: Bob draws two transmissivity values $\eta_0, \eta_1 \in E$ with probability $\Pr(\eta_0)$ and $\Pr(\eta_1)$, respectively. We write in short $\eta = (\eta_0, \eta_1)$ and their indices $j = (j_0, j_1)$. The set E has four levels, and we assume that only the rounds using the highest value for both detectors are used to generate raw key bits. In the simulation we use $E = \{0.94, 0.96, 0.98, 1\}$. Bob also chooses a basis $y \in \mathcal{Y} = \{0, 1, 2\}$ with probability $\Pr(y)$. He will then set his variable attenuation for the first (second) detector to be η_0 (η_1) and perform a measurement in basis y. Finally, he records the measurement outcomes $b = b_0 b_1 \in \mathcal{B} = \{00, 01, 10, 11\}$.
3. **Sifting**: After repeating step 1 and 2 for N times, Alice and Bob use an authenticated classical channel to announce their basis choices, x and y, and their modulation settings μ, η. Then, for each tuple (μ_i, η_j), they partition the rounds into subsets $\mathcal{S}_{x,y,\mu_i,\eta_j}$ according to their basis, intensity, and transitivity modulation choices.
4. **Parameter estimation**: For rounds suitable for key generation, i.e., when $\mu = \max(M)$, $\eta_0 = \eta_1 = \max(E)$ and $x = y = 0$, Bob will disclose a—small—random subset of his measurement outcomes b when $b \neq 00$. For all other rounds, namely basis mismatch, non-key-basis match, nonmaximum signal intensity or detector efficiency, inconclusive outcome $b = 00$, Bob will disclose all outcome results b. By doing so, they can estimate the statistics $f^{\{xyab\}}(\mu, \eta)$ and use Sec. III to compute $q^{\{xya\}}(10|1), q^{\{xya\}}(01|1)$ for all relevant x, y, a and then the achievable secure key rate the way we describe below. If the latter is positive, they proceed to step 5, otherwise they abort the protocol.
5. **Postprocessing**: For the remaining rounds, Alice and Bob apply suitable error correction and privacy amplification procedures to extract the secret key.

The quantities $q^{\{xya\}}(kl|n)$ when $k + l = n = 1$ are enough to characterize the proportion of events that can be analyzed using conventional single-photon security proof. We show below how to relate them to the security of the qubit six-state protocol.

We define the qubit detection probability for a basis match as

$$p_{\text{det}}^{x=y} = \sum_{a\in\mathcal{A}} \sum_{k+l=1} \Pr(a) q^{\{xya\}}(k, l|1) \Big(1 - r_k^{\{0\}}(\eta_0) r_l^{\{0\}}(\eta_1)\Big). \tag{B1}$$

In other words, a qubit detection happens when there is only one photon in any arm of the receiver and any conclusive detection pattern occurs.

Let us assume that the detectors are labeled in a way that in the absence of noise and $x = y$, there could be photons arriving only on detector number a, according to Alice's bit. This allows us to define an ideal detection, hence any other result would be an erroneous detection. We can define the success rate for the match basis:

$$p_{\text{suc}}^{x=y} = \frac{1}{p_{\text{det}}^{x=y}} \sum_{a\in\mathcal{A}} \Pr(a) q^{\{xya\}}(a \oplus 1, a|1) \Big(1 - r_{a\oplus 1}^{\{0\}}(\eta_0) r_a^{\{0\}}(\eta_1)\Big), \tag{B2}$$

where $\oplus$ is the addition modulo 2 and the error rate is defined as $p_{\text{err}}^{x=y} = 1 - p_{\text{suc}}^{x=y}$.

