Quantum cryptography without detector vulnerabilities using optically-seeded lasers

L. C. Comandar,[1,2] M. Lucamarini,[1,*] B. Fröhlich,[1] J. F. Dynes,[1]
A. W. Sharpe,[1] S. Tam,[1] Z. L. Yuan,[1] R. V. Penty,[2] and A. J. Shields[1]

[1] *Toshiba Research Europe Ltd, 208 Cambridge Science Park, Cambridge CB4 0GZ, United Kingdom*
[2] *Cambridge University Engineering Department, 9 JJ Thomson Ave, Cambridge, CB3 0FA, United Kingdom*

Security in quantum cryptography [1, 2] is continuously challenged by inventive attacks [3–7] targeting the real components of a cryptographic setup, and duly restored by new countermeasures [8–10] to foil them. Due to their high sensitivity and complex design, detectors are the most frequently attacked components. Recently it was shown that two-photon interference [11] from independent light sources can be exploited to avoid the use of detectors at the two ends of the communication channel [12, 13]. This new form of detection-safe quantum cryptography, called Measurement-Device-Independent Quantum Key Distribution (MDI-QKD), has been experimentally demonstrated [13–18], but with modest delivered key rates. Here we introduce a novel pulsed laser seeding technique to obtain high-visibility interference from gain-switched lasers and thereby perform quantum cryptography without detector vulnerabilities with unprecedented bit rates, in excess of 1 Mb/s. This represents a 2 to 6 orders of magnitude improvement over existing implementations and for the first time promotes the new scheme as a practical resource for quantum secure communications.

* marco.lucamarini@crl.toshiba.co.uk

In Quantum Cryptography, a sender Alice transmits encoded quantum signals to a receiver Bob, who measures them and distils a secret string of bits with the sender via public discussion [1]. Ideally, the use of quantum signals guarantees the information-theoretical security of the communication [2]. In practice, however, Quantum Cryptography is implemented with real components, which can deviate from the ideal description. This can be exploited to circumvent the quantum protection if the users are unaware of the problem [19].

Usually the most complex components are also the most vulnerable. Therefore the vast majority of the attacks performed so far have targeted Bob's single photon detectors [3–7]. MDI-QKD [12, 13] is a recent form of Quantum Cryptography conceived to remove the problem of detector vulnerability. As depicted in Fig. 1(a), two light pulses are independently encoded and sent by Alice and Bob to a central node, Charlie. This is similar to a quantum access network configuration [20], but in MDI-QKD the central node does not need to be trusted and could even attempt to steal information from Alice and Bob. To follow the MDI-QKD protocol, Charlie must let the two light pulses interfere at the beam splitter inside his station and then measure them. The result can disclose the correlation between the bits encoded by the users, but not their actual values, which therefore remain secret. If Charlie violates the protocol and measures the pulses separately, he can learn the absolute values of the bits, but not their correlation. Therefore he cannot announce the correct correlation to the users, who will then unveil his attempt through public discussion. Irrespective of Charlie's choice, the users' apparatuses no longer need a detector and the detection vulnerability of Quantum Cryptography is removed.

This striking feature of MDI-QKD has fostered intense experimental work and various demonstrations have been provided so far [13–18]. However, to achieve high-visibility interference at Charlie's beam splitter, the light source in previous experiments was set to emit long pulses at modest clock rates, thus restricting the key rate to less than a hundred bit/s (see Table I).

Here we demonstrate a novel high-rate source of indistinguishable pulses from gain-switched laser diodes, ideally suited to MDI-QKD. We use a pair of these sources each generating 10^9 pulses per second, thereby achieving Quantum Cryptography immune to detector attacks at key rates exceeding 1 Mbps for the first time. This is orders of magnitude higher than in previous demonstrations and is comparable to the highest values achieved for conventional Quantum Cryptography [21]. Furthermore we demonstrate operation for channel loss greater than 20 dB, corresponding to over 100 km of standard fibre. Implementation with real fibre and the effect of a finite sample have also been considered in the experiment.

To suit MDI-QKD, the light sources in Alice and Bob have to match stringent criteria. They

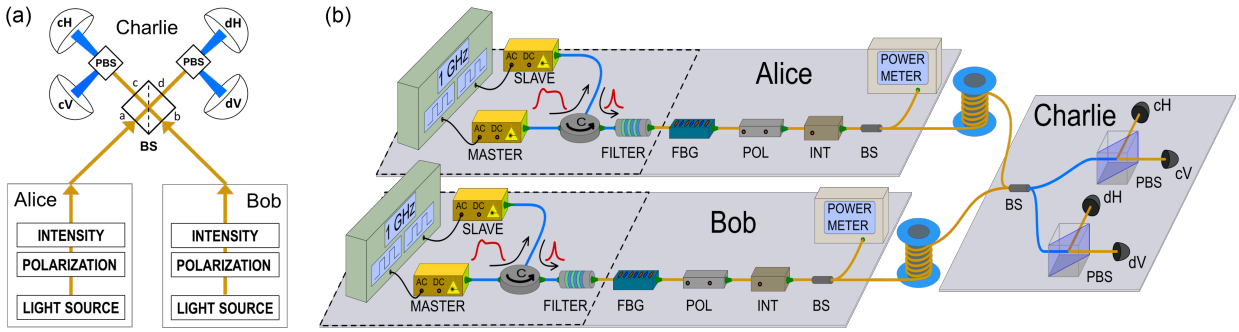

FIG. 1. (a) MDI-QKD scheme. Phase-randomised optical pulses are produced by Alice and Bob, set to the desired polarization and intensity, and sent to Charlie. There, they interfere at the beam splitter (BS), pass through the polarizing BS's (PBS's) and reach the four detectors. Coincidence counts from cH/dV or dH/cV (cH/cV or dH/dV) are grouped under the label $|\Psi^-\rangle$ ($|\Psi^+\rangle$), called 'singlet' ('triplet') [13]. The measurement outcomes are publicly announced by Charlie. (b) Experimental MDI-QKD setup. The light sources, which are essential to the results in this work, are enclosed by the dashed lines in Alice's and Bob's setup. C: circulator; FBG: fibre Bragg grating; POL (INT): polarization (intensity) module.

should emit indistinguishable pulses, to enable high-visibility two-photon interference [11], and at the same time each pulse should display a random optical phase, to meet a fundamental security condition [22]. In most demonstrations so far [13, 15–17], light pulses have been carved from a continuous-wave laser. However, the pulses generated this way have a constant or slowly varying optical phase thus violating the random phase condition. An external phase modulator can obviate this problem [15], but at the expense of increasing cost and complexity of the setup. Semiconductor gain-switched laser diodes can naturally generate short optical pulses (<50 ps) with random phases [23]. However, the emitted light pulses display a substantial time jitter due to the random nature of the spontaneous emission starting the lasing action. Furthermore they have also a significant spectral width, far exceeding the time-bandwidth limit, due to the frequency chirping arising from transient variation of carrier density in the active medium. These effects combine dramatically to reduce the visibility of the interference. As theoretically depicted in Fig. 2(a), temporal jitter and chirp lead to a poor visibility (upper-right corner of the figure). This has so far prevented the use of gain-switched laser diodes to achieve high-speed MDI-QKD.

