nature communications

Article

https://doi.org/10.1038/s41467-023-39219-5

Single-emitter quantum key distribution over 175 km of fibre with optimised finite key rates

Received: 7 September 2022

Accepted: 5 June 2023

Published online: 16 June 2023

Check for updates

Christopher L. Morrison[1], Roberto G. Pousa[2], Francesco Graffitti[1], Zhe Xian Koong[1], Peter Barrow[1], Nick G. Stoltz[3], Dirk Bouwmeester[4,5], John Jeffers[2], Daniel K. L. Oi[2], Brian D. Gerardot[1] & Alessandro Fedrizzi[1]

Quantum key distribution with solid-state single-photon emitters is gaining traction due to their rapidly improving performance and compatibility with future quantum networks. Here we emulate a quantum key distribution scheme with quantum-dot-generated single photons frequency-converted to 1550 nm, achieving count rates of 1.6 MHz with $g^{(2)}(0) = 3.6\%$ and asymptotic positive key rates over 175 km of telecom fibre. We show that the commonly used finite-key analysis for non-decoy state QKD drastically overestimates secure key acquisition times due to overly loose bounds on statistical fluctuations. Using the tighter multiplicative Chernoff bound to constrain the estimated finite key parameters, we reduce the required number of received signals by a factor 10^8. The resulting finite key rate approaches the asymptotic limit at all achievable distances in acquisition times of one hour, and at 100 km we generate finite keys at 13 kbps for one minute of acquisition. This result is an important step towards long-distance single-emitter quantum networking.

Future quantum networks will require bright low-noise sources of single photons to enable applications including secure communication and distributed quantum computing[1]. There is a range of promising platforms for such a source, including quantum dots, molecules, quantum emitters in two-dimensional materials such as WSe_2 and hBN, and colour centres in wide band-gap materials such as diamond and SiC. Comparing these platforms for single-photon emitters, quantum dots (QDs) have demonstrated the highest count rates with the lowest multiphoton emission probability[2–4].

Fibre-based QKD requires single-photons at 1550 nm where loss in fibre is lowest. This can be realised with QDs in two ways, fabricating the QD to emit directly at 1550 nm or using quantum frequency-conversion to shift the wavelength of a QD which emits at shorter wavelengths to 1550 nm. The best available QDs in all relevant metrics emit at shorter wavelengths[2–4], although recent improvements have been made with C-band emitters in terms of brightness and multi-photon noise but not coherence[5]. Quantum frequency-conversion has been shown to be a viable route to realise a bright, coherent telecom QD single-photon source with low multiphoton noise, leveraging the performance of shorter wavelength QDs[6–8].

In this work, we demonstrate Bennett-Brassard '84 (BB84) QKD[9] using a bright frequency-converted QD source over optical fibre. In the asymptotic case the source outperforms previous demonstrations of prepare-and-measure QKD with single-photon emitters in terms of achievable key rate and maximum tolerable loss thanks to the brightness and low $g^{(2)}(0)$ of our source, see Table 1. In the composable security framework, we use improved analytical bounds for the random sampling without replacement problem related to the phase

[1]Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, UK. [2]SUPA Department of Physics, University of Strathclyde, Glasgow G4 0NG, UK. [3]Materials Department, University of California, Santa Barbara, CA 93106, USA. [4]Huygens-Kamerlingh Onnes Laboratory, Leiden University, P.O. Box 9504, 2300 RA Leiden, Netherlands. [5]Department of Physics, University of California, Santa Barbara, CA 93106, USA. e-mail: a.fedrizzi@hw.ac.uk

error rate and the multiplicative Chernoff bound that has been proven to be a tighter finite key bound in other contexts[10]. These bounds are used to calculate the fluctuations between expected and observed values.

The finite key treatment implemented in this work reduces the number of signals Bob must receive to approach the asymptotic case from 10^{15} to 10^{7} compared with widely used previous single-photon source QKD analyses. Equivalently, the integration time required to approach the asymptotic case is reduced from 10^{4} years to just one hour.

Results

Experimental setup

The experimental setup including single-photon source, communication channel and receiver is shown in Fig. 1. The quantum light source consists of an InGaAs/GaAs quantum dot inside an oxide-apertured micropillar[11] emitting photons at 940 nm. The QD is excited using a dark-field confocal microscope; single photons are collected in a cross-polarised scheme with 10^{7} suppression of the excitation laser. The QD is operated under pulsed quasi-resonant excitation using the third order cavity mode detuned by 440 GHz from the QD emission. This quasi-resonant excitation has strongly damped photon-number coherence compared to resonant excitation of the source[6], this allows the output photon number states to be treated as mixed[12] with no inter-pulse coherence. Femtosecond pulses from a Ti:Sapphire laser are stretched to 30 ps using a 4f Fourier pulse shaper and temporally multiplexed up to 160.7 MHz. We measure ≈5 MHz count rate with a $g^{(2)}(0) = 0.019(1)$ directly from the QD. The single-photon emission is converted to 1550 nm in a difference frequency generation (DFG) process in a 48 mm periodically-poled lithium niobate (ppLN) waveguide pumped by a 2400 nm continuous-wave laser. The internal conversion efficiency of the DFG process is 57%. Further details on the source can be found in ref. 6.

The four BB84 polarisation states $\{H,V,D,A\}$ are encoded using a motorised half-wave plate. Photons are then transmitted through the quantum channel consisting of SMF-28 fibre spools with an average propagation loss of 0.1904 dB/km including connectors. The fibre is housed in an insulating box to reduce temperature fluctuations, which keeps the fibre-induced polarisation rotation stable over the typical acquisition time of 30 min per polarisation state.

