PHYSICS

Quantum cryptography with highly entangled photons from semiconductor quantum dots

Christian Schimpf[1]*, Marcus Reindl[1], Daniel Huber[1], Barbara Lehner[1], Saimon F. Covre Da Silva[1], Santanu Manna[1], Michal Vyvlecka[2,3], Philip Walther[2,3], Armando Rastelli[1]

Semiconductor quantum dots are capable of emitting polarization entangled photon pairs with ultralow multi-pair emission probability even at maximum brightness. Using a quantum dot source with a fidelity as high as 0.987(8), we implement here quantum key distribution with an average quantum bit error rate as low as 1.9% over a time span of 13 hours. For a proof of principle, the key generation is performed with the BBM92 protocol between two buildings, connected by a 350-m-long fiber, resulting in an average raw (secure) key rate of 135 bits/s (86 bits/s) for a pumping rate of 80 MHz, without resorting to time- or frequency-filtering techniques. Our work demonstrates the viability of quantum dots as light sources for entanglement-based quantum key distribution and quantum networks. By increasing the excitation rate and embedding the dots in state-of-the-art photonic structures, key generation rates in the gigabits per second range are in principle at reach.

INTRODUCTION

Our everyday communication is secured by classical encryption systems that cannot hold up against attacks from emerging quantum technology (*1*). Quantum key distribution systems with single photons using the BB84 protocol (*2*), albeit being information-theoretically secure, exhibit severe security loopholes, such as splitting attacks (*3*). Furthermore, these systems are limited in range by the fundamental laws of quantum mechanics, rendering them impractical for extensive networks (*4*). Quantum key distribution systems with entangled photon pairs (EQKD) (*5*–*8*) are substantially more robust against attacks from outside and underlie no fundamental range limitations when embedded in quantum networks (*9*–*12*). Most of the EQKD experiments so far have been performed using photon pairs generated via the spontaneous parametric down-conversion (SPDC) process (*13*, *14*). However, for those sources, the multiphoton-pair emission probability is directly coupled to the source brightness by their approximately Poissonian emission characteristics (*15*). This circumstance currently limits the pair extraction efficiency for SPDC sources to about 0.01, as higher values inevitably increase the average photon-pair number (*15*). The excess photons lead to spurious detector clicks during the key generation in EQKD protocols, which results in key errors and security loopholes (*16*) and to a limited performance in quantum networks (*17*). To improve the source brightness without increasing the average multiphoton number, multiplexing of single photons emitted by several weakly pumped SPDCs has been successfully demonstrated (*18*). In this approach, one of the photons of a pair is sacrificed to herald the presence of the other. It is thus not yet clear whether multiplexing or other methods can be used for improving the performance of SPDCs as sources of entangled photon pairs. Semiconductor quantum dots (QDs) can generate polarization-entangled photon pairs (*19*–*22*) and do not suffer from these limitations because of their sub-Poissonian photon-pair emission characteristics (*19*, *23*). QDs were already successfully used in single-photon QKD experiments using optical (*24*) and electrical (*25*, *26*) excitation schemes. In addition, electrically driven QDs were used for a pioneering implementation of the Bennett-Brassard-Mermin-92 (BBM92) EQKD protocol with a sub-Poissonian source (*8*), albeit with moderate quantum bit error rate (QBER) and key rates. (As is customary, the QBER is defined as the number of erroneous detected counts over the total number of detections for a certain time window.)

Optically excited GaAs QDs obtained by droplet etching (*27*) can emit polarization-entangled photon pairs (*28*) with a demonstrated multiphoton emission probability as low as $8(2) \times 10^{-5}$ (*29*). The weak confinement of the multiparticle wave functions in these QDs (*30*) in combination with their high in-plane symmetry (*31*) result in entanglement fidelity values as high as 0.987(8) (see below), without resorting to time filtering or postgrowth tuning (*28*). The high-fidelity values allow for a low QBER and are therefore crucial for the viability and the effective secure key rate of EQKD implementations (*6*, *7*, *32*, *33*). Successful attempts of quantum teleportation (*34*) and entanglement swapping with QDs (*11*, *12*) further encourage the development of QD-based quantum networks for long-haul quantum communication (*10*).

RESULTS

The layout of our EQKD implementation is depicted in Fig. 1A. The first communication node ("Alice") and the GaAs QD-based photon source are situated in a laboratory in the semiconductor physics building at the Johannes Kepler University campus, while the second node ("Bob") is a mobile system placed on an office desk in the LIT Open Innovation Center (OIC) and is connected to the source by a 350-m-long single mode (SM) fiber. Entangled photon pairs are distributed via fibers from the source to Alice and Bob. A more detailed depiction of the setup is shown in Fig. 1B. The BBM92 protocol relies on analyzing the incoming photons in the rectilinear ("+") and diagonal ("×") basis (*6*). A passive choice of the measurement basis plays an essential role for the security of the protocol. We exploit the natural unpredictability of the path taken by a photon impinging on a 50:50 beam splitter (BS) to ensure the randomness. Different techniques can be used to reduce the number of detectors but at the cost of higher effort to ensure the randomness

[1]Institute of Semiconductor and Solid State Physics, Johannes Kepler University Linz, Linz, Austria. [2]Vienna Center for Quantum Science and Technology, Faculty of Physics, University of Vienna, Vienna, Austria. [3]Doppler Laboratory for Photonic Quantum Computers, Faculty of Physics, University of Vienna, Vienna, Austria.
*Corresponding author. Email: christian.schimpf@jku.at

