Quantum key distribution without detector vulnerabilities using optically seeded lasers

L. C. Comandari, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty and A. J. Shields

Security in quantum cryptography is continuously challenged by inventive attacks targeting the real components of a cryptographic set-up, and duly restored by new countermeasures to foil them. Owing to their high sensitivity and complex design, detectors are the most frequently attacked components. It was recently shown that two-photon interference from independent light sources can be used to remove any vulnerability from detectors. This new form of detection-safe quantum key distribution (QKD), termed measurement-device-independent (MDI), has been experimentally demonstrated with modest key rates. Here, we introduce a new pulsed laser seeding technique to obtain high-visibility interference from gain-switched lasers and thereby perform MDI-QKD with unprecedented key rates in excess of 1 megabit per second in the finite-size regime. This represents a two to six orders of magnitude improvement over existing implementations and supports the new scheme as a practical resource for secure quantum communications.

In QKD a sender, Alice, transmits encoded quantum signals to a receiver, Bob, who measures them and distills a secret string of bits with the sender via public discussion. Ideally, the use of quantum signals guarantees the information-theoretical security of the communication. In practice, however, QKD 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.

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. MDI-QKD is a recent advance conceived to remove the problem of detector vulnerability. As depicted in Fig. 1a, 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, 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 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, each users’ apparatus no longer needs a detector and the detection vulnerability of QKD is removed.

This striking feature of MDI-QKD has fostered intense experimental work and various demonstrations have been provided. 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 a few hundreds bps or less (see Table 1). A proof-of-principle demonstration was also recently published using continuous variables.

Here we demonstrate a new 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, to achieve QKD immune to detector attacks at key rates exceeding 1 Mbps for the first time, also in the finite-size regime. This is orders of magnitude higher than in previous demonstrations and is comparable to the highest values achieved for conventional QKD. Furthermore we demonstrate operation with a channel loss greater than 20 dB, corresponding to over 100 km of standard fibre, with a rigorous treatment of the finite-size effect. Implementation with real fibre has also been considered.

To suit MDI-QKD, the light sources in Alice and Bob have to match stringent criteria. They should emit indistinguishable pulses to enable high-visibility two-photon interference and at the same time each pulse should display a random optical phase to meet a fundamental security condition. In most demonstrations so far, light pulses have been carved from a continuous-wave laser. However, the pulses generated this way have a constant or slowly varying optical phase due to the random nature of the spontaneous emission that starts 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 to dramatically reduce the visibility of the interference. This has so far prevented the use of gain-switched laser diodes to achieve high-speed MDI-QKD.

Here we propose a new technique based on pulsed laser seeding (PLS) 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 slave laser through an optical circulator, see Fig. 1b and Methods. 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 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, PLS guarantees that the phase of each slave laser is inherited from its own master laser. Owing to
the fact that the master laser is gain-switched, the master pulse—and hence the slave pulse—has a random optical phase.\(^5\) The improvement in the interference visibility achieved via the PLS technique is visible in Fig. 2a, where the time jitter, bandwidth and visibility of the light sources are experimentally measured and compared against the theoretical prediction.\(^26\) Without PLS, the 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 (upper right corner of the figure). With PLS, on the contrary, they become as small as 4.4 ps and 15 GHz, respectively (lower left corner of the figure). For these values, we expect an interference visibility of 48.5%, in good agreement with the experimentally measured value of 48.2% and close to the theoretical maximum of 50%\(^27\). The phase randomization of the pulses emitted by the seeded slave laser is confirmed in Fig. 2b, where the intensity probability distribution has the typical profile expected from the interference of two pulses with random relative phase.\(^5\)

We performed a series of MDI-QKD experiments using the setup in Fig. 1b (see Methods). The results are summarized in Fig. 3 (see also Table 1 and Supplementary Table I). The data points are obtained by using variable attenuators to reproduce the attenuation of standard single mode fibres (0.2 dB km\(^{-1}\)). The secure key rates in the figure are distilled using the protocol introduced in ref. 28 and detailed in Supplementary Section A. The highest leftmost point corresponds to a rate of 1.660 Mbps, a record in terms of a key rate mediated by two-photon interference. The lowest rightmost point corresponds to about 2 kbps over 20.4 dB attenuation in the finite-size regime, which is still sufficient to generate a 256-bit advanced encryption standard key more frequently than every 200 ms (ref. 29). To maximize the key rate, we chose two different sets of experimental conditions. The operation temperature of the single photon detectors, initially set at 20 °C, is lowered to 0 °C for the points with the highest attenuation to reduce the dark count noise. The resulting data sets belong, de facto, to two different experiments, as is apparent from the figure.

As an extra modification, we increased the photon flux with the channel attenuation to keep the size of the sample approximately invariant for a constant acquisition time (see Supplementary Tables II–IV). It is worth noting that this does not affect the security level, which remains the same (epsilon value equal to 10\(^{-10}\)) irrespective of the sample size. To calculate the finite-size key rate, we use two different methods. The first\(^8\) (filled dots in Fig. 3) has been adopted in previous MDI-QKD experiments\(^5,17\) and allows a direct comparison with the state-of-the-art method. The second\(^8\) (open dots in Fig. 3) guarantees composable security against the most general eavesdropping strategy and provides a positive key rate for the first time in this study.