The BB84 receiver consists of a 50/50 fibre beam-splitter followed by two polarising beam splitters and in-fibre polarisation controllers to project into the H/V and D/A basis respectively. Photons are detected with superconducting nanowire single-photon detectors (SNSPDs).

The average transmittivity of the four arms of the receiver is 87% including relative efficiency of each detector measured by comparing the count rate observed on each detector with a reference parametric down-conversion source. The SNSPDs are biased to have an average dark count rate of 11.5 Hz at the cost of 5-10% of the peak efficiency. The detectors are time gated around the arrival time of the signal photons to reduce the effect of dark counts (see Fig. 2), the average time gate across all distances is 3.19 ns. This gives a dark count probability per pulse of $p_{dc} = 3.67 \times 10^{-8}$.

Table 1 | Comparison of other QKD demonstrations based on single-photon emitters

Reference	AKR at 0 km (kbps)	Maximum tolerable loss (dB)
This work	689	33.3
This work with active encoding[a]	258	34.4
QD[34]	4	23
QD[17]	2	23
QD[35]	25	28
Molecule[36]	500	22
2D Material[37]	0.24	21
2D Material[38]	30	23

For the purposes of comparison, the asymptotic key rate has been calculated with $p_{sift} = \frac{1}{2}$ and with no additional source attenuation. Refs. 34,37 include active switching of the encoded state, all other demonstrations use static encoding. A thorough review of QKD with QDs can be found in ref. 39.

[a]Prediction based on 3 dB loss and 2% polarisation encoding error typical with fibre-based electro-optic modulators.

Asymptotic key rate

We send each of the BB84 states $\{H, V, D, A\}$ in turn and record at least 5×10^{6} detected events for each state for seven distances between 0-175 km. The probability that a given round registers in one of Bob's detectors, p_{click}, is estimated as the ratio of detected events to the number of clock pulses from the Ti:Sapphire which are recorded over the integration period. For convenience, we assume equal probabilities for both bases, i.e. $p_{dc} \equiv p^{X}_{dc} \equiv p^{Z}_{dc}$ and $p_{\text{click}} \equiv p^{X}_{\text{click}} \equiv p^{Z}_{\text{click}}$. We measure a count rate of 1.6 MHz in Bob's receiver at zero distance. This gives a mean photon number of $\langle n \rangle = 0.0142$ injected into the communication channel backing out the known receiver transmission, the relative efficiency on average due to the measured losses of each detector (≈87%) and the estimated quantum efficiency of the detectors (≈75%).

The quantum bit error rate (QBER) $e_{X/Z}$, in the X or Z basis is calculated by comparing the ratio of detected events for the state orthogonal to Alice's encoded state to the total number of detected

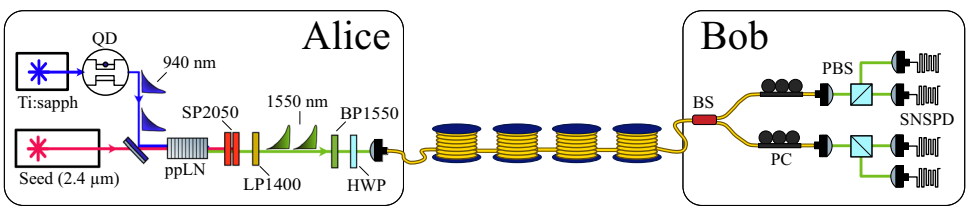

Fig. 1 | Experimental setup of Alice's single-photon source and Bob's passive BB84 receiver. The QD is excited at 160 MHz by temporally multiplexing an 80 MHz pulse train from a Ti:Sapphire laser. The 940 nm single photons are combined with a 2.4 μm seed laser and converted to 1550 nm in a ppLN ridge waveguide designed to be single-mode at 1550 nm. The seed beam is removed with short-pass filters at 2050 nm (SP2050) before the telecom photons are isolated with a long pass filter at 1400 nm (LP1400) and a bandpass filter at 1550 nm (BP1550). The transmission channel consists of spools of fibre of various length which are joined using physical contact connectors for the different distances measured in Fig. 2. Bob's receiver passively chooses between X and Z basis measurements using a 50/50 fibre beam-splitter (BS). Projections are made using polarising beam-splitter (PBS) cubes and in-fibre polarisation controllers (PC) to align the measurement basis.

