

Decoy-State Quantum Key Distribution over 227 km with a Frequency-Converted Telecom Single-Photon Source

Frederik Brooke Barnes¹, Roberto G. Pousa², Christopher L. Morrison¹, Zhe Xian Koong¹, Joseph Ho¹,
 Francesco Graffitti¹, John Jeffers³, Daniel K. L. Oi³, Brian D. Gerardot¹, and Alessandro Fedrizzi^{1,*}

¹*Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences,
 Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*

²*ICFO-Institut de Ciències Fòniques, The Barcelona Institute of Science and Technology,
 Castelldefels (Barcelona) 08860, Spain*

³*SUPA Department of Physics, University of Strathclyde, Glasgow G4 0NG, United Kingdom*



(Received 3 December 2025; revised 9 April 2026; accepted 11 June 2026; published 3 August 2026)

We implement a decoy-state quantum key distribution scheme using a telecom C-band single-emitter source. The decoy states are created by varying the optical excitation of the quantum emitter to modulate the photon-number distribution. We provide an analysis of our scheme based on existing security proofs, allowing the calculation of secret key rates, including finite key effects. This enables us to demonstrate, with a realistic single-photon source, positive secret key rates using our scheme over 227 km of optical fiber, equivalent to a loss tolerance one order of magnitude greater than nondecoy schemes. This Letter broadens the scope of single-photon sources in future quantum networks by enabling long-distance quantum key distribution with realistic levels of single-photon purity.

DOI: 10.1103/5wwp-rbpm

Introduction—Since its inception over 40 years ago [1], quantum key distribution (QKD) has developed into a mature technology [2,3]. Largely, the adoption of schemes based on weak coherent pulses (WCPs) that exploit simpler hardware, e.g., attenuated diode lasers, and the advent of secure decoy-state protocols have enabled implementations of high-rate and long-distance QKD [4–7]. Secure key rates exceeding 100 Mb/s have been achieved in decoy-state protocols [8,9], while more recent twin-field schemes [10] have demonstrated QKD across 1000 km of fiber [11], inspiring the prospect of QKD networks at the metropolitan and national scale using trusted nodes [12,13]. However, there are constraints on WCP-based QKD, notably coherent states of light contain multiphoton terms that must be dealt with by the decoy-state protocol, at the cost of limited key rates and distances compared to an ideal single-photon source (SPS) [5,6,10]. As a secondary effect, the mean photon number per pulse must be kept low—limiting the peak secure transmission rate of WCP-based QKD at short distances.

Genuine SPSs could enable the theoretical upper limits of secure quantum communication to be reached [14] while

also being vital components of quantum repeater-based networks that constitute the vision of a quantum internet [15,16]. Recent efforts have demonstrated a trust-free quantum relay for QKD [17], and demonstration of quantum teleportation between dissimilar quantum dots [18,19]. Meanwhile, heralded sources have also been used for measurement-device-independent and long-range QKD [20,21]. Ideally, SPSs will be developed to be compatible with repeater protocols based on quantum memories [22,23] to move beyond current trusted-node networks. In the near term, the adoption of suitable SPSs can deliver QKD rates beyond the limits of WCP-based schemes.

Significant progress has been made in the use of single-photon emitters for QKD [24–26]. Sources using open cavity designs have demonstrated high collection efficiencies and mean photon numbers [27,28], enabling fractional key rates exceeding the bound for weak coherent pulses [29]. Meanwhile, Purcell-enhanced sources with excited state lifetimes on the order of 100 ps, are capable of operating at GHz clock rates [30] and have been used in high-rate deployed QKD systems [31]. Recent work has begun exploring the development of room-temperature SPSs based on hexagonal boron nitride [32,33], which face challenges in optimizing for brightness and noise. Beyond prepare-and-measure schemes, high-fidelity entangled states have been produced by single-photon emitters and distributed over metropolitan fiber [34,35], and free-space QKD links [36]. Additionally, the photon-number coherence has been proposed as another property of light, produced by single-photon emitters, which can be

*Contact author: A.Fedrizzi@hw.ac.uk

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.

manipulated to enable protocols such as twin-field QKD, or minimized for the consideration of security in prepare-and-measure schemes [37]. Recently, single-photon emitter frequencies converted to telecom wavelengths have enabled QKD demonstrations in optical fibers exceeding 175 km in the lab [38], and 100 km of deployed fiber [39]. However, there remain outstanding challenges to further increasing of attainable distances: detector efficiencies, dark count rates, and multiphoton content in the emission to name a few [40].