To replicate a realistic 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 (star in Fig. 3) is close to the one obtained from the channel attenuation, proving that fibre-induced effects can be effectively mitigated.

---

**Table 1 | Selection of existing MDI-QKD experiments with the highest key rate and comparison with this work.**

| Light source | Clock rate (MHz) | Pulse width (ps) | Equivalent distance (km) | Max. key rate (bps) | Notes |
|--------------|-----------------|------------------|--------------------------|---------------------|-------|
| Master & Slave | 1 GHz          | 35               | 0                        | 6.7 × 10\(^6\)     | PR, 2× SSPD, finite size, real fibre |
| Present study | 1,000           | 35               | 0                        | 6.7 × 10\(^6\)     | PLS   |
| Ref. 18      | 75              | 2,500            | 50                       | 3.4 × 10\(^5\)     | PR, 2× APD, real fibre |
| Ref. 19      | 2               | 250              | 45                       | 6.2 × 10\(^2\)     | Single laser source, 2× SSPD |
| Ref. 14      | 2               | 290              | 80                       | 3 × 10\(^0\)       | No PR, 2× APD, real fibre |
| Ref. 16      | 1               | 500              | 45                       | 1 × 10\(^5\)       | No PR, 4× APD, real fibre |
|               | 1               | 1,500            | 17                       | 1.660 × 10\(^6\)   | PR, 4× 20 °C SD-APD, PLS |
|               | 1               | 35               | 0                        | 1.286 × 10\(^6\)   | + finite size |
|               | 1               | 35               | 52                       | 9.7 × 10\(^6\)     | PR, 4× 20 °C SD-APD, PLS |
|               | 1               | 80               | 80                       | 1.5 × 10\(^8\)     | PR, 4× 0 °C SD-APD, PLS |

---

(a) The phase-randomized weak coherent optical pulses are generated by Alice and Bob, set to the desired polarization (whose basis states are labeled H and V) and intensity, then sent to Charlie. There they interfere at the beam splitter (BS), pass through the polarizing beam splitters (PBS) and reach the four detectors, where they are measured in coincidence (details in Supplementary Section A). The measurement outcomes are publicly announced by Charlie, thus letting Alice and Bob reconstruct their keys. (b) The experimental implementation of the scheme in (a) is shown. The light sources, which are essential to the results in this work, are enclosed by the dashed lines in Alice’s and Bob’s units. C, circulator; FBG, fibre Bragg grating; POL, polarization control; INT, intensity control.
The small discrepancy is ascribable to a slightly different photon flux used in the fibre-based experiment. All the experimental points have been numerically simulated\textsuperscript{26,32} to confirm the results and optimize the system (dashed lines in Fig. 3).

Finally, to illustrate the progress entailed by these results, we include in the figure the current highest-observed key rate of QKD in the finite-size scenario\textsuperscript{23} for a distance of 50 km under similar detection conditions to the present experiment. The QKD key rate is impressively only one order of magnitude higher than the corresponding MDI-QKD rate with no finite-size effect, and about 50 times higher than the MDI-QKD point derived from a comparable finite-size analysis. These results prove that PLS can greatly enhance the key rate of MDI-QKD, allowing high-visibility two-photon interference at large repetition rates. This is accompanied by the emission of narrow pulses, which is an important factor for achieving high single-photon detection efficiency\textsuperscript{33}. With these techniques, MDI-QKD can distribute keys at rates commensurate to conventional QKD and approach applications in real-world secure communications.

**Methods**

Methods and any associated references are available in the online version of the paper.

Received 8 October 2015; accepted 24 February 2016; published online 4 April 2016