https://doi.org/10.1038/s41467-023-39219-5

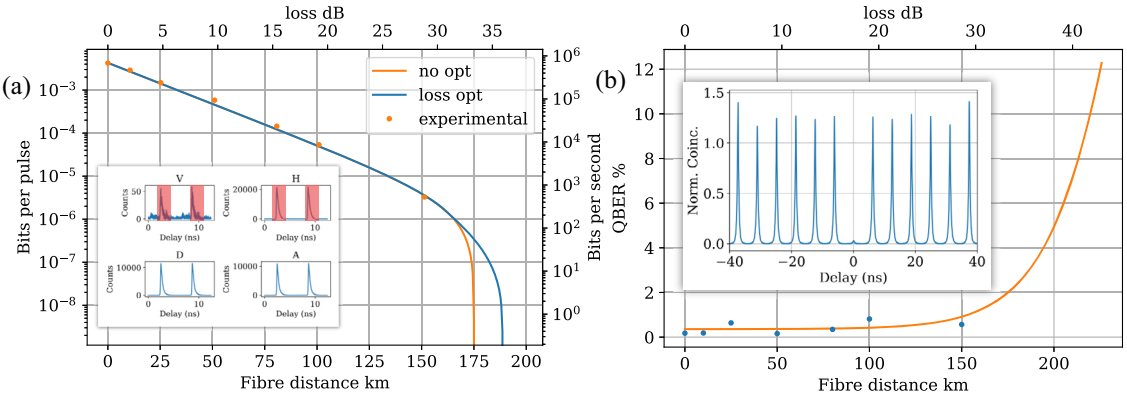

Fig. 2 | Asymptotic key rate and quantum bit error rate. a Experimental asymptotic key rate (orange dots) and the theoretical key rate based on the experimentally measured parameters with and without pre-attenuation of Alice's source. The pre-attenuation increases 2.6 dB the maximum tolerable loss. The inset shows a typical data set for Alice sending horizontally polarised photons over 80 km of fibre. Red boxes show the typical time gating used to optimise the key rate. **b** Measured error rate as a function of fibre distance. The theory fit is based on Eq. (1) with the experimental parameters listed in the main text. The deviations from the best fit are due to inconsistency in aligning the in-fibre polarisation controller. The QBER at the maximum tolerable loss of ~35 dB is ~2%. Maximum tolerable loss is primarily limited by the photon-number noise $g^{(2)}(0) = 0.036(3)$, shown in the inset of **b**.

Table 2 | Baseline QKD system parameters

Description	Parameter	Value
Mean photon number	$\langle n \rangle$	0.0142
Second-order correlation function	$g^{(2)}(0)$	0.036
Source repetition rate	R	160.7 MHz
Misalignment probability	p_{mis}	0.003
Dark count probability	p_{dc}	3.67×10^{-8}
Detector efficiency	η_{det}	0.6525
Detector dead time	τ	27.5 ns
Fibre loss	l	0.1904 dB/km
Parameter estimation failure probability	ε_{PE}	$2 \times 10^{-10}/3$
Privacy amplification failure probability	ε_{PA}	$10^{-10}/6$
Correctness failure probability	ε_{cor}	10^{-15}
Error correction leakage	λ_{EC}	Eq. (23)

events in that basis. By fitting the measured QBER to

$$e_{X/Z} = \frac{p_{dc} + p_{mis}\langle n \rangle T}{2p_{dc} + \langle n \rangle T}, \tag{1}$$

the average polarisation misalignment p_{mis} can be extracted, which typically is found to be $p_{\text{mis}} = 0.3\%$[13]. T represents the total optical efficiency from the quantum channel to Bob's detection apparatus. The dark count probability p_{dc} and mean photon number $\langle n \rangle$ are held as fixed parameters.

With p_{click}, $e_{X/Z}$, $\langle n \rangle$ and $g^{(2)}(0)$ experimentally characterised it is possible to calculate the asymptotic key rate (AKR) according to[14,15]

$$S = p_{\text{sift}} p_{\text{click}} \left[A\left(1 - H\left(\frac{e_X}{A}\right)\right) - f_{EC}(e_Z) H(e_Z) \right], \tag{2}$$

where $p_{\text{sift}} = p_X^2 + (1 - p_X)^2$ is the sifting ratio for the key generation bits assuming both bases are used, p_X is the basis bias, $H(x)$ is the binary Shannon entropy and $f_{EC}(x) > 1$ is the error correction efficiency factor.

For the experimental setup presented here $p_{\text{sift}} = \frac{1}{2}$ which allows for a comparison to previously published work (Table 1). For $f_{EC}(x)$ we use values linearly interpolated between those reported in ref. 16 (typically $f_{EC} = 1.16$ for the range of error rates seen in the experiment). $A = (p_{\text{click}} - p_m)/p_{\text{click}}$ is the fraction of signals which are single-photon pulses and p_m is the upper bound on the probability that Alice emits a multiphoton pulse taken to be $p_m \leq g^{(2)}(0)\langle n \rangle^2/2$[13]. From the measured $\langle n \rangle = 0.0142$ and $g^{(2)}(0) = 0.036(3)$ (see Fig. 2), we estimate $p_m \leq 3.63 \times 10^{-6}$ without any additional pre-attenuation before the final collection fibre. The small increase in $g^{(2)}(0)$ compared to the emission directly from the QD is due to Raman scattering in the frequency-conversion process.

The key rate at shorter distances is increased compared to previous works thanks to the high brightness and temporally multiplexed excitation presented in this work. The maximum tolerable loss is also increased due to the relatively high brightness and low noise compared to previous demonstrations with telecom wavelength QD sources. The current maximum range is limited by $p_{\text{click}} \to p_m$, at which point the fraction of signals received from single photon pulses goes to zero $A \to 0$, and a secure key is no longer possible. As the multiphoton emission and click probabilities are evaluated on a signal-by-signal basis, the multiplexed excitation does not improve the maximum distance over which a secure key can be extracted.

Finite key analysis

In assessing the performance of a practical QKD system the finite key rate must be considered. To date, most experiments with single-photon emitters[17,18] have used the method outlined in[15] to derive finite block size estimates of the secure key. Since the publication of[15], there has been considerable development of tighter statistical estimation bounds, mainly in the context of weak coherent pulse decoy state and entangled protocols. Here, we adapt and employ recent results based on Chernoff bounds to produce significant improvements in the finite key rate. This reduces the block size required for a positive key rate or, conversely, yields a much greater key rate for a fixed block size.

