ARTICLE OPEN

Check for updates

Quantum key distribution using deterministic single-photon sources over a field-installed fibre link

Mujtaba Zahidy[1,5], Mikkel T. Mikkelsen[2,5], Ronny Müller[1], Beatrice Da Lio[2], Martin Krehbiel[2], Ying Wang[2], Nikolai Bart[3], Andreas D. Wieck[3], Arne Ludwig[3], Michael Galili[1], Søren Forchhammer[1], Peter Lodahl[2], Leif K. Oxenløwe[1], Davide Bacco[1,4]✉ and Leonardo Midolo[2]✉

Quantum-dot-based single-photon sources are key assets for quantum information technology, supplying on-demand scalable quantum resources for computing and communication. However, long-lasting issues such as limited long-term stability and source brightness have traditionally impeded their adoption in real-world applications. Here, we realize a quantum key distribution field trial using true single photons across an 18-km-long dark fibre, located in the Copenhagen metropolitan area, using an optimized, state-of-the-art, quantum-dot single-photon source frequency-converted to the telecom wavelength. A secret key generation rate of > 2 kbits/s realized over a 9.6 dB channel loss is achieved with a polarization-encoded BB84 scheme, showing remarkable stability for more than 24 hours of continuous operation. Our results highlight the maturity of deterministic single-photon source technology while paving the way for advanced single-photon-based communication protocols, including fully device-independent quantum key distribution, towards the goal of a quantum internet.

npj Quantum Information (2024)10:2 ; https://doi.org/10.1038/s41534-023-00800-x

INTRODUCTION

With the fast-growing developments of photonic-based quantum information technology, the demand for a reliable and deployable deterministic source of single photons has risen to new heights. In recent years, semiconductor quantum dots (QDs) embedded in photonic nanostructures have drawn significant attention by providing a robust and near-deterministic source of single photons[1]. The ability to generate indistinguishable photons on demand and couple them into optical fibers with high efficiency opens new avenues for the realization of a quantum internet[2,3], where photons will allow the secure exchange of secret cryptographic keys via quantum key distribution (QKD) or more advanced functionalities enabled by distributing quantum information via teleportation or entanglement swapping. To achieve this goal, it is essential that single-photon sources achieve sufficient quality and technological readiness to be operated in the field where virtually no control is available over sources of noise or loss of network infrastructure. Examples of quantum communication field trials using quantum emitters such as color centers in diamond[4], semiconductor QDs[5–9] are to date limited to short distances within university campuses over dedicated fibres or in free space. Recently, a new study on the transmission of QD-generated single-photons for randomness generation was reported at km distances[8]. For the interested reader, a review of semiconductor QDs and their application in quantum communication can be found in[10,11].

In contrast, field trials of QKD links based on weak coherent pulses (i.e., attenuated laser) are regularly carried out at the urban-area network level, over dedicated testbeds[12–14], or even via satellite[15]. While laser sources, combined with decoy state protocols[16] enable remarkably higher communication rates than single-photon sources, the latter offer exciting perspectives in the development of more advanced quantum communication tasks involving entanglement and, eventually, a fully device-independent QKD scheme. Therefore, a field demonstration of a single-photon-based QKD link is an important stepping stone in proving the maturity of QDs in a real-world use-case. In fact, single-photon QKD has been so far hindered by the quality of solid-state emitters: low or fluctuating photon count rates, emission wavelengths far from the telecommunication bands, and collection setup instability.

In this work, we employ an advanced single-photon source based on QDs in photonic crystal waveguides[17] and a frequency conversion scheme based on difference-frequency generation (DFG)[18] to perform QKD between two districts in the Copenhagen metropolitan area. We use an 18-km-long link made of multiple segments of deployed dark fibre pairs, indicatively shown in Fig. 1. The fibres connect the sending station (Alice), located at the Niels Bohr Institute in Copenhagen, to the receiving station (Bob) at the Technical University of Denmark in Lyngby. We perform a complete QKD field-trial using single photons with the setup shown schematically in the lower panel of Fig. 1 and analyze the performance of the QD source in terms of security bounds, stability, and actual secret key generation rate.

