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

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

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.
error rate and the multiplicative Chernoff bound that has been proven to be a tighter finite key bound in other contexts\(^9\). 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 \(10^9\) 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\(^1\) 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\(^7\) 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 \(p_{dc} = 3.67 \times 10^{-7}\).  

### Asymptotic key rate

We send each of the BB84 states \([H,V,D,A]\) in turn and record at least \(5 \times 10^4\) 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, \(p_{\text{click}}\), 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. \(p_{\text{click}} = p_{\text{X}}^{\text{click}} = p_{\text{click}}^{\text{Y}}\) and \(p_{\text{click}} = p_{\text{click}}^{\text{D}} = p_{\text{click}}^{\text{A}}\). We measure a count rate of \(1.6\) MHz in Bob’s receiver at zero distance. This gives a mean photon number of \((n) = 0.0142\) injected into the communication channel backing out the known receiver transmission, the relative efficiency on average due to the measured losses of each detector (\(\approx 87\%\)) and the estimated quantum efficiency of the detectors (\(\approx 75\%\)).

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 photons detected by the Bob’s SNSPDs. For the purposes of comparison, the asymptotic key rate has been calculated with \(p_{\text{det}} = \frac{1}{2}\) 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.

\(\text{Table 1 | Comparison of other QKD demonstrations based on single-photon emitters}\)

| Reference        | AKR at 0 km (kbps) | Maximum tolerable loss (dB) |
|------------------|--------------------|-----------------------------|
| This work        | 689                | 33.3                        |
| This work with active encoding\(^8\) | 258                | 34.4                        |
| QD\(^9\)         | 2                  | 23                          |
| QD\(^10\)        | 2                  | 23                          |
| Molecule\(^11\)  | 25                 | 28                          |
| 2D Material\(^12\) | 0.24              | 21                          |
| 2D Material\(^13\) | 30                | 23                          |

For the purposes of comparison, the asymptotic key rate has been calculated with \(p_{\text{det}} = \frac{1}{2}\) 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.  

\(^8\)Prediction based on 3 dB loss and 2% polarisation encoding error typical with fibre-based electro-optic modulators.

---

**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 \(\mu\)m 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.
The dark count probability for a comparison to previously published work (Table 1). For binary Shannon entropy and \( n \) bits assuming both bases are used, it is possible to calculate the asymptotic key rate (AKR) according to14,15

\[
R = \frac{1}{2} \log_2 \left( 1 + \frac{p_{\text{click}}}{p_{\text{mis}}} - 1 \right). \tag{23}
\]

decreases with an increase in the fibre distance, but with a fixed block size.

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 emitters36,37 have used the method outlined in18 to derive finite block size estimates of the secure key. Since the publication of16, 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 \( \ell \) is

\[
\ell = \left| N_s \right| \left[ -1 + H(\mathcal{P}) \right] - \lambda_{\text{EC}} - 2\log_2 \frac{1}{2\ell_{\text{PA}}} - \log_2 \frac{2}{\epsilon_{\text{cor}}}, \tag{3}
\]

where \( \lambda_{\text{EC}} \) 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), \( \mathcal{P} \) is the upper bound of the phase error rate in the key generation basis, \( \lambda_{\text{EC}} \) 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), and \( \mathcal{P} \) is the upper bound of the phase error rate in the key generation basis, with \( \mathcal{P} \) being 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, \( \mathcal{P} \) is the upper bound of the phase error rate in the key generation basis.

![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.](image)
The key rate is then derived using the methods of [15], the received block size has to be on the order of $10^8$, dotted purple curve Fig. 3a. Our results indicate a factor 10 improvement in 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 and multiphoton suppression, 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,

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

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 [22]. We add a pre-attenuation factor $\eta_{att}^Z$ 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 $\eta_{ch} = 10^{-9}$ 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 $\tau$ and repetition rate $R$ this correction is of the form

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

The error probability is then given by

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

where $p_{\text{mis}}$ 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 \([p_0, p_1, p_2] \) with emission probabilities of vacuum \(p_0 \), single photons \(p_1 \) and two photon states \(p_2 \). Given mean values for photon number \((n)\) and \(g^{(2)}(0)\),

\[
P_2 = \frac{g^{(2)}(0)[n]^2}{2}, \quad p_1 = (n) - 2p_2, \quad p_0 = 1 - p_2 - p_1.
\]

(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 \(\sqrt{N} \).