Here, we show an increase in the achievable distance of QKD using nonideal single-photon emitters by adopting techniques from decoy-state protocols, in which states of different mean photon numbers are injected at random to thwart photon-number splitting (PNS) attacks [6]. We demonstrate this using an InGaAs quantum dot (QD) that produces single photons that are frequency-converted into the telecom C band. We encode decoy states using a dynamic optical excitation scheme, wherein the pump pulse area is chosen to prepare two target photon-number distributions. We present an updated security analysis for a decoy-state QKD protocol that enables the use of sub-Poissonian light sources, e.g., quantum dots. Using this updated security model, we demonstrate in the asymptotic limit a nonzero key rate is achievable for 227 km of optical fiber, which is equivalent to 43.4 dB of loss. Furthermore we present the finite key analysis, using the multiplicative Chernoff bound that has been developed for single-emitter sources in Ref. [38], to firmly establish the regimes where this new protocol outperforms the traditional, nondecoy protocols.

Results—We first outline the steps for ensuring security using the decoy-state protocol using a QD-based SPS. We consider the two-decoy-state method [6] that requires the sender (Alice) to randomly prepare three states obeying photon-number probability distributions labeled as $\delta^{(j)} = \{p_{n|\delta^{(j)}}\}_{n=0}^{\infty}$, where $j \in \{0, 1, 2\}$, corresponding to the vacuum, signal, and decoy states, respectively. The distributions $\delta^{(j)}$ must satisfy

$$\langle n_1 \rangle > \langle n_0 \rangle + \langle n_2 \rangle, \quad (1)$$

and

$$\langle n_2 \rangle > \langle n_0 \rangle \geq 0, \quad (2)$$

where $\langle n_j \rangle$ is the mean photon number of distribution $\delta^{(j)}$. To prevent an adversary from discriminating decoys from signals the state preparation must be identical in all degrees of freedom, except the photon-number distribution, which is typically achieved by attenuating the encoded single-photon states. After Alice has sent the states to Bob, they perform reconciliation of the rounds over a public channel. Bob uses the measurement statistics of the detection and error rates for each distribution to establish lower bounds on the vacuum s_0^Z and single-photon s_1^Z yields as well as an

upper bound on phase error ϕ_1^Z , which is measured in the X basis, to estimate the secret key length [41,42],

$$\begin{aligned} \ell = & s_0^Z + s_1^Z[1 - h(\bar{\phi}_1^Z)] - f_{\text{EC}} n^Z h(E^Z) \\ & - \log_2 \frac{2}{\epsilon_{\text{corr}}} - 6 \log_2 \frac{21}{\epsilon_{\text{sec}}}, \end{aligned} \quad (3)$$

where $h(x)$ is the binary entropy function of x , f_{EC} is the error correction efficiency, E^Z is the error rate measured in the Z basis, ϵ_{corr} is the correctness parameter, and ϵ_{sec} is the security parameter.

Standard decoy-state implementations use weak coherent pulses that simplify the process of bounding multiphoton rates for distributions of different intensities, as the photon-number distributions obey Poisson statistics, typically verified by characterizing the source $g^{(2)}(0) = 1$. In contrast, the photon-number distribution of single-photon emitters depend on the physical properties of the system and must be characterized. The multiphoton terms in the Fock space can be approximately upper-bounded using the $g^{(2)}(0)$ and $\langle n \rangle$, as discussed in [38]. The multiphoton fraction produced by a single emitter is in general smaller than a coherent state with the same $\langle n \rangle$, and ensuring

$$\delta_{n>1}^{(1)} > \delta_{n>1}^{(2)} > \delta_{n>1}^{(0)}, \quad (4)$$

the same decoy-state parameter estimation method used for WCPs can be used with SPSs (see Supplemental Material [43] for further details).

We demonstrate this protocol using the setup shown in Fig. 1. We use a fiber-coupled electronic variable optical attenuator to modulate the intensity of laser light and thus the pulse area. The QD, with a ground state emission at $T = 4$ K of $\lambda = 942$ nm, is driven resonantly with linear polarization and the emission is collected using a cross-polarized, dark-field confocal microscope setup (for more details, see Supplemental Material [43]). The 942 nm photons are coupled into a 40 mm periodically poled lithium-niobate (PPLN) ridge waveguide along with a 2.4 μm continuous-wave laser for difference frequency generation of 942 nm photons to 1550 nm [50]. The $g^{(2)}(0)$ measurements are taken for the frequency converted photons using a Hanbury-Brown and Twiss setup, which is removed when implementing the QKD scheme.

