

Deployed measurement-device independent quantum key distribution and Bell-state measurements coexisting with standard internet data and networking equipment

Berrevoets, Remon C.; Middelburg, Thomas; Vermeulen, Raymond F.L.; Chiesa, Luca Della; Broggi, Federico; Piciaccia, Stefano; Umesh, Prathwiraj; Tittel, Wolfgang; Slater, Joshua A.; More Authors

DOI

[10.1038/s42005-022-00964-6](https://doi.org/10.1038/s42005-022-00964-6)

Publication date

2022

Document Version

Final published version

Published in

Communications Physics

Citation (APA)

Berrevoets, R. C., Middelburg, T., Vermeulen, R. F. L., Chiesa, L. D., Broggi, F., Piciaccia, S., Umesh, P., Tittel, W., Slater, J. A., & More Authors (2022). Deployed measurement-device independent quantum key distribution and Bell-state measurements coexisting with standard internet data and networking equipment. *Communications Physics*, 5(1), Article 186. <https://doi.org/10.1038/s42005-022-00964-6>

Important note

To cite this publication, please use the final published version (if applicable).
Please check the document version above.






Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

Deployed measurement-device independent quantum key distribution and Bell-state measurements coexisting with standard internet data and networking equipment

Remon C. Berrevoets^{1,4} , Thomas Middelburg^{1,4} , Raymond F. L. Vermeulen¹ , Luca Della Chiesa², Federico Broggi², Stefano Piciaccia², Rene Pluis², Prathwiraj Umesh³, Jorge F. Marques³ , Wolfgang Tittel³ & Joshua A. Slater¹ 

The forthcoming quantum Internet is poised to allow new applications not possible with the conventional Internet. The ability for both quantum and conventional networking equipment to coexist on the same fiber network would facilitate the deployment and adoption of coming quantum technology. Most quantum networking tasks, like quantum repeaters and the connection of quantum processors, require nodes for multi-qubit quantum measurements (often Bell-State measurements), and their real-world coexistence with the conventional Internet has yet to be shown. Here we field deploy a Measurement-Device Independent Quantum Key Distribution (MDI-QKD) system, containing a Bell-State measurement node, over the same fiber connection as multiple standard Internet Protocol (IP) data networks, between three nearby cities in the Netherlands. We demonstrate over 10 Gb/s classical data communication rates simultaneously with our next-generation QKD system, and estimate 200 GB/s of classical data transmission would be easily achievable without significantly affecting QKD performance. Moreover, as the system ran autonomously for two weeks, this shows an important step towards the coexistence and integration of quantum networking into the existing telecommunication infrastructure.

¹QuTech, Delft University of Technology, Delft, The Netherlands. ²Cisco Systems, Inc., 170 West Tasman Dr., San Jose, CA, USA. ³QuTech and Kavli Institute of Nanoscience, Delft University of Technology, Delft, The Netherlands. ⁴These authors contributed equally: Remon C. Berrevoets, Thomas Middelburg. ✉email: j.a.slater@tudelft.nl

The conventional internet, the applications that run on it, and the telecommunication networks on which it operates, have had a tremendous impact on society. The coming quantum internet is poised to have a similar impact by enabling new applications that are fundamentally not possible with the conventional internet¹. Amongst those applications are secure access to remote quantum computers and long-distance networked quantum computers², enhanced sensors³, enhanced clock synchronization accuracy⁴, teleportation of quantum information across a network⁵, as well as security-related applications such as information-theoretic secure processing via blind quantum computing⁶ and perhaps the most-known application, quantum key distribution (QKD) for information-theoretic secure distribution of cryptographic keys^{7–10}. With ever-increasing attention from industry and governments on these developments, many academic efforts have turned towards the integration of quantum communication technologies with conventional networking technology. Fundamentally, this means quantum optic signals—e.g., single photons level pulses—and conventional networking signals and data—e.g., telecom bright laser light—share the same optical fiber. In other words, at the physical layer¹¹, there is a desire for quantum signals and telecom signals to coexist on the fiber.

Coexistence of quantum signals and telecom signals is challenging, considering the large intensity difference and the general intolerance to noise by quantum receivers and detectors^{12–26}. The natural approach is to separate quantum signals from telecom signals with well-established wavelength division multiplexing (WDM) techniques. In WDM fiber technology, each signal is transmitted at a dedicated wavelength channel and off-the-shelf components can well multiplex the different wavelengths onto a single fiber, and then demultiplex the channels at the receiver station, directing them to their matched receivers. The difficulty of combining quantum signals and telecom signals on the same fiber, even when employing WDM, comes from spurious noise photons and crosstalk that the bright telecom light will inevitably add to the quantum channel. The primary mechanism by which this occurs is Raman scattering¹⁴, an inelastic process wherein photon–phonon interactions scatter light within a wide range of wavelengths around the bright telecom light, including, potentially, into the quantum dedicated wavelength channel. In addition to WDM devices, ameliorating the effects of Raman scattering can be achieved by the addition of narrow spectral filters, temporal filters, and by maintaining a large wavelength separation between the quantum and telecom channels.

