# Proof-of-Principle Demonstration of Fully Passive Quantum Key Distribution

Chengqiu Hu,[1,*] Wenyuan Wang,[1] Kai-Sum Chan,[1,2] Zhenghan Yuan,[1] and Hoi-Kwong Lo[1,2,3,4,†]
[1]*Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong*
[2]*Quantum Bridge Technologies, Inc., 100 College Street, Toronto, Ontario M5G 1L5, Canada*
[3]*Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*
[4]*Centre for Quantum Information and Quantum Control (CQIQC), Department of Physics, University of Toronto, Toronto, Ontario, M5S 1A7, Canada*

(Received 9 May 2023; accepted 17 August 2023; published 13 September 2023)

Quantum key distribution (QKD) offers information-theoretic security based on the fundamental laws of physics. However, device imperfections, such as those in active modulators, may introduce side-channel leakage, thus compromising practical security. Attempts to remove active modulation, including passive decoy intensity preparation and polarization encoding, have faced theoretical constraints and inadequate security verification, thus hindering the achievement of a fully passive QKD scheme. Recent research [W. Wang *et al.*, Phys. Rev. Lett. **130**, 220801 (2023).; V. Zapatero *et al.*, Quantum Sci. Technol. **8**, 025014 (2023).] has systematically analyzed the security of a fully passive modulation protocol. Based on this, we utilize the gain-switching technique in combination with the postselection scheme and perform a proof-of-principle demonstration of a fully passive quantum key distribution with polarization encoding at channel losses of 7.2 dB, 11.6 dB, and 16.7 dB. Our work demonstrates the feasibility of active-modulation-free QKD in polarization-encoded systems.

DOI: 10.1103/PhysRevLett.131.110801

*Introduction.*—Quantum key distribution (QKD) has emerged as a promising technology to ensure information-theoretically secure communications [3,4]. Despite its strong theoretical foundation, practical QKD systems are susceptible to side-channel attacks, which can compromise their practical security. While measurement-device-independent QKD [5–7] and twin-field QKD protocols [8–11] have been proposed to address side-channel vulnerabilities in the measurement unit, source modulators in current implementations still present significant challenges [12,13].

The conventional method of active modulation using phase and intensity modulators can introduce side channels and are vulnerable to Trojan horse attacks, [14–19] in which an eavesdropper may inject strong light into the modulator and analyze the back-reflected signal to obtain information. In addition, active modulators face other practical issues. The pattern effect arises in high-speed systems when the modulation strength of adjacent pulses influences each other, causing undesired correlations [20,21]. The commonly used electro-optic modulators often require high driving voltages, posing technical challenges for high-speed electronic systems. Besides, commercially available electro-optic modulators tend to be expensive, bulky, and difficult to integrate [22,23].

Previous research has attempted to implement passively decoy-state generating or polarization encoding [24–29]. These approaches have paved the way for further innovation, though they do not achieve a complete passive modulation. Another approach involves the use of injection locking and direct phase modulation [30,31], which enables modulator-free QKD systems based on phase encoding, such as time-bin encoding. However, direct phase modulation often requires meticulous fine-tuning and may involve considerable technical complexity. In recent work [1,2], a fully passive QKD solution was proposed along with a systematic security analysis, but so far a comprehensive experimental demonstration is yet to be completed.

The implementation of fully passive QKD presents several major challenges. First, the scheme requires input coherent pulses with independent and random phases, while ensuring that these pulses have highly consistent intensity and frequency to achieve sufficient interference visibility. Our solution involves using a single laser instead of multiple lasers, driving it in a gain-switch manner [32] to generate intrinsic randomness. By introducing a delay between consecutive pulses, they can be treated as independent pulse sources, thereby avoiding the frequency deviation associated with multilaser protocol. Another challenge here is that the fully passive QKD schemes require local measurements to collect large amounts of data due to postselection needs. We address this issue by using the experimental setup shown in Fig. 2, requiring a minimum of only two photodetectors to complete local measurements, and utilizing a high-speed acquisition card for continuous data collection. By adeptly utilizing a customized postselection approach, we efficiently tackle the challenges posed by the signal intensity and polarization