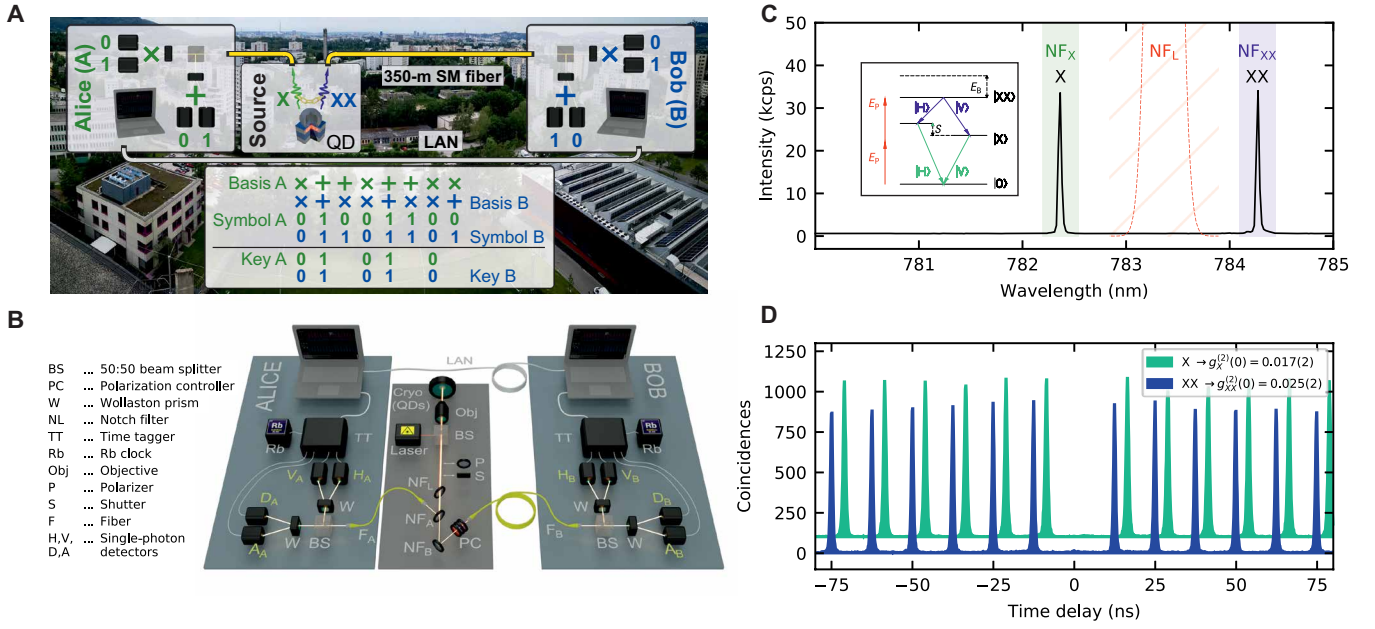

Fig. 1. Experimental setup and QD emission properties. (**A**) Configuration of the fiber-based EQKD system using highly entangled photons from a GaAs quantum dot (QD) photon source. Alice is situated in the laboratory, together with the photon source. Bob is assembled in a movable box placed in the LIT Open Innovation Center and connected to the photon source via a 350-m-long SM fiber. The photons are analyzed in the rectilinear ("+") and diagonal ("×") basis, and each outcome is assigned to a "0" or a "1" symbol. The key sifting, as sketched in the table, is performed over a 100-Mbits/s LAN connection. (**B**) Illustration of the optical and electronic components of the setup. The GaAs QD light source is in a He flow cryostat and is resonantly excited by a pulsed laser with a repetition rate of 80 MHz. A set of identical NFs reject laser stray light and distribute the entangled photons through F_A and F_B to Alice and Bob. The PC corrects for any reversible polarization-altering effects. Two identical four-state analysis setups at Alice and Bob measure the photons in rectilinear and diagonal basis. The TTs are connected to standard computers and backed by 10-MHz Rb frequency standards. A movable linear polarizer (P) and a shutter (S) are used for initial clock synchronization. (**C**) Emission spectrum of the resonantly driven QD after rejecting the laser stray light by NFL and selecting the X and XX lines by NFX and NFXX, respectively. The inset sketches the TPE, with E_P being the laser photon energy, S being the fine structure splitting, and E_B being the binding energy of the $|XX\rangle$ state. (**D**) Autocorrelation of the X and XX signals without background subtraction. The stated $g^{(2)}(0)$ values were extracted by using a time bin of 1 ns. Photo credit: Barbara Lehner, Johannes Kepler University.

of the basis and a higher vulnerability to side-channel attacks (*8*, *13*). Each detector after each of the two outputs of the BS (the two possible bases) is assigned either a symbol "0" or "1." Alice and Bob perform the key sifting procedure by exchanging only information about the measurement basis via a standard 100-Mbits/s local area network (LAN) connection, leaving no information for a potential eavesdropper on the public channel. Only if the entangled photon pairs arriving at the detectors of Alice and Bob are in the maximum entangled polarization state $|\phi^+\rangle$ with respect to the measurement basis, photons analyzed in the same basis cause the same measurement outcome at both sides and therefore identical key strings consisting of "0" and "1" symbols.

To generate entangled photon pairs, the QD is initialized into the biexciton state by a pulsed laser with a repetition rate of R = 80 MHz, using a two-photon excitation scheme (TPE) (*28*) (see inset of Fig. 1C). Figure 1C shows the spectra of the consecutively emitted photons from the biexciton-to-exciton (XX) and the exciton-to-groundstate (X) radiative decay for a selected QD. As we drive the XX state in a resonant process at saturation (at the so-called "π pulse" condition), a pair emission of the QD occurs with a probability of ϵ = 0.87(5) per pump pulse, which was extracted from cross-correlation measurements between the X and the XX photons (*35*). Figure 1D shows the autocorrelation histograms for the XX and X signals under these pumping conditions after filtering the remaining laser stray light. The autocorrelation was measured in situ with the detectors of Bob, as his setup is located inside a box exposed to daylight and therefore represents a worst-case scenario regarding the influence of ambient light. The finite values of the second-order correlation function at zero time delay extracted from the histograms, $g_X^{(2)}(0) = 0.017(2)$ and $g_{XX}^{(2)}(0) = 0.025(2)$, are predominantly governed by this ambient light [about 1000 counts per second (cps)] and to a smaller degree by the dark counts of the avalanche photodiodes (APDs) (about 200 cps). The contribution of the GaAs QD's multiphoton emission probability to the overall $g^{(2)}(0)$ value is largely negligible, as demonstrated by measurements under ultralow-noise conditions (*29*). For SPDC sources, in contrast, the multiphoton emission probability is directly connected to the pair emission probability by the Poissonian emission characteristics (*15*). While multiplexing of heralded single photons generated by multiple SPDC sources provides a possible solution to this problem (*18*), methods to improve the performance of SPDCs as sources of entangled photon pairs are still being sought for.

The maximum excitation pump rate for QD sources is only limited by the XX and X radiative lifetimes $T_{1,XX}$ and $T_{1,X}$, as no excitation can occur until the QD has relaxed into the groundstate. For the photonic structures used here ($T_{1,XX} \approx 120$ ps and $T_{1,X} \approx 230$ ps), a pump rate of about 1 GHz is accessible (see the Supplementary Materials for calculations). Reducing the lifetimes further by Purcell enhancement (*35*, *36*) can allow further increasing the maximum pump rate and, thus, of the key rates, possibly into the gigabits per second regime.