Numerous quantum communication experiments have employed these techniques to demonstrate the coexistence of quantum signals with conventional network data on the same fiber^{12–26}; however, all have been demonstrations of prepare-and-measure (P&M) QKD, in which a transmitting node (Alice) prepares a qubit state and transmits it to a receiving node (Bob) for detection. A drawback to these studies is that P&M quantum communication, while suitable for trusted node QKD^{8,9}, does not include important ingredients for future stages of the quantum internet¹, e.g., multi-photon interference measurements such as Bell-state measurements (BSMs). Such BSM stations—often referred to as midpoints, heralding stations, or center nodes—play a critical role in quantum teleportation⁵, entangling quantum processors, linking distantly separated quantum computers², quantum repeaters²⁷, and next-generation QKD systems and networks^{28–31}.

Measurement-device-independent (MDI) QKD is based on such BSMs and can therefore be seen as a stepping stone towards the quantum internet^{28,29}. In MDI-QKD, two parties (Alice and Bob) individually prepare and send qubits to a center node at which a BSM is performed. After the center node sends the BSM

results back to the two parties, Alice and Bob can form entanglement-like correlations, and thus, they can generate a secret key via the usual QKD post-processing techniques.

MDI-QKD also has other advantages when compared to P&M QKD systems: by placing all single-photon detectors in a BSM at the center node, MDI-QKD is inherently protected against all known and yet-to-be-proposed detector side-channel attacks. This is an important advantage because historically, detection side-channel attacks have proven to be easily implementable and difficult to defend against^{32–45}. Furthermore, MDI-QKD allows many users to connect to each other via a single-center node. This brings improved practicality and scalability as it allows for multipoint-to-multipoint functionality and sharing of potentially expensive resources, such as single-photon detectors, which can all be placed within the center node.

Over the last decade, numerous realizations of MDI-QKD have been shown, both in the lab and in the field^{46–56}. However, so far only one study has examined how conventional optical communication signals may impact this protocol⁵⁷. This research is, however, limited to a laboratory environment, and continuous wave lasers were used as conventional optical communication signals instead of functional telecom Internet Protocol (IP) data networks and equipment.

Here, we report the demonstration of MDI-QKD deployed between three cities, wherein its quantum signals coexist in the same optical fiber as two functional telecom IP data networks. The previous study⁵⁷ guides our development presented here: a field-deployed, multi-node quantum communication system, incorporating a BSM node and coexisting with conventional telecom equipment, signals, and data traffic. The essential technique herein is a single node routing conventional optical data traffic and performing two-photon quantum interference for BSMs. At the center node, we use various strategies to isolate the quantum signals from the telecom signals, while fully maintaining the data networks, and providing over 10 Gb/s IP connectivity.

Results

The MDI-QKD protocol. In the MDI-QKD protocol, the two end nodes (Alice and Bob) are functionally identical: they randomly choose a string of qubit states, each being one of the four BB84 states ($|0\rangle$, $|1\rangle$ in the Z-basis and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ in the X-basis). Alice and Bob associate the states $|0\rangle$ and $|+\rangle$ ($|1\rangle$ and $|-\rangle$) with classical bit value 0 (and 1). They sequentially encode these qubit states into attenuated laser pulses at the single-photon level and transmit them to a center node. For each pair of photons (one from Alice and one from Bob, which arrive simultaneously at the center node) the center node performs a BSM, which may project the qubits onto the maximally entangled $|\psi^-\rangle$ Bell state. After each attempted BSM, the center node immediately announces to the end nodes whether the BSM was successful or not, and Alice and Bob only store information about the states of the created qubits that resulted in a BSM. After a sufficiently large number of BSMs, the end nodes move to the standard QKD post-processing phase. Note that our implementation described below does not use perfect single photons, but instead weak coherent laser pulses. To protect against the threat of the photon number splitting attack⁵⁸, our end nodes also randomly choose between three mean photon numbers for each pulse (referred to as signal, decoy, and vacuum) and employ a three-intensity decoy-state analysis to analyze their data⁵⁹, which allows secure distribution of key, even without a true single-photon source.

For post-processing, Alice and Bob use an authenticated classical channel to first perform basis reconciliation and discard data about qubit pairs for which they have selected different

bases. Of the remaining qubit pairs, they reveal a subset of the bit values so as to estimate for each basis the error rate as well as the probability of a projection onto the $|\psi-\rangle$ Bell state per emitted qubit pair (known as the gain). They use the data from the X-basis to bound information an eavesdropper could have learned about the key during photon transmission. Then, to finally distill a secret key from their data, they perform classical error correction on the Z-basis data and privacy amplification to remove the number of bits of information that could have been leaked to an eavesdropper. This results in a secret key rate:

$$R = [s_{11}^Z[1 - H(e_{11}^X)] - Q_{ss}^Z H(E_{ss}^Z)], \quad (1)$$

where R is the secure key rate per pair of Z-basis signal intensity qubits sent, s_{11}^Z is the single-photon gain of the Z-basis, e_{11}^X is the single-photon error rate in the X-basis, both extracted from the decoy analysis⁵⁹, Q_{ss}^Z and E_{ss}^Z are the gain and qubit error rate (QBER) of the Z-basis signal qubits, H is the binary entropy function, and f is the error correction efficiency (set to 1.12 in this work). Note, however, that in this work we do not run the post-processing algorithms, and thus the presented secret key rates are estimates based on an assumed error correction efficiency.

