Chip-based measurement-device-independent quantum key distribution using integrated silicon photonic systems

Cao, Lin; Luo, W.; Wang, Yunxiang; Zou, J.; Yan, R. D.; Cai, H.; Zhang, Yichen; Hu, X. L.; Jiang, C.; Fan, W. J.; Zhou, X. Q.; Dong, B.; Luo, X. S.; Lo, G. Q.; Wang, Y. X.; Xu, Z. W.; Sun, S. H.; Wang, X. B.; Hao, Y. L.; ...Liu, Aiqun

2020

Cao, L., Luo, W., Wang, Y., Zou, J., Yan, R. D., Cai, H., . . . Liu, A. (2020). Chip-based measurement-device-independent quantum key distribution using integrated silicon photonic systems. *Physical Review Applied*, 14(1), 011001-.
doi:10.1103/PhysRevApplied.14.011001

<https://hdl.handle.net/10356/145454>

<https://doi.org/10.1103/PhysRevApplied.14.011001>

© 2020 American Physical Society (APS). All rights reserved. This paper was published in *Physical Review Applied* and is made available with permission of American Physical Society (APS).

Downloaded on 26 Apr 2023 17:46:29 SGT

Chip-Based Measurement-Device-Independent Quantum Key Distribution Using Integrated Silicon Photonic Systems

L. Cao,^{1,2,†} W. Luo,^{2,†} Y.X. Wang,^{2,3,†} J. Zou,² R.D. Yan,² H. Cai,⁴ Y. Zhang,² X.L. Hu,⁵ C. Jiang,⁵ W.J. Fan,² X.Q. Zhou,⁶ B. Dong,⁷ X.S. Luo,⁷ G.Q. Lo,⁷ Y.X. Wang,⁸ Z.W. Xu,⁸ S.H. Sun,^{9,*} X.B. Wang,^{5,†} Y.L. Hao,¹ Y.F. Jin,¹ D.L. Kwong,⁴ L.C. Kwek,^{2,10,‡} and A.Q. Liu^{2,§,**}

¹*School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China*

²*Quantum Science and Engineering Centre (QSec), Nanyang Technological University, Singapore 639798, Singapore*

³*School of Optoelectronic Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China*

⁴*Institute of Microelectronics, A*STAR (Agency for Science, Technology and Research), Singapore 138634, Singapore*

⁵*State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, China*

⁶*State Key Laboratory of Optoelectronic Materials and Technologies and School of Physics, Sun Yat-sen University, Guangzhou 510275, China*

⁷*Advanced Micro Foundry, Pte Ltd, Singapore 117685, Singapore*

⁸*Institute for Infocomm Research (I2R), A*STAR (Agency for Science, Technology and Research), Singapore 138632, Singapore*

⁹*School of Physics and Astronomy, Sun Yat-Sen University, Zhuhai 519082, China*

¹⁰*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore*

(Received 11 March 2020; revised 14 May 2020; accepted 18 May 2020; published 17 July 2020)

Measurement-device-independent (MDI) quantum key distribution (QKD) employs an untrusted relay to prevent the receiver from side-channel attacks commonly encountered in earlier QKD protocols. Conventional MDI QKD systems rely entirely on bulky and expensive optical setups that present great challenges for system scaling and integration. In this work, an all-chip-based MDI QKD system including two transmitter chips and one server chip is demonstrated using integrated silicon photonic technology. The system is capable of generating polarization-encoded weak coherent states with polarization extinction ratios of over 20 dB, sufficient for low-error MDI QKD. In the proof-of-concept experiment, the chip-based MDI QKD system generates a key rate per pulse of 2.923×10^{-6} over a distance corresponding to a 50-km standard fiber with 25% detection efficiency and a predicted distance of 120 km with 85% detection efficiency. Our proof-of-concept prototype makes a giant step forward towards fully chip-based MDI QKD systems and highly integrated quantum communication networks in the near future with its high scalability and cost effectiveness.