A full derivation of the finite key rate can be found in the Methods section with the main result discussed here. For a finite block size defined as either the number of sent N_S or received signals N_R, the total secure key length ℓ is,

$$\ell = \lfloor \underline{N}^X_{R,nmp}\left(1 - H\left(\overline{\phi}^X\right)\right) - \lambda_{EC} - 2\log_2\frac{1}{2\varepsilon_{PA}} - \log_2\frac{2}{\varepsilon_{cor}} \rfloor, \tag{3}$$

where $\underline{N}^X_{R,nmp}$ is the lower bound on the number of received signals in the key generation basis due to non-multiphoton source emissions (including vacuum and single-photon emissions), $\overline{\phi}^X$ is the upper bound of the phase error rate in the key generation basis, λ_{EC} is the

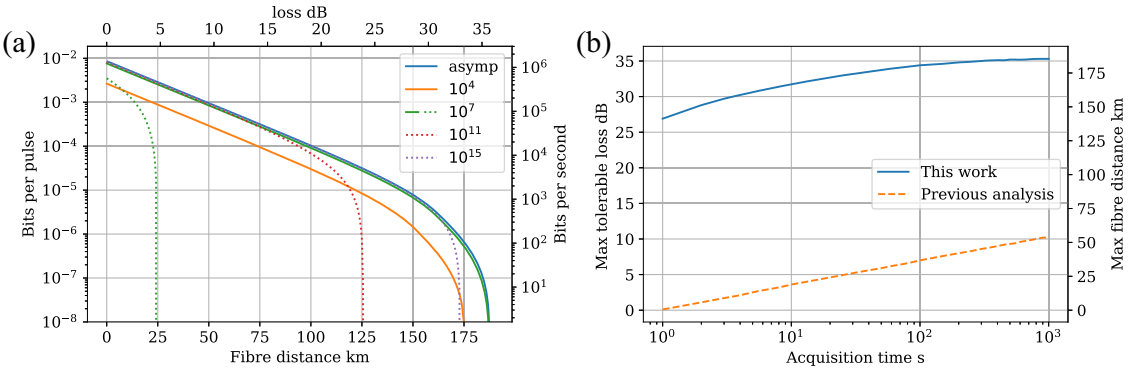

Fig. 3 | Comparison of finite key rate based on the Chernoff bound and previous finite-key analysis based on[15]. The finite key rate for different block sizes is shown in **a**; this work is shown with solid lines and previous work with a dashed line. For both versions, Alice's pre-attenuation and p_X are optimised for each distance and integration time. The bound presented in this work results in substantially better finite key rates using smaller block sizes. **b** shows the maximum tolerable loss achievable as a function of the acquisition time. This work substantially improves the distance over which a key can be generated compared to ref. 15, particularly for short acquisition times.

information leaked during error correction[19], and the remaining terms are security and correctness parameters derived using the methods in[20]. The key rate is then defined as $r = \frac{\ell}{N_S}$ and the fixed parameters used are shown in Table 2. The ratio of signals in the key generation basis to the parameter estimation basis, and the additional attenuation Alice adds to the source to reduce the multiphoton emission probability are all numerically optimised for each distance.

The improvement to the finite key rate can be viewed in two different ways: at long distances the block size required to produce the same key rate is massively reduced, Fig. 3a; alternatively, for a fixed acquisition time we can tolerate more loss and achieve the same secure key rate, Fig. 3b. The improvement to the finite key rate is quantified by comparing the number of signals required to approach the asymptotic key rate. To approach the asymptotic key rate with the method of[15], the received block size has to be on the order of 10^{15}, dotted purple curve Fig. 3a. Our results indicate a factor 10^8 improvement, the finite key rate curve reaches the asymptotic limit with Alice's pre-attenuation for just 10^7 received signals. With respect to a fixed acquisition time, previous security analysis restricts the maximum distance over which a key can be exchanged after one second of acquisition time to less than 1 km, Fig. 3b, whereas we calculate a maximum tolerable loss of 26.9 dB which is equivalent to over 140 km of fibre. For all acquisition times considered the analysis presented here can achieve the same key rate over an additional 25 dB of channel loss.

Discussion

We have demonstrated that fibre-based QKD with frequency-converted quantum dot is possible at high rates for distances and acquisition times relevant for metropolitan communication networks. The source performance exceeds other single-photon emitters suggested for use in QKD systems in terms of key rate and maximum tolerable loss. Combining state-of-the-art QD performance in brightness[2] and multiphoton suppression[21], with the frequency conversion demonstrated here into one device would allow for key rates comparable to decoy-state QKD with weak coherent pulses. Ultimately, surpassing weak coherent pulse implementations will require sources much closer to the ideal performance of unity collection efficiency with multiphoton emission probabilities approaching zero.

Regarding the key rate introduced with Eq. (3), a more up-to-date version for the terms of the security parameters and an additional fluctuation in the phase error rate due to the random sampling without replacement problem were introduced compared to previous studies. The considerable enhancement of the finite key rate is due to the improved bounds of the statistical fluctuations achieved using the Chernoff bound applied to the number of events versus bounding probabilities as in[22].

The deviations of the probabilities from the ideal estimate are magnified when expressed in the total number of events, e.g. number of errors and multiphoton emissions, although they might seem to be relatively small[23]. In particular, the Chernoff bound on events provides tighter estimates on the maximum number of multiphoton emissions increasing the single photon yield at longer distances and consequently the key rate.

Methods

Click and error probability estimation

In this section, we describe the modelling of click probabilities and error rates to later simulate the detections and error events. First, the click probability in each basis is,

$$p_{\text{click}}^{X,Z} = c_{dt} \sum_{n=0}^{\infty} p_n \left[1 - (1 - p_{dc}^{X,Z})(1 - \eta_{ch}\eta_{det}^{X,Z}\eta_{att})^n\right], \tag{4}$$

where p_n is the probability that a pulse emitted by the source contains n photons, $\eta_{det}^{X,Z}$ is the detector detection efficiency and $p_{dc}^{X,Z}$ is the average dark count probability of the two detectors associated with each basis. For simplicity we assume that all detectors have the same efficiencies and dark count rates. If they differ, then the security analysis should be adapted to avoid any loopholes introduced by detector efficiency mismatch[20]. We add a pre-attenuation factor η_{att}[13] which can be inserted between the source and the Eve-controlled channel to reduce multiphoton leakage in the high loss regime. The channel transmittance is given by $\eta_{ch} = 10^{-l/10}$ where l is the channel loss in dB. A correction factor c_{DT} is added to account for the dead time of the detectors. For a dead time τ and repetition rate R this correction is of the form

$$c_{dt} = \frac{1}{1 + R\tau p_{\text{click}}^{X,Z}}. \tag{5}$$

The error probability is then given by

$$p_e^{X,Z} = c_{dt}\left\{p_0\, p_{dc}^{X,Z} + \sum_{n=1}^{\infty} p_n \left[1 - (1 - p_{dc}^{X,Z})(1 - \eta_{ch}\eta_{det}^{X,Z}\eta_{att})^n\right] p_{mis}\right\}, \tag{6}$$

where p_{mis} is the probability of error due to the misalignment of the set-up.

