PHYSICS

Quantum key distribution with entangled photons generated on demand by a quantum dot

Francesco Basso Basset*, Mauro Valeri*, Emanuele Roccia, Valerio Muredda, Davide Poderini, Julia Neuwirth, Nicolò Spagnolo, Michele B. Rota, Gonzalo Carvacho, Fabio Sciarrino†, Rinaldo Trotta†

Quantum key distribution—exchanging a random secret key relying on a quantum mechanical resource—is the core feature of secure quantum networks. Entanglement-based protocols offer additional layers of security and scale favorably with quantum repeaters, but the stringent requirements set on the photon source have made their use situational so far. Semiconductor-based quantum emitters are a promising solution in this scenario, ensuring on-demand generation of near-unity-fidelity entangled photons with record-low multiphoton emission, the latter feature countering some of the best eavesdropping attacks. Here, we use a coherently driven quantum dot to experimentally demonstrate a modified Ekert quantum key distribution protocol with two quantum channel approaches: both a 250-m-long single-mode fiber and in free space, connecting two buildings within the campus of Sapienza University in Rome. Our field study highlights that quantum-dot entangled photon sources are ready to go beyond laboratory experiments, thus opening the way to real-life quantum communication.

INTRODUCTION

The quantum mechanical properties of single photons have proven to be fundamental for the implementation of intrinsically secure cryptographic distribution systems and are the stepping stone for the development of quantum networks (*1*, *2*). One of the technologically ambitious tasks sought after within such approach is to consistently reduce the multiphoton emission using single-photon emitters without suffering from a trade-off in the photon generation rate (*3*). The reason is mainly attributed to different attack strategies, such as number splitting (*4*) or beam splitting attacks (*5*), taking advantage on the nonperfect single-photon distribution of the emitter and hacking the security of the protocol. Sub-Poisson light with low $g^{(2)}(0)$ can improve communication security in the presence of channel losses (*6*, *7*). On-demand photon emitters offer a good solution to these issues at the hardware level (*8*) to make the photon distribution nearly unassailable. Furthermore, the exploitation of Einstein–Podolsky–Rosen (EPR) nonlocality (*9*, *10*) establishes another crucial tool for the prevention of key errors, and a subsequent improvement on security of the communication procedure against individual attacks (*11*). Under certain experimental requirements, it could also provide device-independent operation (*12*, *13*). Last, entangled photon sources with a limited trade-off between brightness and multiphoton generation are needed to improve the scaling or reduce the hardware complexity of quantum repeaters (*14*). Semiconductor quantum dots (QDs) are a promising platform for the accomplishment of all these tasks, due to their low multiphoton emission rate (*15*), increasing brightness (*16*, *17*), and on-demand production of high-purity entangled states (*18*). So far, the application of QD-based light sources has focused on single-photon prepare-and-measure protocols, exploring polarization (*7*, *19*) and time-bin encoding (*20*), electrical (*21*) and optical pumping, and laboratory tests and field demonstrations (*22*), possibly even with spectral multiplexing (*23*). Most recent works foresee even the possibility to outperform state-of-the-art solutions based on the decoy-state protocol and weak coherent pulse sources (*24*). One pioneering demonstration of the entanglement-based BBM92 protocol has been realized using an entangled light-emitting diode (*25*). However, this seminal proof of concept left several opportunities for improvement: The reported quantum bit error rate (QBER) of 9.8%, close to the 11% threshold of the most common error correction algorithms, and the sifted bit rate of 0.17 bit/s would arguably preclude out-of-the-laboratory implementation. Moreover, entangled photons were not generated on demand, one of the key features distinguishing QDs from standard sources on the basis of spontaneous parametric down-conversion (SPDC).

In this letter, we tackle these challenges and present the experimental implementation of an entanglement-based quantum key distribution (QKD) protocol, specifically the asymmetrical Ekert proposal (*10*, *26*), with the use of entangled photons generated by a nearly deterministic QD-based source. In particular, we demonstrate the viability of our QKD system under different choices of quantum channel.

RESULTS

A first overview of our study is given in Fig. 1, which recreates two urban communication scenarios within the campus of Sapienza University of Rome, namely, via a single-mode fiber (SMF) and through free space covering a distance of approximately 270 m. This double approach is motivated by the fact that, on the one hand, networks based on fiber communication are the common solution within urban environments, because of their scalability with moderate losses for short distances. On the other hand, over long distances, free-space links still represent the best choice to connect users because of its low-signal attenuation (*27*, *28*) and the possibility of sending complex states such as those exploiting the orbital angular momentum (OAM) of light—something still under development with optical fibers—despite the need for more complex sender and receiver systems.

Figure 1 illustrates the principle of operation of the QKD protocol. The two parties randomly select a measurement to perform on their subsystem of an entangled state from a set of linear polarization

Department of Physics, Sapienza University of Rome, 00185 Rome, Italy.
*These authors contributed equally to this work.
†Corresponding author. Email: fabio.sciarrino@uniroma1.it (F.S.); rinaldo.trotta@uniroma1.it (R.T.)