DOI: [10.1103/PhysRevApplied.14.011001](https://doi.org/10.1103/PhysRevApplied.14.011001)

Quantum key distribution (QKD) promises a highly secure way of sharing secret keys between two individuals [1–3]. It has been successfully demonstrated in fiber [4,5], free-space [6], and satellite platforms [7,8]. However, conventional QKD systems are unable to guarantee the theoretical unconditional security due to imperfect implementations of QKD in practical scenarios [9–11]. For example, an eavesdropper might be able to remotely control the single-photon detectors in a QKD system and steal the full secret key without leaving a trace [12]. To counter such side-channel attacks, measurement-device-independent (MDI) QKD, which obviates any assumptions made for the measurement device, has been proposed

and demonstrated [13–22]. The MDI QKD architecture is naturally suited for multiuser QKD networks, since the most expensive and intricate component—the measurement device—can be placed in an untrusted relay and shared among many QKD users. Therefore, MDI QKD has been widely recognized as a promising quantum communication technology for star-type secured networks [23,24].

Conventional MDI QKD systems rely entirely on bulky and expensive optical setups that present great challenges for system scaling and integration. In contrast, silicon photonic technology offers many unparalleled benefits including small size, low cost, low power consumption, and well-established batch fabrication techniques [25].

*sunshh8@mail.sysu.edu.cn; †xbwang@mail.tsinghua.edu.cn; ‡kwekleongchuan@nus.edu.sg; §eaqliu@ntu.edu.sg; ¶These authors contributed equally; **To whom requests for materials should be sent.

Over the past few years, much effort has been directed toward chip-level implementation of discrete-variable QKD [26–29] and continuous-variable QKD [30]. In these schemes, silicon photonic chip-based QKD enables quantum communication systems that are not only phase stable and easily tailorable, but also straightforward to realize high-speed QKD with precise time sequence alignment. Recently, several photonic chips for MDI QKD have been fabricated on different substrates, e.g., silica [31], InP [32], and silicon [33]. However, these works only demonstrated hybrid chip-based MDI QKD systems with either two transmitter chips plus a fiber-based server [32,33] or two fiber-based transmitters plus a silica-substrate-based server chip [31]. It still remains a challenge to establish a long-desired, low-cost, and scalable quantum communication network using all-chip-based MDI QKD systems.

Here, a proof-of-concept all-chip-based MDI QKD system with two chip-based transmitters and one chip-based server integrated using silicon photonic technology is demonstrated. Key components of the transmitter chip, including intensity modulators for decoy states, phase modulators, and polarization modulators, are integrated onto a single chip. The server chip integrates polarization-independent beam splitters (BS) and polarizing beam splitters (PBS). The all-chip-based MDI QKD system promises great potential for scalable and cost-effective secured communications.

Figure 1 shows a schematic of the chip-based MDI QKD system comprising two transmitter chips (Alice and Bob) and one server chip (Charlie). For each transmitter chip, a pulse-modulated laser is coupled into the silicon waveguide through a grating coupler. The first Mach-Zehnder interferometer (MZI) modulator modifies the laser intensity to create signal and decoy states, and another phase modulator implements random phase modulations of the input pulses to guarantee the phase randomization assumption. Polarization states $|H\rangle$, $|V\rangle$, $|+\rangle$, and $|-\rangle$ are encoded by a polarization modulator consisting of

a MZI modulator, a path-to-polarization converter (PPC), and phase shifters at the PPC input arms. The resulting states are coupled out of the chip through an adiabatic tapered waveguide coupler and a lensed fiber. After attenuation, the weak coherent pulses from the two transmitter chips reach the server chip (Charlie) via optical fiber spools. The server chip consists of a polarization-independent BS and two PBS and performs Bell state measurement of the incoming pulses. The pulses are compensated for polarization drift by polarization controllers in order to maximize the Hong-Ou-Mandel (HOM) interference between the transmitted photons from Alice and Bob chips. Finally, all coincidence events for secure key generation are publicly announced.

