Decoy-State and Purification Protocols for Superior Quantum Key Distribution with Imperfect Quantum-Dot-Based Single-Photon Sources: Theory and Experiment

Yuval Bloom,[1,*] Yoad Ordan,[1,*] Tamar Levin,[1] Kfir Sulimany,[1] Eric G. Bowes,[2] Jennifer A. Hollingsworth,[2] and Ronen Rapaport[1,†]

[1] *Racah Institute of Physics, The Hebrew University of Jerusalem, Jerusalem 9190401, Israel*
[2] *Materials Physics and Applications Division: Center for Integrated Nanotechnologies, Los Alamos National Laboratory, Los Alamos, New Mexico 87545, USA*

(Received 1 October 2024; revised 26 May 2025; accepted 14 July 2025; published 21 August 2025)

The original proposal of quantum key distribution (QKD) was based on ideal single-photon sources, which, 40 years later, are still challenging to develop. Therefore, the development of decoy-state protocols using weak coherent states (WCS) from lasers set the frontier in terms of secure-key rates and distances. Here, we propose and experimentally demonstrate two simple-to-implement QKD protocols that allow practical far from ideal sub-Poissonian photon sources to outperform state-of-the-art WCS. By engineering the photon statistics of a biexciton-exciton cascade in room-temperature single-photon sources based on giant colloidal quantum dots coupled to nanoantennas, we show that either a truncated decoy-state protocol or a heralded-purification protocol can be employed to achieve a significantly increased performance in terms of the maximal allowed channel loss for secure-key creation, which can exceed even that of ideal WCS by more than 3 dB. We then experimentally emulate a BB84 QKD using such a quantum dot source, verifying the superiority of our protocols over the best possible BB84 WCS performance. These protocols can be utilized efficiently on a host of various quantum emitters having controllable photon statistics with a finite photon-number basis, offering a practical approach to QKD without the hindering requirements on the single-photon purity of the photon source.

DOI: 10.1103/7fdd-m92n

I. INTRODUCTION

Quantum key distribution (QKD) stands as a prominent candidate for post-quantum-computer optical communication, enabling a secure-key-establishing protocol between two parties employing the quantum nature of light [1–3]. In theory, encoding the information for QKD onto pure single-photon states is ultimately secured. In practice, it is limited by imperfections of the transmitter and the receiver, making security proofs a challenging task [4,5], thus reducing the maximal secure-key rate (SKR) and the maximal losses in the communication channel over which the SKR is achievable [6,7].

One of the main practical limitations of QKD systems is the lack of an ideal source for single photons, required to prevent eavesdropping attacks such as photon-number-splitting (PNS) attack [8]. The SKR and maximal allowed channel loss (MCL) of simple QKD protocols decrease dramatically with the increase of two-or-more-photon events being transmitted from the source [9,10]. This leads to very stringent requirements on both the single-photon purity and the photon emission rate of any practical single photon source (SPS) [11].

Despite many years of exploration and engineering [12,13], a simple stable SPS system that has the required aforementioned properties and can be employed in real-life QKD applications is still an outstanding challenge, which has led researchers to suggest and utilize protocols employing attenuated lasers emitting weak coherent states (WCS) [14]. As WCS have a Poissonian distribution of photons, and thus a two-or-more-photons probability is never vanishing, advanced protocols such as decoy-state protocols have been developed to enhance both the SKR and the MCL [11,15–18].

Decoy-state protocols introduce variations in the distribution of the emitted photons to better characterize the channel and obtain a tighter bound on the SKR [19–22], allowing detection of PNS attacks [23,24]. Yet,

*These authors contributed equally to this work.
†Contact author: ronen.rapaport@mail.huji.ac.il

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

even with decoy-state protocols, WCS are highly sensitive [25,26] to the high probability of the vacuum state, due to the dependence between the different photon-number emission probabilities, which overall limits the possible SKR [9]. The above solutions and inherent limitations of WCS for QKD set clear opportunities for improving the security and efficiency of QKD applications using realistic SPS systems, such as solid-state emitters [27–32] and spontaneous parametric down-conversion heralded sources [33,34]. Yet, while efforts to develop a nearly ideal SPS are still ongoing by many groups [35–39], they still fall short as compared to the performance of QKD protocols based on WCS incorporating decoy states.

Here, we introduce a radically different more realistic approach. By utilizing two new simple QKD protocols on compact imperfect SPSs, we significantly enhance the QKD performance in terms of the MCL, as compared to even ideal infinite decoy-state protocols using WCS.

We base our protocols on our recent demonstrations of room-temperature-operating SPS devices based on a giant colloidal nanocrystal quantum dot (gCQD) coupled to a hybrid nanoantenna and plasmonic nanocone [40–44]. These SPS devices displayed a highly enhanced rate of photon emission approaching the gigahertz range, together with near-unity collection efficiencies ($> 90\%$) of the emitted photons. The photon emission from such gCQDs is based on the biexciton-exciton (BX-X) emission cascade under optical excitation [45] and has been shown to be well described by a truncated photon-number Fock space with $N = 0$, 1, and 2 photons, with a negligible probability of $N > 2$ photons [46].

The two protocols are both based on our ability to vary and control the probabilities of emitting the different Fock states, $\{P_0, P_1, P_2\}$, over a wide range of values, by simply varying the optical excitation power. The first protocol that we implement is a simple and realistic decoy-state protocol for such a source. We show that with this new protocol, we can significantly exceed, by more than 3 dB, the MCL value of an ideal decoy-state protocol using a WCS source. The second protocol uses an alternative approach based on heralded photon purification under saturated excitation. We show that a similar performance enhancement can also be achieved. Later, we experimentally verify that the probability for $N > 2$ ($P_{N>2}$) is negligibly small, justifying the assumptions of our protocol. Finally, we experimentally fully emulate a free-space BB84 QKD using a bare gCQD source without an antenna. The results agree well with the models and demonstrate the superiority of our protocols over the best possible BB84 WCS performance even for such a simple imperfect SPS. This shows that even existing SPSs, which are far from being ideal, can outperform the current state-of-the-art protocols based on WCS sources.

II. OPTICAL CONTROL OF PHOTON STATISTICS FROM THE BX-X EMISSION CASCADE IN A gCQD

In Fig. 1(a), we present a schematic sketch of the BX-X cascade in a gCQD (see Appendix A) following a nonresonant pulse excitation with power I. Modeling this process, a BX state $|XX\rangle$ is excited by the absorption of *two pump photons*. This process happens with a probability

$$P_{XX} = \frac{(\alpha I)^2}{1 + \alpha I + (\alpha I)^2}. \tag{1}$$

The probability of excitation of only the X state, $|X\rangle$, by the absorption of *only one pump photon*, is given by

$$P_X = \frac{\alpha I}{1 + \alpha I + (\alpha I)^2}. \tag{2}$$

Here, α is a constant related to the absorption cross section of the gCQD and we assume that any larger excitonic complexes are negligible [46], as will be verified later in this paper.

Following an optical excitation, the biexciton state $|XX\rangle$ decays into a single-exciton state $|X\rangle$ either radiatively, by emitting a single photon with a probability QY_{XX}, representing the BX quantum yield, or nonradiatively with a probability $1 - QY_{XX}$. The exciton state $|X\rangle$ can then recombine radiatively (nonradiatively) with probabilities QY_X $(1 - QY_X)$ to the ground state such that the probability of emitting zero, one, or two photons, defined as $\{P_0, P_1, P_2\}$, respectively, is as follows:

$$P_1 = P_{XX}\,(\phi_X + \phi_{XX} - 2\phi_X\phi_{XX}) + P_X\phi_X, \tag{3}$$

$$P_2 = P_{XX}\phi_X\phi_{XX}, \tag{4}$$

$$P_0 = 1 - P_1 - P_2. \tag{5}$$

where we defined ϕ_i as the QY_i for state i. Since P_{XX} and P_X depend on the excitation power, the probabilities of emitting two, one, or zero photons following excitation become excitation power dependent, allowing external control over the emitted photon statistics, as is required for decoy-state protocols. Such a saturable behavior of the excitonic population allows us to define a relative excitation power $S = I/I_S$, where I_S is the saturation power, for which the detected count rate (which is linearly proportional to the average emission photon number) reaches 90% (a convenient arbitrary value) of the maximum value (which asymptotically occurs at $I \to \infty$).

In Fig. 1(b), we experimentally demonstrate photon statistics control by varying the excitation power from a single bare gCQD. As S increases, the collected photon emission intensity increases sublinearly and saturates at

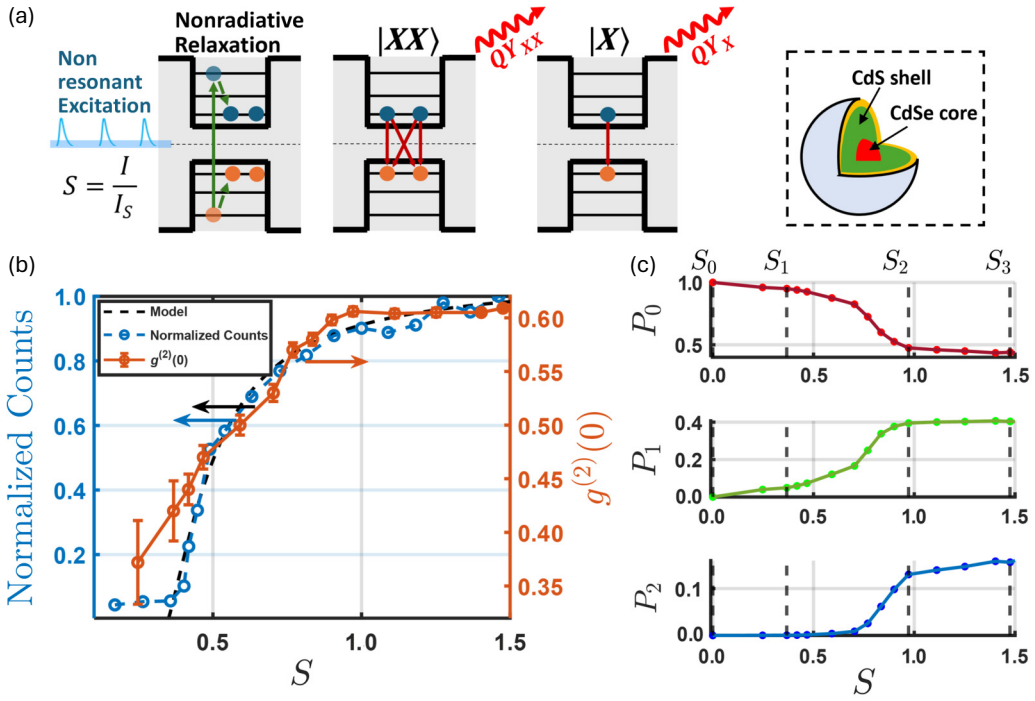


FIG. 1. (a) A schematic of the BX-X cascade in an optically excited gCQD, using a nonresonant pulsed excitation with a normalized intensity $S = I/I_S$. The inset shows a sketch of a typical gCQD, consisting of a CdSe core and a CdS shell. (b) The normalized emission counts (open blue circles) as a function of S, displaying a saturation behavior. The dashed black line is a fit to a model, detailed in Sec. II. The orange circles show the experimentally extracted $g^{(2)}(0)$ for the different powers. (c) The photon probabilities as a function of S. The dashed black lines mark the intensities chosen for the signal S_2 and the two decoy states, S_0 and S_1, for the decoy state on a truncated basis (DTB) protocol, and the intensity S_3, chosen for the heralded-purification (HP) protocol.

$S \gtrsim 1$. A good fit of the theoretical model, based on the absorption probabilities given in Eqs. (1) and (2) and on the subsequent emission probabilities QY_X, QY_{XX} is shown (for details, see Appendix B). This fit confirms the basic assumptions given above for the BX-X cascade process.

At the same time, the measured second-order correlation function, $g^{(2)}(0)$, increases in a similar manner. This is understood in the following way: at low powers, most emission events are empty, as P_0 is the dominant term. As S increases, P_1 increases linearly [Eq. (2)], while P_2 increases quadratically and thus is negligible at $S \ll 1$. Since $g^{(2)}(0)$ is an increasing function of $P_2/(\sum_{i=0,1,2} P_i)$, a saturable behavior of $g^{(2)}(0)$ with increasing S is also expected.

