

Long-range photonic device-independent quantum key distribution using spontaneous parametric down-conversion sources and linear optics

Morteza Moradi,¹ Maryam Afsary¹, Piotr Mironowicz^{2,3}, Enky Oudot,^{4,5} and Magdalena Stobińska-Moretto^{6,*}

¹*Institute of Informatics, Faculty of Mathematics, Informatics and Mechanics, University of Warsaw, Banacha 2c, 02-097 Warsaw, Poland*

²*Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, 02-668 Warsaw, Poland*

³*Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, Narutowicza 11/12, 80-233 Gdańsk, Poland*

⁴*ICFO—Institut de Ciències Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain*

⁵*LIP6, CNRS, Sorbonne Université, 4 place Jussieu, F-75005 Paris, France*

⁶*Center for Hybrid Quantum-Classical Information Technologies “QLAB”, University of Warsaw, Pasteura 5, 02-093 Warsaw, Poland*



(Received 30 August 2025; accepted 6 May 2026; published 12 June 2026)

We address the question of the implementation of long-distance device-independent quantum key distribution (DI QKD) by proposing two experimentally viable schemes. Those schemes use only spontaneous parametric down-conversion sources and linear optics. They achieve favorable key rate scaling proportional to the square root of channel transmittance η , matching the twin-field protocol advantage. We demonstrate positive asymptotic key rates at detector efficiencies as low as 80%, bringing DI QKD within the reach of current superconducting detector technology. Our security analysis employs the entropy accumulation theorem to establish rigorous finite-size bounds, achieving finite-key rates at a detector efficiency of 90%. This work represents a critical milestone toward device-independent security in quantum communication networks, providing experimentalists with practical implementation pathways while maintaining the strongest possible security guarantees against quantum adversaries.

DOI: [10.1103/ycd9-nc6q](https://doi.org/10.1103/ycd9-nc6q)

I. INTRODUCTION

Quantum key distribution (QKD) promises information-theoretic security for communications, leveraging quantum mechanics to detect eavesdropping attempts. Among various protocols, device-independent (DI) schemes offer the highest level of security by eliminating the need to trust the devices [1,2]. This remarkable property addresses a critical vulnerability: In practice, imperfect or compromised devices can leak information, as demonstrated by successful attacks on QKD systems [3–6].

The security of DI QKD is based on a profound insight. The violation of Bell inequality certifies the presence of quantum nonlocality that no classical system can reproduce. By monitoring this violation, users can bound the information accessible to any eavesdropper. The security proof is based solely on observed measurement statistics.

Despite its elegance, implementing DI QKD over long distances faces the challenge of closing the detection loophole while maintaining practical key generation rates. This loophole arises when measurement inefficiencies allow local hidden-variable models to reproduce the observed correlations. For photonic implementations, detector efficiencies exceeding 82.8% are required for Bell tests with maximally

entangled states, although this threshold can be lowered to 66.7% for other states and specific measurements [7,8]. Moreover, in most QKD protocols, key rates decay exponentially with distance due to channel losses, limiting practical distance to 100–150 km in standard fibers [9].

Recent experiments demonstrated DI QKD using matter qubits with near-perfect detection efficiency [10,11]. Although they validated the principle, they underscored the need for fully photonic solutions compatible with optical fiber network infrastructure. Initial steps have been reported in Ref. [12], yet achieving long-distance implementation remains an open challenge. In particular, the quantum repeater approach faces fundamental constraints in DI scenarios [13].

A promising idea to overcome distance limitations in QKD is the twin-field (TF) configuration [14]. This architecture enables key rates that scale with the square root of channel transmittance, a significant improvement over the linear scaling of conventional QKD. By combining the security of DI QKD with the scaling of TF protocols, DI-TF QKD could enable secure communication over long distances without trusting any network nodes. Such a fully photonic DI-TF QKD scheme has recently been proposed and analyzed with respect to security in Ref. [15], but the setup required quantum dot sources and a nonlinear measurement scheme that poses experimental challenges.

In this work, we study two DI-TF QKD protocols based on heralded entanglement distribution using spontaneous parametric down-conversion (SPDC) sources, linear optics, and on/off single-photon detectors. The first scheme, demonstrated experimentally in Ref. [16] and further analyzed for Bell experiments in Ref. [17], produces a maximally entangled single-photon state $|\Psi_{\text{out}}^{(\text{ph})}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm i|10\rangle)$. We

*Contact author: magdalena.stobinska@gmail.com

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.

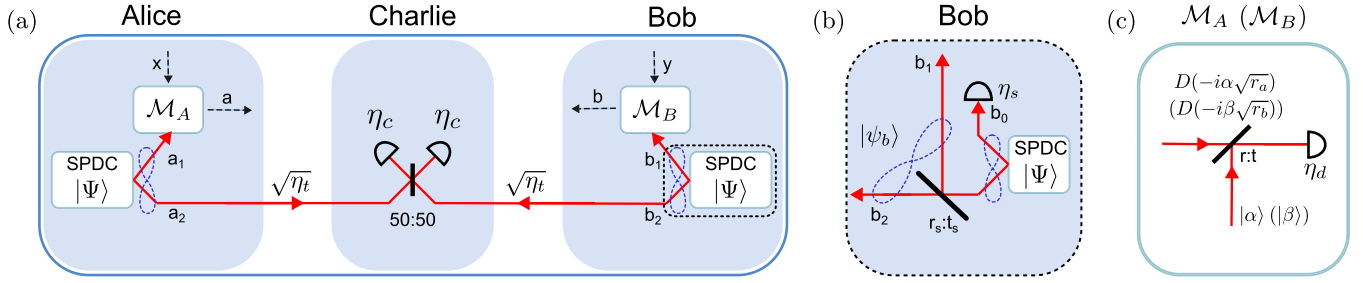


FIG. 1. Long-range DI-TF QKD based on heralded entanglement distribution. (a) In the one-photon protocol, Alice and Bob use SPDC sources pumped by pulsed lasers to generate local bipartite multiphoton entanglement—two-mode squeezed-vacuum states. The idler modes a_2 and b_2 travel through lossy channels with transmittance $\sqrt{\eta_t}$ to reach Charlie's central station, which comprises a symmetric beam splitter and two detectors with efficiency η_c . The events where exactly one of the two detectors registers a photon herald the state in Eq. (1). (b) In the two-photon protocol, Bob employs a single-photon source obtained by heralding one output from an SPDC crystal at a detector of efficiency η_s , with the other output routed through a beam splitter with reflectivity-to-transmissivity ratio $r_s:t_s$, effectively generating local single-photon entanglement $|\psi_b\rangle$. (c) The heralded state, Eq. (1) or (2), enters Alice's and Bob's measurement systems $\mathcal{M}_A$ and $\mathcal{M}_B$. Each measurement comprises a displacement operation, implemented by interfering the signal a_1 (b_1) with a coherent state $|\alpha\rangle$ ($|\beta\rangle$) on a beam splitter with transmissivity $t_{a,b} \approx 1$, followed by a detector with efficiency η_d . All detectors used discriminate only between “photon” and “no-photon” cases (on/off detection).

provide a rigorous security proof for a DI QKD protocol using this state; however, the measurement scheme is suboptimal for $|\Psi_{\text{out}}^{(1\text{ph})}\rangle$, resulting in a high detection-efficiency threshold. We refer to it as the one-photon protocol.

The second scheme constitutes our main contribution and significantly relaxes experimental requirements: For the first time, we achieve threshold efficiencies compatible with state-of-the-art experiments together with a rigorous security proof. The key ingredient is to herald states of the form $|\Psi_{\text{out}}^{(2\text{ph})}\rangle = |00\rangle + \epsilon|11\rangle$; we call this the two-photon protocol. The state $|\Psi_{\text{out}}^{(2\text{ph})}\rangle$ offers two advantages for DI QKD. First, key generation uses Z-basis measurements with on/off detectors, yielding perfectly correlated outcomes; losses only weakly affect the error rate, as most events correspond to the vacuum component $|00\rangle$. Second, it allows the violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality down to the 66% loss threshold. While unbalanced states are known to optimize key rates at a given efficiency [18], the CHSH inequality is suboptimal for DI QKD with such states. We therefore develop numerical methods for rigorous security proofs against general quantum attacks, using the entropy accumulation theorem (EAT) [19,20] with Bell inequalities tailored to $|\Psi_{\text{out}}^{(2\text{ph})}\rangle$.

II. THE PROTOCOL

The setup we consider is depicted in Fig. 1. Alice and Bob each generate multiphoton entangled states at their respective locations. In each round, they randomly choose one of three measurement settings: two for the nonlocality test and one for key generation. Charlie heralds long-range entanglement and communicates via a classical channel that rounds to keep. The basic ingredients are two identical two-mode squeezed vacuum (TMSV) sources, obtained by pumping two SPDC crystals. These sources generate the state $|\Psi\rangle = \sum_n \sqrt{\lambda_n} |n, n\rangle_{1,2}$, with photon-number correlations across modes 1 and 2, correlated in photon number across two modes 1 and 2, where $\lambda_n = \tanh^{2n}(g) / \cosh^2(g)$

quantifies the probability of n -photon emissions in each mode and g is the parametric gain. Since vacuum and single-photon events dominate ($\lambda_0 \gg \lambda_1 \gg \lambda_2 \dots$), for clarity we approximate this state as $|\Psi\rangle \approx \frac{1}{\sqrt{2}}(\sqrt{\lambda_0}|00\rangle + \sqrt{\lambda_1}|11\rangle)$; however, all computations and plots in this article include the full multiphoton contributions as described in the Appendix A.

A. The one-photon protocol

In the scenario depicted in Fig. 1(a), Alice and Bob send one TMSV mode each to Charlie's central station, equidistant from both. Charlie interferes the incoming modes at a symmetric beam splitter and heralds only when exactly one of the two detectors clicks, projecting the distributed state onto high-fidelity entanglement [16,17]:

$$|\Psi_{\text{out}}^{(1\text{ph})}\rangle = \frac{1}{\sqrt{2}}(|0, 1\rangle_{a_1, b_1} \pm i|1, 0\rangle_{a_1, b_1}). \quad (1)$$

With Charlie's detector efficiency η_c , photon-number statistics $\lambda^{(a)}(\lambda^{(b)})$ for Alice (Bob), the heralding probability is $P_h^{(1\text{ph})} = (\lambda_0^{(a)}\lambda_1^{(b)} + \lambda_0^{(b)}\lambda_1^{(a)})\eta_c\sqrt{\eta_t} \approx O(\sqrt{\eta_t})$.

This protocol achieves breakthrough scaling. At distance L , channel transmittance is $\eta_t = 10^{-\alpha_{\text{att}}L/10}$, with attenuation coefficient $\alpha_{\text{att}} = 0.2 \text{ km}^{-1}$. Since the photons travel half distance to Charlie, the losses scale as $\sqrt{\eta_t}$, versus linear decay (η_t) in conventional QKD. This square-root improvement allows previously inaccessible distances.

In practice, Charlie heralds a mixed state ρ_{out} rather than the pure state [Eq. (1)], but $|\Psi_{\text{out}}^{(1\text{ph})}\rangle\langle\Psi_{\text{out}}^{(1\text{ph})}|$ remains dominant. This robustness proves critical for implementations. In our further analysis, we assume perfect heralding detectors at Charlie's ($\eta_c = 1$), since their inefficiency can be treated as an additional channel loss, and it merely reduces protocol success rate without compromising security. In particular, taking $l_c = -100 \log_{10}$, one may assume perfect detectors at Charlie's and incorporate their inefficiency by effectively increasing the channel length from L to $L + l_c$.

B. The two-photon protocol

In this second approach [Fig. 1(b)], Alice's setup remains unchanged while Bob uses a single-photon source, implemented with a heralded SPDC [21] using a detector of efficiency η_s . Bob routes the photon through a beam splitter with transmissivity t_s , creating a local entangled state $|\psi_b\rangle = \sqrt{t_s}|0, 1\rangle_{b_1, b_2} + e^{i\phi} \sqrt{1-t_s}|1, 0\rangle_{b_1, b_2}$. A single click at Charlie's station heralds an entangled state

$$|\Psi_{\text{out}}^{(2\text{ph})}\rangle \propto \sqrt{\lambda_0^{(a)} t_s} |0, 0\rangle_{a_1, b_1} \pm e^{i\phi} \sqrt{\lambda_1^{(a)} (1-t_s)} |1, 1\rangle_{a_1, b_1}. \quad (2)$$

For small t_s , this state takes the form of a two-mode squeezed state, which is known to exhibit strong loss robustness for Bell test with the considered measurement [22].

This protocol achieves the same scaling as the one-photon one, $P_h^{(2\text{ph})} = P_s(\lambda_0^{(a)} t_s + \lambda_1^{(a)} (1-t_s)) \eta_c \sqrt{\eta_t} \approx O(\sqrt{\eta_t})$, where P_s is Bob's single-photon generation probability. For full derivation of density matrices and performance of protocols, see Appendix A.

III. THE NONLOCALITY TEST

To extract the secret key, Alice and Bob perform local measurements $\mathcal{M}_A$ and $\mathcal{M}_B$. Alice selects between two settings $x \in \{1, 2\}$, while Bob chooses from three $y \in \{1, 2, 3\}$, each yielding binary outcomes $a, b \in \{\pm 1\}$ (cf. Ref. [23]).

For the Bell test, both parties randomly select from their first two settings and evaluate the CHSH parameter [24]

$$S = \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle, \quad (3)$$

where A_x and B_y denote Alice's and Bob's measurement observables, respectively, with correlations $\langle A_x B_y \rangle = \sum_{a,b} p(a=b|x, y) - p(a \neq b|x, y)$. This parameter quantifies the observed nonlocality and bounds the information accessible to any eavesdropper, satisfying $S \leq 2$ for all local hidden-variable theories.

To violate Bell inequalities, one must perform mutually incompatible measurements. The states in Eqs. (1) and (2) are encoded in the Fock basis, $\{|0\rangle, |1\rangle\}$. While measuring in the z basis is straightforward using single-photon detectors, optimal Bell tests require challenging projections onto photon-number superpositions $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. To overcome this constraint, we employ a practical alternative accessible in modern laboratories, inspired by Ref. [25].

Our measurement scheme [Fig. 1(c)] implements: (1) displacement operations $D(\delta) = e^{\delta a^\dagger - \delta^* a}$ with setting-dependent $\delta_a = -i\alpha\sqrt{r_a}$ and $\delta_b = -i\beta\sqrt{r_b}$, followed by (2) "photon"/"no-photon" (on/off) detection with efficiency η_d . The effective positive operator-valued measures (POVMs) are

$$\mathcal{M}_0^{(A)} = D(\delta_a) E_0^{\eta_d} D^\dagger(\delta_a), \quad \mathcal{M}_0^{(B)} = D(\delta_b) E_0^{\eta_d} D^\dagger(\delta_b), \quad (4)$$

where $E_0^{\eta_d} = (1 - \eta_d)^{a^\dagger a}$ represents the effective no-click operator. To evaluate the CHSH value under realistic conditions with multimode sources and detection losses, we compute

$$\begin{aligned} p_a(0|\delta_a b) &= \text{Tr}(\rho_{a(b)} \mathcal{M}_0^{(A)}), \\ p(00|\delta_a \delta_b) &= \text{Tr}(\rho_{\text{out}} \mathcal{M}_0^{(A)} \otimes \mathcal{M}_0^{(B)}), \end{aligned} \quad (5)$$

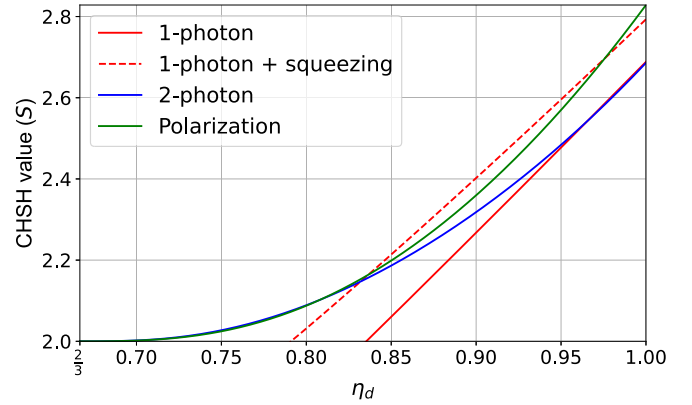


FIG. 2. Maximal CHSH parameter S as a function of detector efficiency η_d computed for one-photon protocol (red solid line, with dashed red line including squeezing operations in the measurements [15]), two-photon protocol (blue), and, for reference, a polarization-based protocol [26] (green).

with $\rho_{a(b)}$ denoting Alice's (Bob's) reduced density matrix. The detailed derivations of the marginals and correlators, including higher photon-number contributions, are presented in Appendixes B and C.

Remarkably, both protocols maintain near-maximal CHSH violations even under severe transmission losses: $S = 2.688$ for $|\Psi_{\text{out}}^{(1\text{ph})}\rangle$ and $S = 2.686$ for $|\Psi_{\text{out}}^{(2\text{ph})}\rangle$. This robustness stems from the protocol's inherent noise tolerance: Under high loss, the heralded state resides in the qubit subspace where violations are strongest. By decreasing the value of g , we limit the contribution of heralded multiphoton components and their impact on reduced violations. However, this affects the heralding probability P_h , which is crucial in the finite-size regime. Consequently, channel loss primarily affects protocol performance, while the CHSH value S and the asymptotic key rate r remain distance independent.

Figure 2 illustrates how detection efficiency η_d influences the maximal CHSH value (S). The state $|\Psi_{\text{out}}^{(1\text{ph})}\rangle$ suffers losses in both superposition components. When photons are lost, the anticorrelation in this state degrades toward a full correlation $|00\rangle$, leading to a rapid drop in S . In Ref. [15], an additional squeezing operation through a nonlinear crystal $\chi^{(2)}$ is inserted between the displacement operation and the detector to partially mitigate this effect, but it is experimentally challenging. In contrast, state $|\Psi_{\text{out}}^{(2\text{ph})}\rangle$ exhibits much higher loss resilience as losses only affect the $|11\rangle$ component. By tuning t_s and g to reduce the coefficient $\lambda_1(1-t_s)$, the protocol can approach the Eberhard limit for photon-counting measurements [8]. We compare these results with the polarization-based protocol [26], where states of the form $\cos(\theta)|HH\rangle + \sin(\theta)|VV\rangle$ experience symmetric losses across both components. Here, however, strategic postprocessing can preserve correlations: If Alice and Bob assign no-detection events the same value as $|H\rangle$ detection, the $|HH\rangle$ correlations remain unaffected by loss. Taking $\theta \rightarrow 0$ suppresses contributions from $|VV\rangle$, achieving robustness comparable to the two-photon protocol.

IV. SECURITY ANALYSIS IN THE ASYMPTOTIC REGIME

The asymptotic secure key rate (SKR) for DI QKD protocols, which offers resilience against collective attacks by a quantum eavesdropper (Eve) [23,27], is lower bounded by the Devetak-Winter formula [28]

$$r_\infty \geq H(A_1|E) - H(A_1|B_3), \quad (6)$$

where $H(X|Y)$ denotes the conditional von Neumann entropy. This expression quantifies Alice and Bob's information advantage over Eve: The first term captures Eve's uncertainty about Alice's outcomes, while the second represents error-correction costs. Although $H(A_1|B_3)$ follows directly from measurement statistics, bounding Eve's information $H(A_1|E)$ requires careful analysis. To evaluate this, we exploit the connection between CHSH inequality violations and information security. Using the analytical framework from Ref. [29] with noisy preprocessing, we obtain

$$r \geq 1 - h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right) - H(A_1|B_3) + h\left(\frac{1 + \sqrt{1 - q(1-q)(8 - S^2)}}{2}\right), \quad (7)$$

where $h(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ is the binary entropy function and q denotes the bit-flip probability during noisy preprocessing, a standard method to enhance key rate (see Appendix F 1).