We characterized the source of 1550 nm photons by measuring the count rates and $g^{(2)}(0)$ as a function of excitation pulse area, as shown in Fig. 2(a). The $g^{(2)}(0)$ increases with the pulse area, indicating the reemission due to the QD emitting before the end of the excitation pulse [51]; see Supplemental Material [43] for details on modeling this behavior. From this, we select two pumping regimes for preparing the signal ($\delta^{(1)}$) and decoy ($\delta^{(2)}$) states as indicated on the plots. The signal state is chosen to maximize the mean photon number, while the decoy state

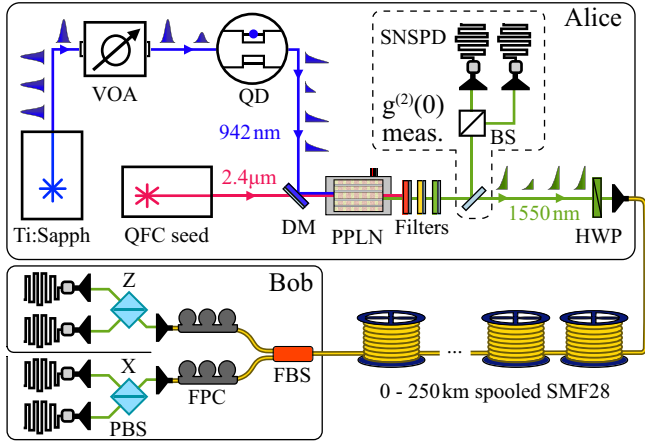


FIG. 1. QKD experimental setup. A Ti:Sapphire laser generates optical excitation pulses with a repetition rate of 80 MHz and the excitation pulse area is controlled by a variable optical attenuator (VOA). The QD is resonantly excited producing single photons at 942 nm that are converted to 1550 nm in a PPLN waveguide using a continuous-wave seed laser at 2.4 μm . The 1550 nm photons are extracted using shortpass, longpass and bandpass spectral filters (SP2050, LP1400, BP1550). An HWP prepares polarization-encoded photons before coupling into single mode (SMF28) fiber and sent to the receiver. A passive receiver performs BB84 measurements using an in-fiber 50:50 beam splitter (FBS) with fiber polarization controllers (FPC) and polarizing beam splitters (PBSs) to project into X and Z bases, before detection with superconducting nanowire single-photon detectors (SNSPDs).

was chosen to optimize the performance of the decoy-state protocol. Notably, the mean photon number of the distributions obeys the relationships in Eqs. (1) and (2). For $\delta^{(1)}$ we used a pulse area of $A_{\delta^{(1)}} = 0.96\pi$, resulting in $\sim 5 \times 10^5$ counts per second with $\langle n_1 \rangle = 1.16 \times 10^{-2}$; $\delta^{(2)}$ used $A_{\delta^{(2)}} = 0.18\pi$, which produced $\sim 5 \times 10^4$ counts per second with $\langle n_2 \rangle = 7.6 \times 10^{-3}$; and we set $\delta^{(0)}$ as vacuum with $\langle n_0 \rangle = 0$ (equivalent to no driving).

Alice prepares one of four polarization-encoded states (H, V, A, D), using a half-wave plate (HWP), for each $\delta^{(j)}$. While we consider the efficient choice of key-generation basis probability, p_Z , for assessing the performance of the protocol, we implement a passive preparation and measurement scheme for convenience in this experiment. Alice then sends the states over variable lengths of single-mode fiber to the receiver. Bob projects the states into the X or Z basis using a pair of fiber polarization controllers and polarizing beam splitters, and records the detection events with four single-photon detectors, as shown in Fig. 1. Additionally, Bob uses a time-gating window of 1.25 ns to mitigate the effect of dark counts.

From the measurement statistics we perform parameter estimation and establish the secure key rates. The single-photon decoy method differs from the coherent-state decoy method in that we use new bounds for $\bar{\phi}$, s_0^Z , and s_1^Z . For ϕ_Z ,