Importantly, as we also show experimentally (see Appendix D) that multiexcitonic ($N > 2$) emissions from the gCQD can be neglected due to their low emission probability and thus $P_{N>2} = 0$.

By measuring both $g^{(2)}(0)(S)$ and the count rate $C(S)$, we can extract the probability distribution precisely, as is detailed in Appendix C.

In Fig. 1(c), we present the extracted photon emission probabilities $\{P_0, P_1, P_2\}(S)$. As expected, the probability of emitting one or two photons increases with the excitation power but at a different rate, allowing optical control of the emitted photon statistics with only varying S.

III. QKD PROTOCOLS OUTPERFORMING WCS

After establishing the control of the different photon-number probabilities, we now utilize this capability for two MCL-enhancing protocols, the first is a decoy-state protocol and the second is a heralded-purification (HP) protocol.

A. Decoy state on a Truncated Fock Basis (DTB)

In Fig. 2(a), we present the conceptual experimental setup of the decoy-state protocol. Here, an SPS with a near-unity photon collection efficiency, $\eta_c \simeq 1$ [43] (labeled as SPS1), is used for implementing a BB84 protocol, but where Alice controls the excitation powers, $S_0 = 0, S_1$, and S_2. This in turn modifies the photon-number statistics, thus allowing for the implementation of decoy and signal states [11,15].

To establish the DTB protocol, we define the gain of the signal (decoy$_i$) state, Q_s ($Q_{d,i}$), as the fraction of encoded photon pulses sent by Alice and detected by Bob [Eq. (11)]. We also define the error rate of the signal (decoy$_i$), E_s

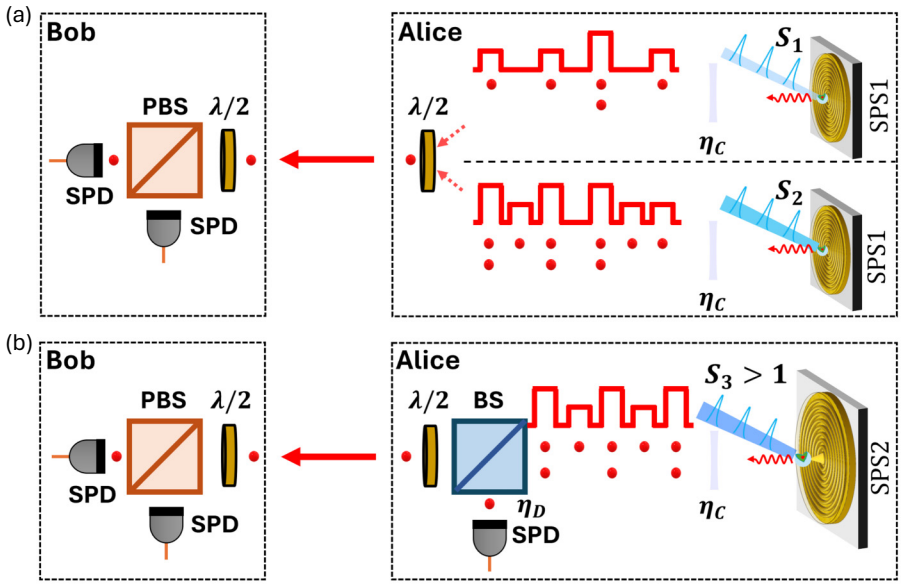


FIG. 2. The concept of two protocols based on a high-rate high-collection-efficiency SPS with imperfect purity. (a) The experimental setup and a sketch of the BB84+DTB protocol, with Alice adjusting the excitation power on the SPS between $S_0 = 0$, S_1, and S_2 to control the emitted photon statistics for the two-decoy protocol, followed by collection optics with efficiency η_C and a standard BB84 encoding unit. (b) The experimental setup and a sketch of the BB84+HP photon-purification protocol. A single excitation power $S_3 > 1$, near the gCQD saturation, is used to excite the SPS, followed by collection optics with efficiency η_C, a beam splitter (BS), a high-efficiency single-photon detector (SPD) with detection efficiency η_D, and a standard BB84 encoding unit. Here, only same-pulse detections at Alice and Bob are used for the secure key. An algorithmic representation of the two protocols is given in Appendix H.

($E_{d,i}$), as the fraction of detected encoded photons that had errors [Eq. (12)]. The signal pulses correspond to pulses with excitation S_2, while the decoy pulses are those excited with S_1 and S_0. We show in the following that due to the truncated photon-number basis of our SPS, only two different decoy states are enough for exact analysis in the framework of the decoy-state protocol [11].

Within the DTB protocol, Alice can randomly choose to replace the signal pulse with one of the two decoy states with different photon-number distributions. These decoy states are not used to create the secure key but to improve the information about the channel and discover any possible eavesdroppers [15]. In the postprocessing stage, Alice and Bob can verify the fraction of detected events and the errors for both signal pulses and decoy pulses, thus obtaining the gain and error rates $\{Q_s, Q_{d,i}, E_s, E_{d,i}\}$.

On the other hand, due to the uncertainty of the photon number in each pulse, the gain and error rate for a specific n-photon state, $\{Q_n, e_n\}$, cannot be measured directly and has to be estimated or calculated. Out of this set, the single-photon gain (Q_1) and error rate (e_1), which are the probability that a detected event (Bob) will originate from a single-photon pulse (Alice) and the error rate for single-photon pulses, respectively, are of particular importance. This is since, considering a possible PNS attack by Eve, only information encoded on the single-photon pulses is secured.

Crucially, in our three-intensity DTB protocol, these parameters can be solved exactly, since the probability distribution of the signal and decoy states, $\{P_n^s\}, \{P_n^{d,i}\}$ is known [see, e.g., Fig. 1(c)]. To relate the measured values $\{Q_s, Q_{d,i}, E_s, E_{d,i}\}$ to the unknown set $\{Q_n, e_n\}$, it is useful to define the n-photon yield, Y_n, as the conditional probability of a detection event given that Alice sent an n-photon state and therefore $Q_n = Y_n P_n$. With these definitions, the following set of equations can be written [15]:

$$\begin{aligned} Q_s &= \sum_{n=0}^{2} P_n^s Y_n, \qquad E_s Q_s = \sum_{n=0}^{2} P_n^s Y_n e_n, \\ Q_{d,i} &= \sum_{n=0}^{2} P_n^{d,i} Y_n, \qquad E_{d,i} Q_{d,i} = \sum_{n=0}^{2} P_n^{d,i} Y_n e_n. \end{aligned} \tag{6}$$

Importantly, unlike the decoy-state protocol implemented for WCS, where $n \to \infty$, which requires an infinite set of decoy states for an exact solution [11], here $n = 0, 1, 2$ only, due to the truncated sub-Poissonian nature of the gCQD photon emission ($N > 2$ photon emissions are neglected). Thus, our equations have only six unknowns, $\{Y_0, e_0, Y_1, e_1, Y_2, e_2\}$, suggesting that two decoy states are enough for an exact solution to these equations. This makes the DTB implementation particularly viable,

TABLE I. Realistic parameter values for the analysis presented in Figs. 3(a), 3(b), and 6(c), done for the DTB protocol using a gCQD-based nanoantenna device [43] (SPS1), the HP protocol using a gCQD-based nanocone and nanoantenna device [41] (SPS2), and an experimental demonstration of both protocols using a bare gCQD. P_1 and P_2 denote the one- and two- photon probabilities, respectively.

Source	Protocol	P_1	P_2
SPS1	DTB	0.529	0.112
SPS2	HP	0.458	0.427
Bare gCQD	DTB—decoy (S_1)	0.096	0.0017
Bare gCQD	DTB—signal (S_2)	0.296	0.029
Bare gCQD	HP (S_3)	0.3231	0.1114

whereas for WCS, using two decoy states would only give a bounded approximation for the yield and errors [15].

The solution of these equations can then be used to estimate the minimum SKR after privacy amplification and error correction, defined as R_1 for the DTB protocol [11]:

$$R_1 \geq q\{-Q_s f(E_s) H_2(E_s) + Q_1 [1 - H_2(e_1)]\}, \quad (7)$$

where $q = 0.5$ for the BB84 protocol [1], H_2 is the binary Shannon information function [11], and $f(E_s)$ is the error-correction efficiency (taken to be 1.22 [47]).

Assuming $\eta_C \simeq 1$ for a gCQD coupled to a nanoantenna [43] and using the P_0, P_1, and P_2 probability values above, we numerically calculate the SKR of such a source for different channel losses. To do this, we use the channel model connecting the losses, yields, and gains and the error rates shown in Ref. [11] and in Appendix E with the parameters values (from Refs. [41,43,48,49]) presented in Table I and Appendix G. Specifically, we set the probability of reaching the wrong detector to $e_d = 3.3\%$ and Bob's detection efficiency to $\eta_{\text{Bob}} = 4.5\%$.

In Fig. 3(a), we show the calculated SKR under different channel losses for a standard WCS with decoy states in the ideal simulated asymptotic case (infinite number of decoy states) with optimized Poissonian distribution parameters, as given by Ref. [15], setting the detection efficiency and error probability as previously explained. This has been compared to an SPS based on a gCQD coupled to a nanoantenna (SPS1) [43] using the above DTB protocol with the realistically obtainable probabilities of the signal state for such a device (see Appendix G). A clear improvement in the SKR and the MCL of our imperfect SPSs over WCS is seen, with over 3-dB MCL enhancement, and also an improvement over the best existing cryogenic

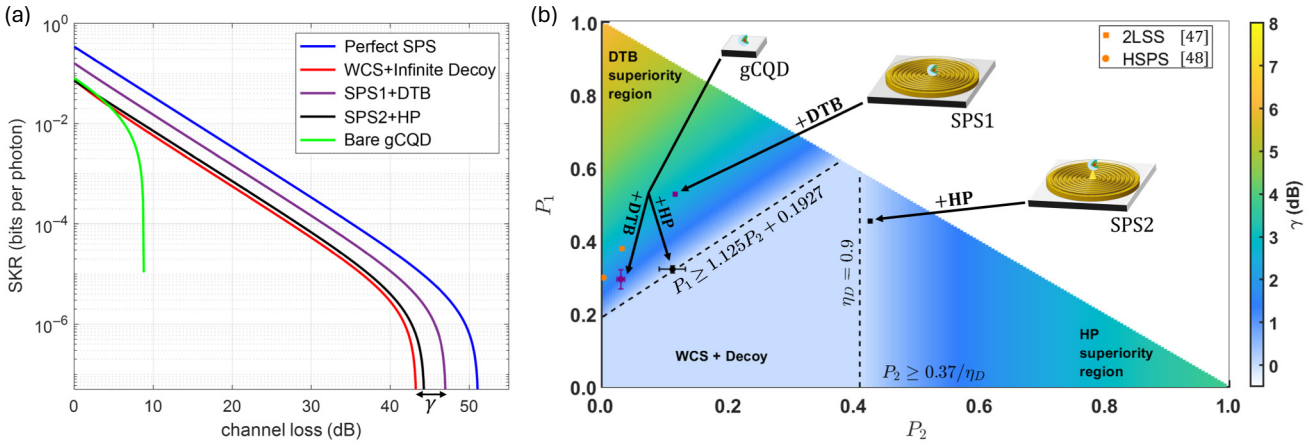


FIG. 3. QKD analysis with imperfect single-photon sources. (a) The secure-key rate (SKR) of the BB84 protocol as a function of the channel loss for a perfect SPS (blue line), WCS with infinite decoy states and optimized intensities (WCS+Infinite Decoy, red), SPS1 with the decoy state on a truncated-Fock-basis protocol (SPS1+DTB, purple), SPS2 with the heralded purification protocol (SPS2+HP, black), and a typical gCQD (bare gCQD, green), with a visual representation of γ, the relative gain. The method and parameters of the calculations are found in Table I and in Appendix G and also in Secs. III A and III B. (b) The relative gain of the maximal allowed channel loss (MCL), γ, as a function of P_1 and P_2, showing two advantageous regimes for SPSs with either DTB or HP separated by dashed black lines, with their respective conditions. We also present our sources: a bare single gCQD experimentally measured for the DTB protocol (purple circle) and the HP scheme (black circle) at different intensities (hence different photon statistics), SPS1 in the purification regime (purple square), SPS2 in the decoy-state regime (black square), and two, previously analyzed, nonclassical sources [49,50] marked with an orange square or dot.

state-of-the-art SPS [28,31,32] or comparable cryogenic fiber-coupled results [51]. We also show a comparison with a perfect single-photon source ($P_1 = 1$). Surprisingly, applying our truncated decoy-state protocol yields performance not far worse than that of a perfect SPS, even though our SPS, operating under ambient conditions, is far from being ideal.