Both the MDI QKD transmitter and server chips are designed and fabricated using advanced silicon photonic fabrication techniques, which utilize silicon-on-insulator wafer with a top silicon layer of 220 nm and a buried oxide layer of 3 μm . Figures 2(a) and 2(b) show optical micrographs of the transmitter and server chips, respectively. Figure 2(c) shows the transmitter chip packaged on a printed circuit board.

The PPC is a key component of the MDI QKD chips. It consists of a mode combiner and a polarization rotator [34]. Figure 3 shows the simulation and characterization results of the PPC. The mode conversion versus the coupling length L_c for TE_0 mode input at the upper and lower port at $\lambda = 1.55 \mu\text{m}$ is illustrated in Fig. 3(a). Nearly 100% power conversion from TE_0 mode in the upper waveguide to TE_1 mode in the lower waveguide occurs at $L_c > 280 \mu\text{m}$, and the transmission of TE_0 mode at the lower input port is unaffected. Figure 3(b) shows the simulated transmission of TE_1 mode to TM_0 mode with respect to the length L_r of the polarization rotator at $\lambda = 1.55 \mu\text{m}$. It is observed that the power is completely transferred from TE_1 mode to TM_0 mode as L_r increases to 80 μm and above, while the propagation of TE_0 mode remains unaffected. Therefore, L_r in the polarization rotator is set

FIG. 1. Schematic of the silicon photonic chip-based MDI QKD system. The system comprises three silicon photonic chips (Alice, Bob, and Charlie) among which Alice and Bob chips are the transmitters and Charlie chip is the server. Alice and Bob chips consist of intensity modulators, phase modulators, and polarization modulators, which are capable of generating phase-randomized signal and decoy-state weak coherent pulses in BB84 polarization states. Charlie comprises a polarization-independent BS and two PBS and performs Bell state measurement of the incoming states with off-chip single-photon detectors (SPDs). MOD, modulator; PPC, path-to-polarization converter; EPC, electrically driven polarization controller.

FIG. 2. Optical images of the MDI QKD chips. (a) Micrograph of the transmitter chip (Alice or Bob). (b) Micrograph of the server chip (Charlie). The chip is designed with adiabatic tapered waveguide couplers at input ports and grating couplers at output ports. The waveguides are marked as magenta. (c) Photograph of a packaged chip on a printed circuit board.

to $90\ \mu\text{m}$ and L_c in the combiner is set to $300\ \mu\text{m}$ (see Supplemental Material for detailed design [34–37]). In the transmitter chip, the PPC is used to combine $\alpha|TE_0\rangle$ of the upper waveguide and $\beta|TE_0\rangle$ of the lower waveguide with different amplitudes and relative phases into an arbitrary polarization state $\alpha|TM_0\rangle + \beta|TE_0\rangle$ that is then coupled to an optical fiber with a polarization of $\alpha|V\rangle + \beta|H\rangle$. In the server chip, the PPC is employed inversely, and the arbitrary polarization of $\alpha|V\rangle + \beta|H\rangle$ from the optical fiber is

converted into $\alpha|TE_0\rangle$ in the upper port and $\beta|TE_0\rangle$ in the lower port. Figure 3(c) shows an optical micrograph of the combiner in the PPC. Figure 3(d) presents the measured transmission spectra of the designed PPC for TE_0 input at the upper and lower ports. It is observed that the on-chip loss of TE_0 input is less than 0.3 dB at the lower port and less than 0.6 dB at the upper port. The polarization extinction ratios (PERs) of the upper and lower output ports are greater than 22.5 and 20.5 dB, respectively, within the testing range between 1530 and 1570 nm. In our chip-based MDI QKD system, the wavelength of the laser is set to 1542.3815 nm, which has a PER of approximately 26 dB for the lower port and approximately 32 dB for the upper port, as indicated by the scarlet line in Fig. 3(d). Such a high PER would decrease the quantum bit error rate (QBER) that in turn improves the key rate in the MDI QKD system.