RESULTS

Field trial apparatus

Figure 2a shows the schematic layout of the setup employed in the field trial experiment. The single-photon emitter used in this work is an Indium Arsenide (InAs) QD embedded in a suspended Gallium Arsenide (GaAs) membrane. A photonic crystal waveguide (PCW) is fabricated around the QD allowing near-unity coupling of the QD emission into the waveguide (see Methods for details). The

[1]Department of Electrical and Photonics Engineering, Technical University of Denmark, Ørsteds Pl., Kgs. Lyngby 2800, Denmark. [2]Center for Hybrid Quantum Networks (Hy-Q), Niels Bohr Institute, University of Copenhagen, Blegdamsvej 17, Copenhagen 2100, Denmark. [3]Lehrstuhl für Angewandte Festköperphysik, Ruhr-Universität Bochum, Universitätsstrasse 150, Bochum D-44780, Germany. [4]Department of Physics and Astronomy, University of Florence, Via Nello Carrara, Firenze 50019, Italy. [5]These authors contributed equally: Mujtaba Zahidy, Mikkel T. Mikkelsen. ✉email: dabac@fotonik.dtu.dk; midolo@nbi.ku.dk

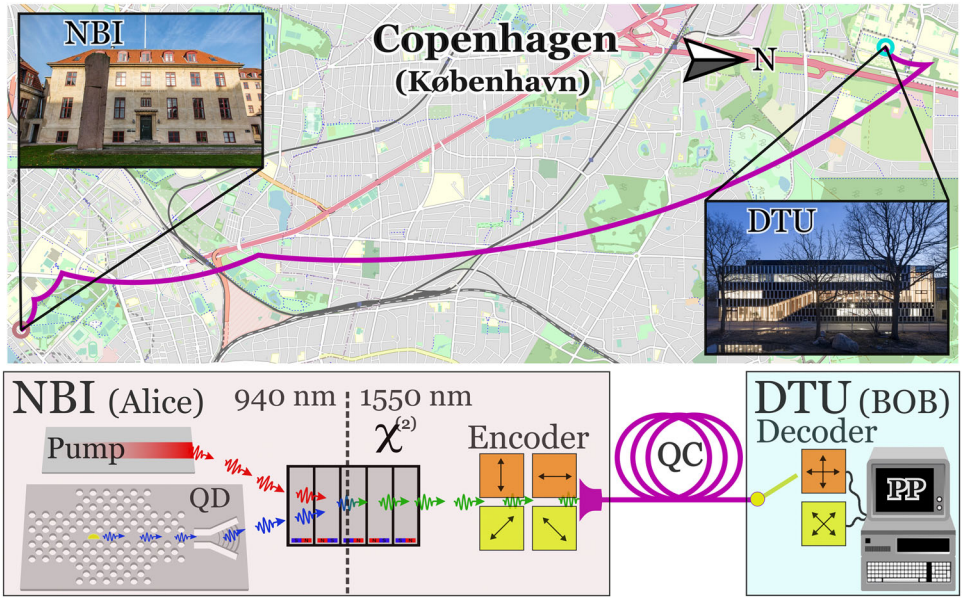

Fig. 1 Illustration of the channel and schematic of the experiment. Map showing the quantum channel connecting the Niels Bohr Institute (NBI) and the Technical University of Denmark (DTU), with a length of 18.1 km (9.6 dB of channel loss) and a simplistic schematic of the experiment from the quantum dot (QD) source through nonlinear down conversion to the telecom C-band ($\chi^{(2)}$), QKD encoder, quantum channel (QC) (the physical link), QKD decoder, and post-processing (PP).

sample is placed in a 1.6 K closed-cycle cryostat and single photons are collected via a high-efficiency focusing grating coupler using a microscope objective. A single QD transition at 942 nm is excited resonantly with a Ti:Sa mode-locked laser at a repetition rate of 72.6 MHz, resulting in 12 MHz count rate in the fibre (i.e. a source efficiency of $\eta_S = 16.5\%$). A scanning electron microscope (SEM) image of the device is shown in Fig. 2b.

To achieve low-loss transmission in fibres, the single photons are down-converted to the telecommunication C-band via DFG[18] in a periodically poled lithium niobate (PPLN) waveguide, as depicted in Fig. 2c. Using a pump laser at 2414 nm wavelength, the single photons are converted from 942 nm to 1545 nm with a $\simeq 50\%$ end-to-end conversion efficiency. Transport of photons from the single-photon source (located in a different lab) to the frequency conversion setup introduces an additional 29% loss. The down-converted source exhibits a low multi-photon contribution ($g^{(2)}(0) = (0.47 \pm 0.14)\%$), as verified by auto-correlation measurements performed on the down-converted photons and shown in Fig. 2d. A low multi-photon contribution is paramount in order to overcome the threat of photon-number splitting (PNS)-type attacks, and hence a significant parameter in the key distillation process.