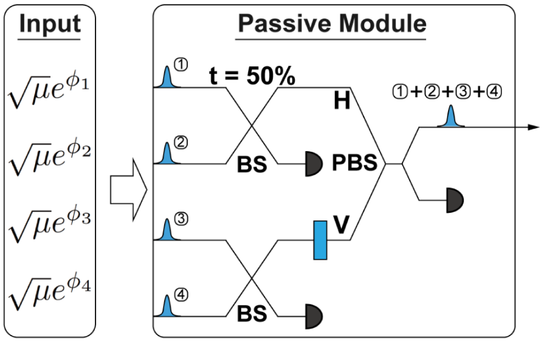

FIG. 1. Illustration of the fully passive protocol. The input here consists of four coherent light pulses with random phases. The so-called passive module is used for fully passive decoy-state preparation and polarization encoding.

coupling in a fully passive setup. Our proof-of-principle experiment validates that this protocol [1] can perform passive decoy-state preparation preparation and polarization encoding simultaneously, successfully demonstrating a fully passive QKD system with improved security and robustness.

*Fully passive modulation.*—As illustrated in Fig. 1, our fully passive modulation module takes four coherent states with identical intensities and random phases as inputs to produce any polarization state on the Bloch sphere with a random intensity between 0 and the maximum value. Generally, we can write the four strong inputs as $\{\sqrt{\mu}e^{\phi_1}, \sqrt{\mu}e^{\phi_2}, \sqrt{\mu}e^{\phi_3}, \sqrt{\mu}e^{\phi_4}\}$, and the whole process can be described as follows. (1) Regarding passive decoy state generation, we divide the four input states of strong light into two groups and inject them into 50:50 beam splitters for interference. Taking one of the groups as an example, we choose one of the interference outputs and keep it for local measurement, while the other output serves as the H(V) polarization component that will be used for the next step. The intensities of the two polarization components can be expressed as $\mu_{H(V)} = \mu[1 + \cos\phi_{H(V)}]$, in which $\phi_{H(V)} = \phi_{1(3)} - \phi_{2(4)}$, $\mu_{H(V)} \in [0, \mu_{\max}]$. Notice that the phase $\phi_i$ $(i = 1, 2, 3, 4)$ here is independent random values uniformly distributed in $[0, 2\pi]$; the obtained intensities of H(V) components follow a U-shaped distribution, whose probability density function is expressed as $f(\mu) = 1/\pi\sqrt{\mu(\mu_{\max} - \mu)}$. Then a postselection strategy will be used to reshape the intensity distribution to $g(\mu) = Ce^{u}$, where $C$ is a constant. (2) With respect to passive polarization encoding, we obtain the final polarization-encoded state by combining the H and V components from the previous step through a polarization beam splitter. We also need to use a beam splitter to split a portion of the strong light for local measurement. The obtained polarization state can be described by

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|H\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|V\rangle, \qquad (1)$$

