Effect of source statistics on utilizing photon entanglement in quantum key distribution

Radim Hošák,[1,*] Ivo Straka,[1] Ana Predojević,[2] Radim Filip,[1] and Miroslav Ježek[1]
[1]*Department of Optics, Palacký University, 17. listopadu 12, 77146 Olomouc, Czech Republic*
[2]*Department of Physics, Stockholm University, 10691 Stockholm, Sweden*

(Received 17 December 2020; accepted 23 March 2021; published 13 April 2021)

A workflow for evaluation of entanglement source quality is proposed. Based on quantum state density matrices obtained from theoretical models and experimental data, we make an estimate of a potential performance of a quantum entanglement source in quantum key distribution protocols. This workflow is showcased for continuously pumped spontaneous parametric down-conversion (SPDC) source, where it highlights the trade-off between entangled pair generation rate and entanglement quality caused by multiphoton nature of the generated quantum states. We employ this characterization technique to show that secure key rate of down-converted photon pairs is limited to 0.029 bits per detection window due to intrinsic multiphoton contributions. We also report that there exists one optimum gain for continuous-wave down-conversion sources. We find a bound for secure key rate extracted from SPDC sources and make a comparison with perfectly single-pair quantum states, such as those produced by quantum dots.

DOI: 10.1103/PhysRevA.103.042411

I. INTRODUCTION

A. The aim of this paper

Quantum entanglement enables a multitude of technological leaps in computing and communications. We address the generation of photonic entanglement in a discrete degree of freedom, such as polarization. Realistic entanglement sources often possess a trade-off between entanglement quality and generation rate. Both of these are important in practical applications. For example, optical nonlinear parametric processes such as spontaneous parametric down-conversion (SPDC) can yield high-fidelity polarization entanglement between two photons [1]. However, with increasing generation rate, inherent multipair contributions deteriorate the measurable quantum correlations [2,3]. On the other hand, sources based on self-assembled quantum dots allow generating polarization entanglement via two energy-degenerate cascades [4] without systematic multipair statistics in the produced states.

Comparing the performance of these entanglement sources is not a clear-cut problem as conventional entanglement measures cannot be applied. The first reason is that quantum states generated by different systems can populate Hilbert spaces of different dimensions. This issue arises for example due to differences in the statistical properties of the corresponding sources. The second reason is that entanglement measures do not reflect entanglement generation rate. That is why we choose to evaluate the entanglement sources by their potential in quantum key distribution (QKD) [5,6]. Namely, the secure key rate is a quantity that benefits both from measurable strong quantum correlations (a Bell factor) and from high generation rate.

As executing entire QKD protocols for the purpose of entanglement source characterization is quite complex practically, we choose to carry out quantum state tomography instead. The effective density matrices are reconstructed within the informational degrees of freedom and are affected by both single-pair entanglement imperfections and multipair effects. Then, we analyze how well these density matrices would fare in a QKD protocol [7]. As we are interested in measuring the potential of a source by itself, we assume that the rest of the QKD protocol does not suffer from further technical limitations or loopholes [8–10]. We evaluate the limit of long-key transmission rate R_{key} per detection window as a function of coincidence rate r_{C}.

B. Quantum key distribution

The field of quantum key distribution exploits quantum correlations to ensure that two distant parties can share messages without their contents being compromised by a possible presence of a malicious party eavesdropping on the communication channel [5]. Many QKD protocols for transmission of discretely encoded information rely on random choices of encoding and decoding bases. Perhaps the best known is the protocol BB84 [11] whose performance relies on nonclassicality of the single-photon source employed [12]. The protocol E91 [13] incorporated entanglement into QKD, employing random switching between projection bases. Furthermore, if the security is guaranteed even in presence of untrustworthy entanglement source or detection equipment, the protocols can be called device-independent QKD [14–17].

The major figure of merit in QKD is the minimum average bit rate at which secure key can be transmitted between distant parties [6]. Evaluating this rate is generally a task different from assessing the presence of entanglement. Secure key rate itself depends on other factors, for example the quantum bit

*hosak@optics.upol.cz

error rate (QBER) [7], or the capabilities of the eavesdropper. Therefore, it can occur that certain sources of entanglement cannot be used at all for secure QKD through a given channel whereas others might be viable. To prove the secure key rate for the sources, the whole protocol would need to be carried out explicitly. Such data are usually not available, because they would require extensive experimental effort. So instead, we make use of quantum tomography data that is commonly available for quantum entanglement sources. This involves reducing the generated states to the informational degrees of freedom by projecting multiphoton contributions into a two-qubit Hilbert space. The resulting two-qubit density matrices are then evaluated in terms of QKD performance. This approach, however, should not be treated as a proof of QKD performance of states containing multiphoton noise, because the multiphoton contribution may have different effect on tomography than in QKD. The secure key rate calculated from the reconstructed two-qubit matrices shows how multipair contributions influence the effective purity and entanglement of intrinsically multiphoton states. The secure key rate also offers a way of quantifying the trade-off between generation rate and entanglement quality. It therefore serves to evaluate entanglement of two-qubit density matrices, given their generation rate. Because only the source is being characterized, we consider the rest of the QKD protocol to be ideal, not taking into account aspects such as finite key size or the detection loophole.

C. Entanglement sources

In this work, we compare two photon-pair sources of polarization entanglement—continuous-wave spontaneous parametric down conversion (SPDC) [18] and self-assembled quantum dots from the perspective of entanglement-based QKD. These two physical platforms produce entangled states of different modal structure.

First, we focus on SPDC. It is a nonlinear optical process which produces entangled photon pairs in two optical modes. We assume a continuous-wave pump and the temporal coherence of the photons to be much shorter than the generation rate and detector resolution. We detect the quantum states in the coincidence basis, meaning only simultaneous detections in both modes are recorded. Consequently, the generated signal can be considered a random Poissonian sequence of photon pairs that are entangled in polarization. Such randomness inevitably leads to detecting multiple pairs within one detection window. This becomes more prominent with increasing detection window and with a higher gain of the source.

We elected cw pumping in favor of pulsed SPDC, because the effect of the multipair contributions is much lower at the same generation rate. Our analysis indicates that if there is one pump pulse in every detection window, the multipair contributions of both cw and pulsed regimes have the same effect on secure key rate. However, the pulse repetition frequency is usually not that high. The detection window width is only limited by the temporal jitter of the detectors, which can easily be $<10^{-9}$ s even for noncryogenic detectors. On the other hand, the typical repetition frequency of pulsed SPDC pumps is on the order of $\approx 10^{8}$ s^{-1}. This means that cw gets an order-of-magnitude advantage in secure key rate. This holds even in the light of the most recent advances in cryogenic detector resolution (3 ps) [19] and SPDC pump frequency (43 GHz) [20].

Multiphoton nature is inherent to SPDC and it has been studied in the context of single-photon sources [21–23], in quantum information processing [24–26] and quantum key distribution [27,28] protocols. SPDC for QKD has also been investigated with respect to noise and its effect on the detection efficiency required to achieve provable protocol security [29].

The second physical platform involves quantum dots. They act as semiconductor embedded quantum emitters and allow the optical generation of photon pairs via decay of a biexciton. The energy degeneracy of two biexciton cascades leads to a superposition of two decay paths and thus to entanglement of the emitted photon pairs. Excitation and deexcitation of such cascades is a Rabi cycle that is pumped by a π-pulse [30]. Therefore, a quantum dot produces no more than one entangled photon pair at a time [22] and with near-unity generation efficiency. This is the key difference between quantum dots and SPDC. However, it is much more challenging to reach a good collection efficiency of the photons, which means that entangled pairs are usually extracted from quantum dot sources at low effective rates.

We provide a model for SPDC entanglement sources pumped by a continuous wave (cw) laser. Then, we compare the model with experimental SPDC data and current state-of-the-art quantum dot sources. We find that the secure key rate using cw SPDC is fundamentally bounded, whereas quantum dot sources are capable of surpassing this bound.