One of the most important parameters affecting the fidelity to the $|\phi^+\rangle$ state for QD sources is the so-called fine structure splitting (FSS) between the two X eigenstates (*37*). The photon pair's polarization state is described by

$$|\psi(t)\rangle_{X,XX} = \frac{1}{\sqrt{2}}\left(|H'\rangle_X |H'\rangle_{XX} + e^{-\frac{i}{\hbar}St}|V'\rangle_X |V'\rangle_{XX}\right) \quad (1)$$

where t is the time the QD dwells in the exciton state before decaying, $|H'\rangle$ and $|V'\rangle$ are two orthogonal linear polarization states, defined by the in-plane symmetry of the QD (*37*), and S is the FSS magnitude. The entangled state undergoes a time-dependent phase evolution, determined by the product of S and t. As no time filtering is used, the two-qubit density matrix is composed by all possible time-dependent states weighted by their emission probability

$$\rho_S = \int_0^\infty \frac{1}{T_{1,X}} e^{-\frac{t}{T_{1,X}}} |\psi(t)\rangle\langle\psi(t)| \, dt \quad (2)$$

The nonzero $g_X^{(2)}(0)$ and $g_{XX}^{(2)}(0)$ approximately lead to a mixing of ρ_S to the Wigner state

$$\rho = (1-g)\,\rho_S + g\frac{I^{(4)}}{4} \quad (3)$$

where $g := 1/2(g_X^{(2)}(0) + g_{XX}^{(2)}(0)) = 0.021(2)$ and $I^{(4)}$ is the 4×4 identity matrix. The Uhlmann-Jozsa fidelity (*38*) of the state ρ to the ideal state $\rho_{|\phi^+\rangle}$ is then given by

$$f_{|\phi^+\rangle}(\rho) := \left(\mathrm{tr}\sqrt{\sqrt{\rho}\,\rho_{|\phi^+\rangle}\sqrt{\rho}}\right)^2 \quad (4)$$

Because of the high in-plane symmetry of GaAs QDs (*31*), the distribution of S over different QDs shows values typically below 5 μeV; i.e., QDs with $S < 1$ μeV are straightforward to find. The QD used here exhibits a value of $S = 0.39(6)$ μeV, resulting in $f_{|\phi^+\rangle} = 0.985$ according to Eq. 4, which matches well with the experimentally determined value of 0.987(8) demonstrated further below.

A practical realization of EQKD requires distribution of entanglement over noisy quantum channels, like the SM fibers used here. The goal is to distribute the entangled photon pairs while ensuring the highest possible fidelity to the $|\phi^+\rangle$ Bell state. The first aspect to be considered in this case is the synchronization between Alice and Bob. The latter requires precise knowledge about the photon's arrival times at the nodes, which are possibly separated by large distances and exposed to different environmental conditions. Their hardware and internal clocks therefore inevitably operate dissimilarly. In Materials and Methods, we describe in detail how we handle the timing and synchronization between Alice and Bob with external Rb clocks and also propose an alternative without reference clocks. An important core feature of the synchronization method used here is the irrelevance of the hardware used, the fiber length, and the latency times, as it relies solely on the strong polarization correlation between the emitted XX and X photons.

The second aspect to be considered is the influence of the fibers themselves on the entangled photons. The most pronounced effect of SM fibers on propagating light is a general damping of the signal, which is about 3 decibels (dB)/km at a wavelength of 780 nm. Besides damping, more profound effects on entangled photons have to be taken into account when distributed over fibers: polarization-dependent loss (PDL) (*39*) and polarization mode dispersion (PMD) (*40*). PDL does not depend on the source's coherence properties and is less of an issue for modern fibers at length scales at which damping becomes the dominating limiting factor anyway (at about 200 km for 1550 nm or 10 km for 780 nm). PMD, on the other hand, not only randomly (but reversibly) alters the polarization state, but can lead to irreversible degradation of the entanglement (*40*, *41*). Sources with a photon coherence time T_2 lower than the fibers' differential group delay (DGD) (typically around 0.5 ps/$\sqrt{\text{km}}$) suffer substantially from PMD and one has to resort to frequency filtering (*42*). Although strategies exist to maximize the entanglement through quantum channels afflicted by PMD and/or PDL (*43*), these measures are complex and require precise knowledge about the effects and control about the polarization modes simultaneously. In the case of QDs, the T_2 time is capped by $T_{1,XX}$ and $T_{1,X}$, which are orders of magnitudes higher than the DGD of SM fibers, and, therefore, PMD has no meaningful impact on the entanglement (see the Supplementary Materials for supporting calculations).

Even in the absence of PMD and PDL, a complex rotation of the polarization state always persists because of the random birefringence induced by SM fibers. However, this rotation is reversible and can be cancelled by a polarization controller (PC). As long as the variation of the rotation (e.g., due to temperature fluctuations) is slow compared to the measurement time, it can be eliminated effectively during the whole key generation procedure by readjusting the PC on demand (see Materials and Methods). For testing the capabilities of the PC and to probe the entanglement fidelity, preliminary experiments were performed, where Bob was placed together with Alice in the laboratory and connected by a 700-m-long fiber (350 m to the OIC and 350 m back to the laboratory). Figure 2 depicts the density matrices of the entangled state determined via full-state tomography before (A) and after (B) polarization correction. The resulting concurrence is 0.95(2), and the fidelity according to Eq. 4 is 0.987(8). From the density matrix, the QBER can be estimated by

$$q = \frac{1}{2}\sum_{i=1}^{4}\langle O_i|\,\rho\,|O_i\rangle \quad (5)$$

where $O_i \in \{H_A V_B,\ V_A H_B,\ D_A A_B,\ A_A D_B\}$ corresponds to cross-correlation measurements between Alice's and Bob's photons in the orthogonal bases. Equation 5 therefore yields the average probability of measuring an unwanted coincidence in the BBM92 measurement configuration using an (ideally) $|\phi^+\rangle$ Bell state, which is 1.5(6)% for the density matrix from Fig. 2B.