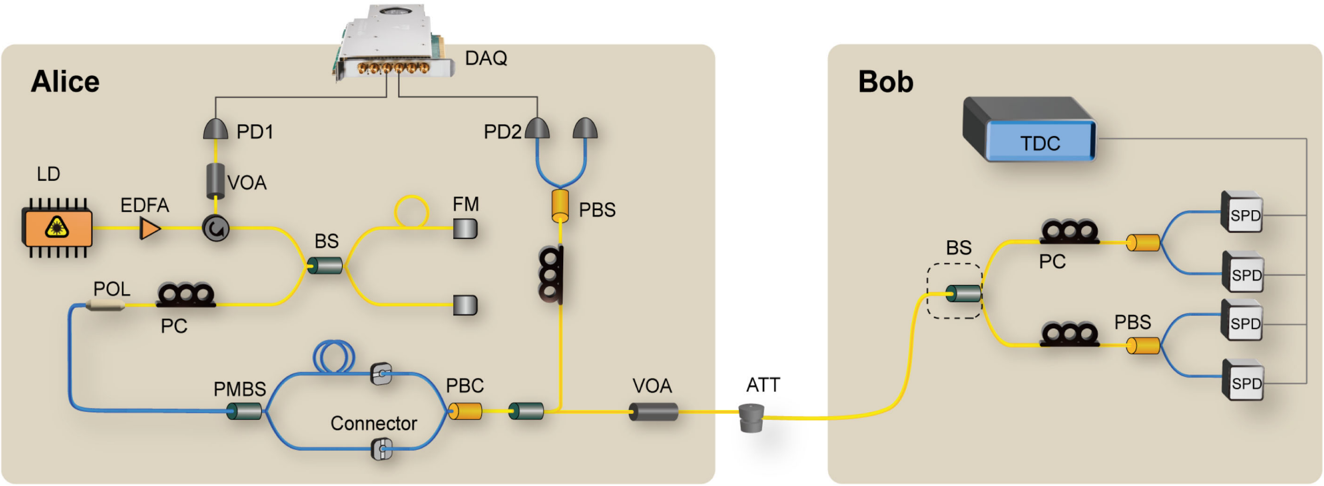

FIG. 2. Experimental setup. On the Alice side, we use an unequal arm MZI for passive decoy-state preparation and employ a polarization beam splitter and a polarization combiner for polarization synthesis. Detector PD1 is used for local measurements on the Z basis, while detector PD2 is used for local measurements on the X basis. The results are collected by a data acquisition card (DAQ). LD, laser; PD, photodiode; BS, beam splitter; PC, polarization controller; POL, polarizer; PMBS, polarization-maintaining beam splitter; PBC (PBS), polarization beam combiner (splitter); ATT, attenuator. On the Bob side, a standard BB84 decoding setup with four single-photon detectors is used. The data are collected by a time-digital converter. SPD, single-photon detector; TDC, time-digital convertor. Single-mode fiber is represented by yellow in this figure while polarization-maintaining fiber is represented by blue. For the part within the dashed box, one can principally use a passive beam splitter with a highly unbalanced basis choice, or an active switch with a Z basis choice probability approaching 1. Here, as a proof-of-principle demonstration, we manually switched between the X and Z bases and measured them separately.

where $\cos(\theta/2) = \sqrt{\mu_H/(\mu_H + \mu_V)}$ and $\phi = \phi_V - \phi_H$. It is not difficult to see from Eq. (1) that for any above-given states $\{\phi_1, \phi_2, \phi_3, \phi_4\}$, the output state corresponds to a point on the Bloch sphere that can be uniquely determined by the polar angle $\theta$ and azimuthal angle $\phi$. Actually, it has been proved that any point on the Bloch sphere can also be generated from a set of input states $\{\phi_i\}$ [1], thus establishing a one-to-one mapping between the input set and output states.

*Experimental setup.*—As illustrated in Fig. 2, an experimental setup with a single laser source is designed for a proof-of-principle demonstration of a fully passive QKD protocol. On the Alice side, in order to generate the initial coherent states with random phases, we utilize a laser diode modeled EP1550-0-NLW and operate it in gain-switch mode. In this mode, by controlling the driving current, the diode emits a pulsed laser with random phases seeded from spontaneous emission. By implementing closed-loop temperature control and precisely setting the driving current, we set the laser's central wavelength at 1547.38 nm. Using the periodic driving signals generated by an arbitrary waveform generator (AWG, Keysight-M8195), we obtained laser pulses with a repetition rate of 20 MHz, an average power of 0.1 mW, and an effective pulse width of 2 ns. Then, we use an erbium-doped fiber amplifier (EDFA) to boost the laser power to about 15 mW, ensuring that high-precision local measurements can still be conducted even after the losses incurred by various devices.

The amplified pulses pass through a circulator and enter an asymmetric Mach–Zehnder interferometer (MZI), composed of a balanced beam splitter and Faraday mirrors (FM). The delay between the two arms of the MZI is set to be precisely equal to one pulse period (50 ns), allowing for interference between consecutive pulses. One output from the interference proceeds to subsequent processing, while the other output is directed back through the circulator and detected by a photodetector (PD1) for local measurement, which corresponds to the projection measurement onto the Z basis on the Bob side.