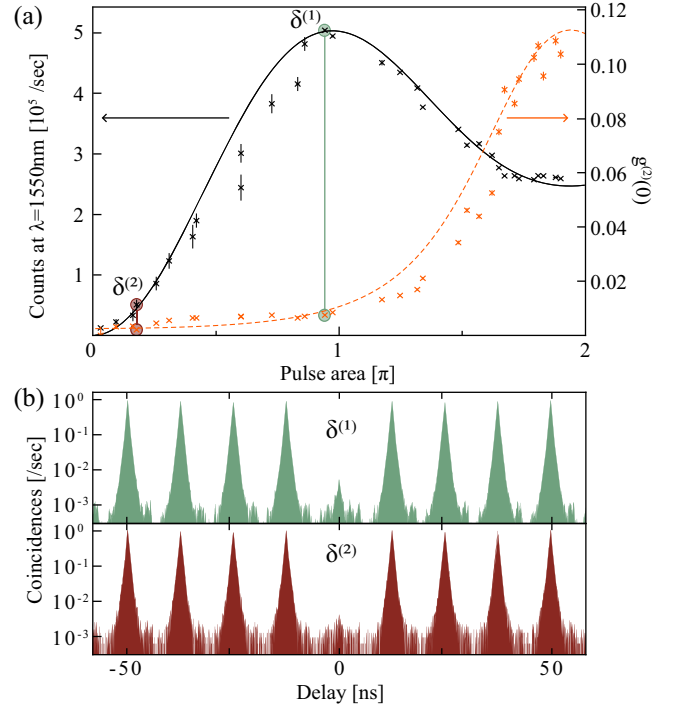


FIG. 2. Source characterization. (a) The measured detection count rates (black data, left-hand axis) and $g^{(2)}(0)$ (orange data, right-hand axis) of the resonantly excited QD emission after quantum frequency conversion (QFC) from 942 to 1550 nm as the excitation pulse area is varied from $[0, 2\pi]$. Solid lines are generated from a simplified two-level model; see Supplemental Material [43] for details. Error bars are estimated assuming Poissonian statistics. (b) Coincidence measurements for the signal state ($\delta^{(1)}$) with $g^{(2)}(0)$ of 0.0159 ± 0.0002 and decoy state ($\delta^{(2)}$) with $g^{(2)}(0)$ of 0.0155 ± 0.0005 .

the experimental parameters required at this stage are the number of detection events in the X basis for each distribution, $n_{X,\delta^{(j)}}$, and the number of errors, $m_{X,\delta^{(j)}}$, for a given block length. We estimate these through measurement of the detection and error events per pulse for each distribution, $p_{c,\delta^{(j)}}$ and $p_{\text{err},\delta^{(j)}}$ respectively. These are measured by analyzing Bob's count rates with respect to the repetition rate, and the ratio of events where Bob measures the incorrect state compared to that prepared by Alice given that Bob chooses the correct basis. This allows extrapolation of $n_{Z,\delta^{(j)}}$ and $m_{Z,\delta^{(j)}}$ for different raw key block lengths. Similarly, s_0^Z and s_1^Z can be derived from $n_{Z,\delta^{(j)}}$ and the previously characterized source parameters and user-defined protocol parameters. A detailed description of the parameter estimation is provided in Supplemental Material [43].

The asymptotic key rate (AKR) at each distance is calculated for the nondecoy protocol as in Ref. [38] and from Eq. (3) for the decoy protocol, as shown in Fig. 3. The same signal and decoy states were used at each distance. AKR extracted from the parameters estimated in our

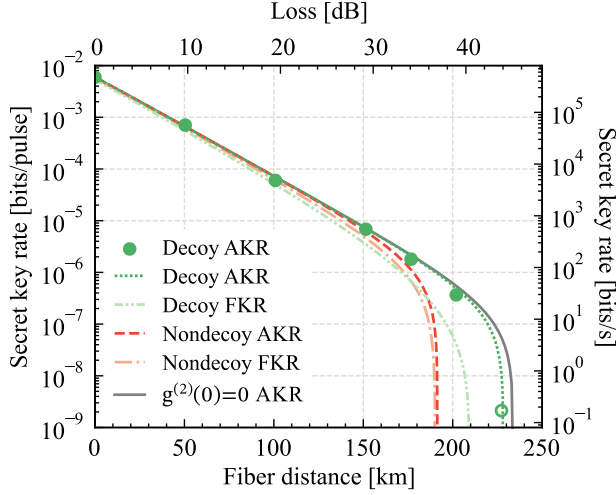


FIG. 3. Comparison of nondecoy and decoy protocols. AKR and FKR (10^{11} states sent) as a function of channel loss for the nondecoy BB84 protocol (red) and decoy protocol (green). Key rate estimates from the experimental data (filled green circles) follow our system model. AKR for a source with the same $\langle n \rangle$ as our source and $g^{(2)}(0) = 0$ is shown to achieve positive key rates at only slightly greater distances than our source with the decoy protocol. The unfilled green circle is the experimentally measured AKR when using a smaller gating window of 250 ps.

experiment are shown to match the expected key rates of our modeled system. In the low-loss regime, both protocols perform similarly as the ratio of prepared signal states to decoy states approaches unity. In the high-loss regime, the decoy protocol shows a clear improvement, allowing positive key rates beyond 227 km (44 dB) compared to 191 km (37 dB) for the standard nondecoy protocol. In this regime, the decoy states $\delta^{(2)}$ and $\delta^{(0)}$ do not themselves contribute to the secure key as their quantum bit error rate exceeds the Holevo bound for secure key generation, but they enable lower bounds on the single-photon yield leading to greater key rates. Notably, the decoy protocol comes close to saturating the nondecoy AKR of a perfectly pure SPS [$g^{(2)}(0) = 0$] of the same brightness, which we model as achieving positive key rates up to 233 km (45 dB). This indicates that, in the asymptotic limit, the decoy protocol is limited by the single-to-noise ratio at Bob rather than the single-photon impurity of Alice's source. This is evidenced by the need to minimize the effect of dark counts by using a tighter gating window of 250 ps in order to extract a positive key rate from our experimental data at a distance of 227 km.