The implemented QKD protocol is the 4-state polarization-based BB84[19], where photons are randomly modulated to one of the four polarizations forming the bases $X = \{|D\rangle, |A\rangle\}$ and $Z = \{|H\rangle, |V\rangle\}$ in the encoder. This is carried out with a phase modulator actively controlled by an arbitrary waveform generator (AWG). A 50:50 beamsplitter at the receiver redirects the incoming photons onto either of the two bases (X or Z), passively at random, upon detection. A master clock phase-locked to the excitation laser by a field programmable gate array (FPGA) is synchronizing the modulation and detection to the photon emission, the latter via an optical service channel parallel to the quantum channel (QC). Residual background noise in both the QC and the service channel is observed in the wavelength range 1550-1555 nm, which has been filtered out by tuning the single photon down-conversion process to channel 40 of the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) and by placing a dense wavelength division multiplexer (DWDM) filter before the state decoder. An overview of the setup is depicted in Fig. 2a while the performance is summarized in Table 1.

Field trial data acquisition

Data was acquired over two different days, referred to as Day 1 and Day 2, over a period of 17 and 30 consecutive hours, respectively. The quantum bit error rate (QBER) measured throughout the whole duration of the field trial is shown in Fig. 3a, for the X and Z basis, respectively (see Methods). The QBER remains stable throughout the duration of the experiment, especially on Day 2. Short temporary fluctuations in the QBER are observed for the Z bases on Day 1, which we attribute to the thermal instability of phase modulators in the state encoder in the early hours of the experiment and not to the QD source itself. Additionally, sporadic jumps in the value of QBERs are observed over short time intervals for both bases due to overshooting in the active compensation of polarization drifts (see Methods). In the analysis, we discard all data chunks with very high QBER caused by the polarization drift compensation.

The secret key is extracted according to a strict finite-size bound[20], with the secret key length given by

$$l_{\text{key}} = \lfloor n\mathcal{A}(1 - \mathrm{H}(\tilde{q}/\mathcal{A})) - \text{leak}_{\text{EC}} - \Delta - \text{leak}_{\text{EV}} \rfloor - v_{\text{auth}}, \quad (1)$$

where n is the number of sifted bits per block used for extracting the secret key bits. We use $n = 2 \cdot 10^5$ to reduce the impact of finite-size effects while maintaining reasonable computational costs and speed. H is the binary Shannon entropy. The factor $\mathcal{A} = 1 - p_{\text{m}}/p_{\text{det}}$ corresponds to the leaked information by possible multi-photon emissions[21,22] $p_{\text{m}} = g^{(2)}(0) \cdot (\eta_S \eta_E)^2/2$ is the multi-photon probability where η_S is the combined QD source, transport, and frequency conversion efficiency, and η_E is the encoder efficiency, while p_{det} is the detection probability. The upper-bound of the qubit error rate $\tilde{q}$ is used to account for finite sampling effects together with the finite size correction term Δ[20]. The terms leak_{EC} and leak_{EV} correspond to the information leakage during the information reconciliation and error verification, respectively. v_{auth} represents the key portion used for authenticating the classical communication during post-processing. An adequate description of the key-extraction