Then, we use a combination of a polarization controller and a polarizer to purify the polarization of the signal light. Subsequently, the pulses enter a polarization-maintaining beam splitter and are equally divided into two paths. We add a 100 ns fiber delay to one of the paths, which is precisely equal to two pulse periods. Then, we perform polarization synthesis for each pulse with its next-to-nearest neighboring pulse using a polarization combiner. The resulting polarized pulses are split into two paths by a beam splitter. Most of the power is used for local polarization measurements that correspond to the projection measurement onto the X basis on the Bob side, while a small portion is further attenuated by the variable optical attenuator (VOA). The VOA is precisely set to ensure that the maximum intensity of the weak coherent pulse (WCP) of H(V) polarization is about 0.5 photons per pulse before entering the quantum channel.

For the local measurement, we use commercial InGaAs-biased photodetectors with a bandwidth of 5 GHz and a rising time of 70 ps. And a high-speed data acquisition card (ADQ series) with the highest sampling rate of 5 GSa/s and 12-bit resolution is used here to record all the local measurement results. On the Bob side, a standard BB84 decoding module is constructed using a beam splitter and two sets of polarization measurements that implement projection onto Z and X bases. Four single photon detectors (Qube series from IDQ) are used here, of which the average efficiency is 10% and the average dark count rate is 500 Hz

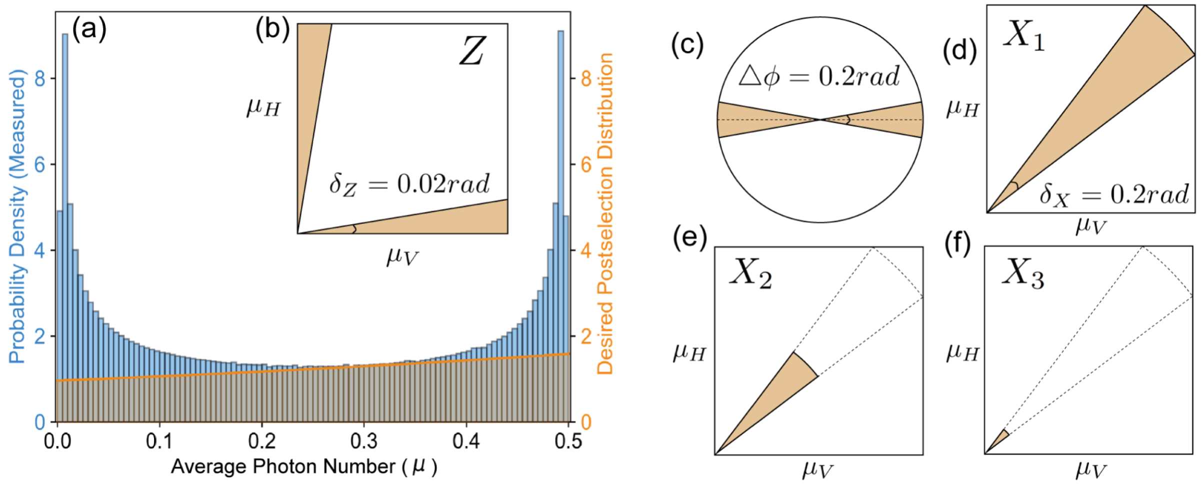

FIG. 3. Illustration of the postselection protocol. (a) The U-shape distribution of pulse intensities measured by PD1 (blue histogram) and the desired intensity distribution after postselection (shaded area). (b) The region that defines Z-base data in the ($\mu_H$, $\mu_V$) plane, where the $\mu_H$ ($\mu_V$) denotes the intensity of the H(V) component measured by PD1. (c) X-basis data (shaded area) defined on the equator of the Bloch sphere. (d)–(f) Three different intensity sets ($X_1$, $X_2$, $X_3$) of X-base data are defined on the ($\mu_H$, $\mu_V$) plane for decoy-state analysis.

in free running mode. We also use a time tagger device modeled ID900 to collect all the single-photon events for postprocessing. We use an optical attenuator instead of a real single-mode fiber spool to serve as the quantum channel for a proof-of-principle demonstration (see the Supplemental Material [33], Sec. I, for more experimental details).