B. Heralded Purification (HP)

In Fig. 2(b), we present the experimental configuration of the HP protocol (BB84+HP). In this scheme, we consider an SPS consisting of a gCQD on a hybrid nanocone-antenna device (here, labeled as SPS2). Such a device has shown both $\eta_C \simeq 1$ together with high attainable values of P_2, resulting from a large Purcell factor induced by the nanocone, which significantly enhances QY_{XX} [41,52]. Alice operates at a single excitation power $S_3 > 1$, deep in the saturation regime, to excite the BX state with a very high probability, thus maximizing P_2, which is now only limited by QY_{XX} and QY_X [41]. A beam splitter (BS) and a single-photon detector (SPD) are added as a purification stage in Alice's system, in the emission line of the SPS and before the standard BB84 encoding unit. As $P_{N>2}$ are negligible (see Appendix D), a real photon detection event in Alice's detector sets $\tilde{P}_2 = 0$ for that pulse, where $\tilde{P}_n$ is the effective photon-number probability after the purification stage. In the sifting step of the QKD protocol, only events with same-pulse detections by Alice and Bob are considered for the secure key, thus eliminating all multiphoton events at a cost of lower signal rates.

Given an SPS having $\{P_0, P_1, P_2\}$, the effective distribution sent to Bob with the HP protocol depends on the reflectance and transmission (R and T) of the BS and the detection efficiency of Alice's detector (η_D), as well as the probability of a dark count at Alice's detector (P_{DC}):

$$\tilde{P}_1 = 2P_2RT(\eta_D + P_{\mathrm{DC}}) + TP_1P_{\mathrm{DC}}, \tag{8}$$

$$\tilde{P}_2 = T^2P_2P_{\mathrm{DC}}. \tag{9}$$

Given this new distribution, we can again follow the well-established method to estimate the SKR of a BB84 protocol (but now implemented with HP) [11,53]. Here, the estimated SKR after privacy amplification and error correction, defined as R_2 for the HP protocol, is given by [2]

$$R_2 \geq qQ_s\left\{-H_2(E_s) + \Omega\left[1 - H_2\left(\frac{E_s}{\Omega}\right)\right]\right\}, \tag{10}$$

where $\Omega = \tilde{P}_1 Y_1/Q_s$ is the relative error of the quantum channel and H_2, q, E_s, and Q_s are defined similarly to the DTB protocol.

The black line in Fig. 3(a) shows a realistic calculation of the SKR using actual parameters of SPS2 measured in Ref. [41] (presented in Table I and in Appendix G). A BS reflectance of 50% has been chosen and we specifically use $P_{\mathrm{DC}} = 2 \times 10^{-7}$ corresponding to 100 dark counts/s for a 500-MHz signal rate, both of which are commonly attainable with current technology. Again, as is seen in the figure, the new BB84+HP allows for a higher MCL (approximately 1 dB) compared to WCS with infinite decoy, due to the extremely low $\tilde{P}_2$. Remarkably, this SKR enhancement can be achieved with SPSs far from being ideal and having a very low single-photon purity.

C. Performance analysis

Next, we analyze the expected performance of a realistic SPS-based BB84 QKD using the above protocols, in comparison to that of WCS with ideal decoy protocols. In particular, we compare the expected performance of our existing room-temperature high-brightness high-collection-efficiency SPS [41,43]. We define the relative gain in the MCL, defined as L, as $\gamma = (L/L_{\mathrm{WCS}})$ and use this parameter to evaluate the relative performance gain.

In Fig. 3(b), we show a color map of the calculated γ for different values of P_1 and P_2 of the SPS. For high P_1 and sufficiently low P_2—namely, for $P_1 > 1.125P_2 + 0.1927$—there is a region (marked as "DTB superiority region") in which $\gamma > 0\,\mathrm{dB}$, indicating that the use of an SPS with the BB84+DTB protocol is advantageous over WCS with BB84 including infinite decoy states (marked as "WCS+Decoy"). In this region, we highlight in orange dots two known nonclassical sources [49,50] along with our device (SPS1) consisting of a gCQD coupled to a metal-dielectric Bragg nanoantenna [43] (purple), demonstrating that already existing sources, when combined with the DTB protocol, can outperform even ideal WCS protocols. Notably, the use of DTB allows for an SPS with higher probabilities of two-photon events and shows that bright devices (with fewer vacuum events) can be used for QKD even with single-photon purities as low as approximately 65% and $g^{(2)}(0)$ values as high as approximately 0.6.

On the other hand, for an SPS with high enough values of P_2, there is a region in which BB84+HP is advantageous over WCS+Decoy, as shown in the right corner of Fig. 3(b) (marked as "HP superiority region"), where again $\gamma > 0\,\mathrm{dB}$. In the implementation of the HP protocol, most one-photon events are discarded and the key is composed largely of two-photon emission events, as indicated in Eq. (8), where the first term is dominant since $P_{\mathrm{DC}} \ll P_1, P_2$. Therefore, the HP method is most advantageous in the regime in which P_2 is large, regardless of P_1. The negligible probability of two-photon events after purification ($< 10^{-7}$) and minor contributions of the second and third terms in Eq. (8) result in an effectively pure source, differing from a perfect SPS only in brightness (through the zero-photon probability).

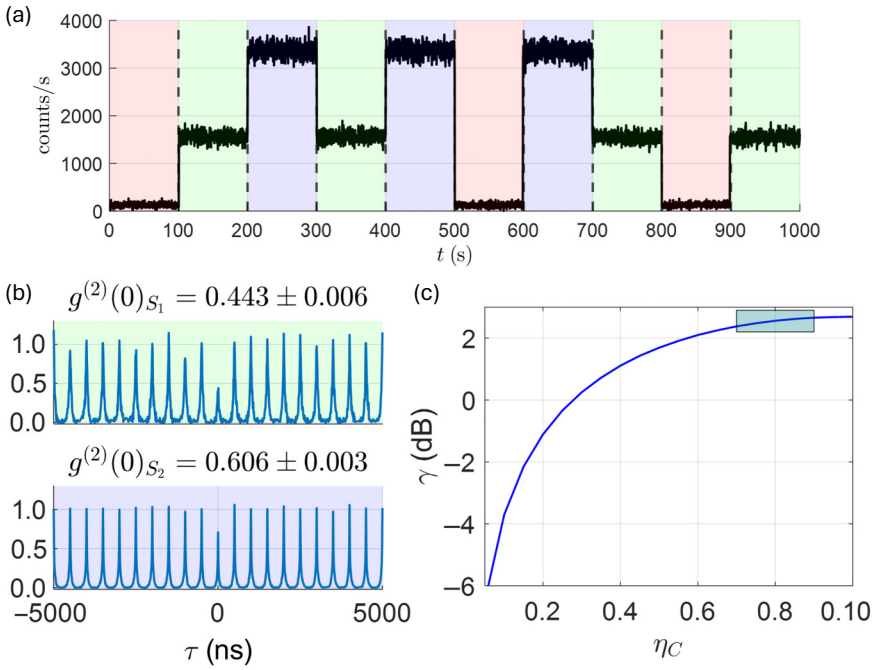


FIG. 4. Experimental results for emulating the DTB protocol. (a) Controlling the photon emission counts by the excitation-laser intensity (405 nm, 2-MHz repetition rate, 2-ns pulse duration). The red regions mark S_0, the green regions mark S_1, and the purple regions mark S_2 appearing in Fig. 1(c). The time steps (100 s) taken for the power modulation of the excitation laser have been chosen to emphasize the feasible control of the photon emission. (b) $g^{(2)}(0)$ for the two different intensities, S_1 and S_2. (c) Calculation of γ values as a function of η_C. The blue box represents the η_C range demonstrated in our devices [41,43], all with $\gamma > 2$ dB.

As indicated by the first term of Eq. (8), the probability of sending one photon is linearly dependent on η_D, suggesting that the minimum value of P_2 required for $\gamma > 0$ dB is inversely proportional to Alice's detection efficiency. Calculations yield this relation, giving the condition $P_2 \geq 0.37/\eta_D$ for a balanced 50:50 BS. The values of γ and the separation line between the WCS and HP in Fig. 3(b) are evaluated for the realistic case $\eta_D = 0.9$, yielding an expected enhancement over WCS when $P_2 > 0.41$. The black dot in Fig. 3(b) represents an actual SPS device consisting of a gCQD coupled to a Bragg antenna with a plasmonic nanocone (SPS2), demonstrated in Ref. [41], again showing that the existing imperfect SPS+HP can compete with WCS+Decoy.

Finally, we present experimental results of a bare gCQD sample (shown here in purple and black circles with corresponding error bars), where the photon probabilities have been experimentally obtained as explained in Appendix C and the SKR has been extracted separately for each protocol with Eqs. (7) and (10), respectively. The gCQD, excited at several intensities, exhibits different photon emission statistics for each intensity, thus allowing us to demonstrate both the DTB and HP protocols. As seen, even bare gCQDs emitting at room temperature, without any special antennas, can reach a regime that is superior to WCS+Decoy.

IV. EXPERIMENTAL RESULTS

A. Proof-of-concept measurements of protocols

After theoretically showing that existing SPSs, combined with the two new protocols, can outperform WCS in terms of the MCL, here we demonstrate experimental proof-of-concept emulations of both protocols using our bare single gCQD presented in Fig. 1(c) as our imperfect SPS emulator.

To experimentally demonstrate the feasibility of the DTB scheme, we use three different pulsed excitation intensities generated by a 405-nm diode laser, marked as $S_0 = 0$, S_1, and S_2 in Fig. 1(c) (for the full experimental information, see Appendix F). In Fig. 4(a), we demonstrate photon emission control showing stable photon counts under each excitation intensity. This allows easy control of the photon statistics, as shown in Fig. 4(b), which presents the $g^{(2)}(0)$ values for S_1 and S_2, consistent with the modification of the photon statistics shown in Fig. 1, where $P_1^{(S_1)} = 0.05$, $P_1^{(S_2)} = 0.4$ and $P_2^{(S_1)} = 0.0005$, $P_2^{(S_2)} = 0.15$.

As shown previously, the gCQD SPS with a near-unity collection efficiency can outperform WCS with decoy states, if implemented with the DTB protocol. In Fig. 4(c), we numerically calculate the expected γ of a gCQD SPS device in terms of η_C (see Appendix I). Remarkably, with the current measured parameters, $\gamma > 0$ dB already for $\eta_C > 0.3$, which is easily attainable even for bare gCQDs, as we show later. Our previously demonstrated gCQD-based SPS devices [43] have $\eta_C > 0.7$ (marked by a blue rectangle), leading to an expected $\gamma > 2$ dB, already constituting a significant improvement over WCS+Decoy.