For tighter bounds, we utilize the full probability distribution $p(a, b|x, y)$. Following the Brown-Fawzi-Fawzi (BFF) method [18], we bound conditional entropy via noncommutative polynomial optimization, implemented through the Navascués-Pironio-Acín (NPA) hierarchy [30]. This semidefinite programming approach yields near-optimal bounds with negligible gaps to collective attack upper bounds. We also investigate bounds based on min-entropy, which directly quantifies Eve's guessing probability [31] (see Appendix F for a detailed description of the lower bound methods).

Building on these theoretical bounds, we examine how practical imperfections affect protocol performance. In particular, mode mismatch at Charlie's station critically affects performance by reducing interferometric visibility (V_c) and degrading heralded entanglement (see Appendix D). In addition, local mismatches between the signal modes and the displacement coherent states in the measurement setups at Alice's (V_a) and Bob's (V_b) local labs can further reduce the observed Bell violation; As shown in Appendix E, their impact is comparable to that of Charlie's visibility. For simplicity, in our main analysis we assume a common visibility parameter $V := V_a = V_b = V_c$.

Figure 3 shows asymptotic key rates versus local detection efficiency η_d for various visibility values. Our numerical optimization reveals critical thresholds: Positive key rates require $\eta_d = 91.5\%$ for the one-photon protocol and $\eta_d = 80.2\%$ for the two-photon one. Importantly, optimization over the parametric gain g enables the two-photon protocol to approach the ideal state $|00\rangle + r|11\rangle$ with the lowest detection-efficiency threshold. Although a smaller g reduces the heralding probability, this effect is fully compensated by increasing the

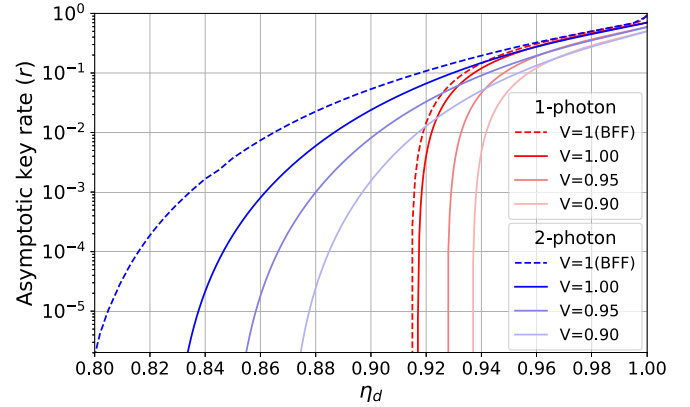


FIG. 3. Asymptotic raw key rates r (logarithmic scale) as a function of local detection efficiency η_d for visibility v at Charlie's, computed for the one-photon protocol (red) and the two-photon protocol (blue), both with optimal preprocessing q_{opt} . The solid lines correspond to the key rate computed using the analytical bound in Eq. (7) for $V = 1, 0.95, 0.9$, while dashed lines show results from the BFF method (see Appendix F 2) for $V = 1$.

number of rounds in the asymptotic case. Both protocols show similar robustness to imperfect visibility $v < 1$, thanks to the fact that a single photon interferes at Charlie's station, leading to a $\sqrt{V}$ dependence of the joint probabilities. In contrast, in polarization-based protocols [26,32], the interferometric visibility enters linearly, causing a considerably stronger degradation in key rate performance.

V. FINITE-KEY SECURITY ANALYSIS

Practical implementation of our DI-TF QKD protocol requires analysis of finite-size effects to determine maximum achievable distances and realistic key rates while ensuring security against general quantum attacks [19,20]. We employ EAT to bound conditional entropy $H(A_1|E)$ over N rounds [19,20].

Here, we implement this analysis through two complementary approaches. First, using Eq. (7), we construct a linear bound via its tangent. This method offers computational simplicity, requiring only CHSH monitoring. Next, we perform full statistics certification exploiting the complete probability distribution $p(a, b|x, y)$, resulting in tighter bounds at increased computational cost. Error correction employs the VHASH hashing algorithm [33], followed by privacy amplification [10].

The finite-size raw key rate for N rounds is $r = \ell/N$, where ℓ denotes the extractable secure key length. We convert it to bits per second (bps) using $R = P_h \nu r$, where $\nu = 100$ MHz is the laser source repetition rate and P_h is the heralding probability. Appendix G provides details on the numerical approaches used to optimize the finite-key rate.

Figure 4(a) compares the finite-size key rates as a function of distance across various protocols at an overall efficiency of $\eta_d = \eta_s = 0.93$. Notably, we observe a significant distance breakthrough: The one-photon protocol maintains key rates above 1 bps beyond 400 km, which is unprecedented for DI QKD protocols. Although the asymptotic rates remain

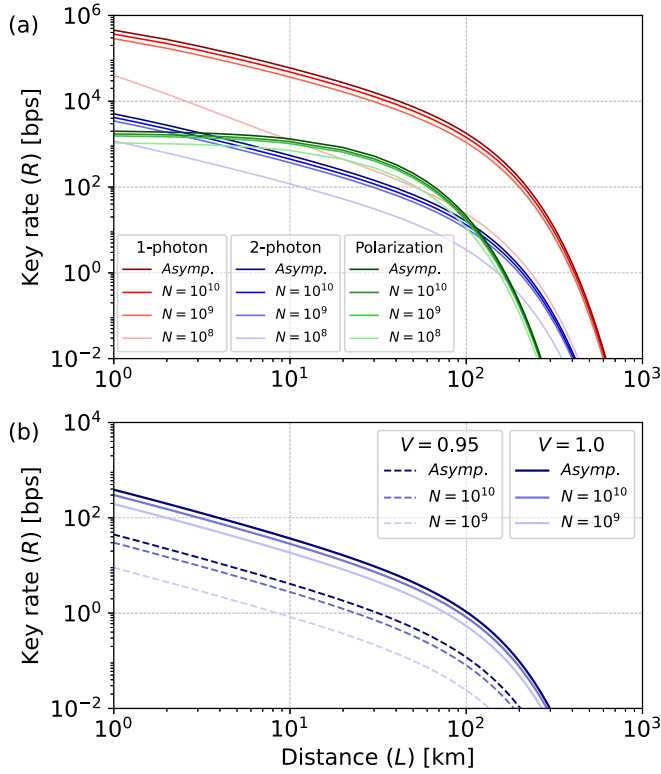


FIG. 4. Comparison of finite-size and asymptotic key rates R vs distance L for $N \in \{10^8, 10^9, 10^{10}, \infty\}$ protocol rounds, assuming repetition rate $\nu = 100$ MHz and optimal parametric gain g , computed for (a) local detection efficiency $\eta_d = 93\%$ for the one-photon protocol (red), the two-photon protocol (blue), and the polarization-based protocol from Ref. [26] (green), all for visibility $V = 1$; and (b) local detection efficiency $\eta_d = 90\%$ for the two-photon protocol, computed for visibilities $V = 0.95$ (dashed lines) and 1 (solid lines).

positive at all distances, finite-size effects impose practical limitations. With $N \geq 10^9$ repetition rounds, the key rates closely approach the asymptotic bound, whereas for $N = 10^8$ we observe their significant decrease.

To explore a more practical scenario, we consider the two-photon protocol at a reduced detection efficiency of $\eta_d = \eta_s = 0.90$ with visibilities $V = 1$ and 0.95 . As depicted in Fig. 4(b), setting an optimal g_a and g_b enables this setup to reach approximately 1 bps for $N = 10^{10}$ rounds over a 100 km distance.

VI. FEASIBILITY

The protocols studied in this article face two main challenges. First, the measurement scheme requires displacement operations combined with single-photon counting. Such measurements have been demonstrated experimentally [16], with efficiency requirements primarily driven by the need for highly efficient two-mode squeezed-vacuum sources. Second, phase drifts in the heralding scheme can lead to heralding of separable states. Reference [16] addressed this using phase stabilization in a single-photon interference-based heralding scheme closely related to our protocol. Solid-state entanglement at metropolitan scales has recently been achieved using single-photon heralding schemes [34,35]. Long-distance device-independent quantum key distribution

TABLE I. Detection-efficiency threshold required to violate CHSH inequality and to achieve a positive secure key rate (denoted by r). For the noisy preprocessing technique (denoted by NP), the optimal value of q rises from 0 to 0.5 as the efficiency decreases from 1 toward the threshold, whereas for the postselection technique (denoted by PS), the optimal value of p drops from 1 to 0 over the same range.

Method	Related parameters	Min η_d	
		One-photon	Two-photon
	Bell violation	0.836	2/3
CHSH method	r	0.924	0.895
	$r + \text{NP}$	0.917	0.826
BFF method	r	0.921	0.868
	$r + \text{NP}$	0.915	0.802
Min-entropy	r	0.945	0.94
	$r + \text{PS}$	0.898	0.903

based on high-visibility single-photon interference has been demonstrated very recently [36].

VII. CONCLUSIONS

We have studied two fully photonic approaches for realizing device-independent quantum key distribution with twin-field scaling. The choice between them involves a trade-off between detector requirements and the key rate achievable at long distances. The two-photon protocol offers the best efficiency threshold up to 80.2% (91.5% for the one-photon protocol) in the asymptotic regime, achieving state-of-the-art threshold for DI-TF QKD (see Table I for a complete comparison). This is lower than the 81.8% required in polarization-based schemes, although both protocols can reach the Eberhard limit for CHSH violation. In the realistic finite-size regime, we find that an efficiency of 90% is required to obtain a high enough key rate. The key rate obtained in the one-photon protocol is higher by one order of magnitude when the efficiency is higher than 92%. State-of-the-art experiments can achieve 82.2% overall efficiency [35], which makes a proof-of-principle experiment for the two-photon protocol available with current setups. We believe that our work represents an important step toward the realization of long-distance DI QKD. Furthermore, during the preparation of this article, we became aware of two related works, which study similar protocols, but only in the asymptotic regime. In Ref. [37], a two-photon protocol was presented. In contrast, Ref. [38] analyzes both one- and two-photon protocols and includes a comprehensive dark count analysis. Compared to them, our work provides both rigorous finite-size security and visibility analyses.

ACKNOWLEDGMENTS

M.M. and M.S.-M. were supported by the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie project "AppQInfo" No. 956071. M.A. and M.S.-M. were supported by the National Science Centre "Sonata Bis" Project No. 2019/34/E/ST2/00273,

and M.S.-M. by the QuantERA II Programme, which has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No. 101017733, Project "PhoMemtor" No. 2021/03/Y/ST2/00177. P.M. was supported by the European Union's Horizon Europe research and innovation program under Grant Agreement No. 101080086/NeQST. E.O. acknowledges funding by the French national quantum initiative managed by Agence Nationale de la Recherche in the framework of France 2030 with the reference ANR-22-PETQ-0009. NPA optimization was implemented using Python library NCPOL2SDPA [39], and MOSEK [40] was used as a solver. The entropy accumulation analysis was performed using EXPDIQRNG package [41].

DATA AVAILABILITY

The data that support the findings of this article are not publicly available. The data are available from the authors upon reasonable request.

APPENDIX A: ENTANGLEMENT DISTRIBUTION

In this Appendix, we derive the density matrices and heralding probabilities for both the one-photon and two-photon protocols, taking into account transmission losses and higher-order photon contributions.

1. The one-photon protocol

In the entanglement distribution protocol shown in Fig. 1(a), Alice and Bob pump their SPDC crystals with pulsed lasers and generate locally TMSV states of the form

$$|\Psi\rangle = \sum_{n=0}^{\infty} \sqrt{\lambda_n} |n, n\rangle_{1,2}, \quad (\text{A1})$$

where $\sqrt{\lambda_n} = \frac{\tanh^n g}{\cosh g}$ is the probability amplitude of n -photon components, g is the parametric gain of SPDC crystals that is governed by the laser power and phase matching conditions, and indices 1 and 2 denote the signal and idler modes, respectively. While $\{\lambda_n\}$ is a geometrically decreasing sequence

with the most probable zero- and one-photon events, in this work we consider the full multiphoton form of $|\Psi\rangle$ to avoid the free-sampling assumption in the subsequent Bell test.

Next, idler modes a_2 and b_2 are sent to Charlie, interfered on a symmetric beam splitter, measured using photon-number-resolved (PNR) detection, and heralded. In the lossless conditions, as a result of this, a generalized Holland-Burnett state [42], which is near-maximally entangled in the photon number, is shared between Alice's and Bob's signal modes, a_1 and b_1 :

$$|\Psi_{\text{out}}^{(\sigma,k)}\rangle = \sum_{n=0}^{\sigma} \mathcal{A}_{\sigma}(k, n) |n, \sigma - n\rangle_{a_1, b_1}, \quad (\text{A2})$$

where k and $\sigma - k$ are the heralded Charlie's readouts, $\mathcal{A}_{\sigma}(k, n) = i^{k-n} \phi_k(n - \frac{\sigma}{2}, \sigma)$ is the probability amplitude, $k = 0, \dots, \sigma$, and ϕ_k are symmetric Kravchuk functions—orthonormal discrete polynomials that converge to Hermite-Gauss polynomials for large σ . For more information on these functions, see the Appendixes in Refs. [17,43]. If $\sigma = 1$, Charlie heralds a single-photon entanglement in one of the following forms:

$$|\Psi_{\text{out}}^{(1,0)}\rangle = \frac{1}{\sqrt{2}}(|0, 1\rangle - i|1, 0\rangle)_{a_1, b_1}, \quad (\text{A3})$$

$$|\Psi_{\text{out}}^{(1,1)}\rangle = \frac{1}{\sqrt{2}}(|0, 1\rangle + i|1, 0\rangle)_{a_1, b_1}. \quad (\text{A4})$$

Without loss of generality, in this work we focus on $|\Psi_{\text{out}}^{(1,1)}\rangle \equiv |\Psi_{\text{out}}^{(1\text{ph})}\rangle$.

In a nonideal scenario, where the idler channels are lossy, the losses can be modeled using a beam splitter with reflectivity r_t and transmissivity η_t , satisfying $r_t + \eta_t = 1$. Denoting S as the total number of photons produced by Alice's and Bob's SPDCs in the idler modes, and σ as the total number of photons arriving at Charlie's station after the photon loss, the state from Eq. (A2) converts into a mixed state

$$\rho_{\text{out}}^{(k,\sigma)} = \sum_{S=\sigma}^{\infty} P_{S|\sigma} \rho_S^{(k,\sigma)}, \quad (\text{A5})$$

in which $P_{S|\sigma} = (r_t \tanh^2 g)^{S-\sigma} (1 - r_t \tanh^2 g)^{\sigma+2} \binom{S+1}{\sigma+1}$, and

$$\rho_S^{(k,\sigma)} = \tilde{\mathcal{N}}_S^{-2} \sum_{n,n'=0}^S |n, S-n\rangle \langle n', S-n'| \sum_{p=\max(0, n-\sigma, n'-\sigma)}^{\min(S-\sigma, n, n')} \sqrt{\binom{n}{p} \binom{n'}{p} \binom{S-n}{S-\sigma-p} \binom{S-n'}{S-\sigma-p}} \mathcal{A}_{\sigma}(k, n-p) \mathcal{A}_{\sigma}^*(k, n'-p), \quad (\text{A6})$$

where $\tilde{\mathcal{N}}_S^2 = \sum_{n=0}^S \sum_{p=\max(0, n-1)}^{\min(S-1, n)} \binom{n}{p} \binom{S-n}{S-p-1} |\mathcal{A}_{\sigma}(k, n-p)|^2 = \binom{S+1}{\sigma+1}$. Here, the corresponding state for $S = \sigma$ in Eq. (A5) is given by $\rho_{\sigma}^{(k,\sigma)} = |\Psi_{\text{out}}^{(\sigma,k)}\rangle \langle \Psi_{\text{out}}^{(\sigma,k)}|$, which remains the dominant term provided that $g \ll 1$. By changing the summation order and redefining the variables in Eqs. (A5) and (A6), the state can be expressed in the following equivalent form:

$$\begin{aligned} \rho_{\text{out}}^{(k,\sigma)} &= (1 - r_t \tanh^2 g)^{\sigma+2} \sum_{p,q=0}^{\sigma} \mathcal{A}_{\sigma}(k, p) \mathcal{A}_{\sigma}^*(k, q) \sum_{m=0}^{\infty} (r_t \tanh^2 g)^m \sqrt{\binom{m+p}{m} \binom{m+q}{m}} |m+p\rangle \langle m+q|_{a_1} \\ &\quad \otimes \sum_{n=0}^{\infty} (r_t \tanh^2 g)^n \sqrt{\binom{n+\sigma-p}{n} \binom{n+\sigma-q}{n}} |n+\sigma-p\rangle \langle n+\sigma-q|_{b_1}. \end{aligned} \quad (\text{A7})$$

To rewrite the state for the one-photon protocol by setting $\sigma = k = 1$, we have

$$\begin{aligned} \rho_{\text{out}}^{(1\text{ph})} = & \frac{(1 - r_t \tanh^2 g)^3}{2} \\ & \times \left[\sum_{m=0}^{\infty} (r_t \tanh^2 g)^m |m\rangle \langle m| \otimes \sum_{n=0}^{\infty} n (r_t \tanh^2 g)^{n-1} |n\rangle \langle n| + \sum_{m=0}^{\infty} m (r_t \tanh^2 g)^{m-1} |m\rangle \langle m| \otimes \sum_{n=0}^{\infty} (r_t \tanh^2 g)^n |n\rangle \langle n| \right. \\ & \left. + \sum_{m=0}^{\infty} (r_t \tanh^2 g)^m \sqrt{m+1} \sum_{n=0}^{\infty} (r_t \tanh^2 g)^n \sqrt{n+1} (|m\rangle \langle m+1| \otimes |n+1\rangle \langle n| + |m+1\rangle \langle m| \otimes |n\rangle \langle n+1|) \right]_{a_1, b_1} \quad (\text{A8}) \end{aligned}$$

The heralding probability of a one-photon protocol can be obtained by substituting $\sigma = k = 1$ in

$$P_h(k, \sigma) = \frac{\lambda_\sigma}{\cosh^2 g} \times \frac{(1 - r_t)^\sigma}{(1 - r_t \tanh^2 g)^{\sigma+2}} = \frac{(\sqrt{\eta_t} \sinh^2 g)^\sigma}{(1 + \sqrt{\eta_t} \sinh^2 g)^{\sigma+2}}, \quad (\text{A9})$$

which is obtained by assuming a perfect detection at Charlie's station [17]. Using $r_t = 1 - 10^{-\alpha_{\text{att}}(L/2)/10} = 1 - \sqrt{\eta_t}$, where α_{att} is the attenuation coefficient of a medium through which the photons travel. For standard telecom fibers, $\alpha_{\text{att}} = 0.2 \text{ km}^{-1}$ and L is the total distance between Alice and Bob in kilometers. Assuming that Charlie is located approximately at the midpoint between Alice and Bob, we replaced L_{AC} with $L/2$. Thus, the total probability of the generation of the one-photon entanglement per pulse is

$$P_h^{(1\text{ph})} = \frac{10^{L/50} \sinh^2 g}{[10^{L/100} + \sinh^2 g]^3} \eta_c \approx 10^{-L/100} \sinh^2 g \eta_c \propto O(\sqrt{\eta_t}), \quad (\text{A10})$$

where η_c accounts for the detection efficiency at Charlie's. The approximation holds for long distances, as $\sinh^2 g \ll 10^{L/100}$ under the fact that $g \ll 1$, and the protocol scaling is consistent with the TF QKD performance.

