

# Quantum key distribution with entanglement-swapped photons from a quantum emitter

Michele B. Rota<sup>1,\*</sup>, Francesco Basso Basset<sup>1,2,\*</sup>, Alessandro Laneve<sup>1</sup>, Francesco Salusti<sup>3</sup>,  
 Nicolas Claro-Rodriguez<sup>3</sup>, Giuseppe Ronco<sup>1</sup>, Mattia Beccaceci<sup>1</sup>, Tobias M. Krieger<sup>4</sup>, Quirin Buchinger<sup>5</sup>,  
 Saimon F. Covre da Silva<sup>4,6</sup>, Sandra Stroj<sup>7</sup>, Mariia Gumberidze<sup>8</sup>, Vladyslav Usenko<sup>8</sup>, Sven Höfling<sup>5</sup>,  
 Tobias Huber-Loyola<sup>5,9,10</sup>, Mario A. Usuga Castaneda<sup>11</sup>, Armando Rastelli<sup>4</sup>, Klaus D. Jöns<sup>3</sup> and Rinaldo Trotta<sup>1,‡</sup>

<sup>1</sup>Dipartimento di Fisica, *Sapienza Università di Roma*, Piazzale Aldo Moro 5, 00185 Roma, Italy

<sup>2</sup>Dipartimento di Fisica, *Politecnico di Milano*, Piazza Leonardo da Vinci 32, 20133 Milano, Italy

<sup>3</sup>Institute for Photonic Quantum Systems (PhoQS), Center for Optoelectronics and Photonics Paderborn (CeOPP)  
 and Department of Physics, *Paderborn University*, Warburger Straße 100, 33098 Paderborn, Germany

<sup>4</sup>Institute of Semiconductor and Solid State Physics, *Johannes Kepler University Linz*, Altenberger Straße 69, 4040 Linz, Austria

<sup>5</sup>Technische Physik, *University of Würzburg*, Am Hubland, D-97074 Würzburg, Germany

<sup>6</sup>*Universidade Estadual de Campinas*, Instituto de Física Gleb Wataghin, 13083-859 Campinas, Brazil

<sup>7</sup>Research Center for Microtechnology, *Vorarlberg University of Applied Sciences*, CAMPUS V, Hochschulstraße 1, 6850 Dornbirn, Austria

<sup>8</sup>Department of Optics, *Palacký University*, 17. listopadu 12, 771 46 Olomouc, Czech Republic

<sup>9</sup>Institute of Photonics and Quantum Electronics, *Karlsruhe Institute of Technology*, Engesserstraße 5, 76131 Karlsruhe, Germany

<sup>10</sup>Center for Integrated Quantum Science and Technology (IQST), *Karlsruhe Institute of Technology*, Karlsruhe, Germany

<sup>11</sup>Single Quantum B.V., HH 2629, Delft, The Netherlands



(Received 30 November 2025; accepted 7 July 2026; published 29 October 2026)

Quantum key distribution (QKD) is a fundamental functionality of quantum networks. Extending its range requires quantum repeaters, a technology still under development and not yet demonstrated in combination with quantum cryptographic protocols. Here, we address the elementary operation of a viable quantum repeater scheme by evaluating whether correlated photons distributed via entanglement swapping can support secret key distribution. We employ a state-of-the-art deterministic photon source based on a strain-tuned GaAs quantum dot embedded in a photonic cavity and implement a source-independent QKD protocol between two nodes using entanglement-swapped photons. We benchmark the system and present how high-resolution temporal postselection can enable secure key exchange, with further rate improvements expected through realistic device and protocol optimizations. Due to its compatibility with a wide range of quantum memory platforms, our approach represents a significant step toward long-distance quantum-safe communication.

DOI: [10.1103/68f1-cjfk](https://doi.org/10.1103/68f1-cjfk)

## I. INTRODUCTION

Quantum communication stands as one of the most impactful areas of quantum technologies, offering fundamentally new capabilities for information security and networked systems [1,2]. Among its various applications, quantum key distribution (QKD) has emerged as the most mature and widely implemented one, enabling secure communication with information-theoretic guarantees [3,4]. However, current QKD implementations face a significant limitation: the distance over which keys can be distributed is fundamentally constrained by photon losses in optical fibers or the atmosphere and the absence of signal amplification. As a result,

long-distance QKD requires either trusted intermediate nodes or the development of quantum repeaters to preserve end-to-end security [5–8]. By dividing a long communication channel into shorter segments and using entanglement swapping to connect them, quantum repeaters promise to extend the reach of quantum communication without compromising its security. Despite substantial theoretical progress and encouraging experimental advances in individual components, quantum repeaters are limited to proof-of-concept experiments [9,10], and crucially, no implementation to date has demonstrated support for a QKD protocol. Several studies have explored this scenario through numerical simulations using photon pairs generated in nonlinear crystals [11,12], both as a stepping stone toward a quantum repeater implementation and as a way to mitigate the impact of detector dark noise [13]. Besides, heralded entanglement distribution granted by entanglement swapping is key to reach unconditional levels of security in QKD [14], as it has been recently demonstrated employing entanglement swapping between spin qubits mediated by photons to enable device-independent secure QKD [15–18]. However, an implementation based on all-photonic entanglement swapping is crucial to foster the realization of efficient

\*These authors contributed equally to this work.

†Contact author: [michele.rota@uniroma1.it](mailto:michele.rota@uniroma1.it)

‡Contact author: [rinaldo.trotta@uniroma1.it](mailto:rinaldo.trotta@uniroma1.it)

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

chained protocols. This type of application has been recently demonstrated on a platform based on probabilistic sources [19], while it is still missing for quantum emitters, which would bring a potential advantage in device-independent heralded protocols [14,20,21].

In this work, we experimentally address this challenge by presenting the successful combination of quantum emitter-based all-photonic entanglement swapping with an entanglement-based QKD protocol, which naturally integrates with the architecture of future entanglement-distribution networks. As the entangled photon source, we employ semiconductor quantum dots (QDs), which offer quasideterministic generation of entangled photon pairs [22] and are compatible with many quantum memory platforms [23], making them attractive candidates for solid-state quantum network nodes [24–27]. In particular, GaAs QDs have been shown to provide high-rate, highly entangled photon pairs [28–30] at wavelengths that match well the working band of several quantum memory devices based on Rb atoms and atomic vapors [31–33] or rare earths [34,35], are compatible for free space and satellite-mediated communication [36], and can be used themselves as stationary qubits [37]. We use entangled photon pairs from a state-of-the-art GaAs quantum dot embedded in a strain-tunable photonic-cavity structure [30] to perform entanglement swapping with high fidelity, allowing us to employ the swapped photons to validate entanglement-based secure QKD. This result is achieved without resorting to entanglement distillation, but only performing temporal postselection, which directly excludes the events resulting in unsuccessful outcomes of the swapping protocol, without acting on the photons distributed to the two communicating parties. This work represents a step forward in the integration of semiconductor QDs in quantum repeater architectures, providing a novel benchmark and motivating further research in the development of these emitters.

## II. EXPERIMENTAL RESULTS

A scheme of the protocol is illustrated in Fig. 1. The all-photonic implementation of entanglement swapping, akin to its first experimental demonstration [38], starts with two photon pairs (1, 2 and 3, 4) generated by the same entangled-photon pair source at subsequent times  $t_1$  and  $t_2$ , each in the same maximally entangled Bell state, e.g.,  $|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ . One photon is taken from each photon pair (2 and 3), and, after delaying the early photon by the difference in generation time  $t_1 - t_2$ , they are subject to a projective Bell state measurement (BSM). As a result, the remaining two photons (1 and 4), which were previously uncorrelated, will be projected into a specific Bell state, which depends on the outcome of the BSM. This photon pair is shared between two communicating parties, together with the result of the BSM, which is sent through a classical information channel. In this way, the parties know which maximally entangled states they share, and they can exploit them as a resource to implement entanglement-based QKD. Here, we consider an asymmetrical variation of the Ekert protocol proposed by Acín *et al.* [39,40] that ensures source-independent security [41,42]. The two parties, denoted as Alice and Bob, each perform a single-qubit measurement, randomly choosing from

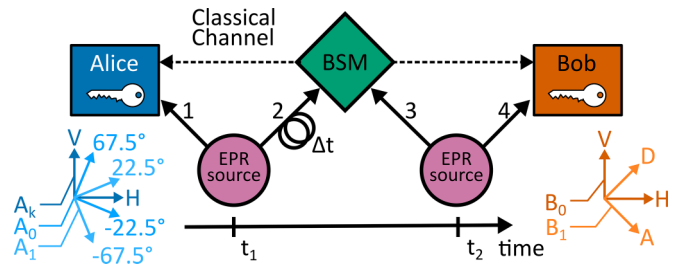


FIG. 1. Protocol scheme for quantum key distribution with swapped photons using a single entangled-photon-pair (EPR) source. A single EPR source is excited at two consecutive times  $t_1$  and  $t_2$ , emitting each time a pair of entangled photons, labeled (1, 2) and (3, 4). Two of these entangled photons (2 and 3) interfere in a 50% efficiency Bell state measurement (BSM) setup by delaying the earlier photon via a delay line. The result of the BSM is shared among Alice and Bob with the pair of now mutually entangled photons 1 and 4. Using the information of the BSM, Alice and Bob perform measurements using different sets of bases,  $A_k$ ,  $A_0$ , and  $A_1$  for Alice and  $B_0$  and  $B_1$  for Bob. Sharing the choice of measurement set and outcome of the BSM afterward allows for key sharing and checks on the Bell inequality violation.

an agreed set of bases, three for Alice and two for Bob. Relative to a common reference system of horizontal (H) and vertical (V) polarization corresponding to  $0^\circ$  and  $90^\circ$  polarization angle, the measurement bases are  $\{A_k, A_0, A_1\} = \{0^\circ/90^\circ, -22.5^\circ/67.5^\circ, -67.5^\circ/22.5^\circ\}$  and  $\{B_0, B_1\} = \{0^\circ/90^\circ, -45^\circ/45^\circ\}$  [43]. The aligned pair of bases  $\{A_k, B_0\}$  is used to reconstruct the shared key. The combinations of the remaining measurement channels  $\{A_0/A_1, B_0/B_1\}$  are used to verify the Clauser-Horne-Shimony-Holt (CHSH) violation [44] and quantify possible eavesdropping.

The protocol performance can be affected by nonideal preparation of the shared state and measurement operations. In general, these kinds of flaws cannot be distinguished from the effects of the malicious action of an eavesdropper; for this reason, any loss of mutual information between Alice and Bob regarding the key due to experimental imperfections must be assimilated to a gain in information for an adversary party, denoted as Eve. The state preparation process is, in this case, the result of an entanglement swapping protocol: the accuracy of the operation, quantified by the fidelity of the obtained state with the expected one, mainly depends on the characteristics of the photon source [45,46].

The emitter we employ is a QD device that can generate strongly polarization-entangled photon pairs in a near-deterministic fashion via the biexciton-exciton cascade under resonant two-photon excitation [22,47]. In the following, we denote the biexciton to exciton transition as XX and the exciton to ground-state transition as X. As the material platform, we choose GaAs/AlGaAs QDs fabricated by droplet etching epitaxy, which have been proven to generate strongly entangled photon pairs [48], arguably due to their short lifetimes, low strain gradient, and moderate spin noise [49]. Additionally, we use a state-of-the-art device in which the QD is embedded in a circular Bragg resonator to enhance brightness and is integrated on a micromachined piezoelectric substrate to enable fine structure splitting (FSS) removal [30], which

is an important requirement to observe highly entangled photons. The emission is characterized by a low multipair component [50,51], granting an advantage in quantum cryptographic applications, as compared to probabilistic approaches based on spontaneous parametric down-conversion light sources [52–54].