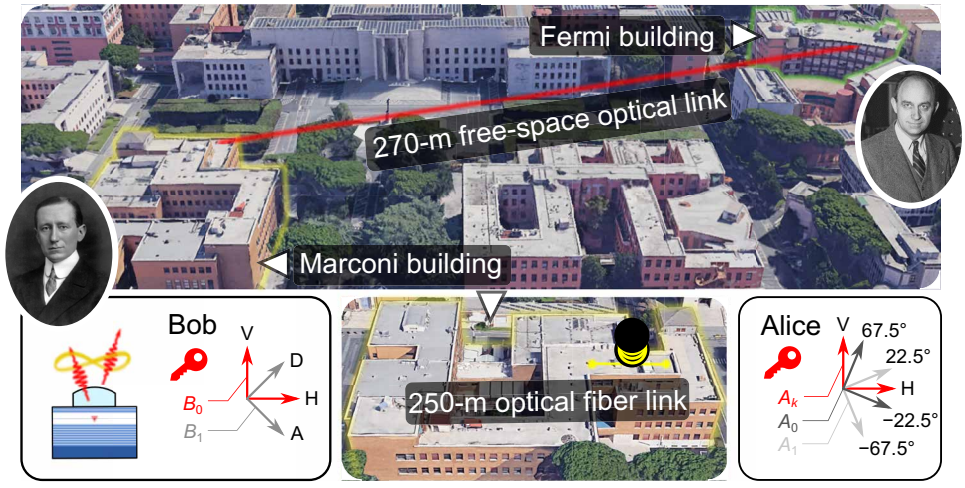

Fig. 1. Entanglement-based QKD and optical link overview. Entangled photon pairs generated by a single QD are shared across the Sapienza University campus in Rome over a 270-m free-space distance and, in addition, between two laboratories in the same building via a 250-m SMF. Map data: Google Earth. We illustrate the main concepts of the asymmetrical Ekert approach: After traveling through the optical link connecting the users, the photons are measured by Alice and Bob on the measurement bases $\{A_k, A_0, A_1\}$ and $\{B_0, B_1\}$ in the Fermi and Marconi buildings, respectively. In this case, the combination of the horizontal and vertical polarization states $\{A_k, B_0\}$ constitutes the basis to share the secure key. In parallel, the other pairs ensure verification of the entanglement quality, by measuring the Bell parameter of the two-photon state. Photo credit: Google Earth.

bases. In a quarter of the cases, Alice and Bob pick a combination of the $\{A_k, B_0\}$ bases, and their local reference frames are aligned in such a way that they will get the same result out of the measurement. When Alice and Bob share among themselves the information that they performed the same measurement, its random outcome is a bit added to the shared secret key. In the presence of noise or imperfect entangled states, the keys may differ by an amount quantified by the QBER

$$\mathrm{QBER} = (1 - E(A_k, B_0))/2 \quad (1)$$

where E is the correlation coefficient, i.e., the expectation value on the $\{A_k, B_0\}$ pair of measurements.

When the two parties select a different combination of polarization bases, they use the results of the measurement to estimate entanglement and monitor the security of the QKD. The measurement bases on Alice ($\{A_0, A_1\}$) and Bob ($\{B_0, B_1\}$) sides are chosen to obtain the maximum value of the Bell parameter S, checking the violation of Bell inequality $|S| \leq 2$, accordingly to the Clauser–Horne–Shimony–Holt (CHSH) figure of merit (*29*)

$$S = E(A_0, B_0) + E(A_0, B_1) + E(A_1, B_0) - E(A_1, B_1) \quad (2)$$

Such procedure is a convenient variation of the well-known Ekert proposal. The asymmetrical scheme reduces the number of required detectors with respect to the original Ekert91 protocol, as reported in the practical implementation illustrated in Fig. 2A. At the same time, the fraction of photons dedicated to the key exchange is increased, while the security check is still performed by monitoring the Bell inequalities (*26*). In addition, the scheme has been demonstrated viable for device-independent operation (*13*).

In our experiment, Bob is placed near the entangled photon source, while Alice is on the other side of the used quantum channel. The mentioned measurements on Alice ($\{A_k, A_0, A_1\}$) and Bob ($\{B_0, B_1\}$) sides are associated to detection events on different avalanche photodiodes. The coincidences between Alice and Bob are obtained by exploiting two GPS-disciplined oscillators (*22*), which allow synchronization with an accuracy of approximately 10 ns.

The photon pairs shared among the two parties are deterministically emitted in the maximally entangled state $|\phi^+\rangle = 1/\sqrt{2}(|\mathrm{HH}\rangle + |\mathrm{VV}\rangle)$ from a single GaAs QD, pumped with a 320-MHz repetition rate laser. The key transmission along the two different quantum channels was performed using two QDs with very similar features (see full comparison in Materials and Methods). The entanglement fidelity reaches up to between 0.941 and 0.958 (see fig. S1 in section S1 for the complete quantum state tomography) because of the choice of QDs with sub-μeV fine structure splitting. This ensures a high polarization indistinguishability between the two photons generated by the radiative biexciton-exciton (XX-X) cascade. The low multiphoton emission efficiency is checked by measuring the autocorrelation function $g^{(2)}(|\tau| < 0.8\ \mathrm{ns})$, normalized by the side peaks from consecutive laser pulses. Figure 2B reports an autocorrelation measurement run on the exciton emission line with a dedicated Hanbury-Brown and Twiss setup in laboratory conditions, corresponding to $g_X^{(2)}(|\tau| < 0.8\ \mathrm{ns}) = 0.0034(2)$, a value mainly limited by the detector time resolution. Even if this figure were to be entirely attributed to multiphoton emission, it would still be a minor cause of below-unity entanglement fidelity, with an expected contribution of 0.3% in a simple model of the density matrix (*30*). With a similar experimental procedure, we measure the cross-correlation function between the two photons of the entangled pair to determine the fidelity of preparation, defined as the probability of a laser pulse to promote the QD from the optically active ground state to the biexciton state, followed by the two-photon emission. We obtain a fidelity of preparation up to 0.943(3), due to the deterministic resonant two-photon excitation of the QD (*31*). This showcases the near on-demand character of the generation of entangled photons. The probability of creating an entangled photon pair at any time is lower because of blinking dynamics that can cause the QD to stay optically inactive on the microsecond time scale. In our work, we have observed