Note that the probability ratio of multiphoton to single-photon arrivals at Charlie can be expressed as

$$\frac{1 - P_h(0, 0) - P_h(0, 1) - P_h(1, 1)}{P_h(0, 1) + P_h(1, 1)} = \frac{(1 + \sqrt{\eta_t} \sinh^2 g)^3 - (1 + \sqrt{\eta_t} \sinh^2 g) - (2\sqrt{\eta_t} \sinh^2 g)}{2\sqrt{\eta_t} \sinh^2 g} = \frac{1}{2} \sqrt{\eta_t} \sinh^2 g (3 + \sqrt{\eta_t} \sinh^2 g). \quad (\text{A11})$$

Since this ratio scales as $o(10^{-L/100} g^2)$, when $g \ll 1$ or the distance is large ($L \gg 1$), replacing the PNR detectors with the on/off detectors leaves $\rho_{\text{out}}^{(1\text{ph})}$ unchanged. One can also argue that, since on/off detectors cannot resolve higher photon numbers, they are effectively equivalent to imperfect PNR detectors, whose inefficiency can be incorporated by increasing the effective channel length.

2. The two-photon protocol

The two-photon protocol described in this work extends the one-photon scheme by employing an asymmetric source configuration where Alice prepares a TMSV state ($|\psi_a\rangle = \sum_{m=0}^{\infty} \sqrt{\lambda_m^{(a)}} |m, m\rangle_{a_1, a_2}$), while Bob ideally generates a heralded single-photon path-entangled (SPPE) state, ($|\psi_b\rangle = \sqrt{t_s} |0, 1\rangle_{b_1, b_2} + e^{i\phi_s} \sqrt{1 - t_s} |1, 0\rangle_{b_1, b_2}$). Upon successful heralding at Charlie's station through single-photon detection, the protocol produces a tunable photon-number path-entangled state between Alice and Bob:

$$|\Psi_{\text{out}}^{(2\text{ph})}\rangle \propto \sqrt{\lambda_0^{(a)} t_s t_c} |0, 0\rangle_{a_1, b_1} + e^{i\phi} \sqrt{\lambda_1^{(a)} r_s r_c} |1, 1\rangle_{a_1, b_1}, \quad (\text{A12})$$

where $t_{s(c)}$ and $r_{s(c)}$ are Bob's (Charlie's) beam splitter transmissivity and reflectivity, respectively (with $t_{s(c)} + r_{s(c)} = 1$), and $\phi = \phi_s + \phi_c$ are the combined phases arising from Bob's and Charlie's beam splitters. This state can be continuously tuned from a product state to a maximally entangled state by adjusting the source parameters.

In the nonideal case, where Bob employs an imperfect "photon"/"no-photon" (on/off) detector of efficiency η_s on beam b_0 to herald a single-photon state, the resulting density matrix in mode b_1 is

$$\rho_0^{(b)} = \mathcal{N}_b^{-2} \text{Tr}_{b_0} [(E_1^{\eta_s} \otimes \mathbb{I})_{b_0, b_2} |\Psi\rangle \langle \Psi|], \quad (\text{A13})$$

where $|\Psi\rangle$ is defined in Eq. (A1), and $E_1^{\eta_s} = \mathbb{I} - \sum_{k=0}^{\infty} (1 - \eta_s)^k |k\rangle\langle k|$ represents the effective POVM element for click detection. Thus, the heralded state in mode b_2 simplifies to

$$\rho_0^{(b)} = \mathcal{N}_b^{-2} \sum_{n=0}^{\infty} \lambda_n^{(b)} (1 - (1 - \eta_s)^n) |n\rangle\langle n|, \quad (\text{A14})$$

with normalization factor $\mathcal{N}_b^2 = 1 - (1 + \eta_s \sinh^2 g_b)^{-1} = P_s$, representing the probability that Bob's detector clicks and the imperfect SPPE state is generated. Then, Bob interferes this state with a vacuum in mode b_1 at a beam splitter, resulting in a path-entangled state across modes b_1 and b_2 given by

$$\begin{aligned} \rho_{\text{in}}^{(b)} &= U_{\text{BS}}^{(b_1, b_2)} (|0\rangle\langle 0| \otimes \rho_0^{(b)})_{b_1, b_2} U_{\text{BS}}^{(b_1, b_2)\dagger} \\ &= \mathcal{N}_b^{-2} \sum_{n=0}^{\infty} \lambda_n^{(b)} (1 - (1 - \eta_s)^n) \sum_{l, l'=0}^n \sqrt{\binom{n}{l} \binom{n}{l'}} t_s^{l+l'} r_s^{2n-l-l'} e^{i\phi_s(l'-l)} |n-l, l\rangle\langle n-l', l'|_{b_1, b_2}. \end{aligned} \quad (\text{A15})$$

Moreover, idler channels experience symmetric loss, i.e., $r_t^{(a_2)} = r_t^{(b_2)}$, which can be modeled using a beam splitter $U_{\text{BS}}^{(a_2, a_3)(b_2, b_3)}$, through which each idler mode $a_2(b_2)$ interferes with a vacuum mode $|0\rangle_{a_3(b_3)}$. Then, after the beams interfere at Charlie's station and a single-photon detection occurs, the resulting shared mixed state can be calculated as

$$\begin{aligned} \rho_{\text{out}}^{(2\text{ph})} &= \mathcal{N}^{-2} (\sqrt{t_c} |01\rangle + e^{-i\phi_c} \sqrt{r_c} |10\rangle)_{a_2, b_2} [\text{Tr}_{a_3} (U_{\text{BS}}^{(a_2, a_3)} (|\psi_a\rangle\langle\psi_a|_{a_1, a_2} \otimes |0\rangle\langle 0|_{a_3}) U_{\text{BS}}^{(a_2, a_3)\dagger}) \\ &\quad \otimes \text{Tr}_{b_3} (U_{\text{BS}}^{(b_2, b_3)} (\rho_{\text{in}}^{(b)} \otimes |0\rangle\langle 0|_{b_3}) U_{\text{BS}}^{(b_2, b_3)\dagger})] (\sqrt{t_c} |01\rangle + e^{i\phi_c} \sqrt{r_c} |10\rangle)_{a_2, b_2}. \end{aligned} \quad (\text{A16})$$

Using $\text{Tr}_{x_3} (U_{\text{BS}} |m, 0\rangle\langle m', 0|_{x_2, x_3} U_{\text{BS}}^\dagger) = \sum_{p=0}^{\min(m, m')} \sqrt{\binom{m}{p} \binom{m'}{p}} (1 - r_t)^{m+m'-2p} r_t^{2p} |m-p\rangle\langle m'-p|_{x_2}$, we have

$$\begin{aligned} \rho_{\text{out}}^{(2\text{ph})} &= (\mathcal{N} \mathcal{N}_b)^{-2} (\sqrt{t_c} |01\rangle + e^{-i\phi_c} \sqrt{r_c} |10\rangle)_{a_2, b_2} \left[\sum_{m, m'=0}^{\infty} \sqrt{\lambda_m^{(a)} \lambda_{m'}^{(a)}} \sum_{p=0}^{\min(m, m')} \sqrt{\binom{m}{p} \binom{m'}{p}} (1 - r_t)^{m+m'-2p} r_t^{2p} \right. \\ &\quad \times |m, m-p\rangle\langle m', m'-p|_{a_1, a_2} \otimes \sum_{n=0}^{\infty} \lambda_n^{(b)} (1 - (1 - \eta_s)^n) \sum_{l, l'=0}^n \sqrt{\binom{n}{l} \binom{n}{l'}} t_s^{l+l'} r_s^{2n-l-l'} e^{i\phi_s(l'-l)} \\ &\quad \times \left. \sum_{q=0}^{\min(l, l')} \sqrt{\binom{l}{q} \binom{l'}{q}} (1 - r_t)^{l+l'-2q} r_t^{2q} |n-l, l-q\rangle\langle n-l', l'-q|_{b_1, b_2} \right] (\sqrt{t_c} |01\rangle + e^{i\phi_c} \sqrt{r_c} |10\rangle)_{a_2, b_2}. \end{aligned} \quad (\text{A17})$$

By performing a straightforward calculation, the state simplifies to

$$\begin{aligned} \rho_{\text{out}}^{(2\text{ph})} &= (\mathcal{N} \mathcal{N}_b)^{-2} (1 - r_t) \sum_{n=0}^{\infty} \lambda_n^{(b)} (1 - (1 - \eta_s)^n) \left[t_c \sum_{m=0}^{\infty} \lambda_m^{(a)} r_t^m |m\rangle\langle m|_{a_1} \otimes \sum_{l=0}^n \binom{n}{l} t_s^l r_s^{n-l} \times l r_t^{l-1} |n-l\rangle\langle n-l|_{b_1} \right. \\ &\quad + r_c \sum_{m=0}^{\infty} \lambda_m^{(a)} m r_t^{m-1} |m\rangle\langle m|_{a_1} \otimes \sum_{l=0}^n \binom{n}{l} t_s^l r_s^{n-l} \times r_t^l |n-l\rangle\langle n-l|_{b_1} \\ &\quad + \sqrt{t_c r_c} e^{i(\phi_c - \phi_s)} \sum_{m=0}^{\infty} \sqrt{\lambda_m^{(a)} \lambda_{m+1}^{(a)}} (m+1) r_t^m |m\rangle\langle m+1|_{a_1} \\ &\quad \otimes \sum_{l'=0}^{n-1} \sqrt{\binom{n}{l'+1} \binom{n}{l'}} t_s^{2l'+1} r_s^{2n-2l'-1} \times (l'+1) r_t^{2l'} |n-l'-1\rangle\langle n-l'-1|_{b_1} \\ &\quad + \sqrt{r_c t_c} e^{i(\phi_s - \phi_c)} \sum_{m'=0}^{\infty} \sqrt{\lambda_{m'+1}^{(a)} \lambda_{m'}^{(a)}} (m'+1) r_t^{m'} |m'+1\rangle\langle m'|_{a_1} \\ &\quad \otimes \left. \sum_{l=0}^{n-1} \sqrt{\binom{n}{l} \binom{n}{l+1}} t_s^{2l+1} r_s^{2n-2l-1} \times (l+1) r_t^{2l} |n-l\rangle\langle n-l-1|_{b_1} \right]. \end{aligned} \quad (\text{A18})$$

The normalization factor $(\mathcal{N}\mathcal{N}_b)^2$ can be calculated by taking trace over $\rho_{\text{out}}^{(2\text{ph})}$:

$$\begin{aligned}
 (\mathcal{N}\mathcal{N}_b)^2 &= (1-r_t) \sum_{n=0}^{\infty} \lambda_n^{(b)} (1-(1-\eta_s)^n) \left[t_c \sum_{m=0}^{\infty} \lambda_m^{(a)} r_t^m \sum_{l=0}^n \binom{n}{l} t_s^l r_s^{n-l} \times l r_t^{l-1} + r_c \sum_{m=0}^{\infty} \lambda_m^{(a)} m r_t^{m-1} \sum_{l=0}^n \binom{n}{l} t_s^l r_s^{n-l} \times r_t^l \right] \\
 &= (1-r_t) \sum_{n=0}^{\infty} \lambda_n^{(b)} (1-(1-\eta_s)^n) \left[\frac{t_c \cosh^{-2} g_a}{1-r_t \tanh^2 g_a} \times \frac{\partial(r_s+t_s r_t)^n}{\partial r_t} + \frac{r_c}{\cosh^2 g_a} \frac{\partial(1-r_t \tanh^2 g_a)^{-1}}{\partial r_t} \times (r_s+t_s r_t)^n \right] \\
 &= (1-r_t) \left[\frac{t_c \cosh^{-2} g_b}{1+(1-r_t) \sinh^2 g_a} \times \frac{\partial}{\partial r_t} + \frac{r_c \sinh^2 g_a \cosh^{-2} g_b}{(1+(1-r_t) \sinh^2 g_a)^2} \right] \left(\sum_{n=0}^{\infty} (1-(1-\eta_s)^n) ((r_s+t_s r_t) \tanh^2 g_b)^n \right) \\
 &= (1-r_t) \left[\frac{t_c}{1+\sqrt{\eta_t} \sinh^2 g_a} \times \frac{\partial}{\partial r_t} + \frac{r_c \sinh^2 g_a}{(1+\sqrt{\eta_t} \sinh^2 g_a)^2} \right] \left(\frac{\cosh^{-2} g_b}{1-(r_s+t_s r_t) \tanh^2 g_b} - \frac{\cosh^{-2} g_b}{1-(1-\eta_s)(r_s+t_s r_t) \tanh^2 g_b} \right), \quad (\text{A19})
 \end{aligned}$$

where we substituted $\lambda_n^{(b)} = \tanh^{2n} g_{a(b)} / \cosh^2 g_{a(b)}$ and used $\sum_{n=0}^{\infty} n x^{n-1} = \frac{\partial}{\partial x} (\sum_{n=0}^{\infty} x^n) = (1-x)^{-2}$ for $x < 1$. Using $1-r_t = 10^{-\alpha_{\text{att}}(\frac{L}{2})/10} = \sqrt{\eta_t}$ and replacing $\mathcal{N}_b^2 = \eta_s \sinh^2 g_b / (1 + \eta_s \sinh^2 g_b)$, we then obtain

$$\begin{aligned}
 \mathcal{N}^2 &= \frac{\sqrt{\eta_t} (1 + \eta_s \sinh^2 g_b)}{(1 + \sqrt{\eta_t} \sinh^2 g_a)(1 + \sqrt{\eta_t} t_s \sinh^2 g_b)(1 + (\eta_s + (1-\eta_s)\sqrt{\eta_t} t_s) \sinh^2 g_b)} \\
 &\times \left[\frac{t_c [(1 + \sinh^2 g_b)^2 - (1-\eta_s)(1 - \sqrt{\eta_t} t_s)^2 \sinh^4 g_b] t_s}{(1 + \sqrt{\eta_t} t_s \sinh^2 g_b)(1 + (\eta_s + (1-\eta_s)\sqrt{\eta_t} t_s) \sinh^2 g_b)} + \frac{r_c (1 - \sqrt{\eta_t} t_s) \sinh^2 g_a}{1 + \sqrt{\eta_t} \sinh^2 g_a} \right], \quad (\text{A20})
 \end{aligned}$$

which, for long distances where $\eta_t \ll 1$, is proportional to $o(\sqrt{\eta_t})$. In the limit $g_b \ll 1$, where Bob's initial state approaches the SPPE state, the shared state and its normalization factor reduce to

$$\begin{aligned}
 \tilde{\rho}_{\text{out}}^{(2\text{ph})} &= \tilde{\mathcal{N}}^{-2} \sqrt{\eta_t} \left[\sum_{n=0}^{\infty} \lambda_n^{(a)} r_t^n (t_s t_c + n t_s r_c) |n, 0\rangle \langle n, 0| + \frac{r_s r_c}{r_t} \sum_{n=0}^{\infty} n \lambda_n^{(a)} r_t^n |n, 1\rangle \langle n, 1| \right. \\
 &\quad \left. + \sqrt{t_s r_s t_c r_c} \sum_{n=0}^{\infty} \sqrt{(n+1) \lambda_n^{(a)} \lambda_{n+1}^{(a)}} r_t^n (e^{i(\phi_c - \phi_s)} |n, 0\rangle \langle n+1, 1| + e^{i(\phi_s - \phi_c)} |n+1, 1\rangle \langle n, 0|) \right]_{a_1, b_1}, \quad (\text{A21})
 \end{aligned}$$

where

$$\tilde{\mathcal{N}}^2 = \sqrt{\eta_t} \sum_{n=0}^{\infty} \lambda_n^{(a)} r_t^n \left(t_s t_c + n t_s r_c + \frac{n r_s r_c}{r_t} \right) = \sqrt{\eta_t} \left(\frac{t_c t_s}{1 + \sqrt{\eta_t} \sinh^2 g_a} + \frac{r_c (1 - t_s \sqrt{\eta_t}) \sinh^2 g_a}{(1 + \sqrt{\eta_t} \sinh^2 g_a)^2} \right). \quad (\text{A22})$$

The probability of detecting a single photon at Charlie's station is given by the product of Bob's single-photon generation probability P_s , the photon arrival probability at Charlie's $\tilde{\mathcal{N}}^2$, and his detector efficiency η_c . Assuming a symmetric beam splitter at Charlie's (i.e., $r_c = t_c = \frac{1}{2}$), the heralding efficiency is given by

$$P_h^{(2\text{ph})} = \tilde{\mathcal{N}}^2 P_s \eta_c = \frac{\sqrt{\eta_t} (t_s + \sinh^2 g_a)}{2(1 + \sqrt{\eta_t} \sinh^2 g_a)^2} P_s \eta_c \propto O(\sqrt{\eta_t}). \quad (\text{A23})$$

For the probability ratio of multiphoton to single-photon arrivals at Charlie, noting that

$$P_h(0, 0) = \frac{(1 + \eta_s \sinh^2 g_b)(1 - \sqrt{\eta_t} t_s)}{(1 + \sqrt{\eta_t} \sinh^2 g_a)(1 + \sqrt{\eta_t} t_s \sinh^2 g_b)(1 + (\eta_s + (1-\eta_s)\sqrt{\eta_t} t_s) \sinh^2 g_b)} \stackrel{g_b \ll 1}{\approx} \frac{1 - \sqrt{\eta_t} t_s}{1 + \sqrt{\eta_t} \sinh^2 g_a} \quad (\text{A24})$$

in the limit $g_b \ll 1$, we can write

$$\frac{1 - P_h(0, 0) - P_h(0, 1) - P_h(1, 1)}{P_h(0, 1) + P_h(1, 1)} = \frac{(1 + \sqrt{\eta_t} \sinh^2 g_a)^2 - (1 + \sqrt{\eta_t} \sinh^2 g_a)(1 - \sqrt{\eta_t} t_s) - \sqrt{\eta_t} (t_s + \sinh^2 g_a)}{\sqrt{\eta_t} (t_s + \sinh^2 g_a)} = \sqrt{\eta_t} \sinh^2 g_a. \quad (\text{A25})$$

Since this ratio scales as $o(10^{-L/100} g_a^2)$, for $g_{a(b)} \ll 1$ or $L \gg 1$, substituting the PNR detectors with the "photon"/"no-photon" (on/off) detectors does not affect $\rho_{\text{out}}^{(2\text{ph})}$. Again, this is equivalent to a perfect on/off detector with an additional channel loss.