II. SECURE KEY RATE

For our investigation we are assuming an entanglement-based QKD protocol, the security of which was analyzed in Refs. [7,14]. Polarization-encoded photonic qubits will be assumed. The protocol relies on Alice and Bob sharing a two-qubit entangled state. Alice can choose one of three measurements A_0, A_1, A_2 to perform on her qubit, and Bob can choose from two measurements B_1 and B_2 to perform on his qubit. The measurement results a_i, b_j are binary: $+1$ or -1. Furthermore, they fulfill the following condition:

$$\langle a_i \rangle = \langle b_j \rangle = 0 \; \forall \; i, j. \tag{1}$$

The results of measurements A_0 and B_1 are used to extract the raw key, whereas the measurements A_1, A_2, B_1, and B_2 are used to calculate the Clauser-Horne-Shimony-Holt (CHSH) polynomial S [31]. The protocol is only secure for S that violates the classical inequality, e.g., $2 < S \leqslant 2\sqrt{2}$. In general, the rate r of the secure key in a given QKD protocol is very difficult to ascertain [32–34] because this asks for a very specific definition of the security level attained. Instead, we limit ourselves here to an estimate of the lower bound on secure key rate per photon pair. This is given by a quantity called the Devetak-Winter rate r_{DW} [6,7]

$$r \geqslant r_{\mathrm{DW}} = I(\mathrm{A}_0 : \mathrm{B}_1) - \chi(\mathrm{B}_1 : \mathrm{E}), \tag{2}$$

where $I(\mathrm{A}_0 : \mathrm{B}_1)$ is the mutual information between Alice and Bob, and $\chi(\mathrm{B}_1 : \mathrm{E})$ is the Holevo quantity [35] between Bob and Eve. For the studied protocol, the mutual information can

be expressed as

$$I(\mathrm{A}_0 : \mathrm{B}_1) = 1 - h(Q), \tag{3}$$

while the Holevo quantity is bounded as follows:

$$\chi(\mathrm{B}_1 : \mathrm{E}) \leqslant h\left(\frac{1+\sqrt{(S/2)^2-1}}{2}\right). \tag{4}$$

Here h denotes the binary entropy function $h(Q) = -Q\log_2 Q - (1-Q)\log_2(1-Q)$, S is the CHSH polynomial, and Q is the quantum bit error rate (QBER) defined as the probability of opposite measurement results when the bases A_0 and B_1 are used

$$Q = P(a \neq b|\mathrm{A}_0, \mathrm{B}_1). \tag{5}$$

Substituting (3) and (4) into (2) leads to the following bound:

$$r_{\mathrm{DW}} = 1 - h(Q) - h\left(\frac{1+\sqrt{(S/2)^2-1}}{2}\right). \tag{6}$$

This quantity represents the minimum ratio of the bits used as the secure key relative to the number of entangled pairs that were detected. To introduce secure key rate, we need to define the coincidence rate r_{C} as the rate of detected photon pairs per detection window. For a measurement with data acquisition subdivided into N_{win} windows, where a total of N_{C} coincidences were registered, the coincidence rate is

$$r_{\mathrm{C}} = \frac{N_{\mathrm{C}}}{N_{\mathrm{win}}}. \tag{7}$$

Then, the secure key rate becomes

$$R_{\mathrm{key}} = r_{\mathrm{DW}} r_{\mathrm{C}}, \tag{8}$$

quantifying the minimum number of secure key bits transferred per one detection window that serves as the basic unit of time.

Because r_{DW} is a function of S and Q, let us calculate these quantities provided that we have the effective quantum state ρ. The correlation tensor T_ρ and the positive symmetric tensor U_ρ [36] are first calculated,

$$T_{\rho,ij} = \mathrm{Tr}[\rho \cdot (\sigma_i \otimes \sigma_j)], \quad i,j = 1,2,3, \tag{9}$$

$$U_\rho = T_\rho^{\mathrm{T}} T_\rho, \tag{10}$$

where σ_i are the Pauli matrices. Consequently the three eigenvalues of U_ρ are sorted in a descending order, $\lambda_1 \geqslant \lambda_2 \geqslant \lambda_3$. The best possible values of S [37] and Q are then

$$S_{\max} = 2\sqrt{\lambda_1 + \lambda_2}, \tag{11}$$

$$Q_{\min} = \frac{1-\sqrt{\lambda_1}}{2} \text{ (see Appendix C)}. \tag{12}$$

Appendix C shows the corresponding optimal configuration of bases $A_{0,1,2}$, $B_{1,2}$ and provides some additional information including an experimental guide to setting the wave plates.

III. SPONTANEOUS PARAMETRIC DOWN-CONVERSION ENTANGLEMENT SOURCE

SPDC sources at very low gains produce maximally entangled two-qubit states with a multiphoton-pair component which is negligible in the context of the QKD protocol. However, at higher interaction gains, the multipair contribution emerges and starts to deteriorate the quality of entanglement [3,38,39]. This leads to diminishing r_{DW}. On the other hand, increasing gain leads to higher brightness, and the rate r_{C} increases.

To study the effect of SPDC multiphoton component on potential performance in QKD, we used a continuously pumped entanglement source with a variable coincidence window. Although the SPDC gain should ideally be controlled by pump power, in the cw case it can be equivalently controlled by the coincidence window τ used for data acquisition. We leveraged this to study a broader range of scenarios with more ease. With longer coincidence windows, there is a chance of photons generated as products of independent SPDC processes to contribute to the coincidence count. As the individual processes are independent and very fast, the amount of pairs collected by the detectors within the coincidence window of length τ obeys the Poissonian statistics with a mean pair number $\bar{n}$ proportional to τ.

The model described in Appendix A enables us to see how the detection of multiple independent copies of the state ρ_0 affects the reconstructed two-qubit density matrix ρ effectively describing the state. The whole model is parametrized by the mean photon pair number $\bar{n}$ per detection window and overall optical transmittances in Alice's and Bob's part of the physical setup η_{A} and η_{B}, respectively. The transmittances consist of signal collection efficiency, transmission loss, and detection efficiency. As we are interested in characterizing entanglement sources exclusively, we do not consider additional noise and loss present in the optical communication channel.

It is possible to choose the state ρ_0 from an experimentally obtained reconstruction of a real quantum entangled state produced by low-gain SPDC. This approach allows us to account for realistic experimental imperfections present in the generated quantum states. To allow for analytical insight, we consider ρ_0 to be one of the Bell states, which we denote $\rho_{\mathcal{B}}$. Then, the maximum-likelihood estimate of ρ is a mixture of the Bell state and white noise,

$$\tilde{\rho}_{\mathcal{B}} = (1-\kappa)\rho_{\mathcal{B}} + \kappa \tfrac{1}{4}\mathbb{1} \otimes \mathbb{1}, \tag{13}$$

where $\mathbb{1}$ is a unity matrix. The parameter κ depends on the physical parameters $\bar{n}$, η_{A}, and η_{B} (see Appendix A).

For a density matrix $\tilde{\rho}_{\mathcal{B}}$ of the form (13), both S and Q are related to κ as follows:

$$S = 2\sqrt{2(1-\kappa)^2}, \quad Q = \frac{\kappa}{2}. \tag{14}$$

From these, r_{DW} can be calculated using (6).

Our model addresses the trade-off between entanglement quality, reflected by r_{DW}, and entangled pair quantity, which corresponds to r_{C}. This is shown in Fig. 1(a). At low r_{C}, r_{DW} maintains a very high value close to one. As r_{C} increases, however, r_{DW} starts to deteriorate quickly, until the QKD protocol ceases to be secure. The underlying mechanism behind this gradual degradation of QKD security lies in the multiphoton component. Multiple pairs inside one window result chiefly in three-photon and four-photon events. As the one-qubit reductions of (13) are always maximally mixed, the extra multiphoton contribution corresponds to white noise.

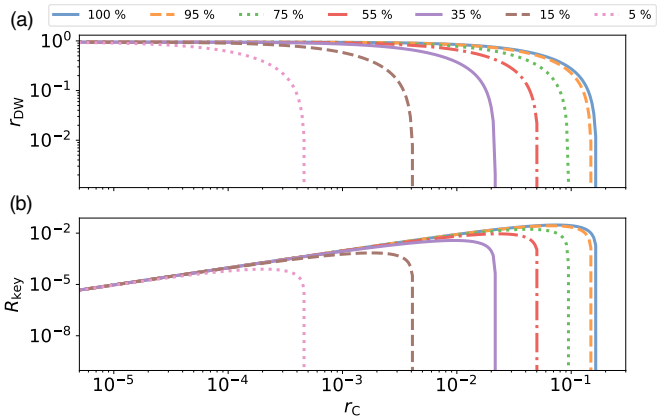

FIG. 1. (a) The lower bound on secure key rate r_{DW} as a function of coincidence rate r_C for a low-gain cw SPDC entanglement source. (b) The key rate R_{key} as a function of r_C. Calculations for various values of symmetric transmittance $\eta_A = \eta_B = \eta$ are shown as differently colored lines. The loss-free case $\eta = 100\%$ is shown as the rightmost solid blue line, and represents a fundamental limitation of SPDC entanglement source performance in the QKD protocol. The quantities r_{DW}, R_{key}, and r_C are a function of $\bar{n}$, as given by (6), (8), (14)–(16); for exact formulas see Appendix A.

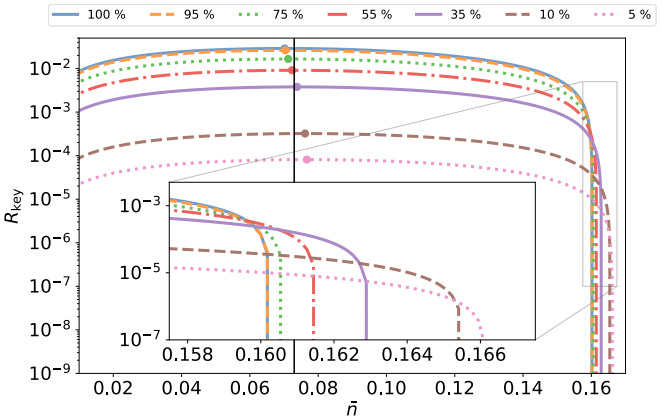

FIG. 2. Secure key rate R_{key} as a function of mean photon pair number $\bar{n}$ for various amounts of symmetric transmittance $\eta_A = \eta_B = \eta$. The optimal values of key rate for each transmittance are shown as dots. The black vertical line represents the $\bar{n} = 0.0737$ for which the R_{key} is within 0.2% of the maximum R_{key} for the given transmittance. The inset shows how the key rate starts to diminish as $\bar{n}$ approaches the critical value.