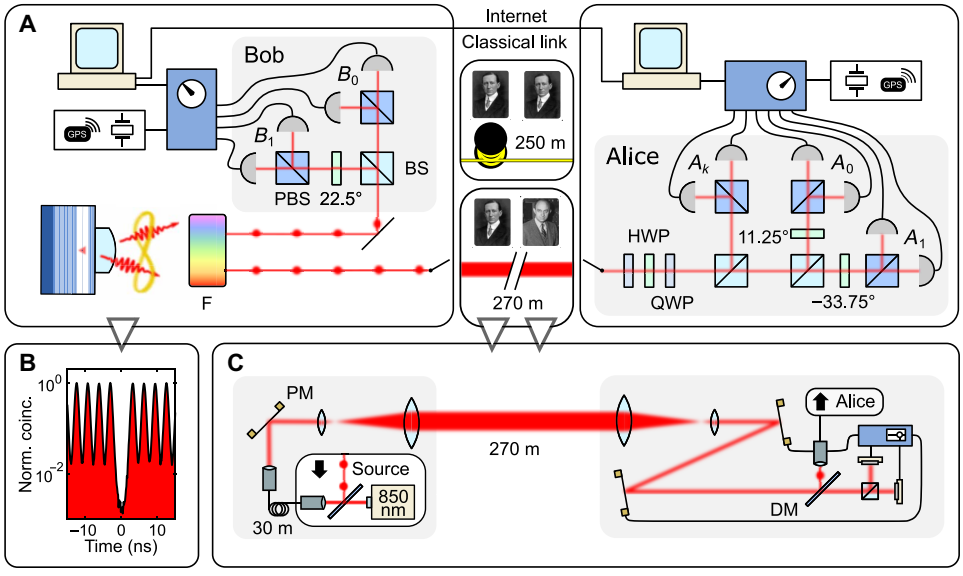

Fig. 2. Experimental realization of the QKD protocol. (**A**) Illustration of the setup used for the entanglement-based QKD protocol. On Bob side, the single GaAs QD generates two entangled photons that are separated by spectral filtering (F). One photon goes directly to the Bob measurement apparatus, while the other travels through one of the quantum channels depicted in Fig. 1. The photons arriving to Alice's station are compensated in polarization with a set of two quarter-wave plates (QWPs) and a half-wave plate (HWP). After a random splitting with 50:50 beam splitters (BS), which also mirror the polarization of the reflected beam, the polarization states are measured in the bases $\{B_0, B_1\}$ on Bob and $\{A_k, A_0, A_1\}$ on Alice using HWPs and polarizing BS (PBS). The photons are lastly collected and detected by avalanche photodiodes connected to two independent time taggers. These are synchronized with the help of GPS-disciplined oscillators. (**B**) Autocorrelation histogram of the X emission line, showing the low multiphoton component of the source. (**C**) Sender and receiver in free-space communication. A diode laser beam at 850 nm is sent together with the single-photon signal and feeds a closed-loop stabilization system, which controls the piezoelectric mirror mounts (PM). The QD signal is selected by a dichroic mirror (DM) and then coupled into a SMF directed to Alice's measurement apparatus.

(*32*) characteristic on-time fractions of 0.22 to 0.26, which, however, do not imply any fundamental limitation, as complete blinking suppression has been experimentally demonstrated (*33*).

The main difference between the two protocol realizations resides in the additional setup required for the signal transmission over free space, which is shown in Fig. 2C. As in this work, we explore both fiber-based and free-space QKD. We emphasize that the latter has proven noticeably more challenging, as it requires a different level of complexity from the technical standpoint, especially for the measures needed to counteract atmospheric turbulence. The system that we set up is composed of two matching telescopes and an active-stabilization system, which is guided by tracking a reference 850-nm laser on two position-sensitive detectors. The system is designed to counteract the effect of beam wander created during the propagation, hence allowing a single-mode coupling of the photon signal (at 785 nm) with approximately 40% efficiency.

The comparison of the experimental results between the fiber and free-space approaches is illustrated in Fig. 3. The data are synchronously collected on the two sides in packets of 1.2-s acquisition time and shared over the university network, for a total time of 224 min. For both optical links, we measure the QBER, the Bell parameter S, and the amount of key shared among the two parties. Using the fiber communication approach, in Fig. 3A, a total 217.76-kB key is shared, with a mean raw key rate of 486 bit s^{-1}. Rates as high as 785 bit s^{-1} were obtained in preliminary tests using a common time-to-digital converter for the two parties and a different QD from the same sample (see section S2). The mean QBER of the key is $Q_{SMF} = 3.37(2)\%$, while the mean Bell parameter is $S_{SMF} = 2.647(2)$.

In free-space communication (see Fig. 3B), we manage to share a 34.589-kB-long key string, relying on 60 bit s^{-1} of mean raw key rate. In this case, the average values of QBER and Bell parameter are $Q_{FS} = 4.0(2)\%$ and $S_{FS} = 2.37(10)$, respectively.

These results constitute a successful field demonstration of QKD using a QD-based deterministic source of entangled photons. Both optical link choices showed a substantial violation of Bell inequality, demonstrating the two-photon entanglement preservation over the quantum communication channel. The reliability of the key quality shared during the communication is verified in both cases by monitoring the QBER, which remains consistently well below the critical insecure value of 11%. The nonzero QBER is attributed to the below-unity entanglement fidelity and to noise, whereas the multiphoton emission is estimated to account for less than 0.2%. The noise is due to dark counts (on average 250 cps), afterpulsing of the detectors, and, after the free-space optical link, undesired photons from the reference laser used for beam stabilization. The latter effects lead to an increase in the value of $g_X^{(2)}(|\tau| < 0.8$ ns), as estimated during the QKD by analyzing the coincidences among the detectors operated by one communicating party (*24*), to 0.02 for the SMF link and 0.038 for the free-space channel.

Part of the distributed key was used to encrypt and decrypt the Sapienza logo as depicted in Fig. 3C. After the binary error correction process (*34*), we apply a Trevisan extractor to restore uniform randomness (*35*) and compensate for setup-induced polarization changes. The complete procedure followed for the key extraction is presented in section S5.