While the AKR provides an upper bound on the tolerable loss for secure key generation, it is important to characterize the performance of a protocol with finite block sizes that can be generated in realistic timescales. Figure 3 shows the finite key rate (FKR) for each protocol in the scenario that Alice sends 10^{11} pulses, equivalent to a practical acquisition time of approximately 20 min. In this scenario, the

nondecoy protocol slightly outperforms the decoy protocol for low losses. The regime of decoy-protocol advantage begins at 175 km (33 dB), and by 190 km (37 dB) the nondecoy FKR drops to zero while the decoy FKR remains above 10 bits/s. Ultimately, the decoy FKR in this scenario remains positive up to 209 km (40 dB). Although we use tight bounds for parameters of both protocols, including Chernoff bounds for finite sampling statistics [41,50,52], we find that the decoy protocol FKR does not follow the AKR as closely as the nondecoy protocol. We attribute this to the decoy protocol having a greater number of parameters than the nondecoy protocol, leading to a greater fraction of raw key being expended by parameter estimation.

Discussion—We note recent work that utilizes photon statistics, such as $g^{(2)}(0)$, observed by the receiver to detect the presence of an eavesdropper performing certain PNS attacks [53]. Under certain assumptions, this allows the range and rate of QKD to be extended for sources with high values of $g^{(2)}(0)$ without the use of a decoy state, but is not secure against the most general PNS attack. We also note that the work of [54] makes a strong assumption that Fock state contributions of three or more photons can be totally neglected for their source. This assumption is not necessarily valid or secure to assume, hence the applicability of their protocol and analysis is restricted. Meanwhile, other work [55] has focused on particular photon-number distributions. The assumptions of the Fock state population distribution and decay in our Letter are less restrictive and are valid for a greater class of SPSs and driving conditions.

This security and composability of our protocol is maintained through existing security analyses. Additionally, it allows us to employ techniques from the well-established field of WCP QKD to create tight bounds on key rates for asymptotic and finite block lengths. In the finite-key regime, the decoy protocol only confers an advantage for our source at the upper limit of practical acquisition times, but sources with similar Purcell enhancement have been successfully operated at GHz repetition rates [30]. Additionally, state-of-the-art QDs have individually exhibited brightness of at least one order of magnitude greater than our QD [27,29] before frequency conversion. Thus, we expect the regime where decoy states confer an advantage to shift increasingly toward practical acquisition times, with the crossover point potentially decreasing to the order of 10 s with existing SPSs. Because the decoy-state method is applicable beyond prepare-and-measure QKD, such as measurement-device-independent and twin-field protocols, our methods could also help to enable nonideal SPSs in more advanced quantum communication protocols.

Our methods could be readily implemented with intensity modulation applied to the QD emission, in a similar fashion to WCP QKD, rather than dynamic optical excitation. However, our dynamic QD excitation method avoids the insertion loss on the generated single-photon states, which is typically > 2 dB for an in-fiber Mach-Zehnder

modulator. In contrast to a WCP source, the brightness of an SPS cannot be increased to compensate for this additional loss. Therefore, this Letter supports the concept of photon number being a useful degree of freedom for quantum communication with single emitters [25,37] and highlights that the dynamic excitation method could be used for applications beyond communications.

To move our scheme to a practical setting with random encoding, an electro-optic modulator intensity modulator would enable random encoding of decoy states at high repetition rates by pulse carving [51] or by selective attenuation of a pulsed laser. Recent work has also shown active encoding of BB84 polarization states can be achieved using similar sources with low encoding error while also being compatible with deployed optical fiber [39]. In a loophole-free implementation, phase randomization between pulses is also necessary [56,57], which we assume to be achieved through the spontaneous emission process. However, a phase modulator could also be used to apply discrete phase randomization without assumptions on the photon-generation process. Alternatively, further exploration of dynamic excitation methods, such as phonon-assisted excitation, could also produce phase-randomized states [25].

In summary, we provide security analysis and experimental demonstration, with a quantum-dot-based telecom C-band SPS, that decoy states can significantly increase the maximum possible key distribution distance, enabling the distribution of a secret key over 227 km and in the asymptotic regime and maintains an advantage over nondecoy protocols for practical acquisition times at long distances. Notably, we find that the FKR performance using decoy states for our imperfect SPS approaches the performance for an SPS with an ideal $g^{(2)}(0) = 0$, i.e., the best-case scenario. Furthermore, we expect our method to be readily accessible for utilization in a deployed fiber network for practical QKD. Therefore, this Letter loosens the bound on single-photon purity required to distribute keys over long distances, opening the door to practical QKD for low purity SPSs, and expands the scope of high performance quantum-dot sources as a general-purpose source in future quantum networks.

