Measurement-device-independent quantum key distribution coexisting with classical communication

Valivarthi, R.; Umesh, P.; John, C.; Owen, K. A.; Verma, V. B.; Nam, S. W.; Oblak, D.; Zhou, Q.; Tittel, W.

DOI
10.1088/2058-9565/ab2e62

Publication date
2019

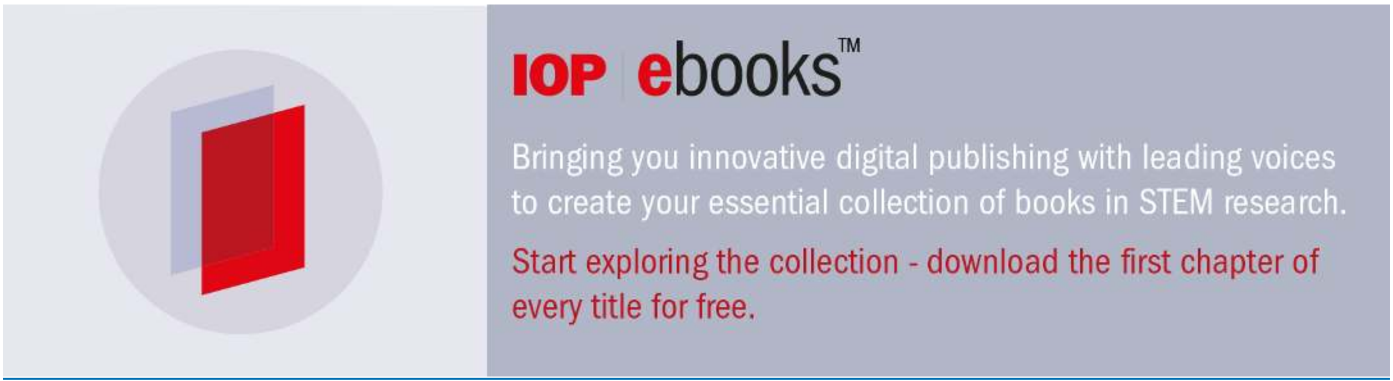
Document Version
Final published version

Published in
Quantum Science and Technology

Quantum Science and Technology

PAPER • OPEN ACCESS

Measurement-device-independent quantum key distribution coexisting with classical communication



Quantum Science and Technology

OPEN ACCESS

RECEIVED
11 April 2019

REVISED
24 June 2019

ACCEPTED FOR PUBLICATION
1 July 2019

PUBLISHED
30 July 2019

PAPER

Measurement-device-independent quantum key distribution coexisting with classical communication

R Valivarthi[1,2], P Umesh[1,7], C John[3], K A Owen[1], V B Verma[4], S W Nam[4], D Oblak[1], Q Zhou[1,5] and W Tittel[1,6]

[1] Department of Physics and Astronomy, and Institute for Quantum Science and Technology, University of Calgary, Calgary, T2N 1N4, Canada
[2] The Institute of Photonic Sciences (ICFO), E-08860 Casteldefels, Barcelona, Spain
[3] Department of Electrical and Computer Engineering, University of Calgary, Calgary, AB, T2N 1N4, Canada
[4] National Institute of Standards and Technology, Boulder, CO 80305, United States of America
[5] Institute of Fundamental and Frontier Science, and School of Optoelectronic Science and Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, People's Republic of China
[6] QuTech, and Kavli Institute of Nanoscience, Delft Technical University, Delft, The Netherlands
[7] Current address: QuTech, and Kavli Institute of Nanoscience, Delft Technical University, Delft, The Netherlands.

E-mail: w.tittel@tudelft.nl

Keywords: quantum communication, quantum key distribution, fiber optics

Abstract

The possibility for quantum and classical communication to coexist on the same fiber is important for deployment and widespread adoption of quantum key distribution (QKD) and, more generally, a future quantum internet. While coexistence has been demonstrated for different QKD implementations, a comprehensive investigation for measurement-device independent (MDI) QKD—a recently proposed QKD protocol that cannot be broken by quantum hacking that targets vulnerabilities of single-photon detectors—is still missing. Here we experimentally demonstrate that MDI-QKD can operate simultaneously with at least five 10 Gbps bidirectional classical communication channels operating at around 1550 nm wavelength and over 40 km of spooled fiber, and we project communication rates in excess of 10 THz when moving the quantum channel from the third to the second telecommunication window. The similarity of MDI-QKD with quantum repeaters suggests that classical and generalized quantum networks can co-exist on the same fiber infrastructure.