\[
P_m = \frac{g^{(2)}(0)[n]^2}{2},
\]

and any other distribution consistent with \((n)\) 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-decay single-photon source case which is akin to weak coherent pulse (WCP) protocols before the advent of decoy-state methods. After basis siftiing, the number of events where both Alice and Bob chose the Z and X bases are \(N^X_{Z,corr} = N^X_{Z} - N^Z_{X,MP} \) and \(N^X_{Z,MP} = N^Z_{X} - N^Z_{X,MP} \) 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 publicly compare all the Z basis results to determine the number of Z errors \(m_z = N^Z_{X,MP} - N^Z_{X,Z,corr} \) which is then used to estimate the phase error rate \(\phi \) 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 \(N^X_{Z,corr} = N^X_{Z} - N^Z_{X,MP} \) where \(N^X_{Z} - N^Z_{X,MP} \) is the expected number (we use \(\bar{m} \) 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, the actual number of multiphoton emissions, the actual number \(N^X_{Z,MP} \) can deviate from statistical fluctuations, and we need to upper bound the tail probability with error \(\epsilon_{PC} \). The upper Chernoff bound (denoted by the overbar) for a sum of binary variables \(X = \sum x_i \) with \(x_i \in [0, 1] \) is given by

\[
\mathbb{F}(X) = (1 + \beta^2)^{\frac{X}{2}},
\]

where \(\beta^2 = 1 + \sqrt{\frac{g^{(2)}(0)}{2}}\), and \(\beta = -\log_2(\epsilon_{PC}) \). This can be applied to derive an upper bound to the actual number of multiphoton emissions \(N^X_{Z,MP}\), hence lower bound the number of received signals from non-multiphoton emission events, \(N^X_{Z,corr} \) in each basis,

\[
N^X_{Z,corr} = N^X_{Z} - N^Z_{X,MP}.
\]

(10)

We note that tighter upper bounds on \(N^X_{Z,corr}\) could in principle be used, such as those based on the “factorial moment” or the Klar bounds. 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 \(\phi \) 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,

\[
\phi^X = \frac{m_z}{N^X_{Z,corr}}.
\]

(11)

However, this estimate is the result of \(N^X_{Z,corr}\) samples in the Z basis but we need to upper bound the phase error rate in the unannounced \(N^X_{Z,corr}\) samples in the X (key generating) basis. For this random sampling without replacement problem and a tail bound error \(\epsilon\), the upper bound of the unobserved value \(\chi\) can be estimated from the observed value \(A\) by

\[
\chi = \lambda + y^U(n, k, \lambda, \epsilon),
\]

(12)

where

\[
y^U(n, k, \lambda, \epsilon) = \frac{1}{2 + 2 \epsilon} \left( \frac{1 - 2\lambda(1 - \lambda G)}{n + k} + \sqrt{\frac{1}{n + k}} \left( \frac{\lambda(1 - \lambda G)}{n + k} + 4\lambda(1 - \lambda G) \right) \right).
\]

(13)

\[
G = \frac{n + k}{nk} \log_2 \frac{n + k}{2\log_2(1 - \lambda \epsilon^2)},
\]

(14)

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

\[
\mathbb{F}(\phi^X) = \phi^U(n, k) = \left( N^X_{Z,corr}, N^X_{Z,MP}, \phi^X, \epsilon_{PC} \right).
\]

(16)

The secrecy of the protocol is \(\epsilon_{corr} \geq \epsilon_{P_A} + \epsilon_{P_E} + \epsilon_{E_{sec}} \) where: \(\epsilon_{P_A} = \epsilon\) is the privacy amplification failure probability; \(\epsilon_{P_E} = 2n_{E_{sec}}\epsilon\) is the parameter estimation failure probability where \(n_{E_{sec}} = 2\) is the number of constraints as quantified in post-processing; \(\epsilon_{E_{sec}} = \epsilon\) is the error correction failure probability. Thus, the secrecy comes from setting each failure probability to a common value \(\epsilon\), i.e. \(\epsilon_{corr} = 6\epsilon\). Moreover, the QKD protocol is \(E_{corr}\) secure if it is \(E_{corr}\)-correct and \(E_{corr}\)-secret with \(\epsilon_{E_{corr}} \geq \epsilon_{corr} + \epsilon_{S_{corr}}\). We set \(\epsilon_{E_{corr}} = 10^{-10}\) and \(\epsilon_{S_{corr}} = 10^{-10}\).

This leads to the length of the secure key fraction,

\[
\ell = [N^X_{Z,corr}(1 - H(\mathbb{F}^X))] - \lambda_{E_{sec}} - 2\log_2 \frac{1}{2\epsilon_{P_A}} - \log_2 \frac{2}{\epsilon_{corr}}.
\]

(17)

where \(\lambda_{E_{sec}}\) is the known leakage of information during error correction. The key rate is then defined as \(r = \frac{\ell}{N^X_{Z,corr}}\).