Moving to emulation of the HP protocol, we show experimental results of the purification of the gCQD emission in Fig. 5 using a 50:50 BS. The second-order correlation measurements of the gCQD without [Fig. 5(a)] and with [Fig. 5(b)] the HP postprocessing protocol are

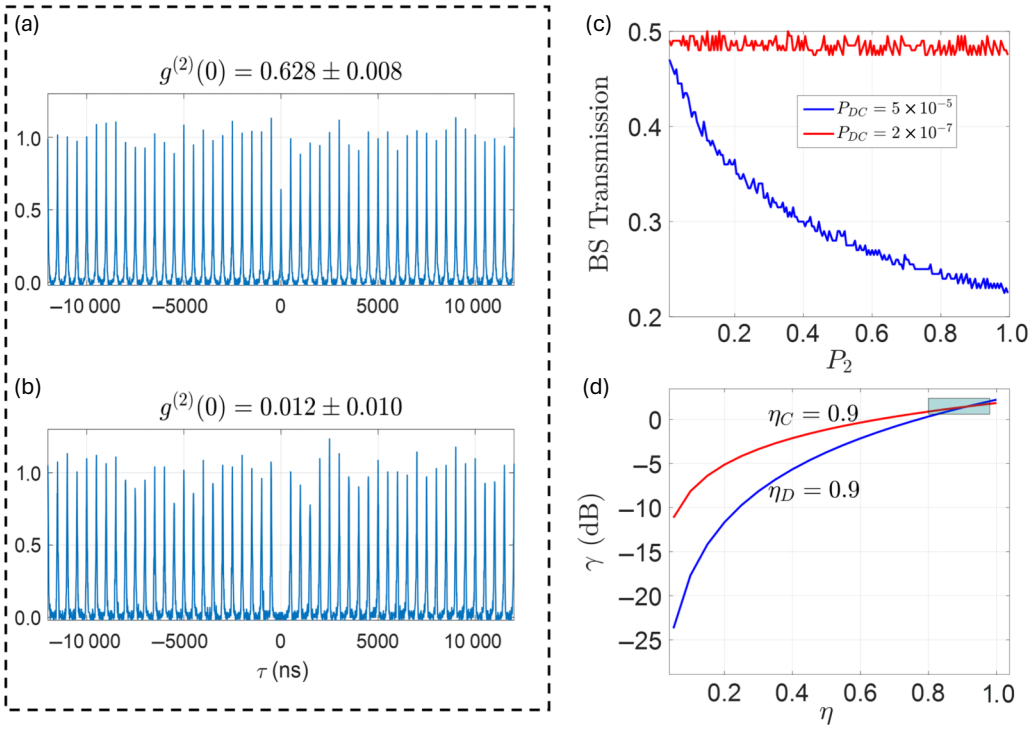


FIG. 5. Experimental results for emulating the HP protocol. Second-order correlation measurements of the bare gCQD SPS (a) without and (b) with the HP postprocessing scheme, resulting in near-zero $g^{(2)}(0)$. The error is mainly due to the SPD dark noise. (c) A calculation showing the optimal transmission T, of Alice's BS, required for maximizing γ as a function of P_2 of the SPS, for two values of P_{DC}, corresponding to 100 dark counts/s of the SPD, and SPS excitation repetition rates of 2 (blue) and 500 (red) MHz. (d) A calculation of γ as a function of η_C with a fixed η_D (blue line) and as a function of η_D with a fixed η_C (red line). The blue box represents the range demonstrated in our devices [41,43].

presented. As can be seen, a near-zero $g^{(2)}(0)$, limited only by detector noise, is achieved, competing with state-of-the-art demonstrations [28,39]. We note that with HP, the photon rate decreases to approximately $0.5P_2\eta_D$ but the collection efficiency η_C is not affected.

Using the results in Figs. 5(a) and 5(b), one can extract the *third-order* correlation measurements ($g^{(3)}(0,0)$) [54] to determine P_3, the probability of a three-photon emission (see Appendix D). Using this method, we find that $P_3 \sim 10^{-5}$; therefore we conclude that $P_{N>2}$ is negligible compared to P_1 and P_2, justifying our initial assumptions.

Interestingly, the HP efficiency can be optimized by adjusting T and R of Alice's BS, depending on the P_2 of the source. In Fig. 5(c), we show a calculation of the optimal BS transmission T to reach the highest MCL, as a function of P_2, for two dark-count probabilities P_{DC}. For low P_{DC}, the optimal transmittance is roughly 0.5. However, for higher values of P_{DC}, the optimal T is smaller than 0.5 and decreases with increasing two-photon probability, in order to minimize the probability of a dark count at Alice's detector simultaneously with two-photon transmission to Bob. Lastly, in Fig. 5(d), we plot the calculated γ for a gCQD-based SPS with the above parameters, as a function of η_D, for a fixed $\eta_C = 0.9$ and as a function of η_C for a fixed $\eta_D = 0.9$. Again, the blue box, representing demonstrated values of SPS devices based on gCQD coupled to nanoantennas, shows an improvement over WCS+Decoy.

B. Experimental demonstration of the protocols in BB84 QKD using a gCQD

Now, we consider a BB84 demonstration using a bare gCQD as the imperfect SPS and utilizing either DTB or HP protocols.

In Fig. 6(a), we show the QKD system that has been used to demonstrate a polarization-based BB84 protocol. The photons emitted from the gCQD sample are collected to Alice's encryption unit, which randomly defines both the qubit value and basis [1,55]. The photons are then propagated through the quantum channel in free space, where we have introduced neutral-density (ND) filters in the optical path to simulate channel loss, before arriving at Bob's decryption unit. Here, we define the two mutually unbiased bases as "+" ($|H\rangle$, $|V\rangle$) and "×" ($|D\rangle$,$|A\rangle$) [55].

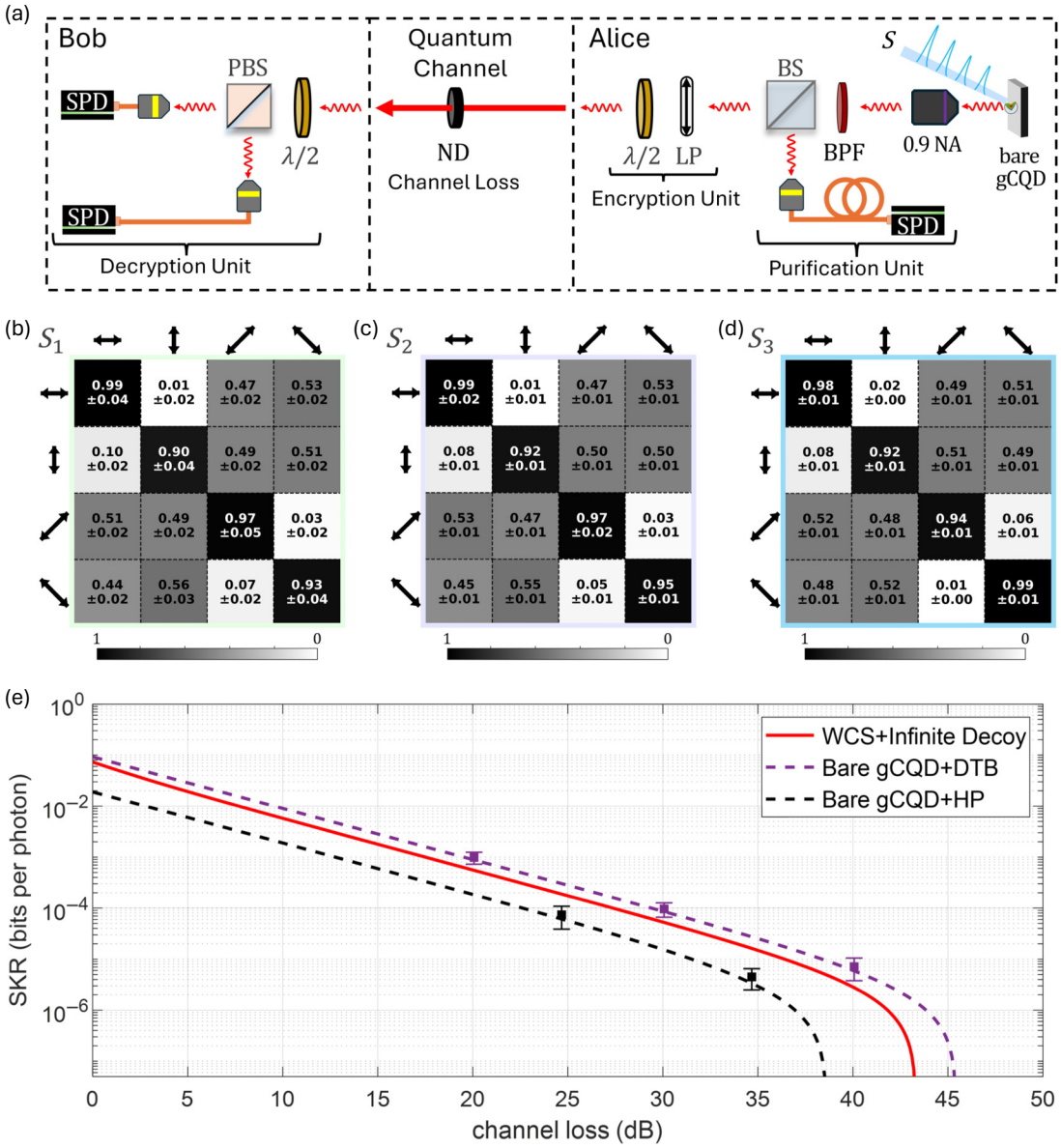


FIG. 6. Polarization-based BB84 QKD measurements of a bare gCQD sample generated with the two protocols. (a) A sketch of the experimental QKD system: Alice's setup includes a purification unit with a BS and an SPD, and an encryption unit with a linear polarizer (LP) and a half-wave plate ($\lambda/2$). The free-space quantum channel includes neutral-density (ND) filters to vary the channel loss. Bob's setup includes the BB84 decryption unit with a $\lambda/2$, a polarizing beam splitter (PBS), and two SPDs. (b)–(d) Tomography-mapping results for different excitation-laser intensities: (b) S_1, (c) S_2, and (d) S_3, respectively, corresponding to the decoy (green frame) and signal (purple frame) states in the DTB protocol, and the $S > 1$ intensity (blue frame) state in the HP protocol. (e) The SKR results extracted from the measurements from a bare gCQD sample compared to WCS with infinite decoy. The different measured points along represent the extracted SKR results for several ND filter settings (see full results in Appendix J) using the DTB protocol (purple) and the HP protocol (black). The dashed lines represent the corresponding calculated SKR. The DTB results demonstrate a clear improvement in the maximal channel loss, γ, over the WCS (red line), while the HP protocol results (dashed black) fall below this due to the small P_2 values of bare gCQDs without a nanoantenna.

By manipulating the different basis settings of both Alice and Bob, the full tomography mapping can be measured. In Figs. 6(b)–6(d), we show the tomography results for three different excitation intensities, S_1, S_2, and S_3, without an ND filter in the quantum channel (for the full set of results, see Appendix J).

From these results, the gain Q_i and error rates E_i for intensity i are extracted using the following relations:

$$Q_i = \frac{\text{total number of detected qubits}}{\text{total number of sent qubits}}, \tag{11}$$

$$E_i = \frac{\text{number of error qubits}}{\text{total number of detected qubits}}. \quad (12)$$

The total number of detected qubits is the measured counts at both of Bob's detectors at a given basis, and the total number of error qubits is the number of counts measured on the wrong detector (assuming that Alice and Bob randomly chose the same basis, according to the BB84 protocol). The total number of qubits sent by Alice is estimated by the following:

$$\text{total number of sent qubits} = N\eta_A\eta_{C_{NA}}, \quad (13)$$

where N is the repetition rate of the excitation laser (2 MHz; see Appendix F), $\eta_A \simeq 19.5\%$ is the transmission of Alice's setup measured in our experiments, and $\eta_{C_{\mathrm{NA}}} \simeq 14.18\%$ is the transmission of the photon-collection optics from the gCQD to Alice extracted previously in Ref. [40], with "NA" denoting "numerical aperture."

The Q_i and E_i, along with the measured photon statistics $\{P_0, P_1, P_2\}$ for each intensity i, have been inserted into Eq. (6) to extract Y_n and e_n, which have then been used for calculating the SKR in Eqs. (7) and (10) for the DTB and HP protocols, respectively. The DTB model requires two decoys (S_0 and S_1), where S_0 is the vacuum state with known parameters (see Appendix G). Here, S_2 is used as the signal state for the DTB protocol and S_3 is used for the HP protocol.

In Fig. 6(c), we plot the SKR of the gCQD measured with the DTB protocol and the HP protocol, for several channel losses set with various ND filters, compared to WCS with infinite decoy states. A clear improvement of approximately 2 dB is demonstrated with the DTB protocol, which agrees well with the theoretical curve. As expected, the results with the HP protocol do not show an improvement compared to WCS with decoy, due to the low P_2 in bare gCQD as compared to those obtained in a full SPS2 devices [41]; nonetheless, they show the feasibility of the two enhanced-QKD protocols with already available SPSs and their advantage over the best existing WCS solutions.

V. CONCLUSIONS

As an alternative to the very challenging push for nearly ideal SPSs that is required to outperform the existing WCS protocols for QKD, we have proposed and experimentally analyzed two simple-to-implement protocols that can allow for even far from ideal SPSs, which are currently technologically ready, to beat the state-of-the-art performance of weak coherent states with decoy protocols, achieving over > 3 dB enhancement in terms of the SKR.