The MDI QKD transmitter chips are calibrated using a fiber-based polarization alignment system that consists of a 50:50 BS for passive selection of the measurement basis, with one arm connected to a PBS to measure $|H\rangle$ and $|V\rangle$ and the other arm coupled to a PBS to measure $|+\rangle$ and $|-\rangle$ (see Supplemental Material for details [35]). By tuning the voltages applied to the MZI modulator and one of the phase shifters in the polarization modulator, polarization states in rectilinear (Z) and diagonal (X) bases are obtained with PERs of over 20 dB (Fig. 4). For the intensity modulator, a typical extinction ratio of 30 dB is achieved, which is sufficient for a decoy-state MDI QKD system.

Lastly, a four-intensity decoy-state MDI QKD protocol is demonstrated on our chip-based system as a proof of concept. Since MDI QKD primarily relies on HOM interference at Charlie chip, the transmitter chips are required to produce indistinguishable states to maximize

FIG. 3. Path-to-polarization converter. (a) Simulated transmission in the combiner for TE_0 input at upper and lower ports, at $\lambda = 1.55\ \mu\text{m}$, with field propagations shown in the inset. (b) Simulated transmission in the polarization rotator for TE_1 and TE_0 mode input, at $\lambda = 1.55\ \mu\text{m}$, with field propagations shown in the inset. (c) Optical micrograph of the fabricated combiner in the PPC. (d) Measured transmission spectra of the PPC for TE_0 input at the upper and lower ports. The scarlet line indicates the wavelength employed in our MDI QKD system.

FIG. 4. On-chip polarization state preparation. Normalized transmission of the polarization states $|H\rangle$ (black triangles), $|V\rangle$ (red circles), $|+\rangle$ (green diamonds), and $|-\rangle$ (blue squares) is plotted versus voltages applied to the MZI modulator in the polarization modulator. The voltages on the phase shifter of the polarization modulator are respectively fixed to 1.50, 2.65, 1.80, and 2.22 V for $|H\rangle$, $|V\rangle$, $|+\rangle$, and $|-\rangle$ states during the measurement. The black, red, green, and blue lines represent the fitted curves for $|H\rangle$, $|V\rangle$, $|+\rangle$, and $|-\rangle$ states, respectively. The polarization modulator is capable of providing an extinction ratio of over 20 dB.

the interference. A HOM visibility of approximately 48% is achieved, which is comparable to the theoretical maximal visibility of 50% with weak coherent states. The four-intensity decoy-state protocol is implemented with intensities of $\{\mu = 0.374, \nu = 0.228, \omega = 0.071, o = 0\}$ and the finite-key effect taken into consideration [38,39]. The parameters are optimized using the joint constraints in statistical fluctuation of different observables. Figure 5 shows a comparison of the theoretical and experimental results of the secure key rate per pulse versus different transmission distances with various types of single-photon detectors. The data are collected using optical attenuators to emulate the attenuation of standard single-mode fiber (0.2 dB/km). Due to the optimal interference, a QBER of approximately 0.67% is observed in the Z basis. The QBER measured in the X basis is approximately 25.6%, which is comparable to the theoretical value of 25% on account of the visibility limit of 50%. At a total loss of 10 dB (corresponding to a distance of 50 km in standard fiber), 4.0×10^{10} pulse pairs are sent from each transmitter chip. The key rate per pulse is 2.923×10^{-6} , which agrees well with the theoretical simulation and is comparable to the results from previous MDI QKD studies (Fig. 5) [14,15,17–20,24]. Considering the clock rate of 0.5 MHz using thermo-optic modulation in the experiment, we have achieved a secret key rate of 1.46 bps with a distance corresponding to 50 km. The key