*Experimental results.*—We characterize the gain-switch light source using the data detected by PD1 (in Fig. 2). And these data are also used as the local measurement for the Z basis, recording all the intensity information of H(V) components denoted by $\mu_H(\mu_V)$. As shown in Fig. 3(a), the histogram shows the statistical analysis of the output intensities of $2\times10^{10}$ pulses (rescaled to the range of [0, 0.5]), revealing a U-shaped distribution, which indicates that the pulse phases are random values uniformly distributed between 0 and $2\pi$ [32]. In order to decouple the distribution of polarization from intensities in decoy-state analysis, we need to randomly discard some of the pulses according to a specific strategy to obtain our desired distribution $g(\mu) = Ce^u$ [as shown in the shaded area of Fig. 3(a); see the Supplemental Material [33], Sec. II, for details].

In this work, we only use the Z-basis data for key generation. Unlike the active QKD, we use a region near the poles of the Bloch sphere that can be defined by $\{\mu_H, \mu_V\}$ to determine the Z basis, denoted by the colored region in Fig. 3(b). We set the tolerance to be $\delta_Z = 0.02$ rad, where $\delta_Z$ can be calculated using $\tan(\delta_Z) = \mu_H/\mu_V$. The determination of the X basis is slightly more complex. First, we need to use $\{\mu_H, \mu_V\}$ to filter out pulses located near the equator of the Bloch sphere, which can be denoted by the colored region in Fig. 3(d). The tolerance is set to be $\delta_X = 0.2$, which can be calculated using $\tan(\pi/4 \pm \delta_X/2) = \mu_H/\mu_V$. Based on that, we further filter out pulses within a specific azimuthal angle range $\triangle\phi = 0.2$ as shown in Fig. 3(c), to obtain the diagonal (antidiagonal) polarization states $D(A)$. To do that, we need to combine all the local measurement results. We denote the measurement results of PD2 as $\mu_D$ and calculate the azimuthal angle $\phi$ by

$$\phi = \arccos\left(\frac{\mu_D - \mu_A}{2\sqrt{\mu_H\mu_V}}\right), \qquad (2)$$

where $\mu_A$ can be calculated with $\{\mu_H, \mu_V, \mu_D\}$. As shown in Fig. 3(c), we define the region $\phi = \pm 0.1$ rad ($\phi = \pi \pm 0.1$ rad) as $D(A)$ states.

It is worth noting that in Fig. 3(d), the selected region is a sector rather than a quadrilateral that includes the top-right corner, which is for the convenience of decoy-state analysis (see the Supplemental Material, [33], Sec. III). We represent this region as X1. Similarly, we represent the other two sector-shaped subregions of X1 as X2 and X3 [shown in Figs. 3(e) and 3(f)], with their radii being 0.5 and 0.1 of X1, respectively. By utilizing these three different intensity sets, we then are able to do the decoy-state analysis [34–36].

TABLE I. Parameters of Z-basis measurement under different channel loss.

| | 7.2 dB | 11.6 dB | 16.7 dB |
|---|---|---|---|
| $E_\mu(\%)$ | $2.13 \pm 0.0026$ | $2.27 \pm 0.0027$ | $2.30 \pm 0.0027$ |
| $Q_\mu(10^{-3})$ | $9.24 \pm 0.017$ | $2.95 \pm 0.009$ | $0.95 \pm 0.005$ |

TABLE II. Parameters of X-basis measurement under the channel loss of 16.7 dB.

| | $X_1$ | $X_2$ | $X_3$ |
|---|---|---|---|
| $E_\mu(\%)$ | $1.60 \pm 0.001$ | $1.80 \pm 0.002$ | $2.20 \pm 0.012$ |
| $Q_\mu(10^{-3})$ | $1.38 \pm 0.002$ | $0.66 \pm 0.003$ | $0.11 \pm 0.008$ |

We conduct QKD experiments at three different channel losses: 7.2 dB, 11.6 dB, and 16.7 dB. For each loss situation, we collect data of 1000 s for testing (3000 s for the 16.7 dB loss situation). Table I lists the error rate $E_u$ and gain $Q_u$ measured in three different channel losses for the Z basis. For the X basis, we analyze data from three different intensity regions $\{X_1, X_2, X_3\}$ under each loss scenario. Here, the parameters for a 16.7 dB loss scenario are presented in Table II, and other parameters can be found in the Supplemental Material [33], Sec. IV. Based on these measured results, we calculate the final key rate using the following formula [1]:

$$\begin{aligned} R = P_Z\{\langle P_1\rangle_{S_Z} Y_1^{Z,\text{perfect},L}[1 - h_2(e_1^{X,\text{perfect},U})] \\ - f_e\langle Q_Z\rangle_{S_Z} h_2(\langle QE_Z\rangle_{S_Z}/\langle Q_Z\rangle_{S_Z})\}, \end{aligned} \qquad (3)$$

