Official journal of the CIOMP 2047-7538
www.nature.com/lsa

ARTICLE Open Access

High-rate intercity quantum key distribution with a semiconductor single-photon source

Jingzhong Yang[1], Zenghui Jiang[1], Frederik Benthin[1], Joscha Hanel[1], Tom Fandrich[1], Raphael Joos[2], Stephanie Bauer[2], Sascha Kolatschek[2], Ali Hreibi[3], Eddy Patrick Rugeramigabo[1], Michael Jetter[2], Simone Luca Portalupi[2], Michael Zopf[1,4], Peter Michler[2], Stefan Kück[3] and Fei Ding[1,4]✉

Abstract

Quantum key distribution (QKD) enables the transmission of information that is secure against general attacks by eavesdroppers. The use of on-demand quantum light sources in QKD protocols is expected to help improve security and maximum tolerable loss. Semiconductor quantum dots (QDs) are a promising building block for quantum communication applications because of the deterministic emission of single photons with high brightness and low multiphoton contribution. Here we report on the first intercity QKD experiment using a bright deterministic single photon source. A BB84 protocol based on polarisation encoding is realised using the high-rate single photons in the telecommunication C-band emitted from a semiconductor QD embedded in a circular Bragg grating structure. Utilising the 79 km long link with 25.49 dB loss (equivalent to 130 km for the direct-connected optical fibre) between the German cities of Hannover and Braunschweig, a record-high secret key bits per pulse of 4.8×10^{-5} with an average quantum bit error ratio of ~ 0.65% are demonstrated. An asymptotic maximum tolerable loss of 28.11 dB is found, corresponding to a length of 144 km of standard telecommunication fibre. Deterministic semiconductor sources therefore challenge state-of-the-art QKD protocols and have the potential to excel in measurement device independent protocols and quantum repeater applications.

Introduction

Realms of communication that transcend the limitations of traditional networks can be accessed by establishing a 'quantum internet'[1,2] through the distribution of quantum light states. Sharing quantum bits of information with distant nodes via optical fibre or free space (satellite) enables new applications such as quantum teleportation[3–5], quantum cloud computing[6,7] or quantum sensor networks[8,9]. A primary advantage of quantum communication lies in its ability to ensure unambiguous security for modern communication networks, a security that is increasingly threatened by the rapid advancement of quantum computing technologies[10–12]. Hence, Quantum Key Distribution (QKD) has attracted worldwide attention for its unique ability to provide security based on the principles of quantum mechanics[13], surpassing the capabilities of classical cryptography[14].

The QKD landscape has evolved significantly over the years, using a variety of protocols and spanning fibre networks[15,16] and satellite-to-ground free-space links[17,18]. Despite this progress, the establishment of large networks currently requires the use of intermediate 'trusted nodes'[19], which provide limited security that can only be fully restored by the implementation of quantum repeaters[20]. Furthermore, conventional quantum light sources based on weak laser pulses[21] or spontaneous parametric down-conversion[22] struggle with a delicate balance between brightness and multiphoton emissions to resist photon number splitting attacks. Decoy state QKD offers a potential solution[23], but at the cost of increased complexity and a penalty in the secret key rate (SKR)[19].

Semiconductor single photon sources (SPSs) hold immense potential in revolutionising large-scale

Correspondence: Fei Ding (fei.ding@fkp.uni-hannover.de)
[1]Institut für Festkörperphysik, Leibniz Universität Hannover, Appelstraße 2, 30167 Hannover, Germany
[2]Institut für Halbleiteroptik und Funktionelle Grenzflächen, Center for Integrated Quantum Science and Technology (IQST) and SCoPE, University of Stuttgart, Stuttgart, Germany
Full list of author information is available at the end of the article

quantum communication. Semiconductor quantum dots (QDs) are capable of emitting indistinguishable single photons on demand with unprecedented efficiency and purity[24,25], offering strong advantages for QKD[25,26]. In particular, for measurement-device-independent (MDI) QKD[27], which requires high visibility of Hong-Ou-Mandel interference between two independent single-photon sources, a scheme involving QDs[28] can significantly improve the key rate[29]. QDs also offer great prospects for the realisation of quantum repeaters, as they allow for inherent storage of quantum information[30] and can emit photonic cluster states[31]. The success of these QDs in the wavelength range between 780 nm and 900 nm is expected to be built on by the continued development of QDs emitting at the telecom bands. Quantum communication experiments utilising QDs have demonstrated their ability to link university campuses and metropolitan areas[32–37]. However, the lack of bright single-photon signals in the telecommunication bands have hindered progress beyond these boundaries to intercity distances. Nevertheless, a recent breakthrough[38] has enabled the emission of bright single photons with high emission rates, thanks to Purcell enhancement, from a QD device directly in the telecommunication C-band and therefore expanding the horizons of quantum communication.

Here we report on the first intercity QKD experiments with a deterministic single-photon source. A semiconductor quantum dot embedded in a circular Bragg grating (CBG) efficiently emitting single photons of high purity in the telecommunication C-band is employed in conjunction with polarisation encoding in the standard BB84 protocol[39]. The photons are routed on a 79 km long deployed fibre between the German cities of Hannover and Braunschweig, featuring a loss of (25.49 ± 0.02) dB corresponding to a standard telecom fibre length of 130.32 km. We verify that high-rate secret key transmission and a low quantum bit error ratio (QBER) of ~0.65% are ensured for 35 h. An average secret key bits (SKBs) per pulse of more than 2×10^{-5} in the finite-key regime can be reached over an acquisition time of 30 min. Positive key rates are determined achievable for distances up to 144 km corresponding to 28.11 dB loss in the laboratory, highlighting the competitiveness of semiconductor SPSs for quantum communication applications.

Results

Overview of the experiment

The intercity experiment is performed in the German federal state of Niedersachsen, in which a deployed fibre of ~79 km length connects the Leibniz University of Hannover (LUH) and Physikalisch-Technische Bundesanstalt (PTB) Braunschweig, as depicted in Fig. 1a. Alice, located at the LUH, statically prepares polarisation-encoded single photons as $\{|H\rangle, |V\rangle, |D\rangle, |A\rangle\}$. Bob, located at the PTB, contains a passive polarisation decoder to measure the polarisation states on two balanced conjugate bases. We denote the rectilinear $\{|H\rangle, |V\rangle\}$ and diagonal $\{|D\rangle, |A\rangle\}$ bases as Z and X bases, respectively.