APPENDIX B: MEASUREMENTS

Alice and Bob implement displacement operations $D(\delta) = e^{\delta a^\dagger - \delta^* a}$, followed by “photon”/“no-photon” (on/off) detection with efficiency η_d . The parties perform their local measurements without quantum memories in the delayed-choice scheme. To apply different measurement settings, each party interferes their signal mode with a coherent pulse $|\alpha\rangle$ or $|\beta\rangle$ on variable beam splitters characterized by reflectivity-to-transmissivity ratios $r_a : t_a$ and $r_b : t_b$, respectively. This procedure effectively implements the displacements $\delta_a = -i\alpha\sqrt{r_a}$ and $\delta_b = -i\beta\sqrt{r_b}$, yielding the final state $D(\delta_a) \otimes D(\delta_b)|\Psi_{\text{out}}\rangle$, which is then measured using local detectors. To account for the imperfection of detectors, we model the effective no-click POVM as a beam splitter followed by a perfect detector, whose inefficiency is represented by losses in the beam splitter. Thus, we can formulate it as

$$E_0^{\eta_d} = \sum_{m=0}^{\infty} (1 - \eta_d)^m |m\rangle\langle m| = (1 - \eta_d)^{a^\dagger a}, \quad (\text{B1})$$

where term $|m\rangle\langle m|$ corresponds to receiving m photons, and $(1 - \eta_d)^m$ corresponds to losing all of them. Thus, the effective local measurement for the output 0 can be written as $\mathcal{M}_0 = D(\delta)E_0^{\eta_d}D^\dagger(\delta)$. To proceed, we need to rewrite and simplify $\mathcal{M}_0$ in the photon-number (Fock) basis:

$$\langle n|\mathcal{M}_0|n'\rangle = \langle n|D(\delta)E_0^{\eta_d}D^\dagger(\delta)|n'\rangle = \sum_{m=0}^{\infty} (1 - \eta_d)^m \langle n|D(\delta)|m\rangle\langle m|D^\dagger(\delta)|n'\rangle. \quad (\text{B2})$$

Continuing the calculation requires representing the displacement operator $D(\delta)$ in the photon-number basis as well:

$$\begin{aligned} \langle n|D(\delta)|m\rangle &= \langle n|D(\delta)\frac{(a^\dagger)^m}{\sqrt{m!}}|0\rangle = \langle n|\frac{(a^\dagger - \delta^*)^m}{\sqrt{m!}}D(\delta)|0\rangle = \sum_{k=0}^{\min(m,n)} \binom{m}{k} \frac{(-\delta^*)^{m-k}}{\sqrt{m!}} \langle n|(a^\dagger)^k|\delta\rangle \\ &= \sum_{k=0}^{\min(m,n)} \binom{m}{k} \frac{(-\delta^*)^{m-k}}{\sqrt{m!}} \sqrt{\frac{n!}{(n-k)!}} e^{-\frac{|\delta|^2}{2}} \frac{\delta^{n-k}}{\sqrt{(n-k)!}} = e^{-\frac{|\delta|^2}{2}} \sum_{k=0}^{\min(m,n)} \frac{\sqrt{m!n!} \delta^{n-k} (-\delta^*)^{m-k}}{k!(m-k)!(n-k)!}. \end{aligned} \quad (\text{B3})$$

Substituting Eq. (B3) into Eq. (B2), we obtain

$$\begin{aligned} \langle n|\mathcal{M}_0|n'\rangle &= e^{-|\delta|^2} \sum_{m=0}^{\infty} (1 - \eta_d)^m \sum_{k=0}^{\min(m,n)} \frac{\sqrt{m!n!} \delta^{n-k} (-\delta^*)^{m-k}}{k!(m-k)!(n-k)!} \sum_{k'=0}^{\min(m,n')} \frac{\sqrt{m!n'!} (\delta^*)^{n'-k'} (-\delta)^{m-k'}}{k'!(m-k')!(n'-k')!} \\ &= e^{-|\delta|^2} \sqrt{n!n'!} \delta^n (\delta^*)^{n'} \sum_{k=0}^n \frac{(-|\delta|^2)^{-k}}{k!(n-k)!} \sum_{k'=0}^{n'} \frac{(-|\delta|^2)^{-k'}}{k'!(n'-k')!} \sum_{m=\max(k,k')}^{\infty} \frac{m!((1 - \eta_d)|\delta|^2)^m}{(m-k)!(m-k')!}. \end{aligned} \quad (\text{B4})$$

Applying part (a) of Lemma B1 to Eq. (B4), the expression for $\mathcal{M}^0$ simplifies to

$$\begin{aligned} \langle n|\mathcal{M}_0|n'\rangle &= e^{-\eta_d|\delta|^2} \sqrt{n!n'!} \delta^n (\delta^*)^{n'} \sum_{k=0}^n \frac{(\eta_d - 1)^k}{k!(n-k)!} \sum_{k'=0}^{n'} \frac{(\eta_d - 1)^{k'}}{k'!(n'-k')!} \sum_{i=0}^{\min(k,k')} \frac{i!}{((1 - \eta_d)|\delta|^2)^i} \binom{k}{i} \binom{k'}{i} \\ &= e^{-\eta_d|\delta|^2} \sqrt{n!n'!} \delta^n (\delta^*)^{n'} \sum_{i=0}^{\min(n,n')} \frac{(1 - \eta_d)^i}{i!|\delta|^{2i}} \sum_{k=i}^n \frac{(\eta_d - 1)^{k-i}}{(n-k)!(k-i)!} \sum_{k'=i}^{n'} \frac{(\eta_d - 1)^{k'-i}}{(n'-k')!(k'-i)!} \\ &= e^{-\eta_d|\delta|^2} \sqrt{n!n'!} \eta_d^{n+n'} \delta^n (\delta^*)^{n'} \sum_{i=0}^{\min(n,n')} \frac{(1 - \eta_d)^i}{i!(n-i)!(n'-i)!(\eta_d|\delta|)^{2i}}, \end{aligned} \quad (\text{B5})$$

where in the second line we changed the order of summations, and in the last line we used binomial expansion of $(1 + (\eta_d - 1))^{n-i}$ and $(1 + (\eta_d - 1))^{n'-i}$.

Lemma B1. For a real number $x \in [0, 1)$ and non-negative integers m, k , and k' , the following equations hold:

(a)

$$\sum_{n=\max(k,k')}^{\infty} \frac{n! x^n}{(n-k)!(n-k')!} = e^x \sum_{i=0}^{\min(k,k')} \frac{k!k'! x^{k+k'-i}}{i!(k-i)!(k'-i)!} \xrightarrow{k=k'} \sum_{n=k}^{\infty} \frac{n! x^n}{(n-k)!^2} = e^x x^k \sum_{i=0}^k \frac{k!}{i!} \binom{k}{i} x^i,$$

(b)

$$\sum_{n=k}^{\infty} \frac{n! x^n}{(n-k)!^2} = e^x x^k \sum_{i=0}^k \frac{k!}{i!} \left[\binom{k+1}{i+1} x^{i+1} + k \binom{k}{i} x^i \right],$$

(c)

$$\sum_{n=k}^{\infty} \binom{n}{k} x^n = \frac{x^k}{(1-x)^{k+1}},$$

(d)

$$\sum_{n=k}^{\infty} n \binom{n}{k} x^{n-1} = \frac{x^k + kx^{k-1}}{(1-x)^{k+2}}.$$

Proof. (a) By defining $m := \min(k, k')$ and $M := \max(k, k')$, the LHS could be written as

$$\begin{aligned} \text{LHS} &= x^m \sum_{i=0}^{\infty} \frac{x^{i+M-m} (i+M)!}{i! (i+M-m)!} = x^m \frac{\partial^m}{\partial x^m} \left(\sum_{i=0}^{\infty} \frac{x^{i+M}}{i!} \right) = x^m \frac{\partial^m}{\partial x^m} (x^M e^x) \\ &= x^m \sum_{i=0}^m \binom{m}{i} \frac{\partial^i (x^M)}{\partial x^i} \frac{\partial^{m-i} (e^x)}{\partial x^{m-i}} = e^x x^m \sum_{i=0}^m \binom{m}{i} \frac{M! x^{M-i}}{(M-i)!} = \text{RHS}. \end{aligned}$$

(b) We can divide the expression in LHS into the two terms:

$$\sum_{n=k}^{\infty} \frac{n \cdot n! x^n}{(n-k)!^2} = \sum_{n=k}^{\infty} \frac{n! x^n}{(n-k)!(n-k-1)!} + k \sum_{n=k}^{\infty} \frac{n! x^n}{(n-k)!^2}.$$

Applying part (a) with $k' = k + 1$ for the first term, and $k' = k$ for the second, we have

$$\text{LHS} = e^x x^k \sum_{i=0}^k \left[\frac{k!(k+1)! x^{k+1-i}}{i!(k-i)!(k+1-i)!} + \frac{k!^2 x^{k-i}}{i!(k-i)!^2} \right].$$

The proof is complete upon applying the substitution $i \rightarrow k - i$.

(c) It follows by taking the k th derivative of the identity $\sum_{n=0}^{\infty} x^n = (1-x)^{-1}$, which is valid for $|x| < 1$:

$$\sum_{n=k}^{\infty} \binom{n}{k} x^n = \frac{x^k}{k!} \sum_{n=k}^{\infty} \frac{n! x^{n-k}}{(n-k)!} = \frac{x^k}{k!} \frac{\partial^k}{\partial x^k} \left(\sum_{n=0}^{\infty} x^n \right) = \frac{x^k}{k!} \frac{\partial^k (1-x)^{-1}}{\partial x^k} = \frac{x^k}{(1-x)^{k+1}}.$$

(d)

$$\sum_{n=k}^{\infty} n \binom{n}{k} x^{n-1} = \frac{\partial}{\partial x} \left[\sum_{n=k}^{\infty} \binom{n}{k} x^n \right] = \frac{\partial}{\partial x} \left[\frac{x^k}{(1-x)^{k+1}} \right] = \frac{x^{k-1} (x+k)}{(1-x)^{k+2}}.$$

■

APPENDIX C: DERIVATION OF MARGINALS AND JOINT PROBABILITY DISTRIBUTIONS

This Appendix presents the derivation of an analytical formula for marginals and joint probabilities of detecting zero photons for the one-photon and two-photon protocols under nonideal assumptions: lossy transmission channels and imperfect local detection.

1. The one-photon protocol

a. Marginals

We first need to write the reduced density matrix of the subsystem A (or B) by tracing out the complementary subsystem B (or A) from the $\rho_{\text{out}}^{(k,\sigma)}$, as

$$\rho_{\text{out}}^{(a)} = \text{Tr}_B(\rho_{\text{out}}^{(k,\sigma)}) = \frac{(1 - r_t \tanh^2 g)^{\sigma+2}}{(r_t \tanh^2 g)^{\sigma}} \sum_{S=\sigma}^{\infty} (r_t \tanh^2 g)^S \sum_{n=0}^S |n\rangle \langle n| \sum_{p=\max(0, n-\sigma)}^{\min(S-\sigma, n)} \binom{n}{p} \binom{S-n}{S-\sigma-p} |\mathcal{A}_{\sigma}(k, n-p)|^2. \quad (\text{C1})$$

By changing the order of summations, shifting the indices $p \rightarrow n - p$ and $S \rightarrow S + n$, and defining $C := r_t \tanh^2 g$, we obtain

$$\begin{aligned} \rho_{\text{out}}^{(a)} &= \frac{(1-C)^{\sigma+2}}{C^{\sigma}} \sum_{p=0}^{\sigma} \binom{n}{p} |\mathcal{A}_{\sigma}(k, p)|^2 \sum_{n=p}^{\infty} C^n |n\rangle \langle n| \sum_{S=\sigma-p}^{\infty} C^S \binom{S}{\sigma-p} \\ &= (1-C) \sum_{p=0}^{\sigma} \left(\frac{1-C}{C} \right)^p |\mathcal{A}_{\sigma}(k, p)|^2 \sum_{n=p}^{\infty} \binom{n}{p} C^n |n\rangle \langle n|. \end{aligned} \quad (\text{C2})$$

In the second line, we used the identity $\sum_{S=k}^{\infty} x^S \binom{S}{k} = x^k / (1-x)^{k+1}$ from part (c) of Lemma B1. Now, by substituting reduced density matrix $\rho_{\text{out}}^{(x)}$ into $\text{Tr}(\rho_{\text{out}}^{(x)} \mathcal{M}_0)$, where x corresponds either to subsystem A or B , we can calculate the marginal probabilities:

$$P(0|\delta) = \text{Tr}(\rho_{\text{out}}^{(x)} \mathcal{M}_0) = (1-C) \sum_{p=0}^{\sigma} \left(\frac{1-C}{C} \right)^p |\mathcal{A}_{\sigma}(k, p)|^2 \sum_{n=p}^{\infty} \binom{n}{p} C^n \langle n | \mathcal{M}_0 | n \rangle$$

$$\stackrel{\text{Eq. (B5)}}{=} (1-C) e^{-\eta_d |\delta|^2} \sum_{p=0}^{\sigma} \left(\frac{1-C}{C} \right)^p |\mathcal{A}_{\sigma}(k, p)|^2 \sum_{n=p}^{\infty} \binom{n}{p} (C \eta_d^2 |\delta|^2)^n \sum_{i=0}^n \frac{\left(\frac{1-\eta_d}{\eta_d^2 |\delta|^2} \right)^i}{i!} \frac{n!}{(n-i)!^2}.$$

For the special case of $\sigma = k = 1$, corresponding to the one-photon protocol, since $|\mathcal{A}_{\sigma}(k, p)|^2 = \frac{1}{2}$, we have

$$P_{\text{1ph}}(0|\delta) = \frac{1-C}{2} e^{-\eta_d |\delta|^2} \sum_{i=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2 |\delta|^2} \right)^i}{i!} \sum_{n=i}^{\infty} \frac{(C \eta_d^2 |\delta|^2)^n n!}{(n-i)!^2} \sum_{p=0}^1 \binom{n}{p} \left(\frac{1-C}{C} \right)^p$$

$$= \frac{1-C}{2} e^{-\eta_d |\delta|^2} \sum_{i=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2 |\delta|^2} \right)^i}{i!} \sum_{n=i}^{\infty} \frac{(C \eta_d^2 |\delta|^2)^n n!}{(n-i)!(n-i)!} \left(1 + n \left(\frac{1-C}{C} \right) \right). \quad (\text{C3})$$

Using part (b) of Lemma B1, we get

$$P_{\text{1ph}}(0|\delta) = \frac{1-C}{2} e^{(C \eta_d^2 - \eta_d) |\delta|^2} \sum_{i=0}^{\infty} \frac{(C(1-\eta_d))^i}{i!} \left[\left(1 + \frac{1-C}{C} i \right) \sum_{j=0}^i \frac{i!}{j!} \binom{i}{j} (C \eta_d^2 |\delta|^2)^j + \frac{1-C}{C} \sum_{j=0}^i \frac{i!}{j!} \binom{i+1}{j+1} (C \eta_d^2 |\delta|^2)^{j+1} \right]$$

$$= \frac{1-C}{2} e^{(C \eta_d^2 - \eta_d) |\delta|^2} \sum_{j=0}^{\infty} \frac{(C \eta_d^2 |\delta|^2)^j}{j!} \sum_{i=j}^{\infty} \left[\frac{2C-1}{C} \binom{i}{j} + \left(\frac{1-C}{C} (j+1) + (1-C) \eta_d^2 |\delta|^2 \right) \binom{i+1}{j+1} \right] (C(1-\eta_d))^i. \quad (\text{C4})$$

Then, by using $\sum_{S=k}^{\infty} x^S \binom{S}{k} = x^k / (1-x)^{k+1}$ we obtain

$$P_{\text{1ph}}(0|\delta) = \frac{1-C}{2} e^{(C \eta_d^2 - \eta_d) |\delta|^2} \sum_{j=0}^{\infty} \frac{(C \eta_d^2 |\delta|^2)^j}{j!} \left[\frac{2C-1}{C} \frac{(C(1-\eta_d))^j}{(1-C(1-\eta_d))^{j+1}} + \frac{1-C}{C} (j+1 + C \eta_d^2 |\delta|^2) \frac{(C(1-\eta_d))^j}{(1-C(1-\eta_d))^{j+2}} \right]$$

$$= \frac{1-C}{2} e^{(C \eta_d^2 - \eta_d) |\delta|^2} \sum_{j=0}^{\infty} \frac{1}{j!} \left(\frac{C^2(1-\eta_d) \eta_d^2 |\delta|^2}{1-C(1-\eta_d)} \right)^j \left[\frac{2C-1}{C(1-C(1-\eta_d))} + \frac{(1-C)(1+C \eta_d^2 |\delta|^2)}{C(1-C(1-\eta_d))^2} + \frac{C(1-C)(1-\eta_d) \eta_d^2 |\delta|^2}{(1-C(1-\eta_d))^3} \right]. \quad (\text{C5})$$

Finally, by applying the series expansion of e^x and simplifying the expression, we get

$$P_{\text{1ph}}(0|\delta) = \frac{1-C}{2} \left[\frac{2(1-C(1-\eta_d))^2 - \eta_d(1-C(1-\eta_d)) + (1-C) \eta_d^2 |\delta|^2}{(1-C(1-\eta_d))^3} \right] \exp \left(- \frac{\eta_d(1-C) |\delta|^2}{1-C(1-\eta_d)} \right). \quad (\text{C6})$$

In the lossless transmission scenario, $r = 0$, by substituting $C = r_t \tanh^2 g = 0$, the expression reduces to

$$P_{\text{1ph}}(0|\delta) = \frac{2 - \eta_d + \eta_d^2 |\delta|^2}{2} e^{-\eta_d |\delta|^2}. \quad (\text{C7})$$

For the perfect detection case ($\eta_d = 1$), by replacing $C = r_t \tanh^2 g$ we obtain

$$P_{\text{1ph}}(0|\delta) = \frac{(1 - r_t \tanh^2 g)}{2} (1 + (1 - r_t \tanh^2 g) |\delta|^2) e^{-(1 - r_t \tanh^2 g) |\delta|^2}. \quad (\text{C8})$$

b. Joint probabilities

To find the joint probability distribution for the state in Eq. (A7), we need to insert it in

$$\begin{aligned}
 P(00|\alpha\beta) &= \text{Tr}[\rho_{\text{out}}^{(k,\sigma)}(D(\alpha)E_0^{\eta_d}D^\dagger(\alpha) \otimes D(\beta)E_0^{\eta_d}D^\dagger(\beta))] \\
 &= (1-C)^{\sigma+2} \sum_{p,q=0}^{\sigma} \mathcal{A}_\sigma(k,p) \mathcal{A}_\sigma^*(k,q) \left[\sum_{m=0}^{\infty} C^m \sqrt{\binom{m+p}{m} \binom{m+q}{m}} \langle m+q | \mathcal{M}_A^0 | m+p \rangle \right] \\
 &\quad \times \left[\sum_{n=0}^{\infty} C^n \sqrt{\binom{n+\sigma-p}{n} \binom{n+\sigma-q}{n}} \langle n+\sigma-q | \mathcal{M}_B^0 | n+\sigma-p \rangle \right]. \tag{C9}
 \end{aligned}$$