The quantities r_C and r_{DW} are multiplied to obtain R_{key} which is the main figure of merit. When plotted against r_C, as shown in Fig. 1(b), a linear increase in key rate can be seen at first, until a peak is reached for a certain r_C, after which key rate drops quickly. In a two-dimensional space of quality (R_{key}) and quantity (r_C) axes, the zero-loss case $\eta = 1$ bounds the area that is accessible to continuous SPDC sources.

The model can be analyzed in another way. When we expand the exact formula for κ (see Appendix A) into a Taylor series, we can see that in the low-gain regime $\bar{n} \ll 1$,

$$\kappa \approx \frac{\bar{n}}{1+\bar{n}}, \tag{15}$$

$$r_C \approx \bar{n}\eta_A\eta_B. \tag{16}$$

This means that the quantum state ρ depends very little on transmittances. Moreover, using these relations, we can see that R_{key} is a factorizable function: $R_{key} \approx \eta_A\eta_B\bar{n}r_{DW}(\bar{n})$. This allows us to optimize the key rate with respect to $\bar{n}$,

$$R_{key}^{opt} \approx 0.029\eta_A\eta_B \text{ for } \bar{n}_{opt} \approx 0.0737. \tag{17}$$

With this particular value of $\bar{n}$, the corresponding key rate will always be within 0.2% of the real maximum value for the given transmittances.

Figure 2 shows that the transmittances are primarily a scaling factor for R_{key} and highlights the optimal points (17). Figure 2 also shows that around $\bar{n} = 0.16$, the key rate starts dropping sharply. The maximal value of $\bar{n}$ giving a nonzero key rate is 0.166 839, in the limit of zero transmittance.

The dependence of the optimal key rate on transmittance is shown in Fig. 3. For easier depiction, we assume symmetric transmittances $\eta_A = \eta_B = \eta$. One can observe the dependence (17). The exact optimal point $\bar{n}$ depends on transmittance as well, albeit not significantly. This result means that setting the SPDC source at a certain gain is going to guarantee the optimal trade-off between entanglement and brightness.

IV. EXPERIMENTAL RESULTS

To validate the predictions of our model, we used a cw pumped noncollinear, type-I SPDC [1] with a BiBO nonlinear crystal. To obtain the maximal Bell factor without the necessity of measurement optimization we performed a full quantum state tomography on the source for varied lengths of coincidence windows, which allowed us to tune the mean pair number $\bar{n}$ and thus the rate r_C of the effective state ρ. The density matrices were each reconstructed from a set of 36 tomographic measurements using the method of maximum likelihood estimation [40,41]. From these density matrices r_{DW} was calculated. Statistical confidence of each measurement was estimated by 2000 Monte Carlo simulations based on Poissonian variance of all coincidence counts. The total number of coincidences N_C for coincidence rate calculation

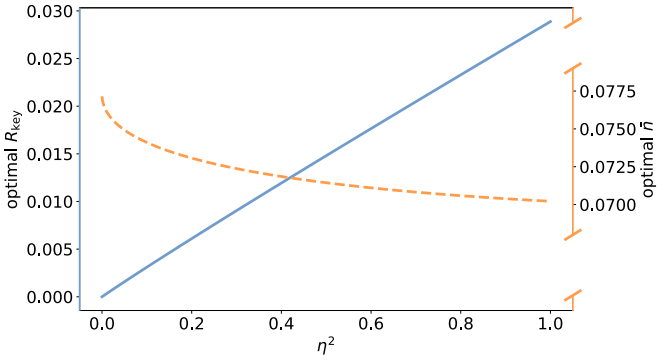

FIG. 3. The optimal achievable key rate R_{key} (blue line) and the corresponding mean photon pair number $\bar{n}$ (orange dashed line) for a given two-mode transmittance η^2. Symmetric single-mode transmittance $\eta_A = \eta_B = \eta$ is assumed. The optimal key rate scales quadratically with η. The corresponding value of the mean photon pair number parameter $\bar{n}$ depends on η very weakly, allowing to choose one fixed value of $\bar{n}$ independently on η to obtain key rate very close to the optimal value.

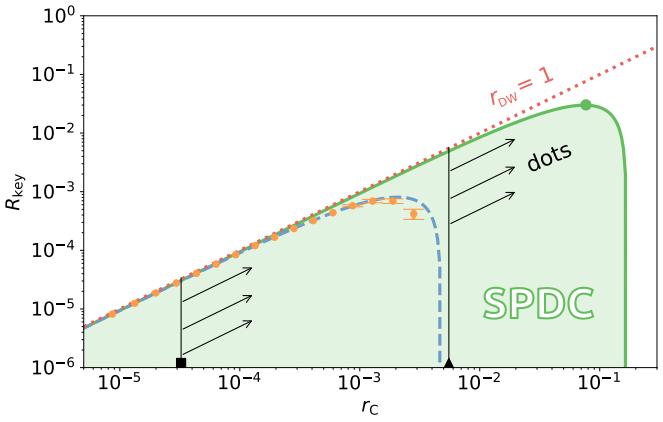

FIG. 4. The dependence of key rate R_{key} on coincidence rate r_C for different implementations of quantum entanglement sources. The orange points represent density matrices reconstructed from a continuously pumped SPDC source, whereas the blue dashed line is the result of a cw SPDC model with $\eta_A = \eta_B = 0.16$. The solid green line represents an ideal no-loss scenario and marks a fundamental limitation of SPDC entanglement sources in the QKD protocol. The green point shows the upper bound on key rate for SPDC entanglement sources, with $R_{key}^{max} = 0.029$. The black square and triangle marks represent the r_C of quantum dot entanglement sources [42] and [19], respectively. The arrows pointing diagonally show that key rate of quantum dot entanglement sources increases linearly with r_C. The red dotted line shows the linear dependence for an ideal quantum dot source with $r_{DW} = 1$. For such an ideal quantum dot source the dependence overlaps with that of a SPDC source for lower values of r_C. For high enough r_{DW} and r_C, quantum dot entanglement sources are going to surpass even the best SPDC sources.

(7) was obtained by summing up coincidence counts for four complementary projections in each of the nine tomographic sets of projections and then averaged, with $N_{win} = T/\tau$ available from known duration of measurement T and length of the coincidence window τ. This is an accurate calculation of N_C for small multiphoton contributions, which holds for our data where $r_C < 10^{-2}$. Both sets of r_C and r_{DW} allow us to compare the experimental data against the prediction of our model (see Fig. 4). For this prediction we choose the quantum state ρ_0 to be a density matrix of an entangled state produced by the source, which was obtained using a 1 ns coincidence window. This quantum state exhibits $S = 2.815(5)$ and $Q = 0.0013(5)$. Following the procedure outlined in Appendix A we arrive at different effective density matrices ρ as the mean pair number $\bar{n}$ varies. The η parameter of the model was set to the value of 0.16 to reflect the two-photon collection efficiency of the experimental setup. A complete data set for the experimental points of Fig. 4 is given in Table I in Appendix E.

V. COMPARISON WITH QUANTUM DOT ENTANGLEMENT SOURCES

Finally, SPDC is compared with recent entanglement sources based on quantum dots. Due to their discrete energy structure and strong sub-Poissonian nature of light emitted individually in the signal and idler mode, there is no multipair component in the generated entangled state. In addition, the generation of photon pairs can be achieved with near-unity efficiency. However, current sources often suffer from imperfect collection of photons, which in turn leads to increased losses and low coincidence rate. This means that improving collection efficiency is an important goal of quantum dot entanglement source engineering. The behavior of the key rate R_{key} with respect to r_C is shown in Fig. 4.

The r_{DW} of quantum dot entanglement sources is not subject to a fundamental quality-quantity trade-off, contrary to SPDC sources. The r_{DW} obtained using quantum dots depends primarily on achieved degree of entanglement and does not deteriorate with the increased excitation rate. We illustrate this behavior in Fig. 4. The most noticeable feature is that the SPDC sources are systematically bounded whereas quantum dot ones are not. For a quantum dot source with known degree of entanglement [42] the key rate will scale linearly with r_C. With increased collection efficiency a quantum dot source can reach r_C that is above the one at which our experimental SPCD source can viably yield a nonzero R_{key}. Ongoing improvements in quantum dot entangled photon pair sources can be seen in their recent realizations [19,42] where collection efficiency and quality of entanglement have been increased.