After the initial polarization correction, the setup is prepared for continuous key generation. During this operation, the software executed at Alice's and Bob's notebooks permanently monitors the QBER by comparing a random and subsequently discarded subset of the generated keys. The random choice prevents a potential attacker from finding predictable time windows for eavesdropping without being detected. During normal operation, only a small fraction of keys has to be sacrificed for this purpose to achieve appropriate accuracy and security. However, the target here was to record the QBER with high frequency and with high accuracy, so we dedicated 10% of the keys and excluded this fraction from the key rate calculations. For the key generation, we include all photons from the QD by choosing a time bin of 1 ns [the same as used for determining $g^{(2)}(0)$], which is about four times as long as X decay time. This excludes the largest amount of background photons from ambient light but includes about 97% of the photons from the QD and

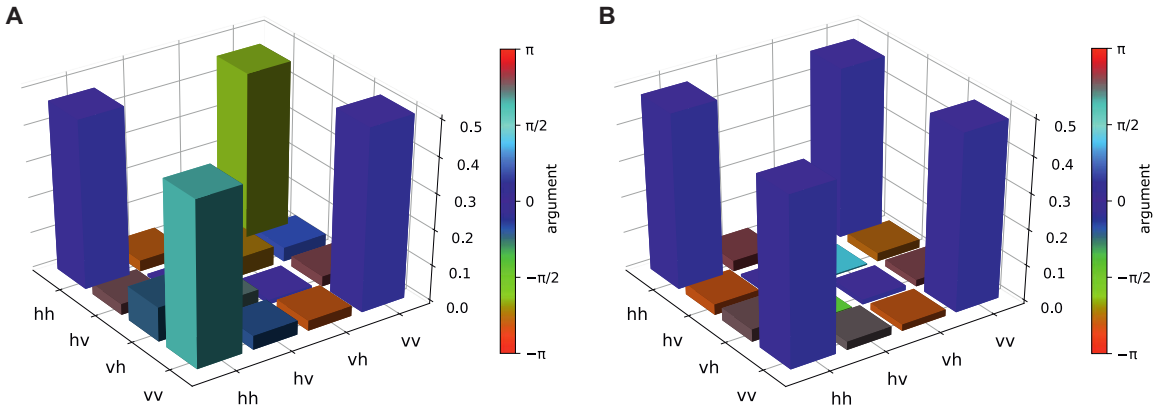

Fig. 2. Full-state tomography of the entangled photon pair. Two-qubit polarization state after transport of the X photons through a 700-m-long fiber. Density matrix with a concurrence of 0.95(2) before (**A**) and after (**B**) polarization correction, resulting in a fidelity of 0.987(8).

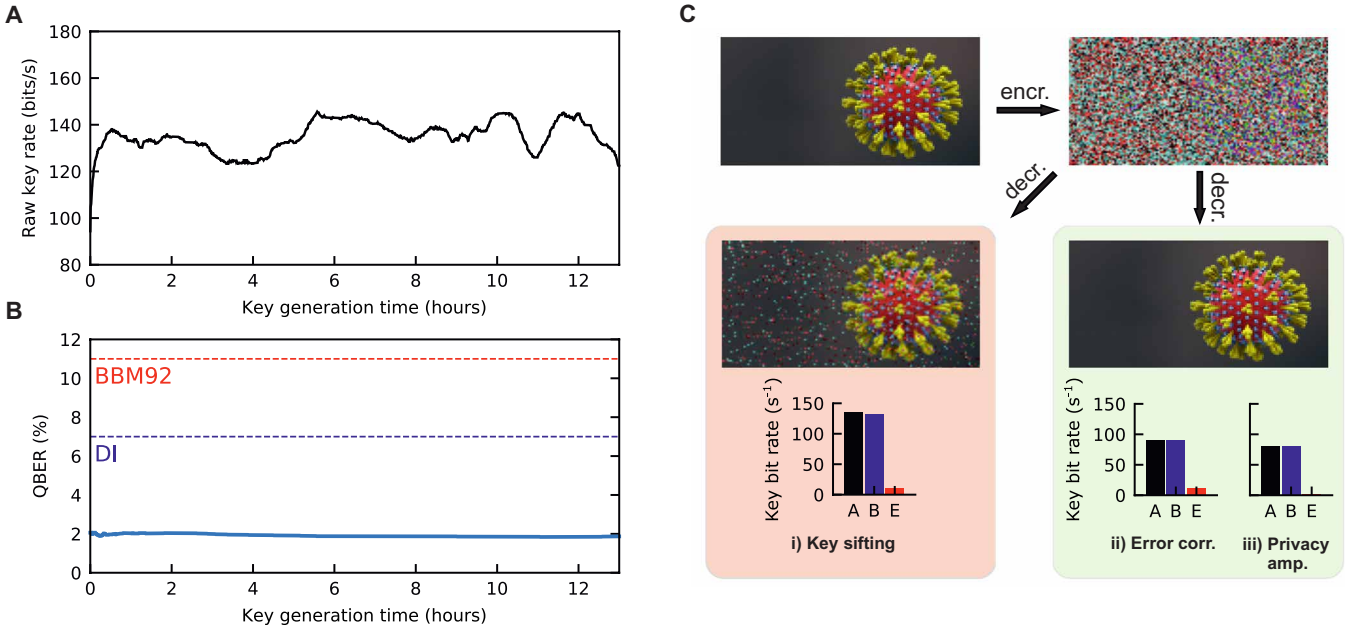

Fig. 3. Key generation and post processing. (**A**) Raw key rate and (**B**) QBER over a time span of 13 hours. The dashed lines indicate the upper limits of 11% for the BBM92 and 7% for the DI protocols. (**C**) Exemplary encryption (encr.) of a 29.2-kilobyte large bitmap with Alice's key using the one-time pad method, with a subsequent decryption (decr.) with Bob's key. The decrypted bitmaps are shown for the cases (i) directly after key sifting and (ii and iii) after error correction and privacy amplification. The bar charts indicate the distribution of information over Alice (A), Bob (B), and the eavesdropper (E) after each step.

therefore does not temporally filter the signal appreciably [which, however, can be done in applications supporting high time resolution (*44*)]. Figure 3A shows the raw key rate, which has an average of 135 bits/s over a time span of 13 hours. The bit rate in our experiment is mainly limited by the extraction and collection efficiencies of the photons and several compromises made within the experimental setup. An additional factor is blinking (*45*, *46*), which decreases the fraction of time over which the QD is optically active to about 0.3 for the QD used here (see the Supplementary Materials for the measurement). Blinking, however, is not a fundamental limit and can be possibly overcome by improving the growth process or by embedding the QD into a charge-tunable device (*47*). We provide a detailed derivation of the raw key rate in Materials and Methods.

The monitored QBER of 1.91% in average is shown in Fig. 3B. The dashed lines indicate the maximum QBER of 11% for the BBM92 used here (*6*, *33*) and 7% for the device-independent (DI) (*7*) protocols, respectively, below which it is still possible to distill secure keys. The DI protocol protects against potential collective attacks and includes an additional measurement basis at one node, which can be readily implemented in the present system. Without adjusting the PC during the measurement, we observed a variation of the QBER between 1.84 and 2.06% over the course of the measurement, probably stemming from slight changes of the fiber's environment,

such as temperature and vibrations. Compared to preliminary tests with short fibers (2 m) in the laboratory, we observed no increase in average QBER, as expected owing to the negligible effect of PDL and PMD on the photons from QDs.