Here we propose a novel technique based on pulsed laser seeding to produce low-jitter close-to-transform-limited phase-randomized light pulses from gain-switched lasers. A master laser injects photons into the cavity of a second slave laser through an optical circulator, see Fig. 1(b). The lasing action of the slave laser is then initiated by stimulated emission from the light of the master laser rather than by its own spontaneous emission, thus reducing the uncertainty in its emission

	Clock [MHz]	Pulse Width [ps]	Equivalent Distance [km]	Max key rate [bit/s]	Notes
A	75	2500	50	6.7×10^{1}	Phase random, 2x SSPD Finite size, real fibre (10 dB)
B	2	250	45	3.4×10^{0}	Active phase random, 2x APD Real fibre of 18.6 km
	20	290	80	6.2×10^{2}	Single laser source, 2x SSPD
C	2	500	45	3×10^{0}	No phase random, 2x APD Real fibre of 18.6 km
D	1	1500	17	1×10^{0}	No phase random, 4x APD Real fibre
This work	1000	35	12	1.257×10^{6}	Phase random, 4x 20 °C SD-APD Laser seeding, optimized protocol
				2.16×10^{5}	+ Finite size
			49	9.8×10^{4}	Phase random, 4x 20 °C SD-APD Laser seeding, optimized protocol
				9.8×10^{4}	+ Real fibre
			80	1.6×10^{4}	Phase random., 4x 0 °C SD-APD Laser seeding, optimized protocol

TABLE I. Key rates in existing MDI-QKD experiments and comparison with this work. Letters A-D correspond to Refs. [14–17], respectively. Low source clock rate (2nd column) and large pulse width (3rd column) have been used in previous experiments to achieve high-visibility two-photon interference. In one case (B, lower line) a single laser has been employed for both users. Obtaining high visibility from two independent light sources at 1 GHz clock rate and 35 ps pulse width is a major challenge, solved in this work, and can dramatically increase the key rate of MDI-QKD. SSPD: superconducting single photon detector; SD: self-differencing; APD: avalanche photo diode.

time. Furthermore, the competition between the cavity modes of the slave laser is immediately resolved by the presence of the master laser's light, thus narrowing the bandwidth of the emitted pulses. The combined effect increases the visibility of the interference between the two narrow pulses emitted by the users' slave lasers. Moreover, the pulsed laser seeding guarantees that the phase of each slave laser is inherited from its own master laser. Due to the fact that the master laser is gain-switched, the master pulse, and hence the slave pulse, has a random optical phase [23].

The improvement in the interference visibility achieved via the pulsed seeding technique is visible from Fig. 2(a), where time jitter, bandwidth and visibility of the light sources are experimentally measured and compared against the theoretical prediction. Without pulsed seeding, time jitter and bandwidth of the source amount to 12.3 ps and 63 GHz, respectively, leading to a poor visibility of 25% and therefore to low key rates. With pulsed laser seeding, on the contrary, they become as small as 4.4 ps and 15 GHz, respectively. For these values we expect an interference visibility

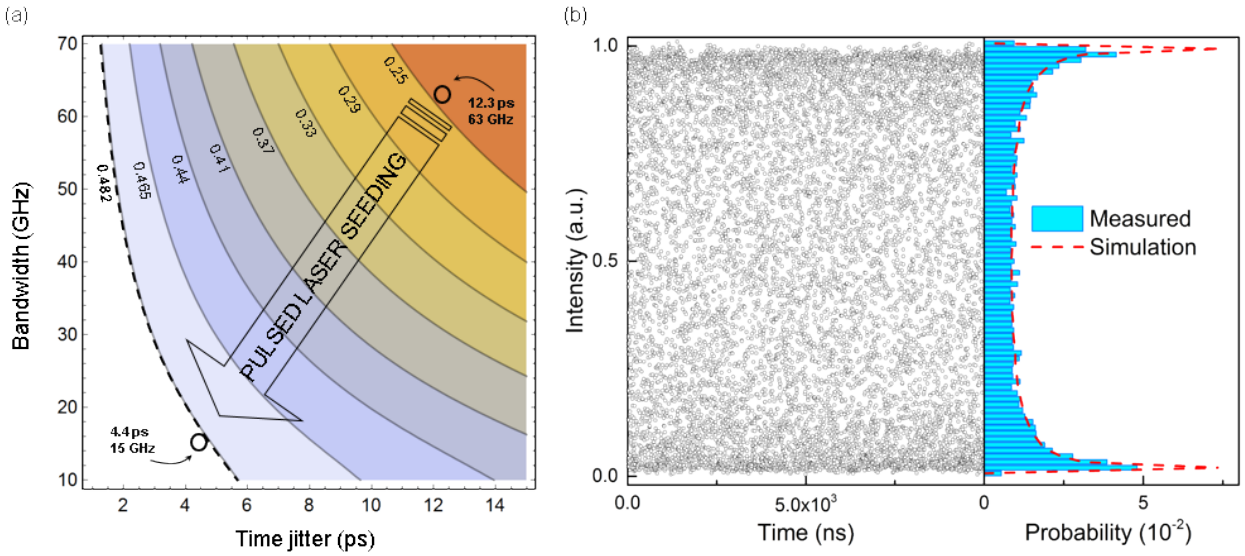

FIG. 2. (a) Theoretical contour plot of the two-photon interference visibility versus emission time jitter (horizontal axis) and bandwidth (vertical axis) of the pulses. The arrow shows how pulsed laser seeding improves the measured time jitter and bandwidth (empty circles), thus enhancing the interference visibility. The dashed black line depicts the maximum measured visibility. (b) Intensity data points and corresponding probability distribution from first-order interference between two consecutive pulses emitted by a seeded laser. The profile of the distribution suggests that the pulses have a random phase [23].

of 48.5%, in good agreement with the experimentally measured value of 48.2% and close to the theoretical maximum of 50% [24]. The phase randomisation of the pulses emitted by the seeded slave laser is confirmed in Fig. 2(b), where the intensity probability distribution has the typical profile expected from the interference of two pulses with random relative phase [23].

We performed a series of MDI-QKD experiments using the setup in Fig. 1(b). The results are summarized in Fig. 3 and detailed in [25] (see also Table I). The data points represented by the solid squares are obtained by using variable attenuators to reproduce the attenuation of standard single mode fibres (0.2 dB/km). The leftmost point corresponds to a rate of 1.257 Mbit/s, a record in terms of key rate mediated by two-photon interference. The rightmost point corresponds to about 4 kbit/s over 21 dB attenuation, which is still sufficient to generate a 256-AES key more frequently than every 100 ms [26].

Following the analysis in Ref. [27], we consider how the statistical fluctuations of a finite data sample can affect the secure key rate. With the empty square point in Fig. 3, we report the finite-size key rate of the system for a 2.33 dB attenuation channel. It amounts to 366 kbit/s and is obtained by gathering the counts from the triplet and singlet states. The finite-size dependence on