The protocols are based on the simple ability to control the statistical distribution of the truncated photon-number basis $\{|0\rangle, |1\rangle, |2\rangle\}$ of a QD BX-X cascaded emission, by varying the excitation power. We have shown that depending on the possible attainable values of P_1 and P_2, either a decoy-state protocol (DTB) or a heralded purification protocol (HP) can be employed to a nonideal SPS.

This is a particularly attractive route for improving the performance of current QKD systems, as we have shown that even room-temperature, on-chip, compact, and easily integrated SPS devices, such as those based on gCQD coupled to nanoantennas, are already well within the parameter range for superior performance over WCS with decoy states by employing either a DTB protocol or HP. Both protocols have very simple requirements and their application is very general; thus we believe they can be employed efficiently on a vast range of sub-Poisson quantum emitters, opening a practical and realistic way to implement novel photon sources with superior QKD performance, without the stringent requirements that have hindered their practical integration into real-world QKD systems.

Our protocols, which improve QKD performance, could also enhance other quantum cryptography technologies. By improving eavesdropping detection, they could strengthen quantum secure direct communication [56], quantum secret sharing [57], and quantum secure computation [58]. These protocols offer versatile improvements across various quantum cryptographic applications.

ACKNOWLEDGMENTS

The gCQD synthesis was conducted at the Center for Integrated Nanotechnologies (CINT), a Nanoscale Science Research Center and User Facility operated for the U.S. Department of Energy (DOE), Office of Science (SC), Office of Basic Energy Sciences (BES). R.R., Y.B, Y.O., T.L., and K.S. acknowledge the financial support from the Quantum Communication consortium of the Israeli Innovation Authority. J.A.H. was supported in part by the U.S. Department of Energy (USDOE), Office of Science (OS) Office of Advanced Scientific Computing Research, through the Quantum Internet to Accelerate Scientific Discovery Program, and E.G.B. was supported by the U.S. Department of Energy Office of Science (USDOE-OS) Basic Energy Sciences, through the Center for Integrated Nanotechnologies.

R.R. conceptualized the protocols and supervised the project. Y.B. and T.L. conducted the experiments. Y.B. fabricated the samples. Y.O. provided the theoretical and numerical analysis. J.A.H. developed the gCQDs and supervised the program at CINT. E.G.B. performed gCQD synthesis and characterization. K.S. assisted the theoretical analysis. All authors contributed to the preparation of the manuscript.

DATA AVAILABILITY

The data are available from the authors upon reasonable request.

APPENDIX A: MATERIALS AND METHODS

Giant colloidal nanocrystal quantum dots (gCQD) of CdSe-CdS core-shell type have been used as the quantum emitters in this work. The gCQD core has a diameter of approximately 3 nm, while the shell has a diameter of approximately 15 nm. The emission wavelength of the gCQD is centered around 650 nm at room temperature. The properties of these quantum dots have been investigated in many works [59–62].

In Fig. 7, we demonstrate several properties of single gCQDs. The extracted lifetime of the gCQD from a biexponential fit due to the emission both from the BX and X states is presented in Fig. 7(a), demonstrating nanosecond radiative transitions on bare gCQDs. As investigated in Refs. [40,41], the plasmonic coupling of the gCQD to the metallic resonator shortens the photon lifetime to approximately 10–100 ps. The stability of the bare gCQD is shown in Fig. 7(b), with a stable emission of a single gCQD on glass at room temperature, exhibiting a nonblinking emission for long times [60]. In Fig. 7(c), we plot the spectrum of the gCQD, with a broad emission [a full width at half maximum (FWHM) of approximately 25 nm] at room temperature. This demonstrates the spectral overlapping between the BX and X states at high temperatures.

The gCQDs have been initially diluted in a hexane and polymethyl methacrylate 495 A5 (PMMA) solution with sparse ratios among each of the materials (1:200:5000), to ensure the distribution of single gCQDs on the sample. To achieve this, we have used an iterative method in which different ratios have been tested, stirred with a shaker, and then spin coated on a glass slide using a two-step process (500 rpm for 5 s, 4000 rpm for 40 s),

The plasmonic device has been fabricated using methods similar to those presented in Refs. [40,41,43], employing the template-stripping method [63] to create an Au metallic device consisting of a Bragg concentric antenna with and without a nanocone resonator. The gCQDs have been coupled to the nanoantennas using fabrication methods similar to those described in Refs. [40,43,64,65].

APPENDIX B: PROBABILITY DISTRIBUTION AND QUANTUM YIELDS

In Sec. II, we have presented a model for the probabilities of exciting one or two excitons depending on the excitation-laser power. One can use this model to combine the emission distribution and the quantum yields (QYs) of the source.

Given that a single exciton was excited, the probability of emitting two photons is zero, while the probability of emitting one photon is given by the exciton quantum yield, QY_X. Given that two excitons are excited (as in the biexciton state), the probability of emitting two photons is the probability that both the exciton and the biexciton have recombined radiatively, suggesting that the probability is $QY_X QY_{XX}$. Therefore, the probability of a single photon emission is the probability that either the exciton or the biexciton has recombined radiatively, giving $QY_X + QY_{XX} - 2QY_X QY_{XX}$.

The complete photon emission distribution is given by

$$P_2 = P_{XX}(I)\phi_{XX}\phi_X, \tag{B1}$$

$$P_1 = P_{XX}(I)(\phi_X + \phi_{XX} - 2\phi_X\phi_{XX}) + P_X(I)\phi_X, \tag{B2}$$

$$P_0 = 1 - P_1 - P_2. \tag{B3}$$

A quantitative metric for the goodness of the fit, the normalized root-mean-square error (NRMSE) [66], has been generated by comparing the theoretical model for the probabilities with the saturable behavior of the source. In our case, the fit has given a result of NRMSE ≤ 0.012, showing a good correlation between the theoretical model and experimental results.

APPENDIX C: PROBABILITY EXTRACTION FROM A TRUNCATED FOCK BASIS

The second-order correlation function is given by

$$g^{(2)}(\tau) = \frac{\langle a^\dagger(t)a^\dagger(t+\tau)a(t+\tau)a(t)\rangle}{\langle a^\dagger(t)a(t)\rangle\langle a^\dagger(t+\tau)a(t+\tau)\rangle},$$

where a and $a^\dagger$ are the annihilation and creation operators. For a stationary source ($\langle n(t)\rangle = \langle n(t+\tau)\rangle$) [67], the zero-delay correlation function can be written as

$$\begin{aligned} g^{(2)}(0) &= \frac{\langle n(n-1)\rangle}{\langle n\rangle^2} = \frac{\langle n^2 - n\rangle}{\langle n\rangle^2} = \frac{\langle n^2\rangle - \langle n\rangle}{\langle n\rangle^2} \\ &= \frac{\langle n^2\rangle + \langle n\rangle^2 - \langle n\rangle^2 - \langle n\rangle}{\langle n\rangle^2} = 1 + \frac{Var(n) - \langle n\rangle}{\langle n\rangle^2}. \end{aligned} \tag{C1}$$

In this way, we describe the second-order correlation function at zero delay as a relation between the mean and variance of the distribution, where $\langle n\rangle = P_1 + 2P_2$, $\langle n^2\rangle = P_1 + 4P_2$, and $Var(n) = \langle n^2\rangle - \langle n\rangle^2$.

With the transmission of the system (η) and the repetition rate (N) of the laser, the photon detection rate, C, is given by

$$\frac{C}{N} = \sum_{n=0}^{\infty} \eta_n P_n \approx \sum_{n=0}^{\infty} \eta n P_n = \eta \langle n\rangle, \tag{C2}$$

where $\eta_n = 1 - (1-\eta)^n$ is the detection-event probability of the n-photon state [11], which can be approximated

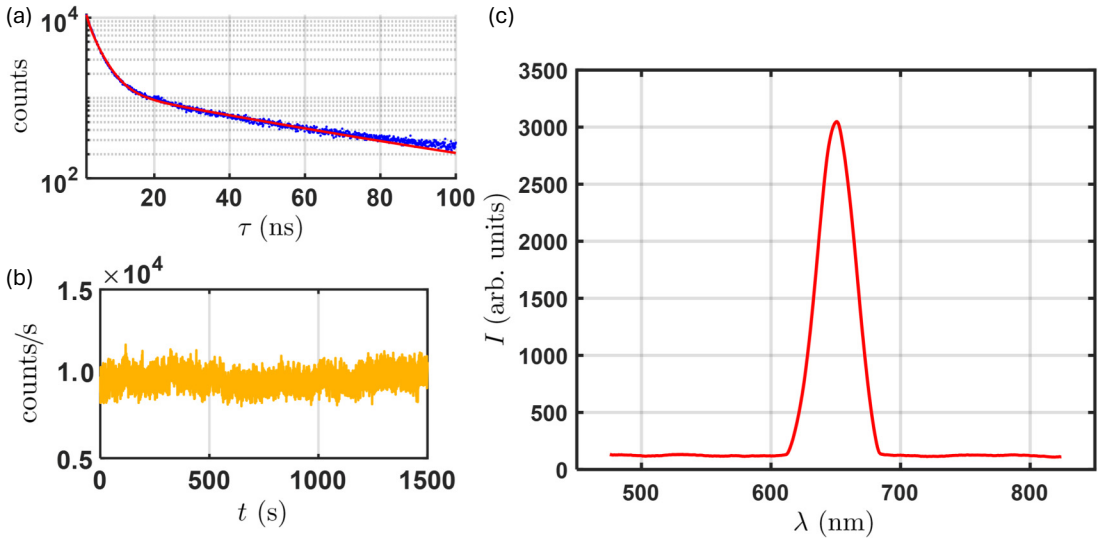


FIG. 7. The bare single-gCQD properties. (a) The lifetime measurement of a single gCQD on glass, with extracted values of $\tau_X = 49.3 \pm 3.7$ ns and $\tau_{XX} = 3.58 \pm 0.16$ ns, for the X and BX emission, respectively. (b) Stability measurement of the photon emission from the gCQD, demonstrating highly stable and nonblinking emission. (c) The spectrum of the gCQD corresponding to the emission both from the X and BX states, centered around approximately 650 nm.

in the limit of $\eta \ll 1$ (approximately 10^{-2} in our case) to $\eta_n \approx n\eta$.

This allows us to experimentally determine P_0 using

$$P_0 = 1 - \frac{C}{\eta N}. \tag{C3}$$

Using Eqs. (C1) and (C3), we can define two equations that relate P_0 and $g^{(2)}(0)$ to P_1 and P_2:

$$P_0 + P_1 + P_2 = 1, \tag{C4}$$

$$g^{(2)}(0) = \frac{2P_2}{(P_1 + 2P_2)^2}. \tag{C5}$$

The experimentally measured P_0 and $g^{(2)}(0)$ are used to solve these equations for P_1 and P_2 and to obtain the first two moments of the distribution. In our case, this contains all the required statistical information, thus allowing us to extract the whole probability distribution for the truncated Fock basis from just two measured quantities.

APPENDIX D: $P_{N\geq 3}$ PROBABILITY EXTRACTION FROM $g^{(3)}(\tau_1, \tau_2)$ MEASUREMENTS

By introducing another detector into our system, as explained for the HP protocol (Sec. III B), we can use a similar set of equations with minor adjustments (as in Appendix C) to estimate P_3, the probability of an emission of three photons from the source. This allows us to estimate the probability of higher photon probabilities, to justify our assumptions regarding the photon statistics.

In this case, the third-order correlation function at zero delay can also be described by the relation between the distribution mean and variance. Here, $\langle n \rangle = P_1 + 2P_2 + 3P_3$, $\langle n^2 \rangle = P_1 + 4P_2 + 9P_3$, and $\langle n^3 \rangle = P_1 + 8P_2 + 27P_3$. In addition, for a stationary source, $g^{(3)}(0,0)$ is given by [54]

$$g^{(3)}(0,0) = \frac{\langle n(n-1)(n-2) \rangle}{\langle n \rangle^3} = \frac{\langle n^3 \rangle - 3\langle n^2 \rangle + 2\langle n \rangle}{\langle n^3 \rangle}. \tag{D1}$$

Now, by using Eqs. (C1), (B3), (D1) we have another set of equations that relate P_0, $g^{(2)}(0)$ and $g^{(3)}(0,0)$ to P_1, P_2 and P_3:

$$P_0 + P_1 + P_2 + P_3 = 1, \tag{D2}$$

$$g^{(2)}(0) = \frac{2P_2 + 6P_3}{(P_1 + 2P_2 + 3P_3)^2}, \tag{D3}$$

$$g^{(3)}(0,0) = \frac{6P_3}{(P_1 + 2P_2 + 3P_3)^3}, \tag{D4}$$

where we have assumed that $P_{N>3} = 0$.