The fraction of "1" symbols in the resulting key strings is 0.513, which reveals a slight bias toward the "1" symbol. This discrepancy arises mostly from slight differences of the efficiencies of the single-photon detectors in the four-state measurement arrangements. The resulting nonunity Shannon entropy poses a minor potential security threat, but can be corrected by inverting a random half of the bits for both keys (*7*). Assuming an unknown measurement apparatus, one always has to expect the initial finite QBER to stem from an intercept-resend attack from an eavesdropper tampering with the quantum channel (*33*). Double clicks within the observed time window, whether they stem from the nonperfect $g^{(2)}(0)$ or from an eavesdropper, are included in the key generation process and will therefore inevitably lead to detected key errors, which closes the double-click security loophole (*16*). The finite QBER can be reduced to zero during the act of error correction by iterative parity exchange (*13*, *32*) and subsequent "bit twiddling" (*48*), where both procedures leak a negligible portion of information about the keys to the public channel. The number of leaked deterministic bits during an intercept-resend attack—plus five SDs—can be estimated (*32*) by $l = 4Nq + 5\sqrt{12Nq}$, where N is the length of the key and q is the QBER. To erase this information, a "privacy amplification" technique (*48*) is applied: The key is compressed to a maximum length of $N - l$ by using a random universal hash function on which Alice and Bob agree over the public channel. Figure 3C depicts the encryption of a bitmap using 29.2 kilobytes of Alice's key (acquired in about 46 min), using the information-theoretically secure one-time pad method. The latter is performed by applying the bit-wise XOR operation of the original bitmap and Alice's key. The decryption is done by performing the same operation with the encrypted message and Bob's key. The bar charts in (i) to (iii) depict the distribution of information about the key among Alice (A), Bob (B), and a potential eavesdropper (E) after key sifting, error correction, and privacy amplification, respectively. The latter decrease the secure key rate depending on the QBER (see the Supplementary Materials for calculations); hence, a small QBER is desired for a high secure key rate. The average raw key rate achieved here with the 350-m-long fiber is 135 bits/s with an average QBER of 1.91%. The resulting secure key rate after correction is 86 bits/s and a final QBER of 0. In addition to the discussed intercept-resend attacks, certain types of side-channel attacks have to be considered when applying the BBM92 protocol. The most relevant of them are listed and well explained in (*14*). The efficiency-mismatch attack and detector dead-time attack are both ruled out because we operate the APDs in free-running mode. A spatial-mode attack cannot be conducted, because Alice and Bob are connected to the source via SM fibers, which only propagates one spatial mode. Our implementation is, however, in principle, still vulnerable to detector-blinding attacks, which could be eliminated by directly monitoring the APD's output voltages. Also, a BS attack, which exploits the wavelength dependency of the splitting ratio of the BS used for the passive basis choice, can be ruled out by using band-pass filters.

DISCUSSION

In conclusion, we have presented the implementation of quantum cryptography using a quantum key derived from near-perfectly entangled photon pairs generated by a GaAs QD obtained by droplet etching (*27*, *31*). Secure communication with an average QBER of 1.91% and a raw (secure) key rate of 135 bits/s (86 bits/s) for a pump rate of 80 MHz was established between two buildings connected by a 350-m-long optical fiber. The very low QBER, achieved without sacrificing photons via time filtering, is a direct consequence of the high fidelity of the source [0.987(8)] and low $g^{(2)}(0)$ values [0.021(2), mostly stemming from ambient light]. While we have used here the BBM92 protocol (*6*) as in a former work using time-filtered photons electrically generated by an InGaAs QD (*8*), the demonstrated QBER would allow for implementing more demanding protocols like the DI scheme (*7*).

The long coherence time of photons emitted by QDs prevents a degradation of the polarization entanglement when transported via SM fibers over practically relevant distances of hundreds of kilometers (*40*). The general damping in fibers, however, currently limits the transmission rates for the wavelength used here (about 780 nm). Although free space entanglement distribution at this wavelength was successfully performed over a distance of 1120 km (*14*), using the well-established fiber-based telecom infrastructure is desirable for the targeted, highly interconnected quantum networks. To this end, entangled photons in the telecom band (around 1550 nm) could be obtained either by down-converting (*49*) photons emitted by the GaAs QDs used here or by further developing QDs based on different materials (*50*, *51*).

The photon-pair collection efficiency of the here demonstrated source (after fiber coupling) is about 0.002. To outperform SPDC sources, we estimate a required value of about 0.06 (see the Supplementary Materials for calculations). The brightness of the QD source can be increased by embedding the QDs into circular Bragg resonators, which have demonstrated pair extraction efficiencies over 0.6 (*36*) (about 0.2 after fiber coupling) and Purcell enhancements of up to 11 (*35*).

Exploiting the substantially higher extraction efficiency, while optimizing the optical setup specifically for QKD, increasing the pump rate to 1 GHz, and eliminating blinking (*47*), raw key rates of hundreds of megabits per second are realistic, while leaving the QBER unaltered. By reducing the radiative lifetimes via Purcell enhancement and by using timing hardware and detectors with appropriate time resolution (like superconducting nanowire single-photon detectors), the pump rate could even be further increased to bring raw key rates in gigabits per second at reach, which is well beyond the capabilities of SPDC sources. Considering the simultaneously high photon indistinguishability (*36*), QDs have the potential to act as nodes in much desired quantum networks (*10*, *11*, *34*).

MATERIALS AND METHODS

Materials

The GaAs QDs used here were grown by the local droplet etching method by molecular beam epitaxy. The QDs are embedded in a planar lambda cavity, consisting of a 117-nm-thick $Al_{0.33}Ga_{0.67}As$ layer between two 57-nm-thick $Al_{0.2}Ga_{0.8}As$ layers, sandwiched between two distributed Bragg reflectors (DBRs). The DBRs are composed of nine (bottom) and two (top) pairs of $Al_{0.20}Ga_{0.80}As$ and $Al_{0.95}Ga_{0.05}As$ layers with 57-nm and 65.6-nm thickness, respectively. With an additional solid immersion lens (SIL) on top, this yields an extraction efficiency of $\eta_e \approx 0.1$.

Resonant TPE

The sample is placed in a He flow cryostat and cooled to $T = 5$ K. Resonant TPE is performed using wavelength-tunable laser pulses with a repetition rate of 80 MHz, a pulse width of about 10 ps, and a pulse energy of about 15 fJ (average pulse power of 1.1 μW), which are focused on a single QD. To minimize the blinking to a minimum [quantified by $\beta = t_{on}/(t_{off} + t_{on}) = 0.3$ for the used QD, with t_{on} and t_{off} being the time during which the QD is optically active and inactive, owing to random charge capture] for the used QD, we feed additional white light from a light-emitting diode into the excitation path.