The MDI-QKD system. A schematic of our end nodes is shown in Fig. 1a, and described in the caption. Our Alice and Bob use 1310 nm wavelength distributed feedback (DFB) lasers to generate the light for the time-bin qubit states. They create the states $|\text{early}\rangle$, $|\text{late}\rangle$ (associated with qubit states $|0\rangle$, $|1\rangle$) and $|\pm\rangle$, as well as various mean photon numbers required in the decoy-state protocol using a series of intensity and phase modulators.

At the center node, incoming qubit pulses interfere on a beam splitter (PMBS) and are detected by single-photon detectors. Successful BSMs are identified by a field programmable gate array (FPGA), which monitors when the two detectors after the PMBS clicked during the same qubit pulse, but with opposite values (i.e., one detector registering $|\text{early}\rangle$ and the other $|\text{late}\rangle$). This corresponds to a projection onto the entangled $|\psi-\rangle$ Bell state, which identifies a successful BSM for the MDI-QKD protocol. During QKD operation, the center node uses two DFB lasers at 1548 nm wavelength to immediately inform Alice and Bob of a successful BSM detection. We refer to this communication channel as the control channel. At Alice and Bob, detection data are processed on FPGAs, with data of interest written to disk. The full schematics of the center node's detection setup are shown in Fig. 1b.

An important requirement for multi-photon interference, such as BSMs, is that input photons must be indistinguishable in all degrees of freedom at the PMBS. Our system accomplishes this through a variety of control and stabilization systems. To synchronize the system between the three locations, a master clock signal of 200 MHz is generated at the center node and optically sent to Alice and Bob via the control channel. Thus, the control channel transmits both the clock signal and detection data described above, which are modulated together into the optical field for communication to the end nodes. Alice and Bob demodulate out the clock signal and distribute it to their FPGAs and pulse generators. Alice's and Bob's optical pulses are aligned to the center node's digitizer windows with a precision of 10 ps.

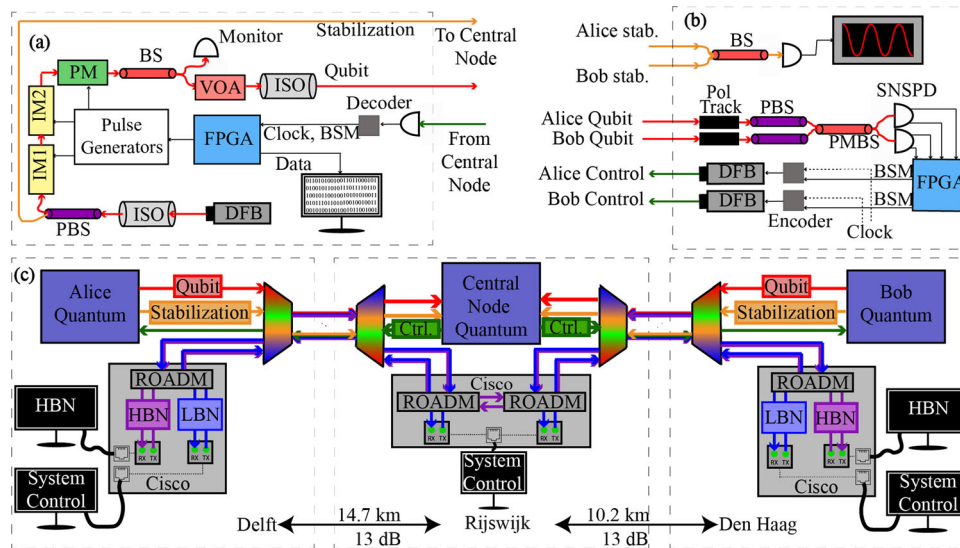


Fig. 1 Schematic drawings of the MDI-QKD system. **a** Alice and Bob use 1310 nm wavelength distributed feedback (DFB) lasers to generate the light for their time-bin qubit states. After the laser, an isolator (ISO) prevents any light moving back into the laser and a polarizing beam splitter (PBS) ensures the light is well polarized. One of the PBS' outputs is used to generate the time-bin qubits via a series of intensity and phase modulators. The first intensity modulator (IM1) creates optical pulses with a full width at half maximum (FWHM) of 600 ps, separated by 1.5 ns. A phase modulator (PM) modulates one of the pulses with a π -phase to create the $|\psi-\rangle$ state and a second intensity modulator (IM2) creates the different mean photon numbers required for the decoy states. A beam splitter (BS) is used to monitor the qubit channel for calibration purposes. The pulses out of the other arm of the BS then pass a variable optical attenuator (VOA) to attenuate all pulses to the single-photon level. Pulse information for the modulators is generated by a field programmable gate array (FPGA), which drives the pulse generators. **b** Qubits interfere at the center node on a polarization-maintaining beam splitter (PMBS), each output of which is connected to a superconducting nanowire single-photon detector (SNSPD) for detection. Digitizer boards with 400-ps wide temporal-filtering windows convert the analog response of the SNSPD into digital signals corresponding to single projections onto qubit states $|\text{early}\rangle$ and $|\text{late}\rangle$. The center node uses two DFB lasers at 1548 nm wavelength to communicate to Alice and Bob this detection data. **c** Schematic drawing of the optical routing and wavelength division multiplexing (WDM) scheme used to demonstrate MDI-QKD coexisting with the two conventional Internet Protocol (IP) data channels (high- and low-bandwidth network (HBN/LBN)). The different colored arrows indicate different data channels and their direction, where the type of data in the channel is specified in the boxes with the corresponding colors. The qubits are co-propagating with the optical fields of the IP data channels. Details are described in the main text.