For simplicity and to relate to existing notation in the literature, we denote

$$p_{\text{err}}^{x=y=0} = e_Z, \tag{B3}$$

$$p_{\text{err}}^{x=y=1} = e_X, \tag{B4}$$

$$p_{\text{err}}^{x=y=2} = e_Y. \tag{B5}$$

We rephrase the results summarised in Appendix A of Ref. [14] that is if we denote $\lambda = (\lambda_0, \lambda_1, \lambda_2, \lambda_3)$ to be the unique solution of:

$$\begin{aligned} \lambda_0 + \lambda_1 &= 1 - e_Z, \\ \lambda_0 + \lambda_2 &= 1 - e_X, \\ \lambda_0 + \lambda_3 &= 1 - e_Y, \\ \lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 &= 1, \end{aligned} \tag{B6}$$

and $H(\lambda) = -\sum_{i=0}^{3} \lambda_i \log_2(\lambda_i)$ the Shannon entropy, then the conditional entropy on Alice's bit value given Eve's side information is as follows:

$$H(A|E) \geq 1 - \Big[H(\lambda) - h_2(e_Z)\Big]. \tag{B7}$$

We also define the signal detection rate and error rate for the key basis 0:

$$Q(\mu,\eta) = 1 - \sum_{a\in\mathcal{A}} \Pr(a) f^{\{x=y=0,a,b=00\}}(\mu,\eta), \tag{B8}$$

$$E(\mu,\eta) = 1 - \frac{1}{Q(\mu,\eta)} \sum_{a\in\mathcal{A}} \Pr(a) f^{\{x=y=0,a,b=(a\oplus 1,a)\}}(\mu,\eta). \tag{B9}$$

Eventually, the achievable secure key rate against collective attacks and without sifting prefactor reads

$$\begin{aligned} K \geq\ & p_0(\mu) q(00|0)\big[1 - r_0^{\{0\}}(\eta_0) r_0^{\{0\}}(\eta_1)\big] \\ & + p_1(\mu) p_{\text{det}}^{x=y=0}\Big\{1 - \big[H(\lambda) - h_2(e_Z)\big]\Big\} \\ & - Q(\mu,\eta) h_2\big[E(\mu,\eta)\big]. \end{aligned} \tag{B10}$$

In the asymptotic analysis, we can always consider an efficient implementation where the maximum intensity μ and efficiency η are used most of the time. Otherwise, the framework allows extraction of the key from any—key state—intensity and efficiency setting. This would be interesting, for example, in combination with a fast passive decoy-state scheme [45–49] since no extra sifting would be required.

We simulate an implementation of this protocol with one common threshold detector: an (In,Ga)As SPAD with dark-count rate 10^{-6} and efficiency 100% (the actual finite efficiency is included in the total loss attributed to the channel); and a fixed channel error rate of 5% in Fig. 2. We compare the upper bound on the channel error rate given by our method and the one given in Ref. [36] in Fig. 3.

[1] F. Flamini, N. Spagnolo, and F. Sciarrino, Photonic quantum information processing: A review, Rep. Prog. Phys. **82,** 016001 (2018).

[2] S. Slussarenko and G. J. Pryde, Photonic quantum information processing: A concise review, Appl. Phys. Rev. **6,** 041303 (2019).

[3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photonics **12,** 1012 (2020).

[4] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92,** 025002 (2020).

[5] N. Gisin and R. Thew, Quantum communication, Nat. Photonics **1,** 165 (2007).

[6] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum-enhanced measurements: Beating the standard quantum limit, Science **306,** 1330 (2004).

[7] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum Metrology, Phys. Rev. Lett. **96,** 010401 (2006).

[8] V. Giovannetti, S. Lloyd, and L. Maccone, Advances in quantum metrology, Nat. Photonics **5,** 222 (2011).

[9] A. N. Boto, P. Kok, D. S. Abrams, S. L. Braunstein, C. P. Williams, and J. P. Dowling, Quantum Interferometric Optical Lithography: Exploiting Entanglement to Beat the Diffraction Limit, Phys. Rev. Lett. **85,** 2733 (2000).