In the transmitter of Alice, a pulsed laser (PriTel, InC.) at a wavelength of 1529.8 nm and with an adjustable clock rate (CR) is employed to excite the p-shell of the positively charged trion transition of the InAs/InGaAs/GaAs QD mounted in a 4 K closed-cycle helium gas cryostat [Fig. 1(b)]. The QD, embedded in a CBG photonic structure, emits circularly polarised single photons at a wavelength of 1555.9 nm with high brightness. The Purcell effect of the CBG cavity reduces the QD's emission lifetime to (592.5 ± 1.8) ps (see details in the Materials and Methods section), theoretically allowing for an increase of the excitation CR up to GHz. One linear component of the photon emissions from the QD is particularly favoured in brightness due to the asymmetry of the CBG cavity. The super-conducting nanowire detector (SNSPD) detects an average photon count rate of (3.591 ± 0.003) MHz from the transmitter, while the QD is excited at its saturation power under the CR of 76 MHz (see also "Materials and methods" section). The average number of photons per pulse[40] for the linearly polarised fraction of the single photon emission at the first lens is calculated to be $\langle n \rangle = (0.138 \pm 0.015)$, taking into account the efficiencies of the transmitter and detector (see Table 1). It is worth noting that the value of $\langle n \rangle$ differs slightly from the reported extraction efficiency[38]. This is because the polariser filters out the single photons with linear polarisation that are not favoured by the CBG cavity. Additionally, a raw blinking-corrected $g^{(2)}(0)$ value of (2.43 ± 0.02)% is measured without any data post-processing (see more details in the "Materials and methods" section).

To first study all of the QKD performance for different transmission distances in the lab, encoded single photons are sent through one or multiple standard telecom fibre spools (ITU-T G.652.D) of 40 km length each. The average loss of $l = (0.1956 \pm 0.0026)\,\mathrm{dB\,km^{-1}}$ per spool is calibrated in the laboratory, taking into account the insertion loss (see Supplementary Information Sec. II.A.1). So as to then realise the intercity QKD experiment over the deployed fibre, a reference signal for local synchronisation is required. Therefore, the single photon signals are transmitted over the intercity link together with attenuated pulses from the excitation laser. On the receiver side, these two signals are de-multiplexed and the single photon states are decoded. SNSPDs are used for detecting the single photons and the reference laser signal,

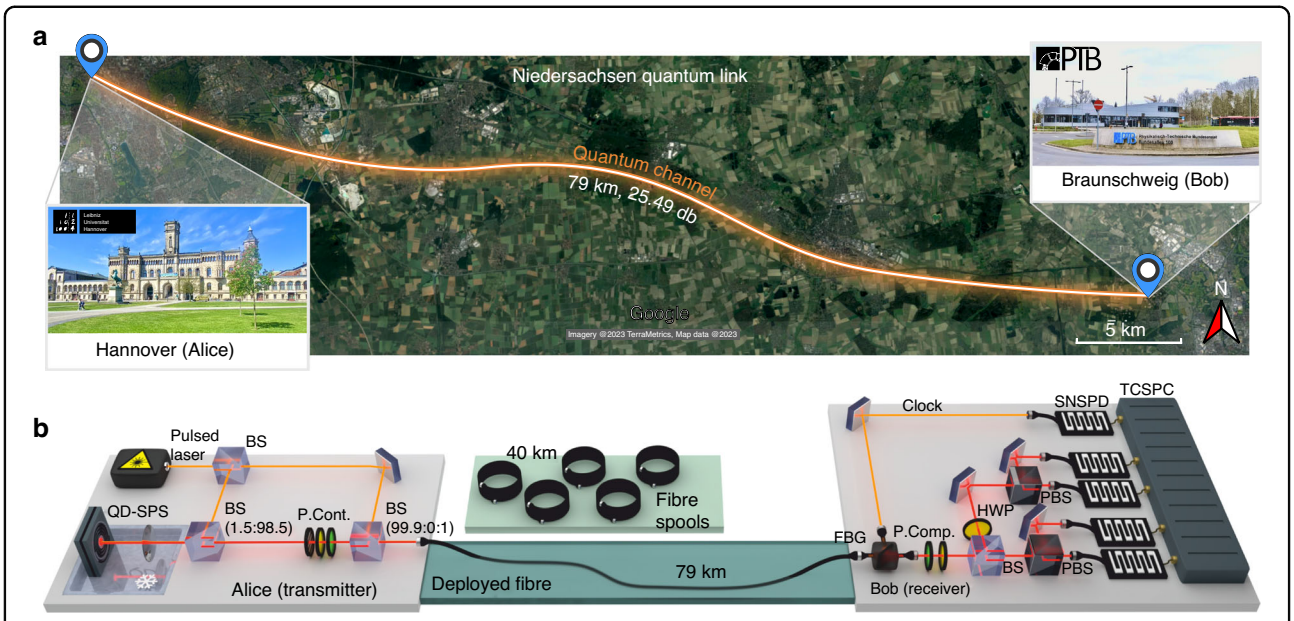

Fig. 1 Overview of the intercity QKD experiments on the 'Niedersachsen quantum link' using single photons from a semiconductor quantum dot (QD). a Distribution of quantum bits between Hannover (Alice) and Braunschweig (Bob) over 79 km of deployed fibre with a total loss of 25.49 dB. Map data from Google (©2023 Google). **b** Sketch of the experimental setup. The QD-based SPS of the transmitter is mounted in a cryostat and excited by a pulsed laser at different clock rates (CRs) (76 MHz, 228 MHz, 608 MHz, and 1063 MHz). The emitted single photons are collected by an aspherical lens with a numerical aperture of 0.7. State encoding is performed by a polarisation control module (P. Cont.) comprising a polariser, a half-wave plate (HWP) and a quarter-wave plate (QWP). The single-photon and excitation laser signals are then together coupled into either a sequence of fibre spools or the deployed fibre. In the receiver module, a fibre Bragg grating (FBG) demultiplexes the single photon and laser signals by wavelength. An electronically controlled polarisation compensation (P. Comp.) module with QWP and HWP counteracts polarisation fluctuations in the quantum channels by monitoring and minimising the quantum bit error ratio (QBER). A non-polarising 50:50 beam splitter (BS) then acts as a random selector of the decoding basis, with rectilinear projection in the transmitted path using a polarisation beam splitter (PBS), and diagonal projection in the reflected path using a HWP at an angle of 22.5° followed by a PBS. The four single-photon signals and the laser signal are detected at superconducting nanowire single-photon detectors (SNSPDs) and the timing events recorded with a time-correlated single-photon counting (TCSPC) unit

which thereby provides a timing reference to the single photon detection events.

One of the figure of merits used to assess the performance of QKD is the SKBs per pulse. In our work, we study this in both the asymptotic and finite-key regimes. For the asymptotic case[40–42],

$$S_A = p_{sift}\left\{\underline{p}_c^{(1)}[1-h(\bar{e}_1)] - f_{EC}p_c h(e_{tot})\right\} \quad (1)$$

where $p_{sift} = p_X^2 + (1-p_X)^2$ is the sifting ratio assuming both QKD bases are used for the key generation; p_X is the bias of the projection basis ($p_X = 0.5$ in our case); $\underline{p}_c^{(1)}$ corresponds to the lower bound of detected events for the single-photon state; $h(\cdot)$ is the binary Shannon entropy function; $\bar{e}_1$ denotes the upper bound of the QBER for single-photon states and e_{tot} is the total QBER for all photon number states. For convenience, we assume balanced efficiencies of the receiver ports and SNSPD channels for each polarisation basis. f_{EC} describes the error correction inefficiency of the algorithm, p_c indicates the total detection probability of the photon number states[43,44].