To ensure Alice's and Bob's qubits are indistinguishable in polarization, their qubits pass through polarization beam splitters (PBS) at the center node. Preceding the PBSs are electronic polarization trackers that maximize the transmission through the PBS. To maintain frequency indistinguishability, Alice and Bob use temperature-stabilized DFB lasers. A PBS directly in front of the laser (see Fig. 1) taps a portion of this light, which the end nodes then send to the center node, and at which it interferes on a beam splitter^{46,48}. This light effectively acts as another communication channel, which we refer to as the stabilization channel. Its interference is registered as intensity beating on a photodiode; the frequency of which allows the center node to generate a feedback signal to send to Alice and Bob. Alice and Bob use temperature controllers to minimize their frequency difference to below 25 MHz, which is sufficiently close for two-photon quantum interference⁶⁰ and a minimal relative phase mismatch between *X*-basis qubits with our set temporal mode spacing.

To estimate the performance of the system in various scenarios, we characterized the quantum state of the emitted qubits, as well as the center node's detection system. The qubits are characterized by two parameters (m, ϕ):

$$|\psi\rangle = \sqrt{m}|0\rangle + e^{i\phi}\sqrt{1-m}|1\rangle, \quad (2)$$

with $0 \leq m \leq 1$. Each qubit state from each end node has distinct parameters, which are listed in Supplementary Table 5. This qubit description is used in a numerical simulation to estimate the performance of the system in various network configurations. The center node's detection system is characterized by its detection efficiency, dark counts (i.e., noise), and the two-photon quantum interference visibility of the BSM. While the m s, and dark counts were directly measured, the visibility as well as the $|\psi\rangle$ state phases was acquired through fitting measured gains and QBERs.

Coexistence with conventional data channels. To demonstrate the coexistence of MDI-QKD with conventional internet technology, we integrated the MDI-QKD system with a variety of network equipment from Cisco such as the ASR9000 and the NCS5500 routers, along with an optical platform such as the NCS2000. Specifically, all three nodes employed an NCS2006 system with 20-FS-SMR Reconfigurable Optical Add-Drop Multiplexer linecards to multiplex conventional WDM optical traffic. Alice and Bob had an ASR9000 and an NCS5500 aggregation service router, respectively, as well as an additional WSE linecard in their NCS2006 systems.

The Cisco routers were configured to provide two IP networks with 10 Gb/s and 100 Mb/s, respectively, which we refer to as the high-bandwidth network (HBN) and lower-bandwidth network (LBN). In all demonstrations discussed below, the MDI-QKD system nodes used the LBN to communicate with each other, while the HBN was used for other data unrelated to the operation of the quantum systems or the experiments; e.g., other users' data, video calls, video streaming, etc.

The HBN and LBN optical signals were multiplexed on the same optical fiber as the qubits from the MDI-QKD system, but using different WDM channels. We constructed the following networks: the LBN was generated by the NCS2006 systems and operated at an out-of-band OSC wavelength of 1510 nm. The IP-level HBN 10 Gb/s service was generated by the ASR9000 and NCS5500 and the optical carrier signals were generated by the WSE linecards in the NCS2006s, and operated in the C-band at 1550.12 nm wavelength. At the center node, the HBN was optically amplified and optically routed from one end node to the other, while the LBN was converted to copper ethernet and re-generated. Both HBN and LBN were set to equal launch powers

throughout all experiments. The full network optical multiplexing design is shown in Fig. 1c.

We designed the network such that it operated over two fibers between each end node and the center node. These fibers were named fiber 1 and fiber 2 for both end-node-to-center-node links. Fiber 1 was used for Alice's and Bob's transmissions (Tx) of the IP networks optical signals and qubits (center node reception, Rx). We chose this co-propagation configuration to minimize scattered light at the single-photon detectors of the center node⁵⁷. The qubit channel generated by the MDI-QKD system operated at 1310 nm wavelength and multiplexing the qubits with the IP data signals was achieved by a standard WDM multiplexer. The advantage of 1310 nm is multifold. First, it is in the standard telecom O-band and optical components are easy to source. Also, as Raman scattering to longer wavelengths is more predominant than to shorter wavelengths, a quantum channel with a much shorter wavelength than the classical channel limits the effects of Raman scattering^{61,62}. Demultiplexing the qubits at the center node from the 1510 and 1550 nm IP network's optical signals was challenging. We used a high isolation WDM (>50 dB) to remove as much IP data signal light as possible, after which we used a narrow-band (2 nm) filter with 45 dB isolation on the qubit line to filter out remaining Raman scattered light around the qubit's wavelength. As will be shown below, these two elements provided sufficient spectral filtering to protect the qubit channel from unwanted noise.

On fiber 2 we set the center node Tx (Alice/Bob Rx), for the LBN, HBN, and MDI control channel (the latter at 1548 nm wavelength). Furthermore, the stabilization channel light at 1310 nm wavelength was placed on fiber 2, due to its spectral indistinguishability with respect to the qubits. These signals were all multiplexed and demultiplexed with standard WDMs, as all of the channels on fiber 2 were comparatively tolerant to noise.

Performance tests. For our first tests of MDI-QKD coexisting with multiple classical IP data channels, we ran the entire system in our laboratory. In the lab, each end node was separated from the center node by 20 km of spooled fiber with an intrinsic loss of 10.5 and 9.0 dB at 1310 nm wavelength, respectively. In these experiments, the launch power of the IP networks was adjusted such that the received power per channel was about 500 nW; close to the minimal required received power at the center node such that both IP networks were running with 100% uptime. The longest period of uninterrupted operation was 61 h.