Photon collection and separation

The emitted XX and X photons collected by the objective (Obj in Fig. 1B) pass a set of notch filters NFL with a bandwidth of 0.2 nm each, which reflect the largest part of the excitation laser stray light. The NF's central wavelength can be tuned from 780 to 786 nm by adjusting their tilting angle. Two NFs of the same type are individually tuned to reflect only the X (NFA) and XX (NFB) photons, which are then coupled into SM fibers FA (leading to Alice) and FB (leading to Bob). Depending on the experiment, the length of FB can vary between 2 and 700 m (2 × 350 m). The 2-m fibers are of type "Thorlabs 780HP" and the 350-m fibers are of type "Nufern 780HP."

Four-state measurement

Alice and Bob both analyze their incoming photons by two nominally identical four-state measurement apparatus, which form the core of the BBM92 arrangement. In each setup, a 50:50 BS is used to randomly select the measurement basis by directing the photons in one of two arms of the setup. In the reflected path, a Wollaston prism (W) is rotated such that one of its eigenaxis is approximately parallel to the optical table plane, which we define as the $|H\rangle$ polarization. As a consequence, the photons are measured in the rectilinear basis $\{|H\rangle, |V\rangle\}$ by the following APDs $H_{A,B}$ and $V_{A,B}$, connected to a time tagger (TT), which registers the detector clicks. As a side effect of this particular arrangement, the rectilinear basis forms an eigenbasis of the polarization transformation caused by the BS reflection, which can therefore safely be neglected in the following considerations (see proof in the Supplementary Materials). In the transmission path of the BS, the W is rotated by 45° with respect to $|H\rangle$, so that the signal is measured in the diagonal basis $\{|D\rangle, |A\rangle\}$ by the APDs $D_{A,B}$ and $A_{A,B}$.

Spectroscopy and autocorrelation measurement

The spectra of the X and XX signals are analyzed by a standard reflective diffraction spectrometer with a resolution of about 30 μeV. The FSS, despite being below the spectrometer's resolution, can be determined by polarization mapping (see the Supplementary Materials for details). The autocorrelation of the X or XX signal can be recorded by combining the detector events from H, V and D, A, respectively, to mimic a Hanbury Brown and Twiss setup. The $g^{(2)}(0)$ is then obtained by summing up all coincidences in the autocorrelation histogram (recorded with a resolution of 128 ps) within a time bin of 1 ns around time delay zero, yielding A_0. No subtraction of the background is performed. This value is then divided by the average peak area of the first six neighbor side peaks (three to the left and three to the right) in the histogram, again by summing up the coincidences within the same time bin around the peak maxima, yielding $\overline{A_S}$. The $g^{(2)}(0)$ is then calculated by $A_0/\overline{A_S}$. From the measurement of the blinking dynamics (see the Supplementary Materials), we observe a bunching spanning over several microseconds, which influences the statistics in a comparatively small time window (a few hundreds of nanoseconds) almost by a constant amount. We therefore assume that the first few side peaks are appropriate for calculating $\overline{A_S}$.

Timing and synchronization

The internal clocks of the TTs are backed up by Rb clocks, acting as a 10-MHz frequency standard. The detection time delay between the X and XX photons can be found by exploiting the strong polarization correlation between the entangled X and XX photons. Once determined, the time delay can be tracked continuously during QKD operation without leaking information about the key on the public channel. See the Supplementary Materials for more details.

Polarization control

For canceling the polarization-altering effects induced by the fibers in an optimal and efficient manner for the given purpose, a heuristic approach was chosen: We assume the static transformations $\hat{F}_A$ and $\hat{F}_B$ in the two-dimensional polarization space for the fibers FA and FB, respectively. The entangled state undergoes the bilocal transformation to $|\psi'(t)\rangle = (\hat{F}_A \otimes \hat{F}_B)|\psi(t)\rangle$. If the transformation is purely governed by PMD, $\hat{F}_A$ and $\hat{F}_B$ are unitary and the following equation holds (see the Supplementary Materials for proof) $|\psi'(t)\rangle = (\hat{1} \otimes \hat{F}_B \hat{F}_A{}^\dagger)|\psi(t)\rangle$, where $\hat{1}$ is the unity operator. This implies that the combined transformations of both fibers can be cancelled by inducing an additional unitary transformation $\hat{U}$ anywhere along X or XX light path, so that $\hat{U}\hat{F}_B\hat{F}_A{}^\dagger = \hat{F}_B\hat{F}_A{}^\dagger\hat{U} = \hat{1}$. A PC (Fig. 1B) consisting of three rotatable wave plates (two quarter–wave plates and one half–wave plate) is capable of generating an arbitrary unitary transformation $\hat{U}(\boldsymbol{\theta}) \in$ SU(2) in the polarization space (see the Supplementary Materials for details), where $\boldsymbol{\theta} = (\theta_1, \theta_2, \theta_3)$ represents the three rotation angles. An optimum for $\boldsymbol{\theta}$ is found by observing the correlation between Alice's and Bob's detectors and minimizing the coincidences in the orthogonal bases $O_i \in \{H_AV_B, V_AH_B, D_AA_B, A_AD_B\}$ (later corresponding to key errors) while maximizing the coincidences in the colinear bases $C_i \in \{H_AH_B, V_AV_B, D_AD_B, A_AA_B\}$ (later corresponding to valid key entries), which is equivalent to minimizing the loss model function.

$L(\boldsymbol{\theta}) := \sum_{i=1}^{4} \langle O_i|\rho(\boldsymbol{\theta})|O_i\rangle + \left(\frac{1}{2} - \langle C_i|\rho(\boldsymbol{\theta})|C_i\rangle\right)$, with $\rho(\boldsymbol{\theta})$ being the two-photon density matrix for the rotation angles $\boldsymbol{\theta}$. A downhill-simplex optimization algorithm is used for minimizing L in about 6 min in average when starting without initial guess.