FIG. 5. Secure key rates per pulse with different transmission distances. The blue solid line is the theoretical simulation result according to the corresponding experimental conditions using InGaAs/InP single-photon avalanche diodes with a detection efficiency of approximately 25%. The red solid triangle shows the experimental result with a total transmission loss of 10 dB (corresponding to fiber distance of 50 km). The green dashed line and red dash-dotted line are simulation results with two different superconducting nanowire single-photon detectors (SNSPD). SNSPD1 has a detection efficiency of 53% and SNSPD2 has a detection efficiency of 85%. Key rates per pulse of previous MDI QKD experiments are also plotted as green star [15], purple diamond [14], blue circle [17], magenta square [18], orange hexagon [24], violet pentagon [19], and pink cross [20].

rate can be further increased by utilizing carrier-depletion modulator that operates more rapidly in the GHz band [40]. By evaluating the parameters of the detector with a higher detection efficiency of 85%, the same MDI QKD chips are capable of transmitting keys over 120 km (see Fig. 5).

In conclusion, we have demonstrated an all-chip-based photonic MDI QKD system with two transmitter chips and one server chip that integrates intensity modulators, phase modulators, polarization modulators, BS, and PBS by using silicon photonic fabrication technology. The photonic chip-based MDI QKD system is capable of generating polarization-encoded weak coherent states with PERs of over 20 dB that meets the requirements for low-error MDI QKD. The system has implemented BB84 MDI QKD protocol over a distance corresponding to 50 km with 25% detection efficiency and a predicted distance over 120 km with 85% detection efficiency for proof of concept. The key rate per pulse of 2.923×10^{-6} is comparable to that reported in previous works [14,15,17–20,24] and can be further optimized using single-photon detectors with higher detection efficiencies. The system reported in this work demonstrates a proof of concept and promises great potential towards highly integrated quantum communication systems for QKD networks and quantum-classical

hybrid communication. With further integration of laser diodes, optical switches, wavelength demultiplexers, and multichannel single-photon detectors on the transmitter and server chips, it is possible to build a fully chip-based commercial MDI QKD system in the near future with high scalability and cost effectiveness.

Experimental setup for MDI QKD. Alice and Bob consist of two independent frequency-locked laser sources (Clarity-NLL-1542-HP) with LiNbO₃ intensity modulators, producing 10-ns laser pulses at 1542.3815 nm with a repetition rate of 0.5 MHz. This configuration allows transmitter chips to prepare weak coherent states in one of four polarization states: $|H\rangle$, $|V\rangle$ (rectilinear or Z basis) or $|+\rangle$, $|-\rangle$ (diagonal or X basis). Alice, Bob, and Charlie share an electrically distributed reference clock to which their preparation and detection equipment are synchronized. Free-running InGaAs/InP avalanche photodiodes (ID230) are synchronized and gated to the arrival time of the photons with a 50- μ s deadline. The coincidence window of the detectors is set to around 22 ns. The efficiency of the detectors is kept around 25% for all the data points in the experiment.

Four-intensity decoy-state MDI QKD. In the MDI QKD experiment, a four-intensity decoy-state protocol is implemented [38]. Each time Alice and Bob chips randomly and independently choose one of the four intensities, $\{\mu, \nu, \omega, o = 0 (\nu > \omega)\}$, with probabilities of p_μ, p_ν, p_ω , and p_o , respectively, to send weak coherent states to Charlie. The states with the intensity μ are prepared in Z basis and those with the intensities ν and ω are prepared in X basis. The states with the intensity o are vacuum states.