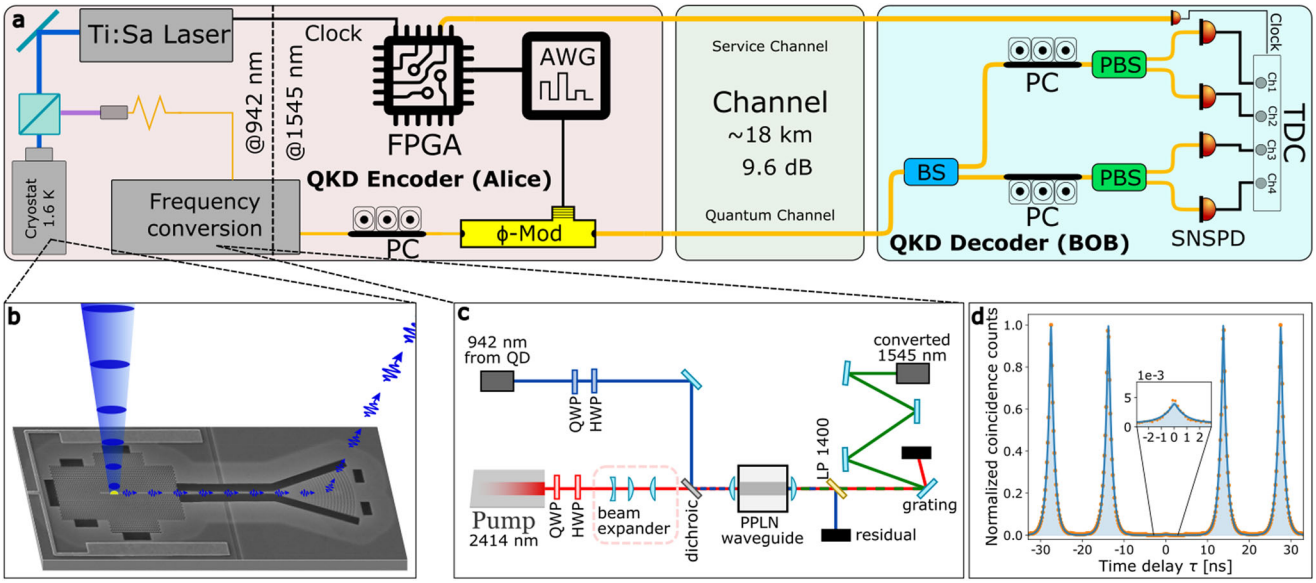

Fig. 2 Experimental layout of the QKD field-trial demonstrator. a Schematic overview of the employed QKD setup with Transmitter, Channel and Receiver. Yellow lines mark optical connections (fibres), while black lines are electronic connection (wires). Additionally, the QKD setup consists of a field programmable gate array (FPGA), an arbitrary waveform generator (AWG), a phase modulator (ϕ-mod), a beam-splitter (BS), two polarising beam-splitters (PBS), three polarization controllers (PC), four superconducting nanowire single-photon detectors (SNSPD) and a time-to-digital converter (TDC). **b** SEM picture of the nanophotonic structure featuring the QD (yellow annotation), annotated to visualize the single photon source operation with pulsed resonant excitation. **c** Frequency conversion setup including polarization control (half/quarter-waveplates (HWP/QWP)) and source and pump mode matching lenses. The periodically poled Lithium Niobate (PPLN) waveguide mediates the conversion. A long pass filter (LP) transmitting > 1400 nm wavelengths is followed by a grating that filters out residual 940 nm photons and the pump laser. **d** Auto-correlation measurement of the down-converted single photons, shown in orange, fitted with a double-sided exponential decay convoluted by the instrument response function modeled as a Gaussian distribution in blue yielding $g^{(2)}(0) = (0.47 \pm 0.14)\%$ and a QD lifetime of (867 ± 5) ps. Inset shows a zoom-in of the central peak.

Table 1. Overview of the experimental performance.

Parameter	Value
ν_S	72.6 MHz
η_{QD}	16.5%
η_T	71%
η_{FC}	50%
$g^{(2)}(0)$	$(0.47 \pm 0.14)\%$
η_E	55%
η_{QC}	10.9%
η_R	11.4%

Source rate (ν_S), QD source efficiency (η_{QD}) measured in fibre, transport efficiency (η_T) and frequency conversion efficiency (η_{FC}), second order correlation ($g^{(2)}$), encoder efficiency (η_E), quantum channel transmission(η_{QC}), and receiver efficiency (η_R) including the detection efficiency.

process is given in the Supplementary Note 2. Figure 3b shows the QBER and secret key rate (SKR) over the whole duration of data acquisition. On Day 1, we achieve the highest average SKR of 2.95 kbit/s. Notably, the bound used here allows for the empirical extraction of a usable secret key, accounting for finite-size effects that occur during the implementation of the post-processing. It is therefore significantly tighter compared to the estimates based on the asymptotic GLLP bound[22] for single photon sources, which is commonly used to report the SKR. While the QBER is higher during Day 1, the final secret key rate is higher compared to Day 2 due to an increased input rate of the unsifted key, see Table 2. Overall, 361 Mbit of usable secret key has been extracted during the field trial.

DISCUSSION

The ≈ 4% QBER measured during the two-day-long data acquisition of the experiment is attributed to two main factors, state preparation of the encoder and channel background noise observed in the C-band. To reduce the background noise, besides placing a DWDM filter, we temporally filtered the incoming photons in a 1 ns temporal filter. Nevertheless, we attribute ~ 1% induced QBER to the signal-to-noise ratio. This temporal filter width provides an acceptable trade-off between the accepted data to process and an increase in QBER. A comparison of the QBER measured in a back-to-back test with weak coherent pulses (WCP) suggests a possible improvement of the QBER by 2 − 2.5%, by improved stabilization of the encoder and the photon transmission line from frequency conversion to the state encoder. Furthermore, we observed 0.8 dB extra loss from day 1 to day 2 that we speculate is due to the out-coupling from the QD.

The secret key extraction is performed under the assumption that each pulse is made of pure single-photon states, which is a good approximation when exciting the QD with short resonant π-pulses[23]. The state generation rate can be effectively increased by pumping the QDs at a higher rate. The measured 0.867 ns lifetime of the QD employed in this work would allow to pump the QD above 0.2 GHz rate, which would readily correspond to a three-fold increase of the secret key generation rate. Moreover, Purcell enhancement of spontaneous emission, would open the door to even higher single-photon rates. QD lifetimes below 50 ps have been reported previously[24], which allow pumping the QD in the GHz regime. In combination with an optimized low-loss encoder and receiver, a key generation rate approaching the Mbit/s might be achievable on the field-trial channel, showing the great potential of current QD technology for applications that demand a high generation rate.