For the emitter used in this experiment (see Ref. [55] for a full characterization of the QD), we measure an  $FSS = 0.3(2)\mu\text{eV}$  via polarization-resolved photoluminescence, which, combined with a Purcell-enhanced X transition lifetime  $\tau_X = 100(10)\text{ps}$ , results in the emission of photon pairs with a  $0.94(1)$  fidelity to the  $|\phi^+\rangle$  state, as acquired with a full quantum state tomography [56]. In addition to fidelity to a maximally entangled state, the performance of an entanglement swapping protocol depends on photon indistinguishability, since the efficient optical implementation of polarization-encoded BSM relies on successful two-photon interference. High indistinguishability is more challenging to achieve, especially for photons generated via the XX-X cascade that are linked by energy-time entanglement [57,58]. We estimate indistinguishability by measuring the interference visibility in a Hong-Ou-Mandel (HOM) experiment using photons from the exciton to ground-state transition excited consecutively with a  $1.6\text{ns}$  delay. The HOM visibility we witness is limited to  $0.520(2)$ , due to an X transition linewidth  $\Delta E = 22(2)\mu\text{eV}$  (more than 6 times its Fourier limit) and which-path information inherent to two-photon cascaded emission [58], given by the ratio between X and XX lifetimes ( $\tau_{XX} = 67(5)\text{ps}$ ). As already demonstrated in the past literature [59], HOM visibility can be significantly increased by using low-time jitter detectors and employing temporal postselection at the cost of retaining a fraction of the total photon detection events. This technique was used to achieve quantum interference between QD photons [60,61], and then exploited in quantum teleportation experiments involving QD light [62–64], recently interfacing remote sources [55,65] and entanglement swapping with single [45,46] and remote sources [66]. By selecting a narrower time window for the coincidence events of our HOM experiment, the measured visibility can be increased up to  $0.79(2)$  (see Appendix A for the complete study of the visibility dependence on the coincidence window). Relying on theoretical modeling, we can expect a source with such features to be able to support a significant violation of Bell's inequality using swapped photons [25,67].

Before proceeding to QKD validation, we assess the fidelity of state preparation resulting from entanglement swapping with photons from our QD. We generate two sequential entangled photon pairs, exciting the same QD with two laser pulses separated by a delay of  $1.6\text{ns}$ . This double excitation is repeated at a rate of  $160\text{MHz}$ . X photons are separated using a volume Bragg grating filter and sent to an unbalanced Mach-Zehnder (MZ) interferometer, with the same excitation time delay on one of the arms, to induce interference between X photons emitted by distinct cascades, which we denote as early ( $X_e$ ) and late ( $X_l$ ) X photons. The BSM setup is composed of a balanced beam splitter (BS) and two polarizing beam splitters (PBSs), which allow the discrimination of two Bell states and is the optimal strategy that can be implemented using only linear optics [68]. Conditioned on

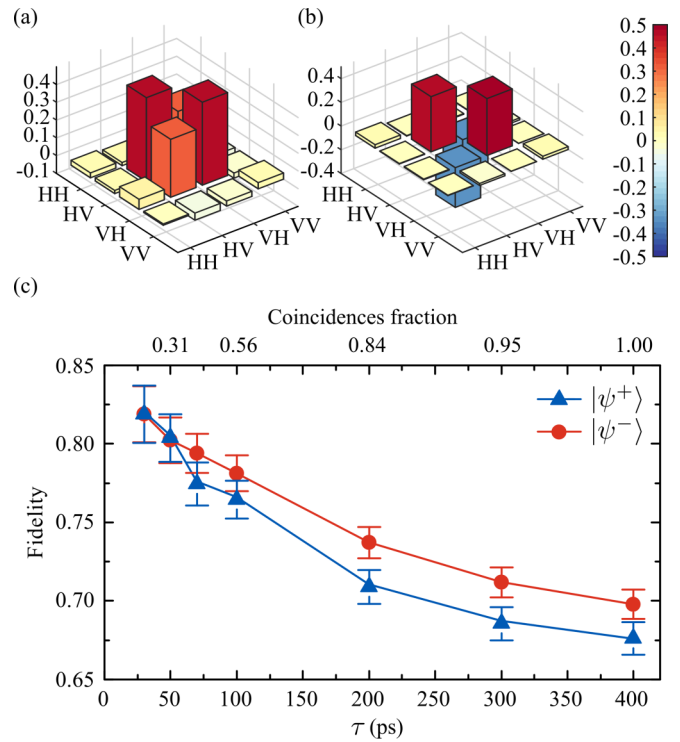


FIG. 2. Experimental entanglement swapping performance. (a) Real part of the density matrix of the biexciton photons given a  $|\psi^+\rangle$  BSM measured with a  $30\text{ps}$  time window on the BSM. (b) Same as in panel (a) for a  $|\psi^-\rangle$  BSM. (c) Fidelity of the biexciton photons state to the expected state as a function of the coincidence time window applied to the BSM events. The retained fraction of coincidence counts for different time windows is reported on the top axis. The total fourfold coincidences corresponding to the largest coincidence window, i.e.,  $400\text{ps}$ , are  $22\,958$ , corresponding to a coincidence rate of  $6.4\text{s}^{-1}$ .

the detection of one of the two outcomes of the BSM, a full quantum state tomography is performed on the remaining XX photon pairs—composed of the early ( $XX_e$ ) and late ( $XX_l$ ) XX photons—which are randomly separated with a  $50:50$  BS, to reconstruct their two-qubit polarization state. We analyze the fidelity of the resulting state to the expected Bell state as a function of the BSM coincidence temporal window. The results are reported in Fig. 2. As expected, the fidelity obtained with a large coincidence window is limited to  $0.69(1)$ , which is arguably insufficient to support an entanglement-based QKD protocol [41,69,70]. However, the fidelity improves with narrower BSM coincidence windows, at the cost of a lower coincidence rate. These results are compatible with a previous similar study [46] with the additional advantage of demonstrating the same operation in a state-of-the-art device with embedding in an optical microcavity for enhanced brightness and strain-tuning capabilities.

To perform entanglement-based QKD, XX photons are randomly separated by the BS and distributed instead to Alice and Bob, so that the two parties will probabilistically share an  $XX_e$  and  $XX_l$  photon pair. The experimental setup employed to realize the full QKD experiment with entanglement-swapped photons is schematically reported in

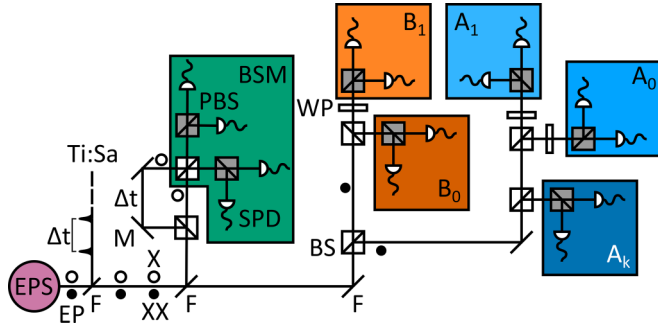


FIG. 3. Scheme of the QKD experimental setup. The entangled pair source (EPS) is excited by a pulsed Ti:Sapphire laser (Ti:Sa), doubled in repetition rate by an unbalanced Mach-Zehnder interferometer with a time delay  $\Delta t$ . The emitted pairs of photons, hollow (X photons) and full (XX photons) circles, are separated employing spectral filters (F) and sent, respectively, to the Bell state measurement setup and Alice and Bob. In the BSM, the state of the photons from subsequent pulses is projected into two possible Bell states by making them interfere in another unbalanced Mach-Zehnder interferometer with the same  $\Delta t$  and measuring coincidence combinations at four single-photon detectors (SPDs) placed at the exits of two PBSs. The remaining photons, in an entangled state after the BSM, are randomly sent to Alice and Bob setups, where their polarization state is measured in different, randomly chosen polarization bases:  $\{A_0, A_1, A_k\}$  and  $\{B_0, B_1\}$  by using SPDs, PBSs, and half-wave plates (WP).

Fig. 3. Alice and Bob implement the protocol measurement bases through BSs (to randomize the measurement choice) and combinations of half-wave plates (HWPs) and PBSs to perform the selected polarization state projections. Eight single-nanowire single-photon detectors from Single Quantum with  $<15$  ps time resolution are used for the four channels of the BSM and the four channels for key sharing, i.e.,  $\{B_0, A_k\}$ . Six single-photon avalanche photodiodes with  $<350$  ps time resolution are instead used for the remaining channels used for the check of Bell inequality violation, i.e.,  $\{B_1, A_1, A_0\}$ . The signal from all the detectors is sent to a time-to-digital converter (Time Tagger Ultra from Swabian Instruments) with a nominal 19 ps time resolution per channel. Only time tags related to fourfold coincidence events within a 15 ns window are retained to reduce the size of saved data and speed up postmeasurement analysis. To evaluate the performance of the QKD protocol, we monitor two crucial parameters from the relevant combinations of BSM-heralded two-photon correlations, namely, the quantum bit error rate (QBER) and the Bell parameter ( $S$ ). The QBER quantifies the discrepancy between the two copies of the raw key after sifting and is defined as  $Q = (1 - E(A_k, B_0))/2$ , where  $E$  is the expectation value calculated from the number of coincidences measured on the different combinations of outcomes of the two given measuring bases. The parameter  $S$  quantifies the violation of the computed CHSH inequality [40,42,44], defined, for our bases choice and distributed states, as  $S^{\psi^\pm} = -E(A_0, B_0) \pm E(A_0, B_1) + E(A_1, B_0) \pm E(A_1, B_1)$ . The parameters have been studied again as a function of the BSM coincidence window to identify the optimal choice to maximize QKD efficiency. We can see in Fig. 4(a) that the

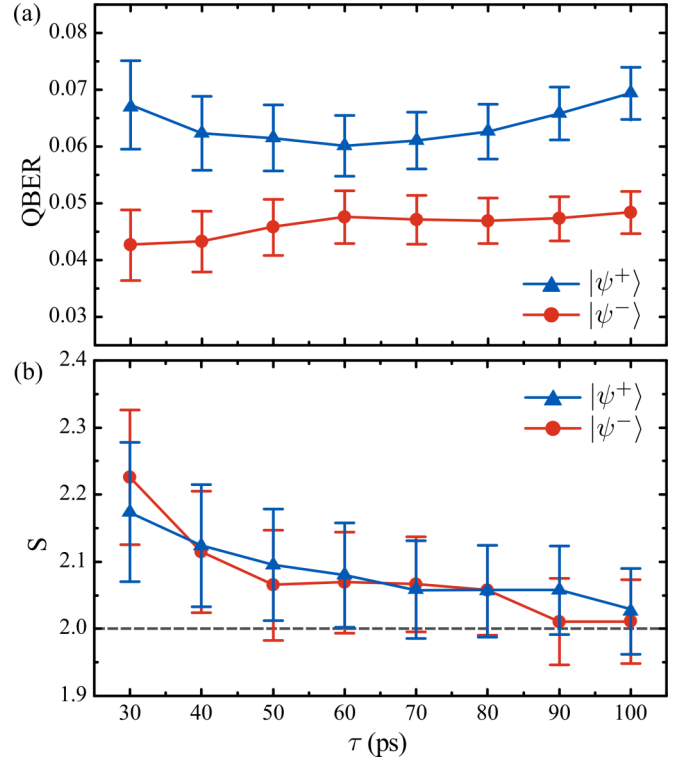


FIG. 4. QKD performance as a function of BSM coincidence time window. (a) QBER as a function of the BSM coincidence time window. (b) Bell parameter  $S$  as a function of the BSM coincidence time window. The threshold  $S = 2$  for classical correlation is highlighted by a dashed gray line.