Estimation of the raw key rate

The raw key rate can be modeled as

$$n = R\,\beta\,\epsilon\,\eta_e^2\,\eta_c^2\,\eta_s^2\,\eta_{f,A}\,\eta_{f,B}\,\eta_{det}^2\,\frac{1}{2} \tag{6}$$

with $R = 80$ MHz being the repetition rate of the excitation laser, $\beta = 0.3$ being the fraction of time during which the QD is optically active because of blinking (*45*, *46*) (see the Supplementary Materials for the measurement), $\epsilon = 0.87(5)$ being the photon-pair emission probability, $\eta_e = 0.1$ being the extraction efficiency of the photons out of the photonic structure, and $\eta_c = 0.7$ being the collection efficiency of the objective with a numerical aperture of 0.42. The efficiency of the optical components in the setup $\eta_S \approx 0.4$ is given by

the transmission through the 90/10 BS used in the confocal setup, the notch filters and the Wollaston prisms, the combined efficiencies of the mirrors, and the coupling efficiencies into the multimode fibers leading to the APDs. The efficiencies $\eta_{f,A} = 0.26$ and $\eta_{f,B} = 0.22$ of the fibers leading to Alice and Bob, respectively, are composed of coupling efficiency, attenuation in the fiber, and losses at fiber mating sleeves. The coupling efficiency of the XX was limited to 0.3—compared to 0.45 of the X—because of the higher distance of the fiber coupler to the objective. To match the efficiencies $\eta_{f,A}$ and $\eta_{f,B}$ as well as possible, the X photon was sent to Bob over the 350-m-long fiber with a total attenuation of about 1 dB and two fiber mating sleeves with 0.85 efficiency each. The XX photons were sent to Alice via two 2-m-long fibers connected by one fiber mating sleeve. The detector efficiency $\eta_{det} = 0.65$ of the used "Excelitas SPCM-ARQH-12-FC" APD was extracted from the data sheet. The factor 1/2 is specific for the BMM92 protocol and represents the probability of the two entangled photons being measured in the same basis. By inserting the above values into Eq. 6, we estimate the raw key rate to be about 190 bits/s, which is close to the measured value of 134 bits/s.

SUPPLEMENTARY MATERIALS

Supplementary material for this article is available at http://advances.sciencemag.org/cgi/content/full/7/16/eabe8905/DC1

REFERENCES AND NOTES

1. P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **41**, 303–332 (1999).
2. C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).
3. H. K. Lo, X. Ma, K. Chen, Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
4. M. Lucamarini, Z. L. Yuan, J. F. Dynes, A. J. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
5. A. K. Ekert, Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
6. C. H. Bennett, G. Brassard, N. D. Mermin, Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **68**, 557–559 (1992).
7. 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).
8. 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).
9. H. J. Briegel, W. Dür, J. I. Cirac, P. Zoller, Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932–5935 (1998).
10. H. J. Kimble, The quantum internet. *Nature* **453**, 1023–1030 (2008).
11. 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, R. Trotta, Entanglement swapping with photons generated on demand by a quantum dot. *Phys. Rev. Lett.* **123**, 160501 (2019).
12. M. Zopf, R. Keil, Y. Chen, J. Yang, D. Chen, F. Ding, O. G. Schmidt, Entanglement swapping with semiconductor-generated photons violates Bell's inequality. *Phys. Rev. Lett.* **123**, 160502 (2019).
13. T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, A. Zeilinger, Quantum cryptography with entangled photons. *Phys. Rev. Lett.* **84**, 4729–4732 (2000).
14. 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).
15. J. Schneeloch, S. H. Knarr, D. F. Bogorin, M. L. Levangie, C. C. Tison, R. Frank, G. A. Howland, M. L. Fanto, P. M. Alsing, Introduction to the absolute brightness and number statistics in spontaneous parametric down-conversion. *J. Opt.* **21**, 043501 (2019).
16. 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).
17. Y. Wu, J. Liu, C. Simon, Near-term performance of quantum repeaters with imperfect ensemble-based quantum memories. *Phys. Rev. A* **101**, 042301 (2020).
18. E. Meyer-Scott, C. Silberhorn, A. Migdall, Single-photon sources: Approaching the ideal through multiplexing. *Rev. Sci. Instrum.* **91**, 041101 (2020).
19. O. Benson, C. Santori, M. Pelton, Y. Yamamoto, Regulated and entangled photons from a single quantum dot. *Phys. Rev. Lett.* **84**, 2513–2516 (2000).
20. N. Akopian, N. H. Lindner, E. Poem, Y. Berlatzky, J. Avron, D. Gershoni, B. D. Gerardot, P. M. Petroff, Entangled photon pairs from semiconductor quantum dots. *Phys. Rev. Lett.* **96**, 130501 (2006).
21. A. Dousse, J. Suffczyński, A. Beveratos, O. Krebs, A. Lemaître, I. Sagnes, J. Bloch, P. Voisin, P. Senellart, Ultrabright source of entangled photon pairs. *Nature* **466**, 217–220 (2010).
22. G. Juska, V. Dimastrodonato, L. O. Mereni, A. Gocalinska, E. Pelucchi, Towards quantum-dot arrays of entangled photon emitters. *Nat. Photonics* **7**, 527–531 (2013).
23. P. Senellart, G. Solomon, A. White, High-performance semiconductor quantum-dot single-photon sources. *Nat. Nanotechnol.* **12**, 1026–1039 (2017).
24. 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).
25. 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**, 83001 (2012).
26. 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).
27. M. Gurioli, Z. Wang, A. Rastelli, T. Kuroda, S. Sanguinetti, Droplet epitaxy of semiconductor nanostructures for quantum photonic devices. *Nat. Mater.* **18**, 799–810 (2019).
28. D. Huber, M. Reindl, S. F. Covre 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).
29. L. Schweickert, K. D. Jöns, K. D. Zeuner, S. F. Covre 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).
30. D. Huber, B. U. Lehner, D. Csontosová, M. Reindl, S. Schuler, S. F. Covre Da Silva, P. Klenovský, A. Rastelli, Single-particle-picture breakdown in laterally weakly confining GaAs quantum dots. *Phys. Rev. B* **100**, 235425 (2019).
31. Y. H. Huo, A. Rastelli, O. G. Schmidt, Ultra-small excitonic fine structure splitting in highly symmetric quantum dots on GaAs (001) substrate. *Appl. Phys. Lett.* **102**, 152105 (2013).
32. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, Experimental quantum cryptography. *J. Cryptol.* **5**, 3–28 (1992).
33. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
34. M. Reindl, D. Huber, C. Schimpf, S. F. Covre Da Silva, M. B. Rota, H. Huang, V. Zwiller, K. D. Jöns, A. Rastelli, R. Trotta, All-photonic quantum teleportation using on-demand solid-state quantum emitters. *Sci. Adv.* **4**, eaau1255 (2018).
35. 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).
36. 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).
37. M. Bayer, G. Ortner, O. Stern, A. Kuther, A. Gorbunov, A. Forchel, P. Hawrylak, S. Fafard, K. Hinzer, T. Reinecke, S. Walck, J. Reithmaier, F. Klopf, F. Schäfer, Fine structure of neutral and charged excitons in self-assembled In(Ga)As/(Al)GaAs quantum dots. *Phys. Rev. B* **65**, 195315 (2002).
38. Y.-C. Liang, Y.-H. Yeh, P. E. M. F. Mendonça, R. Y. Teh, M. D. Reid, P. D. Drummond, Quantum fidelity measures for mixed states. *Reports Prog. Phys.* **82**, 076001 (2019).
39. B. Huttner, C. Geiser, N. Gisin, Polarization-induced distortions in optical fiber networks with polarization-mode dispersion and polarization-dependent losses. *IEEE J. Sel. Top. Quantum Electron.* **6**, 317–329 (2000).
40. C. Antonelli, M. Shtaif, M. Brodsky, Sudden death of entanglement induced by polarization mode dispersion. *Phys. Rev. Lett.* **106**, 080404 (2011).
41. H. T. Lim, K. H. Hong, Y. H. Kim, Effects of polarization mode dispersion on polarization-entangled photons generated via broadband pumped spontaneous parametric down-conversion. *Sci. Rep.* **6**, 25846 (2016).
42. A. Poppe, H. Hübel, T. Lederer, A. Fedrizzi, M. R. Vanner, A. Zeilinger, Detection of polarization entanglement after 75 km of fiber transmission, in *Proc. ECOC* (2006).
43. D. E. Jones, B. T. Kirby, M. Brodsky, Tuning quantum channels to maximize polarization entanglement for telecom photon pairs. *npj Quantum Inf.* **4**, 58 (2018).