1. Introduction

The prospect of building a quantum internet, which promises information-theoretic secure communication [1] as well as blind or networked quantum computing [2], is generating a rapidly increasing amount of academic and corporate development efforts [3]. To minimize operating costs and hence facilitate deployment, it is important to benefit as much as possible from existing infrastructure. Starting in 1995, this has encouraged many experiments with deployed telecommunication fiber [4–6], and, since 1997, demonstrations of quantum key distribution (QKD)—the most mature application of quantum networks—together with classical data on the same fiber [7–13]. Yet, to date, comprehensive studies of the latter have been limited to so-called prepare-and-measure (P&M) QKD [1], in which one user, Alice, encodes a random string of classical bits into non-orthogonal quantum states of photons, and the other user, Bob, makes projection measurements onto a set of randomly chosen bases. Mapping measurement outcomes onto bit values leads to the so-called raw-key—two partially correlated sequences of zeros and ones (one at Alice, and one at Bob)—and, after key distillation, either to the creation of an error-free secret key, or to abortion of the key generation session.

While the security of properly implemented P&M QKD can be proven, it is threatened by quantum hacking that exploits vulnerabilities of single-photon detectors to change their functioning [14–16] (see appendix A for more information). This problem can be overcome by measurement-device-independent (MDI) QKD [17], in which Alice and Bob both send photons to a central station, Charlie, who projects their joint state onto one or more of the four maximally entangled Bell states

$$|\psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}, \tag{1}$$

$$|\phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}. \tag{2}$$

Here $|0\rangle$ and $|1\rangle$ denote two orthogonal quantum states, e.g. orthogonal polarization or temporal modes. As in the case of P&M QKD (or entanglement-based QKD [1]), any eavesdropping during photon transmission will lead to errors and shortening of the secret key—possibly to zero length. However, beyond what is offered by all QKD protocols, this feature also holds in MDI-QKD if the actual measurement devices—that is the detectors—deviate from the ideal, including due to blinding or time-shift attacks by Eve.

The proposal of the MDI-QKD protocol in 2012 triggered rapid experimental progress. The first proof-of-principle demonstrations were reported only a year later [18–20], and the performance of MDI-QKD systems—including maximum distance, secret key rates, and robustness—has improved ever since [21–24]. However, unlike for P&M QKD, coexistence of MDI-QKD with classical data on the same fiber has not yet been investigated in a comprehensive manner, neither experimentally nor through simulations. (But we note that spectrally multiplexed light was used in one MDI-QKD implementation to assess and compensate for polarization transformations in the quantum channel, as well as to transmit a 1 MHz clock signal [20].)

The difficulty of combining classical and quantum communication over the same fiber lies in the generation of noise photons by the strong classical signals by means of Rayleigh, Brillouin or Raman scattering, which may mask the quantum data. Rayleigh scattering is elastic and results in additional photons at the classical communication wavelength. Assuming the quantum channel to be spectrally distinct, they can be prevented from reaching the single photon detectors using adequate spectral filters. Brillouin scattering is inelastic and leads to extra photons that are detuned by around 10 GHz from the classical signal wavelength [25]. Similar to Rayleigh scattering, Brillouin photons can be removed using spectral filters, provided the quantum and classical channels cover spectral intervals that are sufficiently far apart. Raman scattering, another inelastic process, however, generates scattered photons within a wide range of wavelengths below and above the classical communication wavelength, generally including the quantum channel. This makes spectral filtering impossible. Assuming that Rayleigh and Brillouin scattered photons can be removed, we will focus in the following only on Raman scattering.

The scattered power in case of co- and counter-propagating classical and quantum channels, P_{co} and P_{ct}, respectively, is given by [10]

$$P_{\mathrm{co}} = P_l \beta \Delta\lambda \frac{(\mathrm{e}^{-\alpha_{\mathrm{Q}} L} - \mathrm{e}^{-\alpha_{\mathrm{C}} L})}{\alpha_{\mathrm{C}} - \alpha_{\mathrm{Q}}}, \tag{3}$$

$$P_{\mathrm{ct}} = P_l \beta \Delta\lambda \frac{(1 - \mathrm{e}^{-(\alpha_{\mathrm{c}} + \alpha_{\mathrm{Q}})L})}{\alpha_{\mathrm{C}} + \alpha_{\mathrm{Q}}}, \tag{4}$$

where L is the fiber length, P_l is the average power launched in the classical channel, β is the Raman scattering coefficient (β depends on the wavelengths of the quantum and the classical channels as well as properties of the optical fiber), $\Delta\lambda$ is the bandwidth of the quantum channel, and α_{Q} and α_{C} are the fiber attenuation coefficients for quantum and classical channels, respectively. The photon scattering rate, n, and the scattered power, P, are related by $nhc/\lambda = P$, where h is Planck's constant, c the speed of light, and λ the photon wavelength. For bidirectional communication, allowing the exchange of classical data between Alice and Bob over a single fiber, the rates for co- and counter-propagating data have to be added: $P_{\mathrm{bi}} = P_{\mathrm{co}} + P_{\mathrm{ct}}$.