In Fig. 3c, we compare our results to previously reported QKD experiments (all performed in laboratory environment) using

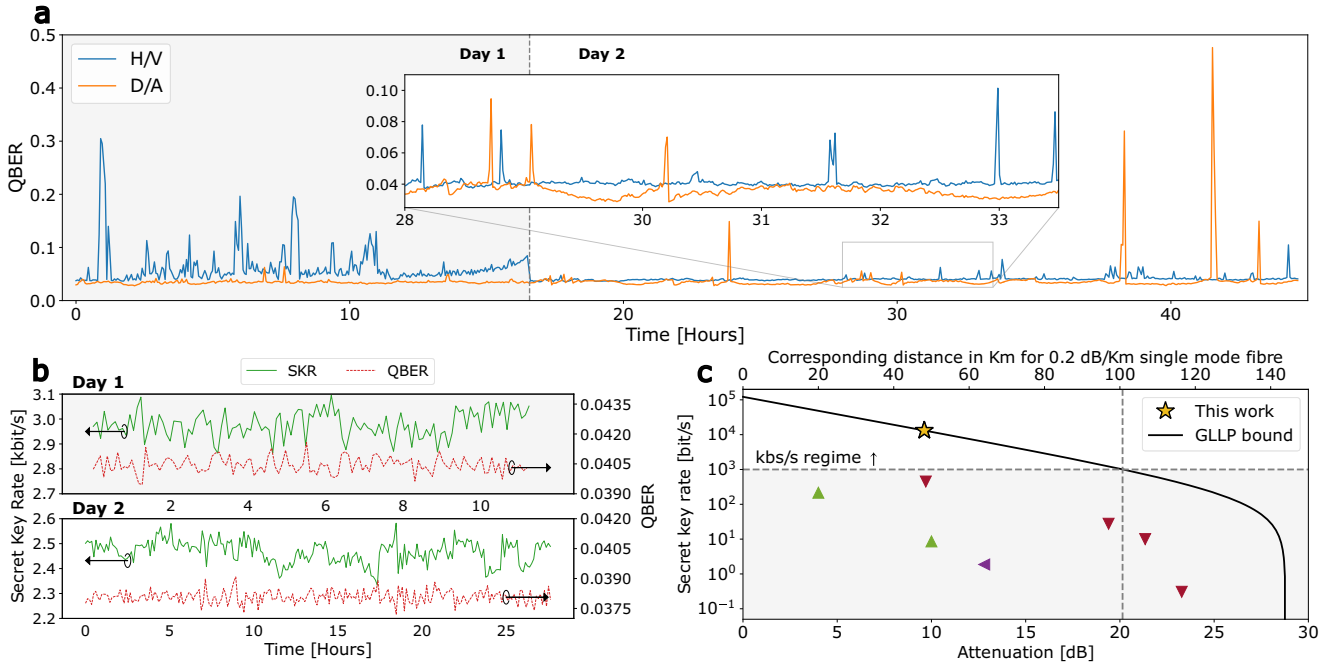

Fig. 3 Performance of the QKD field trial. a QBER for the X and Z basis measurement results during the field trial. Each data point in the figure/inset is the mean of 200/50 seconds, respectively. **b** The secret key rate (SKR) and QBER taken during the field trial. The upper and lower figures show the different days of data acquisition, respectively. Each data point represents the mean of 20 post-processing frames. **c** Comparison of the finite secret key rate of the experimental performance presented in this work based on the asymptotic GLLP bound[22]; commonly used for prepare and measure QKD bench marking. The secret key rate is evaluated for the best performance frame with 47.9 kbit/s raw key and 3.25% QBER and marked with a yellow star. Based on this performance the finite secret key rate is simulated in the asymptotic limit and shown with a black line. Triangles mark previous QKD lab-trials with single photon sources at telecom wavelength (◀ [43], ▲ [44], ▼ [45]), all estimated with GLLP-bound.

Table 2. Result overview.