QBER is relatively low, within the requirements for secure entanglement-based QKD [40,41], and is almost unaffected by the BSM time window. This fact stems from the employment of a 50% efficiency, polarization-selective BSM, and the specific choice of Alice and Bob to align the key channels, i.e.,  $\{A_k, B_0\}$ , to the same polarization axes of the BSM ( $H, V$ ). It can be shown [45,52] that, in this particular case, the expected values yielding the QBER (corresponding to the operators  $|HV\rangle\langle HV|$  and  $|VH\rangle\langle VH|$ ) are theoretically independent of the indistinguishability of the two swapped photons, when computed on their density matrix (explicitly reported in Appendix B). In these circumstances, the QBER coefficient is minimized because it depends almost exclusively on the degree of entanglement of the photon pairs rather than on their indistinguishability, the former being close to unity for our photon source.

In turn, correlations will generally be weaker when measured in other noncommuting bases due to the quantum state discrimination performed by the BSM, which also relies on indistinguishability. Therefore, the Bell parameter  $S$  will be affected by the BSM time window. The recorded experimental values of the Bell parameter are reported in Fig. 4(b). For the largest BSM coincidence window, the Bell parameter is lower than the threshold for classical correlations, but it is projected to exceed it for narrower time windows. Given these figures of merit, we now evaluate how the performed data exchange can support sharing a secret key in the asymptotic limit. In particular, we use the Devetak-Winter (DW) rate as

a lower bound to estimate the fraction of key rate that can be safely considered secure. Under the common assumption of Alice and Bob controlling their measuring apparatuses, this quantity is given by  $r_{\text{DW}} = 1 - h(Q) - h(Q + S/(2\sqrt{2}))$ , where  $h$  is the binary Shannon entropy [40]. This formula does not include the efficiency of the error correction algorithm, which depends on the dataset and the specific chosen implementation [71]. We define then the secure fraction of the distributed key (SKF) as  $\text{SKF} = \max(0, r_{\text{DW}})$ , since no part of the key can be assumed to be safe from an eavesdropper if  $r_{\text{DW}} < 0$ . The value of SKF is calculated as a function of the BSM coincidence window. As expected from the results of the violation of Bell's inequality, it is impossible to support a secure key exchange for large BSM coincidence time windows. It is often necessary to exceed a simple violation, depending on the specific value of QBER. The condition is satisfied for a 40 ps or narrower window, for the  $|\psi^-\rangle$  state only, and we experimentally obtain the maximum positive asymptotic SKF of 9(8)% for a 30 ps window. This result demonstrates that the current figures of merit of QD-based photon sources could already support secure communication in a scenario where entanglement is further distributed using entanglement swapping protocols.

In a quantum networking framework, it is relevant to consider the combination of our approach with entanglement distillation [72,73], a key element in quantum repeater architectures [74]. This operation usually requires efficient quantum memories and reliable application of two-qubit gates, so that an approach based on improving the source features, as ours, might deliver an efficiency improvement both in combination with entanglement distillation procedures and as an alternative to them. Simulating the application of a basic entanglement distillation protocol [72] to the experimental density matrices obtained as the outcome of entanglement swapping, we estimate that, by applying distillation on top of our timewise filtering procedure, it would be possible to achieve a total SKF of up to 15.7% for a coincidence time window of 30 ps, including in this value the success rate of the distillation protocol and a  $\frac{1}{2}$  factor due to the requirement of expending two photon pairs for each protocol run, to get as an outcome a single (more entangled) photon pair. This value corresponds to an average estimated fidelity (considering both  $|\psi^+\rangle$  and  $|\psi^-\rangle$  projections) of 0.92. In Appendix F, we report this analysis in detail and show how the distilled entanglement changes as a function of the time window applied to the BSM, for both  $|\psi^+\rangle$  and  $|\psi^-\rangle$  projections. We note that this distillation analysis is performed on the experimentally reconstructed density matrices assuming ideal local operations, and its practical implementation would involve experimentally significant requirements.

### III. DISCUSSION

Our results provide several valuable insights into which steps forward are required to make the presented approach practical. The first consideration is related to the overall secret key rate (SKR), defined as the product between the sifted key rate  $R_K$  and the SKF,  $\text{SKR} = R_K \times \text{SKF}$ . The sifted key rate depends on fourfold coincidence events, which are strongly affected by source inefficiency and setup

losses. The optimal SKR is given by a trade-off between the sifted key rate, which strictly decreases for narrower BSM coincidence windows, and the SKF, which improves for smaller windows. The optimal time window is obtained for a value of 30 ps corresponding to an estimated secure key rate of  $1 \times 10^{-3}$  bit/s. We want to underline that the chosen temporal window, which maximizes the SKR, does not maximize the photon indistinguishability. We point out that this rate makes the sharing of long keys still impractical, which is the reason why we focused our considerations on the asymptotic limit. It is interesting to consider how additional processing of the swapped photons might change the key rate. For instance, applying a simple distillation protocol, which is often included in quantum repeater architectures [5,75,76], and even for QKD applications [74], we estimate that it would be possible to more than double the secure key rate, mainly due to the improvement in the  $r_{\text{DW}}$  available for the projection  $|\psi^+\rangle$ . However, in this case, the optimal coincidence window would be 40 ps, due to the inevitable trade-off between the losses and the swapping fidelity improvements induced by narrower BSM time windows. Regarding the effective security of such an obtained key, it is important to discuss the specific attacks from an eavesdropper that the timewise filtering we perform might enable. We can consider the case in which such a malicious party had access to the events that were discarded by the communicating parties, namely, possible key events triggered by BSM coincidences featuring a delay larger than the selected window. We consider Alice to be the reference party for the sifted key. We consider then the key string that she would obtain if she considered a 30 ps time window on the BSM or a 400 ps one (that comprises almost all the fourfold coincidences). From the latter, we subtract the events that correspond to the 30 ps key, because Alice will keep only them, while the rest we suppose to be available to an eavesdropper, Eve. By computing the mutual information between the keys now in the hands of Alice and Eve, we find out that Eve can extract a negligible amount of information from her string to guess Alice's one (details are provided in Appendix E). On the other hand, some improvements are well within reach to significantly increase the key rate.

The largest opportunity for improvement is related to the brightness of the source. More specifically, the performance of the QD used in this experiment can be mainly improved in three aspects: blinking, extraction efficiency, and coupling efficiency into a single-mode fiber. Even limiting ourselves to combining state-of-the-art figures achieved for broadband QD sources, that is, negligible blinking [77], 85% extraction efficiency [28], and 65% single-mode coupling efficiency [29], would increase the single-photon rates by an order of magnitude and fourfold coincidences by about a factor of 350. Also, the pumping rate can be increased from 320 MHz to the gigahertz range due to the fast subnanosecond emission times of GaAs QDs.

A further significant area for improvement is linked to the fidelity of the state obtained from the entanglement swapping operation. Since the experimental secret key fraction is very close to the success threshold of the protocol, even small gains in QBER and Bell violation would lead to a much improved key throughput. As already mentioned, at a source level, the main challenge is related to photon indistinguishability. A QD

with better optical quality should already provide a performance closer to the limit imposed by the presence of time correlations in the radiative cascade [58]. Current research is aiming to improve this limit through photonic engineering of the transition lifetimes, by accelerating the first step of the cascade [78]; the application of external electric fields has been recently proved remarkably effective for this purpose [79]. A better trade-off in temporal filtering could be achieved as well with the use of a cutting-edge time-to-digital converter that can deliver a lower time resolution compared to the 19 ps (FWHM) of our current device. More practical scenarios will require the use of separated emitters, avoiding the probabilistic separation of the photon streams—a necessary part of our experimental design—but increasing the technical hurdles related to indistinguishability. However, the challenge of remote two-photon interference has been widely explored for QD sources, leading to the recent demonstrations of single-emitter-like performance in electrically controlled devices with high spectral stability [80] and of application in a benchmarking protocol such as quantum teleportation, even in practical scenarios [55,65]. Future devices able to combine electrical control with high-rate generation of entangled photon pairs will be able to successfully tackle integration into realistic network architectures. Although free-space networks remain the most suitable application framework for the emitters we employ [55], thanks to laser-mediated frequency conversion it is possible to match the optimal wavelength for fiber transmission [65,81,82]. High fidelity of the distributed entangled state is important to ensure that a QKD protocol can be sustained in a complete quantum repeater. Enough performance headroom needs to be available to account for the below-unity fidelity of the quantum memories used to store the qubits while required classical information is exchanged [23], although promising broadband quantum memories with fidelity above 95% are already under development [35].

Further insights could be gained by investigating relevant security aspects, such as quantitative analysis of possible side channels [4] and comparative studies of the viable choices for key refinement algorithms [83,84].

In conclusion, our work is a significant step toward the reliable implementation of QKD protocols over long distances, enabled by quantum repeaters. Quantum dot technology can play an important role in this outlook in combination with compatible high-performance hardware for quantum information storage and detection. This system integration and the anticipated advances in photon generation devices will lead to the practical implementation of quantum cryptography protocols into the next generation of repeater-assisted communication networks.

#### ACKNOWLEDGMENTS

The authors thank Dr. Edoardo Mornacchi from Swabian Instruments and A. Miriametro for the technical support, and K. Broccoletti for administrative support. This project has received funding from the European Union's Horizon 2020 Research and Innovation Program under Grant Agreement No. 899814 (Qurope) and from the QuantERA II Programme that has received funding from the European Union's Horizon 2020 Research and Innovation Program

under Grant Agreement No. 101017733 via the project QD-E-QKD. The authors also acknowledge support from MUR (Ministero dell'Università e della Ricerca) through the PNRR MUR Project No. PE0000023-NQSTI, the European Union's Horizon Europe Research and Innovation Program under the EPIQUE Project Grant Agreement No. 101135288. S.F.C.d.S. acknowledges São Paulo Research Foundation (FAPESP), Brasil, Processes No. 2024/08527-2 and No. 2024/21615-8 for financial support. A.R. acknowledges support of the EU HE EIC Pathfinder challenges action under Grant Agreement No. 101115575 (Q-ONE), from the QuantERA program via the project MEEDGARD (FFG Grant No. 906046), the Austrian Science Fund FWF via the Research Group FG5 (10.55776/FG5), and the cluster of excellence Quantum Science Austria (quantA) (10.55776/COE1) as well as the Linz Institute of Technology (LIT), and the LIT Secure and Correct Systems Lab, supported by the State of Upper Austria. M.G. and V.U. acknowledge support from the European Union's Horizon Europe Research and Innovation Program under the project QSNP, Grant Agreement No. 101114043, and support from the Czech Science Foundation under Project No. 21-44815L. This work is supported by the German Federal Ministry of Research, Technology and Space (BMFTR) through the project QR.N (Project No. 16KIS2206). This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 Research and Innovation Program (LiNQs, Grant Agreement No. 101042672). T.H.-L. acknowledges funding from the German Ministry of Research, Technology and Space (BMFTR) for the project Qecs (FKZ: 13N16272).

#### DATA AVAILABILITY

There are no publicly available research data or software supporting this manuscript. Requests for further information or data should be sent to the authors.

#### APPENDIX A: HONG-OU-MANDEL VISIBILITY

We report here the results from the Hong-Ou-Mandel experiment on consecutive photons from the same QD. The photons are allowed to interfere in the same Mach-Zehnder interferometer used for the BSM, with the difference that the coincidence events out of the last BS of the interferometer are measured with two SPDs. The histograms are built by measuring the coincidences of the co- and cross-polarized exits of the BSM setup, i.e., referring to Fig. 6, A-C and B-D for co-polarized and A-D and B-C for cross-polarized histograms. The results of the histogram for a single co- and cross-polarized combination, namely, A-C and B-C, are shown in the inset of Fig. 5. The raw HOM visibility, calculated as  $V = 1 - \frac{I_{\parallel}}{I_{\perp}}$ , where  $I_{\parallel/\perp}$  are the normalized counts of the co-polarized/cross-polarized coincidence peaks, averaging over all the possible combinations of the detectors, as a function of the delay time window ( $\Delta\tau$ ) is reported in the graph of Fig. 5.