In this paper we experimentally demonstrate that measurement-device independent (MDI) QKD can operate simultaneously with at least five 10 Gbps bidirectional classical communication channels at around 1550 nm wavelength over 40 km of spooled fiber, and we project communication rates in excess of 10 THz when moving the quantum channel from the third to the second telecommunication window. As MDI-QKD is ideally suited for building cost-effective QKD networks with star-type topology, and can be upgraded into quantum-repeater-based networks [26], our demonstration is a first step towards a future quantum network in which secret keys, or qubits, can be distributed over arbitrarily long distances, and using which networked quantum information processing and blind quantum computing will become possible.

2. Methods

Our demonstration of coexistence with classical data is based on the MDI-QKD setup depicted in figure 1 and further detailed in appendix B (see also [27]). Additional classical communication channels are prepared using four 1548 nm DFB lasers, sending continuous-wave light from Alice to Charlie, from Charlie to Alice, from Bob to Charlie, and from Charlie to Bob. The launch power of each laser is chosen such that at the remaining power at the receiver side is an integer multiple of 2 μW—the minimum power needed for a 10 Gbps link [9]. For

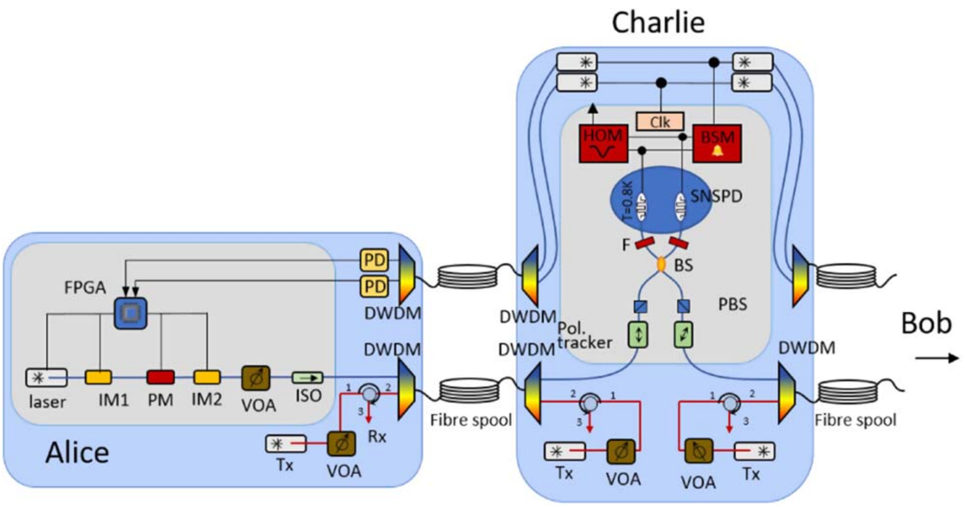


Figure 1. Experimental setup. Only one sender unit and the central receiver is shown. See appendix B for details. Intensity modulator (IM), phase modulator (PM), variable optical attenuator (VOA), optical isolator (ISO), field-programmable gate array (FPGA), dense wavelength demultiplexer (DWDM), classical transmitter (Tx), classical receiver (Rx), polarizing beam splitter (PBS), beam splitter (BS), narrow spectral filter (F), superconducting nanowire single-photon detectors (SNSPD), photo-detector (PD), Hong–Ou–Mandel dip measurement (HOM), Bell-state measurement (BSM).