DISCUSSION

The comparison of the measurements highlights some interesting considerations on the quantum channel choice performing an EPR-based

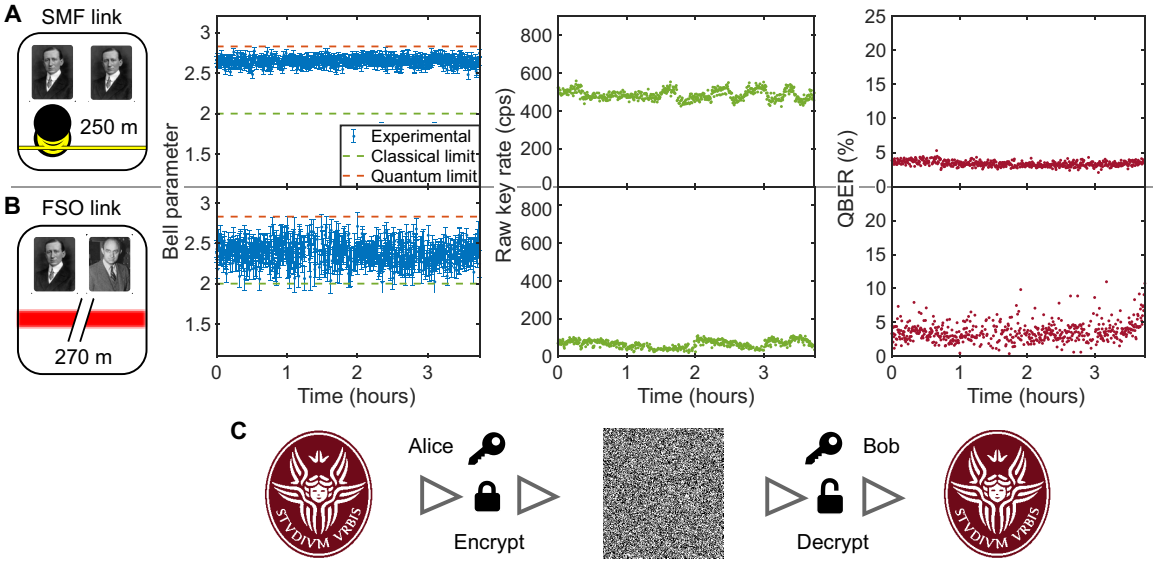

Fig. 3. Experimental key sharing via the modified Ekert protocol. (**A** and **B**) The Bell parameter, raw key rate, and QBER measured with both the SMF optical link (A) and the free-space optical (FSO) link (B). In the latter case, the data transmission was conducted overnight and interrupted at dawn. Each data point corresponds to five acquisitions of 1.2 s. The error bars in the Bell parameter are calculated by Gaussian propagation assuming a Poissonian distribution for the coincidence counts. (**C**) The encryption and decryption of Sapienza logo using the one-time pad technique with the shared free-space key, after the error correction and randomness enhancement steps.

QKD approach using QDs. Atmospheric turbulence and the complex stability requirements of optical apparatuses for free-space communication lead to signal loss and performance degradation when compared with the in-fiber solution for short distances. This is unavoidable to a certain degree, even if we can identify excessive losses and room for optimization in our current implementation. The complete characterization of the quantum channel is important for controlling hacking strategies such as side-channel attacks. In this regard, a potentially useful feature in our free-space implementation is the modular approach of the receiver apparatus, dividing the collection table from the table dedicated to the measurements (see section S3). In particular, the former is used for the correct stabilization of the signal, but in general, it could be used for adding particular scheme-dependent defense elements, such as an optical isolator (*36*) or a spatial filter (*37*), to avoid possible attacks based on hardware limitations. While we do not consider an a priori defense against possible side-channel attacks, our setup is robust, for instance, to spatial-mode side-channel attacks, because we do not allow multiple spatial modes at the detectors by filtering the signal through a SMF. In a more general context of application, by increasing the distance between the QKD users, the free-space communication is expected to deteriorate less markedly, becoming a more advisable solution. Moreover, it allows to use the OAM degree of freedom, which can be used in QKD schemes, e.g., for independence from local reference frames (*38*). Up to date, the generation of OAM states using QD-based light sources is mostly unexplored, but there is a developing effort to make use of semiconductor microcavities designed to control the chirality of emitted light (*39*, *40*) and embed QDs in them for the generation of single photons carrying OAM (*41*, *42*).

In conclusion, we have experimentally performed an entanglement-based QKD protocol with the use of a QD photon-pair source, demonstrated to be viable both with in-fiber and free-space quantum communication channels. Exactly 20 years after the first theoretical proposal on the possibility of using QDs to generate regulated and entangled photons (*43*), our study demonstrates that this semiconductor-based quantum technology is mature to go out of the laboratory, and further improvements have the potential to make it the best performing solution for some quantum communication applications in the near future. Even if our experimental results present several improvements over the first in-laboratory QKD demonstration with an entangled light-emitting diode (*25*)—related to the near-deterministic excitation scheme, the more realistic test bed and the overall performance—the secure key throughput is still below what can be achieved with a SPDC source (see section S6 for a quantitative comparison between different QD emitters and a realistic high-efficiency SPDC source). This is due to our improvable current value of collection photon-pair collection rate at the first lens. Existing QD-based light sources relying on optical microcavities with near-Gaussian far-field emission (*16*) could already perform better than a realistic pulsed SPDC source (*44*), even taking into account the penalty due to the current lack of optimization in terms of degree of entanglement. The threshold for outperforming the theoretically maximum secure key rate achievable by SPDC is more demanding, especially in the least favorable case for comparison, that is a lossless transmission channel. Even this higher standard is within reach of foreseeable technical advances. The QBER, and, consequently, the protocol throughput, can be further improved using strategies to completely remove the fine structure splitting, among which the most promising is the state-of-the-art solution based on strain control via micromachined piezoelectric actuators (*45*, *46*). Not only this approach can be combined with photonic structures, but also it has already been predicted that even a moderate Purcell factor of 3 would allow the existing GaAs-QDs technology to reach entanglement fidelity above 0.99 (*18*). While the light-emitting device operates at cryogenic temperature, strategies are being devised in the literature to reduce its global footprint (*47*) and possibly to integrate it with high-efficiency superconducting nanowire

single-photon detectors (*48*–*50*), which have the same requirement. Last, we envisage that the possibility of interfacing entangled photons from QDs with the same or other quantum systems (*46*, *51*), together with the prospect of enhancing photon extraction (*16*, *17*), will be the key to boost secure quantum cryptography over large distances.