We first tested the performance of the system for various attenuations in the fiber network by adding fixed attenuators. In general, the performance of decoy-state QKD varies not just with fiber attenuation, but also with the mean photon number of the signal and decoy states. We thus selected, for both end nodes, mean photon numbers that optimized secret key rate at high attenuation and used these values for all lab experiments. For all experiments, we calculated the expected key rate in the asymptotic regime using Eq. (1)⁵⁹. These results are displayed as the blue points and curve in Fig. 2. The losses and resulting gains, QBERs, and secret key rates can be found in Supplementary Tables 1 and 2. We found that even with the two coexisting data channels, the system performance would be sufficient for QKD key generation over a large parameter regime: up to about 50 dB fiber attenuation, corresponding to about 250 km of spooled fiber.

In our second set of experiments, we sought to explore the number of simultaneous conventional IP data channels that can coexist on the same fiber as the QKD system without causing significant performance degradation. Effectively, we tested the performance of the QKD network for various launch powers of

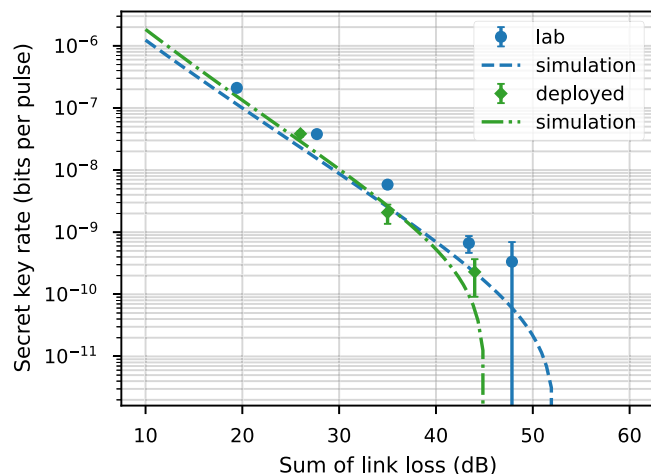


Fig. 2 Secure key rates versus loss in lab and deployed environments.

Secret key rate as a function of the total link loss between end nodes. All data were collected while the high-bandwidth network (HBN: 10 Gb/s) and low-bandwidth network (LBN: 100 Mb/s) Internet Protocol (IP) data channels were present on the same fiber as the qubits. The IP data channels' received power was kept constant at 500 nW for all measurements. Points are measured data with uncertainty bars representing 1-standard deviation. Dashed lines are simulated results generated from a full characterization of the QKD system.

the IP data channels. In general, as shown in Fig. 3a, we found a linear relationship between data launch power and noise on the center node's single-photon detectors (i.e., clicks in the absence of qubits), indicating that there exists some remaining crosstalk and/or Raman scattering from the data channels into the qubit channels. Thus, adding further data channels should, at some level, degrade the performance of the QKD channel. The asymptotic secret key rate for various launch powers can be seen in the blue points and curve of Fig. 3b. The far-left point (3.5 μ W launch power per channel) on the plot is the initial configuration in which the two data channels (HBC and LBC) have the minimally required received power at the center node. The losses and resulting gains, QBERs, and secret key rates can be found in Supplementary Tables 3 and 4. We generally observe that increasing the launch power initially has little effect on the MDI-QKD system performance. In fact, 150 μ W launch power (corresponding to 42 WDM channels) had nearly zero impact, and even pushing to 400 μ W (corresponding to 114 WDM channels) decreased the secret key rate by only a factor of two. This shows a strong resilience of the QKD system to the coexisting data channels. Furthermore, the WDM and filtering setup used here was specifically optimized for the lowest launch powers, and low (20 dB) loss, of these tests. Thus, better QKD system performance could be expected at higher launch powers by a WDM and filtering designed for those higher powers, e.g., with more isolation. Nevertheless, assuming a metropolitan-distance network with the same loss as the fiber spools (about 20 dB), it shows the possibility of an MDI-QKD system coexisting with potentially a hundred conventional 10 Gb/s data channels.

Deployment. Finally, we deployed the entire system between three cities in the Netherlands: Alice was situated in Delft (QuTech), Bob was situated in Den Haag (KPN test and release center), and the center node was situated in Rijswijk (KPN telco distribution/exchange building). Dedicated fibers were made available from each location to the center node in Rijswijk with a length of 14.7 and 10.2 km from Delft and Den Haag, respectively (Fig. 4). The fibers' losses were equalized to 13 dB using variable