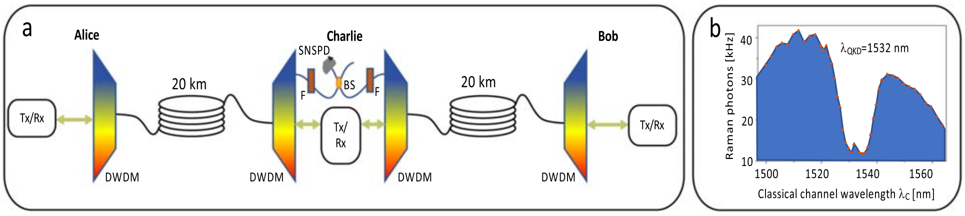


Figure 2. Crosstalk. (a) Schematics of the setup used for assessing crosstalk due to Raman scattering. Classical transmitter (Tx) and receiver (Rx), dense wavelength demultiplexers (DWDM), beam splitter (BS), narrow spectral filter (F), superconducting nanowire single-photon detector (SNSPD). Classical light was injected bi-directionally into two 20 km long fibers (Corning SMF-28 standard telecommunication fiber) connecting Alice, and Bob, to Charlie. The launch power for each classical channel, ~8 μW, was chosen so that each output power was 2 μW—sufficient for 10 Gbps classical communication [9]. (b) Raman noise measured using a single-photon detector at Charlie in a 6 GHz broad spectral channel centered at $\lambda_{\mathrm{QKD}} = 1532.68$ nm wavelength for different classical channel wavelengths λ_{C}.

instance, 10 μW at the receiver side corresponds to either one 50 Gbps channel, or to five 10 Gbps channels realized using different frequencies within the ITU grid. Provided neighboring channels are chosen, the Raman noise created by all classical channels at the quantum channel wavelength 16 nm away can be considered equal, and it does therefore not matter over how many channels classical data is distributed. Quantum and classical data are combined and split using dense wavelength division multiplexer.

2.1. Raman noise

To assess the effect of Raman scattering on MDI-QKD, we first measured the noise in a narrow spectral window centered at 1532 nm—the operating wavelength of our MDI-QKD system—caused by strong light of various wavelengths propagating bi-directionally through 20 km long standard telecommunication fiber between Alice and Charlie, and Bob and Charlie. The measurement is described in more detail in figure 2(a).

2.2. Experimental secret key rates

Next, we ran our QKD system over two different lengths of spooled fiber—2 × 20 km, and 2 × 40 km. As in the case of assessing cross-talk, the quantum channels between Alice and Charlie, and Bob and Charlie, were combined with pairs of bi-directional classical data channels. To test the worst case in which Raman noise is maximized, we used 1548 nm laser light for the data channel (this choice is motivated by the result of the measurement shown in figure 2(b)), and to emulate different numbers of classical channels, we changed the power at each input in integer multiples of ~8 μW (~20 μW), corresponding to 2 μW steps in output power after 20 km (40 km) transmission. As shown in [9], 2 μW suffices to operate one 10 Gbps data channel with bit error rates $\leqslant 10^{-12}$, and having hence N times that power at the four receivers hence allows for N bi-directional 10 Gbps links between Alice and Bob. However, we note that the modulation scheme used to encode classical data may have an impact on the minimum power per channel, and hence on the interpretation of our results. We also remark that telecommunication operators currently do not optimize input power with respect to detector sensitivity, transmission loss and, if relevant, modulation scheme. However, this could change through software defined networking, which allows dynamic network configuration and hence optimization.

For each configuration of fiber length and number of bi-directional 10 Gbps channels, emulated using continuous-wave light with appropriately chosen power, we created sifted keys and evaluated the secret key rate according to

$$R_{\mathrm{inf}} \geqslant [Q_{11}^{Z}[1 - h_2(e_{11}^{X})] - Q_{\mu\sigma}^{Z} f h_2(e_{\mu\sigma}^{Z})]. \tag{5}$$

Here, Q_{11} is the gain (the probability of a projection onto a Bell state) per emitted pair of qubits; e_{11} the associated error rate; and the superscript indicates the jointly used basis (the Z basis features eigenvectors $|0\rangle$ and $|1\rangle$), and the X-basis eigenvectors $(|0\rangle \pm |1\rangle)/\sqrt{2}$). Furthermore, $h_2(x) = -x \ \log_2(x) - (1 - x) \ \log_2(1 - x)$ is the binary Shannon entropy function; $f = 1.14$ is the efficiency of error correction; and the subscript 'inf' denotes the assumption of infinitely long keys.

2.3. Simulations

We simulated secret key rates in the presence of classical communications using the code described in detail in our previous studies [27, 28]. Noise caused by Raman scattering is taken into account by increasing the detector noise according to the results shown in figure 2. For simulations that require Raman noise within a quantum channel centered around 1310 nm wavelength and a classical channel within the C-band, we used experimental data published elsewhere [11].