MATERIALS AND METHODS

Entangled photon source

Polarization-entangled photons are generated by a single GaAs QD embedded in a crystalline matrix of $Al_{0.4}Ga_{0.6}As$. The QDs are fabricated using the Al droplet etching technique, as described in (*52*). Because of the presence of distributed Bragg reflectors in the sample structure and the use of a hemispherical solid immersion lens, an extraction efficiency of approximately 8% is usually achieved in the investigated sample. This value allows to use the source in realistic quantum communication schemes, but further improvements are required to overcome state-of-the-art SPDC. Two different QDs from the same sample and with similar characteristics were used in the two parts of the experiment. The multiphoton emission is very similar, $g_X^{(2)}(|\tau| < 0.8\ \text{ns}) = 0.0034(2)$ and $g_{XX}^{(2)}(|\tau| < 0.8\ \text{ns}) = 0.0041(3)$ for the QD used in the fiber experiment, $g_X^{(2)}(|\tau| < 0.8\ \text{ns}) = 0.0040(4)$ and $g_{XX}^{(2)}(|\tau| < 0.8\ \text{ns}) = 0.0045(4)$ for the QD used in the free-space experiment. Achieving these values does not require polarization suppression for the cancelation of background radiation from the laser. The entanglement fidelity is only slightly different, 0.958(12) in the free-space case and 0.941(10) in the in-fiber case, because of the different fine structure splitting, 0.35 and 0.85 μeV, respectively. The single-photon count at the output of the first SMF, disregarding losses in the quantum channels and in the Alice and Bob apparatuses (which are discussed in the following section), is 700 and 620 kcps for the QD in the free-space and in-fiber case, respectively. The reduction with respect to the rate of pump pulses can be related to photon generation probability, transmission and detection in the setup, and extraction efficiency. The preparation fidelity and the blinking on-time fraction are 0.943(3) and 0.22, respectively, for the free-space implementation and 0.90(1) and 0.26 for the SMF demonstration. The total transmission of the setup up to the first SMF is approximately 33%, the SMF coupling efficiency 65%, and the detector efficiency 60%. Last, we can estimate extraction efficiencies, defined as the fraction of emitted photons collected at the first lens, of 8.2 and 6.3% for the QD in the free-space and in-fiber case, respectively.

Setup description

The entangled photon source is kept at 5 K in a low-vibration closed-cycle He cryostat. The optical excitation is performed with a Ti:Sapphire laser together with a 4f pulse shaper, to reduce its bandwidth to 0.1 nm, and two Mach-Zehnder interferometers, to increase its repetition rate fourfold. The signal is collected from the QD using a 0.81–numerical aperture objective, and the backscattered laser light is filtered out with notch filters. The two photons from a single XX-X cascade are then separated by two volume Bragg gratings, collected by two SMFs, and distributed to the measurement setups of the two QKD users, Alice and Bob. The SMF quantum channel consists of a 780-HP fiber with 80% transmission after its 250 m of length at the wavelength of operation (785 nm). In the free-space experiment, an 850-nm diode laser is collected through a 30-m SMF together with the photon associated to the exciton line and brought to the transmission platform. Here, the beam is magnified by a factor of 6, to obtain a diameter ($1/e^2$ level) of 22 mm, by exploiting a telescope, with the aim of keeping collimation and reducing the effect of beam wandering during the 270-m travel in air, where the atmospheric attenuation losses amount at 10%. A mirror with piezoelectric adjusters is used to compensate for slow drifts in the pointing direction. On the receiver side, the beam diameter is reduced with a telescope similar to the one used by the sender. This permits to couple the signal in a SMF connected to Alice's apparatus. The 850-nm laser is separated from the QD signal using a dichroic mirror and sent to two position-sensitive detectors that provide feedback for an active beam stabilization system implemented with two mirrors with piezoelectric adjusters. The single-photon signal is lastly collected in the SMF with an average coupling efficiency of 40% and sent to Alice's measurement apparatus. The overall transmission efficiency of the free-space optical channel, from the fiber output on the sender platform to the fiber output in Alice's setup, is 10%. A more detailed account of the stabilization strategy and the channel losses is presented in section S3. After going through the polarization optics shown in Fig. 2A and coupled again into SMFs (75% coupling efficiency), the QD signal is lastly collected by single-photon silicon avalanche diodes. The detection events are recorded on each side by a time-to-digital converter that is also connected to a GPS-disciplined double-oven oscillator, acting as a reference clock. The coincidences are collected within an acceptance time window of ±0.8 ns, which prevents accidental counts due to the limitations in the time accuracy of the synchronization and to noise, while being large enough to not discard photons emitted by the QD based on their time of emission. A more in-depth description of the synchronization procedure is found in section S4.