#### APPENDIX B: DENSITY MATRIX FOR SWAPPED PHOTONS

We provide here a general description of the state of the swapped photons, depending on their level of indistinguishability.

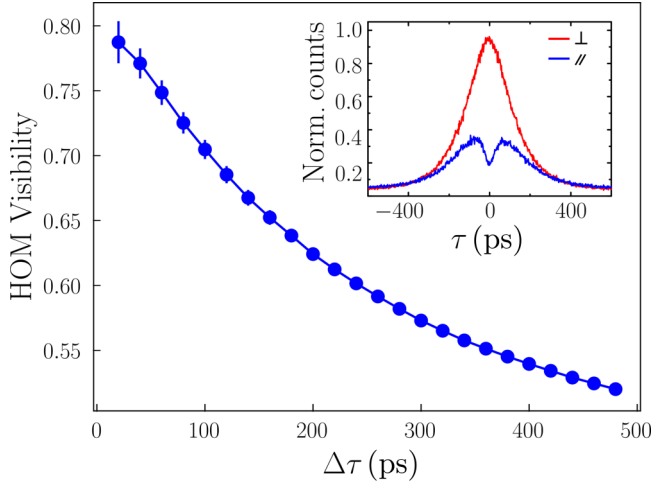


FIG. 5. Visibility of Hong-Ou-Mandel interference between subsequently emitted photons from the same QD as a function of the time delay window between the coincidence events. The inset shows the histograms of the coincidences in the case of co-polarized photons (blue) and cross-polarized photons (red).

bility. For the present discussion, we will not take into account further detrimental effects such as dephasing or decoherence, because we mainly aim to show the general dependence of QBER and  $S$  parameters on the quantum resources we exploit in the protocol, i.e., entanglement and indistinguishability. A more detailed modeling of entanglement swapping of QD photon pairs can be found in Refs. [45,67]. We also wish to highlight the importance of using a polarization-sensitive BSM to grant performances. We consider an entanglement swapping between two photon pairs in the maximally entangled state  $|\phi^+\rangle_{XX} = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$ , where we consider a zero FSS value, which is a good approximation of our experimental conditions. We opt for a density matrix representation, devoid of any spin scattering or cross-dephasing contribution,  $\rho_{XX}$ , and then we can write the four-photon density matrix as  $\rho_{X_2,X_1} \otimes \rho_{X_3,X_4}$ , where photon pairs  $\{1, 2\}$  and  $\{3, 4\}$  are generated by uncorrelated cascaded emissions. The BSM can be described as a projector  $\Pi$  on a specific Bell state, acting on the X photons 2 and 3. The “swapped” polarization state of the two XX photons after the BSM can be obtained by tracing out  $X_2$  and  $X_3$  from the four-photon density matrix [85]. For instance, we consider the projection on the  $|\psi^-\rangle$  Bell state:

$$\rho_{XX_1,XX_4}^{\psi^-} = \frac{\text{Tr}_{X_2,X_3}[\Pi_{X_2,X_3}^{\psi^-}(\rho_{X_2,XX_1} \otimes \rho_{X_3,XX_4})\Pi_{X_2,X_3}^{\psi^-}]}{\mathcal{N}_{\psi^-}} \quad (\text{B1})$$

including a normalization factor  $\mathcal{N}_{\psi^-}$ . We are interested in measuring and assimilating all events, as is common in quantum tomography and QKD. We will then integrate over the time distribution of photons, obtaining a  $\rho_{XX_1,XX_4}^{\psi^-}$ , independent of time. The final state of the two photons depends on the level of indistinguishability of the photon pairs involved, which determines the successful outcome of the swapping by shaping the probability distribution of the BSM results. We have to consider that, in the case of photon distinguishability, the probability of errors in the BSM becomes relevant, even if we neglect any experimental setup imperfections. We can

compute the probability that a  $|\psi^\pm\rangle$  event results in the BSM being triggered by a  $|\psi^\mp\rangle$ ,  $|\phi^-\rangle$  or  $|\phi^+\rangle$ ; thus, the probability that the swapping protocol results in the wrong output state. In this sense, employing a polarization-sensitive BSM helps, granting theoretical perfect discrimination between the subset  $\{|\psi^-\rangle, |\psi^+\rangle\}$  and  $\{|\phi^-\rangle, |\phi^+\rangle\}$ . The probabilities for the  $|\psi^\pm\rangle$  projections enabled by the 50% efficiency BSM then read as [45,52,67]

$$\begin{aligned} p(|\psi^-\rangle | \text{BSM}_{\psi^\pm}) &= \frac{1 \mp V}{2}, \\ p(|\psi^+\rangle | \text{BSM}_{\psi^\pm}) &= \frac{1 \pm V}{2}, \\ p(|\phi^+\rangle | \text{BSM}_{\psi^\pm}) &= p(|\phi^-\rangle | \text{BSM}_{\psi^\pm}) = 0, \end{aligned} \quad (\text{B2})$$

where  $V$  is the visibility obtained from a HOM experiment conducted on the two X photons. We point out that we are neglecting dephasing to highlight the effect of imperfect indistinguishability on the QKD performances. Finally, we can compute the total resulting density matrix for the swapping protocol, mixing the terms corresponding to the possible outcomes of the BSM. In particular, we consider the projection on the  $|\psi^-\rangle$  state:

$$\begin{aligned} \rho_{XX_1,XX_4}^{\text{swap}} &= \sum_{i=\phi^+, \phi^-, \psi^+, \psi^-} p(i | \text{BSM}_{\psi^-}) \times \rho_{XX_1,XX_4}^i \\ &= p(\psi^- | \text{BSM}_{\psi^-}) \times \rho_{XX_1,XX_4}^{\psi^-} \\ &\quad + p(\psi^+ | \text{BSM}_{\psi^-}) \times \rho_{XX_1,XX_4}^{\psi^+} \\ &= \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -V & 0 \\ 0 & -V & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \end{aligned} \quad (\text{B3})$$

From this very simple expression, it is clear that the indistinguishability does not have any effect on the QBER when the measurement is performed in the same polarization basis as the polarization-sensitive BSM. On the other hand, noise and experimental imperfections can decrease the correlation between the two photons, notwithstanding a very low FSS [45,67,86], as we witness in our results.

### APPENDIX C: DATA COLLECTION AND ANALYSIS WORKFLOW

The data collection is performed using a program that saves all time tags from the detector channels, conditioned on a fourfold coincidence within a 15 ns time window. This has been done to reduce the amount of data saved while still allowing for all postprocessing steps, such as coincidence data time filtering. The collected raw data are then processed and analyzed to extract relevant information. From these data, we calculate the total amount of fourfold coincidences over the whole period and, subsequently, the raw key rate, sifted key rate, and SKF. No accidentals count (background noise and imperfect value of the  $g^{(2)}(0)$ ) have been subtracted from the coincidence data.

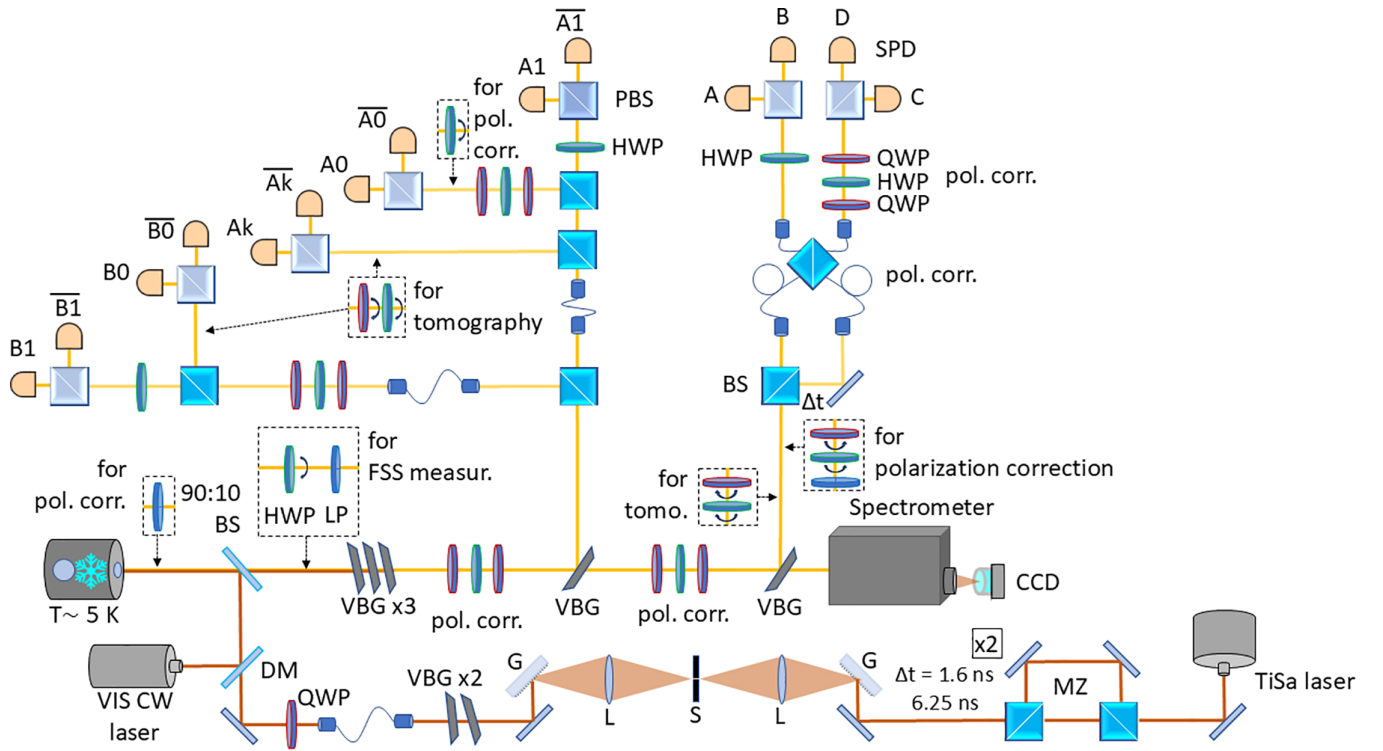


FIG. 6. Scheme of the experimental setup with all the different optical elements used. For the sake of simplicity, some of the mirrors were left out. The QD sits in a cryostat at 5 K. It is excited by a tunable Ti:Sapphire laser with a repetition rate of 80 MHz, doubled twice with a series of two unbalanced Mach-Zehnder (MZ) interferometers with delays on one of their arms of 1.6 and 6.25 ns. The pulse width of the laser is reduced with a 4-f pulse shaper equipped with two gratings (G), two lenses (L), and a movable and tunable slit (S). Two volume Bragg gratings (VBG) clean the laser spectrum to avoid unwanted laser light below the QD emission. A continuous-wave visible laser is used to stabilize the charge environment around the QD and reduce the amount of blinking. The laser excitation is sent to the QD via a 90:10 beam splitter. The light is focused on the sample by an aspheric lens mounted inside the cryostat. A series of three VBGs removes the backscattered laser light and cleans the signal from the QD. The emission from the X and XX transitions is separated with two VBGs. X photons are sent to the BSM measurement setup, where they are allowed to interfere with an unbalanced MZ matching the 1.6 ns delay of the excitation laser, and coincidences are measured at the exit ports of the last BS of the interferometer by two PBSs and four fiber-coupled, single-photon detectors (SPD). The XX photons are separated by a 50:50 BS and sent to Alice's and Bob's setups. The QKD is performed by sending the photons to the different channels via BSs and by counting coincidences with polarizing-beam splitters (PBSs), half-wave plates (HWP), and two fiber-coupled single-photon detectors for each basis. Several combinations of HWP and quarter-wave plates (QWPs) are used in the setup for polarization compensation.