With the finite-key effect taken into consideration [39], the key rate of the protocol is given by

$$R = p_\mu^2 \left\{ \mu e^{-\mu} \underline{s}_{11} [1 - H(\overline{e}_{11}^{\text{ph}})] - f S_{\mu\mu} H(E_{\mu\mu}) \right\} - \frac{1}{N_{\text{total}}} \left(\log_2 \frac{2}{\varepsilon_{\text{cor}}} + 2 \log_2 \frac{1}{\sqrt{2} \varepsilon_{\text{PA}} \hat{\varepsilon}} \right),$$

where $\underline{s}_{11}$ and $\overline{e}_{11}^{\text{ph}}$ are the bound of counting rate and phase-flip error rate of single-photon pulse pairs that can be obtained by the decoy-state method, $S_{\mu\mu}$ and $E_{\mu\mu}$ are counting rate and bit-flip error rate when Alice and Bob both send states with the intensity μ , $H(p) = -p \log_2 p - (1-p) \log_2 (1-p)$ is the binary entropy function, f is the correction efficiency, which is set to 1.1, N_{total} is the total number of pulses that each of Alice and Bob sends, and ε_{cor} , ε_{PA} , and $\hat{\varepsilon}$ are some failure probabilities in the finite-key analysis, all of which are set to 10^{-10} in the calculation. The four-intensity protocol uses the joint constraints in statistical fluctuation of different observables [38,41], which greatly improves the key rate.

Acknowledgments. This work is supported by the Singapore Ministry of Education (MOE) Tier 3 grant (No. MOE2017-T3-1-001), the Singapore National Research Foundation (NRF) National Natural Science Foundation of

China (NSFC) joint grant (No. NRF2017NRF-NSFC002-014), and the Singapore National Research Foundation under the Competitive Research Program (No. NRF-CRP13-2014-01).

- [1] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (IEEE Press, New York, 1984), pp. 175–179.
- [2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [3] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, *Nat. Photonics* **8**, 595 (2014).
- [4] C. Gobby, Z. Yuan, and A. Shields, Quantum key distribution over 122 km of standard telecom fiber, *Appl. Phys. Lett.* **84**, 3762 (2004).
- [5] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Broui, S. W. McLaughlin *et al.*, Quantum key distribution over 25 km with an all-fiber continuous-variable system, *Phys. Rev. A* **76**, 042305 (2007).
- [6] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, *J. Cryptol.* **5**, 3 (1992).
- [7] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang *et al.*, Direct and full-scale experimental verifications towards ground-satellite quantum key distribution, *Nat. Photonics* **7**, 387 (2013).
- [8] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, Satellite-to-ground quantum key distribution, *Nature* **549**, 43 (2017).
- [9] V. Makarov, A. Anisimov, and J. Skaar, Effects of detector efficiency mismatch on security of quantum cryptosystems, *Phys. Rev. A* **74**, 022313 (2006).
- [10] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Time-shift attack in practical quantum cryptosystems, *Quantum Inf. Comput.* **7**, 73 (2007).
- [11] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, *Phys. Rev. A* **78**, 042333 (2008).
- [12] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, *Nat. Photonics* **4**, 686 (2010).
- [13] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent Quantum key Distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [14] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Real-world two-Photon Interference and Proof-of-Principle Quantum key Distribution Immune to Detector Attacks, *Phys. Rev. Lett.* **111**, 130501 (2013).
- [15] T. F. Da Silva, D. Vitoireti, G. Xavier, G. Do Amaral, G. Temporao, and J. Von Der Weid, Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits, *Phys. Rev. A* **88**, 052303 (2013).
- [16] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Experimental Demonstration of Polarization Encoding