For modelling purposes, we will assume that the multiphoton contribution is dominated by the 2-photon component, hence consider a source distribution of the form $\{p_n\} = \{p_0, p_1, p_2\}$ with emission probabilities of vacuum p_0, single photons p_1 and two photon states p_2. Given mean values for photon number $\langle n\rangle$ and $g^{(2)}(0)$,

$$p_2 = \frac{g^{(2)}(0)\langle n\rangle^2}{2}, \quad p_1 = \langle n\rangle - 2p_2, \quad p_0 = 1 - p_2 - p_1. \tag{7}$$

Note that the security of the key rate analysis is not compromised by such an assumed form of the photon number distribution as the distribution that only has non-zero $\{p_0, p_1, p_2\}$ saturates the bound of[13],

$$p_m \le \frac{g^{(2)}(0)\langle n\rangle^2}{2}, \tag{8}$$

and any other distribution consistent with $\langle n\rangle$ and $g^{(2)}(0)$ will have a lower p_m.

Finite key length based on Chernoff bounds

In this section, we follow the method and notation as described in ref. 10 though suitably adapted for the non-decoy single-photon source case which is akin to weak coherent pulse (WCP) protocols before the advent of decoy-state methods[24].

After basis sifting, the number of events where both Alice and Bob chose the Z and X bases are $N_R^X = N_S p_X^2 p_{\text{click}}^X$ and $N_R^Z = N_S p_Z^2 p_{\text{click}}^Z$, respectively, these are directly observed. Here, we adopt the convention that the Z basis is used for parameter estimation and the X basis is used to generate the key. The legitimate parties publically compare all the Z basis results to determine thenumber of Z errors $m_Z = N_S p_Z^2 p_e^Z$ which is then used to estimate the phase error rate ϕ^X in the X basis. The X basis results are never directly revealed.

The expected number of received signals that result from non-multiphoton emissions by Alice (lumping together the vacuum and single photon yields) is given by $N_{R,nmp}^{X,Z} = N_R^{X,Z} - N_{S,mp}^{X,Z^*}$ where $N_{S,mp}^{X,Z^*} = N_S p_X^2 p_m$ is the expected number (we use * to denote the mean) of sifted multiphoton emissions from Alice in the X, Z basis respectively. We assume that p_m can be determined in a pre-calibration phase with negligible uncertainty (similar to the pulse intensities in WCP protocols), else a suitable upper bound can be chosen for p_m itself. Here, we assume that all multiphoton pulses are detected by Bob (Eve introducing a lossless channel in this case) and that the remaining detected pulses come from the non-multiphoton fraction (if $N_R^{X,Z} > N_{S,mp}^{X,Z}$). As we do not directly observe the actual number of multiphoton emissions, the actual number $N_{S,mp}^{X,Z}$ can deviate from $N_{S,mp}^{X,Z^*}$ due to statistical fluctuations, and we need to upper bound the tail probability with error ε_{PE}. The upper Chernoff bound (denoted by the overbar) for a sum of binary variables $x = \sum x_j$ with $x_j \in \{0, 1\}$ is given by

$$\bar{x} = (1 + \delta^U)x^*, \tag{9}$$

where $\delta^U = \frac{\beta + \sqrt{8\beta x^* + \beta^2}}{2x^*}$, and $\beta = -\log_e(\varepsilon_{PE})$. This can be applied to derive an upper bound to the actual number of multiphoton emissions $\bar{N}_{S,mp}^{X,Z}$, hence lower bound the number of received signals from non-multiphoton emission events, $\underline{N}_{R,nm}^{X,Z}$ in each basis,

$$\underline{N}_{R,nmp}^{X,Z} = N_R^{X,Z} - \bar{N}_{S,mp}^{X,Z}. \tag{10}$$

We note that tighter upper bounds on $\bar{N}_{S,mp}^{X,Z}$ could in principle be used, such as those based on the "factorial moment"[25] or the Klar bounds[26]. Practically, the scope for potential improvement is minimal in our case and only possible for the highest tolerable losses of each finite block. These alternate bounds are also less amenable for numerical evaluation for the parameter ranges typical in QKD.

The phase error rate ϕ^X now needs to be upper bounded based on the observed number of errors in the Z basis m_Z. We conservatively assume that all Z basis errors occur on the received non-multiphoton fraction, hence we have an estimate of the phase error rate,

$$\phi^X = \frac{m_Z}{\underline{N}_{R,nmp}^Z}. \tag{11}$$

However, this estimate is the result of N_R^Z samples in the Z basis but we need to upper bound the phase error rate in the unannounced N_R^X samples in the X (key generating) basis. For this random sampling without replacement problem and a tail bound error ε, the upper bound of the unobserved value χ can be estimated from the observed value λ by

$$\chi = \lambda + \gamma^U(n, k, \lambda, \varepsilon'), \tag{12}$$

where

$$\gamma^U(n,k,\lambda,\varepsilon') = \frac{1}{2 + 2\frac{A^2 G}{(n+k)^2}}\left\{\frac{(1-2\lambda)AG}{n+k} + \sqrt{\frac{A^2G^2}{(n+k)^2} + 4\lambda(1-\lambda)G}\right\}, \tag{13}$$

$$A = \max\{n, k\}, \tag{14}$$

$$G = \frac{n+k}{nk}\log_e\frac{n+k}{2\pi nk\lambda(1-\lambda)\varepsilon'^2}, \tag{15}$$

under the assumption that $0 < \lambda < \chi < 0.5$ which is true for typical QKD scenarios. This now allows us to calculate an upper bound,

$$\bar{\phi}^X = \phi^X + \gamma^U\left(N_R^X, N_R^Z, \phi^X, \frac{\varepsilon_{sec}}{6}\right). \tag{16}$$