3. Results

3.1. Raman noise

The results of the measurements of the Raman noise are shown in figure 2(b) (the numerical data is listed in appendix C). The region in which $\lambda_{\mathrm{C}} > \lambda_{\mathrm{QKD}}$ corresponds to anti-Stokes scattering while the region of $\lambda_{\mathrm{C}} < \lambda_{\mathrm{QKD}}$ shows Stokes scattering. The variation of Raman photons as a function of the difference between classical and quantum channel wavelength reflects the known behavior in optical fiber [10, 29]. However, we note that in our case classical data traveled bi-directionally and that we furthermore kept the output power of the classical channel constant. This leads to a slightly different result as compared to the usual measurement in which classical data only travels uni-directionally and the input power is held at a fixed value.

Confirming previous observations [10], we find Raman noise even if the quantum and classical channels are separated by many tens' of nanometers, and that the gain of the underpining interaction is reduced if the channel spacing is less than a few nanometers. Limiting classical channels to the extensively used C-band (extending from 1530 to 1565 nm wavelength), we furthermore see that the most cross-talk happens at a wavelength of approximately 1548 nm.

3.2. Experimental key rates

Secret key rates in the infinite (key length) limit, together with predictions based on an independent characterization of the complete setup (no fits) are depicted in figure 3 (the numerical data are listed in tables [C1, C2] of appendix C).

4. Discussion

Most importantly, we find that MDI-QKD and bi-directional classical communication is possible over the same fiber. More precisely, we experimentally demonstrated positive secret key rates over a total of 40 km fiber together with the possibility for up to 50 Gbps bi-directional classical communication, and theoretically predicted positive secret key rates with up to 70 Gbps of classical data over the same fiber length. In addition, we demonstrated the possibility for QKD over a total of 80 km fiber with 10 Gbps of classical data. This is comparable to results obtained for P&M QKD, e.g. in [9] where the possibility for secure key exchange over 70 km fiber distance and coexisting with 10 Gbps of bi-directional classical communication was demonstrated. However, the quantum-classical channel spacing was only of 2.5 nm in this case, resulting in approximately three times less Raman noise as compared to the worst-case scenario of 16 nm spacing chosen in our implementation (see figure 2). The apparent increased resilience of MDI-QKD to Raman noise may be due to

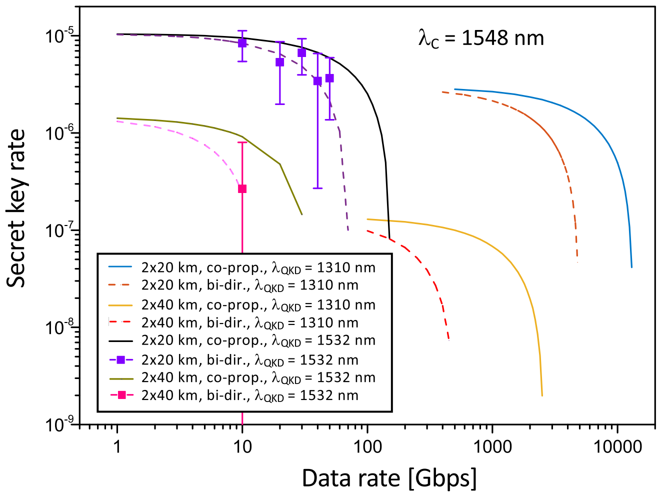


Figure 3. Results. Predicted (lines) and experimentally obtained (squared) secret key rates (per clock cycle and assuming the infinite key limit) for different fiber lengths, data rates, wavelengths of the quantum channel, and assuming bi-directional or uni-directional (co-propagating) classical communication between Alice and Bob (connected via Charlie). Classical data is assumed to be at $\lambda_C = 1548$ nm wavelength. Experimental error bars indicate one standard deviation and are obtained assuming Poisson detection statistics.

the need for detecting two photons per key bit. However, the flip-side is a reduced key rate, at least as long as single-photon detectors with quantum efficiencies significantly below unity are employed.

The classical communication rate or, alternatively, the number of classical data channels at neighboring spectral channels can straightforwardly be increased by 50% by moving the classical data within the C-band from 1548 to 1565 nm wavelength, where Raman noise is reduced (see figure 2(b)). Furthermore, as shown by the simulations depicted in figure 3, the maximum classical data rate would increase by almost two orders of magnitude, e.g. for a total distance of 40 km from around 70 Gbps to around 5 Tbps, when shifting the QKD wavelength to 1310 nm wavelength (the classical data is assumed to be at 1548 nm wavelength, but changes within the C-band barely affect performance). In this configuration, increased photon transmission loss—normally degrading QKD performance—is more than compensated for by a reduction of Raman scattering.