Using Eq. (B5), we obtain

$$\begin{aligned}
 P(00|\alpha\beta) &= e^{-\eta_d(|\alpha|^2+|\beta|^2)} \eta_d^{2\sigma} (1-C)^{\sigma+2} \sum_{p,q=0}^{\sigma} \frac{(\alpha^*)^p (\beta^*)^{\sigma-p} \mathcal{A}_\sigma(k,p)}{\sqrt{p!(\sigma-p)!}} \times \frac{\alpha^q \beta^{\sigma-q} \mathcal{A}_\sigma^*(k,q)}{\sqrt{q!(\sigma-q)!}} \\
 &\quad \times \left[\sum_{i=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\alpha|^2}\right)^i}{i!} \sum_{\substack{m \geq 0 \\ m \geq i-p \\ m \geq i-q}}^{\infty} \frac{(C\eta_d^2|\alpha|^2)^m (m+p)!(m+q)!}{m!(m+p-i)!(m+q-i)!} \right] \\
 &\quad \times \left[\sum_{j=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\beta|^2}\right)^j}{j!} \sum_{\substack{n \geq 0 \\ n \geq j+p-\sigma \\ n \geq j+q-\sigma}}^{\infty} \frac{(C\eta_d^2|\beta|^2)^n (n+\sigma-p)!(n+\sigma-q)!}{n!(n+\sigma-p-j)!(n+\sigma-q-j)!} \right]. \tag{C10}
 \end{aligned}$$

For the one-photon protocol, by setting $\sigma = k = 1$, the expression for $p(00|\alpha\beta)$ includes four terms corresponding to the possible pairs $(p, q) \in \{(0, 0), (0, 1), (1, 0), (1, 1)\}$:

$$\begin{aligned}
 P_{\text{1ph}}(00|\alpha\beta) &= e^{-\eta_d(|\alpha|^2+|\beta|^2)} \frac{\eta_d^2(1-C)^3}{2} \left[|\beta|^2 \sum_{i=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\alpha|^2}\right)^i}{i!} \sum_{m=i}^{\infty} \frac{(C\eta_d^2|\alpha|^2)^m m!}{(m-i)!(m-i)!} \times \sum_{j=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\beta|^2}\right)^j}{j!} \sum_{n=j}^{\infty} \frac{(C\eta_d^2|\beta|^2)^{n-1} n \times n!}{(n-j)!(n-j)!} \right. \\
 &\quad - i\alpha\beta^* \sum_{i=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\alpha|^2}\right)^i}{i!} \sum_{m=i}^{\infty} \frac{(C\eta_d^2|\alpha|^2)^m (m+1)!}{(m-i)!(m+1-i)!} \times \sum_{j=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\beta|^2}\right)^j}{j!} \sum_{n=j}^{\infty} \frac{(C\eta_d^2|\beta|^2)^n (n+1)!}{(n+1-j)!(n-j)!} \\
 &\quad + i\alpha^*\beta \sum_{i=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\alpha|^2}\right)^i}{i!} \sum_{m=i}^{\infty} \frac{(C\eta_d^2|\alpha|^2)^m (m+1)!}{(m+1-i)!(m-i)!} \times \sum_{j=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\beta|^2}\right)^j}{j!} \sum_{n=j}^{\infty} \frac{(C\eta_d^2|\beta|^2)^n (n+1)!}{(n-j)!(n+1-j)!} \\
 &\quad \left. + |\alpha|^2 \sum_{i=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\alpha|^2}\right)^i}{i!} \sum_{m=i}^{\infty} \frac{(C\eta_d^2|\alpha|^2)^{m-1} m \times m!}{(m-i)!(m-i)!} \times \sum_{j=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\beta|^2}\right)^j}{j!} \sum_{n=j}^{\infty} \frac{(C\eta_d^2|\beta|^2)^n n!}{(n-j)!(n-j)!} \right]. \tag{C11}
 \end{aligned}$$

By applying parts (a) and (b) of Lemma B1 to the summations over m and n , we obtain

$$\begin{aligned}
 P_{\text{1ph}}(00|\alpha\beta) &= e^{(C\eta_d^2-\eta_d)(|\alpha|^2+|\beta|^2)} \frac{\eta_d^2(1-C)^3}{2} \left[|\alpha|^2 \sum_{i=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\alpha|^2}\right)^i}{i!} \sum_{u=0}^i \frac{i!}{u!} \left[\binom{i+1}{u+1} (C\eta_d^2|\alpha|^2)^{i+u} + i \binom{i}{u} (C\eta_d^2|\alpha|^2)^{i+u-1} \right] \right. \\
 &\quad \times \sum_{j=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\beta|^2}\right)^j}{j!} \sum_{v=0}^j \binom{j}{v} \frac{j!(C\eta_d^2|\beta|^2)^{j+v}}{v!} + |\beta|^2 \sum_{i=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\alpha|^2}\right)^i}{i!} \sum_{u=0}^i \binom{i}{u} \frac{i!(C\eta_d^2|\alpha|^2)^{i+u}}{u!} \\
 &\quad \times \sum_{j=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\beta|^2}\right)^j}{j!} \sum_{v=0}^j \frac{j!}{v!} \left[\binom{j+1}{v+1} (C\eta_d^2|\beta|^2)^{j+v} + j \binom{j}{v} (C\eta_d^2|\beta|^2)^{j+v-1} \right] \\
 &\quad \left. + 2\text{Im}(\alpha\beta^*) \sum_{i=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\alpha|^2}\right)^i}{i!} \sum_{u=0}^i \binom{i+1}{u+1} \frac{i!(C\eta_d^2|\alpha|^2)^{i+u}}{u!} \times \sum_{j=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2|\beta|^2}\right)^j}{j!} \sum_{v=1}^j \binom{j+1}{v+1} \frac{j!(C\eta_d^2|\beta|^2)^{j+v}}{v!} \right], \tag{C12}
 \end{aligned}$$

where $\text{Im}(x)$ returns the imaginary part of a complex number x . Changing the order of summation yields

$$\begin{aligned}
 P_{\text{1ph}}(00|\alpha\beta) &= e^{(C\eta_d^2 - \eta_d)(|\alpha|^2 + |\beta|^2)} \frac{\eta_d^2(1-C)^3}{2} \left[|\alpha|^2 \sum_{u=0}^{\infty} \frac{(C\eta_d^2|\alpha|^2)^u}{u!} \sum_{i=u}^{\infty} (C(1-\eta_d))^i \left[\binom{i+1}{u+1} + \frac{i \binom{i}{u}}{C\eta_d^2|\alpha|^2} \right] \right. \\
 &\quad \times \sum_{v=0}^{\infty} \frac{(C\eta_d^2|\beta|^2)^v}{v!} \sum_{j=v}^{\infty} \binom{j}{v} (C(1-\eta_d))^j + |\beta|^2 \sum_{u=0}^{\infty} \frac{(C\eta_d^2|\alpha|^2)^u}{u!} \sum_{i=u}^{\infty} \binom{i}{u} (C(1-\eta_d))^i \\
 &\quad \times \sum_{v=0}^{\infty} \frac{(C\eta_d^2|\beta|^2)^v}{v!} \sum_{j=v}^{\infty} (C(1-\eta_d))^j \left[\binom{j+1}{v+1} + \frac{j \binom{j}{v}}{C\eta_d^2|\beta|^2} \right] \\
 &\quad \left. + 2 \text{Im}(\alpha\beta^*) \sum_{u=0}^{\infty} \frac{(C\eta_d^2|\alpha|^2)^u}{u!} \sum_{i=u}^{\infty} \binom{i+1}{u+1} (C(1-\eta_d))^i \times \sum_{v=0}^{\infty} \frac{(C\eta_d^2|\beta|^2)^v}{v!} \sum_{j=v}^{\infty} \binom{j+1}{v+1} (C(1-\eta_d))^j \right]. \quad (\text{C13})
 \end{aligned}$$

Next, we use parts (c) and (d) of Lemma B1 for summations over i and j :

$$\begin{aligned}
 P_{\text{1ph}}(00|\alpha\beta) &= e^{(C\eta_d^2 - \eta_d)(|\alpha|^2 + |\beta|^2)} \frac{\eta_d^2(1-C)^3}{2} \left[|\alpha|^2 \sum_{u=0}^{\infty} \frac{(C\eta_d^2|\alpha|^2)^u}{u!} \left[\frac{(C(1-\eta_d))^u}{(1-C(1-\eta_d))^{u+2}} + \frac{(C(1-\eta_d))^{u+1} + u(C(1-\eta_d))^u}{C\eta_d^2|\alpha|^2(1-C(1-\eta_d))^{u+2}} \right] \right. \\
 &\quad \times \sum_{v=0}^{\infty} \frac{(C\eta_d^2|\beta|^2)^v}{v!} \frac{(C(1-\eta_d))^v}{(1-C(1-\eta_d))^{v+1}} + |\beta|^2 \sum_{u=0}^{\infty} \frac{(C\eta_d^2|\alpha|^2)^u}{u!} \frac{(C(1-\eta_d))^u}{(1-C(1-\eta_d))^{u+1}} \\
 &\quad \times \sum_{v=0}^{\infty} \frac{(C\eta_d^2|\beta|^2)^v}{v!} \left[\frac{(C(1-\eta_d))^v}{(1-C(1-\eta_d))^{v+2}} + \frac{(C(1-\eta_d))^{v+1} + v(C(1-\eta_d))^v}{C\eta_d^2|\beta|^2(1-C(1-\eta_d))^{v+2}} \right] \\
 &\quad \left. + 2 \text{Im}(\alpha\beta^*) \sum_{u=0}^{\infty} \frac{(C\eta_d^2|\alpha|^2)^u}{u!} \frac{(C(1-\eta_d))^u}{(1-C(1-\eta_d))^{u+2}} \times \sum_{v=0}^{\infty} \frac{(C\eta_d^2|\beta|^2)^v}{v!} \frac{(C(1-\eta_d))^v}{(1-C(1-\eta_d))^{v+2}} \right]. \quad (\text{C14})
 \end{aligned}$$

Using the Taylor series expansion for $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$, the joint probability simplifies to

$$P_{\text{1ph}}(00|\alpha, \beta) = \frac{(1-C)^3}{2} \left(\frac{2(1-\eta_d)(1-C(1-\eta_d)) + \eta_d^2(|\alpha|^2 + |\beta|^2 + 2\text{Im}(\alpha\beta^*))}{(1-C(1-\eta_d))^4} \right) \exp \left(-\frac{\eta_d(1-C)(|\alpha|^2 + |\beta|^2)}{1-C(1-\eta_d)} \right). \quad (\text{C15})$$

In the lossless transmission scenario ($r = 0$), by substituting $C = r_t \tanh^2 g = 0$, the expression reduces to

$$P_{\text{1ph}}(00|\alpha\beta) = \frac{1}{2} e^{-\eta_d(|\alpha|^2 + |\beta|^2)} [2 - 2\eta_d + \eta_d^2(|\alpha|^2 + |\beta|^2 + 2\text{Im}(\alpha\beta^*))]. \quad (\text{C16})$$

For the perfect detection case ($\eta_d = 1$), replacing $C = r_t \tanh^2 g$, we obtain

$$P_{\text{1ph}}(00|\alpha\beta) = \frac{(1 - r_t \tanh^2 g)^3}{2} [|\alpha|^2 + |\beta|^2 + 2\text{Im}(\alpha\beta^*)] e^{-(|\alpha|^2 + |\beta|^2)(1 - r_t \tanh^2 g)}. \quad (\text{C17})$$

2. The two-photon protocol

For the two-photon protocol, the calculations closely follow those of the one-photon case.

a. Marginals

Since the state is not symmetric in the two-photon protocol, Alice's marginal distribution differs from Bob's. To calculate these distributions, we first determine the reduced density matrices for Alice and Bob by taking the partial trace of the state in Eq. (A19):

$$\begin{aligned}
 \rho_{\text{out}}^{(a)} &= \frac{(\mathcal{N}\mathcal{N}_b)^{-2} \sqrt{\eta_t}}{\cosh^2 g_b} \left[t_c \sum_{m=0}^{\infty} \lambda_m^{(a)} r_t^m |m\rangle \langle m|_{a_1} \times \frac{\partial}{\partial r_t} + r_c \frac{\partial}{\partial r_t} \left(\sum_{m=0}^{\infty} \lambda_m^{(a)} r_t^m |m\rangle \langle m|_{a_1} \right) \right] \\
 &\quad \times \left(\frac{\cosh^{-2} g_b}{1 - (r_s + t_s r_t) \tanh^2 g_b} - \frac{\cosh^{-2} g_b}{1 - (1 - \eta_s)(r_s + t_s r_t) \tanh^2 g_b} \right), \quad (\text{C18})
 \end{aligned}$$

$$\rho_{\text{out}}^{(b)} = (\mathcal{N}\mathcal{N}_b)^{-2} \sqrt{\eta_t} \sum_{n=0}^{\infty} \lambda_n^{(b)} (1 - (1 - \eta_s)^n) \times \left[\frac{t_c}{1 + \sqrt{\eta_t} \sinh^2 g_a} \times \frac{\partial}{\partial r_t} \left(\sum_{l=0}^n \binom{n}{l} r_s^l (r_t t_s)^{n-l} |l\rangle \langle l|_{b_1} \right) + \frac{r_c \sinh^2 g_a}{(1 + \sqrt{\eta_t} \sinh^2 g_a)^2} \times \sum_{l=0}^n \binom{n}{l} r_s^l (r_t t_s)^{n-l} |l\rangle \langle l|_{b_1} \right]. \quad (\text{C19})$$

Using a similar calculation as in the one-photon protocol, with the symmetric beam splitter in Charlie's ($t_c = r_c = 0.50$), the marginals can be obtained as follows:

$$P_{2\text{ph}}(0|\alpha) = \text{Tr}(\rho_{\text{out}}^{(a)} \mathcal{M}_0^{(A)}) = \frac{1}{2} (\mathcal{N}\mathcal{N}_b)^{-2} \sqrt{\eta_t} \left[\sum_{m=0}^{\infty} \lambda_m^{(a)} r_t^m \langle m | \mathcal{M}_0^{(A)} | m \rangle \times \frac{\partial}{\partial r_t} + \frac{\partial}{\partial r_t} \left(\sum_{m=0}^{\infty} \lambda_m^{(a)} r_t^m \langle m | \mathcal{M}_0^{(A)} | m \rangle \right) \right] \times \left(\frac{\cosh^{-2} g_b}{1 - (r_s + t_s r_t) \tanh^2 g_b} - \frac{\cosh^{-2} g_b}{1 - (1 - \eta_s)(r_s + t_s r_t) \tanh^2 g_b} \right), \quad (\text{C20})$$

$$P_{2\text{ph}}(0|\beta) = \text{Tr}(\rho_{\text{out}}^{(b)} \mathcal{M}_0^{(B)}) = \frac{1}{2} (\mathcal{N}\mathcal{N}_b)^{-2} \sqrt{\eta_t} \sum_{n=0}^{\infty} \lambda_n^{(b)} (1 - (1 - \eta_s)^n) \times \left[\frac{1}{1 + \sqrt{\eta_t} \sinh^2 g_a} \times \frac{\partial}{\partial r_t} \left(\sum_{l=0}^n \binom{n}{l} r_s^l (t_s r_t)^{n-l} \langle l | \mathcal{M}_0^{(B)} | l \rangle \right) + \frac{\sinh^2 g_a}{(1 + \sqrt{\eta_t} \sinh^2 g_a)^2} \times \sum_{l=0}^n \binom{n}{l} r_s^l (t_s r_t)^{n-l} \langle l | \mathcal{M}_0^{(B)} | l \rangle \right]. \quad (\text{C21})$$

Using Eq. (B5), $\langle m | \mathcal{M}_0 | m \rangle = e^{-\eta_d |\delta|^2} m! (\eta_d |\delta|)^{2m} \sum_{k=0}^m \frac{(\frac{1-\eta_d}{\eta_d^2 |\delta|^2})^k}{k!(m-k)!^2}$, and defining $C_{t,a(b)} := r_t \tanh^2 g_{a(b)}$, $C_{s,a(b)} := r_s \tanh^2 g_{a(b)}$, we get

$$\begin{aligned} \sum_{m=0}^{\infty} \lambda_m^{(a)} r_t^m \langle m | \mathcal{M}_0^{(A)} | m \rangle &= \cosh^{-2} g_a e^{-\eta_d |\alpha|^2} \sum_{k=0}^{\infty} \frac{(\frac{1-\eta_d}{\eta_d^2 |\alpha|^2})^k}{k!} \sum_{m=k}^{\infty} \frac{m! (C_{t,a} \eta_d^2 |\alpha|^2)^m}{(m-k)!^2} \\ &\stackrel{(a)}{=} \cosh^{-2} g_a e^{-\eta_d |\alpha|^2} e^{C_{t,a} \eta_d^2 |\alpha|^2} \sum_{i=0}^{\infty} \frac{(C_{t,a} \eta_d^2 |\alpha|^2)^i}{i!} \sum_{k=i}^{\infty} \binom{k}{i} (C_{t,a} (1 - \eta_d))^k \\ &\stackrel{(c)}{=} \cosh^{-2} g_a e^{-\eta_d |\alpha|^2} e^{C_{t,a} \eta_d^2 |\alpha|^2} \sum_{i=0}^{\infty} \frac{(C_{t,a} \eta_d^2 |\alpha|^2)^i}{i!} \frac{(C_{t,a} (1 - \eta_d))^i}{(1 - C_{t,a} (1 - \eta_d))^{i+1}} \\ &= \frac{\cosh^{-2} g_a}{1 - C_{t,a} (1 - \eta_d)} \exp \left(-\frac{\eta_d (1 - C_{t,a}) |\alpha|^2}{1 - C_{t,a} (1 - \eta_d)} \right), \end{aligned} \quad (\text{C22})$$

$$\begin{aligned} \sum_{n=0}^{\infty} \lambda_n^{(b)} (1 - (1 - \eta_s)^n) \sum_{l=0}^n \binom{n}{l} r_s^l (t_s r_t)^{n-l} \langle l | \mathcal{M}_0^{(B)} | l \rangle \\ \stackrel{\text{Eq. (B5)}}{=} \cosh^{-2} g_b e^{-\eta_d |\beta|^2} \sum_{k=0}^{\infty} \frac{(\frac{1-\eta_d}{\eta_d^2 |\beta|^2})^k}{k!} \sum_{l=k}^{\infty} \frac{l! (\frac{r_s \eta_d^2 |\beta|^2}{t_s r_t})^l}{(l-k)!^2} \sum_{n=l}^{\infty} \binom{n}{l} (C_{t,b} t_s)^n (1 - (1 - \eta_s)^n) \\ \stackrel{(c)}{=} \cosh^{-2} g_b e^{-\eta_d |\beta|^2} \sum_{k=0}^{\infty} \frac{(\frac{1-\eta_d}{\eta_d^2 |\beta|^2})^k}{k!} \sum_{l=k}^{\infty} \frac{l! (\frac{r_s \eta_d^2 |\beta|^2}{t_s r_t})^l}{(l-k)!^2} \left[\frac{(C_{t,b} t_s)^l}{(1 - C_{t,b} t_s)^{l+1}} - \frac{(C_{t,b} t_s (1 - \eta_s))^l}{(1 - C_{t,b} t_s (1 - \eta_s))^{l+1}} \right] \\ \stackrel{(a)}{=} \cosh^{-2} g_b e^{-\eta_d |\beta|^2} \left[\frac{e^{\frac{C_{s,b} \eta_d^2 |\beta|^2}{1 - C_{t,b} t_s}}}{1 - C_{t,b} t_s} \sum_{i=0}^{\infty} \frac{(\frac{C_{s,b} \eta_d^2 |\beta|^2}{1 - C_{t,b} t_s})^i}{i!} \sum_{k=i}^{\infty} \binom{k}{i} \left(\frac{C_{s,b} (1 - \eta_d)}{1 - C_{t,b} t_s} \right)^k \right. \\ \left. - \frac{e^{\frac{C_{s,b} \eta_d^2 |\beta|^2 (1 - \eta_s)}{1 - C_{t,b} t_s (1 - \eta_s)}}}{1 - C_{t,b} t_s (1 - \eta_s)} \sum_{i=0}^{\infty} \frac{(\frac{C_{s,b} \eta_d^2 |\beta|^2 (1 - \eta_s)}{1 - C_{t,b} t_s (1 - \eta_s)})^i}{i!} \sum_{k=i}^{\infty} \binom{k}{i} \left(\frac{C_{s,b} (1 - \eta_d) (1 - \eta_s)}{1 - C_{t,b} t_s (1 - \eta_s)} \right)^k \right] \\ \stackrel{(c)}{=} \cosh^{-2} g_b e^{-\eta_d |\beta|^2} \left[\frac{e^{\frac{C_{s,b} \eta_d^2 |\beta|^2}{1 - C_{t,b} t_s}}}{1 - C_{t,b} t_s - C_{s,b} (1 - \eta_d)} \sum_{i=0}^{\infty} \frac{(\frac{C_{s,b} (1 - \eta_d) \eta_d^2 |\beta|^2}{(1 - C_{t,b} t_s)(1 - C_{t,b} t_s - C_{s,b} (1 - \eta_d))})^i}{i!} \right. \end{aligned}$$