**References**

1. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. Rev. Mod. Phys. 74, 145–195 (2002).
2. Scarani, V. et al. The security of practical quantum key distribution. Rev. Mod. Phys. 81, 1301–1350 (2009).
3. Gerhardt, I. et al. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nature Commun. 2, 349 (2011).
4. Lydersen, L. et al. Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photon. 4, 686–689 (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 cryptography systems. Quantum Inf. Comput. 7, 73–82 (2007).
8. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. Nature Photon. 8, 475–478 (2014).
9. Yuan, Z. L., Dynes, J. F. & Shields, A. J. Avoiding the blinding attack in QKD. Nature Photon. 4, 800–801 (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. Quantum Inf. Comput. 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, 2044–2046 (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. 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).
15. Fröhlich, B. et al. Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111**, 130502 (2013).
16. Pirandola, S. et al. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88**, 052303 (2013).
17. Tang, Z. et al. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **112**, 190503 (2014).
18. Tang, Y.-L. et al. Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.* **113**, 190501 (2014).
19. Valivarthi, R. et al. Measurement-device-independent quantum key distribution: from idea towards application. *J. Mod. Optic.* **62**, 1141–1150 (2015).
20. Scarran, V. & Kurtsiefer, C. The black paper of quantum cryptography: real implementation problems. *Theor. Comput. Sci.* **560**, 27–32 (2014).
21. Fröhlich, B. et al. A quantum access network. *Nature* **501**, 69–72 (2013).
22. Pirandola, S. et al. High-rate measurement-device-independent quantum cryptography. *Nature Photon.* **9**, 397–402 (2015).
23. Comandar, L. C. et al. Room temperature single-photon detectors for high bit rate quantum key distribution. *Appl. Phys. Lett.* **104**, 021101 (2014).
24. Lo, H.-K. & Preskill, J. Security of quantum key distribution using weak coherent states with nonrandom phases. *Quantum Inf. Comput.* **8**, 431–458 (2007).
25. Yuan, Z. L. et al. Robust random number generation using steady-state emission of gain-switched laser diodes. *Appl. Phys. Lett.* **104**, 261112 (2014).
26. Yuan, Z. L. et al. Interference of short optical pulses from independent gain-switched laser diodes for quantum secure communications. *Phys. Rev. Appl.* **2**, 064006 (2014).
27. Rarity, J. G., Tapster, P. R. & Loudon, R. Non-classical interference between independent sources. *J. Opt. B* **7**, S171–S175 (2005).
28. Zhou, Y.-H., Yu, Z.-W. & Wang, X.-B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. Preprint at http://arxiv.org/abs/1502.01262 (2015).
29. Choi, I. et al. Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber. *Opt. Express* **22**, 23121–23128 (2014).
30. Ma, X., Fung, C. H. F. & Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 052305 (2012).
31. Curty, M. et al. Finite-key analysis for measurement-device-independent quantum key distribution. *Nature Commun.* **5**, 3732 (2014).
32. Xu, F., Curty, M., Qi, B. & Lo, H.-K. Practical aspects of measurement-device-independent quantum key distribution. *New J. Phys.* **15**, 113007 (2013).
33. Comandar, L. C. et al. Gigahertz-gated InGaAs/InP single-photon detector with detection efficiency exceeding 55% at 1550 nm. *J. App. Phys.* **117**, 083109 (2015).

**Acknowledgements**
The authors acknowledge useful discussions with M. Curty. L.C.C. acknowledges personal support via the Engineering and Physical Sciences Research Council funded Centre for Doctoral Training in Photonic Systems Development and Toshiba Research Europe.

**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., L.C.C. and S.W.-B.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.

**Additional information**
Supplementary information is available in the online version of the paper. Reprints and permissions information is available online at www.nature.com/reprints. Correspondence and requests for materials should be addressed to M.L.

**Competing financial interests**
The authors declare no competing financial interests.
**Methods**

**Experimental set-up.** Alice and Bob consist of two independent PLS-enabled light sources producing phase-randomized 35 ps-long laser pulses at 1,550 nm and a repetition rate of 1 GHz. Variable optical band pass filters with a 20 GHz nominal bandwidth are aligned to remove any spurious emission. Fibre Bragg gratings are added to pre-compensate for the pulse broadening in the fibre experiment. The 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 selected with a fixed probability equal to 15/16 and is used to distil the key bits, whereas the X basis is selected with probability 1/16 and is used to test the noise on the quantum channel. The users send the resulting states to Charlie, who performs a Bell measurement of the incoming states. Alice, Bob and Charlie share a common reference clock electrically distributed to which their preparation and detection equipment is synchronized. This enables them (using a real-time feedback) to align and compensate any temporal drifts. In future implementations the clock can be wavelength-multiplexed with the quantum signal or distributed on a different fibre, as routinely done in QKD experiments. 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 synchronized to the arrival time of the photons with a 1 ns intrinsic deadtime. The detectors have an effective active window of around 100 ps and are able to measure up to 500 Mbps (ref. 33). Their efficiency is kept around 30% for all the data points in 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, whereas for larger attenuation values it is beneficial to operate them at 0 °C to produce a smaller dark count rate. At 20 and 0 °C, the afterpulse probabilities amount to 6.5 and 8.6%, respectively, and the dark count probabilities per gate are $6.5 \times 10^{-5}$ and $2.6 \times 10^{-5}$, 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.

**PLS.** 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 a.c. port. An electrical delay allows the timing between the two driving signals to be varied. The d.c. level of the master laser is set below the threshold, ensuring a random phase, but is sufficiently high to have a small turn-on delay and produce ~250 ps pulses. With seeding photons from the master lasers, the slave lasers produce low-jitter light pulses with pulse widths around 35 ps and bandwidths of less than 0.2 nm. All lasers are temperature stabilized to ensure wavelength stability and we observed little drift for the duration of the experiments. In Fig. 2a, 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 set-up we perform a two-photon interference experiment using superconducting single photon detectors. The photon count rate was tuned to give ~$10^6$ counts s$^{-1}$ per detector. Data was acquired for 50 s 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. 2b, 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 the acquisition of $10^7$ points.