Therefore, one can extract P_1, P_2, and P_3 from the measured P_0, $g^{(2)}(0)$, and $g^{(3)}(0,0)$, which gives the first three moments of the distribution. In our case, the third-order correlation at zero delay has been measured in the $S > 1$

regime, with the highest probability for higher multiexciton emission. The measured result of correlations between the three detectors was found to be

$$\boxed{g^{(3)}(0,0) = 0.00065}, \tag{D5}$$

with a measured $g^{(2)}(0) = 0.747 \pm 0.003$ and $P_0 = 0.57 \pm 0.030$. Plugging all these into Eq. (D2) gives

$$P_1 = 0.3233 \pm 0.0094, \tag{D6}$$

$$P_2 = 0.1112 \pm 0.0207, \tag{D7}$$

$$P_3 = 0.0000177 \pm 0.00000052. \tag{D8}$$

Therefore, we conclude that $P_3 \ll P_1, P_2$, leading to the conclusion that for $N \geq 3$ photons, the probability is negligible. This finalizes our assumptions regarding the characterization of the photon statistics.

APPENDIX E: DTB MODEL

In this appendix, we present the model used for the estimation of the SKR for the decoy-state protocol on a truncated basis (DTB) that has been presented in the main text. With the probability distributions for the signal and the decoy states, $\{P_n^s\}_{n=0}^2$, $\{P_n^{d,i}\}_{n=0}^2$, and the n-photon yield, Y_n, the gains are given by

$$Q_s = Y_0 P_0^s + Y_1 P_1^s + Y_2 P_2^s, \tag{E1}$$

$$Q_{d,i} = Y_0 P_0^{d,i} + Y_1 P_1^{d,i} + Y_2 P_2^{d,i}, \tag{E2}$$

where i represents the two corresponding decoy states.

Similarly, the error rates are

$$E_s Q_s = Y_0 P_0^s e_0 + Y_1 P_1^s e_1 + Y_2 P_2^s e_2, \tag{E3}$$

$$E_{d,i} Q_{d,i} = Y_0 P_0^{d,i} e_0 + Y_1 P_1^{d,i} e_1 + Y_2 P_2^{d,i} e_2, \tag{E4}$$

where e_n is the n-photon error rate. According to the channel model, the n-photon yield is given by the n-photon transmission of the channel, η_n, and the dark-count probability, P_{DC}:

$$Y_n = \eta_n + P_{\mathrm{DC}} - \eta_n P_{\mathrm{DC}}, \tag{E5}$$

where η_n is given by $\eta_n = 1 - (1-\eta)^n$ such that η is the overall channel transmittance. Finally, the n-photon error-rate expression for our model is

$$e_n = (e_d \eta_n + \frac{1}{2} P_{\mathrm{DC}})/Y_n, \tag{E6}$$

where e_d is the probability of reaching the wrong detector. Experimentally, Y_1 is calculated by measuring the photon probabilities $\{P_0, P_1, P_2\}$ along with the gain Q and error E to solve Eqs. (E1)–(E4), as explained in Sec. IV B. In the numerical performance, presented in Fig. 3(a), the gain is estimated using Eq. (E5), by measuring the dark-count probability P_{DC} in our system and setting the overall transmission η. This gives all the required parameters for R_1 [Eq. (7)], which are valued and can be inserted to yield the bound of the SKR. To obtain the SKR per channel loss, we iterate through different transmissions.

APPENDIX F: EXPERIMENTAL DETAILS

The optical setup for correlation measurements and the BB84-QKD protocol demonstration is illustrated in Fig. 8. A diode laser (Toptica IBeam Smart) operating at a wavelength of 405 nm generated pulses at a repetition rate of 2 MHz. The excitation-laser properties were chosen to allow for a full relaxation of the biexciton and exciton states through the radiative transition channels [68,69], thus eliminating unwanted nonradiative effects.

In the DTB scheme, the excitation power was tuned between three different intensities, one of which was zero, to obtain information on the photon statistics for each pump. The two other intensities corresponded to an average power of $S_1 \sim 0.01$ mW and $S_2 \sim 0.05$ mW.

In the HP scheme, the excitation power was set to a high intensity as described in the main text, corresponding to an average power of $S_3 \sim 0.15$ mW.

The excitation laser was focused on the gCQD sample with a 0.9-NA objective (Olympus MPLFLN100xBD) and was scanned using Galil and Zaber electrical stages. The emission from the gCQD devices was collected using the same objective and spectrally filtered from the excitation laser using a 567-nm long-pass dichroic mirror.

Photoluminescence (PL) measurements were performed using a Hamamatsu CMOS camera to identify single gCQDs and the SPS devices. A white-light source was introduced into the optical setup alongside the excitation-laser path, to scan the device area and locate PL from active emitters.

To ensure that the emission originated from gCQD-based devices, the emission was directed to a spectrometer (Princeton SpectraPro 2500) connected to a CCD camera (PIXIS 256BR), verifying that the emission is centered around the gCQD emission energy [40,41].

For time-resolved single-photon correlation measurements, the emission was directed to a Hanbury Brown–Twiss (HBT) [70] module, consisting of a BS and a set of SPDs (Excelitas SPCM-AQRH-14-FC), referred to as Bob's detectors, which were coupled to the system using multimode fibers. The signal from each detector was routed to different channels in the time-tagging instrument (Swabian TimeTagger 20). The time tagger provided output of all arrival times and channel labels of photons within the set of exposure times, commonly referred to as global times.

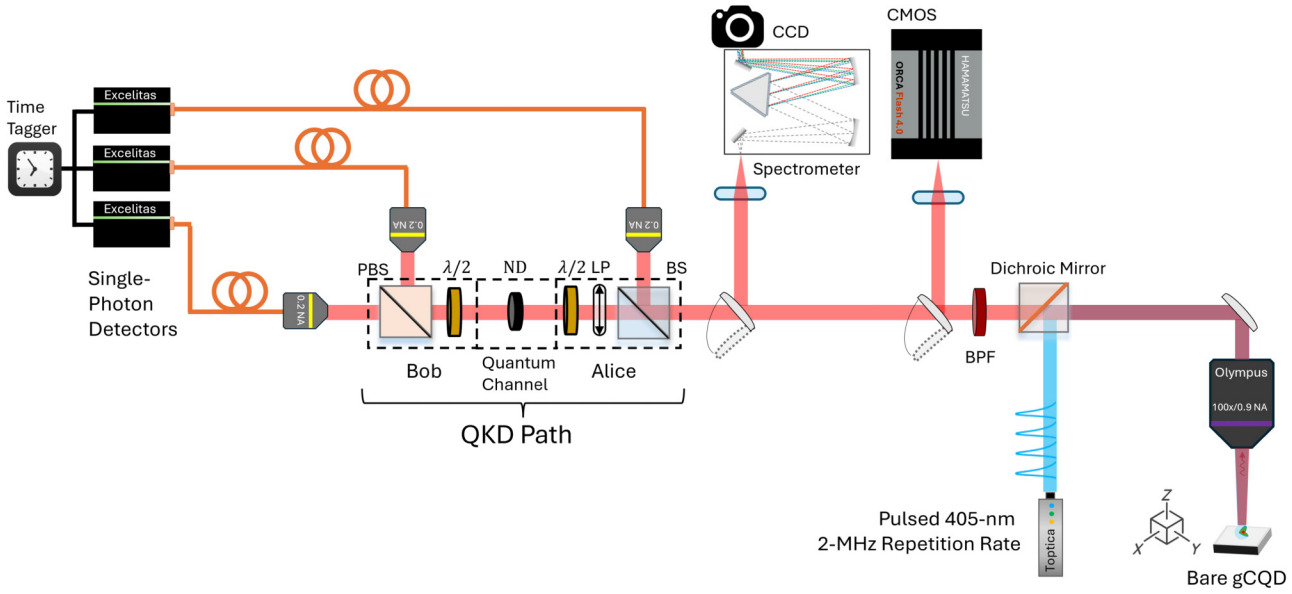


FIG. 8. The experimental setup. Excitation with a 405-nm diode pulsed laser operating at 2 MHz has been focused on the gCQD-based sample, emitting photons to the channel. Correlation measurements and stability and saturation curves have been measured using the SPDs after the HBT setup. The CMOS camera and spectrometer have been used to characterize the gCQD emission. The DTB protocol [shown in Fig. 2(a)] has been demonstrated using different intensity powers for the excitation laser. The HP scheme [shown in Fig. 2(b)] has been demonstrated using a third detector introduced in the channel along with a 50:50 BS. A standard BB84 encryption (Alice) and decryption (Bob) unit has also been introduced into the system.

Another channel in the time tagger recorded the excitation-pulse times, commonly referred to as local times, which served as a trigger channel for the detectors. The histogram of local times is required for lifetime extraction [41].

Specifically in the HP scheme, a second BS was introduced into the system and coupled to a third SPD (referred to as Alice's detector). During a postprocessing step, data were retained only when both Alice's detector and either of Bob's detectors registered a photon appearance in the same pulse. This was determined using the local times issued for each channel in the time-tagger recorded data. The dark-count rate of the SPDs, as provided by the manufacturer and verified experimentally, was approximately 100 counts/s.

APPENDIX G: PARAMETER TABLE FOR THE PERFORMANCE ANALYSIS OF THE DTB AND HP PROTOCOLS

In the experimental and numerical analysis, the realistic dark-count probability is given as $P_{DC} = 2 \times 10^{-7}$ as explained in the main text. In addition, $\eta_C = 1$ and $\eta_D = 0.9$ define the optimal but realistic collection and detector efficiencies, as explained previously. Lastly, $Y_0 = 1.7 \times 10^{-6}$ and $e_0 = 0.5$, denoting the vacuum yield and error rate, respectively, are used for the vacuum decoy signal in the DTB protocol, S_0. In addition, the probability of reaching the wrong detector has been set to $e_d = 3.3\%$ and Bob's detection efficiency has been set to $\eta_{\text{Bob}} = 4.5\%$, as explained in the main text. The P_1 and P_2 parameters for different sources are presented in Table I.

The error bars for the photon emission probabilities P_1 and P_2 have been calculated by error propagation, accounting for the $g^{(2)}(0)$ and P_0 deviations. In addition, the error bars for the SKR have been extracted by error propagation, considering the gain and error-rate uncertainties as extracted from the tomography maps. These uncertainties have been measured by the deviation from a mean-count value over long exposure times, for each row in the tomography map.

APPENDIX H: ALGORITHMIC REPRESENTATION OF THE QKD PROTOCOLS

The algorithm representation of the DTB protocol and the HP protocol is given in Algorithms 1 and 2, respectively.

APPENDIX I: EFFICIENCIES ESTIMATION

To examine the dependence on the collection and detection efficiencies (η_C and η_D, respectively) and on the BS as shown in Sec. IV, we have included some modifications to the emission distributions.

ALGORITHM 1. Decoy State on a Truncated-Fock-Basis Protocol (DTB).

Input: Realistic quantum emitter with photon statistics $\{P_0, P_1, P_2\}$, controlled laser excitation powers of S_0, S_1, S_2.
Output: Ensure a shared secure key between Alice and Bob using decoy states.
Initialization: Set laser excitation powers to S_0, S_1, S_2; according to the photon statistics at each power.
for each clock cycle defined by the excitation laser's pulse repetition rate **do.**
  Alice randomly selects an excitation power:
  S_2 as the signal state with a single photon probability of $P_1^{(s)}$.
  S_1 as the first decoy state.
  S_0 as the second (vacuum) decoy state.
  Alice excites the device with the selected excitation power. The photons emitted from the device are propagated in free-space to Alice's encryption unit.
  Alice encodes the photon using the BB84 encryption unit and sends the photon to Bob through the free-space quantum channel.
end for
Bob measures each received photon per clock cycle in a random BB84 basis and records the outcomes.
In the sifting step, Alice and Bob reveal their bases over a classical channel and retain only matching basis detection events.
Alice informs Bob which detections are signal or decoy states.
Bob estimates the gains and errors of the signal and decoy states, and extracts the single photon yield Y_1 and error rate e_1 to find the secure key rate.
Error correction and privacy amplification are applied to obtain the final secret key.