For the case of a finite block size of the keys, we evaluate the SKBs per pulse using the multiplicative Chernoff bound[45,46],

$$S_F = \frac{\underline{n}_{R,nmp}^{X,Z}}{Rt}\left[1 - h(\bar{\phi}^Z) - \lambda_{EC} - \log_2\frac{2}{\epsilon_{cor}} - 2\log_2\frac{1}{2\epsilon_{PA}}\right] \quad (2)$$

Here, R is the CR, t is the acquisition time, $\underline{n}_{R,nmp}^{X,Z}$ the lower bound of non-multiphoton emissions in the receiver module for X and Z bases, $\bar{\phi}^Z$ the upper bound of the phase error rate, λ_{EC} the lower bound of information leakage[47] and ϵ_{cor} are the bits used for verification during the error correction process. ϵ_{PA} is the failure probability of privacy amplification. Table 1 presents both the performance of our QD-based SPS and security parameters of our QKD system, in which we

Table 1 In-lab QKD system and security parameters

Description	Parameter	Value
Average photon number per pulse	$\langle n \rangle$	0.138
Clock rate	R	228 MHz
Second-order correlation	$g^{(2)}(0)$	2.43%
Transmitter efficiency	η_T	0.464
Receiver efficiency	η_R	0.740
System misalignment probability	p_{mis}	2.57×10^{-4}
Detector efficiency	η_D	0.740
Dark count probability	p_{dc}	8.74×10^{-7}
Dead time	τ_{dt}	35.865 ns
Averaged fibre-spool loss	l	0.1956 dB km^{-1}
Field-installed fibre loss	L	25.49 dB
Parameter estimation failure probability	ϵ_{PE}	$^{2\times10^{-10}}/_{3}$
Error correction failure probability	ϵ_{EC}	$^{10^{-10}}/_{6}$
Privacy amplification failure probability	ϵ_{PA}	$^{10^{-10}}/_{6}$
Error verification failure probability	ϵ_{cor}	10^{-15}
Error correction leakage	f_{EC}	1.16
	λ_{EC}	SI[a]

[a]see Supplementary Information Sec. VI.E

consider ϵ-secret $\epsilon_{sec} = 10^{-10}$ and ϵ-correct $\epsilon_{cor} = 10^{-15}$ for reaching ϵ_{qkd}-secure ($\epsilon_{qkd} \geq \epsilon_{sec} + \epsilon_{cor}$)[48].

Source performance for in-lab QKD

We now investigate the performance of the semiconductor SPS for the in-lab QKD experiment. In Fig. 2a, the SKBs per pulse is shown in dependence of excitation power when the QD is excited under CR of 76 MHz. The average photon number per pulse $\langle n \rangle$ and blinking-corrected $g^{(2)}(0)$ are measured and fed into Eqs. (1) and (2) (see more details in Supplementary Information Sec. VI), assuming a received block size of $n_R^Z = 10^8$ bits for the Z-basis in the finite-key regime. Both the asymptotic and finite SKBs per pulse start to drop above the excitation power of (2.98 ± 0.15) μW because of a decreasing source brightness due to the damping of Rabi-oscillation under p-shell excitation[49].

To assess the performance of semiconductor SPS-based QKD for long-distance transmission, we study the SKBs per pulse over varying transmission loss in the laboratory, as shown in Fig. 2(b). The QD is pumped under a CR of 228 MHz with the excitation power ~3 times in case of 76 MHz and the emitted single photon signal is coupled into the fibre spools mentioned above. To emulate distances of 20 km and 60 km, we added a variable fibre optical attenuator with a fixed loss of (4.0 ± 0.4) dB. To obtain the data points, the truth table and second-order

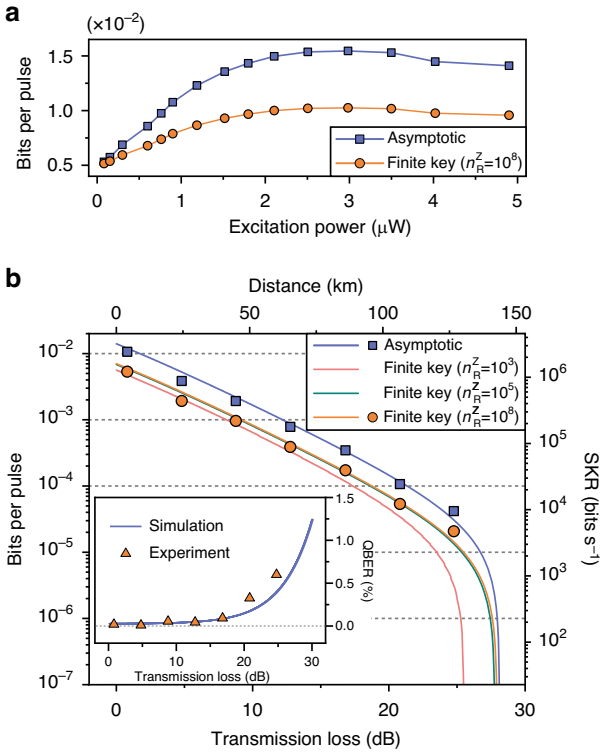

Fig. 2 In-lab characterisation of the QD-based single-photon source and the experimental setup. a Secret key per clock pulse as a function of excitation laser power in the asymptotic and finite-key regime. **b** Secret key bits (SKBs) per pulse as a function of the transmission loss. The maximum tolerable losses (MTLs) for the asymptotic case and finite-key block cases with different block sizes of $n_R^Z = 10^3, 10^5, 10^8$ are extracted to be 28.11, 25.51, 27.78 and 27.95 dB, respectively. The inset shows the measured and simulated QBER as a function of transmission loss with the dashed grey line indicating the QBER at zero

auto-correlation measurements are recorded based on the statically encoded polarisation qubits at each transmission loss, in order to extract the average photon number per pulse ($\langle n \rangle$), quantum bit error ratio (QBER) (e_{tot}), and single photon purity (see Supplementary Information Sec. VI.B). The solid lines in Fig. 2b illustrate the simulation of QBER and SKBs per pulse by employing the values of parameters measured from the QD (Table 1). With an increased block size n_R^Z in the finite-key regime, the simulated maximum tolerable loss (MTL) approaches the one for the asymptotic regime at 28.11 dB, corresponding to a transmission distance of 141.05 km in a standard telecommunication fibre. In this experiment, the MTL for both the asymptotic and finite-key block cases are limited by the blinking-corrected $g^2(0)$, since the multi-photon emission probability is detrimental for generating high SKRs with single-photon states in the high-loss regime. The SKR and MTL can be improved by employing adequate pre-attenuation[46] and employing time gating on the

Table 2 Averaged QBER, A-SKR and F-SKR $\left(n_R^Z = 10^8\right)$ measured under different CRs for the fibre spool distance of 80 km

CR (MHz)	QBER (%)	A-SKR (kbits s^{-1})	F-SKR (kbits s^{-1})
76	0.344	28.12	14.19
228	0.099	67.97	33.88
608	0.089	151.57	75.93
1063	0.064	216.74	108.36

histograms of second-order correlation and truth table during post-processing[44,50].