[10] Y. Shih, Quantum imaging, IEEE J. Sel. Top. Quantum Electron. **13,** 1016 (2007).

[11] S. Aaronson and A. Arkhipov, in *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing*, STOC '11 (Association for Computing Machinery, New York, NY, USA, 2011), p. 333.

[12] D. J. Brod, E. F. Galvão, A. Crespi, R. Osellame, N. Spagnolo, and F. Sciarrino, Photonic implementation of boson sampling: A review, Adv. Photonics **1,** 1 (2019).

[13] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Aspects Quantum Cryptogr. **560,** 7 (2014). Celebrating 30 years of BB84.

[14] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81,** 1301 (2009).

[15] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of Quantum Key Distribution Using *d*-Level Systems, Phys. Rev. Lett. **88,** 127902 (2002).

[16] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Securing quantum key distribution systems using fewer states, Phys. Rev. A **97,** 042347 (2018).

[17] N. T. Islam, C. C. W. Lim, C. Cahall, B. Qi, J. Kim, and D. J. Gauthier, Scalable high-rate, high-dimensional time-bin encoding quantum key distribution, Quantum Sci. Technol. **4,** 035008 (2019).

[18] W. Becker, A. W. Castleman, J. Toennies, and W. Zinth, in *Advanced Time-Correlated Single Photon Counting Techniques* (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005), p. 11.

[19] D. V. O'Connor and D. Phillips, in *Time-Correlated Single Photon Counting*, edited by D. V. O'Connor and D. Phillips (Academic Press, London, UK, 1984), p. 36.

[20] M. Ren, X. Gu, Y. Liang, W. Kong, E. Wu, G. Wu, and H. Zeng, Laser ranging at 1550 nm with 1-GHz

sine-wave gated InGaAs/InP APD single-photon detector, Opt. Express **19**, 13497 (2011).

[21] A. McCarthy, X. Ren, A. Della Frera, N. R. Gemmell, N. J. Krichel, C. Scarcella, A. Ruggeri, A. Tosi, and G. S. Buller, Kilometer-range depth imaging at 1550 nm wavelength using an InGaAs/InP single-photon avalanche diode detector, Opt. Express **21**, 22098 (2013).

[22] A. M. Pawlikowska, A. Halimi, R. A. Lamb, and G. S. Buller, Single-photon three-dimensional imaging at up to 10 km range, Opt. Express **25**, 11919 (2017).

[23] R. Tobin, A. Halimi, A. McCarthy, M. Laurenzis, F. Christnacher, and G. S. Buller, Three-dimensional single-photon imaging through obscurants, Opt. Express **27**, 4590 (2019).

[24] J. Yguerabide, in *Methods in Enzymology* (Academic Press, 1972), Vol. 26, p. 498.

[25] B. Li, Q. Miao, S. Wang, D. Hui, T. Zhao, K. Liang, R. Yang, and D. Han, in *Advanced Photon Counting Techniques X*, edited by M. A. Itzler and J. C. Campbell (SPIE, Baltimore, US, 2016), Vol. 9858, p. 65.

[26] L. Dai, J. Liu, K. Liang, R. Yang, D. Han, and B. Lu, Realization of a time-correlated photon counting technique for fluorescence analysis, Biomed. Opt. Express **11**, 2205 (2020).

[27] M. Lobino, D. Korystov, C. Kupchak, E. Figueroa, B. C. Sanders, and A. I. Lvovsky, Complete characterization of quantum-optical processes, Science **322**, 563 (2008).

[28] S. Rahimi-Keshari, A. Scherer, A. Mann, A. T. Rezakhani, A. I. Lvovsky, and B. C. Sanders, Quantum process tomography with coherent states, New J. Phys. **13**, 013006 (2011).

[29] A. Anis and A. I. Lvovsky, Maximum-likelihood coherent-state quantum process tomography, New J. Phys. **14**, 105021 (2012).