Acknowledgments—This work was supported by the EPSRC Quantum Technology Hub in Quantum Communication (EP/T001011/1), International Network in Space Quantum Technologies (EP/W027011/1), and the Integrated Quantum Networks Research Hub (EP/Z533208/1). B.D.G. acknowledges support from the Royal Academy of Engineering for a Chair in Emerging Technology. R. G. P. acknowledges this work was partially funded by CEX2024-001490-S [MICIU/AEI/10.13039/501100011033], Fundació Cellex, Fundació Mir-Puig, and Generalitat de Catalunya through CERCA, and also supported by the Government of Spain (Severo Ochoa CEX2019-000910-S, FUNQIP, and NextGeneration EU PRTR-C17.I1) and European Union (QSNP, 101114043).

Data availability—The data that support the findings of this article are not publicly available upon publication because it is not technically feasible and/or the cost of preparing, depositing, and hosting the data would be prohibitive within the terms of this research project. The data are available from the authors upon reasonable request.

- [1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.*, **560**, 7 (2014).
- [2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* **92**, 025002 (2020).
- [3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, *Adv. Opt. Photonics* **12**, 1012 (2020).
- [4] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [5] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).
- [6] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [7] J. Qiu, Quantum communications leap out of the lab, *Nature (London)* **508**, 441 (2014).
- [8] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, Q. Li, Y. Liu, Q. Zhang, C.-Z. Peng, L. You, F. Xu, and J.-W. Pan, High-rate quantum key distribution exceeding 110 Mb s⁻¹, *Nat. Photonics* **17**, 416 (2023).
- [9] F. Grönenfelder, A. Boaron, G. V. Resta, M. Perrenoud, D. Rusca, C. Barreiro, R. Houlmann, R. Sax, L. Stasi, S. El-Khoury, E. Hänggi, N. Bosshard, F. Bussi eres, and H. Zbinden, Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems, *Nat. Photonics* **17**, 422 (2023).
- [10] 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).
- [11] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental twin-field quantum key distribution over 1000 km fiber distance, *Phys. Rev. Lett.* **130**, 210801 (2023).
- [12] V. Martin *et al.*, MadQCI: A heterogeneous and scalable SDN-QKD network deployed in production facilities, *npj Quantum Inf.* **10**, 1 (2024).
- [13] Y.-A. Chen *et al.*, An integrated space-to-ground quantum communication network over 4,600 kilometres, *Nature (London)* **589**, 214 (2021).
- [14] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, *Nat. Commun.* **8**, 15043 (2017).