VI. CONCLUSION

We predicted the dependence of key rate in entanglement-based QKD on the generation rate of photon-pair sources based on continuous-wave SPDC and enabled their comparison with quantum dot sources of entanglement. The SPDC is systematically limited by multiple photon pairs being generated during a single detection window. The multiphoton contribution corresponds to white noise proportional to the SPDC gain. Consequently, the secure key rate is fundamentally bound by the value $R_{key}^{max} = 0.029$ bits/window. The optimal gain for SPDC was shown to be $\bar{n}_{opt} = 0.0737$ pairs/window.

Quantum dot sources, on the other hand, do not have a fundamental limit that is bound to photon statistics. This means that an increase of the coincidence rate r_C should not reduce the quality of the source, and with it related Devetak-Winter rate r_{DW}. Therefore, it is reasonable to expect that quantum dot sources could overcome the SPDC ones in performance. How superior they can be depends on several factors, some of them limiting. First, there is the source emission efficiency that is affected by phonons [43]. These phonon effects can be minimized by embedding the quantum dot in a narrowband cavity. However, an efficient extraction of photon pairs demands broadband cavities, limiting the emission efficiency to 90%. There are various proposed schemes that target an ideal broadband cavity that allows for near unity collection of the emitted photons [44], promising efficiencies of up to 99%. The state preparation could also have a limit in biexciton binding energy [45] which could be overcome by adequate preparation of the excitation pulse. However, efficiency is not the only parameter determining the key rate R_{key}. The currently achievable degree of entanglement is relatively high. Furthermore, the indistinguishability of the excitonic states would be further improved by embedding the quantum dot in a structure that features a high Purcell factor [44]. If we consider only dephasing noise

and a concurrence of 95%, the minimum coincidence rate per excitation necessary to overcome the SPDC upper bound would be $r_C > 0.035$; 0.044 in the case of a white noise. The secure key rate of quantum dot sources therefore has the potential to overcome SPDC following a number of technical optimizations.

The proposed quantification of a key rate per window could be extended to a key rate per time. This would include a multiplication by the number of detection windows per time, which is usually limited by the temporal resolution of the detectors. In the case of quantum dots, the lifetimes of the photons—typically on the order of ≈100 ps—represent the limit for the excitation frequency and for the coincidence rate per time. SPDC, on the other hand, can easily get the biphoton coherence to picosecond range, which is the current resolution limit of single-photon detectors [46]. As a result, SPDC can benefit from narrower coincidence windows and therefore have an additional advantage in terms of key rate per time.

The authors have recently become aware of a recent work which demonstrates the feasibility of experimental employment of quantum dot entanglement sources for the purposes of QKD [47].

ACKNOWLEDGMENTS

This work has received national funding from the MEYS and the funding from European Union's Horizon 2020 research and innovation framework programme under Grant Agreement No. 731473 (Project No. 8C18002). Project Hyper-U-P-S has received funding from the QuantERA ERA-NET Cofund in Quantum Technologies implemented within the European Union's Horizon 2020 Programme. This work was also supported by the Czech Science Foundation (17-26143S). R.H. acknowledges the support of the Palacky University (projects IGA-PrF-2020-009 and IGA-PrF-2021-006). R.F. acknowledges the project CZ.02.1.01/0.0/0.0/16_-026/0008460 of MEYS CR. A.P. would also like to acknowledge Swedish Research Council and Carl Tryggers Stiftelse.

APPENDIX A: TOMOGRAPHY IN CONTINUOUS WAVE

The effect of multiphoton contributions will be modeled in this section. The initial quantum state ρ_0 corresponds to a single photon pair and represents the low-gain limit of the SPDC process. The state ρ_0 is subjected to a set of tomographic measurements. Each qubit is projected onto a state $|\psi_i\rangle$, typically one of the polarization states H, V, D, A, R, L. This would normally lead to a set of 36 two-qubit projections $c^0_{ij} = \langle\psi_i\psi_j|\rho_0|\psi_i\psi_j\rangle$.

Here we also need the reduced one-qubit density matrices ρ_0^{A}, ρ_0^{B} by tracing over the other mode,

$$\rho_0^{\mathrm{A/B}} = \mathrm{Tr}_{\mathrm{B/A}}[\rho_0]. \tag{A1}$$

For all projections $\{i, j\}$, we need to calculate probabilities of each detector clicking (1) or not clicking (0). Because the transmittances $\eta_{\mathrm{A,B}}$ may cause photons to be lost, the possible combinations are

$$p^{(11)}_{ij} = \eta_{\mathrm{A}}\eta_{\mathrm{B}}\langle\psi_i\psi_j|\rho_0|\psi_i\psi_j\rangle, \tag{A2}$$

$$p^{(10)}_{ij} = \eta_{\mathrm{A}}\eta_{\mathrm{B}}\langle\psi_i\psi_j^{\perp}|\rho_0|\psi_i\psi_j^{\perp}\rangle + \eta_{\mathrm{A}}(1-\eta_{\mathrm{B}})\langle\psi_i|\rho_0^{\mathrm{A}}|\psi_i\rangle, \tag{A3}$$

$$p^{(01)}_{ij} = \eta_{\mathrm{A}}\eta_{\mathrm{B}}\langle\psi_i^{\perp}\psi_j|\rho_0|\psi_i^{\perp}\psi_j\rangle + (1-\eta_{\mathrm{A}})\eta_{\mathrm{B}}\langle\psi_j|\rho_0^{\mathrm{B}}|\psi_j\rangle, \tag{A4}$$

$$p^{(00)}_{ij} = \eta_{\mathrm{A}}\eta_{\mathrm{B}}\langle\psi_i^{\perp}\psi_j^{\perp}|\rho_0|\psi_i^{\perp}\psi_j^{\perp}\rangle + \eta_{\mathrm{A}}(1-\eta_{\mathrm{B}})\langle\psi_i^{\perp}|\rho_0^{\mathrm{A}}|\psi_i^{\perp}\rangle + (1-\eta_{\mathrm{A}})\eta_{\mathrm{B}}\langle\psi_j^{\perp}|\rho_0^{\mathrm{B}}|\psi_j^{\perp}\rangle + (1-\eta_{\mathrm{A}})(1-\eta_{\mathrm{B}}), \tag{A5}$$

with $\langle\psi_i|\psi_i^{\perp}\rangle = 0$. The order of the modes was set to $\rho_0 \in \mathcal{H}_{\mathrm{Alice}} \otimes \mathcal{H}_{\mathrm{Bob}}$, whereas the other variant can be expressed by swapping A and B.

In a real tomographic measurement, only coincidences (11) are registered, but they can be caused by multiple pairs. Assuming a short coherence time, the number of generated pairs n follows the Poisson distribution. Then, the probability of a coincidence is

$$c_{ij} = \sum_{n=0}^{\infty}\left[1 - \left(p^{(10)}_{ij} + p^{(00)}_{ij}\right)^n - \left(p^{(01)}_{ij} + p^{(00)}_{ij}\right)^n + \left(p^{(00)}_{ij}\right)^n\right]\frac{n^{\bar{n}}}{n!}e^{-\bar{n}}. \tag{A6}$$

The mean pair number $\bar{n}$ is a parameter of the model proportional to the coincidence window width τ and the gain of the SPDC process. The density matrix ρ is then found as the maximum-likelihood estimation that best explains the measured set of probabilities $\{c_{ij}\}$ [40,41].

If the initial state is chosen as one of the Bell states $\rho_0 = \rho_{\mathcal{B}}$, the result has the form

$$\rho = (1-\kappa)\rho_{\mathcal{B}} + \kappa\tfrac{1}{4}\mathbb{1}\otimes\mathbb{1}, \quad \kappa \in [0,1]. \tag{A7}$$

The tomography of the state ρ yields model probabilities that can be analytically calculated,

$$C_{ij} = \langle\psi_i\psi_j|\rho|\psi_i\psi_j\rangle. \tag{A8}$$

The log-likelihood function then is (see Appendix B)

$$\log\mathcal{L} = \sum_{i,j} c_{ij}\log(C_{ij}). \tag{A9}$$

The parameter κ is obtained by solving $\partial(\log\mathcal{L})/\partial\kappa = 0$,

$$\kappa = \frac{2\left(e^{\frac{\eta_{\mathrm{A}}\bar{n}}{2}} - 1\right)\left(e^{\frac{\eta_{\mathrm{B}}\bar{n}}{2}} - 1\right)}{1 - 2e^{\frac{\eta_{\mathrm{A}}\bar{n}}{2}} - 2e^{\frac{\eta_{\mathrm{B}}\bar{n}}{2}} + e^{\frac{\eta_{\mathrm{A}}\eta_{\mathrm{B}}\bar{n}}{2}} + 2e^{\frac{(\eta_{\mathrm{A}}+\eta_{\mathrm{B}})\bar{n}}{2}}}. \tag{A10}$$

From (A7) it is possible to arrive to analytical expressions for the CHSH polynomial S and QBER Q, which in turn can be used to calculate r_{DW}:

$$S = 2\sqrt{2(1-\kappa)^2}, \quad Q = \frac{\kappa}{2}, \tag{A11}$$

$$r_{\mathrm{DW}} = 1 - h(Q) - h\left(\frac{1+\sqrt{(S/2)^2-1}}{2}\right). \tag{A12}$$

The coincidence rate r_C is

$$r_C = \sum_{n=0}^{\infty} (1-(1-\eta_A)^n)[1-(1-\eta_B)^n]\frac{n^{\bar{n}}}{n!}e^{-\bar{n}}$$
$$= 1 - e^{-\eta_A\bar{n}} - e^{-\eta_B\bar{n}} + e^{-(\eta_A+\eta_B-\eta_A\eta_B)\bar{n}}. \quad \text{(A13)}$$

APPENDIX B: LIKELIHOOD DEFINITION

To recapitulate, the objective of the quantum state tomography is to find a suitable density matrix ρ that best explains the relative frequencies (probabilities) $\{c_{ij}\}$ that were either measured or modeled by (A6). Likelihood is a probability of obtaining the results $\{c_{ij}\}$ conditional on ρ. We denote the density matrix ρ that maximizes the probability of obtaining the relative frequencies $\{c_{ij}\}$ as the maximum-likelihood estimate.