#### APPENDIX D: COINCIDENCE RATES AND EFFICIENCIES

In this Appendix, we report on the experimental details and conditions of our work, focusing on the coincidence rates and efficiencies of the different parts of our experimental apparatus. A detailed description of all the optical components of the experimental setup is depicted in Fig. 6. The QD source emits a pair of photons with a probability  $\eta_{\text{pair}}$ , which is calculated from the single-channel rates of X and XX photons ( $R_X$  and  $R_{XX}$ ), the twofold coincidence rates ( $R_c$ ) measured during quantum tomography, and the repetition rate of the laser for the experiment  $R_{\text{laser}} = 320$  MHz, obtained by using a series of two Mach-Zehnder interferometers with delays of 6.25 and 1.6 ns. The latter delay is used to simulate the emission from two remote sources by matching it to the delay of the MZ interferometer in the BSM setup. The formula and the value for  $\eta_{\text{pair}}$  are the following:

$$\eta_{\text{pair}} = \frac{R_X \times R_{XX}}{R_c \times R_{\text{laser}}} = 0.278(2).$$

The extraction efficiency, defined as the fraction of photons collected by the first lens, was derived elsewhere for this source [30] and is taken here as  $\eta_{\text{extr}} = 0.69(4)$ . The count rates of each channel in the experiment were measured at the beginning of the data session, which lasted 24 h, and are reported in Table I. By dividing each channel count rate by the repetition rate of the laser  $R_{\text{laser}}$ , the detector efficiency  $\eta_{\text{det}}$  from the technical specifications of the manufacturer, and taking into account the protocol efficiency for each channel  $\eta_{\text{prot}}$ , attributable to the number of beam splitters and polarizing beam splitters in the path to the single detector (see Fig. 6), we calculate the end-to-end efficiency of the protocol  $\eta_{e2e}$ :

$$\eta_{e2e} = \frac{R_{\text{ch}}}{R_{\text{laser}} \times \eta_{\text{det}} \times \eta_{\text{prot}}}.$$

$\eta_{e2e}$  represents the probability that a single laser pulse results in a photon at the detector. By dividing the end-to-end efficiency by the extraction efficiency and the pair emission probability, we can remove the losses due to the source

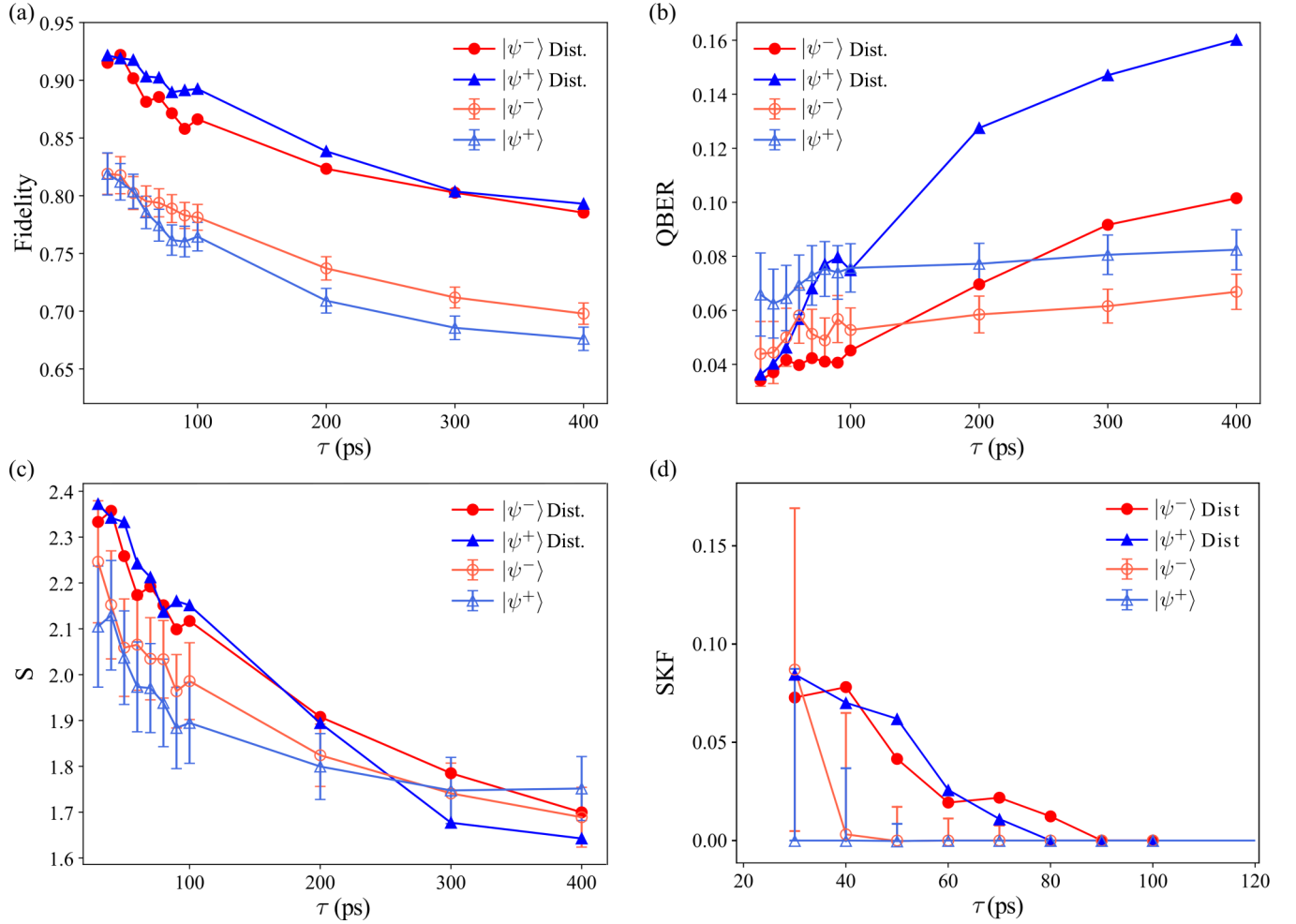


FIG. 7. Results of entanglement distillation on top of time filtering. We report here the resulting figures of merit estimated by simulating one single application of the DEJMPS entanglement purification protocol to the measured density matrix of the swapped photons for both  $|\psi^-\rangle$  and  $|\psi^+\rangle$  projections. Even only one step of distillation grants (a) a remarkable increase in the fidelity to the target state, for any chosen BSM coincidence time window. On the other hand, (b) QBER and (c) Bell violation ( $S$  parameter) are enhanced only for narrow time windows: this is because the protocol may need several steps to converge, if the initial fidelity is lower [72]. In any case, for time windows below 100 ps, both QBER and  $S$  are remarkably better after distillation, yielding (d) a positive secure key fraction for both  $|\psi^-\rangle$  and  $|\psi^+\rangle$ . The SKF for the distilled case takes into account the protocol efficiency, i.e.,  $\text{SKF}^{(D)} = \eta^{(D)}(\tau) \times \max(0, r_{\text{DW}}^{(D)}(\tau))$ . The swapping fidelity, the QBER, and the Bell parameter  $S$  for the case with no distillation are derived from the entanglement swapping experiment. The SKF is derived from the QKD data. For the distilled case they are all estimated from the output density matrix of the entanglement swapping. All error bars are computed with a Monte Carlo simulation, accounting for the Poissonian distribution of detection events. The points reporting  $\text{SKF} = 0$  (i.e.,  $r_{\text{DW}} \leq 0$ ) correspond to the failure of the protocol.

and estimate the setup efficiency  $\eta_{\text{setup}}$  for each channel (see Table I):

$$\eta_{\text{setup}} = \frac{\eta_{e2e}}{\eta_{\text{pair}} \times \eta_{\text{extr}}}.$$

The BSM setup coincidence rate was characterized during the HOM measurement. We report the twofold coincidence rates measured for the  $|\psi^+\rangle$  state, which is 1.8 kcps, under comparable conditions to those of the experiment, with comparable countrates on the single channels. We expect similar numbers for the  $|\psi^-\rangle$  state.

The total number of fourfold coincidences measured during the experiment is 27 450, measured by counting all the possible combinations of four channels in the BSM setup (including double clicks stemming from unwanted combinations

due to the subpar indistinguishability of the source) and between Alice's and Bob's setups (disregarding double clicks on a single party's setup). The  $|\psi^+\rangle$  and  $|\psi^-\rangle$  triggered fourfold coincidences are, respectively, 10 725 and 11 199. Of these events, the ones generating a cryptographic key, i.e., the sifted key, are 11 235 resulting in a sifted key rate of  $r_{\text{sift}} = 0.13$  cps.

#### APPENDIX E: CALCULATION OF THE MUTUAL INFORMATION BETWEEN EVE AND ALICE

We consider the case of an eavesdropper Eve having access to the key string that Alice has dropped because they correspond to fourfold coincidences featuring a long delay between photons undergoing the BSM. We wish to understand if Eve can infer anything about Alice's key (which we suppose

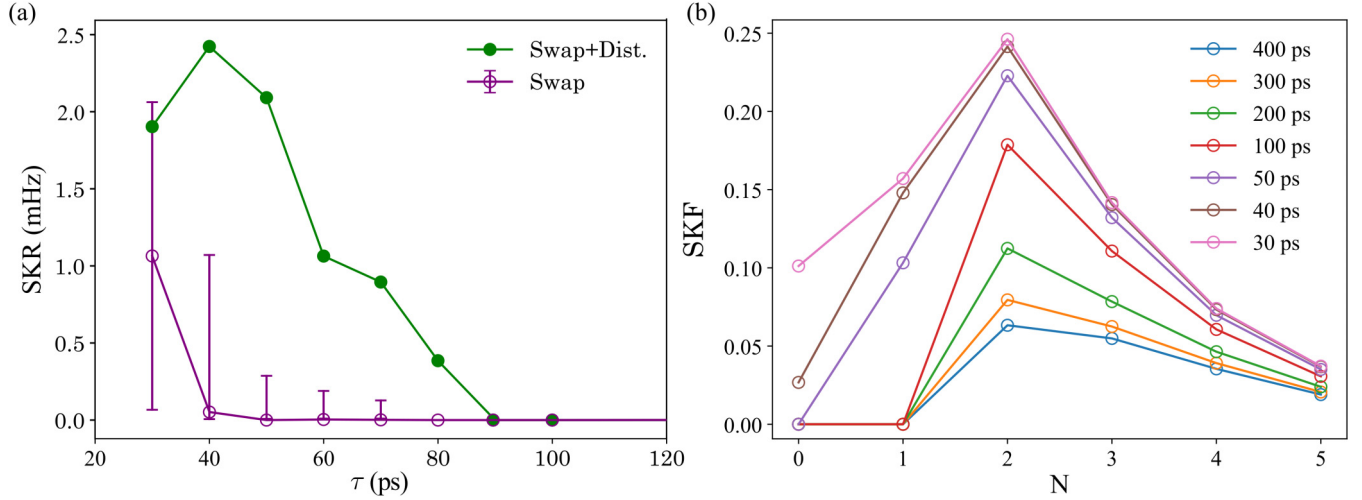


FIG. 8. Optimal distillation parameters. We seek the distillation parameters maximizing the SKR, accounting for the losses due to time filtering. For one distillation step, (a) the optimal BSM time window is  $\tau = 40$  ps, maximizing the trade-off between collected events and SKR. We investigate how multiple applications of the purification protocol benefit the entanglement distribution performance. We report (b) the SKF as a function of the  $N$  number of distillation rounds, for different BSM time windows. The distillation protocol is so efficient that saturation is already reached for  $N = 2$  purification steps: following applications of the protocol only cause a decrease in the overall efficiency of the protocol, given the loss of half the shared pairs due to the DEJMPS distillation scheme.