One outstanding feature of SPS is the on-demand photon emission, allowing ultra-high photon count rates with GHz CRs[51,52]. To explore the CR-dependent SKR capabilities of our system, we perform the truth table measurements using 80 km of fibre spool and different excitation laser CRs. In our experiment, the pump power approximately linearly increases with the CRs based on the saturation power at 76 MHz (Fig. 2a). However, this is not the case for the 1063 MHz because the excitation CR approaches the radiative decay rate of the emitter, as can be seen in the lifetime histograms discussed in the following section. The QBER, Asymptotic-SKR (A-SKR), and Finite-SKR (F-SKR) are extracted from the truth tables as shown in Table 2. The QBER decreases with increasing CR due to the lower dark count contributions resulting from smaller integration windows. Although the SKR is limited by the QD lifetime and detector dead times, the achievable high SKRs of > 100 kbits s^{-1} would enable QKD secured live video conferences encrypted with an one-time-pad (OTP) encryption[53–55].

Intercity QKD over the deployed fibre

Now, the intercity QKD experiments are performed by sending telecom C-band single photons emitted by the semiconductor QD SPS from Hannover to Braunschweig via the 'Niedersachsen Quantum Link'. In the optics laboratory in Braunschweig (Bob), we employ a second SNSPD system (Single Quantum company) to detect the single-photon signals. The detection system's performance in terms of average efficiency, dark count rate has been given in the Section III of the Supplementary Information. Time traces of the single photon emission under different CRs are obtained by correlating the reference laser and single photon signals (Fig. 3a). For CRs ranging from 76 MHz up to 1.06 GHz the single photon pulse trains are clearly identified. Still, at 608 MHz and above the peaks start to overlap, implying a saturation in the achievable photon counts for high CRs. The Purcell factor of the device can be improved through optimisation of the structure, such as more accurate positioning of QDs[56] in the cavity centre or modifications in the photonic structure[57]. Alternatively, it can be improved by placing it in an open and tunable micro-cavity within the cryostat[58]. These methods reduce the radiative lifetime of the QDs towards a higher excitation CR. Figure 3(b) represents a continuous second-order auto-correlation measurement of up to 12 h at the deployed fibre end in Braunschweig. The blinking-corrected $g^{(2)}(0)$ plotted over the measurement time reveals high and stable single-photon purity which is important for long-term communication applications. The single-photon purity is preserved at > 85% for the first three CRs and reduces to ~81.5% for 1063 MHz due to coincidence events involving photons from adjacent pulse trains, as visible from the right inset graph. It has to be noted that no temporal filtering has been applied here, which could be used to increase the single-photon purity at higher CRs at the expense of the number of coincidences. The higher blinking-corrected $g^{(2)}(0)$ under 76 MHz in comparison to 228 MHz is due to the contribution of dark counts due to a wider temporal coincidence window (the inverse CR).

To evaluate the performance of real-world QKD over the fibre link, the truth table is measured by accumulating the coincidence histograms between the reference laser and QD signals from the receiver ports, while four polarisation states are statically encoded by the transmitter. An automatic polarisation compensation algorithm at the receiver is developed by minimising the locally measured QBER, in order to counteract polarisation fluctuations of the fibre link (see Supplementary Information Sec. II.B). Figure 3c illustrates the normalised truth table, obtained with a CR of 228 MHz and a measurement time of more than 6 h for each encoded state. The diagonal histograms in the table correspond to the sifted keys that are usable for error correction and privacy amplification, and the grey histograms illustrate the discarded keys by basis sifting. A fidelity of 99.6% is extracted from the projection on the ideal truth table with flawless key decryption. By now measuring the time-dependent truth table, eventually the A-SKR, F-SKR, and QBER time traces are obtained and displayed in Fig. 3d. In addition to extracting the raw time tags, temporal filtering with a 2D-filter is applied by monitoring the $g^{(2)}$ and truth table histograms in order to maximise the SKRs and minimise the QBERs[50] (see detail in Supplementary Information Sec. VII). The fluctuation of the SKR and QBER while the $|H\rangle$ state is projected onto Z basis, results from the sensitive fibre coupling of $|H\rangle$ signals on the receiver module. Nevertheless, the dynamic temporal filter reduces the blinking-corrected $g^{(2)}(0)$ from ~6.24% to ~4.75% with the averaged window size ~3.56 ns in the full duration of Fig. 3d.