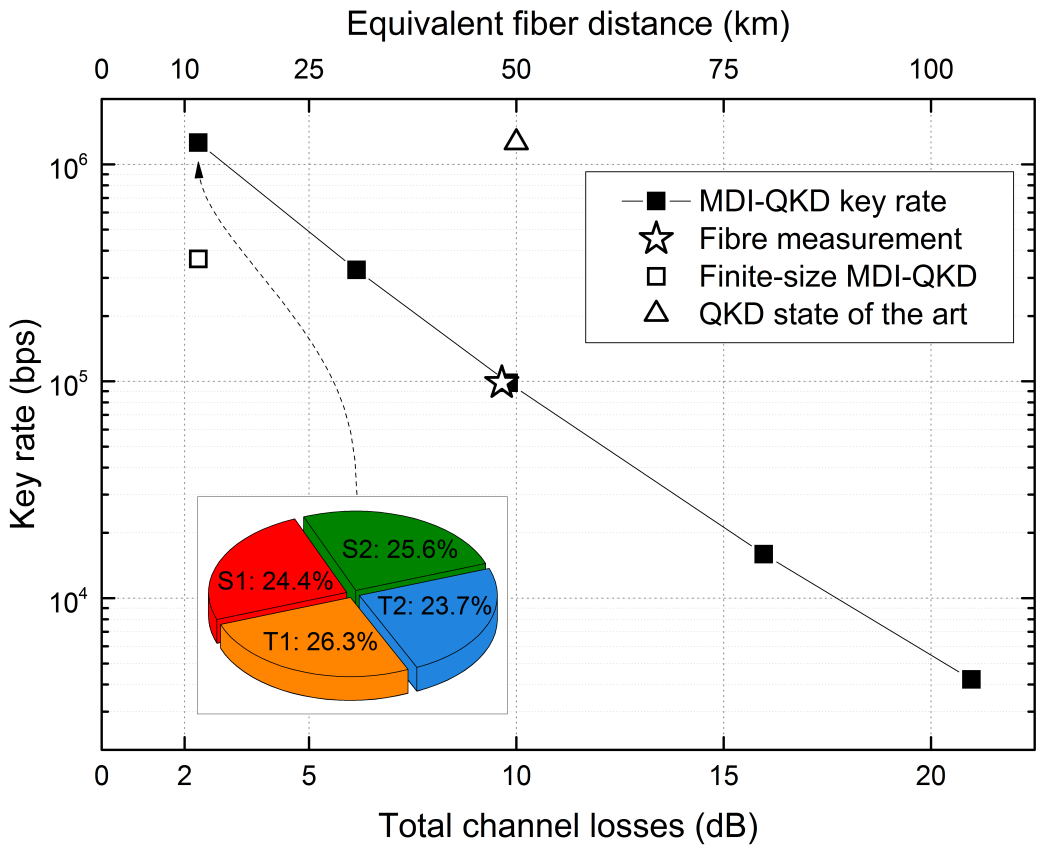

FIG. 3. MDI-QKD key rates versus total attenuation (lower axis) and equivalent fibre distance (upper axis) of the quantum channel. Solid squares refer to the key rates obtained by varying the channel attenuation in the setup. The empty star is for the rate obtained using two 25-km reels of single mode fibre. The empty square represents the rate after the finite size of the data sample is taken into account. In this case, the total sample size is $\sim 2.4 \times 10^7$, acquired in 12,000 seconds. For comparison, we also add the highest observed finite-size key rate to date for conventional QKD (empty triangle) [21]. The pie-chart contains the distribution of coincidence counts among the four possible outcomes of Charlie's measurement, for the 2.33 dB loss case. With reference to Fig. 1(a), S1, S2, T1 and T2 indicate the coincidence counts of detectors cH/dV, dH/cV, cH/cV and dH/dV, respectively.

the channel attenuation is observed to have a similar slope as that in the asymptotic regime.

To replicate a real deployment scenario, we replace the channel attenuation with two single mode fibre spools of 25 km each. We employ two dispersion compensation modules designed for 20 km to cancel the broadening of the pulses due to the chromatic dispersion in the fibre. We also compensate the temporal drift of the arrival time of the pulses at Charlie's beam splitter due to temperature variations. We find that the distilled key rate (empty star in Fig. 3) is almost identical to the one obtained from the channel attenuation, proving that fibre-induced effects can

be effectively mitigated. All the points in Fig. 3 have been numerically simulated along the lines of Refs. [28, 29] to confirm the results and optimize the system.

To illustrate the progress entailed by these results, we report in Fig. 3 with an empty triangle the state-of-the-art point [21] of finite-size decoy-state QKD, for a distance of 50 km under similar detection conditions as in the present experiment. Quite impressively, the QKD key rate is only one order of magnitude higher than the corresponding MDI-QKD asymptotic rate, the difference being largely accountable to the non-unitary efficiency of the single photon detectors.

These results prove that MDI-QKD can distribute keys at rates similar to conventional Quantum Cryptography and promote it as a practical solution to serve real-world secure communications.

METHODS

Experimental setup

Alice and Bob consist of two independent pulsed laser seeding-enabled light sources producing phase-randomised 35 ps-long laser pulses at 1550 nm at the repetition rate of 1 GHz. Variable optical band pass filters with 20 GHz bandwidth are aligned to remove any spurious emission. Fibre Bragg gratings are added to pre-compensate for the pulse broadening in the fibre experiment. Polarization and intensity of the pulses are set as required in the protocol and power meters are used to monitor the average photon fluxes. This lets each user prepare weak coherent states in one of four polarization states: H, V (rectilinear basis, or Z) or D, A (diagonal basis, or X). The Z basis is used to distil the key bits, while the X basis is used to test the noise on the quantum channel. Alice and Bob select the intensity of the states among four possible values, or "classes": s (signal), u (decoy 1), v (decoy 2), w (vacuum). This is different from previous protocols [13], where three intensity settings rather than four were used, and allows for higher key rates [30]. For the class s, they assign a polarization state from the Z basis, either H or V. For the other classes, they assign a polarization state from the X basis, either D or A. The intensity is in the range of 0.7 photons/pulse for the Z basis and between 0 and 0.08 photons/pulse for the X basis. The users send the resulting states to Charlie, with probabilities $p_s = p_Z = 1 - p_X = 45/48$ and $p_u = p_v = p_w = p_X/3$. In Charlie, the beam splitter output ports are spliced to the polarizing beam splitter input ports to ensure polarization alignment to the rectilinear basis and reduce losses. Four InGaAs self-differencing avalanche photodiodes are gated at 1 GHz and synchronised to the arrival time of the photons with 1 ns intrinsic deadtime. Under these conditions the detectors have

an effective active window of around 100 ps and are able to measure up to 500 Mcps [31]. Their efficiency is kept close to 30% for the whole duration of the experiment. For attenuation levels up to 16 dB it is advantageous to operate detectors at room temperature (20 °C), to reduce the afterpulse probability, while for larger attenuation values it is beneficial to operate them at 0 °C, to produce a smaller dark count rate. At 20 °C and 0 °C, the afterpulse probability amounts to 6.5% and 8.6%, respectively, and the dark count probability per gate is 6.50×10^{-5} and 2.64×10^{-5}, respectively. Temporal overlap between the pulses is initially achieved by maximizing the single counts within the detection window of the gated detector. This is then fine-tuned by directly measuring the interference visibility in the matched Z basis.

Pulsed laser seeding

Each user is endowed with two gain-switched lasers, one of which acts as the master and the other as the slave. The two lasers are driven by square waves at 1 GHz through their AC port. An electrical delay allows to vary the timing between the two driving signals. The DC level of the master laser is set below the threshold ensuring a random phase, but is sufficiently high to have little turn-on delay and produce ∼250 ps pulses. That of the slave is set low enough to assure that no lasing is possible in the absence of the master laser photons. With seeding photons from the master laser, the slave laser produces pulses around 35 ps wide and close to the time-bandwidth product limit. In Fig. 2(a), the time jitter and frequency bandwidth of the pulses are measured using a fast sampling oscilloscope and an optical spectrum analyser. To test the visibility of the setup we perform a two-photon interference experiment using superconducting single photon detectors. The photon count rate was tuned to give $\sim 10^6$ counts/s per detector. Data was acquired for 50 seconds using a time window of 350 ps around the central peak resulting in a visibility value of 0.482. For the data presented in Fig. 2(b), we use an asymmetric Mach-Zehnder interferometer with an added delay of 1 ns in one arm connected to the output of a seeded slave laser. The interference intensity between subsequent pulses is measured using a PIN photodiode and an oscilloscope. The histogram presented is the result of an acquisition of 10^5 points.