to be the reference for the key reconciliation) from the bits in her possession. In principle, we expect no correlation at all between Alice's key (X string) and Eve's string of bits (Y string): they are the result of two similar distributions, but they should be two random sequences of equally distributed 0s and 1s, so we expect them to be independent. To confirm that, we compute mutual information between the two strings X and Y. Since the two sequences have different lengths and the events cannot be put in correspondence, we cannot compute pointwise mutual information [87], which would require a clear notion of joint occurrence to build a joint probability

distribution. On the other hand, we can sample the individual probability distributions underlying Alice's string  $P_A$  and Eve's string  $P_E$  and compute the mutual information  $I(X|Y)$  using, for instance, the Jensen-Shannon divergence [88,89]:

$$I(X|Y) = \text{JSD}(P_A|P_E) = H\left(\frac{P_A + P_E}{2}\right) - \frac{H(P_A) + H(P_E)}{2}, \quad (\text{E1})$$

where  $H(P) = -\sum_{x \in \{0,1\}} P(x) \log_2(P(x))$  is the Shannon entropy. This estimate of mutual information quantifies how

TABLE I. Measured countrates on each channel of the experiment and efficiencies. Channels A, B, C, and D are related to the BSM and  $A_n$  and  $B_n$  to Alice and Bob, respectively (see Fig. 6).  $\eta_{\text{prot}}$  is the efficiency of the protocol related to the number of BSs and PBSs in the relative channel path.  $\eta_{\text{pair}}$  is the pair emission probability, calculated from the single and twofold counting rates between Xs and XXs.  $\eta_{\text{extr}}$  is the brightness at the first lens calculated for this source in Ref. [30]. The detector efficiencies  $\eta_{\text{det}}$  are extracted from the technical specifications provided by the manufacturer. The end-to-end efficiency ( $\eta_{e2e}$ ) is the probability that a laser pulse generates a photon at the detector. The setup efficiency  $\eta_{\text{setup}}$  is calculated from the previous efficiencies.

| Channel name | Countrate (kcps) | $\eta_{\text{prot}}$ | $\eta_{\text{pair}}$ | $\eta_{\text{extr}}$ | $\eta_{\text{det}}$ | $\eta_{e2e}$             | $\eta_{\text{setup}}$   |
|--------------|------------------|----------------------|----------------------|----------------------|---------------------|--------------------------|-------------------------|
| A            | 667(26)          | 0.25                 | 0.278(2)             | 0.69(4)              | 0.80                | $1.04(4) \times 10^{-2}$ | $5.4(4) \times 10^{-2}$ |
| B            | 496(22)          | "                    | "                    | "                    | 0.84                | $7.4(3) \times 10^{-3}$  | $3.9(3) \times 10^{-2}$ |
| C            | 612(25)          | "                    | "                    | "                    | 0.84                | $9.1(4) \times 10^{-3}$  | $4.7(3) \times 10^{-2}$ |
| D            | 549(23)          | "                    | "                    | "                    | 0.84                | $8.2(3) \times 10^{-3}$  | $4.3(3) \times 10^{-2}$ |
| $A_k$        | 332(18)          | 0.125                | "                    | "                    | 0.80                | $1.04(6) \times 10^{-2}$ | $5.4(4) \times 10^{-2}$ |
| $\bar{A}_k$  | 265(16)          | "                    | "                    | "                    | 0.80                | $8.3(5) \times 10^{-3}$  | $4.3(4) \times 10^{-2}$ |
| $A_0$        | 86(9)            | 0.0625               | "                    | "                    | 0.64                | $6.8(7) \times 10^{-3}$  | $3.5(4) \times 10^{-2}$ |
| $\bar{A}_0$  | 82(9)            | "                    | "                    | "                    | 0.64                | $6.4(7) \times 10^{-3}$  | $3.3(4) \times 10^{-2}$ |
| $A_1$        | 111(11)          | "                    | "                    | "                    | 0.64                | $8.6(8) \times 10^{-3}$  | $4.5(5) \times 10^{-2}$ |
| $\bar{A}_1$  | 72(8)            | "                    | "                    | "                    | 0.64                | $5.6(7) \times 10^{-3}$  | $2.9(4) \times 10^{-2}$ |
| $B_0$        | 139(12)          | 0.125                | "                    | "                    | 0.82                | $4.3(4) \times 10^{-3}$  | $2.2(2) \times 10^{-2}$ |
| $\bar{B}_0$  | 115(11)          | "                    | "                    | "                    | 0.75                | $3.8(4) \times 10^{-3}$  | $2.0(2) \times 10^{-2}$ |
| $B_1$        | 120(11)          | "                    | "                    | "                    | 0.50                | $6.0(5) \times 10^{-3}$  | $3.1(3) \times 10^{-2}$ |
| $\bar{B}_1$  | 98(10)           | "                    | "                    | "                    | 0.61                | $4.0(4) \times 10^{-3}$  | $2.1(2) \times 10^{-2}$ |

easy it would be to recognize whether a character has been extracted from  $X$  or  $Y$ , i.e., whether it is part of the key or not, knowing its probability distribution [89]. The computation of this quantity over  $X$  and  $Y$  returns a negligible  $I(X|Y) = 2 \times 10^{-5}$ , which can be attributed to the slight unbalancing in the distribution of 0s and 1s due to experimental imperfections.

## APPENDIX F: ENTANGLEMENT DISTILLATION

We apply an entanglement distillation protocol to the swapped biphoton polarization state reconstructed from measurements to explore the performance of combining distillation with our time-sensitive entanglement swapping protocol. We consider two basic seminal protocols as a reference [72,90], applied to the case of the states employed in our QKD protocol  $|\psi^\pm\rangle$ . The protocol works by employing two copies of the state for each distillation round to obtain a higher entangled single qubit pair. In the protocol, two qubit pairs are distributed between the two communicating parties, Alice and Bob, with initial fidelity  $F > \frac{1}{2}$  to the state  $|\psi^\pm\rangle$  (they do not necessarily have to be in a Werner state [72]). First, Alice applies a one-qubit transformation on her qubits; this operation turns  $|\psi^\pm\rangle$  into  $|\phi^\pm\rangle$ . After that, the polarization state of the two qubit pairs will have an  $F > \frac{1}{2}$  to the  $|\phi^\pm\rangle$  state, and we can apply the Deutsch-Ekert-Jozsa-Macchiavello-Popescu-Sanpera (DEJMPS) protocol [72]. Alice and Bob perform a bilateral (asymmetrical) “twist” to the state of their qubits, then they perform a bilateral CNOT gate on the qubits they hold, using as control the qubits from the first pair and as target the qubits of the second pair. Then, they measure the target qubit pair in the  $Z$  basis ( $H/V$  polarization basis) and keep the qubits from the control pair if the result of the measurement coincides. Depending on the starting fidelity, the efficiency of this protocol will generally be lower than 1, and the number of iterations required for bringing the output state to a maximally entangled state will differ. The state of the retained qubit is then transformed back to more closely match the target final state  $|\psi^\pm\rangle$ . To adapt this protocol to our case, we consider the reconstructed matrices from the entanglement swapping experiment (see Fig. 2)  $\bar{\rho}$  and use two identical copies of them as the two states to be used in the distillation protocol, resulting in a distilled average matrix  $\bar{\rho}_T$ . The reason for this is that it is not possible to reconstruct the original “swapped” density matrices from the coincidence counts collected in the QKD protocol. Since we used a 50% BSM, we will have two different input states  $\bar{\rho}^+$  and  $\bar{\rho}^-$  that we treat separately and transform to be more similar to  $|\phi^\pm\rangle$ , using a different operator depending on the BSM projection. For example, if the state of the system has an  $F > \frac{1}{2}$  to the state  $|\psi^+\rangle$ , we have to apply the following transformation:

$$\begin{aligned} \bar{\rho}_T^+ &= U(|\psi^+\rangle \rightarrow |\phi^+\rangle) \bar{\rho} U(|\psi^+\rangle \rightarrow |\phi^+\rangle)^\dagger \\ &= (I \otimes \sigma_X) \bar{\rho} (I \otimes \sigma_X)^\dagger. \end{aligned} \quad (F1)$$

In the case of a  $|\psi^-\rangle$  target state, the operator to apply would be  $U(|\psi^-\rangle \rightarrow |\phi^+\rangle) = I \otimes \sigma_X \sigma_Z$  [90]. We apply this operation on two copies of the state  $\bar{\rho}$ , so that the total considered state is  $\bar{\rho}_T^+ \otimes \bar{\rho}_T^+$ . The qubits from the first pair are denoted as 0, 1, and the ones from the second pair are addressed as

2, 3. In our framework, Alice holds qubits 0 and 2, and Bob holds qubits 1 and 3. Then, we run the DEJMPS purification protocol [72]: the first step is a bilateral rotation along the  $x$  axis:

$$R_X(\phi) = \begin{pmatrix} \cos(\frac{\phi}{2}) & -i \sin(\frac{\phi}{2}) \\ -i \sin(\frac{\phi}{2}) & \cos(\frac{\phi}{2}) \end{pmatrix}. \quad (F2)$$

Alice applies to both her qubits an  $R_X(\pi/2)$  rotation, and Bob applies to his qubits an  $R_X(-\pi/2)$ . Then, Alice and Bob apply a CNOT gate, using qubits from the first pair as control and the ones from the second pair as targets, obtaining a state  $\rho_{\text{CNOT}}$ . Then, a projection over the  $\{H, V\}$  basis is performed on qubits 2, 3 (the target qubits), which selects only those outcomes where both qubits are measured in the same polarization state. This corresponds to the application of the projector  $P^{//} = |HH\rangle\langle HH| + |VV\rangle\langle VV|$  on qubits 2 and 3. Finally, qubits 2, 3 are traced away, leaving Alice and Bob with the qubit pair 0 and 1 only. Explicitly, Alice and Bob hold the state

$$\rho_{0,1} = \text{Tr}_{2,3}((I_{0,1} \otimes P_{2,3}^{//}) \rho_{\text{CNOT}} (I_{0,1} \otimes P_{2,3}^{//})). \quad (F3)$$

Now, the state features a  $F' > F$  to the  $|\phi^\pm\rangle$  state, which can be turned into fidelity to the  $|\psi^\pm\rangle$  state by applying a suitable two-qubit operator. The success probability of the protocol is  $p_{\text{succ}} = \text{Tr}((I_{1,2} \otimes P_{3,4}^{//}) \rho_{\text{CNOT}} (I_{1,2} \otimes P_{3,4}^{//}))$  resulting in a compound efficiency for a single distillation step  $\eta = \frac{p_{\text{succ}}}{2}$ .

We apply the protocol to the density matrices measured at different BSM postselection time windows. In Fig. 7(a), we show the fidelity to the target state after application of a single entanglement distillation. From the distilled matrices, we compute both the Bell parameter  $S$  and QBER (Figs. 7(b) and 7(c)). Since the distillation yield depends on the initial entanglement, all these quantities depend on the BSM coincidence time window. We compare the QKD figures of merit expected from the distilled swapped state with those directly obtained by the entanglement swapping experiment. Distillation clearly enhances the potential QKD performances of the swapped two-photon state, considering the measured density matrices. To correctly compare the key rates between the case with or without distillation, we have to additionally consider the entanglement purification efficiency. Since the probability of success of the distillation depends on the fidelity  $F$  of the initial state, also  $p_{\text{succ}}$  depends on the BSM coincidence time window  $\tau$ , and we have to consider a time-window-dependent overall distillation protocol efficiency  $\eta^{(D)}(\tau)$ . In Fig. 7(d), we report the  $\text{SKF}(\tau) = \max(0, r_{\text{DW}}(\tau))$  for different  $\tau$ 's as obtained in the QKD experiment, in comparison with the  $\text{SKF}^{(D)}(\tau) = \eta^{(D)}(\tau) \times \max(0, r_{\text{DW}}^{(D)}(\tau))$  effective secure fraction expected for a QKD experiment after distillation. As stated in the main text, in the case of the actual QKD experiment, the  $|\psi^+\rangle$  projection does not yield a positive SKF for any  $\tau$ . A distillation step after swapping gives instead the possibility to extract a secure key from both the projections, practically doubling the effective SKF, which would amount to a total 15.7% for a BSM time window  $\tau = 30$  ps. This advantage might be even larger, considering optimized or more sophisticated distillation protocols [91]. If we consider the experimental count rates recorded for the various  $\tau$ 's in the QKD protocol, we can actually identify the optimal BSM time

window to get the highest SKR, accounting for the trade-off between the SKF and the number of lost counts due to time filtering.