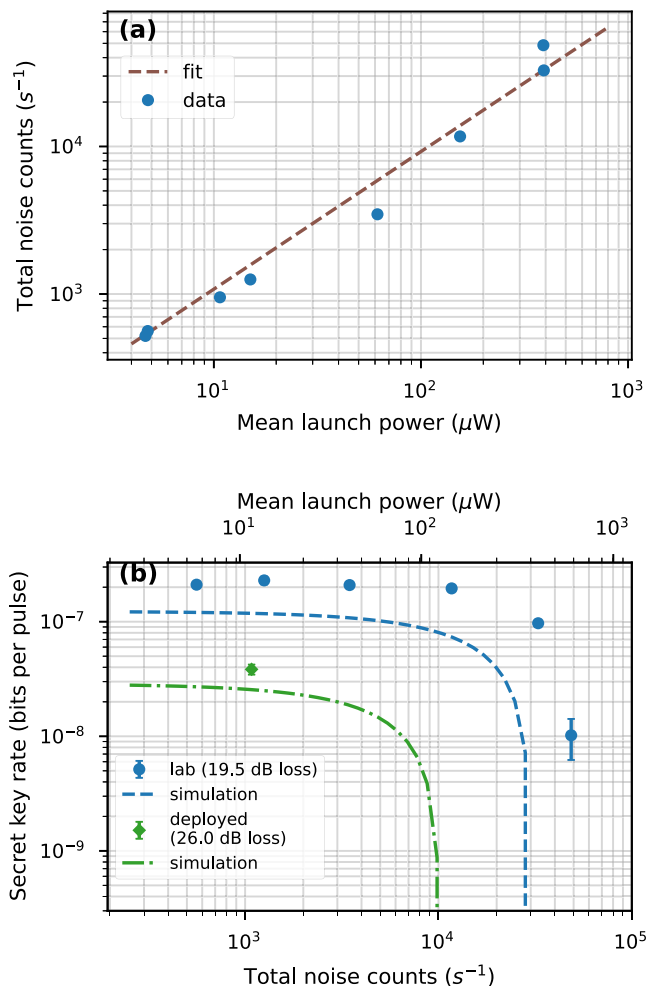


Fig. 3 Secure key rates versus classical channel launch power and corresponding detector noise counts. a Secret key rates for increasing Internet Protocol (IP) data network launch power (top x-axis) and corresponding noise counts per second on the Bell-state measurement (BSM) detectors (bottom x-axis). The smallest launch powers correspond to the minimally required received power at the center node for the two IP data networks. **b** shows the background noise counts per second, summed over all detector windows, as a function of IP data networks' launch power (average launch power from a single end node). Points are measured data with uncertainty bars representing 1-standard deviation.

optical attenuators, totaling 26 dB loss from Alice to Bob. The system was deployed over a 6-week period (including setup, measurements, demonstration events, and tear down), and fully operating for 2 weeks in June 2021. During that time the system ran autonomously, except when the network was changed for new measurements, which was the main limiting factor to the time available for data collection.

In the field, we performed the same experiments as during the lab test. The performance of the deployed system for various losses is displayed in Fig. 2 as the green points and curve. Generally, we see that the deployed system performs similarly to the lab system. The main difference from the lab setting was that we used higher and optimized mean photon numbers for the deployed fiber losses, meaning that the deployed system performed slightly better at lower losses than the lab system, and the lab system was optimized to tolerate higher loss. Nevertheless, there is good agreement between both data sets, and with the simulated performance. This demonstrates that

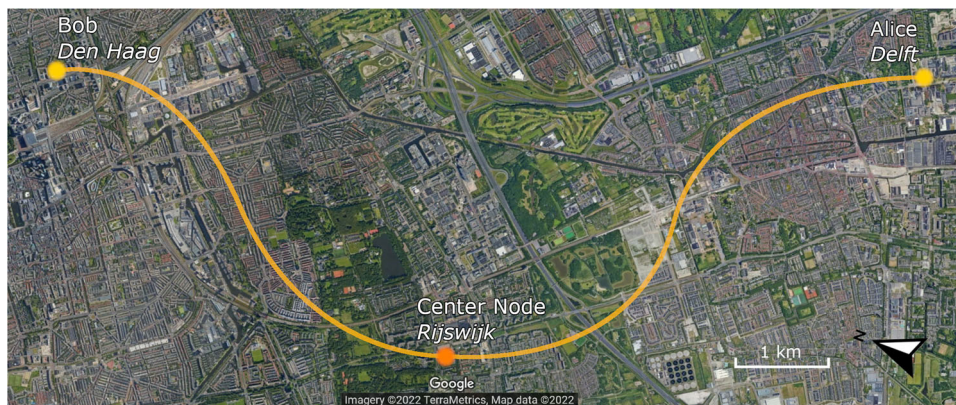


Fig. 4 Locations of the deployed MDI-QKD system. Satellite image showing the locations of the deployed MDI-QKD system. Source: Google, Imagery ©2022 TerraMetrics, Map data ©2022.

coexisting MDI-QKD and conventional IP data networks can function well, in the field, at metropolitan distances.

Lastly, in Fig. 3, we also show the deployed system's secret key rate as a function of the launch power of the IP data network. While the launch powers of the two IP networks were slightly higher to accommodate for the extra loss, the received power was the same as in the lab. The deployed system has lower secret key rates ($4\text{e-}8$ instead of $2\text{e-}7$ secret key bits per pulse), only because it operated over more loss (26 dB loss instead of 19.5 dB). We see that the secret key rate of the deployed system decreased by the expected amount. This again demonstrates the resilience of the MDI-QKD system and the center node's BSM detection unit to coexisting conventional data channels. Moreover, our simulations show that a launch power of $100\text{ }\mu\text{W}$, corresponding to twenty 10 Gb/s data channels, would only decrease the secret key rate by a factor of 2. Said differently, given sufficient telecom transceivers, it would be possible to achieve MDI-QKD coexisting with 200 Gb/s conventional IP data transmission in our 26-dB-loss deployed fiber network.