ACKNOWLEDGMENTS

L. C. Comandar acknowledges personal support via the EPSRC funded CDT in Photonic Systems Development and Toshiba Research Europe Ltd.

AUTHOR CONTRIBUTIONS

Measurements and calculations were performed by L.C.C. and M.L., respectively. The system was readied by B.F., J.F.D., A.W.S., and S.T. Z.L.Y. and A.J.S. conceived the experiment and guided the work. L.C.C. and M.L. wrote the manuscript with contributions from the other authors. All authors discussed experiments, results and the interpretation of results.

---

[1] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).

[2] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dusek, M., Lütkenhaus, N. & Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).

[3] Gerhardt, I., Liu, Q., Lamas-Linares A., Skaar J., Kurtsiefer C. & Makarov, V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Comm.* **2**, 349 (2011).

[4] Lydersen, L., Wiechers, C., Wittman, C., Elser, D., Skaar, D. & Makarov V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4**, 686 (2010).

[5] Xu, F., Qi, B. & Lo, H.-K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system *New J. Phys.* **12**, 113026 (2010).

[6] Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C. & Lo, H.-K. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems *Phys. Rev. A* **78**, 042333 (2008).

[7] Qi, B., Fung, C.-H. F., Lo, H.-L. & Ma, X. Time-shift attack in practical quantum cryptosystems. *Quant. Inf. Comp.* **7**, 73 (2007).

[8] Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance, *Nature* **509**, 475478 (2014).

[9] Yuan, Z. L., Dynes, J. F., & Shields, A. J. Avoiding the blinding attack in QKD. *Nat. Photon.* **4**, 686 (2010). **4**, 800 (2010).

[10] Fung, C.-H. F., Tamaki, K., Qi, B., Lo, H.-K., & Ma, X. Security proof of quantum key distribution with detection efficiency mismatch, *Quant. Inf. and Comp.* **9**, 131-165 (2009).

[11] Hong, C. K., Ou, Z. Y. & Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 20442046 (1987).

[12] Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).

[13] Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).

[14] Tang, Y.-L., Yin, H.-L., Chen, S.-J., Liu, Y., Zhang, W.-J., Jiang, X., Zhang, L., Wang, J., You, L.-X., Guan, J.-Y., Yang, D.-X., Wang, Z., Liang, H., Zhang, Z., Zhou, N., Ma, X., Chen, T.-Y., Zhang, Q. &

Pan, J.-W. Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.* **113**, 190501 (2014).

[15] Valivarthi, R., Lucio-Martinez, I., Chan, P., Rubenok, A., John, C., Korchinski, D., Duffin, C., Marsili, F., Verma, V., Shaw, M. D., Stern, J. A., Nam, S. W., Oblak, D., Zhou, Q., Slater, J. A. & Tittel, W. Measurement-device-independent quantum key distribution: from idea towards application. *arXiv*, 1501.07307 (2015).

[16] Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111**, 130501 (2013).

[17] Ferreira da Silva, T., Vitoreti, D., Xavier, G. B., do Amaral, G. C., Temporão, G. P. & von der Weid, J. P. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88**, 052303 (2013).

[18] Pirandola, S., Ottaviani, C., Spedalieri, G., Weedbrook, C., Braunstein, S. L., Lloyd, S., Gehring, T., Jacobsen, C. S., & Andersen U. L. High-rate measurement-device-independent quantum cryptography, *Nat. Photon.* **9**, 397402 (2015).

[19] Scarani, V. & Kurtsiefer, C. The black paper of quantum cryptography: Real implementation problems. *Theor. Comp. Sci.* **560**, 27-32 (2014).

[20] Fröhlich, B., Dynes, J. F., Lucamarini, M., Sharpe, A. W., Yuan, Z. L., & Shields, A. J. A quantum access network, *Nature* **501**, 6972 (2013).

[21] Comandar, L. C., Fröhlich, B., Lucamarini, M., Patel, K. A., Sharpe, A. W., Dynes, J. F., Yuan, Z. L., Penty, R. V. & Shields, A. J. Room temperature single-photon detectors for high bit rate quantum key distribution. *App. Phys. Lett.* **104**, 021101 (2014).

[22] Lo, H.-K. & Preskill, J. Security of quantum key distribution using weak coherent states with nonrandom phases. *Quant. Inf. Comput.* **8**, 431 (2007).

[23] Yuan, Z. L., Lucamarini, M., Dynes, J. F., Fröhlich, B., Plews, A., & Shields, A. J. Robust random number generation using steady-state emission of gain-switched laser diodes, *Appl. Phys. Lett.* **104**, 261112 (2014).

[24] Rarity, J. G., Tapster, P. R., & Loudon, R. Non-classical interference between independent sources. *J. Opt. B: Quantum Semiclass. Opt.* **7**, S171 (2005).

[25] Supplementary Information.

[26] Choi, I., Zhou, Y. R., Dynes, J. F., Yuan, Z. L., Klar, A., Sharpe, A. W., Plews, A., Lucamarini, M., Radig, C., Neubert, J., Griesser, H., Eiselt, M., Chunnilall, C., Lepert, G., Sinclair, A., Elbers, J.-P., Lord, A., & Shields, A. J. Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber. *Opt. Express* **22**, 23121-23128 (2014).

[27] Ma, X., Fung, C.H. F., Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 052305 (2012).

[28] Xu, F., Curty, M., Qi, B., Lo, H.-K., Practical aspects of measurement-device-independent quantum key distribution. *New J. Phys.* **15**, 113007-113034 (2013).

[29] Yuan, Z. L., Lucamarini, M., Dynes, J. F., Fröhlich, B., Ward, M. B. & Shields, A. J. Interference of short optical pulses from independent gain-switched laser diodes for quantum secure communications. *Phys. Rev. Applied* **2**, 064006 (2014).

[30] Zhou, Y.-H., Yu, Z.-W. & Wang, X.-B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *arXiv* 1502:01262 (2015).

[31] Comandar, L. C., Fröhlich, B., Dynes, J. F., Sharpe, A. W, Lucamarini, M., Yuan, Z. L., Penty, R. V. & Shields, A. J. Gigahertz-gated InGaAs/InP single-photon detector with detection efficiency exceeding 55% at 1550 nm. *J. App. Phys.* **117**, 083109 (2015).

SUPPLEMENTARY INFORMATION

A. Protocol

To increase the final key rate, we adopt an optimised protocol, similar to the one described in [1]. It makes use of four intensity settings rather than three to decouple the data basis Z from the test basis X. This allows a large photon flux in the Z basis, in the range of 0.7 photons/pulse, thus resulting in a high count rate, in the order of tens of millions counts per second for short distances. It also allows a small photon flux in the X basis, which is optimal for the parameter estimation based on decoy states [2, 3]. Moreover, we perform decoy state estimation through a numerical routine based on linear programming, detailed below. This increases size and stability of the resulting key rate. All the relevant experimental settings and rates for this protocol are given below in Tables II, III, IV, V.

The steps of the protocol are as follows:

Preparation: Alice and Bob prepare phase-randomised weak coherent states with mean photon number μ_i (Alice) and μ_j (Bob). The mean photon number μ_l, $l = \{i, j\}$, is randomly chosen among four possible values [1]: s (signal), u (decoy 1), v (decoy 2), w (vacuum). When $\mu_l = s$, the users randomly assign a polarization state from the Z basis, either H or V. When $\mu_l \neq s$, they randomly assign a polarization state from the X basis, either D or A. They send the resulting state to Charlie with probabilities $p_s = p_Z = 1 - p_X = 45/48$ and $p_u = p_v = p_w = p_X/3$.