$$\begin{aligned}
& - \frac{e^{\frac{C_{s,b} \eta_d^2 |\beta|^2 (1-\eta_s)}{1-C_{t,b} t_s (1-\eta_s)}}}{1 - (C_{t,b} t_s + C_{s,b} (1 - \eta_d))(1 - \eta_s)} \sum_{i=0}^{\infty} \frac{\left(\frac{C_{s,b}^2 (1-\eta_d) \eta_d^2 |\beta|^2 (1-\eta_s)^2}{(1-C_{t,b} t_s (1-\eta_s))(1-(C_{t,b} t_s + C_{s,b} (1-\eta_d))(1-\eta_s))} \right)^i}{i!} \Bigg] \\
& = \cosh^{-2} g_b \left[\frac{\exp \left(- \frac{\eta_d (1-C_{t,b} t_s - C_{s,b}) |\beta|^2}{1-C_{t,b} t_s - C_{s,b} (1-\eta_d)} \right)}{1 - C_{t,b} t_s - C_{s,b} (1-\eta_d)} - \frac{\exp \left(- \frac{\eta_d (1-(C_{t,b} t_s + C_{s,b} (1-\eta_d)) |\beta|^2}{1-(C_{t,b} t_s + C_{s,b} (1-\eta_d))(1-\eta_s)} \right)}{1 - (C_{t,b} t_s + C_{s,b} (1-\eta_d))(1-\eta_s)} \right], \quad (\text{C23})
\end{aligned}$$

where we applied parts (a) and (c) of Lemma B1, and used the Taylor expansion of e^x to simplify the expression. Substituting Eqs. (C22) and (C23) into Eqs. (C20) and (C21) then yields the marginals $P_{2\text{ph}}(0|\alpha)$ and $P_{2\text{ph}}(0|\beta)$, respectively. In the limit $g_b \ll 1$, where Bob's initial state approaches the SPPE state, the marginals are given by

$$\begin{aligned}
\tilde{P}_{2\text{ph}}(0|\alpha) &= \exp \left(- \frac{(1 - C_{t,a}) \eta_d |\alpha|^2}{1 - C_{t,a} (1 - \eta_d)} \right) \times \left(\frac{1 - C_{t,a}}{1 - C_{t,a} (1 - \eta_d)} \right)^2 \times \frac{t_s \left(1 + \frac{C_{t,a} \eta_d^2 |\alpha|^2}{1 - C_{t,a} (1 - \eta_d)} \right) + C_{s,a} \left(1 - \eta_d + \frac{\eta_d^2 |\alpha|^2}{1 - C_{t,a} (1 - \eta_d)} \right)}{t_s + r_s \tanh^2(g_a)}, \\
\tilde{P}_{2\text{ph}}(0|\beta) &= e^{-\eta_d |\beta|^2} \times \frac{t_s + C_{s,a} (1 - \eta_d + \eta_d^2 |\beta|^2)}{t_s + r_s \tanh^2 g_a}.
\end{aligned}$$

b. Joint probabilities

The joint probability distribution corresponding to the state in Eq. (A19) is obtained from $\text{Tr}[\rho_{\text{out}}^{(2\text{ph})}(\mathcal{M}_0^{(A)} \otimes \mathcal{M}_0^{(B)})]$. For a symmetric BS at Charlie's ($t_c = r_c = 0.50$), this probability is calculated as

$$\begin{aligned}
P_{2\text{ph}}(00|\alpha, \beta) &= \frac{1}{2} (\mathcal{N} \mathcal{N}_b)^{-2} \sqrt{\eta_t} \sum_{n=0}^{\infty} \lambda_n^{(b)} (1 - (1 - \eta_s)^n) \left[\sum_{m=0}^{\infty} \lambda_m^{(a)} r_t^m \langle m | \mathcal{M}_0^{(A)} | m \rangle \times \frac{\partial}{\partial r_t} \left(\sum_{l=0}^n \binom{n}{l} r_s^l (r_t t_s)^{n-l} \langle l | \mathcal{M}_0^{(B)} | l \rangle \right) \right. \\
&+ \frac{\partial}{\partial r_t} \left(\sum_{m=0}^{\infty} \lambda_m^{(a)} r_t^m \langle m | \mathcal{M}_0^{(A)} | m \rangle \right) \times \sum_{l=0}^n \binom{n}{l} r_s^l (r_t t_s)^{n-l} \langle l | \mathcal{M}_0^{(B)} | l \rangle \\
&+ \left. 2 \sqrt{\frac{t_s}{r_s}} \text{Re} \left(e^{i\phi} \sum_{m=0}^{\infty} \sqrt{\lambda_m^{(a)} \lambda_{m+1}^{(a)}} (m+1) r_t^m \langle m+1 | \mathcal{M}_0^{(A)} | m \rangle \times \sum_{l=1}^n \sqrt{l} \binom{n}{l} r_s^l (r_t t_s)^{n-l} \langle l | \mathcal{M}_0^{(B)} | l-1 \rangle \right) \right], \quad (\text{C24})
\end{aligned}$$

which consists of three terms: The first two can be obtained from Eqs. (C22) and (C23), while for the last term we have

$$\begin{aligned}
& \sum_{m=0}^{\infty} \sqrt{\lambda_m^{(a)} \lambda_{m+1}^{(a)}} (m+1) r_t^m \langle m+1 | \mathcal{M}_0^{(A)} | m \rangle \stackrel{\text{Eq. (B5)}}{=} \frac{\eta_d \alpha \tanh g_a}{\cosh^2 g_a} e^{-\eta_d |\alpha|^2} \sum_{i=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2 |\alpha|^2} \right)^i}{i!} \sum_{m=i}^{\infty} \frac{(m+1)! (C_{t,a} \eta_d^2 |\alpha|^2)^m}{(m+1-i)! (m-i)!} \\
& \stackrel{(a)}{=} \frac{\eta_d \alpha \tanh g_a}{\cosh^2 g_a} e^{-\eta_d |\alpha|^2} e^{C_{t,a} \eta_d^2 |\alpha|^2} \sum_{i=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2 |\alpha|^2} \right)^i}{i!} \sum_{j=0}^i \frac{i! (i+1)! (C_{t,a} \eta_d^2 |\alpha|^2)^{i+j}}{j! (j+1)! (i-j)!} \\
& = \frac{\eta_d \alpha \tanh g_a}{\cosh^2 g_a} e^{(C_{t,a} \eta_d^2 - \eta_d) |\alpha|^2} \sum_{j=0}^{\infty} \frac{(C_{t,a} \eta_d^2 |\alpha|^2)^j}{j!} \sum_{i=j}^{\infty} \binom{i+1}{j+1} (C_{t,a} (1 - \eta_d))^i \\
& \stackrel{(c)}{=} \frac{\eta_d \alpha \tanh g_a}{\cosh^2 g_a} e^{(C_{t,a} \eta_d^2 - \eta_d) |\alpha|^2} \sum_{j=0}^{\infty} \frac{(C_{t,a} \eta_d^2 |\alpha|^2)^j}{j!} \frac{(C_{t,a} (1 - \eta_d))^j}{(1 - C_{t,a} (1 - \eta_d))^{j+2}} \\
& = \frac{\eta_d \alpha \tanh g_a \cosh^{-2} g_a}{(1 - C_{t,a} (1 - \eta_d))^2} \exp \left(- \frac{\eta_d (1 - C_{t,a}) |\alpha|^2}{1 - C_{t,a} (1 - \eta_d)} \right), \quad (\text{C25}) \\
& \sum_{n=0}^{\infty} \lambda_n^{(b)} (1 - (1 - \eta_s)^n) \sum_{l=1}^n \sqrt{l} \binom{n}{l} r_s^l (r_t t_s)^{n-l} \langle l | \mathcal{M}_0^{(B)} | l-1 \rangle \\
& \stackrel{\text{Eq. (B5)}}{=} \frac{e^{-\eta_d |\beta|^2}}{\eta_d \beta^* \cosh^2 g_b} \sum_{k=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2 |\beta|^2} \right)^k}{k!} \sum_{l=k+1}^{\infty} \frac{l! \left(\frac{r_s \eta_d^2 |\beta|^2}{t_s r_t} \right)^l}{(l-k)! (l-k-1)!} \sum_{n=l}^{\infty} \binom{n}{l} (C_{t,b} t_s)^n (1 - (1 - \eta_s)^n) \\
& \stackrel{(c)}{=} \frac{e^{-\eta_d |\beta|^2}}{\eta_d \beta^* \cosh^2 g_b} \sum_{k=0}^{\infty} \frac{\left(\frac{1-\eta_d}{\eta_d^2 |\beta|^2} \right)^k}{k!} \sum_{l=k}^{\infty} \frac{l! \left(\frac{r_s \eta_d^2 |\beta|^2}{t_s r_t} \right)^l}{(l-k)! (l-k-1)!} \left[\frac{(C_{t,b} t_s)^l}{(1 - C_{t,b} t_s)^{l+1}} - \frac{(C_{t,b} t_s (1 - \eta_s))^l}{(1 - C_{t,b} t_s (1 - \eta_s))^{l+1}} \right]
\end{aligned}$$

$$\begin{aligned}
& \stackrel{(a)}{=} \frac{\eta_d \beta e^{-\eta_d |\beta|^2}}{(1 - \eta_d) \cosh^2 g_b} \left[\frac{e^{\frac{C_{s,b} \eta_d^2 |\beta|^2}{1 - C_{t,b} t_s}}}{1 - C_{t,b} t_s} \sum_{i=0}^{\infty} \frac{\left(\frac{C_{s,b} \eta_d^2 |\beta|^2}{1 - C_{t,b} t_s} \right)^i}{i!} \sum_{k=i}^{\infty} \binom{k+1}{i+1} \left(\frac{C_{s,b}(1 - \eta_d)}{1 - C_{t,b} t_s} \right)^{k+1} \right. \\
& \quad \left. - \frac{e^{\frac{C_{s,b} \eta_d^2 |\beta|^2 (1 - \eta_s)}{1 - C_{t,b} t_s (1 - \eta_s)}}}{1 - C_{t,b} t_s (1 - \eta_s)} \sum_{i=0}^{\infty} \frac{\left(\frac{C_{s,b} \eta_d^2 |\beta|^2 (1 - \eta_s)}{1 - C_{t,b} t_s (1 - \eta_s)} \right)^i}{i!} \sum_{k=i}^{\infty} \binom{k+1}{i+1} \left(\frac{C_{s,b}(1 - \eta_d)(1 - \eta_s)}{1 - C_{t,b} t_s (1 - \eta_s)} \right)^{k+1} \right] \\
& \stackrel{(c)}{=} \frac{C_{s,b} \eta_d \beta e^{-\eta_d |\beta|^2}}{\cosh^2 g_b} \left[\frac{e^{\frac{C_{s,b} \eta_d^2 |\beta|^2}{1 - C_{t,b} t_s}}}{(1 - C_{t,b} t_s - C_{s,b}(1 - \eta_d))^2} \sum_{i=0}^{\infty} \frac{\left(\frac{C_{s,b}^2 (1 - \eta_d) \eta_d^2 |\beta|^2}{(1 - C_{t,b} t_s)(1 - C_{t,b} t_s - C_{s,b}(1 - \eta_d))} \right)^i}{i!} \right. \\
& \quad \left. - \frac{e^{\frac{C_{s,b} \eta_d^2 |\beta|^2 (1 - \eta_s)}{1 - C_{t,b} t_s (1 - \eta_s)}}}{(1 - (C_{t,b} t_s + C_{s,b}(1 - \eta_d))(1 - \eta_s))^2} \sum_{i=0}^{\infty} \frac{\left(\frac{C_{s,b}^2 (1 - \eta_d) \eta_d^2 |\beta|^2 (1 - \eta_s)}{(1 - C_{t,b} t_s (1 - \eta_s))(1 - (C_{t,b} t_s + C_{s,b}(1 - \eta_d))(1 - \eta_s))} \right)^i}{i!} \right] \\
& = \frac{C_{s,b} \eta_d \beta e^{-\eta_d |\beta|^2}}{\cosh^2 g_b} \left[\frac{\exp\left(\frac{C_{s,b} \eta_d^2 |\beta|^2}{1 - C_{t,b} t_s - C_{s,b}(1 - \eta_d)}\right)}{(1 - C_{t,b} t_s - C_{s,b}(1 - \eta_d))^2} - \frac{\exp\left(\frac{C_{s,b} \eta_d^2 |\beta|^2}{1 - (C_{t,b} t_s + C_{s,b}(1 - \eta_d))(1 - \eta_s)}\right)}{(1 - (C_{t,b} t_s + C_{s,b}(1 - \eta_d))(1 - \eta_s))^2} \right]. \tag{C26}
\end{aligned}$$

For an SPPE initial state at Bob's station ($g_b \ll 1$), the joint probability takes the form

$$\begin{aligned}
\tilde{P}_{2\text{ph}}(00|\alpha, \beta) = & \frac{\exp\left(-\frac{(1-C)\eta_d|\alpha|^2}{1-C(1-\eta_d)} - \eta_d|\beta|^2\right)(1-C)^2}{(t_s + r_s \tanh^2 g)(1 - C(1 - \eta_d))^2} \left[t_s \left(1 + \frac{C\eta_d^2|\alpha|^2}{1 - C(1 - \eta_d)} \right) \right. \\
& \left. + r_s \tanh^2 g \left(1 - \eta_d + \frac{\eta_d^2|\alpha|^2}{1 - C(1 - \eta_d)} \right) (1 - \eta_d + \eta_d^2|\beta|^2) + 2\eta_d^2 \tanh g \sqrt{t_s r_s} \text{Re}(e^{i\phi} \alpha \beta) \right].
\end{aligned}$$

APPENDIX D: VISIBILITY BETWEEN TWO SPDCs

In this Appendix, we analyze the effect of visibility between two SPDC outputs on the CHSH value and the secure key rate of the protocols. Let $\hat{a}_\omega^\dagger$ be the creation operator of a photon with frequency ω , satisfying the continuous-mode commutation relation $[\hat{a}_\omega, \hat{a}_{\omega'}^\dagger] = \delta(\omega - \omega')$. Considering the spectral modes, the output of an SPDC generates spectrally correlated photons in the following form:

$$|\psi\rangle_{\text{SPDC}} = \sqrt{\lambda_0}|00\rangle + \sqrt{\lambda_1} \int d\omega_i d\omega_s F(\omega_i, \omega_s) a_{\omega_i}^\dagger a_{\omega_s}^\dagger |00\rangle + \dots, \tag{D1}$$

where $F(\omega_i, \omega_s) \propto \exp\left[-\frac{(\omega_i + \omega_s - 2\mu)^2}{2\sigma_p}\right] \text{sinc}\left[\frac{L\Delta k}{2}\right]$ is the joint spectral amplitudes (JSA) [47] of the outputs, $\text{sinc}(x) = \sin x/x$, and L is the crystal length. In this relation, $\Delta k = k_i(\omega_i) + k_s(\omega_s) - k_p(\omega_i + \omega_s)$ and k is the wave number, σ_p is bandwidth, and μ is variance of pump pulse. Under specific conditions of $\frac{2}{\sigma^2} + \gamma L^2(k'_s - k'_p)(k'_i - k'_p) = 0$ [47], which occurs for SPDC crystals of a certain length, JSA functions become separable, and the state produced by SPDC can be written as

$$|\psi\rangle_{\text{SPDC}} = \sum_{n=0}^{\infty} \sqrt{\lambda_n} \left[\frac{1}{\sqrt{n!}} \bigotimes_{i=1}^n \int d\omega_i f_1(\omega_i) a_{\omega_i}^\dagger |0\rangle \right]_1 \otimes \left[\frac{1}{\sqrt{n!}} \bigotimes_{i=1}^n \int d\omega_i f_2(\omega_i) a_{\omega_i}^\dagger |0\rangle \right]_2 = \sum_{n=0}^{\infty} \sqrt{\lambda_n} |n\rangle_f \otimes |n\rangle_f, \tag{D2}$$

where we defined the corresponding n -photon wave packet state characterized by $f(\omega)$ as $|n\rangle_f := \frac{(\hat{A}_f^\dagger)^n}{\sqrt{n!}} |0\rangle$, with the creation operator for a single photon in a wave packet given by $\hat{A}_f^\dagger = \int d\omega f(\omega) \hat{a}_\omega^\dagger$.