In Fig. 8(a), we report the effective SKR that can be expected considering the sifted key count rate  $R_K$  and the SKF,  $\text{SKR} = R_K(\tau) \times \text{SKF}(\tau)$ , summing the contribution from both projections  $|\psi^\pm\rangle$ . The practical optimal BSM window is found to be  $\tau = 40$  ps, granting, for one distillation step, an SKR of  $\approx 2.5 \times 10^{-3}$  bit/s. Finally, we explore the effect of the application of multiple distillation steps to the swapped density matrix, from  $N = 0$  (no distillation) to  $N = 5$  steps. We wish to estimate the number of purification rounds yielding the highest SKF. In general, such an estimate is not trivial: since for each purification round, half the qubit pairs are discarded, we can expect that, after the protocol saturation, no beneficial effect is recorded by further distillation rounds. As we show in Fig. 8(b), starting from the fidelity values of the swapping experiment, already two distillation steps are enough to reach a maximum in the SKF.

Nonetheless, we need to emphasize that the analysis presented above assumes ideal two-qubit gates and does not account for imperfections inherent to a practical implementation of the distillation protocol. In a realistic quantum repeater, entanglement purification via DEJMPS requires heralded quantum memories to synchronize and retune photons after transmission, as well as reliable bilateral two-qubit gate operations [6]. Furthermore, rates would be limited by finite memory storage-and-retrieval efficiency, gate fidelity, and additional channel losses, all of which would reduce the effective distillation yield and possibly shift the optimal operating point. Our analysis should therefore be understood as a state-quality benchmark: it establishes that the swapped states produced by our source lie above the distillation threshold and that very few purification rounds ( $N = 2$ ) suffice to saturate the achievable secure key fraction, with both BSM projections becoming usable for key generation after a single distillation step. These results are encouraging in view of integration with quantum memory platforms operating at compatible wavelengths.

- 
- [1] H. J. Kimble, The quantum internet, *Nature (London)* **453**, 1023 (2008).
  - [2] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, *Science* **362**, eaam9288 (2018).
  - [3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, *Adv. Opt. Photonics* **12**, 1012 (2020).
  - [4] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* **92**, 025002 (2020).
  - [5] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, Quantum repeaters: From quantum networks to the quantum internet, *Rev. Mod. Phys.* **95**, 045006 (2023).
  - [6] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Quantum repeaters: The role of imperfect local operations in quantum communication, *Phys. Rev. Lett.* **81**, 5932 (1998).
  - [7] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, Quantum repeaters based on atomic ensembles and linear optics, *Rev. Mod. Phys.* **83**, 33 (2011).
  - [8] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, Inside quantum repeaters, *IEEE J. Sel. Top. Quantum Electron.* **21**, 78 (2015).
  - [9] D. Lago-Rivera, S. Grandi, J. V. Rakonjac, A. Seri, and H. de Riedmatten, Telecom-heralded entanglement between multi-mode solid-state quantum memories, *Nature (London)* **594**, 37 (2021).
  - [10] X. Liu, J. Hu, Z.-F. Li, X. Li, P.-Y. Li, P.-J. Liang, Z.-Q. Zhou, C.-F. Li, and G.-C. Guo, Heralded entanglement distribution between two absorptive quantum memories, *Nature (London)* **594**, 41 (2021).
  - [11] A. Khalique and B. C. Sanders, Practical long-distance quantum key distribution through concatenated entanglement swapping with parametric down-conversion sources, *J. Opt. Soc. Am. B* **32**, 2382 (2015).
  - [12] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, Rate-loss analysis of an efficient quantum repeater architecture, *Phys. Rev. A* **92**, 022357 (2015).
  - [13] A. Scherer, B. C. Sanders, and W. Tittel, Long-distance practical quantum key distribution by entanglement swapping, *Opt. Express* **19**, 3004 (2011).
  - [14] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, and M. Curty, Advances in device-independent quantum key distribution, *npj Quantum Inf.* **9**, 10 (2023).
  - [15] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim, *et al.*, A device-independent quantum key distribution system for distant users, *Nature (London)* **607**, 687 (2022).
  - [16] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E.-Z. Tan, *et al.*, Experimental quantum key distribution certified by Bell's theorem, *Nature (London)* **607**, 682 (2022).
  - [17] B.-W. Lu, C.-W. Yang, R.-Q. Wang, B.-F. Gao, Y.-Z. Zhen, Z.-G. Wang, J.-K. Shi, Z.-Q. Ren, T. A. Hahn, E. Y.-Z. Tan, *et al.*, Device-independent quantum key distribution over 100 km with single atoms, *Science* **391**, 592 (2026).
  - [18] W.-Z. Liu, Y.-B. Zhou, J.-P. Chen, B. Wang, A. Teng, X.-W. Han, G.-C. Liu, Z.-J. Zhang, Y. Yang, F.-G. Liu, *et al.*, Long-lived remote ion-ion entanglement for scalable quantum repeaters, *Nature (London)* **652**, 51 (2026).
  - [19] Y.-F. Jiang, L. Huang, Y.-Z. Zhang, L. Zhang, Q.-C. Sun, Z.-P. Li, H. Li, W. Zhang, L. You, F. Xu, *et al.*, Entanglement swapping enables the practical security of quantum cryptography, *Entropy* **28**, 518 (2026).
  - [20] N. Gisin, S. Pironio, and N. Sangouard, Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier, *Phys. Rev. Lett.* **105**, 070501 (2010).

- [21] J. Kołodzyński, A. Máttar, P. Skrzypczyk, E. Woodhead, D. Cavalcanti, K. Banaszek, and A. Acín, Device-independent quantum key distribution with single-photon sources, *Quantum* **4**, 260 (2020).
- [22] H. Jayakumar, A. Predojević, T. Huber, T. Kauten, G. S. Solomon, and G. Weihs, Deterministic photon pairs and coherent optical control of a single quantum dot, *Phys. Rev. Lett.* **110**, 135505 (2013).
- [23] J. Neuwirth, F. Basso Basset, M. B. Rota, E. Roccia, C. Schimpf, K. D. Jöns, A. Rastelli, and R. Trotta, Quantum dot technology for quantum repeaters: From entangled photon generation toward the integration with quantum memories, *Mater. Quantum Technol.* **1**, 043001 (2021).
- [24] P. Lodahl, Quantum-dot based photonic quantum networks, *Quantum Sci. Technol.* **3**, 013001 (2018).
- [25] C. Schimpf, M. Reindl, F. Basso Basset, K. D. Jöns, R. Trotta, and A. Rastelli, Quantum dots as potential sources of strongly entangled photons: Perspectives and challenges for applications in quantum networks, *Appl. Phys. Lett.* **118**, 100502 (2021).
- [26] C.-Y. Lu and J.-W. Pan, Quantum-dot single-photon sources for the quantum internet, *Nat. Nanotechnol.* **16**, 1294 (2021).
- [27] Y. Yu, S. Liu, C.-M. Lee, P. Michler, S. Reitzenstein, K. Srinivasan, E. Waks, and J. Liu, Telecom-band quantum dot technologies for long-distance quantum networks, *Nat. Nanotechnol.* **18**, 1389 (2023).
- [28] J. Liu, R. Su, Y. Wei, B. Yao, S. F. C. da Silva, Y. Yu, J. Iles-Smith, K. Srinivasan, A. Rastelli, J. Li, *et al.*, A solid-state source of strongly entangled photon pairs with high brightness and indistinguishability, *Nat. Nanotechnol.* **14**, 586 (2019).
- [29] H. Wang, H. Hu, T.-H. Chung, J. Qin, X. Yang, J.-P. Li, R.-Z. Liu, H.-S. Zhong, Y.-M. He, X. Ding, *et al.*, On-demand semiconductor source of entangled photons which simultaneously has high fidelity, efficiency, and indistinguishability, *Phys. Rev. Lett.* **122**, 113602 (2019).
- [30] M. B. Rota, T. M. Krieger, Q. Buchinger, M. Beccaceci, J. Neuwirth, H. Huet, N. Horová, G. Lovicu, G. Ronco, S. F. C. da Silva, *et al.*, A source of entangled photons based on a cavity-enhanced and strain-tuned GaAs quantum dot, *eLight* **4**, 13 (2024).
- [31] Y.-H. Chen, M.-J. Lee, I.-C. Wang, S. Du, Y.-F. Chen, Y.-C. Chen, and I. A. Yu, Coherent optical memory with high storage efficiency and large fractional delay, *Phys. Rev. Lett.* **110**, 083601 (2013).
- [32] M. Namazi, C. Kupchak, B. Jordaan, R. Shahrokhshahi, and E. Figueroa, Ultralow-noise room-temperature quantum memory for polarization qubits, *Phys. Rev. Appl.* **8**, 034023 (2017).
- [33] J. Wolters, G. Buser, A. Horsley, L. Béguin, A. Jöckel, J.-P. Jahn, R. J. Warburton, and P. Treutlein, Simple atomic quantum memory suitable for semiconductor quantum dot single photons, *Phys. Rev. Lett.* **119**, 060502 (2017).
- [34] J.-S. Tang, Z.-Q. Zhou, Y.-T. Wang, Y.-L. Li, X. Liu, Y.-L. Hua, Y. Zou, S. Wang, D.-Y. He, G. Chen, *et al.*, Storage of multiple single-photon pulses emitted from a quantum dot in a solid-state quantum memory, *Nat. Commun.* **6**, 8652 (2015).
- [35] J. H. Davidson, P. Lefebvre, J. Zhang, D. Oblak, and W. Tittel, Improved light-matter interaction for storage of quantum states of light in a thulium-doped crystal cavity, *Phys. Rev. A* **101**, 042333 (2020).
- [36] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, A comprehensive design and performance analysis of low Earth orbit satellite quantum communication, *New J. Phys.* **15**, 023006 (2013).
- [37] M. H. Appel, A. Ghorbal, N. Shofar, L. Zaporski, S. Manna, S. F. C. da Silva, U. Haeusler, C. Le Gall, A. Rastelli, D. A. Gangloff, and M. Atatüre, A many-body quantum register for a spin qubit, *Nat. Phys.* **21**, 368 (2025).
- [38] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Experimental entanglement swapping: Entangling photons that never interacted, *Phys. Rev. Lett.* **80**, 3891 (1998).
- [39] A. Acín, S. Massar, and S. Pironio, Efficient quantum key distribution secure against no-signalling eavesdroppers, *New J. Phys.* **8**, 126 (2006).
- [40] 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).
- [41] A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [42] 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).
- [43] A. Ling, M. P. Peloso, I. Marcikic, V. Scarani, A. Lamas-Linares, and C. Kurtsiefer, Experimental quantum key distribution based on a Bell test, *Phys. Rev. A* **78**, 020301 (2008).
- [44] 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).
- [45] F. Basso Basset, M. B. Rota, C. Schimpf, D. Tedeschi, K. D. Zeuner, S. F. Covre da Silva, M. Reindl, V. Zwiller, K. D. Jöns, A. Rastelli, *et al.*, Entanglement swapping with photons generated on demand by a quantum dot, *Phys. Rev. Lett.* **123**, 160501 (2019).
- [46] M. Zopf, R. Keil, Y. Chen, J. Yang, D. Chen, F. Ding, and O. G. Schmidt, Entanglement swapping with semiconductor-generated photons violates Bell's inequality, *Phys. Rev. Lett.* **123**, 160502 (2019).
- [47] M. Müller, S. Bounouar, K. D. Jöns, M. Glässl, and P. Michler, On-demand generation of indistinguishable polarization-entangled photon pairs, *Nat. Photon.* **8**, 224 (2014).
- [48] D. Huber, M. Reindl, S. F. Covre da Silva, C. Schimpf, J. Martín-Sánchez, H. Huang, G. Piredda, J. Edlinger, A. Rastelli, and R. Trotta, Strain-tunable GaAs quantum dot: A nearly dephasing-free source of entangled photon pairs on demand, *Phys. Rev. Lett.* **121**, 033902 (2018).
- [49] C. Schimpf, F. Basso Basset, M. Aigner, W. Attenender, L. Ginés, G. Undeutsch, M. Reindl, D. Huber, D. Gangloff, E. A. Chekhovich, C. Schneider, S. Höfling, A. Predojević, R. Trotta, and A. Rastelli, Hyperfine interaction limits polarization entanglement of photons from semiconductor quantum dots, *Phys. Rev. B* **108**, L081405 (2023).
- [50] L. Hanschke, K. A. Fischer, S. Appel, D. Lukin, J. Wierzbowski, S. Sun, R. Trivedi, J. Vučković, J. J. Finley, and K. Müller, Quantum dot single-photon sources with ultra-low multi-photon probability, *npj Quantum Inf.* **4**, 43 (2018).
- [51] J. Neuwirth, F. Basso Basset, M. B. Rota, J.-G. Hartel, M. Sartison, S. F. Covre da Silva, K. D. Jöns, A. Rastelli, and R. Trotta, Multipair-free source of entangled photons in the solid state, *Phys. Rev. B* **106**, L241402 (2022).