Conclusion

While we believe that our networks of 19.5 and 26 dB fiber attenuation could tolerate 100 and 26 10-Gb/s channels, respectively, increasing the coexisting data capacities further would require extra improvements. For instance, data channel filtering could be further optimized with custom-built, narrower filters. Alternatively, the MDI-QKD system key rates could be increased and thus make it more resilient to added noise. Moreover, in a real-world application, one should include the standard QKD post-processing steps (as explained above), including a full finite key analysis of the measurement results. While this typically decreases the size of the final secret key as compared to the asymptotic regime presented here, this decrease can be ameliorated by collecting sufficiently large amounts of data, or by using an efficient finite-size analysis⁶³. Nevertheless, such a step needs to be implemented before QKD-distributed key should be securely used to secure an operational communication channel.

By using high-end routers provided by Cisco for the routing of IP data channels we have demonstrated the integration of MDI-QKD with conventional networks and networking equipment: a milestone for next-generation QKD systems. Furthermore, as our system uses a center node facilitating BSMs with qubits coming from nodes in other locations, we thus have evidence that the technology for the coming quantum internet may be made compatible with conventional networks more easily than thought.

This marks a step to practically useful, and scalable quantum communication networks.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Received: 21 January 2022; Accepted: 1 July 2022;

Published online: 16 July 2022

References

- Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: a vision for the road ahead. *Science* **362**, 9288 (2018).
- Pompili, M. et al. Realization of a multinode quantum network of remote solid-state qubits. *Science* **372**, 259–264 (2021).
- Ge, W., Jacobs, K., Eldredge, Z., Gorshkov, A. V. & Foss-Feig, M. Distributed quantum metrology with linear networks and separable inputs. *Phys. Rev. Lett.* **121**, 043604 (2018).
- Kómár, P. et al. Quantum network of atom clocks: a possible implementation with neutral atoms. *Phys. Rev. Lett.* **117**, 060506 (2016).
- Bennett, C. H. et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895 (1993).
- Broadbent, A., Fitzsimons, J. and Kashefi, E. Universal blind quantum computation. *50th Annual IEEE Symposium on Foundations of Computer Science* 517–526 (2009).
- Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *Proc. Int. Conf. on Computer Systems and Signal Processing* 175–179 (New York: IEEE) (Bangalore, 1984).
- Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
- Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **8**, 595 (2014).
- Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **12**, 1012–1236 (2020).
- Zimmermann, H. OSI reference model-the ISO model of architecture for open systems interconnection. *IEEE Trans. Commun.* **28**, 425 (1980).
- Townsend, P. D. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing. *Elec. Lett.* **33**, 188 (1997).
- Peters, N. et al. Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments. *N. J. Phys.* **11**, 045012 (2009).
- Chapuran, T. E. et al. Optical networking for quantum key distribution and quantum communications. *N. J. Phys.* **11**, 105001 (2009).
- Eraerds, P., Walenta, N., Legré, M., Gisin, N. & Zbinden, H. Quantum key distribution and 1 Gbps data encryption over a single fibre. *N. J. Phys.* **12**, 063027 (2010).
- Patel, K. A. et al. Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Phys. Rev. X* **2**, 041010 (2012).
- Patel, K. A. et al. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks. *Appl. Phys. Lett.* **104**, 051123 (2014).