Detection and announcement: Charlie performs a Bell measurement on the incoming states. In every run, if at least two detectors click, Charlie publicly announces which detectors clicked. From the announcement, the users draw the successful events, defined as the coincidence counts from

two detectors associated to orthogonal (H/V) polarizations. When more than two detectors are announced, the users draw all pairwise detector events compatible with the announcement. With reference to Fig. 1, a coincidence count from detectors cH/dV or cV/dH (cH/cV or dH/dV) is assigned to the *singlet* state $|\psi^-\rangle = 1/\sqrt{2}(|HV\rangle - |VH\rangle)$ (*triplet* state $|\psi^+\rangle = 1/\sqrt{2}(|HV\rangle + |VH\rangle)$) [4].

Sifting: Alice and Bob announce the bases (Z or X) for all the successful events. They perform sifting by keeping the results whenever they have used identical bases and discard the others. Bob performs a bit flip of all his measured bits, except when the matching basis is X and the successful event is a triplet [4].

Key distillation: From the sifted bits, Alice and Bob quantify the gains $Q_{ZZ}^{(k)}$, $Q_{XX}^{(k)}$ and the error rates $E_{ZZ}^{(k)}$, $E_{XX}^{(k)}$ separately for each basis and for the triplet ($k = T$) and singlet ($k = S$) states. From the X-basis quantities the users estimate the single photon gain $q_X^{(k)}$ and the error rate $e_X^{(k)}$ using the decoy state technique. They then use $q_X^{(k)}$ to infer a lower bound on $q_Z^{(k)}$. The final key rate R of the system is determined by the rate equations: $R = R^{(T)} + R^{(S)}$; $R^{(k)} = q_Z^{(k)}[1 - h(e_X^{(k)})] - f_{EC} Q_{ZZ}^{(k)} h(E_{ZZ}^k)$, where $k = \{T, S\}$, h is the binary entropy function and $f_{EC} = 1.16$ quantifies how close to the Shannon limit the error correction (EC) performs.

Post-processing: The users run error correction, privacy amplification and all the due post-processing to obtain the final key and secure the overall communication. In this protocol, only results from the rectilinear basis are error-corrected and privacy-amplified. Diagonal basis results are used only for the estimation of the single photon quantities and do not contribute to the raw keys.

B. Distillation procedure

In the described protocol, the users distill two separate key rates, one for the singlet ($|\Psi^-\rangle$) and one for the triplet ($|\Psi^+\rangle$) state. The final key rate is given by the sum of the two contributions. Here, we aim to explain the distillation procedure that links the raw count rates to the final key bits. It can be applied to the singlet and triplet data sets separately or to the data set obtained by gathering the data from the two states in a single group. This makes the index k redundant and we drop it from the following discussion. We can then rewrite the key rate equation given above in a more explicit way:

$$R = p_Z^2 \left(s_i e^{-s_i}\right) \left(s_j e^{-s_j}\right) y_Z^{1,1} \left[1 - h\left(e_X^{1,1}\right)\right] - f_{EC} Q_{ZZ}^{s_i,s_j} h\left(E_{ZZ}^{s_i,s_j}\right). \quad (1)$$

In Eq. (1), $Q_{ZZ}^{s_i,s_j}$ and $E_{ZZ}^{s_i,s_j}$ are the gain and the error rate, respectively, measured in the rectilinear basis (see Table III) when Alice (index 'i') and Bob (index 'j') send weak coherent states with mean photon numbers (or "classes") s_i and s_j, respectively. We note that according to our protocol, the 's' class is selected whenever the basis Z is chosen, so the probability p_s to prepare s coincides with p_Z. The key bits are extracted from the s class only, whereas the classes u, v and w are used to perform the decoy state estimation [2, 3]. Because independent weak coherent states are used, the probability that the users simultaneously emit a single photon is the product of two Poisson distributions, which appears in the first pair of brackets in Eq. (1). The quantity $y_Z^{1,1}$ is the single photon yield in the Z basis, i.e., the probability that Charlie declares a detection given that Alice and Bob sent out single photon signals. This quantity is not measurable without true single photon sources and has to be estimated using the decoy state technique. Similarly, the quantity $e_X^{1,1}$ is the single photon error rate, i.e., the probability that the users detect an error from Charlie's declared data given that they sent out single photon signals, and has to be estimated using the decoy state technique.

Decoy state estimation

We perform the decoy state estimation using a constrained optimization numerical routine similar to Ref. [5]. The first step is to estimate a lower bound for the quantity $y_Z^{1,1}$ in Eq. (1), to lower bound the key rate R. This is a typical constrained minimization problem, where $y_Z^{1,1}$ is the objective function and the constraints are given by the counts acquired in the experiment. However, instead of minimizing $y_Z^{1,1}$, we minimize $y_X^{1,1}$, i.e. the single photon yield in the X basis. In the asymptotic limit, this is justified by the equality $y_Z^{1,1} = y_X^{1,1}$. In the finite-size case, we can use the fact that, provided that the sample in the X basis is smaller than the one in the Z basis, the lower bound to $y_X^{1,1}$ also represents a lower bound to $y_Z^{1,1}$ [6]. The condition about the sizes of the two samples in the bases Z and X is fulfilled in our experiment, due to the higher photon flux used in the Z basis.

For the objective function $y_X^{1,1}$, the constraints are given by the coincidence counts in the X basis. By dividing the coincidence counts in the X basis (see Table IV below) by the number of pulses sent by the users in the X basis (see following section), we can obtain the quantities $Q_{XX}^{\mu_i,\mu_j}$, which can be plugged in the following equation [4]:

$$Q_{XX}^{\mu_i,\mu_j} = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty}\left(\frac{\mu_i^m}{m!}e^{-\mu_i}\right)\left(\frac{\mu_j^n}{n!}e^{-\mu_j}\right)y_X^{m,n}.$$

Here, m and n indicate the number of photons emitted by Alice and Bob, respectively. When μ_i and μ_j run over u, v and w, we obtain 9 independent equations, representing the constraints of the problem. We can rewrite the constraints as:

$$\begin{aligned} Q_{XX}^{\mu_i,\mu_j} e^{\mu_i} e^{\mu_j} &= \sum_{m,n=0}^{\infty} \frac{\mu_i^m}{m!} \frac{\mu_j^n}{n!} y_X^{m,n} \\ &= \sum_{m,n=0}^{K} \frac{\mu_i^m}{m!} \frac{\mu_j^n}{n!} y_X^{m,n} + \sum_{m=0}^{K} \sum_{n=K+1}^{\infty} \frac{\mu_i^m}{m!} \frac{\mu_j^n}{n!} y_X^{m,n} + \\ &+ \sum_{m=K+1}^{\infty} \sum_{n=0}^{K} \frac{\mu_i^m}{m!} \frac{\mu_j^n}{n!} y_X^{m,n} + \sum_{m,n=K+1}^{\infty} \frac{\mu_i^m}{m!} \frac{\mu_j^n}{n!} y_X^{m,n} \end{aligned}$$

From the above equation, the following bounds can be obtained:

$$\sum_{m,n=0}^{K} \frac{\mu_i^m}{m!} \frac{\mu_j^n}{n!} y_X^{m,n} \leq e^{\mu_i} e^{\mu_j} Q_{XX}^{\mu_i,\mu_j}, \tag{2}$$

$$\sum_{m,n=0}^{K} \frac{\mu_i^m}{m!} \frac{\mu_j^n}{n!} y_X^{m,n} \geq e^{\mu_i} e^{\mu_j} \left[Q_{XX}^{\mu_i,\mu_j} - \left(1 - \frac{\Gamma\left(1+K,\mu_i\right)}{K!} \frac{\Gamma\left(1+K,\mu_j\right)}{K!} \right) \right], \tag{3}$$

where $\Gamma\left(a,b\right) = \int_b^{\infty} t^{a-1} e^{-t} dt$ is the incomplete gamma function. Eqs. (2), (3) represent a total of $9 + 9 = 18$ constraints. However, as it can be seen from Table IV, the counts obtained from the classes vw, wv and ww are much fewer than those from the other classes, leading to larger statistical fluctuations. In this case, we found it advantageous to combine the counts from these classes and rewrite the associated constraints in a single cumulative constraint (see also [7]). This reduces the total number of constraints for the above-described problem to $7 + 7 = 14$. Finally, in addition to Eqs. (2), (3), we also set the condition that the yields are probabilities, i.e., $y_X^{m,n} \in [0,1]$ for every m, n.