Given the probability distribution, $\{P_n\}$, of the source and some collection efficiency, η_C, one can perform a modification to the emission distribution of the form

$$P_2' = P_2\eta_C^2, \tag{I1}$$

$$P_1' = P_1\eta_C + P_2 2\eta_C(1-\eta_C), \tag{I2}$$

$$P_0' = 1 - P_1' - P_2'. \tag{I3}$$

Here, we do not add the modification to the channel loss, as this loss is fully defined inside Alice's setup and is inaccessible to Bob and Eve.

The consideration of the parameters of the BS and of η_D in the HP scheme is shown in Eq. (8).

With the new emission distributions and the model for the channel described in the previous appendix, the calculated parameters can be inserted to the SKR equations for either the regular BB84 protocol (for HP) or the decoy-state protocol (for DTB), given in Ref. [11], to obtain the behavior for different channel losses. This yields the corresponding MCL as shown in Sec. IV.

ALGORITHM 2. Heralded-Purification (HP) Protocol.

Input: Realistic quantum emitter with photon statistics of $\{P_0, P_1, P_2\}$.
Output: Ensure a shared secure key between Alice and Bob using highly pure single photons.
Initialization: Set laser excitation power to $S_3 > 1$ near saturation and configure Alice's heralding single photon detector (SPD) with its detection efficiency of η_D.
for each clock cycle defined by the excitation laser's pulse repetition rate **do.**
  Alice excites the device with S_3.
  The photons emitted from the device are propagated in free-space to Alice's beam splitter (BS): one output to the SPD and the other to Alice's encryption unit.
  if the SPD clicks, the heralding is successful **then.**
    Alice encodes the photon using the BB84 encryption unit and sends the photon to Bob through the free-space quantum channel.
  else
    Alice discards the pulse, even if Bob received photons.
  end if
end for
Bob measures each received photon per clock cycle in a random BB84 basis and records the outcomes.
In the sifting step, Alice informs Bob which pulses were heralded. Alice and Bob retains only matching heralded detection events.
Bob estimates the gain and error based on the heralded photons.
Error correction and privacy amplification are applied to obtain the final secret key.

APPENDIX J: TOMOGRAPHY MAPPINGS FOR QKD EXPERIMENTAL RESULTS

The BB84 experimental demonstration has been done by measuring the full Hilbert space of polarization-based encryption, given a qubit value in a specific basis sent by Alice and a given basis measured by Bob. In Fig. 9, the additional results of the tomography maps with an ND filter placed in the quantum channel are presented [for the results without an ND filter, see Figs. 6(b)–6(d)]. The ND filters are used to demonstrate the channel losses.

APPENDIX K: POSSIBLE VALUES OF $g^{(2)}(0)$ WITH A $\{P_0, P_1, P_2\}$ TRUNCATED FOCK BASIS

We provide a derivation that shows that for a realistic imperfect source, which has a total $QY < 1$ and $P_{N\geq 3} = 0$, the vacuum state affects the second-order correlation function such that a valid solution may have $g^{(2)}(0) \geq 0.5$:

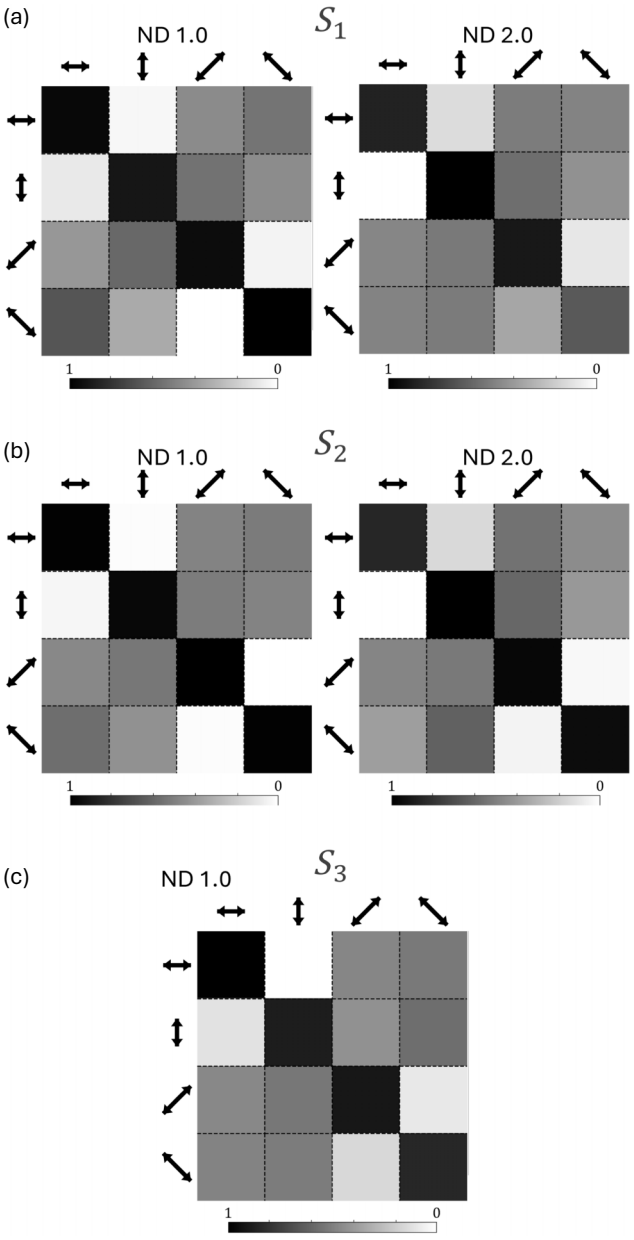


FIG. 9. Tomography results for different excitation-laser intensities. (a),(b) The intensity corresponding to (a) the decoy state S_1 and (b) the signal state S_2 in the DTB protocol, measured with a 1.0-dB ND filter (left) and a 2.0-dB ND filter (right). (c) The intensity used in the HP protocol, S_3, measured with a 1.0-dB ND filter.

First, assume that $P_0 = 0$, meaning that there is no vacuum state in the system and that $QY = 1$. In this case, we use Eqs. (B3) and (C1) to derive

$$g^{(2)}(0) = g = \frac{2(1-P_1)}{(2-P_1)^2}. \tag{K1}$$

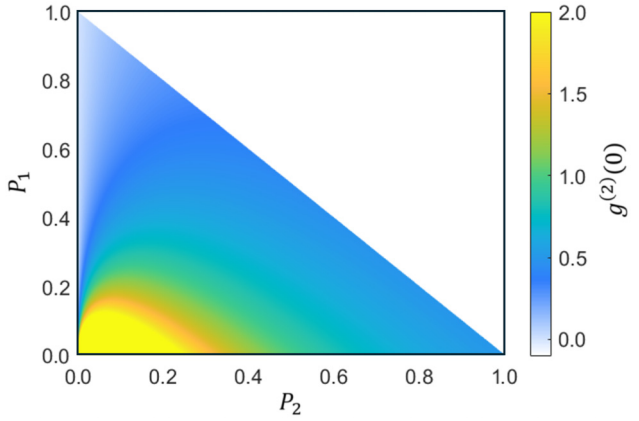


FIG. 10. $g^{(2)}(0)$ as a function of P_1, P_2 for a truncated basis source, showing that values > 0.5 are possible with increasing P_0 probability.

Now, we can find the maximum by looking at the derivative:

$$\frac{dg}{dP_1} = 0 \rightarrow -2P_1 = 0$$
$$\rightarrow P_1 = 0 \rightarrow P_2 = 1 \rightarrow g = \frac{1}{2}. \tag{K2}$$

As expected, a Fock state $|2\rangle$ has a $g^{(2)}(0)$ equal to exactly $\frac{1}{2}$.

Next, let us assume that $P_0 \neq 0$. Similarly, we can use Eqs. (B3) and (C1) to derive

$$g^{(2)} = g = \frac{2P_2}{(1-P_0+P_2)^2}, \tag{K3}$$

where we use P_2 in our analysis.

Similarly, we can look at the derivative to find

$$\frac{dg}{dP_2} = 0 \rightarrow 1 - P_0 - P_2 = 0, \tag{K4}$$

$$\rightarrow P_2 = 1 - P_0. \tag{K5}$$

Assuming that for the maximal value $P_1 = 0$, we can plug the result into Eq. (K3) to find that

$$g = \frac{1}{2(1-P_0)}. \tag{K6}$$

Interestingly, for $P_0 \rightarrow 0$, we indeed obtain the previous result of $g = \frac{1}{2}$. But, for $P_0 \rightarrow 1$, $g \rightarrow \infty$ and the result diverges.

Similar results may be obtained for $P_1 \neq 0$, as we show in Fig. 10, demonstrating a contour plot of the $g^{(2)}(0)$ results by varying P_1 and P_2. In our system, we work with

high QYs and therefore the extracted probabilities exhibit $g^{(2)}(0) \sim 0.67$.

This leads to the conclusion that relatively low-vacuum state probabilities and high-brightness emission are required for practical implementation of realistic imperfect quantum emitters. In addition, the purity of the source is not only justified by the value of $g^2(0)$ but, rather, can be calculated by the ratio between $P_1/(P_1 + P_2)$ for a $\{P_0, P_1, P_2\}$ source.

[1] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. **85**, 441 (2000).

[2] R. Alléaume *et al.*, Using quantum key distribution for cryptographic purposes: A survey, Theor. Comput. Sci. **560**, 62 (2014).

[3] S. Pirandola *et al.*, Advances in quantum cryptography, Adv. Opt. Photonics **12**, 1012 (2020).

[4] H. P. Yuen, Problems of security proofs and fundamental limit on key generation rate in quantum key distribution, ArXiv:1205.3820.

[5] H. K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photonics **8**, 595 (2014).

[6] 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).

[7] 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).

[8] R. G. Pousa, D. K. L. Oi, and J. Jeffers, Comparison of non-decoy single-photon source and decoy weak coherent pulse in quantum key distribution, Arxiv:2405.19963v1.

[9] R. D. Somma and R. J. Hughes, Security of decoy-state protocols for general photon-number-splitting attacks, Phys. Rev. A—At., Mol., Opt. Phys. **87**, 062330 (2013).

[10] M. Pereira, M. Curty, and K. Tamaki, Quantum key distribution with flawed and leaky sources, npj Quantum Inf. **5**, 62 (2019).

[11] H. K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[12] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, Invited Review Article: Single-photon sources and detectors, Rev. Sci. Instrum. **82**, 71101 (2011).

[13] B. Lounis and M. Orrit, Single-photon sources, Rep. Prog. Phys. **68**, 1129 (2005).

[14] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Fast and simple one-way quantum key distribution, Appl. Phys. Lett. **87**, 194108 (2005).

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

[16] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Provably secure and high-rate quantum key distribution with time-bin qudits, Sci. Adv. **3**, e1701491 (2017).

[17] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, Satellite-to-ground quantum key distribution, Nature **549**, 43 (2017).

[18] K. Sulimany, G. Pelc, R. Dudkiewicz, S. Korenblit, H. S. Eisenberg, Y. Bromberg, and M. Ben-Or, High-dimensional coherent one-way quantum key distribution, npj Quantum Inf. **11**, 16 (2025).

[19] C. H. Zhang, S. L. Luo, G. C. Guo, and Q. Wang, Approaching the ideal quantum key distribution with two-intensity decoy states, Phys. Rev. A—At., Mol. Opt. Phys. **92**, 022332 (2015).

[20] S. H. Sun, M. Gao, C. Y. Li, and L. M. Liang, Practical decoy-state measurement-device-independent quantum key distribution, Phys. Rev. A **87**, 052329 (2013).

[21] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A—At., Mol. Opt. Phys. **89**, 022307 (2014).

[22] B. Kraus, C. Branciard, and R. Renner, Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses, Phys. Rev. A—At., Mol. Opt. Phys. **75**, 012316 (2007).

[23] X. B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[24] G. J. Fan-Yuan, Z. H. Wang, S. Wang, Z. Q. Yin, W. Chen, D. Y. He, G. C. Guo, and Z. F. Han, Optimizing decoy-state protocols for practical quantum key distribution systems, Adv. Quantum Technol. **4**, 2000131 (2021).