The secrecy of the protocol is $\varepsilon_{sec} \ge \varepsilon_{PA} + \varepsilon_{PE} + \varepsilon_{EC}$ where: $\varepsilon_{PA} = \varepsilon'$ is the privacy amplification failure probability; $\varepsilon_{PE} = 2n_{PE}\varepsilon'$ is the parameter estimation failure probability where $n_{PE} = 2$ is the number of constraints as quantified in post-processing; $\varepsilon_{EC} = \varepsilon'$ is the error correction failure probability. Thus, the secrecy comes from setting each failure probability to a common value ε', i.e. $\varepsilon_{sec} = 6\varepsilon'$. Moreover, the QKD protocol is ε_{qkd}-secure if it is ε_{cor}-correct and ε_{sec}-secret with $\varepsilon_{qkd} \ge \varepsilon_{cor} + \varepsilon_{sec}$. We set $\varepsilon_{cor} = 10^{-15}$ and $\varepsilon_{sec} = 10^{-10}$.

This leads to the length of the secure key fraction,

$$\ell = \lfloor \underline{N}_{R,nmp}^X\left(1 - H\left(\bar{\phi}^X\right)\right) - \lambda_{EC} - 2\log_2\frac{1}{2\varepsilon_{PA}} - \log_2\frac{2}{\varepsilon_{cor}}\rfloor, \tag{17}$$

where λ_{EC} is the known leakage of information during error correction. The key rate is then defined as $r = \frac{\ell}{N_S}$.

Security bounds and secure key rate

The security analysis follows that of[20] using min-entropy and the failure probabilities that appear in Table 2 therein. We use uncertainty relations for bounding Bob's raw key obtained from Alice's raw key and conditioned on Eve's information. Let us first consider Eve's information E and Alice's raw key X_A, that is generated by choosing a random sample from $N_{R,nmp}^X$, after the error correction and verification steps. The question is how much information Eve can extract from X_A that is completely unknown to her. The probability of guessing X_A given E is

defined as the classical min-entropy,

$$H_{min}(X_A|E) = \log_2 p_{guess}(X_A|E), \tag{18}$$

where $p_{guess}(X_A|E)$ represents the probability of correctly guessing X_A applying an optimal extraction strategy having access to E. The optimal strategy means to guess the value x of X with the highest conditional probability $p_{X|E=e}(x)$ for each value e of E. For this process, let us assume that a part X_B of X_A with length ℓ, that is uniform conditioned on the information E, can be extracted by Bob. In other words, there is a function f_s that maps X_A to Bob's raw key $X_B = f_s(X_A)$ considering the quantum state between Alice and Eve $\rho_{X_A E}$ is fixed. It has been shown that the probability of guessing X_B is $p_{guess}(X_B|E) = 2^{-\ell}$ and using Eq. (18) we obtain,

$$H_{min}(X_B|E) = \ell, \tag{19}$$

where ℓ is the secure key length. Furthermore, because X_B comes from mapping X_A, the probability of correctly guessing X_B has to be greater than the probability of guessing X_A. Therefore, these min-entropies can be expressed as the following inequality

$$H_{min}(X_B|E) \le H_{min}(X_A|E) \Rightarrow \ell \le H_{min}(X_A|E). \tag{20}$$

To extend this to the general case of almost uniform randomness, the smooth min-entropy $H^{\varepsilon}_{min}(X_A|E)$ needs to be introduced. This is set as the maximum value of $H_{min}(X_A|E)$. For privacy amplification, we consider that Alice and Bob apply a two-universal hash function. The Leftover Hashing Lemma[27] gives us an exact equation for the inequality of Eq. (20) using the smooth min-entropy to relate the already mentioned Eve's information E and Alice's raw key X_A

$$\ell = H^{\varepsilon}_{min}(X_A|E) - 2\log_2 \frac{1}{2\varepsilon_{PA}} \tag{21}$$

for the maximum number of extractable bits l that are ε_{PA}-close to uniform, conditioned on E.

We consider leakage λ_{EC} during error correction as well as additional bits for verification. Thus, the information that remains in Eve's system E' after error correction is related by,

$$H^{\varepsilon}_{min}(X_A|E) \ge H^{\varepsilon}_{min}(X_A|E') - \lambda_{EC} - \log_2 \frac{2}{\varepsilon_{cor}}. \tag{22}$$

The leakage in one-way protocols is lower bounded as[19],

$$\begin{aligned} \lambda_{EC} \ge\ & n_X H(e_X) \\ &+ \left[n_X(1-e_X) - F^{-1}(\varepsilon_{cor}; n_X, 1-e_X)\right]\log_2 \frac{1-e_X}{e_X} \\ &- \frac{1}{2}\log_2 n_X - \log_2 \frac{1}{\varepsilon_{cor}}, \end{aligned} \tag{23}$$

where $H(x)$ is the binary Shannon entropy, and $F^{-1}(\varepsilon_{cor}; n_X, 1-e_X)$ is the inverse of the cumulative distribution of the binomial distribution. Achievable rates by practical codes may not achieve this bound for large blocks so we choose the greater estimate of leakage given either by the above or $f_{EC} = 1.16$[16].