For the single photon error rate we adopt a procedure similar to the one just described. This time, we need to maximize the quantity $e_X^{1,1}$. The constraints are given by the following equations [4]:

$$Q_{XX}^{\mu_i,\mu_j} E_{XX}^{\mu_i,\mu_j} = e^{-\mu_i} e^{-\mu_j} \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} \frac{\mu_i^m}{m!} \frac{\mu_j^n}{n!} y_X^{m,n} e_X^{m,n},$$

which leads to the following bound:

$$\begin{aligned} Q_{XX}^{\mu_i,\mu_j} E_{XX}^{\mu_i,\mu_j} e^{\mu_i} e^{\mu_j} &= \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} \frac{\mu_i^m}{m!}\frac{\mu_j^n}{n!} y_X^{m,n} e_X^{m,n} \\ &= y_X^{0,0} e_X^{0,0} + \sum_{n=1}^{\infty} \frac{\mu_j^n}{n!} y_X^{0,n} e_X^{0,n} + \sum_{m=1}^{\infty} \frac{\mu_i^m}{m!} y_X^{m,0} e_X^{m,0} + \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} \frac{\mu_i^m}{m!}\frac{\mu_j^n}{n!} y_X^{m,n} e_X^{m,n} \\ &= \frac{1}{2} y_X^{0,0} + \frac{1}{2}\sum_{n=1}^{\infty} \frac{\mu_j^n}{n!} y_X^{0,n} + \frac{1}{2}\sum_{m=1}^{\infty} \frac{\mu_i^m}{m!} y_X^{m,0} + \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} \frac{\mu_i^m}{m!}\frac{\mu_j^n}{n!} y_X^{m,n} e_X^{m,n} \\ &\geq \frac{1}{2} y_X^{0,0} + \frac{1}{2}\sum_{n=1}^{K} \frac{\mu_j^n}{n!} y_X^{0,n} + \frac{1}{2}\sum_{m=1}^{K} \frac{\mu_i^m}{m!} y_X^{m,0} + \sum_{m=1}^{J}\sum_{n=1}^{J} \frac{\mu_i^m}{m!}\frac{\mu_j^n}{n!} y_X^{m,n} e_X^{m,n}. \end{aligned} \tag{4}$$

In the third line we set $e_X^{0,0} = e_X^{0,n} = e_X^{m,0} = \frac{1}{2}$ and in the last line we have dropped some non-negative terms from the sum. From the last line of Eq. (4), we carry on only the terms corresponding to $J = 1$ and drop all the remaining ones. Because the dropped terms are non-negative, we can write:

$$Q_{XX}^{\mu_i,\mu_j} E_{XX}^{\mu_i,\mu_j} e^{\mu_i} e^{\mu_j} \geq \frac{1}{2} y_X^{0,0} + \frac{1}{2}\sum_{n=1}^{K} \frac{\mu_j^n}{n!} y_X^{0,n} + \frac{1}{2}\sum_{m=1}^{K} \frac{\mu_i^m}{m!} y_X^{m,0} + \mu_i\mu_j y_X^{1,1} e_X^{1,1}. \tag{5}$$

This can be rewritten as:

$$\begin{aligned} e_X^{1,1} &\leq \frac{1}{\mu_i\mu_j y_X^{1,1}} \left(Q_{XX}^{\mu_i,\mu_j} E_{XX}^{\mu_i,\mu_j} e^{\mu_i} e^{\mu_j} - \frac{1}{2} y_X^{0,0} - \frac{1}{2}\sum_{n=1}^{K} \frac{\mu_j^n}{n!} y_X^{0,n} - \frac{1}{2}\sum_{m=1}^{K} \frac{\mu_i^m}{m!} y_X^{m,0} \right) \\ &\leq \frac{1}{\mu_i\mu_j \underline{y_X^{1,1}}} \left(Q_{XX}^{\mu_i,\mu_j} E_{XX}^{\mu_i,\mu_j} e^{\mu_i} e^{\mu_j} - \frac{1}{2} y_X^{0,0} - \frac{1}{2}\sum_{n=1}^{K} \frac{\mu_j^n}{n!} y_X^{0,n} - \frac{1}{2}\sum_{m=1}^{K} \frac{\mu_i^m}{m!} y_X^{m,0} \right), \end{aligned} \tag{6}$$

where in the last line we have indicated with $\underline{y_X^{1,1}}$ the lower bound to $y_X^{1,1}$ obtained in the previous yield minimization problem. Eq. (6) represents a set of 9 constraints. As mentioned for the single photon yield optimization problem, the data sets obtained from the classes vw, wv and ww are much smaller than the others, so it is beneficial to gather them. We write explicitly the constraints for the least significant classes:

$$\begin{aligned} e_X^{1,1} &\leq \frac{1}{\underline{y_X^{1,1}}} \times \frac{1}{vw} \left(Q_{XX}^{vw} E_{XX}^{vw} e^v e^w - \frac{1}{2} y_X^{0,0} - \frac{1}{2}\sum_{m=1}^{K} \frac{v^m}{m!} y_X^{m,0} - \frac{1}{2}\sum_{n=1}^{K} \frac{w^n}{n!} y_X^{0,n} \right) \\ e_X^{1,1} &\leq \frac{1}{\underline{y_X^{1,1}}} \times \frac{1}{wv} \left(Q_{XX}^{wv} E_{XX}^{wv} e^w e^v - \frac{1}{2} y_X^{0,0} - \frac{1}{2}\sum_{m=1}^{K} \frac{w^m}{m!} y_X^{m,0} - \frac{1}{2}\sum_{n=1}^{K} \frac{v^n}{n!} y_X^{0,n} \right) \\ e_X^{1,1} &\leq \frac{1}{\underline{y_X^{1,1}}} \times \frac{1}{w^2} \left(Q_{XX}^{ww} E_{XX}^{ww} e^{2w} - \frac{1}{2} y_X^{0,0} - \frac{1}{2}\sum_{m=1}^{K} \frac{w^m}{m!} y_X^{m,0} - \frac{1}{2}\sum_{n=1}^{K} \frac{w^n}{n!} y_X^{0,n} \right) \end{aligned}$$