[30] I. A. Fedorov, A. K. Fedorov, Y. V. Kurochkin, and A. I. Lvovsky, Tomography of a multimode quantum black box, New J. Phys. **17**, 043063 (2015).

[31] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Generating the Local Oscillator “Locally” in Continuous-Variable Quantum Key Distribution Based on Coherent Detection, Phys. Rev. X **5**, 041009 (2015).

[32] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Self-Referenced Continuous-Variable Quantum Key Distribution Protocol, Phys. Rev. X **5**, 041010 (2015).

[33] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).

[34] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[35] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[36] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).

[37] T. Tsurumaru, A. Soujaeff, and S. Takeuchi, Exact minimum and maximum of yield with a finite number of decoy light intensities, Phys. Rev. A **77**, 022319 (2008).

[38] X. Ma, C.-H. F. Fung, and M. Razavi, Statistical fluctuation analysis for measurement-device-independent quantum key distribution, Phys. Rev. A **86**, 052305 (2012).

[39] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun. **5**, 3732 (2014).

[40] T. Moroder, M. Curty, and N. Lütkenhaus, Detector decoy quantum key distribution, New J. Phys. **11**, 045008 (2009).

[41] A. Navarrete, W. Wang, F. Xu, and M. Curty, Characterizing multi-photon quantum interference with practical light sources and threshold single-photon detectors, New J. Phys. **20**, 043018 (2018).

[42] Y.-Z. Zhang, K. Wei, and F. Xu, Generalized Hong-Ou-Mandel quantum interference with phase-randomized weak coherent states, Phys. Rev. A **101**, 033823 (2020).

[43] K. Banaszek, Maximum-likelihood estimation of photon-number distribution from homodyne statistics, Phys. Rev. A **57**, 5013 (1998).

[44] S. M. Tan, An inverse problem approach to optical homodyne tomography, J. Mod. Opt. **44**, 2233 (1997).

[45] W. Mauerer and C. Silberhorn, Quantum key distribution with passive decoy state selection, Phys. Rev. A **75**, 050305 (2007).

[46] M. Curty, T. Moroder, X. Ma, and N. Lütkenhaus, Non-Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution, Opt. Lett. **34**, 3238 (2009).

[47] F. Xu, Z. Han, and G. Guo, in *Photonics and Optoelectronics Meetings (POEM) 2008: Fiber Optic Communication and Sensors*, edited by D. S. Jäger, D. Liu, and P. Shum (SPIE, Wuhan, 2009), Vol. 7278, p. 237.

[48] M. Curty, X. Ma, B. Qi, and T. Moroder, Passive decoy-state quantum key distribution with practical light sources, Phys. Rev. A **81**, 022310 (2010).

[49] C. Zhang, D. Wang, C. Zhang, and Q. Wang, A simple scheme for realizing the passive decoy-state quantum key distribution, J. Lightwave. Technol. **36**, 2868 (2018).

[50] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, Invited review article: Single-photon sources and detectors, Rev. Sci. Instrum. **82**, 071101 (2011).

[51] G.-J. Fan-Yuan, C. Wang, S. Wang, Z.-Q. Yin, H. Liu, W. Chen, D.-Y. He, Z.-F. Han, and G.-C. Guo, Afterpulse Analysis for Quantum Key Distribution, Phys. Rev. Appl. **10**, 064032 (2018).

[52] J. Shapiro, Quantum noise and excess noise in optical homodyne and heterodyne receivers, IEEE J. Quantum Electron. **21**, 237 (1985).

[53] G. Szego, in *Orthogonal Polynomials* (American Mathematical Society Colloquium Publications, Providence, US, 1939), Vol. 23, p. 105.

[54] S. Thangavelu, in *Lectures on Hermite and Laguerre Expansions* (Princeton University Press, Princeton, NJ, 1993), Vol. 42, p. 1.