1. The one-photon protocol

We consider two SPDC sources at Alice's and Bob's stations, producing photons with separable JSA functions $f(\omega)$ and $g(\omega)$, respectively. To evaluate Hong-Ou-Mandel (HOM) visibility at Charlie's, defined as $V := |v|^2$, with visibility amplitude $v := \int f^*(\omega) g(\omega) d\omega$, the beams must interfere in a HOM interferometer [47]. The projector for a detector that perfectly distinguishes single-photon events without revealing any frequency information about the photon is given by [48]

$$\Pi = \int d\omega a_\omega^\dagger |0\rangle \langle 0| a_\omega. \tag{D3}$$

Accordingly, Charlie's POVM, incorporating his 50:50 beam splitter, can be written as

$$\Pi_{\text{BS}}^{(c)} = \frac{1}{2} \int_{-\infty}^{\infty} d\omega (a_\omega^\dagger - i b_\omega^\dagger) |00\rangle \langle 00| (a_\omega + i b_\omega) = \frac{1}{2} \int_{-\infty}^{\infty} d\omega (|1_\omega 0\rangle - i |0 1_\omega\rangle) (\langle 1_\omega 0| + i \langle 0 1_\omega|), \tag{D4}$$

with $a_\omega(b_\omega)$ and $a_\omega^\dagger(b_\omega^\dagger)$ the annihilation and creation operators, respectively, acting on the idler mode received from Alice (Bob). To find the impact of the visibility of two beams arriving at Charlie's station on the final state shared between Alice and Bob, we begin by writing the state generated by their SPDC sources:

$$\rho_{\text{in}} = \sum_{n,n',m,m'=0}^{\infty} \sqrt{\lambda_n \lambda_{n'} \lambda_m \lambda_{m'}} \sum_{p=0}^{\min(n,n')} \sum_{q=0}^{\min(m,m')} \sqrt{\binom{n}{p} \binom{n'}{p} \binom{m}{q} \binom{m'}{q}} (1-r)^{n+n'+m+m'-2(p+q)} r^{2(p+q)} \\ \times [|n\rangle \langle n'|_f \otimes |m\rangle \langle m'|_g]_{a_1, b_1} \times [|n-p\rangle \langle n'-p|_f \otimes |m-q\rangle \langle m'-q|_g]_{a_2, b_2}, \quad (\text{D5})$$

where transmission losses are modeled by a BS with reflectivity r , and p and q indicate the number of photons lost in the idler beams. For simplicity, we focus on the idler beams and rewrite the state as below:

$$\rho_{\text{in}} = \sum_{n,n',m,m',p,q} \mathcal{F}_{m,n,m',n',p,q}^{(a_1, b_1)} \times [|n-p\rangle \langle n'-p|_f \otimes |m-q\rangle \langle m'-q|_g]_{a_2, b_2}, \quad (\text{D6})$$

with $\mathcal{F}_{m,n,m',n',p,q}^{(a_1, b_1)}$ containing all the coefficients and terms associated with the signal beams, i.e., a_1, b_1 . To calculate the shared density matrix after Charlie's measurement, we need to apply his POVM on this state:

$$\rho_{\text{out}} = \text{Tr}_{c_1 c_2} (\Pi_{\text{BS}}^{(c)} \rho_{\text{in}}) = \frac{1}{2} \sum_{n,n',m,m',p,q} \mathcal{F}_{m,n,m',n',p,q}^{(a_1, b_1)} \int d\omega \langle 00 | (\alpha_\omega + i\beta_\omega) | n-p \rangle_f | m-q \rangle_g \times \langle n'-p |_f \langle m'-q |_g (\alpha_\omega^\dagger - i\beta_\omega^\dagger) | 00 \rangle \\ = \frac{1}{2} \sum_{n,n',m,m',p,q} \mathcal{F}_{m,n,m',n',p,q}^{(a_1, b_1)} \int d\omega ((f(\omega)\delta_{n,p+1}\delta_{m,q} + ig(\omega)\delta_{n,p}\delta_{m,q+1})(f^*(\omega)\delta_{n',p+1}\delta_{m',q} - ig^*(\omega)\delta_{n',p}\delta_{m',q+1}) \\ = \frac{1}{2} \sum_{n,n',m,m',p,q} \mathcal{F}_{m,n,m',n',p,q}^{(a_1, b_1)} (\delta_{n,n',p+1}\delta_{m,m',q} + \delta_{n,n',p}\delta_{m,m',q+1} + i v^* \delta_{n,n'-1,p}\delta_{m-1,m',q} - i v \delta_{n-1,n',p}\delta_{m,m'-1,q}). \quad (\text{D7})$$

Applying the δ functions to $\mathcal{F}_{m,n,m',n',p,q}^{(a_1, b_1)}$ reproduces the density matrix given in Eq. (A8), where v appears exclusively in the off-diagonal components. Consequently, the visibility amplitude v enters into the joint probabilities of Alice and Bob as follows, while leaving the marginal distributions unaffected:

$$P_{\text{1ph}}^v(00|\alpha, \beta) = \frac{(1-C)^3}{2} \left(\frac{2(1-\eta)(1-C(1-\eta)) + \eta^2(|\alpha|^2 + |\beta|^2 + 2\text{Im}(v\alpha\beta^*))}{(1-C(1-\eta))^4} \right) \exp\left(-\frac{(1-C)\eta(|\alpha|^2 + |\beta|^2)}{1-C(1-\eta)}\right).$$

2. The two-photon protocol

For the two-photon protocol, a similar analysis reveals that visibility affects the state in Eq. (A19) in the same way; that is, v appears exclusively in off-diagonal terms and consequently modifies only the joint probabilities as follows:

$$\tilde{P}_{\text{2ph}}^v(00|\alpha, \beta) = \frac{\exp\left(-\frac{(1-C)\eta|\alpha|^2}{1-C(1-\eta)} - \eta|\beta|^2\right)(1-C)^2}{(t_s + r_s \tanh^2 g)(1-C(1-\eta))^2} \left[t_s \left(1 + \frac{C\eta^2|\alpha|^2}{1-C(1-\eta)} \right) \right. \\ \left. + r_s \tanh^2 g \left(1 - \eta + \frac{\eta^2|\alpha|^2}{1-C(1-\eta)} \right) (1 - \eta + \eta^2|\beta|^2) + 2\eta^2 \tanh g \sqrt{t_s r_s} \text{Im}(v\alpha\beta^*) \right].$$

APPENDIX E: LOCAL VISIBILITY BETWEEN STATE AND MEASUREMENT

Here, we study the impact of local visibility between the photons in the quantum state and those involved in the measurement. Compared to our previous calculation, the only modification appears in the effective local measurement operators $\mathcal{M}_0^{(A)}$ and $\mathcal{M}_0^{(B)}$, and the shared state between Alice and Bob remains unchanged. The marginals and joint probability distributions can be calculated using

$$P(0|\delta) = \text{Tr}(\rho_{\text{out}}^{(x)} \mathcal{M}_0) = \sum_{n,n'=0}^{\infty} (\rho_{\text{out}}^{(x)})_{n'n} \langle n|_{f_x} \mathcal{M}_0 | n' \rangle_{f_x}, \quad (\text{E1})$$

$$P(00|\alpha\beta) = \text{Tr}[\rho_{\text{out}}^{(ab)} (\mathcal{M}_0^{(A)} \otimes \mathcal{M}_0^{(B)})] = \sum_{\substack{n,n'=0 \\ m,m'=0}}^{\infty} (\rho_{\text{out}}^{(ab)})_{n'm'} \langle n|_{f_a} \mathcal{M}_0^{(A)} | n' \rangle_{f_a} \langle m|_{f_b} \mathcal{M}_0^{(B)} | m' \rangle_{f_b}, \quad (\text{E2})$$

where $\mathcal{M}_0 := D_g(\delta)E_0^{\eta_d}D_g^\dagger(\delta)$ consists of the no-click POVM $E_0^{\eta_d} = \sum_{m=0}^{\infty} (1 - \eta_d)^m \hat{\Pi}_m$ in the presence of a displacement operator $D_g(\alpha)$, defined in a mode with normalized spectral amplitude $g(\omega)$. We now compute the matrix elements of $\mathcal{M}_0$ in the Fock state basis $|n\rangle_f$, characterized by the normalized spectral amplitude $f(\omega)$.

The displacement operator $D_g(\alpha)$ acts on a specific mode with spectral amplitude $g(\omega)$, which can be expressed as

$$D_g(\alpha) = \exp(\alpha \hat{A}_g^\dagger - \alpha^* \hat{A}_g). \quad (\text{E3})$$

By utilizing the fact that any two normalized functions $f(\omega)$ and $g(\omega)$ in the Hilbert space $L^2(\mathbb{R})$ span a two-dimensional subspace, we decompose the function f into a component parallel to the displacement mode g and an orthogonal “dark” component $g^\perp$ via the Gram-Schmidt process:

$$f(\omega) = v g(\omega) + u g^\perp(\omega) \Rightarrow \hat{A}_f^\dagger = v^* \hat{A}_g^\dagger + u \hat{A}_{g^\perp}^\dagger, \quad (\text{E4})$$

where $v = \int f^*(\omega)g(\omega)d\omega$ is the spectral overlap integral and $|u| = \sqrt{1 - |v|^2}$. Using this decomposition, the initial state $|n\rangle_f$ can be expanded in terms of the number of photons in these two orthogonal modes:

$$|n\rangle_f = \frac{(\hat{A}_f^\dagger)^n}{\sqrt{n!}}|0\rangle = \frac{(v\hat{A}_g^\dagger + u\hat{A}_{g^\perp}^\dagger)^n}{\sqrt{n!}}|0\rangle = \sum_{p=0}^n \sqrt{\binom{n}{p}} v^{n-p} u^p |n-p\rangle_g |p\rangle_{g^\perp}. \quad (\text{E5})$$

The displacement operator $D_g^\dagger(\alpha)$ acts exclusively on the g mode, leaving the orthogonal mode $g^\perp$ unchanged:

$$D_g^\dagger(\alpha)|n\rangle_f = \sum_{p=0}^n \sqrt{\binom{n}{p}} v^{n-p} u^p (D_g^\dagger(\alpha)|n-p\rangle_g) |p\rangle_{g^\perp}. \quad (\text{E6})$$

For a mode-blind detector, which clicks for any photon regardless of its frequency, the detection of m photons mathematically defined as a projection operator $\hat{\Pi}_m$ onto the subspace where the sum of photons across all modes equals m is

$$\hat{\Pi}_m = \sum_{j=0}^m |m-j\rangle_g |j\rangle_{g^\perp} \langle m-j|_g \langle j|_{g^\perp}. \quad (\text{E7})$$

Combining Eqs. (E6) and (E7) yields the matrix elements of $\mathcal{M}_0$ as

$$\begin{aligned} \langle n|_f \mathcal{M}_0 |n'\rangle_f &= \sum_{m=0}^{\infty} (1 - \eta_d)^m \langle n|_f D_g(\delta) \hat{\Pi}_m D_g^\dagger(\delta) |n'\rangle_f \\ &= \sum_{m=0}^{\infty} (1 - \eta_d)^m \left[\sum_{p=0}^n \sqrt{\binom{n}{p}} (v^*)^{n-p} (u^*)^p \langle n-p|_g D_g(\alpha) |p\rangle_{g^\perp} \right] \\ &\quad \times \left[\sum_{j=0}^m |m-j\rangle_g |j\rangle_{g^\perp} \langle m-j|_g \langle j|_{g^\perp} \right] \left[\sum_{p'=0}^{n'} \sqrt{\binom{n'}{p'}} v^{n'-p'} u^{p'} (D_g^\dagger(\alpha) |n'-p'\rangle_g) |p'\rangle_{g^\perp} \right] \\ &= \sum_{m=0}^{\infty} (1 - \eta_d)^m \sum_{j=0}^{\min(m, n, n')} \sqrt{\binom{n}{j} \binom{n'}{j}} (v^*)^{n-j} v^{n'-j} |u|^{2j} \langle n-j|_g D_g(\alpha) |m-j\rangle_g \langle m-j|_g D_g^\dagger(\alpha) |n'-j\rangle_g, \end{aligned} \quad (\text{E8})$$

where in the last line we used the identities $\langle p|j\rangle_{g^\perp} = \delta_{p,j}$ and $\langle p'|j\rangle_{g^\perp} = \delta_{p',j}$. The single-mode matrix element $\langle n-j|D(\alpha)|m-j\rangle$ can be evaluated using the normal-ordered expansion of the displacement operator, as derived in Eq. (B3):

$$\langle n-j|_g D_g(\alpha) |m-j\rangle_g = e^{-\frac{|\alpha|^2}{2}} \sum_{k=j}^{\min(n, m)} \frac{\sqrt{(n-j)!(m-j)!} \alpha^{n-k} (-\alpha^*)^{m-k}}{(n-k)!(m-k)!(k-j)!}. \quad (\text{E9})$$

By performing similar calculation as in Eq. (B5), we get

$$\langle n|_f \mathcal{M}_0 |n'\rangle_f = e^{-\eta_d |\delta|^2} \sqrt{n!n'} \eta_d^{n+n'} (v^* \delta)^n (v \delta^*)^{n'} \sum_{j=0}^{\min(n, n')} \frac{|u|^{2j}}{j!} \sum_{i=j}^{\min(n, n')} \frac{\left(\frac{1-\eta_d}{\eta_d^2 |\delta|^2}\right)^i}{i!(n-i)!(n'-i)!}. \quad (\text{E10})$$

In the limit of perfect matching ($V = 1$), the only nonzero term corresponds to $j = 0$, for which the above expression

reduces to Eq. (B5). To find the probability distributions, one needs to substitute Eq. (E10) into Eqs. (E1) and (E2).

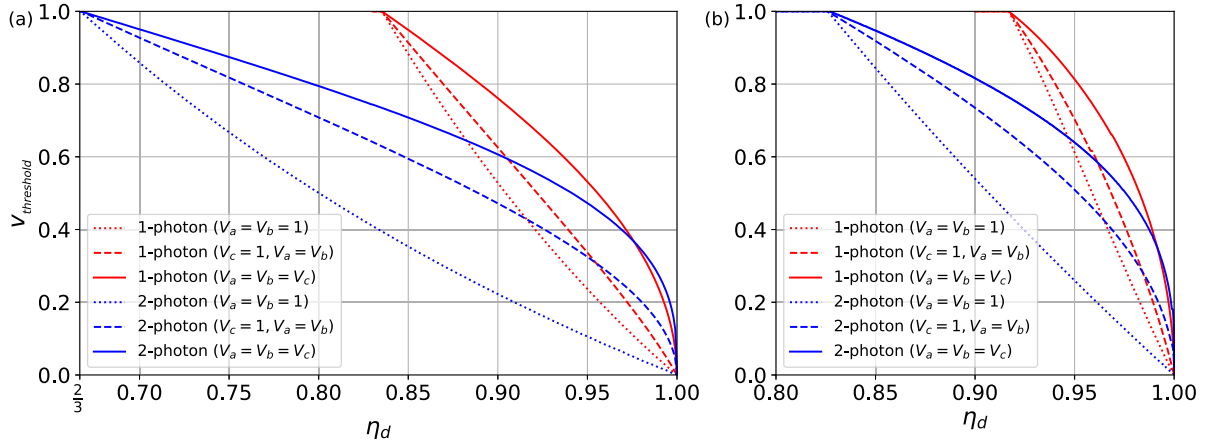


FIG. 5. Required visibility (a) to violate the CHSH inequality and (b) to achieve a positive SKR as a function of detection efficiency, shown for the one-photon (red) and two-photon (blue) protocols. Solid lines correspond to imperfect visibility in all laboratories ($V_a = V_b = V_c < 1$), while the dashed line assumed the perfect visibility in Charlie's laboratory ($V_c = 1$), and in the dotted line correspond to perfect visibility in the local laboratories ($V_a = V_b = 1$).

Figure 5 illustrates how the required visibility threshold varies with detection efficiency for the two protocols. Specifically, panel (a) shows the required visibility to violate the CHSH inequality at each detection efficiency, while panel (b) shows the thresholds needed to achieve a positive SKR for both the one-photon and two-photon cases.

APPENDIX F: LOWER BOUNDS ON THE KEY RATE

The asymptotic key rate is determined using the Devetak-Winter formula, $r_{\text{DW}} = H(A_1|E) - H(A_1|B_3)$, where the first term quantifies Eve's uncertainty about Alice's outcomes, and the second term represents the information leaked during error correction. In our analysis, we employ three distinct computational techniques to obtain a rigorous lower bound on it, and complement these with two postprocessing strategies designed to enhance the final value.:

1. Analytical approach: CHSH-based method

The asymptotic secure key rate can be lower bounded analytically using

$$r \geq 1 - h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right) - H(A_1|B_3) + h\left(\frac{1 + \sqrt{1 - q(1 - q)(8 - S^2)}}{2}\right), \quad (\text{F1})$$

where q is the probability that Alice flips her output, a procedure known as noisy preprocessing. Using this lower bound, Fig. 6(a) illustrates the key rate dependence on distance for the two-photon protocol with perfect visibility $V = 1$, optimized over g_a for various values of efficiencies, assuming $\eta_s = 1$ and $g_b = 0.1$. The results are obtained using the probability distribution from Appendix C 2 and the heralding efficiency from Eq. (A24). The corresponding optimal values of g for each distance and efficiency are shown in Fig. 6(b).

2. Numerical approach: Brown-Fawzi-Fawzi method

The results of Ref. [18] enable the construction of a numerical upper bound on the relative entropy, approximated by a polynomial. Using this, a lower bound on the conditional von Neumann entropy of the state ρ is established based on its connection with the relative entropy $D(\rho||\sigma) = \text{Tr}[\rho(\log_2 \rho - \log_2 \sigma)]$ in the following way:

$$H(A|B)_\rho := -D(\rho_{AB}||\mathbb{I}_A \otimes \rho_B). \quad (\text{F2})$$

Subsequently, NPA hierarchy is employed to transform the optimization problem of this noncommutative polynomial into an SDP, and the lower bound for the conditional entropy of Alice and Eve is calculated with the following program:

$$\begin{aligned} H(A|X = x^*, \mathcal{H}_E) &\geq \sum_{i=1}^{m-1} \frac{\omega_i}{t_i \ln 2} + \inf \sum_{i=1}^{m-1} \frac{\omega_i}{t_i \ln 2} \\ &\sum_a \langle \psi | M_{a|x^*} ((Z_{a,i} + Z_{a,i}^* + (1 - t_i)Z_{a,i}^* Z_{a,i}) + t_i Z_{a,i} Z_{a,i}^*) | \psi \rangle, \\ \text{s.t. } &\sum_{abxy} c_{abxy} j \langle \psi | M_{a|x} N_{b|y} | \psi \rangle \geq v_j, \quad \text{for all } 1 \leq j \leq r \\ &\sum_a M_{a|x} = \sum_b N_{b|y} = \mathcal{I}, \quad \text{for all } x, y \\ &M_{a|x} \geq 0, \quad \text{for all } a, x \\ &N_{b|y} \geq 0, \quad \text{for all } b, y \\ &Z_{a,i}^* Z_{a,i} \leq \alpha_i, \quad \text{for all } a, i = 1, \dots, m-1 \\ &Z_{a,i} Z_{a,i}^* \leq \alpha_i, \quad \text{for all } a, i = 1, \dots, m-1 \\ &[M_{a|x}, N_{b|y}] = [M_{a|x}, Z_{b,i}^*] = [N_{b|y}, Z_{a,i}^*] = 0, \quad \text{for all } a, b, x, y, i \\ &M_{a|x}, N_{b|y}, Z_{z,i} \in B(H), \quad \text{for all } a, b, x, y, i. \end{aligned} \quad (\text{F3})$$

Note that considering pure states is enough for this optimization. In the above relation, ω_i 's are the weights in Gauss-Radau quadrature, Z_i 's are Eve's bounded operators, and $\{\{M_{a|x}\}_a\}_x$ are preselected POVMs used by Alice. Fur-

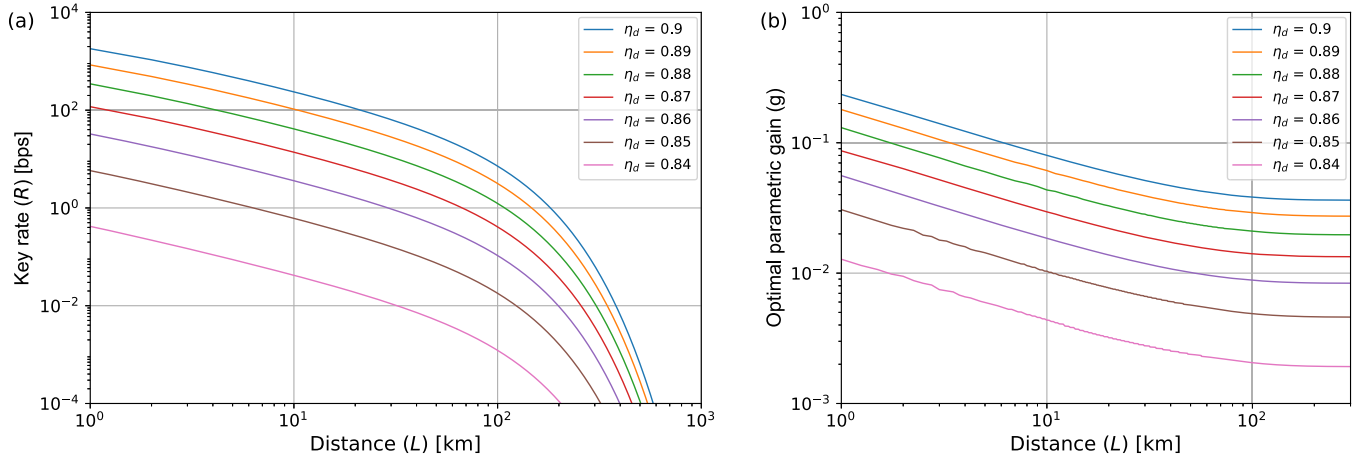


FIG. 6. (a) Asymptotic secure key rate (bits per second, bps) vs distance for the two-photon protocol using the optimal parametric gain g_a with visibility $V = 1$, assuming laser repetition rate $f_{\text{rep}} = 100$ MHz, $\eta_s = 1$, and $g_b = 0.1$, using the bound from Eq. (7). (b) Optimal value of g_a as a function of distance for the two-photon protocol with visibility $V = 1$. Lines correspond to detection efficiencies from 84% to 90%.

thermore, $B(\mathcal{H}_E)$ is von Neumann algebra on Eve's separable Hilbert space $\mathcal{H}_E$. For more details refer to Ref. [18].