Day	QBER	SKR [bits/s]	KR [kbit/s]	SK [Mbit]	Dur [h]
1	4.04%	2950	25.7	123	11.6
2	3.83%	2441	19.7	238	27.1

Mean final secret key rate (SKR), mean rate of unsifted key (KR), and total accumulated and usable secret key. Data was collected on two days with the respective running time (Dur).

deterministic single-photon sources in the C- or O-band. In those experiments, a full QKD protocol has been implemented, which allows for a fair comparison of the asymptotic key rates achievable. Several other single-photon QKD experiments (at different wavelengths or without encoding) have been reported[25–29] which cannot be directly compared to ours. A list of reported single-photon QKD experiments is given in the Supplementary Note 1. We achieve the highest asymptotic secret key rate reported so far for single-photon QKD, of up to 13.2 kbit/s at a channel loss of 9.6 dB, which for a 0.2 dB/km bare fibre loss would correspond to a distance of 48 km (yellow star in Fig. 3c). Notably, we still achieve kbit/s key rates, which would allow for real-time one time pad encryption of voice recordings[30], to about 100 km equivalent reach with the commonly used GLLP-bound[22].

The advancement in QDs which directly emit in C- or O- band will greatly improve the performance of the quantum communication, if brought on par with 930 nm sources in terms of brightness, while simultaneously eliminating the need for a frequency conversion setup. Such QDs were the subject of investigation recently[31,32] and promising results were achieved.

We have presented a QKD field trial with a near-deterministic single-photon source. We extract actual usable secret key frames and establish secret key rates in the C-band for single-photon sources to more than 2 kbit/s at ≈ 10 dB of loss. By demonstrating a stable and usable single-photon connection in a metropolitan environment, we pave the way towards realistic implementations of single-photon-based communication infrastrcuture, where deterministic and coherent QD-based single-photon sources constitute a mature resource for advanced applications, including device-independent QKD[33–35], one-way quantum repeaters[36] and, ultimately, the quantum internet[2].

METHODS

Single-photon source

The single-photon sources are fabricated on a GaAs membrane grown by molecular beam epitaxy on a (100) GaAs substrate. The 180-nm-thick membrane consists of a layer of self-assembled InAs QDs (density <10 μm^{-1}) grown in the middle of an ultra-thin *p-i-n* diode junction, to reduce charge noise and control the charge state while also enabling Stark tuning of the QD emission wavelength. The diode bias is controlled by a stable and low-noise voltage source. Additionally, a distributed Bragg reflector (AlAs/GaAs, 79/66 nm) is grown below the membrane to enhance the vertical collection of photons out of the chip. The photonic crystal waveguides are fabricated via electron-beam lithography and dry etching following the methods presented in[37], while electrical contacts to the diode are deposited via electron-beam evaporation and lift-off.

Setup

The state encoder is formed by an in-line one-pass polarization modulation[38,39] in which birefringence of a Titanium-diffused $LiNbO_3$ crystal [iXBlue, MPZ-LN-10] induces a relative phase(ϕ) between the two rectilinear components of the input diagonal

polarization. The scheme features low loss compared to other modulation techniques[40,41] as photons encounter only one insertion loss. Prior to the experiment, the phase modulator is left operating for 24 hours in order to reach thermal equilibrium with its environment.

A 4-level RF signal generated by a Siglent, SDG6052X AWG with levels $\{0, V_{\pi/2}, V_{\pi}, V_{3\pi/2}\}$, corresponding to an induced $\phi = \{0, \pi, \frac{\pi}{2}, \frac{3\pi}{2}\}$ relative phase shift, enables the preparation of states in the two bases {X} and {Z}. The X/Z ratio is decided according to the protocol, a one-to-one ratio has been deployed in this work.

The state encoder and the mode-locked laser are synchronized by first down-sampling the mode-locked laser clock and then triggering the AWG. A Cyclone V FPGA evaluation board provides a down-sampled clock at 120 kHz which is also transmitted through the service channel for synchronization. Upon triggering, the AWG bursts out a waveform to modulate 605 consecutive photons to one of the four polarization states chosen at random. The AWG repeats over the sequence for the duration of the data acquisition. A seamless update of the sequence requires more advanced electronics and is necessary to guarantee security, however, it does not affect the performance in terms of SKR and QBER. It should be noted that to guarantee the security of the implementation, the pseudo-random sequence of the states must be replaced with a truly random sequence generated with a quantum random number generator[42].

The receiver, see Fig. 2, is comprised of a 50:50 beam-splitter (BS) followed by two sets of polarization controllers and polarizing beam-splitters (PBS). The output port of the PBSs is connected to a superconducting nano-wire single photon detector (SNSPD). Each PBS is aligned to measure one of the bases {X} and {Z} through initial alignment with manual polarization controllers. Two HP 11896A motorized polarization controllers - not depicted in the figure - in line with the manual ones are executing an optimization algorithm based on coordinate-descent search which compensates for any polarization drift that has occurred in the quantum channel. This maintains the QBER below a certain threshold. The SNSPDs feature 33 ns of deadtime, 50 Hz dark count, and ≈ 83% detection efficiency. The detection events and their accurate timing is registered with a time-to-digital converter (TDC), from qutools, qutag standard, with 1 ps resolution for post-processing.