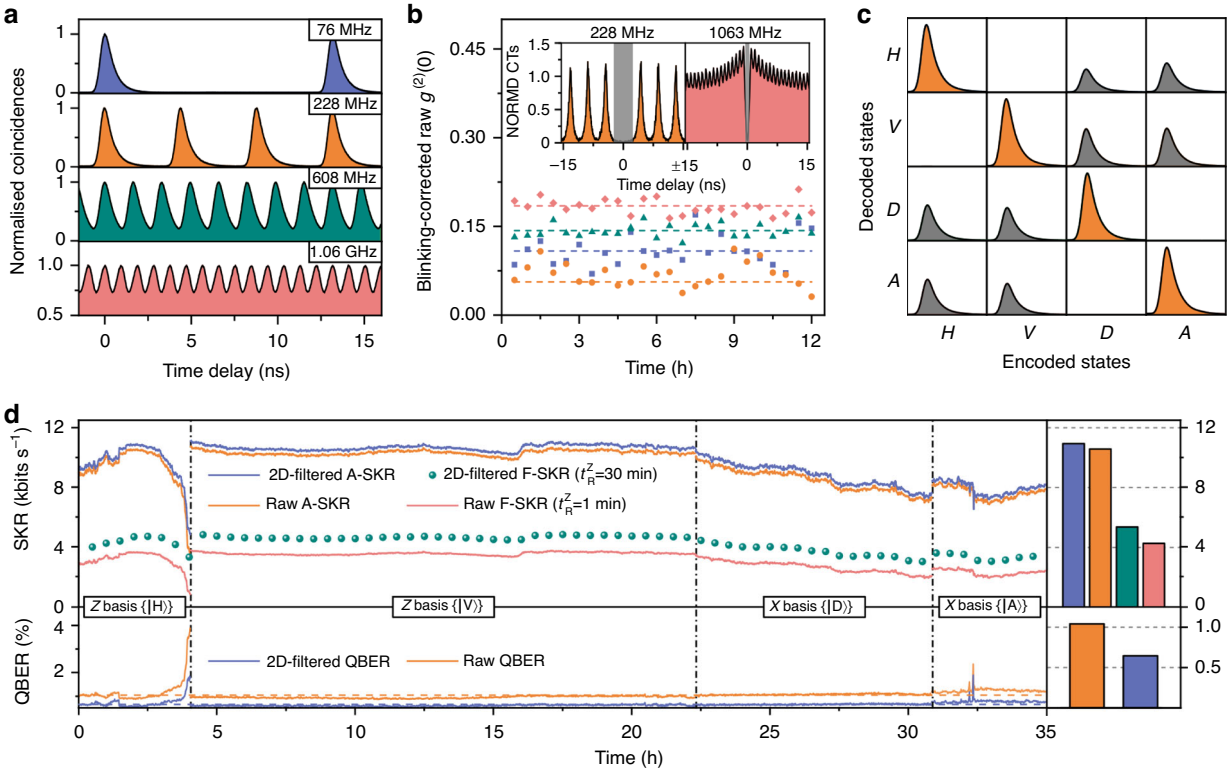

Fig. 3 Intercity quantum key distribution using telecom C-band single photons from a semiconductor source, transmitted over the deployed fibre with a loss of 25.49 dB. a Time-resolved QD emission for different CRs. **b** Blinking-corrected, second-order auto-correlation at zero time delay $g^{(2)}(0)$ as a function of measurement time recorded in Braunschweig for the CRs ■ 76 MHz, ● 228 MHz, ▲ 608 MHz and ♦ 1.06 GHz. Each data point represents 0.5 h of measurement time, and no time gating was applied. The dashed lines show the average $g^{(2)}(0)$ over the whole measurement with values of 0.108 ± 0.005, 0.056 ± 0.002, 0.143 ± 0.002 and 0.185 ± 0.002. Insets: normalised (NORMD) second-order correlation histograms for the CRs of 228 MHz and 1064 MHz. **c** Truth table of the polarisation encoded BB84 protocol. The correlation histograms in each column are normalised by the decoded coincidences resulting from the encoded states (diagonal histograms in the table). **d** A-SKR, F-SKR and QBER over time for different encoding bases $\{X, Z\}$ at a fixed CR of 228 MHz. Each data point in the solid lines represents the average of 1 min. The colour-coded inset graphs on the right-hand side shows the average asymptotic, finite SKR, as well as QBER over the 35 h- key transmission time with and without the 2-D temporal filter. The SKBs per pulse are evaluated to be $(4.797 \pm 0.011) \times 10^{-5}$, $(4.464 \pm 0.011) \times 10^{-5}$, $(2.349 \pm 0.031) \times 10^{-5}$ and $(1.867 \pm 0.005) \times 10^{-5}$. The average QBER (dashed line) decreases from (1.041 ± 0.004)% to (0.646 ± 0.002)%

The averaged QBER down to (0.646 ± 0.002)% is therefore the lowest value achieved over such a transmission loss so far in QKDs with SPSs, by excluding the ~1.17 kHz noise rate from the raw key rate of ~103.16 kHz. This leads to efficient extraction of secret keys from the X basis, according to the keys sifted by the Z basis for phase error rate estimation. The average A-SKR and F-SKR are then obtained to be (10.93 ± 1.19) kbits s^{-1} and (5.35 ± 0.58) kbits s^{-1}, respectively. Such SKRs allow for, e.g., live encryption of speech between the two cities via the shared keys[59]. Slow polarisation fluctuations are observed on the fibre link (see Supplementary Information Sec. II.A.3), allowing for effective polarisation drift compensation. For networks in harsh environments where fibres are, e.g., aerially deployed, the time-phase coding protocol[60] or time-bin qubits[61–64] could be employed with our source, offering less sensitivity to polarisation fluctuations.

Comparison with state-of-the-art

Here we present a comparative analysis involving other SPS-based QKD experiments and the high-rate decoy-state BB84 protocol in the telecom C-band as depicted in Fig. 4. Recent QKD implementations have reported two noteworthy approaches, both utilising SPSs. The first involves QDs in photonic crystal waveguides[37], while the second employs a QD contained in an oxide-apertured micropillar[46]. Both SPS were not directly emitting into the telecom C-band, and therefore frequency conversion techniques were employed, introducing additional losses. In contrast, our implementation features a highly efficient source emitting at the telecom C-band, and both simulation and experimental data reveal a substantial increase in the SKBs per pulse for data transmission.

Furthermore, we illustrate the asymptotic SKBs per pulse from other QKDs based on telecom single photon emitters[50,60,65–67]. Notably, the achieved finite SKBs per

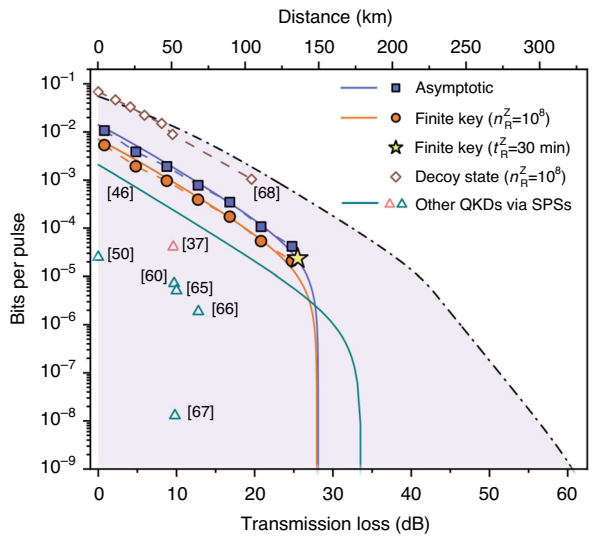

Fig. 4 Comparison of the SKBs per pulse with other QKD experiments. The in-lab SKBs per pulse (■, ●) and the field-based SKBs per pulse in the finite-key regime (★) surpass previous realisations based on single-photon sources with photons in the telecom C-band and approach state-of-the-art decoy state QKD. The triangles (△, △) show the QKDs with SPSs based via deployed fibre and fibre spools, respectively. The solid lines represent simulated SKBs per pulse using the experimental parameters. The dashed, black line represents the SKBs per pulse that is achievable with experimentally feasible source optimisations. Corresponding distance is calculated for 0.1956 dB km^{-1} standard telecommunication fibre

pulse over the intercity fibre testbed, denoted by a star, also represents the highest SKR achieved to date in SPS-based QKD under 228 MHz CR. In addition, our results approach the current record of finite SKBs per pulse achieved by decoy-state BB84 with weak coherent pulses in laboratory settings[68].