- [15] H. J. Kimble, The quantum internet, *Nature (London)* **453**, 1023 (2008).
- [16] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, *Science* **362**, eaam9288 (2018).
- [17] M. Zou *et al.*, Realization of an untrusted intermediate relay architecture using a quantum dot single-photon source, *Nat. Phys.* **21**, 1670 (2025).
- [18] T. Strobel, M. Vyvlecka, I. Neureuther, T. Bauer, M. Schäfer, S. Kazmaier, N. L. Sharma, R. Joos, J. H. Weber, C. Nawrath, W. Nie, G. Bhayani, C. Hopfmann, C. Becher, P. Michler, and S. L. Portalupi, Telecom-wave-length quantum teleportation using frequency-converted photons from remote quantum dots, *Nat. Commun.* **16**, (2025) 10027.
- [19] A. Laneve *et al.*, Quantum teleportation with dissimilar quantum dots over a hybrid quantum network, *Nat. Commun.* **16**, 10028 (2025).
- [20] X.-H. Zhan, Z.-Q. Zhong, S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, Measurement-device-independent quantum key distribution with practical spontaneous parametric down-conversion sources, *Phys. Rev. Appl.* **20**, 034069 (2023).
- [21] X.-H. Zhan, Z.-Q. Zhong, J.-Y. Ma, S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, Experimental demonstration of long distance quantum communication with independent heralded single photon sources, *npj Quantum Inf.* **11**, 73 (2025).
- [22] P. van Loock, W. Alt, C. Becher, O. Benson, H. Boche, C. Deppe, J. Eschner, S. Höfling, D. Meschede, P. Michler, F. Schmidt, and H. Weinfurter, Extending quantum links: Modules for fiber- and memory-based quantum repeaters, *Adv. Quantum Technol.* **3**, 1900141 (2020).
- [23] C.-Y. Lu and J.-W. Pan, Quantum-dot single-photon sources for the quantum internet, *Nat. Nanotechnol.* **16**, 1294 (2021).
- [24] D. A. Vajner, L. Rickert, T. Gao, K. Kaymazlar, and T. Heindel, Quantum communication using semiconductor quantum dots, *Adv. Quantum Technol.* **5**, 2100116 (2022).
- [25] M. Bozzio, M. Vyvlecka, M. Cosacchi, C. Nawrath, T. Seidelmann, J. C. Loredó, S. L. Portalupi, V. M. Axt, P. Michler, and P. Walther, Enhancing quantum cryptography with quantum dot single-photon sources, *npj Quantum Inf.* **8**, 1 (2022).
- [26] T. Heindel, J.-H. Kim, N. Gregersen, A. Rastelli, and S. Reitzenstein, Quantum dots for photonic quantum information technology, *Adv. Opt. Photonics* **15**, 613 (2023).
- [27] N. Tömm, A. Javadi, N. O. Antoniadis, D. Najer, M. C. Löbl, A. R. Korsch, R. Schott, S. R. Valentin, A. D. Wieck, A. Ludwig, and R. J. Warburton, A bright and fast source of coherent single photons, *Nat. Nanotechnol.* **16**, 399 (2021).
- [28] X. Ding, Y.-P. Guo, M.-C. Xu, R.-Z. Liu, G.-Y. Zou, J.-Y. Zhao, Z.-X. Ge, Q.-H. Zhang, H.-L. Liu, L.-J. Wang, M.-C. Chen, H. Wang, Y.-M. He, Y.-H. Huo, C.-Y. Lu, and J.-W. Pan, High-efficiency single-photon source above the loss-tolerant threshold for efficient linear optical quantum computing, *Nat. Photonics* **19**, 387 (2025).
- [29] Y. Zhang, X. Ding, Y. Li, L. Zhang, Y.-P. Guo, G.-Q. Wang, Z. Ning, M.-C. Xu, R.-Z. Liu, J.-Y. Zhao, G.-Y. Zou, H. Wang, Y. Cao, Y.-M. He, C.-Z. Peng, Y.-H. Huo, S.-K. Liao, C.-Y. Lu, F. Xu, and J.-W. Pan, Experimental single-photon quantum key distribution surpassing the fundamental weak coherent-state rate limit, *Phys. Rev. Lett.* **134**, 210801 (2025).
- [30] L. Rickert, D. A. Vajner, M. von Helversen, J. Schall, S. Rodt, S. Reitzenstein, H. Liu, S. Li, H. Ni, Z. Niu *et al.*, High purcell enhancement in quantum-dot hybrid circular Bragg grating cavities for GHz clock rate generation of indistinguishable photons, *ACS Photonics* **12**, 464 (2024).
- [31] J. Yang, Z. Jiang, F. Benthin, J. Hanel, T. Fandrich, R. Joos, S. Bauer, S. Kolatschek, A. Hreibi, E. P. Rugeramigabo, M. Jetter, S. L. Portalupi, M. Zopf, P. Michler, S. Kück, and F. Ding, High-rate intercity quantum key distribution with a semiconductor single-photon source, *Light Sci. Appl.* **13**, 150 (2024).
- [32] Ç. Samaner, S. Paçal, G. Mutlu, K. Uyanık, and S. Ateş, Free-space quantum key distribution with single photons from defects in hexagonal boron nitride, *Adv. Quantum Technol.* **5**, 2200059 (2022).
- [33] Ö. S. Tapşın, F. Ağlarçı, R. G. Pousa, D. K. Oi, M. Gündoğan, and S. Ateş, Quantum key distribution using hBN single-photon emitters at a 40 MHz clock rate, *Quantum Sci. Technol.* **11**, 025058 (2026).
- [34] C. Schimpf, M. Reindl, D. Huber, B. Lehner, S. F. Covre Da Silva, S. Manna, M. Vyvlecka, P. Walther, and A. Rastelli, Quantum cryptography with highly entangled photons from semiconductor quantum dots, *Sci. Adv.* **7**, eabe8905 (2021).
- [35] T. Strobel, S. Kazmaier, T. Bauer, M. Schäfer, A. Choudhary, N. L. Sharma, R. Joos, C. Nawrath, J. H. Weber, W. Nie, G. Bhayani, L. Wagner, A. Bisquerra, M. Geitz, R.-P. Braun, C. Hopfmann, S. L. Portalupi, C. Becher, and P. Michler, High-fidelity distribution of triggered polarization-entangled telecom photons via a 36 km intra-city fiber network, *Opt. Quantum* **2**, 274 (2024).
- [36] F. Basso Basset, M. Valeri, E. Roccia, V. Muredda, D. Poderini, J. Neuwirth, N. Spagnolo, M. B. Rota, G. Carvacho, F. Sciarrino, and R. Trotta, Quantum key distribution with entangled photons generated on demand by a quantum dot, *Sci. Adv.* **7**, eabe6379 (2021).
- [37] Y. Karli, D. A. Vajner, F. Kappe, P. C. A. Hagen, L. M. Hansen, R. Schwarz, T. K. Bracht, C. Schimpf, S. F. Covre da Silva, P. Walther, A. Rastelli, V. M. Axt, J. C. Loredó, V. Remesh, T. Heindel, D. E. Reiter, and G. Weihs, Controlling the photon-number coherence of solid-state quantum light sources for quantum cryptography, *npj Quantum Inf.* **10**, 1 (2024).
- [38] C. L. Morrison, R. G. Pousa, F. Graffitti, Z. X. Koong, P. Barrow, N. G. Stoltz, D. Bouwmeester, J. Jeffers, D. K. L. Oi, B. D. Gerardot, and A. Fedrizzi, Single-emitter quantum key distribution over 175 km of fiber with optimised finite key rates, *Nat. Commun.* **14**, 3573 (2023).
- [39] M. Zahidy, M. T. Mikkelsen, R. Müller, B. Da Lio, M. Krehbiel, Y. Wang, N. Bart, A. D. Wieck, A. Ludwig, M. Galili, S. Forchhammer, P. Lodahl, L. K. Oxenløwe, D. Bacco, and L. Midolo, Quantum key distribution using deterministic single-photon sources over a field-installed fiber link, *npj Quantum Inf.* **10**, 1 (2024).
- [40] R. G. Pousa, D. K. L. Oi, and J. Jeffers, Comparison of non-decoy single-photon source and decoy weak coherent pulse in quantum key distribution, *arXiv:2405.19963*.
- [41] H.-L. Yin, M.-G. Zhou, J. Gu, Y.-M. Xie, Y.-S. Lu, and Z.-B. Chen, Tight security bounds for decoy-state quantum key distribution, *Sci. Rep.* **10**, 14312 (2020).