Even better performance is expected when moving from bi-directional transmission of classical data to uni-directional transmission, where data co-propagates with QKD photons. In this case, most Raman photons, created in the region of highest laser power, i.e. close to Alice or Bob, would be absorbed in the fiber before arriving at Charlie's detector. As shown in figure 3—and still assuming a QKD wavelength of 1310 nm and classical data to be encode in the C-band—this would allow the distribution of secret keys together with classical communications over a total of 40 km at more than 10 Tbps rate. This suffices for most applications.

Obviously, our results depend on the necessary power at the receiver. For instance, increasing its value by a factor of 10 would lead to a reduction of the secure key rate to zero and by 26% if the quantum channel is at 1532 or 1310 nm wavelength, respectively. Hence, while the possibility for multiplexing of quantum and classical data will rapidly fade if encoding both channels within the same telecommunication window, using different windows—one centered at 1550 nm and one at 1310 nm—will make it very likely that both types of communication can coexist.

We note that our QKD system currently employs pairs of fibers—one fiber for clock synchronization and announcement of successful measurements at Charlie, and one for quantum communication, see figure 1. However, our results shows that quantum and classical signals can be multiplexed into the same fiber. We also point out that the calculation of the secret key rate in equation (5) assumes the limit of an infinitely long sifted key. This is in reality impossible, and an additional reduction that depends on the key length before post processing has to be taken into account [30]. For instance, with ~0.2 kbps of sifted key, as in our current setup over 2 × 20 km fiber, it would take ~139 h to pass the threshold between no secret key and secret key. While feasible, this is is impractical. The time can be reduced by two orders of magnitude by increasing the clock rate from its current value of 20 MHz to a few GHz. Current bottlenecks to this solution are the maximum clock rate of the (sequentially-operated) FPGAs in the QKD senders; limited accuracy (e.g. ringing) of the signals used to drive intensity and phase modulators; and the recovery time of the superconducting nanowire single-photon detectors (SNSPDs). They can be overcome by more advanced FPGA programming, better electronics, and the use of detector arrays [31].

5. Conclusion

Our investigation establishes the possibility for MDI-QKD to coexist with classical communication on the same fiber. Moreover, as MDI-QKD shares an essential feature with quantum repeater-based communication—the need for a Bell state measurement with photons that are created far apart—it also shows that classical and generalized quantum networks can co-exist on the same fiber infrastructure. We additionally note that MDI-QKD is ideally suited for building QKD networks with star-type topology in which several users are connected to the same central measurement node (Charlie). Using optical switches, it becomes then possible to connect any pair of users on demand. As users only need sender modules but no receivers (the latter will be located at the central node and be accessible to all users), this solution is both simpler and more cost-effective than the creation of a fully connected network using P&M QKD, which requires all users to have both a sender and a receiver module. Hence, our demonstration increases the commercial viability of MDI-QKD and, more generally, quantum communications, will facilitate the adoption of the new quantum technology, and therefore constitutes an important step towards a world in which quantum information processing will help meeting challenges in secure data transmission, and will provide opportunities for unparalleled data processing.

Acknowledgments

The authors thank Vladimir Kiselyov for technical help, and Alberta Innovates Technology Futures (AITF), the National Science and Engineering Research Council of Canada (NSERC), and the Netherlands Organization for Scientific Research (NWO) for financial support. Furthermore, WT acknowledges funding as a Senior Fellow of the Canadian Institute for Advanced Research (CIFAR), QZ from the National Key R&D Program of China (2018YFA0307400) and the National Natural Science Foundation of China under grants 61775025 and 61405030, and VBV and SWN acknowledge partial funding for detector development from the Defense Advanced Research Projects Agency (DARPA) Information in a Photon (InPho) program. Part of the research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration (NASA).

Appendix A. Quantum hacking

During recent years, it became apparent that the ideal security of QKD protocols may not carry over to actual implementations. By exploiting deviations—possibly induced by the eavesdropper herself—of the used technology compared to the assumptions that underpin the security proof, it may be possible for Eve to acquire full information about the key without abortion of the QKD session. In particular, single-photon detectors have been shown vulnerable to such side-channel attacks, e.g. time-shift [14, 15] or blinding attacks [16], and while countermeasures to certain attacks have been demonstrated [32], their effectiveness remains questionable [33]. Furthermore, a countermeasure can only be implemented once an attack has been discovered, leaving all keys exchanged in the intermediate period insecure. In light of this, alternative protocols whose security against side-channel attacks is rooted in fundamental quantum mechanical principles have been proposed. Currently the most practical of these protocols is MDI QKD [17], which is described next.