[55] M. Munroe, D. Boggavarapu, M. E. Anderson, and M. G. Raymer, Photon-number statistics from the phase-averaged quadrature-field distribution: Theory and ultrafast measurement, Phys. Rev. A **52**, R924 (1995).

[56] U. Leonhardt, M. Munroe, T. Kiss, T. Richter, and M. Raymer, Sampling of photon statistics and density matrix using homodyne detection, Opt. Commun. **127**, 144 (1996).

[57] J. Appel, D. Hoffman, E. Figueroa, and A. I. Lvovsky, Electronic noise in optical homodyne tomography, Phys. Rev. A **75**, 035802 (2007).

[58] D. Bruß, Optimal Eavesdropping in Quantum Cryptography with Six States, Phys. Rev. Lett. **81**, 3018 (1998).

[59] H. Bechmann-Pasquinucci and N. Gisin, Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography, Phys. Rev. A **59**, 4238 (1999).

[60] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, Phys. Rev. A **51**, 1863 (1995).

[61] N. Lütkenhaus and M. Jahma, Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack, New J. Phys. **4**, 44 (2002).

[62] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, in *Proceedings, International Symposium on Information Theory, 2004. ISIT 2004* (IEEE, Chicago, US, 2004), p. 136.

[63] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Squashing Models for Optical Measurements in Quantum Communication, Phys. Rev. Lett. **101**, 093601 (2008).

[64] T. Tsurumaru, Squash operator and symmetry, Phys. Rev. A **81**, 012328 (2010).

[65] C.-H. F. Fung, H. F. Chau, and H.-K. Lo, Universal squash model for optical communications using linear optics and threshold detectors, Phys. Rev. A **84**, 020303 (2011).

[66] T. Tsurumaru and K. Tamaki, Security proof for quantum-key-distribution systems with threshold detectors, Phys. Rev. A **78**, 032302 (2008).

[67] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. **85**, 441 (2000).

[68] R. Renner, N. Gisin, and B. Kraus, Information-theoretic security proof for quantum-key-distribution protocols, Phys. Rev. A **72**, 012332 (2005).

[69] R. H. Hadfield, Single-photon detectors for optical quantum information applications, Nat. Photonics **3**, 696 (2009).

[70] D. Phillips, R. Drake, D. O'Connor, and R. Christensen, Time correlated single-photon counting (TCSPC) using laser excitation, Instrum. Sci. Technol. **14**, 267 (1985).

[71] F. Arecchi, A. Berne, A. Sona, and P. Burlamacchi, 1A4—photocount distributions and field statistics, IEEE J. Quantum Electron. **2**, 341 (1966).

[72] L. Mandel, Fluctuations of photon beams: The distribution of the photo-electrons, Proc. Phys. Soc. **74**, 233 (1959).

[73] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, Reference-frame-independent quantum key distribution, Phys. Rev. A **82**, 012304 (2010).

[74] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Loss-tolerant quantum cryptography with imperfect sources, Phys. Rev. A **90**, 052314 (2014).

[75] S. Watanabe, R. Matsumoto, and T. Uyematsu, Tomography increases key rates of quantum-key-distribution protocols, Phys. Rev. A **78**, 042316 (2008).

[76] Y. Zhan and H.-K. Lo, Tomography-based quantum key distribution, ArXiv:2008.11628 (2020).

[77] B. Qi, Bennett-Brassard 1984 quantum key distribution using conjugate homodyne detection, Phys. Rev. A **103**, 012606 (2021).

[78] J. S. Massa, G. S. Buller, A. C. Walker, S. Cova, M. Umasuthan, and A. M. Wallace, Time-of-flight optical ranging system based on time-correlated single-photon counting, Appl. Opt. **37**, 7298 (1998).

[79] J. Indritz, An inequality for hermite polynomials, Proc. Am. Math. Soc. **12**, 981 (1961).

[80] G. Szego, in *Orthogonal Polynomials* (American Mathematical Society Colloquium Publications, Providence, US, 1939), Vol. 23, p. 166.