We use an uncertainty relation for smooth min-entropy to establish a bound between the remaining information that Eve has, E', and Alice's raw key, X_A. This reflects that the better Bob can estimate Alice's raw key in the Z basis, the worse Eve can guess Alice's raw key in the X basis, formally expressed as,

$$H^{\varepsilon}_{min}(X_A|E') \ge q\, N^{X}_{R,nmp} - H^{\varepsilon}_{max}(Z_A|Z_B), \tag{24}$$

limited to the non-multiphoton events in the key generation basis X. Here, q quantifies the efficiency of Bob's orthogonal qubit measurements, in this work we assume $q = 1$, although in practice the sent states by Alice are not perfect qubits. $H^{\varepsilon}_{max}(Z_A|Z_B)$ is the smooth max-entropy of Z_B conditioned on Z_A. If Z_B and Z_A are highly correlated, we can deduce that $H^{\varepsilon}_{max}(Z_A|Z_B)$ is small and thus, as the following bound shows[28], the observed number of errors is small,

$$H^{\varepsilon}_{max}(Z_A|Z_B) \le N^{X}_{R,nmp} H(\phi_X), \tag{25}$$

where ϕ_X is the X-basis phase error rate of non-multiphoton events. Finally, the bound for the min-entropy is,

$$H^{\varepsilon}_{min}(X_A|E') \ge N^{X}_{R,nmp}\left[1 - H(\phi_X)\right]. \tag{26}$$

Protocol optimisation

To maximise the rate and tolerable loss whilst maintaining security, we consider optimisations of the basis bias and signal pre-attenuation that can provide some improvement over standard protocol values, i.e. equal basis choice and no-attenuation.

The Efficient BB84 protocol simplifies standard BB84 by utilising one basis for key generation and the other basis for parameter estimation of the phase error rate, without compromising security[29]. In this paper, we adopt the convention that the X basis is used for the key with the Z basis used for phase error rate estimation. Alice and Bob randomly and independently choose their basis for each signal with bias p_X and $p_Z = (1 - p_X)$. The sifting ratio is $1 - 2p_X(1 - p_X) > \frac{1}{2}$ for unequal bias, higher than the sifting ratio $\frac{1}{2}$ for $p_X = \frac{1}{2}$ as in standard BB84. Additionally, this simplification also reduces the number of parameters to be estimated, hence improving finite-statistical bounds and the reduction in key length due to composable security parameters[20,30–33]. The value of p_X can be optimised to balance the amount of raw key bits (proportional to p_X^2) and parameter estimation signals (proportional to $(1 - p_X)^2$). In the asymptotic limit, $p_X \to 1$, hence the sifting ratio also approaches unity.

At long distances and high losses, the key rate is limited by the multi-photon emission probability. When the upper bound on the number of multiphoton emission events exceeds the number of detections, then Eve must be assumed to have full information about Alice and Bob's string, hence there can be no secure key. Waks et al.[13] proposed the addition of linear attenuation (characterised by transmission factor η_{att}) of the signals prior to injection into the quantum channel controlled by Eve. The bound on the multiphoton components is reduced by a factor of η_{att}^2 while the average photon number is only reduced by η_{att}. At high losses and with low dark count rates, the reduction in detection probability (and increase in QBER) may be offset by the greater fraction of Bob's received events being the result of non-multiphoton emissions by Alice, potentially leading to increased key rate and extending the non-zero key rate region to longer ranges.

Data availability

The datasets generated during and/or analysed during the current study are available from the corresponding author upon request.

References

1. Lu, C.-Y. & Pan, J.-W. Quantum-dot single-photon sources for the quantum internet. *Nat. Nanotechnol.* **16**, 1294 (2021).
2. Tomm, N. et al. A bright and fast source of coherent single photons. *Nat. Nanotechnol.* **16**, 399 (2021).