The transmitter and the receiver are connected with a pair of fiber channels of ≈ 18.1 km length, formed by 6 patches, and exhibit 9.6 dB of loss. The fibers transmit the quantum and clock signal. While running the protocol the basis sequence is also transmitted to the receiver for sifting and error estimation.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding authors upon reasonable request.

CODE AVAILABILITY

All codes used in this paper are available from the corresponding authors upon reasonable request.

Received: 29 August 2023; Accepted: 14 December 2023;
Published online: 02 January 2024

REFERENCES

1. Uppu, R., Midolo, L., Zhou, X., Carolan, J. & Lodahl, P. Quantum-dot-based deterministic photon–emitter interfaces for scalable photonic quantum technology. *Nat. Nanotechnol.* **16**, 1308–1317 (2021).
2. Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030 (2008).
3. Lu, C.-Y. & Pan, J.-W. Quantum-dot single-photon sources for the quantum internet. *Nat. Nanotechnol.* **16**, 1294–1296 (2021).
4. Hensen, B. et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682–686 (2015).
5. Basset, F. B. et al. Quantum key distribution with entangled photons generated on demand by a quantum dot. *Sci. Adv.* **7**, eabe6379 (2021).
6. Schimpf, C., Manna, S., da Silva, S. F. C., Aigner, M. & Rastelli, A. Entanglement-based quantum key distribution with a blinking-free quantum dot operated at a temperature up to 20K. *Adv. Photon.* **3**, 065001 (2021).
7. Schimpf, C. et al. Quantum cryptography with highly entangled photons from semiconductor quantum dots. *Sci. Adv.* **7**, eabe8905 (2021).
8. Gyger, S. et al. Metropolitan single-photon distribution at 1550 nm for random number generation. *Appl. Phys. Lett.* **121**, 194003 (2022).
9. Zhou, X., Zhai, L. & Liu, J. Epitaxial quantum dots: a semiconductor launchpad for photonic quantum technologies. *Photonics Insights* **1**, R07 (2023).
10. Vajner, D. A., Rickert, L., Gao, T., Kaymazlar, K. & Heindel, T. Quantum communication using semiconductor quantum dots. *Adv. Quantum Technol.* **5**, 2100116 (2022).
11. Heindel, T., Kim, J.-H., Gregersen, N., Rastelli, A. & Reitzenstein, S. Quantum dots for photonic quantum information technology. *Adv. Opt. Photon.* **15**, 613–738 (2023).
12. Liu, H. et al. Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km. *Phys. Rev. Lett.* **126**, 250502 (2021).
13. Bacco, D. et al. Field trial of a three-state quantum key distribution scheme in the florence metropolitan area. *EPJ Quantum Technol.* **6**, 5 (2019).
14. Ribezzo, D. et al. Deploying an inter-european quantum network. *Adv. Quantum Technol.* 2200061 https://onlinelibrary.wiley.com/doi/abs/10.1002/qute.202200061 (2022).
15. Liao, S.-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017).
16. Hwang, W.-Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
17. Uppu, R. et al. Scalable integrated single-photon source. *Sci. Adv.* **6**, eabc8268 (2020).
18. Da Lio, B. et al. A pure and indistinguishable single-photon source at telecommunication wavelength. *Adv. Quantum Technol.* **5**, 2200006 (2022).
19. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* **560**, 7–11 (2014). Theoretical Aspects of Quantum Cryptography - celebrating 30 years of BB84.
20. Cai, R. Y. Q. & Scarani, V. Finite-key analysis for practical implementations of quantum key distribution. *New J. Phys.* **11**, 045024 (2009).
21. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61**, 052304 (2000).
22. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Info. Comput.* **4**, 325–360 (2004).
23. Loredo, J. C. et al. Generation of non-classical light in a photon-number superposition. *Nat. Photonics* **13**, 803–808 (2019).
24. Tomm, N. et al. A bright and fast source of coherent single photons. *Nat. Nanotechnol.* **16**, 399–403 (2021).
25. Collins, R. J. et al. Quantum key distribution system in standard telecommunications fiber using a short wavelength single photon source. *J. Appl. Phys.* **107**, 073102 (2010).
26. Beveratos, A. et al. Single photon quantum cryptography. *Phys. Rev. Lett.* **89**, 187901 (2002).
27. Alléaume, R. et al. Experimental open-air quantum key distribution with a single-photon source. *New J. Phys.* **6**, 92–92 (2004).
28. Murtaza, G. et al. Efficient room-temperature molecular single-photon sources for quantum key distribution. *Opt. Express* **31**, 9437–9447 (2023).
29. Morrison, C. L. et al. Single-emitter quantum key distribution over 175 km of fibre with optimised finite key rates. *Nat Commun* **14**, 3573 (2023).
30. McCree, A. & Barnwell, T. A mixed excitation lpc vocoder model for low bit rate speech coding. *IEEE Transactions on Speech and Audio Processing* **3**, 242–250 (1995).
31. Müller, T. et al. A quantum light-emitting diode for the standard telecom window around 1550 nm. *Nat Commun* **9**, 862 (2018).
32. Lettner, T. et al. Strain-controlled quantum dot fine structure for entangled photon generation at 1550 nm. *Nano Lett.* **21**, 10501–10506 (2021).
33. Kołodyński, J. et al. Device-independent quantum key distribution with single-photon sources. *Quantum* **4**, 260 (2020).
34. González-Ruiz, E. M., Das, S. K., Lodahl, P. & Sørensen, A. S. Violation of bell's inequality with quantum-dot single-photon sources. *Phys. Rev. A* **106**, 012222 (2022).
35. González-Ruiz, E. M. et al. Device-independent quantum key distribution with realistic single-photon source implementations. In *Optica Quantum 2.0 Conference and Exhibition*, QM3B.3 (Optica Publishing Group, 2023). https://opg.optica.org/abstract.cfm?URI=QUANTUM-2023-QM3B.3
36. Borregaard, J. et al. One-way quantum repeater based on near-deterministic photon-emitter interfaces. *Phys. Rev. X* **10**, 021071 (2020).