Let us suppose that we are running N two-qubit projection measurements in a two-qubit basis $\{|\Psi_k\rangle\}_{k=1}^4$, where $\sum_k |\Psi_k\rangle\langle\Psi_k| = \mathbb{1}\otimes\mathbb{1}$. Then we obtain the projection probabilities

$$C_k = \langle\Psi_k|\rho|\Psi_k\rangle, \quad \text{(B1)}$$

where $\sum_k C_k = 1$. Such a measurement run would result in n_k projections of each $|\Psi_k\rangle$, ($\sum_k n_k = N$), and the probability of this result follows the multinomial distribution,

$$\Pr[\{n_k\}] = \frac{N!}{\prod_k (n_k!)}\prod_k C_k^{n_k}. \quad \text{(B2)}$$

In our model, we consider relative frequencies c_k rather than counts n_k, which would be obtained for $N\to\infty$, and we denote

$$c_k \simeq \frac{n_k}{N}. \quad \text{(B3)}$$

The likelihood of obtaining $\{c_k\}$ when measuring in basis $\{|\Psi_k\rangle\}$ then follows from (B2),

$$\mathcal{L}_\Psi = \frac{N!}{\prod_k (Nc_k)!}\prod_k C_k^{Nc_k}. \quad \text{(B4)}$$

The quantum state tomography consists of multiple projection bases, most commonly nine that correspond to all possible products of Pauli matrices. So, the overall probability (likelihood) of obtaining $\{c_{ij}\}$ is

$$\mathcal{L} = \prod_\Psi \mathcal{L}_\Psi, \quad \text{(B5)}$$

where indexing over Ψ and k just becomes indexing over i, j in the paper.

To maximize the likelihood $\mathcal{L}$, it is more convenient to maximize $\log(\mathcal{L})$. These are equivalent, because logarithm is a monotonically increasing function. This lets us rewrite (B4) and (B5) as

$$\log\mathcal{L} = N\sum_{ij} c_{ij}\log C_{ij} + \sum_\Psi \log(N!) - \sum_{ij}\log[(Nc_{ij})!]. \quad \text{(B6)}$$

Now we find the maximum-likelihood estimate ρ (represented by C_{ij}) by solving for the parameter κ,

$$\frac{d\log\mathcal{L}}{d\kappa} = 0. \quad \text{(B7)}$$

For the maximization, the likelihood does not have to be normalized (we leave out the factor N), and we can also omit constant terms that do not depend on C_{ij} [the second and third sums in (B6)]. The likelihood is then simplified to the common form [41]

$$\log\mathcal{L} = \sum_{ij} c_{ij}\log C_{ij}. \quad \text{(B8)}$$

APPENDIX C: EXPERIMENTAL COOKBOOK

Following the approach introduced in Ref. [37], let us formulate the optimal configuration of Alice's and Bob's bases A_0, A_1, A_2, B_1, B_2 [7] given a reconstructed quantum state ρ. The bases A_1, A_2, B_1, B_2 need to give the maximum CHSH violation [48] and the bases A_0, B_1 need to minimize the QBER. The respective derivations are presented in Appendix D.

We denote the measurement in basis X by the operator $X = |\psi\rangle\langle\psi| - |\psi^\perp\rangle\langle\psi^\perp|$, where the direction of $|\psi\rangle$ can be parametrized using the unit vector $\boldsymbol{x}\in\mathbb{R}^3$ and the vector of Pauli matrices $\boldsymbol{\sigma} = \{\sigma_1,\sigma_2,\sigma_3\}$: $X = \boldsymbol{x}\cdot\boldsymbol{\sigma}$. The bases will therefore be given by real unit vectors $\boldsymbol{a}_{0,1,2}$ for Alice and $\boldsymbol{b}_{1,2}$ for Bob.

We begin by introducing the real tensor T_ρ and the positive symmetric tensor U_ρ [37]:

$$T_{\rho,ij} = \mathrm{Tr}[\rho\cdot(\sigma_i\otimes\sigma_j)], \quad \text{(C1)}$$
$$U_\rho = T_\rho^{\mathrm{T}}T_\rho. \quad \text{(C2)}$$

Let us find the eigenvalues and unit eigenvectors of U_ρ,

$$U_\rho\boldsymbol{e}_i = \lambda_i\boldsymbol{e}_i, \quad |\boldsymbol{e}_i| = 1, \quad i = 1,2,3, \quad \text{(C3)}$$

and index them in the descending order $\lambda_1 \geqslant \lambda_2 \geqslant \lambda_3$.

The optimal choice of bases depends on which modes are assigned to Alice and Bob (see Appendix D).

(1) $\rho\in\mathcal{H}_{\mathrm{Alice}}\otimes\mathcal{H}_{\mathrm{Bob}}$

$$\boldsymbol{a}_0 = \frac{T_\rho\boldsymbol{e}_1}{|T_\rho\boldsymbol{e}_1|}, \quad \text{(C4)}$$

$$\boldsymbol{a}_1 = \sqrt{\frac{\lambda_1}{\lambda_1+\lambda_2}}\frac{T_\rho\boldsymbol{e}_1}{|T_\rho\boldsymbol{e}_1|} + \sqrt{\frac{\lambda_2}{\lambda_1+\lambda_2}}\frac{T_\rho\boldsymbol{e}_2}{|T_\rho\boldsymbol{e}_2|}, \quad \text{(C5)}$$

$$\boldsymbol{a}_2 = \sqrt{\frac{\lambda_1}{\lambda_1+\lambda_2}}\frac{T_\rho\boldsymbol{e}_1}{|T_\rho\boldsymbol{e}_1|} - \sqrt{\frac{\lambda_2}{\lambda_1+\lambda_2}}\frac{T_\rho\boldsymbol{e}_2}{|T_\rho\boldsymbol{e}_2|}, \quad \text{(C6)}$$

$$\boldsymbol{b}_{1,2} = \boldsymbol{e}_{1,2}. \quad \text{(C7)}$$

(2) $\rho\in\mathcal{H}_{\mathrm{Bob}}\otimes\mathcal{H}_{\mathrm{Alice}}$

$$\boldsymbol{a}_0 = \boldsymbol{e}_1, \quad \text{(C8)}$$

$$\boldsymbol{a}_1 = \sqrt{\frac{\lambda_1}{\lambda_1+\lambda_2}}\boldsymbol{e}_1 + \sqrt{\frac{\lambda_2}{\lambda_1+\lambda_2}}\boldsymbol{e}_2, \quad \text{(C9)}$$

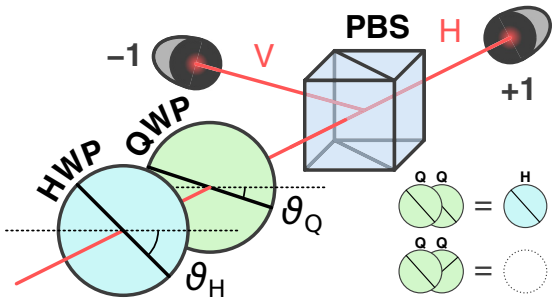

FIG. 5. Polarization projection measurement using two wave plates (half-wave—HWP, and quarter-wave—QWP) and a polarizing beam splitter (PBS). Let us assign the outcome $+1$ to a detection in the horizontal output and -1 to the vertical output. The angles ϑ_H, ϑ_Q are between the respective wave plate axes and the horizontal plane. The HWP and QWP angles exhibit periodicity: $\vartheta_H \Leftrightarrow \vartheta_H + k\pi/2$, $\vartheta_Q \Leftrightarrow \vartheta_Q + l\pi; k, l \in \mathbb{Z}$.

$$\boldsymbol{a}_2 = \sqrt{\frac{\lambda_1}{\lambda_1+\lambda_2}}\boldsymbol{e}_1 - \sqrt{\frac{\lambda_2}{\lambda_1+\lambda_2}}\boldsymbol{e}_2, \tag{C10}$$

$$\boldsymbol{b}_{1,2} = \frac{T_\rho \boldsymbol{e}_{1,2}}{|T_\rho \boldsymbol{e}_{1,2}|}. \tag{C11}$$

The optimal quantities are given by the two largest eigenvalues,

$$S = 2\sqrt{\lambda_1+\lambda_2}, \tag{C12}$$

$$Q = \frac{1-\sqrt{\lambda_1}}{2}. \tag{C13}$$

Upon obtaining a basis vector $\boldsymbol{x} = \{x_1, x_2, x_3\}$, an experimentalist needs to know how to set up the polarization measurement. Let us suppose that our basis is chosen in a horizontal-vertical polarization so that $\sigma_1 = \sigma_x, \sigma_2 = \sigma_y, \sigma_3 = \sigma_z = |\mathrm{H}\rangle\langle\mathrm{H}| - |\mathrm{V}\rangle\langle\mathrm{V}|$. Also, let us assume the projection setup shown in Fig. 5.