Appendix B. The MDI-QKD system

B.1. Qubit preparation at Alice and Bob

By shaping (using intensity and phase modulators, IM, PM) and attenuating (using a variable optical attenuator, VOA) phase-randomized pulsed of light emitted by laser diodes driven from below threshold, Alice and Bob randomly create qubit states encoded into superpositions of early and late temporal modes:

$$|0\rangle \equiv |e\rangle;\ |1\rangle \equiv |\ell\rangle$$
$$|+\rangle \equiv (|e\rangle + |\ell\rangle)/\sqrt{2};\ |-\rangle \equiv (|e\rangle - |\ell\rangle)/\sqrt{2}.$$

The first two states are eigenstates of the Z-basis, and the two latter of the X-basis. Each temporal mode extends over 500 ps, and early and late modes are separated by 2.5 ns. Security against photon number splitting attacks [1], exploiting that more than one photon may may be present in an attenuated laser pulse, is derived by randomly changing their mean photon numbers between three different values, according to the three-intensity decoy-state protocol described in [30]. Furthermore, optical isolators (ISO) that prevent light from the outside to enter the QKD senders protect against Trojan horse attacks [1].

Random numbers, both for selecting qubit states as well as intensity levels of attenuated laser pulses, are created off-line using a quantum random number generator [34], stored in field programmable gate arrays (FPGA) within each sender module, and then used to determine phase and intensity modulator settings.

B.2. Qubit measurement at Charlie

A projection onto the $|\psi^-\rangle = (|e\ell\rangle - |\ell e\rangle)/\sqrt{2}$ Bell state takes place if two photons, one from Alice and one from Bob, are detected behind a 50/50 beamsplitter in different temporal modes—one early, and one late. To ensure the required indistinuishability of the two photons, we employ several automated feedback loops. First, arrival time differences are measured using Hong–Ou–Mandel interference, and synchronization is maintained by delaying the clock signal sent from Charlie to either Alice or Bob. Furthermore, polarization indistinguishability is ensured by means of polarizing beam-splitters (with feedback to maximize transmission) and polarization-maintaining fibers that connect to the 50/50 beam-splitter that is at the heart of the Bell-state measurement. In addition, we verify the frequency difference between Alice's and Bob's temperature-stabilized laser diodes every 5 min and, if necessary, reduce it to less than 10 MHz.

Photons are detected using WSi SNSPDs cooled to 0.8 K in a sorption cooler [35]. They feature system efficiencies of around 50%, dark counts of around 100 Hz, and detection time jitter of 100 ps. Successful Bell-state measurements are communicated to Alice and Bob using laser pulses sent over additional fiber.

B.3. Key sifting

The first step in key sifting is the reduction of the local bit strings at Alice's and Bob's to those that describe the states of photons that were detected in Charlie's Bell-state measurement. In order to avoid memory-intensive storage of time-tagged data that characterizes all photon states-most of which will be discarded during this step-Alice and Bob send the information of their prepared qubits (with the exception of time) into first-in-first-out buffers in their FPGAs while the corresponding qubits are sent to Charlie. The delays in the buffers equal the combined time required by the qubits to reach Charlie, and by the BSM signals to travel back to Alice or Bob. A simple logic operation then allows singling out only qubit generations that resulted in a successful BSM—only those are further processed during subsequent basis reconciliation.

Appendix C. Data

Table C1. Raman noise measured at Charlie in a 6 GHz wide spectral window centered at 1532 nm wavelength for different classical channel wavelengths.

Wavelength (nm)	Noise counts (kHz)	Wavelength (nm)	Noise counts (kHz)
1500	33.33	1505	35.33
1510	40.67	1515	41.33
1520	38.00	1525	30.00
1530	13.00	1535	11.67
1540	23.67	1545	31.00
1550	28.67	1555	26.33
1560	23.00	1565	17.67

Table C2. Experimentally obtained secret key rate (R_∞) with number of co-existing 10 Gbps channels, N, for different transmission lengths of spooled fiber.