SUPPLEMENTARY MATERIALS

Supplementary material for this article is available at http://advances.sciencemag.org/cgi/content/full/7/12/eabe6379/DC1

REFERENCES AND NOTES

1. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
2. F. Flamini, N. Spagnolo, F. Sciarrino, Photonic quantum information processing: A review. *Rep. Prog. Phys.* **82**, 016001 (2018).
3. M. Takeoka, R.-B. Jin, M. Sasaki, Full analysis of multi-photon pair effects in spontaneous parametric down conversion based photonic quantum information processing. *New J. Phys.* **17**, 043030 (2015).
4. N. Lütkenhaus, M. Jahma, Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack. *New J. Phys.* **4**, 44 (2002).
5. M. Dušek, O. Haderka, M. Hendrych, Generalized beam-splitting attack in quantum cryptography with dim coherent states. *Optics Commun.* **169**, 103–108 (1999).
6. E. Waks, C. Santori, Y. Yamamoto, Security aspects of quantum key distribution with sub-Poisson light. *Phys. Rev. A* **66**, 042315 (2002).
7. E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, Y. Yamamoto, Quantum cryptography with a photon turnstile. *Nature* **420**, 762 (2002).
8. R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle, J.-P. Poizat, P. Grangier, Experimental open-air quantum key distribution with a single-photon source. *New J. Phys.* **6**, 92 (2004).
9. C. H. Bennett, Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121–3124 (1992).
10. A. K. Ekert, Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
11. E. Waks, A. Zeevi, Y. Yamamoto, Security of quantum key distribution with entangled photons against individual attacks. *Phys. Rev. A* **65**, 052310 (2002).
12. X. Ma, C.-H. F. Fung, H.-K. Lo, Quantum key distribution with entangled photon sources. *Phys. Rev. A* **76**, 012307 (2007).