Then, the wave plate axes rotations with respect to the horizontal plane can be obtained by

$$\vartheta_Q = \frac{1}{2}\arcsin(x_2), \tag{C14}$$

$$\vartheta_H = \frac{1}{4}\Big[\arctan\Big(\frac{x_1}{x_3}\Big) + \arcsin(x_2)\Big]. \tag{C15}$$

There is an important caveat about the quarter-wave plates of Alice and Bob. While the choice of slow or fast axis is arbitrary for all wave plates, the QWP axes need to be oriented consistently in both modes. That is, for $\vartheta_Q = 0$, both Alice's and Bob's QWPs need to have either both their fast axes horizontal, or both their slow axes horizontal. Since it is easy to calibrate the directions of all axes up to $\pi/2$ using linear polarizers, the two QWPs only need to be matched together. This can be achieved by aligning any of their axes and rotating both QWPs simultaneously. If their slow and fast axes are parallel, the overall transformation corresponds to a HWP. If the axes are perpendicular, the wave plates cancel each other out and no polarization modulation occurs (Fig. 5).

APPENDIX D: ALICE'S AND BOB'S OPTIMAL CHOICE OF BASES

Equations (C4) to (C11) are the result of a conjunction of two conditions—minimizing Q and maximizing S. Here we present the respective derivations.

1. Optimal Quantum Bit Error Rate

The optimal QBER is obtained by the same principle as described in Ref. [37]. The definition follows from (5), assuming projection measurements in bases Q_1, Q_2, and can be written as

$$Q = \mathrm{Tr}\big[\rho(\hat{\Pi}^{(+)}_{\mathrm{Q}_1} \otimes \hat{\Pi}^{(-)}_{\mathrm{Q}_2})\big] + \mathrm{Tr}\big[\rho(\hat{\Pi}^{(-)}_{\mathrm{Q}_1} \otimes \hat{\Pi}^{(+)}_{\mathrm{Q}_2})\big], \tag{D1}$$

where $\hat{\Pi}^{(\pm)}_{\mathrm{Q}_1}$ and $\hat{\Pi}^{(\pm)}_{\mathrm{Q}_2}$ are the projector operators onto the $(+)$ or $(-)$ states in the respective bases. Using the real-vector formalism, the bases are given by $\boldsymbol{q}_1, \boldsymbol{q}_2$, and the QBER operator is

$$\mathcal{Q} = \tfrac{1}{2}[\mathbb{1}\otimes\mathbb{1} - (\boldsymbol{q}_1\cdot\boldsymbol{\sigma})\otimes(\boldsymbol{q}_2\cdot\boldsymbol{\sigma})], \tag{D2}$$

$$Q = \mathrm{Tr}[\mathcal{Q}\rho]. \tag{D3}$$

If we rewrite the QBER as

$$Q = \tfrac{1}{2}\big(1 - \boldsymbol{q}_1^{\mathrm{T}}\cdot T_\rho \cdot \boldsymbol{q}_2\big), \tag{D4}$$

the optimum requires maximizing the second term. The inner product of $\boldsymbol{q}_1$ and $T_\rho\boldsymbol{q}_2$ is clearly maximized by choosing the unit vector $\boldsymbol{q}_1$ to be in the same direction, $\boldsymbol{q}_1 = T_\rho\boldsymbol{q}_2/|T_\rho\boldsymbol{q}_2|$. If follows that

$$Q = \tfrac{1}{2}\big(1 - \sqrt{\boldsymbol{q}_2^{\mathrm{T}}U_\rho\boldsymbol{q}_2}\big). \tag{D5}$$

By considering $\boldsymbol{q}_2$ in the eigenbasis of U_ρ, the maximum of the product can be easily found to be the largest eigenvalue of U_ρ, that is λ_1, and so $\boldsymbol{q}_2 = \boldsymbol{e}_1$. If there are multiple maximum eigenvalues, such as for the Bell states, the vector $\boldsymbol{q}_2$ may belong to any subspace spanned by the corresponding eigenvectors. This result corresponds to the Eqs. (C4), (C7), (C8), and (C11).

2. Optimal Clauser-Horne-Shimony-Holt Violation

The derivation follows the U_ρ-matrix approach outlined in Ref. [37], and was explicitly calculated in Ref. [48]. Let us follow the procedure in Ref. [37] by adopting the notation of $\boldsymbol{a}$ and $\boldsymbol{b}$ corresponding to $\rho \in \mathcal{H}_{\mathrm{Alice}} \otimes \mathcal{H}_{\mathrm{Bob}}$. Following the definition of the CHSH polynomial given for the protocol in Ref. [7], we obtain

$$S = \boldsymbol{a}_1^{\mathrm{T}}T_\rho(\boldsymbol{b}_1 + \boldsymbol{b}_2) + \boldsymbol{a}_2^{\mathrm{T}}T_\rho(\boldsymbol{b}_1 - \boldsymbol{b}_2). \tag{D6}$$

We introduce two orthogonal unit vectors

$$\boldsymbol{c}_1 = \frac{\boldsymbol{b}_1 + \boldsymbol{b}_2}{2\cos\theta}, \tag{D7}$$

$$\boldsymbol{c}_2 = \frac{\boldsymbol{b}_1 - \boldsymbol{b}_2}{2\sin\theta}, \tag{D8}$$

where $\theta \in (0, \pi/2)$ is half the angle between $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$. This is just a different parametrization of $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$, as any pair of such vectors can be represented by a unique combination

of $\boldsymbol{c}_1$, $\boldsymbol{c}_2$, and the angle θ; and vice versa. This allows us to rewrite the Bell factor as a sum of two scalar products,

$$S = [\boldsymbol{a}_1 \cdot (T_\rho \boldsymbol{c}_1)]2\cos\theta + [\boldsymbol{a}_2 \cdot (T_\rho \boldsymbol{c}_2)]2\sin\theta. \tag{D9}$$

Trivially, the maximum of each scalar product is reached for the unit vectors $\boldsymbol{a}_{1,2}$ that have the same direction as the right side,

$$\boldsymbol{a}_{1,2} = \frac{T_\rho \boldsymbol{c}_{1,2}}{|T_\rho \boldsymbol{c}_{1,2}|}. \tag{D10}$$

This gives us

$$S = |T_\rho \boldsymbol{c}_1|2\cos\theta + |T_\rho \boldsymbol{c}_2|2\sin\theta. \tag{D11}$$

Now we maximize with respect to θ by solving $\partial S/\partial\theta = 0$, yielding

$$S = 2\sqrt{|T_\rho \boldsymbol{c}_1|^2 + |T_\rho \boldsymbol{c}_2|^2}, \tag{D12}$$

$$\tan\theta = \frac{|T_\rho \boldsymbol{c}_2|}{|T_\rho \boldsymbol{c}_1|}. \tag{D13}$$

By denoting $U_\rho = T_\rho^{\mathrm{T}} T_\rho$, we can rewrite the norms and scalar products as

$$S = 2\sqrt{\boldsymbol{c}_1^{\mathrm{T}} U_\rho \boldsymbol{c}_1 + \boldsymbol{c}_2^{\mathrm{T}} U_\rho \boldsymbol{c}_2}. \tag{D14}$$

U_ρ is a symmetrical non-negative diagonalizable matrix. The property of these matrices is that the sum of the products of two orthogonal unit vectors—such as in (D14)—is constant for all such vectors within a single plane. This is also related to invariance of the matrix trace under rotation around a coordinate axis.

The sum in (D14) can be maximized either using Lagrange multipliers and $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ taken in the eigenbasis of U_ρ, or using standard differential maximization of a rotated matrix U_ρ in spherical coordinates and vectors $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ rotating in the x-y plane.