By adding the three inequalities above we obtain the following cumulative constraint:

$$e_X^{1,1} \leq \frac{1}{3\underline{y_X^{1,1}}}\left[\frac{1}{vw}\left(Q_{XX}^{vw}E_{XX}^{vw}e^v e^w - \frac{1}{2}\sum_{m=0}^{K}\frac{v^m}{m!}y_X^{m,0} - \frac{1}{2}\sum_{n=1}^{K}\frac{w^n}{n!}y_X^{0,n}\right) + \right.$$
$$+\frac{1}{wv}\left(Q_{XX}^{wv}E_{XX}^{wv}e^w e^v - \frac{1}{2}\sum_{m=0}^{K}\frac{w^m}{m!}y_X^{m,0} - \frac{1}{2}\sum_{n=1}^{K}\frac{v^n}{n!}y_X^{0,n}\right) +$$
$$\left.+\frac{1}{w^2}\left(Q_{XX}^{ww}E_{XX}^{ww}e^{2w} - \frac{1}{2}\sum_{m=0}^{K}\frac{w^m}{m!}y_X^{m,0} - \frac{1}{2}\sum_{n=1}^{K}\frac{w^n}{n!}y_X^{0,n}\right)\right]. \tag{7}$$

The 7 constraints given in Eqs. (6) and (7) have to be added to the 14 specified for the yields in Eqs. (2) and (3) (including the mentioned cumulative constraint), thus providing a total of 21 constraints for the maximization of $e_X^{1,1}$. In addition to these constraints, we also specify in the problem the range of the quantities $y_X^{m,n}$, which is the closed interval $[0, 1]$.

Finite size key rate

To derive the secure key rate in the presence of the statistical fluctuations of the finite sample, we follow the approach in Ref. [8] (see also [9] for a detailed analysis of this subject). We assume that the statistical fluctuations obey a Gaussian distribution [10]. Therefore it is possible to set the desired failure probability ε of the estimation procedure by solving the equation $1-\mathrm{erf}\left(n/\sqrt{2}\right) = \varepsilon$, where n is the (not necessarily integer) number of standard deviations adding up to form the statistical error of the measured value. We find it convenient to set $n = 7$ and obtain $\varepsilon = 2.56 \times 10^{-12}$. Because in our decoy state estimation we use 21 constraints, this choice assures that the overall failure probability of the estimation of the parameters is less than 5.4×10^{-11}.

We then consider the fluctuation function:

$$F(x, n) = \frac{n}{\sqrt{x}}, \tag{8}$$

where x represents the size of the considered data sample. This function is used to make the constraints in the optimization problems for $y_X^{1,1}$ and $e_X^{1,1}$ looser. For example, the inequality in Eq. (2)

$$\sum_{m,n=0}^{K}\frac{\mu_i^m}{m!}\frac{\mu_j^n}{n!}y_X^{m,n} \leq e^{\mu_i}e^{\mu_j}Q_{XX}^{\mu_i,\mu_j}$$

in the finite-size scenario becomes:

$$\sum_{m,n=0}^{K}\frac{u^m}{m!}\frac{v^n}{n!}y_X^{m,n} \leq e^u e^v Q_{XX}^{u,v}\left[1 + F\left(N_{XX}^{u,v}Q_{XX}^{u,v}, 7\right)\right],$$

where $N_{XX}^{u,v}$ is the total number of runs where Alice and Bob emitted pulses in the class u and v, respectively. Because the resulting constraint is looser, the finite-size solution is always worse than the one in the asymptotic scenario, and the key rate is reduced. This explains why the finite-size key rate for a channel attenuation of 2.33 dB is about 30% of the asymptotic key rate when the total size of the sample is $\sim 2.4\times10^7$ (see Table IV). The presence of a factor $\sqrt{x}$ in the fluctuation function F, Eq. (8), explicitly shows that it is always best to gather the counts from the singlet and triplet data sets in a single group to maximize the finite-size key rate. Because the sizes of the separate triplet and singlet data sets are approximately equal, the size of the total sample is about twice as large as the separate samples. This, according to Eq. (8), entails a factor $\sqrt{2}$ advantage in the key rate if the total sample is used.

The key rate obtained by joining the data sets from the singlet and the triplet states amounts to 366 kbit/s. The number of prepared pulses are $N_{XX}^{u,u} = N_{XX}^{u,v} = N_{XX}^{u,w} = N_{XX}^{v,u} = N_{XX}^{w,u} = (5\times10^2)\times(4\times10^9)$, acquired in 500 seconds, and $N_{XX}^{v,v} = N_{XX}^{v,w} = N_{XX}^{w,v} = N_{XX}^{w,w} = (1.25\times10^2)\times(4\times10^9)$, acquired in 125 seconds, where $N_{XX}^{\mu_i,\mu_j}$ is the total number of runs where Alice and Bob simultaneously emitted pulses in the class μ_i and μ_j, respectively.

C. Key rates

Channel attenuation/distance	Key rate [kbit/s]
2.33 dB (11.65 km)	1256.5
2.33 dB (11.65 km) | Finite size	366.3
6.15 dB (30.75 km)	325.8
9.82 dB (49.10 km)	98.2
50 km (9.65 dB) | Real fibre	98.4
15.97 dB (79.85 km)	15.9
20.98 dB (104.9 km)	4.2

TABLE II. Key rate R versus channel attenuation (dB) or equivalent distance (km) in a single mode optical fibre featuring 0.2 dB/km attenuation.

D. Count and error rates in the rectilinear basis

Channel attenuation/distance	Singlet $\|\Psi^-\rangle$		Triplet $\|\Psi^+\rangle$		$s_A = s_B$
	$C_{ZZ}^{(S)}$	$E_{ZZ}^{(S)}$	$C_{ZZ}^{(T)}$	$E_{ZZ}^{(T)}$	ph/pulse
2.33 dB (11.65 km)	288399	0.33%	287902	0.35%	0.7
2.33 dB (11.65 km) — Finite size	307574	0.29%	308259	0.25%	0.7
6.15 dB (30.75 km)	139817	0.47%	139345	0.52%	0.7
9.82 dB (49.10 km)	39881	0.61%	39993	0.63%	0.7
50 km (9.65 dB) — Real fibre	53411	0.81%	54058	0.86%	0.7
15.97 dB (79.85 km)	14704	0.95%	14657	1.14%	0.6
20.98 dB (104.9 km)	3238	1.20%	3211	0.97%	0.55

TABLE III. Measured coincidence counts (C_{ZZ}) and error rates (E_{ZZ}) in the rectilinear basis, separately for the singlet and the triplet states. Acquisition time is 80 ms for each attenuation/distance value.

E. Count rates in the diagonal basis

Channel attenuation/distance		Singlet $\|\Psi^-\rangle$			Triplet $\|\Psi^+\rangle$			$\mu_i = \mu_j$
	Class	u	v	w	u	v	w	ph/pulse
2.33 dB (11.65 km)	u	223041	92393	80410	225777	93290	80759	0.01
	v	84703	14119	9514	85996	14362	9780	0.002
	w	71263	9218	5516	72727	9353	5778	0.001
2.33 dB (11.65 km) — Finite size	u	4771407	1967827	1693057	4853012	1969107	1690185	0.01
	v	1774040	73783	47749	1773149	73789	48136	0.002
	w	1506023	46317	27113	1510257	46591	27348	0.001
6.15 dB (30.75 km)	u	218848	79813	67269	222021	80688	67866	0.016
	v	93154	13655	8681	93588	13955	8710	0.0032
	w	80250	9458	5276	81479	9410	5377	0.0016
9.82 dB (49.10 km)	u	170331	69123	59436	174234	70675	60709	0.025
	v	67118	11298	7674	68020	11749	7831	0.005
	w	57570	7397	4694	57787	7526	4759	0.0025
50 km (9.65 dB) — Real fibre	u	239876	98512	85722	244648	98477	85958	0.025
	v	88586	14526	9854	89817	14946	9721	0.005
	w	74187	9310	5604	74644	9275	5745	0.0025
15.97 dB (79.85 km)	u	226108	82071	69065	225133	83685	70665	0.05
	v	88114	11477	6971	87615	11730	7033	0.01
	w	74616	7051	3401	75312	7078	3461	0.005
20.98 dB (104.9 km)	u	142656	50799	42995	145584	52744	44096	0.08
	v	56455	7057	4233	57492	7308	4322	0.0155
	w	48101	4391	2237	49104	4578	2211	0.008

TABLE IV. Measured coincidence counts in the diagonal basis (C_{XX}) separately for the singlet and the triplet states. Acquisition time is 25 seconds per combination, with the exception of the line containing the finite-size data. There the total sample was acquired in 12,000 seconds.