13. A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
14. H. Krovi, S. Guha, Z. Dutton, J. A. Slater, C. Simon, W. Tittel, Practical quantum repeaters with parametric down-conversion sources. *Appl. Phys. B* **122**, 52 (2016).
15. L. Schweickert, K. D. Jöns, K. D. Zeuner, S. F. C. da Silva, H. Huang, T. Lettner, M. Reindl, J. Zichi, R. Trotta, A. Rastelli, V. Zwiller, On-demand generation of background-free single photons from a solid-state source. *Appl. Phys. Lett.* **112**, 093106 (2018).
16. J. Liu, R. Su, Y. Wei, B. Yao, S. F. C. da Silva, Y. Yu, J. Iles-Smith, K. Srinivasan, A. Rastelli, J. Li, X. Wang, A solid-state source of strongly entangled photon pairs with high brightness and indistinguishability. *Nat. Nanotechnol.* **14**, 586–593 (2019).
17. H. Wang, H. Hu, T.-H. Chung, J. Qin, X. Yang, J.-P. Li, R.-Z. Liu, H.-S. Zhong, Y.-M. He, X. Ding, Y.-H. Deng, Q. Dai, Y.-H. Huo, S. Höfling, C.-Y. Lu, J.-W. Pan, On-demand semiconductor source of entangled photons which simultaneously has high fidelity, efficiency, and indistinguishability. *Phys. Rev. Lett.* **122**, 113602 (2019).
18. D. Huber, M. Reindl, S. F. C. da Silva, C. Schimpf, J. Martín-Sánchez, H. Huang, G. Piredda, J. Edlinger, A. Rastelli, R. Trotta, Strain-tunable GaAs quantum dot: A nearly dephasing-free source of entangled photon pairs on demand. *Phys. Rev. Lett.* **121**, 033902 (2018).
19. R. J. Collins, P. J. Clarke, V. Fernández, K. J. Gordon, M. N. Makhonin, J. A. Timpson, A. Tahraoui, M. Hopkinson, A. M. Fox, M. S. Skolnick, G. S. Buller, Quantum key distribution system in standard telecommunications fiber using a short wavelength single photon source. *J. Appl. Phys.* **107**, 073102 (2010).
20. K. Takemoto, Y. Nambu, T. Miyazawa, Y. Sakuma, T. Yamamoto, S. Yorozu, Y. Arakawa, Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors. *Sci. Rep.* **5**, 14383 (2015).
21. T. Heindel, C. A. Kessler, M. Rau, C. Schneider, M. Fürst, F. Hargart, W.-M. Schulz, M. Eichfelder, R. Roßbach, S. Nauerth, M. Lermer, H. Weier, M. Jetter, M. Kamp, S. Reitzenstein, S. Höfling, P. Michler, H. Weinfurter, A. Forchel, Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range. *New J. Phys.* **14**, 083001 (2012).
22. M. Rau, T. Heindel, S. Unsleber, T. Braun, J. Fischer, S. Frick, S. Nauerth, C. Schneider, G. Vest, S. Reitzenstein, M. Kamp, A. Forchel, S. Höfling, H. Weinfurter, Free space quantum key distribution over 500 meters using electrically driven quantum dot single-photon sources—A proof of principle experiment. *New J. Phys.* **16**, 043003 (2014).
23. T. Aichele, G. Reinaudi, O. Benson, Separating cascaded photons from a single quantum dot: Demonstration of multiplexed quantum cryptography. *Phys. Rev. B* **70**, 235329 (2004).
24. T. Kupko, M. von Helversen, L. Rickert, J.-H. Schulze, A. Strittmatter, M. Gschrey, S. Rodt, S. Reitzenstein, T. Heindel, Tools for the performance optimization of single-photon quantum key distribution. *npj Quantum Inf.* **6**, 29 (2020).
25. B. Dzurnak, R. M. Stevenson, J. Nilsson, J. F. Dynes, Z. L. Yuan, J. Skiba-Szymanska, I. Farrer, D. A. Ritchie, A. J. Shields, Quantum key distribution with an entangled light emitting diode. *Appl. Phys. Lett.* **107**, 261101 (2015).
26. A. Acín, S. Massar, S. Pironio, Efficient quantum key distribution secure against no-signalling eavesdroppers. *New J. Phys.* **8**, 126 (2006).
27. R. Bedington, J. M. Arrazola, A. Ling, Progress in satellite quantum key distribution. *npj Quantum Inf.* **3**, 30 (2017).
28. J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A. K. Ekert, J.-W. Pan, Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* **582**, 501–505 (2020).
29. J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880–884 (1969).
30. M. B. Rota, F. Basso Basset, D. Tedeschi, R. Trotta, Entanglement teleportation with photons from quantum dots: Towards a solid-state based quantum network. *IEEE J. Sel. Top. Quantum Electron.* **26**, 6400416 (2020).
31. H. Jayakumar, A. Predojević, T. Huber, T. Kauten, G. S. Solomon, G. Weihs, Deterministic photon pairs and coherent optical control of a single quantum dot. *Phys. Rev. Lett.* **110**, 135505 (2013).
32. J.-P. Jahn, M. Munsch, L. Béguin, A. V. Kuhlmann, M. Renggli, Y. Huo, F. Ding, R. Trotta, M. Reindl, O. G. Schmidt, A. Rastelli, P. Treutlein, R. J. Warburton, An artificial Rb atom in a semiconductor with lifetime-limited linewidth. *Phys. Rev. B* **92**, 245439 (2015).
33. L. Zhai, M. C. Löbl, G. N. Nguyen, J. Ritzmann, A. Javadi, C. Spinnler, A. D. Wieck, A. Ludwig, R. J. Warburton, Low-noise GaAs quantum dots for quantum photonics. *Nat. Commun.* **11**, 4745 (2020).
34. B. Colombier, L. Bossuet, V. Fischer, D. Hély, Key reconciliation protocols for error correction of silicon PUF responses. *IEEE Trans. Inf. Foren. Sec.* **12**, 1988–2002 (2017).
35. L. Trevisan, Extractors and pseudorandom generators. *J. ACM* **48**, 860–879 (2001).
36. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **73**, 022320 (2006).
37. S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, V. Makarov, Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. *Phys. Rev. A* **91**, 062301 (2015).
38. G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, P. Villoresi, Free-space quantum key distribution by rotation-invariant twisted photons. *Phys. Rev. Lett.* **113**, 060503 (2014).
39. H. Li, D. B. Phillips, X. Wang, Y.-L. D. Ho, L. Chen, X. Zhou, J. Zhu, S. Yu, X. Cai, Orbital angular momentum vertical-cavity surface-emitting lasers. *Optica* **2**, 547–552 (2015).
40. N. C. Zambon, P. St-Jean, M. Milićević, A. Lemaître, A. Harouri, L. Le Gratiet, O. Bleu, D. D. Solnyshkov, G. Malpuech, I. Sagnes, S. Ravets, A. Amo, J. Bloch, Optically controlling the emission chirality of microlasers. *Nat. Photonics* **13**, 283–288 (2019).
41. C. F. Fong, Y. Ota, S. Iwamoto, Y. Arakawa, Scheme for media conversion between electronic spin and photonic orbital angular momentum based on photonic nanocavity. *Opt. Express* **26**, 21219–21234 (2018).
42. Y. Bao, Q. Lin, R. Su, Z.-K. Zhou, J. Song, J. Li, X.-H. Wang, On-demand spin-state manipulation of single-photon emission from quantum dot integrated with metasurface. *Sci. Adv.* **6**, eaba8761 (2020).
43. O. Benson, C. Santori, M. Pelton, Y. Yamamoto, Regulated and entangled photons from a single quantum dot. *Phys. Rev. Lett.* **84**, 2513–2516 (2000).
44. M. Bock, A. Lenhard, C. Chunnilall, C. Becher, Highly efficient heralded single-photon source for telecom wavelengths based on a PPLN waveguide. *Opt. Express* **24**, 23992–24001 (2016).
45. R. Trotta, J. Martín-Sánchez, I. Daruka, C. Ortix, A. Rastelli, Energy-tunable sources of entangled photons: A viable concept for solid-state-based quantum relays. *Phys. Rev. Lett.* **114**, 150502 (2015).
46. R. Trotta, J. Martín-Sánchez, J. S. Wildmann, G. Piredda, M. Reindl, C. Schimpf, E. Zallo, S. Stroj, J. Edlinger, A. Rastelli, Wavelength-tunable sources of entangled photons interfaced with atomic vapours. *Nat. Commun.* **7**, 10375 (2016).
47. A. Schlehahn, S. Fischbach, R. Schmidt, A. Kaganskiy, A. Strittmatter, S. Rodt, T. Heindel, S. Reitzenstein, A stand-alone fiber-coupled single-photon source. *Sci. Rep.* **8**, 1340 (2018).
48. G. Reithmaier, S. Lichtmannecker, T. Reichert, P. Hasch, K. Müller, M. Bichler, R. Gross, J. J. Finley, On-chip time resolved detection of quantum dot emission using integrated superconducting single photon detectors. *Sci. Rep.* **3**, 1901 (2013).
49. M. Schwartz, E. Schmidt, U. Rengstl, F. Hornung, S. Hepp, S. L. Portalupi, K. Ilin, M. Jetter, M. Siegel, P. Michler, Fully on-chip single-photon Hanbury-Brown and Twiss experiment on a monolithic semiconductor–superconductor platform. *Nano Lett.* **18**, 6892–6897 (2018).
50. R. Gourgues, I. E. Zadeh, A. W. Elshaari, G. Bulgarini, J. W. N. Los, J. Zichi, D. Dalacu, P. J. Poole, S. N. Dorenbos, V. Zwiller, Controlled integration of selected detectors and emitters in photonic integrated circuits. *Opt. Express* **27**, 3710–3716 (2019).
51. S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, W. Tittel, Rate-loss analysis of an efficient quantum repeater architecture. *Phys. Rev. A* **92**, 022357 (2015).
52. F. Basso Basset, M. Rota, C. Schimpf, D. Tedeschi, K. D. Zeuner, S. F. C. da Silva, M. Reindl, V. Zwiller, K. D. Jöns, A. Rastelli, R. Trotta, Entanglement swapping with photons generated on demand by a quantum dot. *Phys. Rev. Lett.* **123**, 160501 (2019).
53. J. B. Altepeter, E. R. Jeffrey, P. G. Kwiat, S. Tanzilli, N. Gisin, A. Acín, Experimental methods for detecting entanglement. *Phys. Rev. Lett.* **95**, 033601 (2005).
54. O. Bouchet, H. Sizun, C. Boisrobert, F. de Fornel, *Free-Space Optics: Propagation and Communication* (John Wiley & Sons, 2010), vol. 91.
55. A. Carrasco-Casado, V. Fernández, N. Denisenko, Free-Space Quantum Key Distribution in *Optical Wireless Communications*, M. Uysal, C. Capsoni, Z. Ghassemlooy, A. Boucouvalas, E. Udvary, Eds. (Springer International Publishing, 2016), pp. 589–607.
56. J. Mikołajczyk, Z. Bielecki, M. Bugajski, J. Piotrowski, J. Wojtas, W. Gawron, D. Szabra, A. Prokopiuk, Analysis of free-space optics development. *Metrol. Meas. Syst.* **24**, 653–674 (2017).
57. V. I. Tatarski, *Wave Propagation in a Turbulent Medium* (Courier Dover Publications, 2016).
58. F. Koushanfar, A. Mirhoseini, A unified framework for multimodal submodular integrated circuits Trojan detection. *IEEE Trans. Inf. Foren. Sec.* **6**, 162–174 (2011).
59. M. Hayashi, T. Tsurumaru, More efficient privacy amplification with less random seeds via dual universal hash function. *IEEE Trans. Inf. Theory* **62**, 2213–2232 (2016).
60. R. Renner, Security of quantum key distribution. *Int. J. Quantum Inf.* **6**, 1–127 (2008).
61. U. Vazirani, T. Vidick, Fully device independent quantum key distribution. *Commun. ACM* **62**, 133 (2019).
62. A. De, C. Portmann, T. Vidick, R. Renner, Trevisan's extractor in the presence of quantum side information. *SIAM J. Comput.* **41**, 915–940 (2001).
63. M. Aspelmeyer, H. R. Böhm, T. Gyatso, T. Jennewein, R. Kaltenbaek, M. Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther, A. Zeilinger, Long-distance free-space distribution of quantum entanglement. *Science* **301**, 621–623 (2003).
64. D. Walls, G. J. Milburn, *Quantum Optics* (Springer Berlin Heidelberg, 2008).
65. H. Wang, Y.-M. He, T.-H. Chung, H. Hu, Y. Yu, S. Chen, X. Ding, M.-C. Chen, J. Qin, X. Yang, R.-Z. Liu, Z.-C. Duan, J.-P. Li, S. Gerhardt, K. Winkler, J. Jurkat, L.-J. Wang, N. Gregersen, Y.-H. Huo, Q. Dai, S. Yu, S. Höfling, C.-Y. Lu, J.-W. Pan, Towards optimal single-photon sources from polarized microcavities. *Nat. Photonics* **13**, 770–775 (2019).