3. Wang, H. et al. Towards optimal single-photon sources from polarized microcavities. *Nat. Photonics* **13**, 770 (2019).
4. Thomas, S. E. et al. Bright polarized single-photon source based on a linear dipole. *Phys. Rev. Lett.* **126**, 233601 (2021).
5. Nawrath, C. et al. High emission rate from a Purcell-enhanced, triggered source of pure single photons in the telecom C-band. Preprint at https://arxiv.org/abs/2207.12898 (2022).
6. Morrison, C. L. et al. A bright source of telecom single photons based on quantum frequency conversion. *Appl. Phys. Lett.* **118**, 174003 (2021).
7. Da Lio, B. et al. A pure and indistinguishable single-photon source at telecommunication wavelength. *Adv. Quant. Technol.* **5**, 2200006 (2022).
8. You, X. et al. Quantum interference between independent solid-state single-photon sources separated by 300 km fiber. Preprint at https://arxiv.org/abs/2106.15545 (2021).
9. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).
10. Yin, H.-L. et al. Tight security bounds for decoy-state quantum key distribution. *Sci. Rep.* **10**, 1 (2020).
11. Strauf, S. et al. High-frequency single-photon source with polarization control. *Nat. Photonics* **1**, 704 (2007).
12. Bozzio, M. et al. Enhancing quantum cryptography with quantum dot single-photon sources. *npj Quant. Inf.* **8**, 104 (2022).
13. Waks, E., Santori, C. & Yamamoto, Y. Security aspects of quantum key distribution with sub-Poisson light. *Phys. Rev. A* **66**, 042315 (2002).
14. Gottesman, D., Lo, H.-K., Lutkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput.* **5**, 325 (2004).
15. Cai, R. Y. Q. & Scarani, V. Finite-key analysis for practical implementations of quantum key distribution. *N. J. Phys.* **11**, 045024 (2009).
16. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61**, 052304 (2000).
17. Gao, T. et al. A quantum key distribution testbed using a plug&play telecom-wavelength single-photon source. *Appl. Phys. Rev.* **9**, 011412 (2022).
18. Chaiwongkhot, P. et al. Enhancing secure key rates of satellite QKD using a quantum dot single-photon source. Preprint at https://arxiv.org/abs/2009.11818 (2020).
19. 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**, 1 (2017).
20. Bunandar, D., Govia, L. C., Krovi, H. & Englund, D. Numerical finite-key analysis of quantum key distribution. *npj Quant. Inf.* **6**, 1 (2020).
21. Schweickert, L. et al. On-demand generation of background-free single photons from a solid-state source. *Appl. Phys. Lett.* **112**, 093106 (2018).
22. Cai, R. Y. & Scarani, V. Erratum: Finite-key analysis for practical implementations of quantum key distribution. *N. J. Phys.* **11**, 109801 (2009).
23. Lucamarini, M., Dynes, J. F., Yuan, Z. L., & Shields, A. J. Practical treatment of quantum bugs. In *Electro-Optical Remote Sensing, Photonic Technologies, and Applications VI* Vol. 8542, 427–436 (SPIE, 2012).
24. Lütkenhaus, N. & Jahma, M. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *N. J. Phys.* **4**, 44 (2002).
25. Schmidt, J. P., Siegel, A. & Srinivasan, A. Chernoff–Hoeffding bounds for applications with limited independence. *SIAM J. Discrete Math.* **8**, 223 (1995).
26. Klar, B. Bounds on tail probabilities of discrete distributions. *Probability Eng. Inf. Sci.* **14**, 161 (2000).
27. Tomamichel, M., Schaffner, C., Smith, A. & Renner, R. Leftover hashing against quantum side information. *IEEE Trans. Inf. Theory* **57**, 5524 (2011).
28. Tomamichel, M. & Renner, R. Uncertainty relation for smooth entropies. *Phys. Rev. Lett.* **106**, 110506 (2011).
29. Lo, H.-K., Chau, H. F. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.* **18**, 133 (2005).
30. Sidhu, J. S., Brougham, T., McArthur, D., Pousa, R. G. & Oi, D. K. in *Quantum Technology: Driving Commercialisation of an Enabling Science II*, Vol. 11881, 1188106 (SPIE, 2021).
31. Brougham, T. & Oi, D. in *Quantum Technology: Driving Commercialisation of an Enabling Science II*, Vol. 11881, 14–23 (SPIE, 2021).
32. Brougham, T. & Oi, D. K. Modelling efficient BB84 with applications for medium-range, terrestrial free-space QKD. *N. J. Phys.* **24**, 075002 (2022).
33. Sidhu, J. S., Brougham, T., McArthur, D., Pousa, R. G. & Oi, D. K. Finite key effects in satellite quantum key distribution. *npj Quant. Inf.* **8**, 1 (2022).
34. 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).
35. Waks, E. et al. Quantum cryptography with a photon turnstile. *Nature* **420**, 762 (2002).
36. Murtaza, G. et al. Efficient room-temperature molecular single-photon sources for quantum key distribution. *Opt. Express* **31**, 9437–9447 (2023).
37. Samaner, C., Paçal, S., Mutlu, G., Uyanıkk, K. & Ateş, S. Free-space quantum key distribution with single photons from defects in hexagonal boron nitride. *Adv. Quant. Technol.* **5**, 2200059 (2022).
38. Gao, T., Helversen, M. V., Anton-Solanas, C., Schneider, C. & Heindel, T. Atomically-thin single-photon sources for quantum communication. *npj 2D Mater. Appl.* **7**, 4 (2023).
39. Vajner, D. A., Rickert, L., Gao, T., Kaymazlar, K. & Heindel, T. Quantum communication using semiconductor quantum dots. *Adv. Quant. Technol.* **5**, 2100116 (2022).

Acknowledgements

D.K.L.O. is supported by the EPSRC Researcher in Residence programme at the Satellite Applications Catapult (EP/T517288/1). R.G.P. acknowledges support from the EPSRC Research Excellence Award (REA) Studentship. D.K.L.O. and R.G.P. are supported by the EPSRC International Network in Space Quantum Technologies (EP/W027011/1). J.J. is supported by QuantIC, the EPSRC Quantum Technology Hub in Quantum Imaging (EP/T00097X/1). A.F., D.K.L.O., and R.G.P. are supported by the EPSRC Quantum Technology Hub in Quantum Communication (EP/T001011/1). B.D.G. is supported by a Wolfson Merit Award from the Royal Society, a Chair in Emerging Technology from the Royal Academy of Engineering, and the ERC (grant no. 725920). F.G. and Z.X.K. acknowledge studentship funding from EPSRC under Grant No. EP/L015110/1. D.B. acknowledges support by the UC Santa Barbara NSF QuantumFoundry funded via the Q-AMASE-i program GrantNo. DMR-1906325, and the NWO Gravitation-grantQuantum Software Consortium, Grant No. 024.003.037.

Author contributions

C.L.M., F.G., and Z.X.K. performed the measurements and collected the experimental data. P.B. assisted with data analysis. N.G.S. and D.B. fabricated the quantum dot sample. R.G.P., J.J., and D.K.L.O. derived the finite key bounds and performed the finite key optimisation. B.D.G. and A.F. conceived and supervised the experiment. All authors contributed to writing the manuscript.

Competing interests
The authors declare no competing interests.

Additional information
Correspondence and requests for materials should be addressed to Alessandro Fedrizzi.

Peer review information *Nature Communications* thanks the anonymous reviewer(s) for their contribution to the peer review of this work.