The demonstrated QKD performance can be further enhanced through optimisations of source quality, detection systems, and protocols. The shaded purple region, delineated by a black dash line, represents an emulation of the achievable finite SKBs per pulse ($n_R^Z = 10^8$) by considering experimentally accessible parameters, such as an improved source efficiency[58], single-photon purity[69], and system dark counts[16]. Regarding the protocol, optimal pre-attenuation of single-photon counts[46] and an asymmetric projection basis choice[70] for each individual transmission loss result in higher SKR and MTL without compromising security. A complete, real-time QKD system based on SPSs is considered, which incorporates a high-speed modulation of polarisation states encoded via quantum random numbers. The secret key is then extracted after error correction and privacy amplification. The additional losses and errors introduced by the additional electro-optical modulator are quantified by using a pre-defined random sequence to encode the polarisation of laser light (see Supplementary Information Sec. VIII). By incorporating these feasible primary parameters (see Supplementary Information Sec. VI.F), we anticipate achieving a MTL of ~61 dB, corresponding to a distance of 311.86 km in the finite-key regime. Furthermore, a SKR approaching 1 MHz under a transmission loss of ~25 dB is attainable assuming a CR of 1 GHz, a configuration well-suited for distributed secure storage[71]. For a more comprehensive comparison of our findings with other QKD protocols, refer to the Supplementary Information Sec. IX.

Discussion

In conclusion, the first intercity QKD experiments using a deterministic telecom SPS has been demonstrated. This advancement was made possible by harnessing single-photon emissions from a semiconductor QD embedded in a CBG structure, emitting within the telecom C-band and excitation rates up to the GHz range. SKRs have been investigated for different excitation powers and transmission losses under both asymptotic and finite-key scenarios. The measurements and simulations indicate an asymptotic MTL of 28.11 dB, corresponding to 143.71 km channel length in repeaterless quantum communication with standard fibre-optic networks. The experiment spanned a deployed optical fibre link of approximately 79 km and a total loss of 25.49 dB, over which high-rate secret key transmission over an extended period of 35 h is obtained. The average QBER is impressively low at around 0.65%, highlighting the robustness and reliability of the system. Comparative analysis with existing QKD systems involving SPS reveals that the SKR achieved in this work goes beyond all current SPS-based implementations. Even without further optimisation of the source and setup performance it approaches the levels attained by established decoy state QKD protocols based on weak coherent pulses. This outcome underscores the viability of seamlessly integrating semiconductor single-photon sources into realistic, large-scale and high-capacity quantum communication networks. Moreover, semiconductor QDs, acting as high-speed and deterministic single-photon emitters, hold promising implications for MDI-QKD and may serve as enablers for quantum repeater based star-like networks.

Materials and methods

Source characteristics

The average photon number per pulse of the linear component of the circularly polarised light from the device is determined using the SNSPD. The p-shell of the QD's trion state was saturably pumped by a pulsed laser at a clock rate (CR) of 76 MHz. The measurement of single-photon count from the transmitter's fibre is conducted

over a duration of 1 min (see Fig. S8 in Supplementary Information IV.A). The average photon count μ is calibrated at 3.591 MHz with a mean uncertainty of $^{\sigma}/_{\sqrt{N}} =$ 0.03 MHz, where σ and N represent the standard deviation and the number of data points, respectively. Accounting for the optical transmitter efficiency $\eta_T = (46.4 \pm 3.4)\%$, SNSPD detection efficiency $\eta_D = (74.0 \pm 6.0)\%$, and CR of 76 MHz, the average number of photons per pulse for the linearly polarised single photons is calibrated to be $\langle n \rangle = (0.138 \pm 0.015)$.

In our experiments, we excited the quantum dot in a quasi-resonant manner. The exciton is initially excited to the p-shell of the QD. Subsequently, it decays to the s-shell and, thereafter to the ground state by emitting a single photon. Hence to fit the lifetime, we assume, that a decay model for a three-level system is sufficiently accurate (see Fig. S9 in Supplementary Information Sec. IV.B). These then lead to the following identity, which is used to describe the population in the s-shell:

$$f(t) = a_0 \cdot \frac{T_s}{T_p - T_s} \cdot \left[\exp\left(-\frac{t - t_0}{T_p} \right) - \exp\left(-\frac{t - t_0}{T_s} \right) \right] \tag{3}$$

$$g(t) = \frac{1}{\sigma\sqrt{2\pi}} \cdot \exp\left(\frac{-t^2}{2\sigma^2} \right) \tag{4}$$

$$N_s(t) = (f * g)(t) \tag{5}$$

In order to account for the time jitter of the detector and the mode shape of the laser pulse, we employ least-square iterative re-convolution with the instrument response function, which is fitted with a Gaussian function (Eq. (4)). The lifetimes of T_p and T_s are extracted as (149.3 ± 1.0) ps and (443.20 ± 1.58) ps using Eq. (5), yielding the total lifetime of (592.5 ± 1.8) ps with the cascade process.

In SPS-based QKD, the average photon number per pulse and single-photon purity are two essential parameters that must be considered in the QKD algorithm to calculate the secret key rate and the maximum tolerated loss. For the non-blinking SPS, the single-photon purity is typically assessed as $\left[1 - g^{(2)}(0)\right]$[44]. However, the regular definition of $g^{(2)}(0)$ with blinking effect will be higher than the non-blinking $g^{(2)}(0)$, and this results in the underestimation of the single photon purity with $\left[1 - g^{(2)}(0)\right]$. To analyse the asymptotic and finite secret key rates in our experiment, we employed the blinking-corrected $g^{(2)}(0)$[36]. We begin by integrating the raw second-order auto-correlation histogram with a temporal bin size of approximately 4.38 ns (the inverted value of the 228 MHz pulsed-CR). The raw $g^{(2)}(0)$ value without blinking correction and temporal filtering on the background is $(2.95 \pm 0.02)\%$. To correct the blinking, we apply the blinking fitting function by calculating the ratio between the measured data and fitted value[36]. The normalised second-order auto-correlation after the blinking correction is then obtained, from which we extract the blinking-corrected $g^{(2)}(0) = (2.43 \pm 0.02)\%$ (see more details in Supplementary Information Sec. IV.C).