N	2 × 20 km	2 × 40 km
0	1.13E-05 ± 5.52E-06	1.72E-06 ± 6.16E-07
1	8.37E-06 ± 2.93E-06	2.66E-07 ± 5.35E-07
2	5.34E-06 ± 3.36E-06	
3	6.66E-06 ± 2.69E-06	
4	3.43E-06 ± 3.16E-06	
5	3.66E-06 ± 2.29E-06	

ORCID iDs

D Oblak https://orcid.org/0000-0002-0277-3360
W Tittel https://orcid.org/0000-0003-3136-8919

References

[1] Gisin N, G Ribordy W T and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Broadbent A, Fitzsimons J and Kashefi E 2009 Universal blind quantum computation *50th Ann. IEEE Symp. on Foundations of Computer Science (Atlanta, GA)* (Piscataway, NJ: IEEE) pp 517–26
[3] Riedel M F, Binosi D, Thew R and Calarco T 2017 *Quantum Sci. Technol.* **2** 030501
[4] Muller A, Zbinden H and Gisin N 1995 *Nature* **378** 449
[5] Tittel W, Brendel J, Zbinden H and Gisin N 1998 *Phys. Rev. Lett.* **81** 3563
[6] Valivarthi R, Zhou Q, Aguilar G H, Verma V B, Marsili F, Shaw M D, Nam S W, Oblak D and Tittel W 2016 *Nat. Photon.* **10** 676
[7] Townsend P D 1997 *Electron. Lett* **33** 188–90
[8] Eraerds P, Walenta N, Legré M, Gisin N and Zbinden H 2010 *New J. Phys.* **12** 063027
[9] Patel K, Dynes J, Lucamarini M, Choi I, Sharpe A, Yuan Z, Penty R and Shields A 2014 *Appl. Phys. Lett.* **104** 051123
[10] Fröhlich B, Dynes J F, Lucamarini M, Sharpe A W, Tam S W B, Yuan Z and Shields A J 2015 *Sci. Rep.* **5** 18121
[11] Wang L J *et al* 2017 *Phys. Rev.* A **95** 012301
[12] Eriksson T A, Hirano T, Ono M, Fujiwara M, Namiki R, Yoshino K I, Tajima A, Takeoka M and Sasaki M 2018 *IEEE Photonics Society Summer Topical Meeting Series (Waikoloa Village, HI)* pp 71–2
[13] Mao Y *et al* 2018 *Opt. Express* **26** 6010–20
[14] Lamas-Linares A and Kurtsiefer C 2007 *Opt. Express* **15** 9388–93
[15] Zhao Y, Fung C H F, Qi B, Chen C and Lo H K 2008 *Phys. Rev.* A **78** 042333
[16] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686
[17] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[18] Rubenok A, Slater J A, Chan P, Lucio-Martinez I and Tittel W 2013 *Phys. Rev. Lett.* **111** 130501
[19] Liu Y *et al* 2013 *Phys. Rev. Lett.* **111** 130502
[20] Da Silva T F, Vitoreti D, Xavier G, Do Amaral G, Temporao G and Von Der Weid J 2013 *Phys. Rev.* A **88** 052303
[21] Valivarthi R *et al* 2015 *J. Mod. Opt.* **62** 1141–50
[22] Yin H L *et al* 2016 *Phys. Rev. Lett.* **117** 190501
[23] Comandar L, Lucamarini M, Fröhlich B, Dynes J, Sharpe A, Tam S B, Yuan Z, Penty R and Shields A 2016 *Nat. Photon.* **10** 312
[24] Tang Y L *et al* 2016 *Phys. Rev.* X **6** 011024
[25] Yeniay A, Delavaux J M and Toulouse J 2002 *J. Lightwave Technol.* **20** 1425
[26] Sangouard N, Simon C, De Riedmatten H and Gisin N 2011 *Rev. Mod. Phys.* **83** 33
[27] Valivarthi R, Zhou Q, John C, Marsili F, Verma V B, Shaw M D, Nam S W, Oblak D and Tittel W 2017 *Quantum Sci. Technol.* **2** 04LT01
[28] Chan P, Slater J A, Lucio-Martinez I, Rubenok A and Tittel W 2014 *Opt. Express* **22** 12716–36
[29] Stolen R H, Gordon J P, Tomlinson W and Haus H A 1989 *J. Opt. Soc. Am.* B **6** 1159–66
[30] Xu F, Xu H and Lo H K 2014 *Phys. Rev.* A **89** 052333
[31] Allman M S *et al* 2015 *Appl. Phys. Lett.* **106** 192601
[32] Yuan Z, Dynes J and Shields A 2010 *Nat. Photon.* **4** 800
[33] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 801
[34] Zhou Q, Valivarthi R, John C and Tittel W 2019 *Quantum Eng.* **1** e8
[35] Marsili F *et al* 2013 *Nat. Photon.* **7** 210