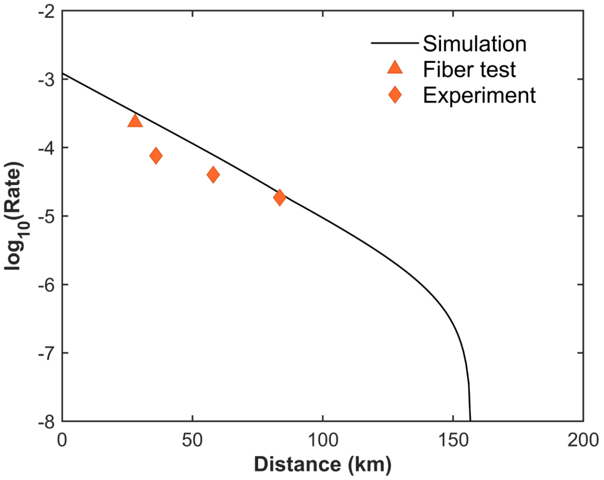

FIG. 4. Final key rate simulation and experimental results. The line in the graph represents the simulation of the key rate at different distances, assuming that the channel is a standard telecom fiber with an attenuation of 0.2 dB/km. Other parameters include the single-photon detection efficiency of 10% and the dark count rate of $10^{-6}$. The triangle represents the key rate obtained by the fiber test shown in the Supplemental Material [33], Sec. V.

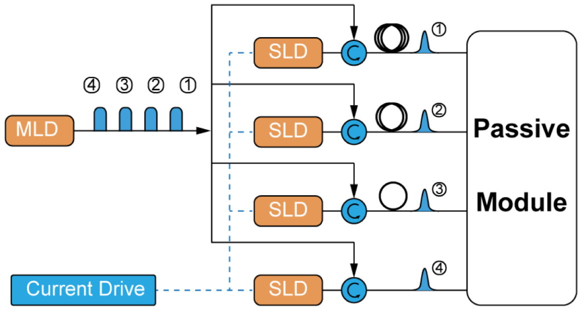

FIG. 5. Fully passive source with injection locking. When the first seed pulse arrives, the drive current of the first slave laser is activated. Similarly, when the second seed pulse arrives, the drive current of the second laser is activated, and so on. MLD, master laser; SLD, slave laser.

where $h_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function. As plotted in Fig. 4, the obtained final key rates are $7.62 \times 10^{-5}$ in 7.2 dB, $4.01 \times 10^{-5}$ in 11.6 dB, and $1.86 \times 10^{-5}$ in 16.7 dB in the asymptotic regime. A rigorous finite-size analysis will be the subject of future studies.

*Discussion.*—In summary, we successfully demonstrated fully passive quantum key distribution using a single laser source with polarization encoding, under different channel losses, which completely eliminates the side channels introduced by active modulation.

Compared with multilaser schemes, using a single laser can avoid wavelength side channels and prevent the decrease in interference visibility caused by frequency deviations [37,38]. However, since we use interference between early-late pulse pairs, the output WCPs sequence will not be completely independent of each other. In our protocol, only the first pulse out of every four can be used as a quantum signal, while the remaining three need to be discarded (as a proof-of-principle demonstration, we discard these pulses through postselection). One solution to this would be adding extra intensity modulators or optical switches to pick the valid pulse. Notice that those modulators or optical switches are only used to periodically switch the signal on and off, without involving any modulation information, so it does not generate side channels.

Here, we also propose another possible solution: one can combine injection locking techniques and fully passive modulation to achieve a completely modulator-free scheme [39]. As illustrated in Fig. 5, the master laser generates phase-randomized pulses in gain-switch mode, grouping these pulses in sets of four. By applying driving currents at appropriate timings, the four slave lasers are each seeded by one of the four pulses, thus inheriting their respective phase information. After a suitable delay, the pulses generated by the slave lasers are injected into a fully passive modulation system, thereby resolving the issue of nonindependence between adjacent pulses.