In our numerical calculations, we go up to the second level of NPA hierarchy plus some additional constraints of higher level “ABZ + AZZ + ABB + AAB,” where $A \in \{I\} \cup \{M_{a|x}\}_{a,x}$, $B \in \{I\} \cup \{N_{b|y}\}_{b,y}$, and $Z \in \{I\} \cup \{Z_{c,i}, Z_{c,i}^*\}_{c,i}$. We do not go to further levels due to computational complexity.

To combine noisy preprocessing with this method, we should modify the measurement operators in Eq. (F3) to $\tilde{M}_{a|x} = (1 - q)M_{a|x} + qM_{a|x}$. In addition, the first term in the right-hand side of this relation should be replaced with $c_m = 2q(1 - q) + \sum_{i=1}^{m-1} \frac{\omega_i}{i \ln 2}$. For detailed calculations, see Ref. [18].

3. Numerical approach: min-entropy ($H_{\min}$) method

Here, we present a numerical approach, based on min-entropy as a lower bound for the conditional von Neumann entropy [31], to calculate the key rate. Although this method may not yield better results compared to the BFF method, it offers a computational advantage. Besides, its combination with the postselection method leads to an improvement in the efficiency threshold. Postselection is a technique that is used to overcome errors caused by detection deficiencies in which Alice and Bob randomly and independently keep bits “0” with probability p , discard them with probability $1 - p$, and keep all bits “1” intact during their key generation rounds.

The min-entropy $H_{\min}$ is tied to guessing probability $G(A_1|E, \nu_p)$ in the following way:

$$H_{\min}(A_1|E, \nu_p) = -\log_2 G(A_1|E, \nu_p), \quad (\text{F4})$$

where $\nu_p = \{ab \mid ab = 00, 01, 10, 11\}$ is the set of postselected events with coefficients $\omega_{00} = 1$, $\omega_{10} = \omega_{01} = p$, and $\omega_{11} = p^2$, and the guessing probability is defined as

$$G(A_1|E, \nu_p) = \frac{1}{p_{\nu_p}} \max_{P(a,b,e|1,3,z)} \sum_{a,b \in \nu_p} \omega_{ab} P(a, b, a|1, 3, z), \quad (\text{F5})$$

with $p_{\nu_p} = \sum_{a,b \in \nu_p} \omega_{ab} P(a, b|1, 3)$ the total probability of keeping a pair of bits. This optimization can be realized by

means of SDP method, with the following constraints:

$$\sum_{e \in \{0,1\}} P(a, b, e|1, 3, z) = P(a, b|1, 3),$$

$$P(a, b, e|1, 3, z) \in \tilde{\mathcal{Q}}.$$

The second constraint ensures that the conditional probabilities remain within the quantum set. To verify this, we utilize the NPA hierarchy [30,44]. The optimized lower bound on key rate in this case is calculated using the following modification of Eq. (6):

$$r \geq p_{\nu_p} [H_{\min}(A_1|E, \nu_p) - H(A_1|B_3, \nu_p)]. \quad (\text{F6})$$

The technique improves the threshold efficiency to 89.8% in the one-photon protocol, but compromises security by restricting it to collective attacks rather than the coherent attacks.

4. Comparison

Here, we compare the previously described lower-bound approaches and present numerical values for the parameters introduced in the article.

Figure 7 illustrates the maximum achievable key rate for both protocols as a function of detection efficiency. Moreover, Table I compares the detection efficiency required to obtain a positive key rate and Bell violation for the lower bound methods discussed in this Appendix.

APPENDIX G: FINITE-KEY RATE

To optimize the key rate in the finite-size regime, we developed a three-tier security certification strategy:

(1) *CHSH certificate*. For each distance L , we optimize the Devetak-Winter bound using the analytical CHSH formula with noisy preprocessing. This allowed us to identify optimal optical parameters and bit-flip probability q_{opt} , from which the expected probability distribution $P(a, b|x, y)_L$ is obtained. Using the CHSH inequality as the Bell certificate, we then apply the BFF method to construct a min-tradeoff function and evaluate the finite-size key rate via the EAT.

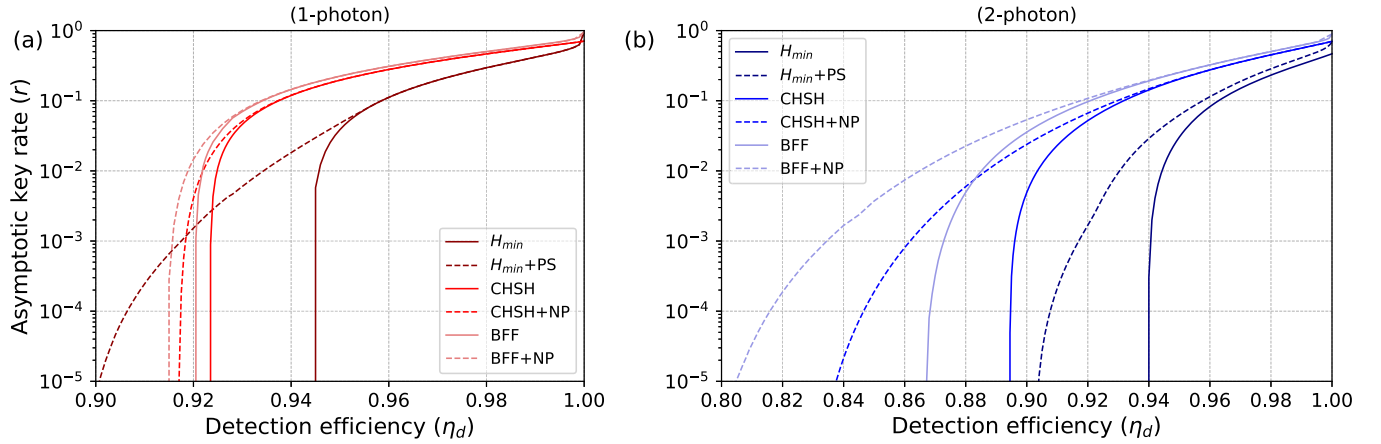


FIG. 7. Secure key rate computed using CHSH, BFF, and $H_{\min}$ methods, without (solid) and with postprocessing (dashed) using noisy preprocessing (NP) and postselection (PS) techniques for (a) the one-photon protocol and (b) the two-photon protocol.

(2) *Full statistic certificate.* Using $P(a, b|x, y)_L$, we apply the full statistics approach [18,45,46], which puts constraints on the complete probability distribution rather than only the CHSH value. The resulting min-tradeoff functions f_L were then used in conjunction with the EAT to compute finite-size key rates. This method provides the tightest security bounds but requires monitoring of the whole measurement statistics.

(3) *Optimal Bell certificate.* To overcome the real-time implementation challenges of method (2), we define a distance-dependent Bell inequality using the min-tradeoff function f_L derived from full-statistics optimization. We computed the observed value of this optimal Bell certificate for $P(a, b|x, y)_L$ and enforced this value as a constraint in a subsequent BFF procedure, with the final key rate obtained again

through the EAT. This custom certificate achieves key rates that significantly exceed CHSH-based bounds while maintaining practical implementability.

The effect of the three certification methods on the finite-key rate is illustrated in Fig. 8. The optimized Bell certificate consistently outperforms CHSH-based certification, delivering 2–3 times higher key rates at maximum distances. Full statistics provide marginal additional gains at a substantial implementation cost. Notably, numerical optimization yields only modest improvements over the analytical bound, Eq. (7), reflecting near-optimality of CHSH bounds for maximally entangled states. This simplifies experimental implementation, as monitoring the CHSH value S alone suffices for accurate key rate estimation.

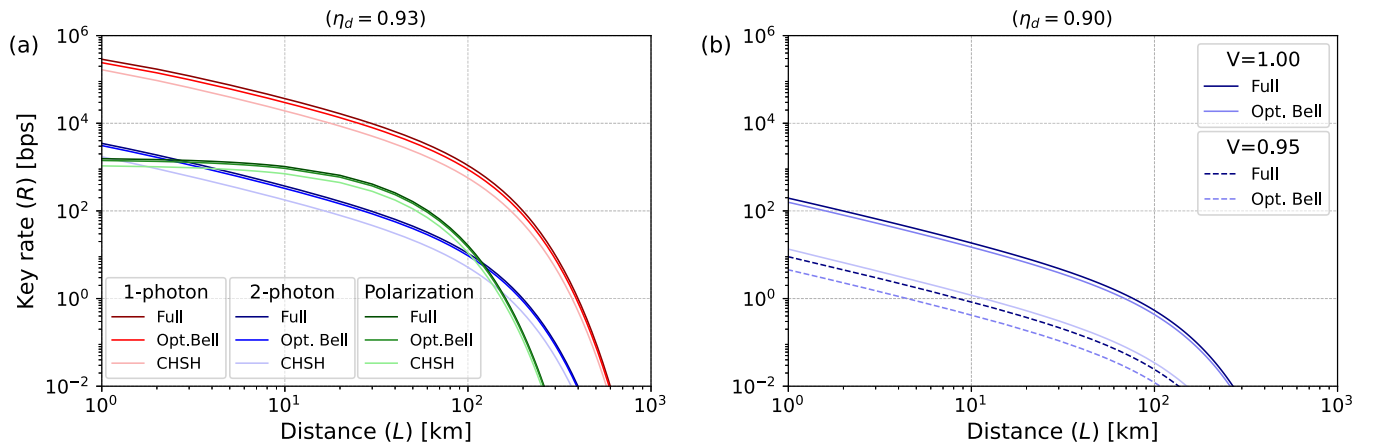


FIG. 8. Comparison of finite-size and asymptotic key rates R vs distance L under different certification approaches, assuming $N = 10^9$ protocol rounds, repetition rate $f_{\text{rep}} = 100$ MHz, and optimal parametric gain g , computed for (a) local detection efficiency $\eta_d = 93\%$ for the one-photon protocol (red), the two-photon protocol (blue), and the polarization-based protocol from Ref. [26] (green), all for visibility $V = 1$; and (b) local detection efficiency $\eta_d = 90\%$ for the two-photon protocol, computed for visibilities $V = 0.95$ (dashed lines) and 1 (solid lines).

- [1] V. Zapatero *et al.*, Advances in device-independent quantum key distribution, *npj Quantum Inf.* **9**, 10 (2023).
- [2] I. W. Primaatmaja *et al.*, Security of device-independent quantum key distribution protocols: A review, *Quantum* **7**, 932 (2023).
- [3] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, *Nat. Commun.* **2**, 349 (2011).
- [4] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, *Nat. Photon.* **4**, 686 (2010).
- [5] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, *Phys. Rev. A* **78**, 042333 (2008).
- [6] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors, *New J. Phys.* **13**, 073024 (2011).
- [7] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger, Bell violation using entangled photons without the fair-sampling assumption, *Nature (London)* **497**, 227 (2013).
- [8] T. McDermott, M. Moradi, A. Mikos-Nuszkiewicz, and M. Stobińska, Eberhard limit for photon-counting Bell tests and its utility in quantum key distribution, *arXiv:2211.15033*.
- [9] S. Pirandola *et al.*, Advances in quantum cryptography, *Adv. Opt. Photon.* **12**, 1012 (2020).
- [10] D. P. Nadlinger *et al.*, Experimental quantum key distribution certified by Bell's theorem, *Nature (London)* **607**, 682 (2022).
- [11] W. Zhang *et al.*, A device-independent quantum key distribution system for distant users, *Nature (London)* **607**, 687 (2022).
- [12] W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, M.-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J.-W. Pan, Toward a photonic demonstration of device-independent quantum key distribution, *Phys. Rev. Lett.* **129**, 050502 (2022).
- [13] A. Sadhu, M. A. Somayajula, K. Horodecki, and S. Das, Practical limitations on robustness and scalability of quantum Internet, *arXiv:2308.12739*.
- [14] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, *Nature (London)* **557**, 400 (2018).
- [15] A. Steffanlongo, M. Navarro, M. Cenni, X. Valcarce, A. Acín, and E. Oudot, Long-distance device-independent quantum key distribution using single-photon entanglement, *arXiv:2409.17075*.
- [16] P. Caspar, E. Verbanis, E. Oudot, N. Maring, F. Samara, M. Caloz, M. Perrenoud, P. Sekatski, A. Martin, N. Sangouard, H. Zbinden, and R. T. Thew, Heralded distribution of single-photon path entanglement, *Phys. Rev. Lett.* **125**, 110506 (2020).
- [17] M. E. Mycroft, T. McDermott, A. Buraczewski, and M. Stobińska, Proposal for the distribution of multiphoton entanglement with optimal rate-distance scaling, *Phys. Rev. A* **107**, 012607 (2023).
- [18] P. Brown, H. Fawzi, and O. Fawzi, Device-independent lower bounds on the conditional von Neumann entropy, *Quantum* **8**, 1445 (2024).
- [19] F. Dupuis and O. Fawzi, Entropy accumulation with finite-size corrections, *IEEE Trans. Inf. Theory* **65**, 7596 (2019).
- [20] F. Dupuis, O. Fawzi, and R. Renner, Entropy accumulation, *Commun. Math. Phys.* **379**, 867 (2020).
- [21] F. Kaneda, K. Garay-Palmett, A. B. U'Ren, and P. G. Kwiat, Heralded single-photon source utilizing highly nondegenerate, spectrally factorable spontaneous parametric downconversion, *Opt. Express* **24**, 10733 (2016).
- [22] V. C. Vivoli, T. Barnea, C. Galland, and N. Sangouard, Proposal for an optomechanical Bell test, *Phys. Rev. Lett.* **116**, 070405 (2016).
- [23] 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).
- [24] 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).
- [25] K. Banaszek and K. Wódkiewicz, Testing quantum nonlocality in phase space, *Phys. Rev. Lett.* **82**, 2009 (1999).
- [26] E. M. González-Ruiz, J. Rivera-Dean, M. F. B. Cenni, A. S. Sørensen, A. Acín, and E. Oudot, Device-independent quantum key distribution with realistic single-photon source implementations, *Opt. Express* **32**, 13181 (2024).
- [27] 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).
- [28] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, *Proc. R. Soc. A: Math. Phys. Eng. Sci.* **461**, 207 (2005).
- [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] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, *New J. Phys.* **10**, 073013 (2008).
- [31] F. Xu, Y.-Z. Zhang, Q. Zhang, and J.-W. Pan, Device-independent quantum key distribution with random postselection, *Phys. Rev. Lett.* **128**, 110506 (2022).
- [32] M. Masini, S. Pironio, and E. Woodhead, Simple and practical DIQKD security analysis via BB84-type uncertainty relations and Pauli correlation constraints, *Quantum* **6**, 843 (2022).
- [33] W. Dai, T. Krovetz, VHASH security, Cryptology ePrint Archive (2007), available at: <https://ia.cr/2007/338>.
- [34] A. J. Stolk *et al.*, Metropolitan-scale heralded entanglement of solid-state qubits, *Sci. Adv.* **10**, eadp6442 (2024).
- [35] S.-R. Zhao, S. Zhao, H.-H. Dong, W.-Z. Liu, J.-L. Chen, K. Chen, Q. Zhang, and J.-W. Pan, Loophole-free test of local realism via Hardy's violation, *Phys. Rev. Lett.* **133**, 060201 (2024).
- [36] B.-W. Lu *et al.*, Device-independent quantum key distribution over 100 km with single atoms, *Science* **391**, 592 (2026).
- [37] Y. K. Alwehaibi, E. Mer, G. J. Machado, S. Yu, I. A. Walmsley, and R. B. Patel, A tractable protocol for detection-loophole-free Bell tests over long distances, *Phys. Rev. Res.* **7**, 043198 (2025).
- [38] M. Ishihara, A. Brendan, W. Roga, U. L. Andersen, and M. Takeoka, Long-distance device-independent quantum key distribution with standard optics tools, *Opt. Quantum* **3**, 535 (2025).

- [39] P. Wittek, Algorithm 950: Ncpol2sdpa—Sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables, *ACM Trans. Math. Softw.* **41**, 1 (2015).
- [40] MOSEK ApS, The MOSEK Python Fusion API manual, Version 11.0 (2025), available at: <https://docs.mosek.com/11.0/pythonfusion/index.html>.
- [41] P. Mironowicz and M. Bourennane, Finite-size security analysis for quantum protocols: A Python framework using the entropy accumulation theorem with graphical interface, [arXiv:2506.18888](https://arxiv.org/abs/2506.18888).
- [42] G. S. Thekkadath, M. E. Mycroft, B. A. Bell, C. G. Wade, A. Eckstein, D. S. Phillips, R. B. Patel, A. Buraczewski, A. E. Lita, T. Gerrits, S. W. Nam, M. Stobińska, A. I. Lvovsky, and I. A. Walmsley, Quantum-enhanced interferometry with large heralded photon-number states, *npj Quantum Inf.* **6**, 89 (2020).
- [43] M. Stobińska, A. Buraczewski, M. Moore, W. R. Clements, J. J. Renema, S. W. Nam, A. Lita, W. S. Kolthammer, A. Eckstein, and I. A. Walmsley, Quantum interference enables constant-time quantum information processing, *Sci. Adv.* **5**, eaau9674 (2019).
- [44] P. Mironowicz, Semi-definite programming and quantum information, *J. Phys. A: Math. Theor.* **57**, 163002 (2024).
- [45] O. Nieto-Silleras, S. Pironio, and J. Silman, Using complete measurement statistics for optimal device-independent randomness evaluation, *New J. Phys.* **16**, 013035 (2014).
- [46] J. D. Bancal, L. Sheridan, and V. Scarani, More randomness from the same data, *New J. Phys.* **16**, 033011 (2014).
- [47] A. M. Brańczyk, Hong–Ou–Mandel interference, *Can. J. Phys.* **102**, 411 (2024).
- [48] A. M. Brańczyk, T. C. Ralph, W. Helwig, and C. Silberhorn, Optimized generation of heralded Fock states using parametric down-conversion, *New J. Phys.* **12**, 063001 (2010).