Experimental setups

The experimental setups includes the transmitter, fibre spools, receiver, and the SNSPD (see Fig. S1 in Supplementary Information Sec. I). In the transmitter, the clock variable pulsed fibre laser is coupled into free space to excite the QD after passing through a beam splitter (Altechna company) with a splitting ratio of (R:T=98.5:1.5). The Attodry1100 system is equipped with a Thorlabs aspheric lens (C330TMD-C) with a numerical aperture of 0.7 to collected the single photons from the device. Thorlabs polariser (LPNIR050-MP2), zero-order half-waveplate (WPH05M-1550), and quarter-waveplate (WPQ05M-1550) are employed to purify and encode the polarisation states, respectively. The Thorlabs electronic stages (K10CR1/M) control these components. The encoded single photon qubits are coupled into Corning SMF-28® Ultra fibre spools, each spanning 40 km. The receiver utilises a fibre-based Bragg grating (1560 nm half-wave CWDM) to split the reference laser and single-photon signals. The single photons, which are encoded, are detected by the SNSPDs (Single Quantum company) after passing through a 50:50 beam splitter (10B20NP.31) and two plate polarising beam splitters (PBSW-1550). Finally, the photon arrival times are registered by the timetagger (Time Tagger Ultra from Swabian Instrument company). More details about the efficiencies of the transmitter and receiver are shown in the section IA and IB of the Supplementary Information.

Acknowledgements

We thank J. Wang, C. Nawrath, M. Auer, T. van Leent, and H. Weinfurter for fruitful discussions, R. Guan for helping with the optical setups, and J. Wang for the electronics control of the system. We thank J. Kronjäger, A.K. Kniggendorf, and A. Kuhl for efficiently organising the deployed fibre infra-structure. We would also like to thank the companies Single Quantum, Quantum Optics Jena, and PriTel Inc. for their continued and timely support. The authors gratefully acknowledge the funding by the German Federal Ministry of Education and Research (BMBF) within the project QR.X (16KISQ013 and 16KISQ015), SQuaD (16KISQ117) and SemIQON (13N16291), the European Research Council (QD-NOMS GA715770, MiNet GA101043851), European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 899814 (Qurope), EMPIR programme co-financed by the Participating States and from the European Union's Horizon 2020 research and innovation programme (20FUN05 SEQUME), the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) within the project InterSync (GZ: INST 187/880-1 AOBJ: 683478), and under Germany's Excellence Strategy (EXC-2123) Quantum Frontiers (390837967), and Flexible Funds programme by Leibniz University Hannover (51410122).

Author details
[1]Institut für Festkörperphysik, Leibniz Universität Hannover, Appelstraße 2, 30167 Hannover, Germany. [2]Institut für Halbleiteroptik und Funktionelle Grenzflächen, Center for Integrated Quantum Science and Technology (IQST) and SCoPE, University of Stuttgart, Stuttgart, Germany. [3]Physikalisch-Technische Bundesanstalt, Braunschweig, Germany. [4]Laboratorium für Nano- und Quantenengineering, Leibniz Universität Hannover, Schneiderberg 39, 30167 Hannover, Germany

Author contributions
J. Yang and R. Joos implemented the optical characterisation of the sample. J. Yang, Z. Jiang, F. Benthin and J. Hanel, A. Hreibi and M. Zopf carried out the QKD experiment. S. Bauer, S. Kolatschek, and M. Jetter designed and fabricated the sample. T. Fandrich, J. Hanel, J. Yang, F. Benthin and Z. Jiang performed the data analysis and the interpretation of the results. J. Yang wrote the manuscript with the help from M. Zopf, F. Ding, E. P. Rugeramigabo, S.L. Portalupi, P. Michler, and the other co-authors. F. Ding, P. Michler, and S. Kück conceived and supervised the project.

Funding
Open Access funding enabled and organized by Projekt DEAL.

Data availability
The data that support the plots within this paper and other findings of this study are available from the corresponding author upon reasonable request.

Conflict of interest
Fei Ding serves as an Editor for the Journal. No other author has reported any competing interests.

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41377-024-01488-0.

Received: 11 April 2024 Accepted: 16 May 2024
Published online: 02 July 2024

References

1. Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: a vision for the road ahead. *Science* **362**, eaam9288 (2018).
2. Gyongyosi, L. & Imre, S. Advances in the quantum internet. *Commun. ACM* **65**, 52–63 (2022).
3. Bennett, C. H. et al. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.* **70**, 1895–1899 (1993).
4. Boschi, D., Branca, S., Martini, F. D., Hardy, L. & Popescu, S. Experimental realization of teleporting an unknown pure quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.* **80**, 1121–1125 (1998).
5. Bouwmeester, D. et al. Experimental quantum teleportation. *Nature* **390**, 575–579 (1997).
6. Soeparno, H. & Perbangsa, A. S. Cloud quantum computing concept and development: a systematic literature review. *Proc. Comput. Sci.* **179**, 944–954 (2021).
7. Taleb, N. & Mohamed, E. A. Cloud computing trends: a literature review. *Acad. J. Interdiscip. Stud.* **9**, 91 (2020).
8. Qian, T., Bringewatt, J., Boettcher, I., Bienias, P. & Gorshkov, A. V. Optimal measurement of field properties with quantum sensor networks. *Phys. Rev. A* **103**, l030601 (2021).
9. Ge, W., Jacobs, K., Eldredge, Z., Gorshkov, A. V. & Foss-Feig, M. Distributed quantum metrology with linear networks and separable inputs. *Phys. Rev. Lett.* **121**, 043604 (2018).
10. Aaronson, S. & Chen, L. Complexity-theoretic foundations of quantum supremacy experiments. *arXiv* https://doi.org/10.48550/arXiv.1612.05903 (2017).
11. Preskill, J. Quantum computing in the nisq era and beyond. *Quantum* **2**, 79 (2018).
12. Zhong, H.-S. et al. Quantum computational advantage using photons. *Science* **370**, 1460–1463 (2020).
13. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **8**, 595–604 (2014).
14. Rivest, R. L., Shamir, A. & Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**, 120–126 (1978).
15. Chen, J.-P. et al. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. *Nat. Photon.* **15**, 570–575 (2021).
16. Liu, Y. et al. Experimental twin-field quantum key distribution over 1000 km fiber distance. *Phys. Rev. Lett.* **130**, 210801 (2023).
17. Bedington, R., Arrazola, J. M. & Ling, A. Progress in satellite quantum key distribution. *npj Quant. Inf.* **3**, 30 (2017).
18. Lu, C.-Y., Cao, Y., Peng, C.-Z. & Pan, J.-W. Micius quantum experiments in space. *Rev. Mod. Phys.* **94**, 035001 (2022).
19. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
20. Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932–5935 (1998).
21. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
22. Schneeloch, J. et al. Introduction to the absolute brightness and number statistics in spontaneous parametric down-conversion. *J. Opt.* **21**, 043501 (2019).
23. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
24. Lu, C.-Y. & Pan, J.-W. Quantum-dot single-photon sources for the quantum internet. *Nat. Nanotechnol.* **16**, 1294–1296 (2021).
25. Vajner, D. A., Rickert, L., Gao, T., Kaymazlar, K. & Heindel, T. Quantum communication using semiconductor quantum dots. *Adv. Quant. Technol.* **5**, 2100116 (2022).
26. Couteau, C. et al. Applications of single photons to quantum communication and computing. *Nat. Rev. Phys.* **5**, 326–338 (2023).
27. Ferreira da Silva, T. et al. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88**, 052303 (2013).
28. Owen, K. A. Towards mdi qkd using quantum dot single photon sources. MSc thesis https://prism.ucalgary.ca/items/0332ba90-c08e-4737-828d-332dfc1d02fd (2021).
29. Zhou, Y.-H. et al. Measurement-device-independent quantum key distribution via quantum blockade. *Sci. Rep.* **8**, 4115 (2018).
30. Zaporski, L. et al. Ideal refocusing of an optically active spin qubit under strong hyperfine interactions. *Nat. Nanotechnol.* **18**, 257–263 (2023).
31. Schwartz, I. et al. Deterministic generation of a cluster state of entangled photons. *Science* **354**, 434–437 (2016).
32. Alléaume, R. et al. Experimental open-air quantum key distribution with a single-photon source. *N. J. Phys.* **6**, 92–92 (2004).
33. Rau, M. et al. Free space quantum key distribution over 500 meters using electrically driven quantum dot single-photon sources—a proof of principle experiment. *N. J. Phys.* **16**, 043003 (2014).
34. Xiang, Z.-H. et al. Long-term transmission of entangled photons from a single quantum dot over deployed fiber. *Sci. Rep.* **9**, 4111 (2019).
35. Basset, F. B. et al. Quantum key distribution with entangled photons generated on demand by a quantum dot. *Sci. Adv.* **7**, eabe6379 (2021).
36. Schimpf, C. et al. Quantum cryptography with highly entangled photons from semiconductor quantum dots. *Sci. Adv.* **7**, eabe8905 (2021).
37. Zahidy, M. et al. Quantum key distribution using deterministic single-photon sources over a field-installed fibre link. *npj Quant. Inf.* **10**, 2 (2023).
38. Nawrath, C. et al. Bright source of purcell-enhanced, triggered, single photons in the telecom c-band. *Adv. Quant. Technol.* **6**, 2300111 (2023).
39. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).
40. Waks, E., Santori, C. & Yamamoto, Y. Security aspects of quantum key distribution with sub-poisson light. *Phys. Rev. A* **66**, 042315 (2002).
41. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput.* **4**, 325–360 (2004).
42. Cai, R. Y. Q. & Scarani, V. Finite-key analysis for practical implementations of quantum key distribution. *N. J. Phys.* **11**, 045024 (2009).
43. Bozzio, M. et al. Enhancing quantum cryptography with quantum dot single-photon sources. *npj Quant. Inf.* **8**, 104 (2022).
44. Vyvlecka, M. et al. Robust excitation of c-band quantum dots for enhanced quantum communication. *Appl. Phys. Lett.* **123**, 174001 (2023).
45. Yin, H.-L. et al. Tight security bounds for decoy-state quantum key distribution. *Sci. Rep.* **10**, 14312 (2020).