- [52] F. Basso Basset, F. Salusti, L. Schweickert, M. B. Rota, D. Tedeschi, S. F. Covre da Silva, E. Roccia, V. Zwiller, K. D. Jöns, A. Rastelli, *et al.*, Quantum teleportation with imperfect quantum dots, *npj Quantum Inf.* **7**, 7 (2021).
- [53] R. Hošák, I. Straka, A. Predojević, R. Filip, and M. Ježek, Effect of source statistics on utilizing photon entanglement in quantum key distribution, *Phys. Rev. A* **103**, 042411 (2021).
- [54] M. Gumberidze and V. Usenko, Feasibility of entanglement-based QKD protocols with SPDC and quantum-dot sources, *Opt. Express* **34**, 27264 (2026).
- [55] A. Laneve, G. Ronco, M. Beccaceci, P. Barigelli, F. Salusti, N. Claro-Rodriguez, G. De Pascalis, A. Suprano, L. Chiaudano, E. Schöll, *et al.*, Quantum teleportation with dissimilar quantum dots over a hybrid quantum network, *Nat. Commun.* **16**, 10028 (2025).
- [56] J. B. Altepeter, E. R. Jeffrey, and P. G. Kwiat, Photonic state tomography, *Adv. At. Mol. Opt. Phys.* **52**, 105 (2005).
- [57] C. Simon and J.-P. Poizat, Creating single time-bin-entangled photon pairs, *Phys. Rev. Lett.* **94**, 030502 (2005).
- [58] E. Schöll, L. Schweickert, L. Hanschke, K. D. Zeuner, F. Sbrenny, T. Lettner, R. Trivedi, M. Reindl, S. F. Covre da Silva, R. Trotta, *et al.*, Crux of using the cascaded emission of a three-level quantum ladder system to generate indistinguishable photons, *Phys. Rev. Lett.* **125**, 233605 (2020).
- [59] T. Legero, T. Wilk, M. Hennrich, G. Rempe, and A. Kuhn, Quantum beat of two single photons, *Phys. Rev. Lett.* **93**, 070503 (2004).
- [60] R. B. Patel, A. J. Bennett, K. Cooper, P. Atkinson, C. A. Nicoll, D. A. Ritchie, and A. J. Shields, Postselective two-photon interference from a continuous nonclassical stream of photons emitted by a quantum dot, *Phys. Rev. Lett.* **100**, 207405 (2008).
- [61] R. B. Patel, A. J. Bennett, I. Farrer, C. A. Nicoll, D. A. Ritchie, and A. J. Shields, Two-photon interference of the emission from electrically tunable remote quantum dots, *Nat. Photon.* **4**, 632 (2010).
- [62] J. Huwer, R. M. Stevenson, J. Skiba-Szymanska, M. B. Ward, A. J. Shields, M. Felle, I. Farrer, D. A. Ritchie, and R. V. Pentz, Quantum-dot-based telecommunication-wavelength quantum relay, *Phys. Rev. Appl.* **8**, 024007 (2017).
- [63] M. Anderson, T. Müller, J. Huwer, J. Skiba-Szymanska, A. Krysa, R. Stevenson, J. Heffernan, D. Ritchie, and A. Shields, Quantum teleportation using highly coherent emission from telecom C-band quantum dots, *npj Quantum Inf.* **6**, 14 (2020).
- [64] M. Anderson, T. Müller, J. Skiba-Szymanska, A. B. Krysa, J. Huwer, R. M. Stevenson, J. Heffernan, D. A. Ritchie, and A. J. Shields, Gigahertz-clocked teleportation of time-bin qubits with a quantum dot in the telecommunication C band, *Phys. Rev. Appl.* **13**, 054052 (2020).
- [65] 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-wavelength quantum teleportation using frequency-converted photons from remote quantum dots, *Nat. Commun.* **16**, 10027 (2025).
- [66] M. Beccaceci, G. Ronco, F. Cienzo, P. Bassetti, A. Laneve, F. Basso Basset, T. M. Krieger, Q. Buchinger, F. Salusti, B. Souza, S. Kuhn, T. Huber-Loyola, A. Rastelli, M. B. Rota, and R. Trotta, All-photonic entanglement swapping with remote quantum dots, [arXiv:2512.10651](https://arxiv.org/abs/2512.10651).
- [67] M. B. Rota, F. Basso Basset, D. Tedeschi, and R. Trotta, Entanglement teleportation with photons from quantum dots: Toward a solid-state based quantum network, *IEEE J. Sel. Top. Quantum Electron.* **26**, 1 (2020).
- [68] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, Bell measurements for teleportation, *Phys. Rev. A* **59**, 3295 (1999).
- [69] X. Ma, C.-H. F. Fung, and H.-K. Lo, Quantum key distribution with entangled photon sources, *Phys. Rev. A* **76**, 012307 (2007).
- [70] S. I. Davis, R. Valivarthi, A. Cameron, C. Pena, S. Xie, L. Narvaez, N. Lauk, C. Li, K. Taylor, R. Youssef, *et al.*, Entanglement swapping systems toward a quantum internet, [arXiv:2503.18906](https://arxiv.org/abs/2503.18906).
- [71] J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, Demystifying the information reconciliation protocol cascade, *Quantum Inf. Comput.* **15**, 453 (2015).
- [72] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Quantum privacy amplification and the security of quantum cryptography over noisy channels, *Phys. Rev. Lett.* **77**, 2818 (1996).
- [73] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Quantum repeaters based on entanglement purification, *Phys. Rev. A* **59**, 169 (1999).
- [74] S. Bratzik, S. Abruzzo, H. Kampermann, and D. Bruß, Quantum repeaters and quantum key distribution: The impact of entanglement distillation on the secret key rate, *Phys. Rev. A* **87**, 062335 (2013).
- [75] K. Goodenough, D. Elkouss, and S. Wehner, Optimizing repeater schemes for the quantum internet, *Phys. Rev. A* **103**, 032610 (2021).
- [76] P. Mantri, K. Goodenough, and D. Towsley, Comparing one- and two-way quantum repeater architectures, *Commun. Phys.* **8**, 300 (2025).
- [77] C. Schimpf, S. Manna, S. F. Covre da Silva, M. Aigner, and A. Rastelli, Entanglement-based quantum key distribution with a blinking-free quantum dot operated at a temperature up to 20 K, *Adv. Photonics* **3**, 065001 (2021).
- [78] T. Huber, A. Predojević, H. Zoubi, H. Jayakumar, G. S. Solomon, and G. Weihs, Measurement and modification of biexciton-exciton time correlations, *Opt. Express* **21**, 9890 (2013).
- [79] G. Undeutsch, M. Aigner, A. J. Garcia Jr, J. Reindl, M. Peter, S. Mader, C. Weidinger, S. F. Covre da Silva, S. Manna, E. Schöll, *et al.*, Electric-field control of photon indistinguishability in cascaded decays in quantum dots, *Nano Lett.* **25**, 7121 (2025).
- [80] L. Zhai, G. N. Nguyen, C. Spinnler, J. Ritzmann, M. C. Löbl, A. D. Wieck, A. Ludwig, A. Javadi, and R. J. Warburton, Quantum interference of identical photons from remote GaAs quantum dots, *Nat. Nanotechnol.* **17**, 829 (2022).
- [81] R. Ikuta, T. Kobayashi, T. Kawakami, S. Miki, M. Yabuno, T. Yamashita, H. Terai, M. Koashi, T. Mukai, T. Yamamoto, *et al.*, Polarization insensitive frequency conversion for an atom-photon entanglement distribution via a telecom network, *Nat. Commun.* **9**, 1997 (2018).
- [82] J. H. Weber, B. Kambs, J. Kettler, S. Kern, J. Maisch, H. Vural, M. Jetter, S. L. Portalupi, C. Becher, and P. Michler, Two-photon interference in the telecom C-band after frequency conversion of photons from remote quantum emitters, *Nat. Nanotechnol.* **14**, 23 (2019).

- [83] M. Tomamichel and A. Leverrier, A largely self-contained and complete security proof for quantum key distribution, [Quantum](#) **1**, 14 (2017).
- [84] C. C.-W. Lim, F. Xu, J.-W. Pan, and A. Ekert, Security analysis of quantum key distribution with small block length and its application to quantum space communications, [Phys. Rev. Lett.](#) **126**, 100501 (2021).
- [85] B. T. Kirby, S. Santra, V. S. Malinovsky, and M. Brodsky, Entanglement swapping of two arbitrarily degraded entangled states, [Phys. Rev. A](#) **94**, 012336 (2016).
- [86] A. J. Hudson, R. M. Stevenson, A. J. Bennett, R. J. Young, C. A. Nicoll, P. Atkinson, K. Cooper, D. A. Ritchie, and A. J. Shields, Coherence of an entangled exciton-photon state, [Phys. Rev. Lett.](#) **99**, 266802 (2007).
- [87] T. M. Cover, *Elements of Information Theory* (John Wiley & Sons, New York, 1999).
- [88] J. Lin, Divergence measures based on the Shannon entropy, [IEEE Trans. Inf. Theory](#) **37**, 145 (1991).
- [89] I. Grosse, P. Bernaola-Galván, P. Carpena, R. Román-Roldán, J. Oliver, and H. E. Stanley, Analysis of symbolic sequences using the Jensen-Shannon divergence, [Phys. Rev. E](#) **65**, 041905 (2002).
- [90] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Purification of noisy entanglement and faithful teleportation via noisy channels, [Phys. Rev. Lett.](#) **76**, 722 (1996).
- [91] F. Rozpędek, T. Schiet, L. P. Thinh, D. Elkouss, A. C. Doherty, and S. Wehner, Optimizing practical entanglement distillation, [Phys. Rev. A](#) **97**, 062333 (2018).