The result is that maximal CHSH violation is reached for all orthogonal pairs of $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ in the plane corresponding to two greatest eigennumbers of U_ρ. If we maintain the notation of $\boldsymbol{e}_i$ being the eigenvectors of U_ρ with the corresponding eigennumbers $\lambda_1 \geqslant \lambda_2 \geqslant \lambda_3$, then the solution is given by

$$\boldsymbol{c}_1 = \boldsymbol{e}_1 \cos\varphi + \boldsymbol{e}_2 \sin\varphi, \tag{D15}$$

$$\boldsymbol{c}_2 = \boldsymbol{e}_1 \sin\varphi - \boldsymbol{e}_2 \cos\varphi, \tag{D16}$$

where φ is an arbitrary angle [48]. The bases $\boldsymbol{a}_1, \boldsymbol{a}_2$ and $\boldsymbol{b}_1, \boldsymbol{b}_2$ are then obtained using Eqs. (D7), (D8), (D10), and (D13).

The optimal bases have at least one degree of freedom (φ; more degrees if any two eigennumbers λ_i are equal). Alice's and Bob's projections belong to two respective planes on the Bloch sphere that are generally different. $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ belong to the plane spanned by $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ due to the above-mentioned rotational symmetry of $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ under the free parameter φ. The T_ρ image of this plane contains all vectors $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$ owing to the property of linear transformations mapping planes unto planes.

3. Conjunction for $\rho \in \mathcal{H}_{\mathrm{Alice}} \otimes \mathcal{H}_{\mathrm{Bob}}$

As we showed above, the optimal QBER requires

$$\boldsymbol{a}_0 = \boldsymbol{q}_1 = T_\rho \boldsymbol{e}_1 / |T_\rho \boldsymbol{e}_1|, \tag{D17}$$

$$\boldsymbol{b}_1 = \boldsymbol{q}_2 = \boldsymbol{e}_1. \tag{D18}$$

From Eqs. (D7), (D8), (D15), and (D16), we obtain

$$\boldsymbol{b}_1 = \cos(\varphi - \theta)\boldsymbol{e}_1 + \sin(\varphi - \theta)\boldsymbol{e}_2, \tag{D19}$$

$$\boldsymbol{b}_2 = \cos(\varphi + \theta)\boldsymbol{e}_1 + \sin(\varphi + \theta)\boldsymbol{e}_2. \tag{D20}$$

Equation (D18) introduces a binding condition $\varphi = \theta$. To find θ, we take (D13) and remember that

$$|T_\rho \boldsymbol{c}_{1,2}| = \sqrt{\boldsymbol{c}_{1,2}^{\mathrm{T}} U_\rho \boldsymbol{c}_{1,2}}. \tag{D21}$$

When substituting (D15) and (D16), we arrive at

$$\tan\theta = \sqrt{\frac{\lambda_1 \tan\theta + \lambda_2}{\lambda_1 + \lambda_2 \tan\theta}}. \tag{D22}$$

Since $\theta \in (0, \pi/2)$, the result leads to a quadratic equation with a single solution

$$\varphi = \theta = \frac{\pi}{4}. \tag{D23}$$

Substituting into (D19) and (D20), we obtain (C7). Equation (D10) yields

$$\boldsymbol{a}_{1,2} = \frac{T_\rho(\boldsymbol{e}_1 \pm \boldsymbol{e}_2)}{\sqrt{\lambda_1 + \lambda_2}}, \tag{D24}$$

which, after normalizing the vectors, leads to (C5) and (C6), completing the optimal QKD bases.

4. Conjunction for $\rho \in \mathcal{H}_{\mathrm{Bob}} \otimes \mathcal{H}_{\mathrm{Alice}}$

To maintain mode consistency with the derivation of optimal CHSH and with the polynomial (D6), we assign vectors $\widetilde{\boldsymbol{a}}$ to Bob and $\widetilde{\boldsymbol{b}}$ to Alice, with the tilde serving as a reminder to swap the notation eventually.

The QBER optimization reads

$$\widetilde{\boldsymbol{a}}_1 = \boldsymbol{q}_1 = T_\rho \boldsymbol{e}_1 / |T_\rho \boldsymbol{e}_1|, \tag{D25}$$

$$\widetilde{\boldsymbol{b}}_0 = \boldsymbol{q}_2 = \boldsymbol{e}_1. \tag{D26}$$

Here, Bob's first basis $\widetilde{\boldsymbol{a}}_1$ introduces a binding condition, which, after looking at (D10), (D15), and (D16), simply gives

$$\boldsymbol{c}_1 = \boldsymbol{e}_1, \tag{D27}$$

$$\boldsymbol{c}_2 = \boldsymbol{e}_2, \tag{D28}$$

$$\widetilde{\boldsymbol{a}}_2 = T_\rho \boldsymbol{e}_2 / |T_\rho \boldsymbol{e}_2|. \tag{D29}$$

Like before, we substitute the vectors $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ into (D13), so we can have both angles solved,

$$\varphi = 0, \tag{D30}$$

$$\theta = \arctan\sqrt{\lambda_2/\lambda_1}. \tag{D31}$$

For $\theta \in (0, \pi/2)$, we know that

$$\cos\theta = \frac{1}{\sqrt{1 + \tan^2\theta}}, \tag{D32}$$

$$\sin\theta = \frac{\tan\theta}{\sqrt{1 + \tan^2\theta}}. \tag{D33}$$

TABLE I. A list of r_C, S, Q, r_{DW}, and R_{key} values for the respective coincidence window lengths τ used during the experimental study of the dependence of R_{key} on r_C.

τ [ns]	r_C	S	Q	r_{DW}	R_{key}
1.0	$8.66(3)\times10^{-6}$	2.815(5)	0.0013(5)	0.94(2)	$8.2(2)\times10^{-6}$
1.4	$1.330(5)\times10^{-5}$	2.814(5)	0.0015(6)	0.94(2)	$1.25(2)\times10^{-5}$
2.1	$1.992(7)\times10^{-5}$	2.814(5)	0.0013(6)	0.94(2)	$1.88(3)\times10^{-5}$
3.0	$2.96(1)\times10^{-5}$	2.814(4)	0.0016(6)	0.94(2)	$2.77(5)\times10^{-5}$
4.3	$4.35(1)\times10^{-5}$	2.812(5)	0.0017(6)	0.93(2)	$4.04(7)\times10^{-5}$
6.2	$6.35(2)\times10^{-5}$	2.808(5)	0.0022(8)	0.92(2)	$5.8(1)\times10^{-5}$
8.9	$9.23(3)\times10^{-5}$	2.807(5)	0.0023(9)	0.91(2)	$8.4(2)\times10^{-5}$
12.7	$1.341(4)\times10^{-4}$	2.802(6)	0.003(1)	0.90(2)	$1.20(3)\times10^{-4}$
18.3	$1.946(7)\times10^{-4}$	2.790(6)	0.004(1)	0.86(2)	$1.68(5)\times10^{-4}$
26.4	$2.824(9)\times10^{-4}$	2.779(7)	0.004(2)	0.83(2)	$2.35(7)\times10^{-4}$
37.9	$4.10(1)\times10^{-4}$	2.763(7)	0.007(2)	0.78(2)	$3.2(1)\times10^{-4}$
54.6	$5.97(2)\times10^{-4}$	2.743(7)	0.009(2)	0.73(2)	$4.4(1)\times10^{-4}$
78.5	$8.72(3)\times10^{-4}$	2.716(8)	0.012(3)	0.66(3)	$5.8(2)\times10^{-4}$
112.9	$1.279(4)\times10^{-3}$	2.67(1)	0.020(4)	0.54(4)	$6.9(5)\times10^{-4}$
162.4	$1.888(6)\times10^{-3}$	2.60(1)	0.033(4)	0.37(3)	$6.9(6)\times10^{-4}$
233.6	$2.814(8)\times10^{-3}$	2.49(1)	0.053(4)	0.15(3)	$4.2(8)\times10^{-4}$
336.0	$4.25(1)\times10^{-3}$	2.35(1)	0.080(4)	0	0
483.3	$6.53(2)\times10^{-3}$	2.18(1)	0.109(4)	0	0
695.2	$1.022(3)\times10^{-2}$	1.98(1)	0.146(3)	0	0
1000.0	$1.641(4)\times10^{-2}$	1.73(1)	0.191(3)	0	0

Substituting (D31)–(D33) into (D7) and (D8), we straightforwardly solve for

$$\widetilde{\boldsymbol{b}}_{1,2} = \sqrt{\frac{\lambda_1}{\lambda_1+\lambda_2}}\boldsymbol{e}_1 \pm \sqrt{\frac{\lambda_2}{\lambda_1+\lambda_2}}\boldsymbol{e}_2. \tag{D34}$$

Now, by swapping the notation, $\widetilde{\boldsymbol{a}} \to \boldsymbol{b}$, $\widetilde{\boldsymbol{b}} \to \boldsymbol{a}$, we have derived the results (C8) to (C11).

APPENDIX E: EXPERIMENTAL DATA

In the experiment, we used varying coincidence window lengths to study the effect of multiphoton components. In Table I, we list the values of S, Q, r_{DW} and R_{key} calculated from the tomographic reconstructions, for different values of the coincidence window length τ. Experimentally obtained values of r_C are also included.

[1] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Ultrabright source of polarization-entangled photons, Phys. Rev. A **60**, R773 (1999).