46. 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).
47. Tomamichel, M., Martinez-Mateo, J., Pacher, C. & Elkouss, D. Fundamental finite key limits for one-way information reconciliation in quantum key distribution. *Quant. Inf. Process.* **16**, 280 (2017).
48. Bunandar, D., Govia, L. C. G., Krovi, H. & Englund, D. Numerical finite-key analysis of quantum key distribution. *npj Quant. Inf.* **6**, 104 (2020).
49. Ester, P. et al. p-shell rabi-flopping and single photon emission in an InGaAs/GaAs quantum dot. *Phys. E: Low.-Dimens. Syst. Nanostruct.* **40**, 2004–2006 (2008).
50. Gao, T. et al. A quantum key distribution testbed using a plug&play telecom-wavelength single-photon source. *Appl. Phys. Rev.* **9**, 011412 (2022).
51. Schlehahn, A. et al. An electrically driven cavity-enhanced source of indistinguishable photons with 61% overall efficiency. *APL Photon.* **1**, 011301 (2016).
52. Shooter, G. et al. 1ghz clocked distribution of electrically generated entangled photon pairs. *Opt. Express* **28**, 36838–36848 (2020).
53. Sasaki, M. et al. Field test of quantum key distribution in the tokyo QKD network. *Opt. Express* **19**, 10387–10409 (2011).
54. Liao, S.-K. et al. Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.* **120**, 030501 (2018).
55. Zhu, D. et al. A hybrid encryption scheme for quantum secure video conferencing combined with blockchain. *Mathematics* **10**, 3037 (2022).
56. Rickert, L., Kupko, T., Rodt, S., Reitzenstein, S. & Heindel, T. Optimized designs for telecom-wavelength quantum light sources based on hybrid circular bragg gratings. *Opt. Express* **27**, 36824–36837 (2019).
57. Ma, C. et al. Circular photonic crystal grating design for charge-tunable quantum light sources in the telecom c-band. *Opt. Express* **32**, 14789–14800 (2024).
58. Tomm, N. et al. A bright and fast source of coherent single photons. *Nat. Nanotechnol.* **16**, 399–403 (2021).
59. McCree, A. & Barnwell, T. A mixed excitation LPC vocoder model for low bit rate speech coding. *IEEE Trans. Speech Audio Process.* **3**, 242–250 (1995).
60. 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).
61. Jayakumar, H. et al. Time-bin entangled photons from a quantum dot. *Nat. Commun.* **5**, 4251 (2014).
62. Huber, T. et al. Coherence and degree of time-bin entanglement from quantum dots. *Phys. Rev. B* **93**, 201301 (2016).
63. Anderson, M. et al. Gigahertz-clocked teleportation of time-bin qubits with a quantum dot in the telecommunication c band. *Phys. Rev. Appl.* **13**, 054052 (2020).
64. Ginés, L. et al. Time-bin entangled photon pairs from quantum dots embedded in a self-aligned cavity. *Opt. Express* **29**, 4174–4180 (2021).
65. 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).
66. Intallura, P. M. et al. Quantum key distribution using a triggered quantum dot source emitting near 1.3μm. *Appl. Phys. Lett.* **91**, 161103 (2007).
67. Soujaeff, A. et al. Quantum key distribution at 1550 nm using a pulse heralded single photon source. *Opt. Express* **15**, 726–734 (2007).
68. Li, W. et al. High-rate quantum key distribution exceeding 110 mb s–1. *Nat. Photon.* **17**, 416–421 (2023).
69. Schweickert, L. et al. On-demand generation of background-free single photons from a solid-state source. *Appl. Phys. Lett.* **112**, 093106 (2018).
70. Lo, H.-K., Chau, H. F. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.* **18**, 133–165 (2004).
71. Sasaki, M. Quantum networks: where should we be heading? *Quant. Sci. Technol.* **2**, 020501 (2017).