66. S. Ates, L. Sapienza, M. Davanco, A. Badolato, K. Srinivasan, Bright single-photon emission from a quantum dot in a circular Bragg grating microcavity. *IEEE J. Sel. Top. Quant. Electron.* **18**, 1711–1721 (2012).
67. L. Rickert, T. Kupko, S. Rodt, S. Reitzenstein, T. Heindel, Optimized designs for telecom-wavelength quantum light sources based on hybrid circular Bragg gratings. *Opt. Express* **27**, 36824–36837 (2019).

Acknowledgments: We thank A. Rastelli and S. F. Covre da Silva for providing high-quality GaAs QD samples, P. Mataloni for fruitful discussions, and A. Miriametro for helpful technical assistance. **Funding:** This work was financially supported by the European Research Council (ERC) under the European Union's Horizon 2020 Research and Innovation Programme (SPQRel, grant agreement no. 679183), by the Regione Lazio program "Progetti di Gruppi di ricerca" legge Regionale n. 13/2008 (SINFONIA project, prot. n. 85-2017-15200) via LazioInnova spa, and by MIUR (Ministero dell'Istruzione, dell'Università e della Ricerca) via project PRIN 2017 "Taming complexity via QUantum Strategies a Hybrid Integrated Photonic approach" (QUSHIP) Id. 2017SRNBRK. This project has received funding from the European Union's Horizon 2020 Research and Innovation Program under Grant Agreement no. 899814 (Qurope). **Author contributions:** The experiment was performed, in the Marconi building, by F.B.B., E.R., and J.N., and, in the Fermi building, by M.V., G.C., D.P., and N.S., D.P. and E.R. wrote the software for data acquisition and secret key extraction. F.B.B. and E.R. performed the source characterization. M.V., V.M., and G.C. designed and assembled the receiver setup and the active stabilization system. F.B.B., E.R., and M.B.R. designed and assembled the source and sender setup. F.B.B., E.R., M.V., and D.P. wrote the manuscript with feedback from all authors. All the authors participated in the discussion of the results. R.T. and F.S. conceived the experiments and coordinated the project. **Competing interests:** The authors declare that they have no competing interests. **Data and materials availability:** All data needed to evaluate the conclusions in the paper are present in the paper and/or the Supplementary Materials. Additional data related to this paper may be requested from the authors.

Submitted 21 September 2020
Accepted 3 February 2021
Published 19 March 2021
10.1126/sciadv.abe6379

Citation: F. Basso Basset, M. Valeri, E. Roccia, V. Muredda, D. Poderini, J. Neuwirth, N. Spagnolo, M. B. Rota, G. Carvacho, F. Sciarrino, R. Trotta, Quantum key distribution with entangled photons generated on demand by a quantum dot. *Sci. Adv.* **7**, eabe6379 (2021).