44. 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).
45. A. V. Kuhlmann, J. Houel, A. Ludwig, L. Greuter, D. Reuter, A. D. Wieck, M. Poggio, R. J. Warburton, Charge noise and spin noise in a semiconductor quantum device. *Nat. Phys.* **9**, 570–575 (2013).
46. 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).
47. 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).
48. C. H. Bennett, G. Brassard, J. M. Robert, Privacy amplification by public discussion. *SIAM J. Comput.* **17**, 210–229 (1988).
49. J. H. Weber, B. Kambs, J. Kettler, S. Kern, J. Maisch, H. Vural, M. Jetter, S. L. Portalupi, C. Becher, P. Michler, Two-photon interference in the telecom C-band after frequency conversion of photons from remote quantum emitters. *Nat. Nanotechnol.* **14**, 23–26 (2019).
50. F. Olbrich, J. Höschele, M. Müller, J. Kettler, S. L. Portalupi, M. Paul, M. Jetter, P. Michler, Polarization-entangled photons from an InGaAs-based quantum dot emitting in the telecom C-band. *Appl. Phys. Lett.* **111**, 133106 (2017).
51. Z. H. Xiang, J. Huwer, R. M. Stevenson, J. Skiba-Szymanska, M. B. Ward, I. Farrer, D. A. Ritchie, A. J. Shields, Long-term transmission of entangled photons from a single quantum dot over deployed fiber. *Sci. Rep.* **9**, 4111 (2019).
52. H. G. Berry, G. Gabrielse, A. E. Livingston, Measurement of the Stokes parameters of light. *Appl. Optics* **16**, 3200–3205 (1977).
53. Y. Chen, M. Zopf, R. Keil, F. Ding, O. G. Schmidt, Highly-efficient extraction of entangled photons from quantum dots using a broadband optical antenna. *Nat. Commun.* **9**, 2994 (2018).
54. C. Schimpf, M. Reindl, P. Klenovský, T. Fromherz, S. F. Covre Da Silva, J. Hofer, C. Schneider, S. Höfling, R. Trotta, A. Rastelli, Resolving the temporal evolution of line broadening in single quantum emitters. *Opt. Express* **27**, 35290–35307 (2019).
55. J. Watrous, *The Theory of Quantum Information* (Cambridge Univ. Press, 2018).
56. R. Simon, N. Mukunda, Minimal three-component SU(2) gadget for polarization optics. *Phys. Lett. A* **143**, 165–169 (1990).
57. A. J. Hudson, R. M. Stevenson, A. J. Bennett, R. J. Young, C. A. Nicoll, P. Atkinson, K. Cooper, D. A. Ritchie, A. J. Shields, Coherence of an entangled exciton-photon state. *Phys. Rev. Lett.* **99**, 266802 (2007).

Acknowledgments: C.S. is a recipient of a DOC Fellowship of the Austrian Academy of Sciences at the Institute of Semiconductor Physics at Johannes Kepler University, Linz, Austria. We thank C. Diskus for providing the Rb clocks, S. Zeppetzauer for assistance in the laboratory, and J. Handsteiner, M. Bozzio, R. Kueng, and R. Wille for fruitful discussions. **Funding:** This work was financially supported by the Austrian Science Fund (FWF) via SFB-BeyondC (F71), Forschergruppe (FG5), P 29603, P 30459, I 4320, I 4380, I 3762, the European Union's Horizon 2020 research and innovation programs under GA No 731473 (QUANTERA), GA no. 899814 (Qurope) and GA no. 871130 (ASCENT+), the Linz Institute of Technology (LIT), and the LIT Secure and Correct Systems Lab, supported by the State of Upper Austria. **Author contributions:** C.S., M.R., and D.H. established the optical setup and the electronics for the experiment. C.S. programmed the software; performed the measurements with the support of B.L., M.R., M.V., and P.W.; carried out the theoretical modeling with the support of B.L.; analyzed and processed the data; and wrote the manuscript with inputs from A.R., P.W., and M.V. S.F.C.D.S. grew the sample with the support of S.M. A.R. initiated 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 and the Supplementary Materials can be accessed via https://doi.org/10.5281/zenodo.4432366. Additional data and information related to this paper may be requested from the authors.

Submitted 21 September 2020
Accepted 25 February 2021
Published 14 April 2021
10.1126/sciadv.abe8905

Citation: C. Schimpf, M. Reindl, D. Huber, B. Lehner, S. F. Covre Da Silva, S. Manna, M. Vyvlecka, P. Walther, A. Rastelli, Quantum cryptography with highly entangled photons from semiconductor quantum dots. *Sci. Adv.* **7**, eabe8905 (2021).

ScienceAdvances

Quantum cryptography with highly entangled photons from semiconductor quantum dots

Christian SchimpfMarcus ReindlDaniel HuberBarbara LehnerSaimon F. Covre Da SilvaSantanu MannaMichal VyvleckaPhilip WaltherArmando Rastelli

Sci. Adv., 7 (16), eabe8905. • DOI: 10.1126/sciadv.abe8905