- Measurement-Device-Independent Quantum key Distribution, *Phys. Rev. Lett.* **112**, 190503 (2014).
- [17] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan *et al.*, Measurement-device-independent Quantum key Distribution Over 200 km, *Phys. Rev. Lett.* **113**, 190501 (2014).
- [18] Z. Tang, K. Wei, O. Bedroia, L. Qian, and H.-K. Lo, Experimental measurement-device-independent quantum key distribution with imperfect sources, *Phys. Rev. A* **93**, 042308 (2016).
- [19] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang *et al.*, Measurement-device-independent Quantum key Distribution Over a 404 km Optical Fiber, *Phys. Rev. Lett.* **117**, 190501 (2016).
- [20] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, Quantum key distribution without detector vulnerabilities using optically seeded lasers, *Nat. Photonics* **10**, 312 (2016).
- [21] X.-B. Wang, Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors, *Phys. Rev. A* **87**, 012320 (2013).
- [22] F. Xu, H. Xu, and H.-K. Lo, Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution, *Phys. Rev. A* **89**, 052333 (2014).
- [23] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, A quantum access network, *Nature* **501**, 69 (2013).
- [24] R. Valivarthi, Q. Zhou, C. John, F. Marsili, V. B. Verma, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, A cost-effective measurement-device-independent quantum key distribution system for quantum networks, *Quantum Sci. Technol.* **2**, 04LT01 (2017).
- [25] A. Orieux and E. Diamanti, Recent advances on integrated quantum communications, *J. Opt.* **18**, 083002 (2016).
- [26] C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. Poon, Silicon photonic transmitter for polarization-encoded quantum key distribution, *Optica* **3**, 1274 (2016).
- [27] P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, Integrated silicon photonics for high-speed quantum key distribution, *Optica* **4**, 172 (2017).
- [28] D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein *et al.*, Metropolitan quantum key distribution with silicon photonics, *Phys. Rev. X* **8**, 021009 (2018).
- [29] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits, *npj Quantum Inf.* **3**, 25 (2017).
- [30] G. Zhang, J. Haw, H. Cai, F. Xu, S. Assad, J. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu *et al.*, An integrated silicon photonic chip platform for continuous-variable quantum key distribution, *Nat. Photonics*, **13**, 839 (2019).
- [31] C.-Y. Wang, J. Gao, Z.-Q. Jiao, L.-F. Qiao, R.-J. Ren, Z. Feng, Y. Chen, Z.-Q. Yan, Y. Wang, H. Tang, and X.-M. Jin, Integrated measurement server for measurement-device-independent quantum key distribution network, *Opt. Express* **27**, 5982 (2019).
- [32] H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, Chip-based measurement-device-independent quantum key distribution, *Optica* **7**, 238 (2020).
- [33] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. arXiv preprint arXiv:1911.00690 (2019).
- [34] W. D. Sacher, T. Barwicz, B. J. Taylor, and J. K. Poon, Polarization rotator-splitters in standard active silicon photonics platforms, *Opt. Express* **22**, 3777 (2014).
- [35] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevApplied.14.011001> for further information about fabrication, component design, calibration setup and experimental results.
- [36] H. Guan, Y. Ma, R. Shi, A. Novack, J. Tao, Q. Fang, A. E.-J. Lim, G.-Q. Lo, T. Baehr-Jones, and M. Hochberg, Ultracompact silicon-on-insulator polarization rotator for polarization-diversified circuits, *Opt. Lett.* **39**, 4703 (2014).
- [37] Y. Ma, Y. Liu, H. Guan, A. Gazman, Q. Li, R. Ding, Y. Li, K. Bergman, T. Baehr-Jones, and M. Hochberg, Symmetrical polarization splitter/rotator design and application in a polarization insensitive WDM receiver, *Opt. Express* **23**, 16052 (2015).
- [38] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Making the decoy-state measurement-device-independent quantum key distribution practically useful, *Phys. Rev. A* **93**, 042324 (2016).
- [39] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, *Nat. Commun.* **5**, 3732 (2014).
- [40] A. Liu, L. Liao, D. Rubin, H. Nguyen, B. Ciftcioglu, Y. Chetrit, N. Izhaky, and M. Paniccia, High-speed optical modulation based on carrier depletion in a silicon waveguide, *Opt. Express* **15**, 660 (2007).
- [41] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method, *Phys. Rev. A* **91**, 032318 (2015).