[2] H. Takesue and K. Shimizu, Effects of multiple pairs on visibility measurements of entangled photons generated by spontaneous parametric processes, Opt. Commun. **283**, 276 (2010).

[3] M. Takeoka, R.-B. Jin, and M. Sasaki, Full analysis of multi-photon pair effects in spontaneous parametric down conversion based photonic quantum information processing, New J. Phys. **17**, 043030 (2015).

[4] T. Huber, A. Predojević, M. Khoshnegar, D. Dalacu, P. J. Poole, H. Majedi, and G. Weihs, Polarization entangled photons from quantum dots embedded in nanowires, Nano Lett. **14**, 7107 (2014).

[5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, J. Cryptol. **5**, 3 (1992).

[6] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. London, Ser. A **461**, 207 (2005).

[7] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, New J. Phys. **11**, 045021 (2009).

[8] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Nature (London) **526**, 682 (2015).

[9] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, Strong Loophole-Free Test Of Local Realism, Phys. Rev. Lett. **115**, 250402 (2015).

[10] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons, Phys. Rev. Lett. **115**, 250401 (2015).

[11] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Comput. Sci. **560**, 7 (2014).

[12] M. Lasota, R. Filip, and V. C. Usenko, Sufficiency of quantum non-Gaussianity for discrete-variable quantum key distribution over noisy channels, Phys. Rev. A **96**, 012301 (2017).

[13] A. K. Ekert, Quantum Cryptography Based On Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[14] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (2007).

[15] U. Vazirani and T. Vidick, Fully Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **113**, 140501 (2014).

[16] 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).

[17] 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).

[18] A. Ling, M. P. Peloso, I. Marcikic, V. Scarani, A. Lamas-Linares, and C. Kurtsiefer, Experimental quantum key distribution based on a Bell test, Phys. Rev. A **78**, 020301(R) (2008).

[19] H. Wang, H. Hu, T.-H. Chung, J. Qin, X. Yang, J.-P. Li, R.-Z. Liu, H.-S. Zhong, Y.-M. He, X. Ding, Y.-H. Deng, Q. Dai, Y.-H. Huo, S. Höfling, C.-Y. Lu, and J.-W. Pan, On-Demand Semiconductor Source of Entangled Photons Which Simultaneously Has High Fidelity, Efficiency, and Indistinguishability, Phys. Rev. Lett. **122**, 113602 (2019).

[20] S. Zeiger, F. Laudenbach, B. Schrenk, M. Hentschel, and H. Hübel, A ps-pulse laser for ultrafast entanglement generation at 42.66 GHz repetition rate, in *2019 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC), Munich, Germany* (Optical Society of America, 2019), pp. 1–1.

[21] I. Straka, A. Predojević, T. Huber, L. Lachman, L. Butschek, M. Miková, M. Mičuda, G. S. Solomon, G. Weihs, M. Ježek, and R. Filip, Quantum Non-Gaussian Depth of Single-Photon States, Phys. Rev. Lett. **113**, 223603 (2014).

[22] A. Predojević, M. Ježek, T. Huber, H. Jayakumar, T. Kauten, G. S. Solomon, R. Filip, and G. Weihs, Efficiency vs multiphoton contribution test for quantum dots, Opt. Express **22**, 4789 (2014).

[23] N. Somaschi, V. Giesz, L. D. Santis, J. C. Loredo, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Antón, J. Demory, C. Gómez, I. Sagnes, N. D. Lanzillotti-Kimura, A. Lemaître, A. Auffeves, A. G. White, L. Lanco, and P. Senellart, Near-optimal single-photon sources in the solid state, Nat. Photonics **10**, 340 (2016).

[24] J. L. O'Brien, Optical quantum computing, Science **318**, 1567 (2007).

[25] M. Varnava, D. E. Browne, and T. Rudolph, How Good Must Single Photon Sources and Detectors Be for Efficient Linear Optical Quantum Computation? Phys. Rev. Lett. **100**, 060502 (2008).

[26] T. Jennewein, M. Barbieri, and A. G. White, Single-photon device requirements for operating linear optics quantum computing outside the post-selection basis, J. Mod. Opt. **58**, 276 (2011).

[27] X. Ma, C.-H. F. Fung, and H.-K. Lo, Quantum key distribution with entangled photon sources, Phys. Rev. A **76**, 012307 (2007).

[28] C. Holloway, J. A. Doucette, C. Erven, J.-P. Bourgoin, and T. Jennewein, Optimal pair-generation rate for entanglement-based quantum key distribution, Phys. Rev. A **87**, 022342 (2013).

[29] M. Ho, P. Sekatski, E. Y.-Z. Tan, R. Renner, J.-D. Bancal, and N. Sangouard, Noisy Preprocessing Facilitates a Photonic Realization of Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **124**, 230502 (2020).

[30] H. Jayakumar, A. Predojević, T. Huber, T. Kauten, G. S. Solomon, and G. Weihs, Deterministic Photon Pairs and Coherent Optical Control of a Single Quantum Dot, Phys. Rev. Lett. **110**, 135505 (2013).

[31] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett. **23**, 880 (1969).

[32] S. Camalet, Quantifying nonlocality as a resource for device-independent quantum key distribution, Phys. Rev. A **102**, 012617 (2020).

[33] E. Y.-Z. Tan, R. Schwonnek, K. T. Goh, I. W. Primaatmaja, and C. C.-W. Lim, Computing secure key rates for quantum key distribution with untrusted devices, arXiv:1908.11372.

[34] E. Kaur, M. M. Wilde, and A. Winter, Fundamental limits on key rates in device-independent quantum key distribution, New J. Phys. **22**, 023039 (2020).

[35] A. S. Holevo, Bounds for the quantity of information transmitted by a quantum communication channel, Probl. Inform. Trans. **9**, 177 (1973).

[36] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[37] R. Horodecki, P. Horodecki, and M. Horodecki, Violating Bell inequality by mixed spin-$\frac{1}{2}$ states: Necessary and sufficient condition, Phys. Lett. A **200**, 340 (1995).

[38] A. B. Klimov, J. L. Romero, and S. Wallentowitz, Quantum-state tomography for optical polarization with arbitrary photon numbers, Phys. Rev. A **89**, 020101(R) (2014).

[39] C. R. Müller, L. S. Madsen, A. B. Klimov, L. L. Sánchez-Soto, G. Leuchs, C. Marquardt, and U. L. Andersen, Parsing polarization squeezing into Fock layers, Phys. Rev. A **93**, 033816 (2016).

[40] Z. Hradil, Quantum-state estimation, Phys. Rev. A **55**, R1561 (1997).

[41] M. Ježek, J. Fiurášek, and Z. Hradil, Quantum inference of states and processes, Phys. Rev. A **68**, 012305 (2003).

[42] F. B. Basset, M. B. Rota, C. Schimpf, D. Tedeschi, K. D. Zeuner, S. F. C. da Silva, M. Reindl, V. Zwiller, K. D. Jöns, A. Rastelli, and R. Trotta, Entanglement Swapping with Photons Generated on Demand by a Quantum Dot, Phys. Rev. Lett. **123**, 160501 (2019).

[43] E. V. Denning, J. Iles-Smith, N. Gregersen, and J. Mork, Phonon effects in quantum dot single-photon sources, Opt. Mater. Express **10**, 222 (2019).

[44] A. D. Osterkryger, J. Claudon, J.-M. Gérard, and N. Gregersen, Photonic 'hourglass' design for efficient quantum light emission, Opt. Lett. **44**, 2617 (2019).

[45] T. Huber, L. Ostermann, M. Prilmüller, G. S. Solomon, H. Ritsch, G. Weihs, and A. Predojević, Coherence and degree of

time-bin entanglement from quantum dots, Phys. Rev. B **93**, 201301(R) (2016).

[46] B. Korzh, Q.-Y. Zhao, J. P. Allmaras, S. Frasca, T. M. Autry, E. A. Bersin, A. D. Beyer, R. M. Briggs, B. Bumble, M. Colangelo, G. M. Crouch, A. E. Dane, T. Gerrits, A. E. Lita, F. Marsili, G. Moody, C. Peña, E. Ramirez, J. D. Rezac, N. Sinclair, M. J. Stevens, A. E. Velasco, V. B. Verma, E. E. Wollman, S. Xie, D. Zhu, P. D. Hale, M. Spiropulu, K. L. Silverman, R. P. Mirin, S. W. Nam, A. G. Kozorezov, M. D. Shaw, and K. K. Berggren, Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector, Nat. Photonics **14**, 250 (2020).

[47] F. Basso Basset, M. Valeri, E. Roccia, V. Muredda, D. Poderini, J. Neuwirth, N. Spagnolo, M. B. Rota, G. Carvacho, F. Sciarrino, and R. Trotta, Quantum key distribution with entangled photons generated on-demand by a quantum dot, arXiv:2007.12727.

[48] A. G. Kofman, Optimal conditions for Bell-inequality violation in the presence of decoherence and errors, Quantum Inf. Process. **11**, 269 (2012).