18. Fröhlich, B. et al. Quantum secured gigabit optical access networks. *Sci. Rep.* **5**, 1–7 (2015).
19. Aleksic, S. et al. Perspectives and limitations of QKD integration in metropolitan area networks. *Opt. Exp.* **23**, 10359–10373 (2015).
20. cKumar, R., Qin, H. & Alléaume, R. Coexistence of continuous variable QKD with intense DWDM classical channels. *N. J. Phys.* **17**, 043027 (2015).
21. Wang, L. et al. Long-distance copropagation of quantum key distribution and terabit classical optical data channels. *Phys. Rev. A* **95**, 012301 (2017).
22. Fröhlich, B. et al. Long-distance quantum key distribution secure against coherent attacks. *Optica* **4**, 163–167 (2017).
23. Eriksson, T. et al. Coexistence of continuous variable quantum key distribution and 7×12.5 Gbit/s classical channels. *IEEE Phot. Soc. Summer Topical Meeting* 71–72 (2018).
24. Grünenfelder, F., Sax, R., Boaron, A. & Zbinden, H. The limits of multiplexing quantum and classical channels: case study of a 2.5 GHz discrete variable quantum key distribution system. *Appl. Phys. Lett.* **119**, 124001 (2021).
25. Alléaume, R., Aymeric, R., Ware, C. & Jaouën, Y. Technology trends for mixed QKD/WDM transmission up to 80 km. *Optical Fiber Communications Conference* 1–3 (2020).
26. Vokić, N., Milovančev, D., Schrenk, B., Hentschel, M. & Hübel, H. Deployment opportunities for DPS-QKD in the co-existence regime of lit GPON/NG-PON2 access networks. *Optical Fiber Communications Conference* 56 (2020).
27. Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932 (1998).
28. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
29. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
30. Pile, D. F. P. et al. Twin field QKD. *Nat. Photonics* **12**, 377 (2018).
31. Liu, Y. et al. Experimental twin-field quantum key distribution through sending or not sending. *Phys. Rev. Lett.* **123**, 100505 (2019).
32. Lim, C. C. W., Walenta, N., Legré, M., Gisin, N. & Zbinden, H. Random variation of detector efficiency: a countermeasure against detector blinding attacks for quantum key distribution. *IEEE J. Sel. Top. Quantum Electron.* **21**, 192 (2015).
33. Lu, H., Fung, C.-H. F. & Cai, Q.-Y. Two-way deterministic quantum key distribution against detector-side-channel attacks. *Phys. Rev. A* **88**, 044302 (2013).
34. Alhussein, M. & Inoue, K. Differential phase shift quantum key distribution with variable loss revealing blinding and control side-channel attacks. *Jpn. J. Appl. Phys.* **58**, 102001 (2019).
35. Yin, Z.-Q. et al. Reference-free-independent quantum key distribution immune to detector side channel attacks. *Quantum Inf. Process.* **13**, 1237 (2014).
36. Dušek, M., Jahma, M. & Lütkenhaus, N. Unambiguous state discrimination in quantum cryptography with weak coherent states. *Phys. Rev. A* **62**, 022306 (2000).
37. Makarov, V., Anisimov, A. & Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **74**, 022313 (2006).
38. 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).
39. Makarov, V. Controlling passively quenched single photon detectors by bright light. *N. J. Phys.* **11**, 065003 (2009).
40. Lydersen, L. et al. Thermal blinding of gated detectors in quantum cryptography. *Opt. Exp.* **18**, 27938 (2010).
41. Lydersen, L. et al. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **4**, 686 (2010).
42. Jain, N. et al. Device calibration impacts security of quantum key distribution. *Phys. Rev. Lett.* **107**, 110501 (2011).
43. Gerhardt, I. et al. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2**, 1 (2011).
44. Bugge, A. N. et al. Laser damage helps the eavesdropper in quantum cryptography. *Phys. Rev. Lett.* **112**, 070503 (2014).
45. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
46. 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).
47. Ferreira da Silva, T. et al. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88**, 052303 (2013).
48. Valiavarthi, R. et al. Measurement-device-independent quantum key distribution: from idea towards application. *J. Mod. Opt.* **62**, 1141 (2015).
49. Yin, H.-L. et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **117**, 190501 (2016).
50. Liu, H. et al. Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels. *Phys. Rev. Lett.* **122**, 160501 (2019).
51. Comandar, L. C. et al. Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nat. Photonics* **10**, 312 (2016).
52. Tang, Y.-L. et al. Measurement-device-independent quantum key distribution over untrusted metropolitan network. *Phys. Rev. X* **6**, 011024 (2016).
53. Wang, X.-B., Yu, Z.-W. & Hu, X.-L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **98**, 062323 (2018).
54. Chen, J.-P. et al. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. *Nat. Photonics* **15**, 570–575 (2021).
55. Liu, H. et al. Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km. *Phys. Rev. Lett.* **126**, 250502 (2021).
56. Woodward, R. I. et al. Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers. *NPJ Quantum Inf.* **1**, 1 (2021).
57. Valiavarthi, R. et al. Measurement-device-independent quantum key distribution coexisting with classical communication. *Quantum Sci. Technol.* **4**, 045002 (2019).
58. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85**, 1330 (2000).
59. Yu, Z.-W., Zhou, Y.-H. & Wang, X.-B. Three-intensity decoy-state method for measurement-device-independent quantum key distribution. *Phys. Rev. A* **88**, 2044 (2013).
60. Hong, C. K., Ou, Z.-Y. & Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044 (1987).
61. Bahrani, S., Razavi, M. & Salehi, J. A. Wavelength assignment in hybrid quantum-classical networks. *Sci. Rep.* **8**, 1–13 (2018).
62. Elmabrok, O., Ghalaii, M. & Razavi, M. Quantum-classical access networks with embedded optical wireless links. *J. Opt. Soc. Am. B* **35**, 487–499 (2018).
63. Zhou, Y.-H., Yu, Z.-W. & Wang, X.-B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys. Rev. A* **93**, 042324 (2016).

Acknowledgements

The authors thank Cisco Systems for the equipment and support in the project, especially Robert Broberg, Michael Beesley, and Bill Gartner during the conception, incubation, and early planning of the project, including procuring the Cisco equipment and seeing to its delivery, as well as Al Lynn for his support throughout the endeavor, Walter van de Garde and Cisco Cyber Security Netherlands for further support, Koninklijke KPN N. V. for hosting the network and providing fiber and technical support, and David Elkouss for valuable discussions. The authors acknowledge funding through the Netherlands Organization for Scientific Research (NWO) and the European project OpenQKD.

Author contributions

R.C.B., T.M., and J.A.S. performed the experiments, and with R.F.L.V. built the quantum setup, and with important contributions from all authors, wrote the manuscript. The conventional IP networks design was led by L.D.C., F.B., S.P., and R.P., with inputs from all authors. P.U., J.F.M., and W.T. contributed to the early stages of the work. R.C.B., T.M., L.D.C., F.B., S.P., R.P., and J.A.S. integrated the quantum and IP networks.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at <https://doi.org/10.1038/s42005-022-00964-6>.

Correspondence and requests for materials should be addressed to Joshua A. Slater.

Peer review information *Communications Physics* thanks Yichen Zhang and the other, anonymous, reviewer(s) for their contribution to the peer review of this work.

Reprints and permission information is available at <http://www.nature.com/reprints>

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



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

© The Author(s) 2022