- [42] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, *Phys. Rev. A* **89**, 022307 (2014).
- [43] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/5wwp-rbpm>, which includes Refs. [44–49].
- [44] A. Nazir, Photon statistics from a resonantly driven quantum dot, *Phys. Rev. B* **78**, 153309 (2008).
- [45] K. A. Fischer, K. Müller, K. G. Lagoudakis, and J. Vučković, Dynamical modeling of pulsed two-photon interference, *New J. Phys.* **18**, 113053 (2016).
- [46] J. Johansson, P. Nation, and F. Nori, QuTiP 2: A Python framework for the dynamics of open quantum systems, *Comput. Phys. Commun.* **184**, 1234 (2013).
- [47] K. A. Fischer, L. Hanschke, J. Wierzbowski, T. Simmet, C. Dory, J. J. Finley, J. Vučković, and K. Müller, Signatures of two-photon pulses from a quantum two-level system, *Nat. Phys.* **13**, 649 (2017).
- [48] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Provably secure and practical quantum key distribution over 307 km of optical fiber, *Nat. Photonics* **9**, 163 (2015).
- [49] E. Waks, C. Santori, and Y. Yamamoto, Security aspects of quantum key distribution with sub-Poisson light, *Phys. Rev. A* **66**, 042315 (2002).
- [50] C. L. Morrison, M. Rambach, Z. X. Koong, F. Graffitti, F. Thorburn, A. K. Kar, Y. Ma, S.-I. Park, J. D. Song, N. G. Stoltz, D. Bouwmeester, A. Fedrizzi, and B. D. Gerardot, A bright source of telecom single photons based on quantum frequency conversion, *Appl. Phys. Lett.* **118**, 174003 (2021).
- [51] A. C. Dada, T. S. Santana, R. N. E. Malein, A. Koutroumanis, Y. Ma, J. M. Zajac, J. Y. Lim, J. D. Song, and B. D. Gerardot, Indistinguishable single photons with flexible electronic triggering, *Optica* **3**, 493 (2016).
- [52] K. Tamaki, M. Curty, and M. Lucamarini, Decoy-state quantum key distribution with a leaky source, *New J. Phys.* **18**, 065008 (2016).
- [53] C. Cholsuk, F. Ađlarçı, D. K. Oi, S. Ateş, and T. Vogl, A decoy-like protocol for quantum key distribution: Enhancing the performance with imperfect single photon sources, [arXiv:2510.09454](https://arxiv.org/abs/2510.09454).
- [54] Y. Bloom, Y. Ordan, T. Levin, K. Sulimany, E. G. Bowes, J. A. Hollingsworth, and R. Rapaport, Decoy-state and purification protocols for superior quantum key distribution with imperfect quantum-dot-based single-photon sources: Theory and experiment, *PRX Quantum* **6**, 030332 (2025).
- [55] G. Fioletto, F. Picciariello, C. Agnesi, P. Villoresi, and G. Vallone, Security bounds for decoy-state quantum key distribution with arbitrary photon-number statistics, *Phys. Rev. A* **105**, 012603 (2022).
- [56] H.-K. Lo and J. Preskill, Phase randomization improves the security of quantum key distribution, [arXiv:quant-ph/0504209](https://arxiv.org/abs/quant-ph/0504209).
- [57] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, Discrete-phase-randomized coherent state source and its application in quantum key distribution, *New J. Phys.* **17**, 053014 (2015).