37. Midolo, L., Pregnolato, T., Kiršanskė, G. & Stobbe, S. Soft-mask fabrication of gallium arsenide nanomembranes for integrated quantum photonics. *Nanotechnology* **26**, 484002 (2015).
38. Grünenfelder, F., Boaron, A., Rusca, D., Martin, A. & Zbinden, H. Simple and high-speed polarization-based qkd. *Appl. Phys. Lett.* **112**, 051108 (2018).
39. Jofre, M. et al. 100 mhz amplitude and polarization modulated optical source for free-space quantum key distribution at 850 nm. *Journal of Lightwave Technology* **28**, 2572–2578 (2010).
40. Lucio-Martinez, I., Chan, P., Mo, X., Hosier, S. & Tittel, W. Proof-of-concept of real-world quantum key distribution with quantum frames. *New J. Phys.* **11**, 095001 (2009).
41. Agnesi, C., Avesani, M., Stanco, A., Villoresi, P. & Vallone, G. All-fiber self-compensating polarization encoder for quantum key distribution. *Opt. Lett.* **44**, 2398–2401 (2019).
42. Zahidy, M. et al. Quantum randomness generation via orbital angular momentum modes crosstalk in a ring-core fiber. *AVS Quantum Sci.* **4**, 011402 (2022).
43. Intallura, P. M. et al. Quantum key distribution using a triggered quantum dot source emitting near 1.3μm. *Appl. Phys. Lett.* **91**, 161103 (2007).
44. Takemoto, K. et al. Transmission experiment of quantum keys over 50 km using high-performance quantum-dot single-photon source at 1.5 μm wavelength. *Appl. Phys. Express* **3**, 092802 (2010).
45. Takemoto, K. et al. Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors. *Sci Rep* **5**, 14383 (2015).

ACKNOWLEDGEMENTS

We acknowledge funding from: The Center of Excellence SPOC (ref DNRF123), Innovations fonden project Fire-Q (No. 9090-00031B), Danish National Research Foundation (Center of Excellence Hy-Q DNRF139), and Styrelsen for Forskning og Innovation (FI) (5072-00016B QUANTECH). L.M. acknowledges the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (Grant Agreement No. 949043, NANOMEQ). N.B., A.D.W. and A.L. acknowledge funding from the BMBF contract (No. 16KISQ009). D. B. acknowledges the programme Rita Levi Montalcini (PGR19GKW5T).

AUTHOR CONTRIBUTIONS

L.M., D.B., M. Z., and M.T.M. conceived the research idea and designed the experiment. M.Z, M.T.M., B.D.L., and M.K. performed the experiment. R.M, M.T.M, and M.Z. performed the data analysis. N.B., A.D.W., and A.L. performed epitaxial growth of the quantum dot. Y.W fabricated the single-photon source. M.G., S.F., P.L., L.K.O., D.B., and L.M. supervised the project. M.Z., M.T.M. and R.M. wrote the manuscript, all authors discussed and revised the manuscript and data.

COMPETING INTERESTS

Peter Lodahl is founder of the company Sparrow Quantum, which commercializes single-photon sources. The authors declare no other competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-023-00800-x.

Correspondence and requests for materials should be addressed to Davide Bacco or Leonardo Midolo.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.