F. Error rates in the diagonal basis

Channel attenuation/distance		Singlet $\|\Psi^-\rangle$			Triplet $\|\Psi^+\rangle$			$\mu_i = \mu_j$
	Class	u	v	w	u	v	w	ph/pulse
2.33 dB (11.65 km)	u	31.82%	41.60%	45.37%	31.55%	40.77%	44.36%	0.01
	v	40.17%	38.39%	42.21%	40.67%	37.68%	41.95%	0.002
	w	44.07%	41.53%	43.22%	44.55%	41.28%	42.13%	0.001
2.33 dB (11.65 km) — Finite size	u	33.12%	41.20%	44.90%	32.08%	41.62%	45.33%	0.01
	v	40.95%	38.98%	41.64%	40.56%	38.98%	41.49%	0.002
	w	45.79%	41.30%	42.61%	43.93%	41.63%	43.39%	0.001
6.15 dB (30.75 km)	u	32.81%	40.06%	44.66%	30.83%	39.92%	43.54%	0.016
	v	41.56%	38.22%	41.25%	41.06%	37.46%	41.00%	0.0032
	w	45.06%	42.17%	43.33%	45.01%	39.90%	41.27%	0.0016
9.82 dB (49.10 km)	u	32.69%	41.94%	45.88%	32.42%	41.32%	44.08%	0.025
	v	41.41%	40.23%	42.39%	40.92%	40.07%	41.21%	0.005
	w	45.17%	43.75%	44.91%	44.90%	40.95%	43.12%	0.0025
50 km (9.65 dB) — Real fibre	u	32.72%	42.87%	46.10%	31.45%	41.25%	44.68%	0.025
	v	39.98%	39.60%	43.00%	40.96%	37.68%	42.41%	0.005
	w	43.21%	40.49%	42.95%	45.29%	42.24%	43.19%	0.0025
15.97 dB (79.85 km)	u	30.39%	39.77%	44.48%	31.71%	38.75%	43.13%	0.05
	v	39.30%	34.94%	37.56%	41.35%	34.53%	36.93%	0.01
	w	43.31%	38.15%	37.31%	45.25%	36.54%	39.12%	0.005
20.98 dB (104.9 km)	u	32.09%	40.09%	44.18%	30.83%	39.69%	44.12%	0.08
	v	41.70%	35.47%	37.04%	39.42%	34.21%	37.58%	0.0155
	w	45.32%	37.94%	37.33%	43.24%	37.27%	36.27%	0.008

TABLE V. Measured error rates (E_{XX}) in the diagonal basis separately for the singlet and the triplet states. Acquisition times are as in Table IV.

G. Theoretical estimation of the visibility

The two-photon interference visibility $V(\sigma_\tau, \Delta v)$ obtained from two independent gain-switched laser diodes is a function of the time jitter τ and of the bandwidth $\Delta\nu$ of the interfering pulses, which are reported on the horizontal and vertical axis of Fig. 2(a) in the main text, respectively. Their values for the slave lasers in our setup, with and without the pulse laser seeding technique, have been measured and are given as abscissas and ordinates, respectively, of the two empty circles in the figure. The time jitter is assumed to follow a Normal distribution $N_\tau(0, \sigma_\tau)$ centred at 0. The visibility is plotted from the expression:

$$\widetilde{V}(\sigma_\tau, \Delta v) = \int_{-\infty}^{\infty} d\tau V(\tau, \Delta v) N_\tau(0, \sigma_\tau),$$

where

$$V(\tau, \Delta v) = \frac{1}{2} \exp\left[-\frac{\tau^2 + 4(\omega_{ij} + 2\tau\beta)^2 \sigma_t^4}{4\sigma_t^2}\right]. \tag{9}$$

The quantity $V(\tau, \Delta v)$ in Eq. (9) is obtained from the electric fields

$$\xi_l(t) = \sqrt{I(t)} e^{i\left(\omega_l t + \beta t^2 + \theta_l\right)}$$

emitted by Alice ($l = i$) and Bob ($l = j$), which are used to estimate the coincidence counts at Charlie's detectors [11, 12]. The random variable τ in Eq. (9) represents the total time jitter between the two pulses emitted by the users measured from Charlie's beam splitter; $\omega_{ij} = 2\pi(\nu_j - \nu_i)$ accounts for the (small) difference in the central frequencies ν_i and ν_j of the interfering pulses emitted by Alice and Bob, respectively; σ_t is the standard deviation of the optical pulses having intensity profile $I(t)$, assumed be Gaussian, and are related to the measurable full-width-at-half-maximum of the pulses, Δt, by the relation $\sigma_t = \Delta t / \left(2\sqrt{2\ln 2}\right)$. The parameter β accounts for the frequency chirp. We assume that frequency chirp is the only cause of a bandwidth larger than the one prescribed by the time-bandwidth product. In this case it can be shown that $\Delta v = \Delta v^{(0)} \sqrt{1 + 16\beta^2 \sigma_t^4}$ [13]. By measuring σ_t and the time-bandwidth product of the emitted pulses, it is possible to invert this relation and determine the parameter β.

---

[1] Zhou, Y.-H., Yu, Z.-W. & Wang, X.-B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *arXiv* 1502:01262 (2015).

[2] Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).

[3] Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).

[4] Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).

[5] Lucamarini, M., Patel, K. A., Dynes, J. F., Fröhlich, B., Sharpe, A. W., Dixon, A. R., Yuan, Z. L., Penty, R. V., & Shields, A. J. Efficient decoy-state quantum key distribution with quantified security. *Opt. Express* **21**, 24550-24565 (2013).

[6] Lucamarini, M., Dynes, J. F., Fröhlich, B., Yuan, Z. L., & Shields, A. J. Security bounds for efficient decoy-state quantum key distribution. *IEEE J. Sel. Topics Quantum Electron.* **21**, 1-8 (2015).

[7] Yu, Z.-W., Zhou, Y.-H., & Wang, X.-B. Improved statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method. *arXiv* 1410.3265 (2014).

[8] Ma, X., Fung, C.H. F., Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 052305 (2012).

[9] Curty, M., Xu, F., Cui, W., Lim, C. C. W., Tamaki, K. & Lo, H.-K. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Comm.* **5**, 3732 (2014).

[10] Ma, X., Qi, B., Zhao, Y., Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).

[11] Xu, F., Curty, M., Qi, B., Lo, H.-K., Practical aspects of measurement-device-independent quantum key distribution. *New J. Phys.* **15**, 113007-113034 (2013).

[12] Yuan, Z. L., Lucamarini, M., Dynes, J. F., Fröhlich, B., Ward, M. B. & Shields, A. J. Interference of short optical pulses from independent gain-switched laser diodes for quantum secure communications. *Phys. Rev. Applied* **2**, 064006 (2014).

[13] Agrawal, G. P. Fiber-optic Communication Systems, 3rd Edition. Wiley Series in Microwave and Optical Engineering (2002).