**Security bounds and secure key rate**

The security analysis follows that of \(\mathbb{F}^X\) 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 \(X_e\), that is generated by choosing a random sample from \(N^X_{Z,corr}\) after the error correction and verification steps. The question is how much information Eve can extract from \(X_e\) that is completely unknown to her. The probability of guessing \(X_e\) given \(E\) is
defined as the classical min-entropy,
\[ H_{\text{min}}(X_A|E) = \log_2 p_{\text{guess}}(X_A|E), \tag{18} \]
where \( p_{\text{guess}}(X_A|E) \) 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 \( p_{\text{guess}}(x|E) \) for each value \( e \) of \( E \). For this process, let us assume that a part \( X_0 \) of \( X_A \) with length \( \ell \) that is uniform conditioned on the information \( E \), can be extracted by Bob. In other words, there is a function \( f_E \) that maps \( X_A \) to Bob’s raw key \( X_B = f_{\ell}(X_0) \) considering the quantum state between Alice and Eve \( p_{x_{\ell}}(x) \) is fixed. It has been shown that the probability of guessing \( X_0 \) is \( p_{\text{guess}}(X_0|E) = 2^{-\ell} \) and using Eq. (18) we obtain,
\[ H_{\text{min}}(X_0|E) = \ell, \tag{19} \]
where \( \ell \) is the secure key length. Furthermore, because \( X_0 \) comes from mapping \( X_A \), the probability of correctly guessing \( X_0 \) has to be greater than the probability of guessing \( X_A \). Therefore, these min-entropies can be expressed as the following inequality
\[ H_{\text{min}}(X_A|E) \leq H_{\text{min}}(X_A|E) \Rightarrow \ell \leq H_{\text{min}}(X_A|E). \tag{20} \]

To extend this to the general case of almost uniform randomness, the smooth min-entropy \( H_{\text{min}}^f(X_A|E) \) needs to be introduced. This is set as the maximum value of \( H_{\text{min}}(X_A|E) \). For privacy amplification, we consider that Alice and Bob apply a two-universal hash function. The Leftover Hashing Lemma2 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 \( X_A \)
\[ \ell = H_{\text{min}}^f(X_A|E) - 2 \log_2 \left( \frac{1}{2 \epsilon_{PA}} \right) \tag{21} \]
for the maximum number of extractable bits \( l \) that are \( \epsilon_{PA} \) close to uniform, conditioned on \( E \).

We consider leakage \( \lambda_{EC} \) 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,
\[ H_{\text{min}}^f(X_A|E) \geq H_{\text{min}}^f(X_A|E) - \lambda_{EC} - \log_2 \left( \frac{2}{\epsilon_{cor}} \right). \tag{22} \]
The leakage in one-way protocols is lower bounded as\(^{39} \),
\[ \lambda_{EC} \geq n_X \epsilon_X H(\epsilon_X) + \left[ n_X (1 - \epsilon_X) - F^{-1}(\epsilon_{cor}; n_X, 1 - \epsilon_X) \right] \log_2 \left( \frac{1 - \epsilon_X}{\epsilon_X} \right) - \frac{1}{2} \log_2 n_X - \log_2 \left( \frac{1}{\epsilon_{cor}} \right), \tag{23} \]
where \( H(x) \) is the binary Shannon entropy, and \( F^{-1}(\epsilon_{cor}; n_X, 1 - \epsilon_X) \) 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 \( \lambda_{EC} \geq 1.16^{36} \).

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, \( X_E \). 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,
\[ H_{\text{min}}^f(X_A|E) \geq q N_{R_{\text{mp}}} - H_{\text{max}}^f(Z_A|Z_B), \tag{24} \]
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. \( H_{\text{max}}^f(Z_A|Z_B) \) is the smooth max-entropy of \( Z_E \) conditioned on \( Z_A \). If \( Z_E \) and \( Z_A \) are highly correlated, we can deduce that \( H_{\text{max}}^f(Z_A|Z_B) \) is small and thus, as the following bound shows\(^{39} \), the observed number of errors is small,
\[ H_{\text{max}}^f(Z_A|Z_B) \leq N_{R_{\text{mp}}} H(\epsilon_X), \tag{25} \]
where \( \phi_X \) is the X-basis phase error rate of non-multiphoton events. Finally, the bound for the min-entropy is,
\[ H_{\text{min}}^f(X_A|E) \geq N_{R_{\text{mp}}} + 1 - H(\phi_X). \tag{26} \]

### 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 utilizing 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 \( 1 - 2p_X(1 - p_Z)^2 > \frac{1}{2} \) 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\(^{30,30} \). 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 \( \eta_{\text{att}} \)) 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 \( \eta_{\text{att}} \), while the average photon number is only reduced by \( \eta_{\text{att}} \). 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 preprint. 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. Process. 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-and-play telecom-wavelength single-photon source. Appl. Phys. Rev. 9, 011412 (2022).
18. Chaiewongkhot, 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 Quantum 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. Probabilty 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, 118806 (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 Quantum 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., Uyanik, 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. 4, 2 (2023).
39. Vajner, D. A., Rickert, L., Gao, T., Kaymazlar, K. & Heindel, T. Quantum communication using semiconductor quantum dots. Adv. Quantum 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 International Network in Space Quantum Technologies (EP/W027011/1). R.G.P. is supported by the EPSRC Researcher in Residence programme at the Satellite Applications Catapult (EP/T517288/1). R.G.P., J.J., and D.K.L.O. derived 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. are supported by the EPSRC Researcher in Residence programme at the Satellite Applications Catapult (EP/T517288/1). R.G.P. and J.J. are supported by 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 Quantum Foundry 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.

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

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

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/.

© The Author(s) 2023