[25] Y. Chen, C. Huang, Z. Chen, W. He, C. Zhang, S. Sun, and K. Wei, Experimental study of secure quantum key distribution with source and detection imperfections, Phys. Rev. A **106**, 022614 (2022).

[26] W. P. Grice and B. Qi, Quantum secret sharing using weak coherent states, Phys. Rev. A **100**, 022339 (2019).

[27] Y. Zhang, X. Ding, Y. Li, L. Zhang, Y.-P. Guo, G.-Q. Wang, Z. Ning, M.-C. Xu, R.-Z. Liu, J.-Y. Zhao, G.-Y. Zou, H. Wang, Y. Cao, Y.-M. He, C.-Z. Peng, Y.-H. Huo, S.-K. Liao, C.-Y. Lu, F. Xu, and J.-W. Pan, Experimental single-photon quantum key distribution surpassing the fundamental coherent-state rate limit, Phys. Rev. Lett. **134**, 210801 (2025).

[28] N. Somaschi, V. Giesz, L. De Santis, J. Loredo, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Anton, J. Demory *et al.*, Near-optimal single-photon sources in the solid state, Nat. Photonics **10**, 340 (2016).

[29] R. Uppu, F. T. Pedersen, Y. Wang, C. T. Olesen, C. Papon, X. Zhou, L. Midolo, S. Scholz, A. D. Wieck, A. Ludwig *et al.*, Scalable integrated single-photon source, Sci. Adv. **6**, eabc8268 (2020).

[30] M. Müller, H. Vural, C. Schneider, A. Rastelli, O. Schmidt, S. Höfling, and P. Michler, Quantum-dot single-photon sources for entanglement enhanced interferometry, Phys. Rev. Lett. **118**, 257402 (2017).

[31] J. C. Loredo, N. A. Zakaria, N. Somaschi, C. Anton, L. De Santis, V. Giesz, T. Grange, M. A. Broome, O. Gazzano, G. Coppola, I. Sagnes, A. Lemaitre, A. Auffeves, P. Senellart, M. P. Almeida, and A. G. White, Scalable performance in solid-state single-photon sources, Optica **3**, 433 (2016).

[32] Y.-M. He, Y. He, Y.-J. Wei, D. Wu, M. Atatüre, C. Schneider, S. Höfling, M. Kamp, C.-Y. Lu, and J.-W.

Pan, On-demand semiconductor single-photon source with near-unity indistinguishability, Nat. Nanotechnol. **8**, 213 (2013).

[33] X.-H. Zhan, S. Wang, Z.-Q. Zhong, Z.-Q. Yin, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, Quantum key distribution with a continuous-wave-pumped spontaneous-parametric-down-conversion heralded single-photon source, Phys. Rev. Appl. **19**, 034027 (2023).

[34] X.-H. Zhan, Z.-Q. Zhong, J.-Y. Ma, S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, Experimental demonstration of long distance quantum communication with independent heralded single photon sources, npj Quantum Inf. **11**, 1 (2025).

[35] M. Bozzio, M. Vyvlecka, M. Cosacchi, C. Nawrath, T. Seidelmann, J. C. Loredo, S. L. Portalupi, V. M. Axt, P. Michler, and P. Walther, Enhancing quantum cryptography with quantum dot single-photon sources, npj Quantum Inf. **8**, 1 (2022).

[36] C. R. Kagan, L. C. Bassett, C. B. Murray, and S. M. Thompson, Colloidal quantum dots as platforms for quantum information science, Chem. Rev. **121**, 3186 (2021).

[37] J.-H. Kim, T. Heindel, S. Reitzenstein, A. Rastelli, and N. Gregersen, Quantum dots for photonic quantum information technology, Adv. Opt. Photonics **15**, 613 (2023).

[38] H. Qian, J. Sun, X. Lu, P. Grangier, B. Sanders, J. Vuckovic, S. Zhi Xia, K. Li, S. Buckley, K. Rivoire, and J. Vučkovi, Engineered quantum dot single-photon sources, Rep. Prog. Phys. **75**, 126503 (2012).

[39] D. Nelson, S. Byun, J. Bullock, K. B. Crozier, and S. Kim, Colloidal quantum dots as single photon sources, J. Mater. Chem. C **12**, 5684 (2024).

[40] A. Nazarov, Y. Bloom, B. Lubotzky, H. Abudayyeh, A. Mildner, L. Baldessarini, Y. Shemla, E. G. Bowes, M. Fleischer, J. A. Hollingsworth *et al.*, Ultrafast and highly collimated radially polarized photons at room temperature from a colloidal quantum dot coupled to a hybrid nanoantenna, ACS Photonics **11**, 4453 (2024).

[41] H. Abudayyeh, A. Mildner, D. Liran, B. Lubotzky, L. Lüder, M. Fleischer, and R. Rapaport, Overcoming the rate-directionality trade-off: A room-temperature ultrabright quantum light source, ACS Nano **15**, 17384 (2021).

[42] B. Lubotzky, A. Nazarov, H. Abudayyeh, L. Antoniuk, N. Lettner, V. Agafonov, A. V. Bennett, S. Majumder, V. Chandrasekaran, E. G. Bowes, H. Htoon, J. A. Hollingsworth, A. Kubanek, and R. Rapaport, Room-temperature fiber-coupled single-photon sources based on colloidal quantum dots and SiV centers in back-excited nanoantennas, Nano Lett. **24**, 640 (2024).

[43] H. Abudayyeh, B. Lubotzky, A. Blake, J. Wang, S. Majumder, Z. Hu, Y. Kim, H. Htoon, R. Bose, A. V. Malko, J. A. Hollingsworth, and R. Rapaport, Single photon sources with near unity collection efficiencies by deterministic placement of quantum dots in nanoantennas, APL Photonics **6**, (2021).

[44] D. Halevi, B. Lubotzky, K. Sulimany, E. G. Bowes, J. A. Hollingsworth, Y. Bromberg, and R. Rapaport, High-dimensional quantum key distribution using orbital angular momentum of single photons from a colloidal quantum dot at room temperature, Optica Quantum **2**, 351 (2024).

[45] B. Li, G. Zhang, Y. Zhang, C. Yang, W. Guo, Y. Peng, R. Chen, C. Qin, Y. Gao, J. Hu, R. Wu, J. Ma, H. Zhong, Y. Zheng, L. Xiao, and S. Jia, Biexciton dynamics in single colloidal CdSe quantum dots, J. Phys. Chem. Lett. **11**, 10425 (2020).

[46] H. Abudayyeh, B. Lubotzky, S. Majumder, J. A. Hollingsworth, and R. Rapaport, Purification of single photons by temporal heralding of quantum dot sources, ACS Photonics **6**, 446 (2019).

[47] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on practical quantum cryptography, Phys. Rev. Lett. **85**, 1330 (2000).

[48] C. Gobby, a. Yuan, and A. Shields, Quantum key distribution over 122 km of standard telecom fiber, Appl. Phys. Lett. **84**, 3762 (2004).

[49] D. J. Gauthier, H. Zheng, and H. U. Baranger, Decoy-state quantum key distribution with nonclassical light generated in a one-dimensional waveguide, Opt. Lett. **38**, 622 (2013).

[50] Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z. F. Han, G. C. Guo, and A. Karlsson, Experimental decoy-state quantum key distribution with a sub-Poissionian heralded single-photon source, Phys. Rev. Lett. **100**, 090501 (2008).

[51] C. L. Morrison, R. G. Pousa, F. Graffitti, Z. X. Koong, P. Barrow, N. G. Stoltz, D. Bouwmeester, J. Jeffers, D. K. Oi, B. D. Gerardot *et al.*, Single-emitter quantum key distribution over 175 km of fibre with optimised finite key rates, Nat. Commun. **14**, 3573 (2023).

[52] K. Matsuzaki, S. Vassant, H. W. Liu, A. Dutschke, B. Hoffmann, X. Chen, S. Christiansen, M. R. Buck, J. A. Hollingsworth, S. Götzinger, and V. Sandoghdar, Strong plasmonic enhancement of biexciton emission: Controlled coupling of a single quantum dot to a gold nanocone antenna, Sci. Rep. **7**, 1 (2017).

[53] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, International Symposium on Information Theory, 2004. ISIT 2004. Proceedings. (2004), p. 135.

[54] M. J. Stevens, S. Glancy, S. W. Nam, and R. P. Mirin, Third-order antibunching from an imperfect single-photon source, Opt. Express **22**, 3244 (2014).

[55] Y. Bloom, I. Fields, A. Maslennikov, and G. G. Rozenman, Quantum cryptography—a simplified undergraduate experiment and simulation, Physics **4**, 104 (2022).

[56] J.-Y. Hu, B. Yu, M.-Y. Jing, L.-T. Xiao, S.-T. Jia, G.-Q. Qin, and G.-L. Long, Experimental quantum secure direct communication with single photons, Light: Sci. Appl. **5**, e16144 (2016).

[57] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).

[58] K. Sulimany, S. K. Vadlamani, R. Hamerly, P. Iyengar, and D. Englund, Quantum-secure multiparty deep learning, ArXiv:2408.05629.

[59] J. M. Pietryga, Y.-S. Park, J. Lim, A. F. Fidler, W. K. Bae, S. Brovelli, and V. I. Klimov, Spectroscopic and device aspects of nanocrystal quantum dots, Chem. Rev. **116**, 10513 (2016).

[60] Y. Chen, J. Vela, H. Htoon, J. L. Casson, D. J. Werder, D. A. Bussian, V. I. Klimov, and J. A. Hollingsworth,

"Giant" multishell CdSe nanocrystal quantum dots with suppressed blinking, J. Am. Chem. Soc. **130**, 5026 (2008).

[61] H. Htoon, A. V. Malko, D. Bussian, J. Vela, Y. Chen, J. A. Hollingsworth, and V. I. Klimov, Highly emissive multiexcitons in steady-state photoluminescence of individual giant CdSe/CdS core/shell nanocrystals, Nano Lett. **10**, 2401 (2010).

[62] F. García-Santamaría, Y. Chen, J. Vela, R. D. Schaller, J. A. Hollingsworth, and V. I. Klimov, Suppressed auger recombination in "giant" nanocrystals boosts optical gain performance, Nano Lett. **9**, 3482 (2009).

[63] P. Nagpal, N. C. Lindquist, S.-H. Oh, and D. J. Norris, Ultrasmooth patterned metals for plasmonics and metamaterials, Science **325**, 594 (2009).

[64] J. Fulmes, R. Jäger, A. Bräuer, C. Schäfer, S. Jäger, D. A. Gollmer, A. Horrer, E. Nadler, T. Chassé, D. Zhang, A. J. Meixner, D. P. Kern, and M. Fleischer, Self-aligned placement and detection of quantum dots on the tips of individual conical plasmonic nanostructures, Nanoscale **7**, 14691 (2015).

[65] A. J. Meixner, R. Jager, S. Jäger, A. Bräuer, K. Scherzinger, J. Fulmes, S. zur Oven-Krockhaus, D. A. Gollmer, D. P. Kern, and M. Fleischer, Coupling single quantum dots to plasmonic nanocones: Optical properties, Faraday Discuss. **184**, 321 (2015).

[66] M. V. Shcherbakov, A. Brebels, N. L. Shcherbakova, A. P. Tyukov, T. A. Janovsky, V. A. Kamaev *et al.*, A survey of forecast error measures, World Applied Sciences Journal **24**, 171 (2013).

[67] A. M. Fox, *Quantum Optics: an Introduction* (Oxford University Press, Oxford, 2006), Vol. 15.

[68] N. J. Orfield, S. Majumder, J. R. McBride, F. Yik-Ching Koh, A. Singh, S. J. Bouquin, J. L. Casson, A. D. Johnson, L. Sun, X. Li *et al.*, Photophysics of thermally-assisted photobleaching in "giant" quantum dots revealed in single nanocrystals, ACS Nano **12**, 4206 (2018).

[69] A. Singh, S. Majumder, N. J. Thompson Orfield, I. Sarpkaya, D. Nordlund, K. C. Bustillo, J. Ciston, V. Nisoli, S. A. Ivanov, E. G. Bowes *et al.*, From inside out: How the buried interface, shell defects, and surface chemistry conspire to determine optical performance in nonblinking giant quantum dots, Small Sci. **3**, 2300092 (2023).

[70] R. Hanbury Brown and R. Q. Twiss, Correlation between photons in two coherent beams of light, Nature **177**, 27 (1956).