We thank Li Qian, Zhiliang Yuan, Gai Zhou, Xiong Wu, Rong Wang, and Chenyang Li for their helpful discussions. The project is supported by the University of Hong Kong start-up grant. W. W. acknowledges support from the Hong Kong RGC General Research Fund (GRF) and the University of Hong Kong Seed Fund for Basic Research for New Staff. H.-K. L. is also supported by NSERC, MITACS, and Innovative Solutions Canada.

*Note added.*—Recently, we become aware of a related work [40].

---

[*] hucq@hku.hk

[†] hoikwong@hku.hk

[1] W. Wang, R. Wang, C.-Q. Hu, V. Zapatero, L. Qian, B. Qi, M. Curty, and H.-K. Lo, Phys. Rev. Lett. **130**, 220801 (2023).
[2] V. Zapatero, W. Wang, and M. Curty, Quantum Sci. Technol. **8**, 025014 (2023).
[3] C. H. Bennett and G. Brassard, in *Proceedings of the International Conference on Computer System and Signal Processing* (IEEE, New York, 1984).
[4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[5] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[6] H. Liu, W. Wang, K. Wei, X.-T. Fang, L. Li, N.-L. Liu, H. Liang, S.-J. Zhang, W. Zhang, H. Li *et al.*, Phys. Rev. Lett. **122**, 160501 (2019).
[7] Y. Cao, Y.-H. Li, K.-X. Yang, Y.-F. Jiang, S.-L. Li, X.-L. Hu, M. Abulizi, C.-L. Li, W. Zhang, Q.-C. Sun *et al.*, Phys. Rev. Lett. **125**, 260503 (2020).
[8] M. Lucamarini, Z.-L. Yuan, J.-F. Dynes, and A.-J. Shields, Nature (London) **557**, 400 (2018).
[9] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen *et al.*, Nat. Photonics **16**, 154 (2022).
[10] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang *et al.*, Phys. Rev. Lett. **130**, 210801 (2023).
[11] L. Zhou, J. Lin, Y. Jing, and Z. Yuan, Nat. Commun. **14**, 928 (2023).
[12] N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).
[13] X.-L. Pang, A.-L. Yang, C.-N. Zhang, J.-P. Dou, H. Li, J. Gao, and X.-M. Jin, Phys. Rev. Appl. **13**, 034008 (2020).
[14] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[15] K. Tamaki, M. Curty, and M. Lucamarini, New J. Phys. **18**, 065008 (2016).
[16] J. E. Bourassa, A. Gnanapandithan, L. Qian, and H.-K. Lo, Phys. Rev. A **106**, 062618 (2022).
[17] K.-i. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, and A. Tomita, npj Quantum Inf. **4**, 8 (2018).
[18] A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, Phys. Rev. Appl. **12**, 064043 (2019).

[19] Y.-L. Tang, H.-L. Yin, X. Ma, C. H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Phys. Rev. A **88**, 022308 (2013).

[20] G. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, Opt. Lett. **43**, 5110 (2018).

[21] F.-Y. Lu, X. Lin, S. Wang, G.-J. Fan-Yuan, P. Ye, R. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, G.-C. Guo *et al.*, npj Quantum Inf. **7**, 75 (2021).

[22] T. K. Paraïso, I. De Marco, T. Roger, D. G. Marangon, J. F. Dynes, M. Lucamarini, Z. Yuan, and A. J. Shields, npj Quantum Inf. **5**, 42 (2019).

[23] R. I. Woodward, Y. Lo, M. Pittaluga, M. Minder, T. Paraïso, M. Lucamarini, Z. Yuan, and A. Shields, npj Quantum Inf. **7**, 58 (2021).

[24] M. Curty, T. Moroder, X. Ma, and N. Lütkenhaus, Opt. Lett. **34**, 3238 (2009).

[25] M. Curty, X. Ma, B. Qi, and T. Moroder, Phys. Rev. A **81**, 022310 (2010).

[26] Q.-C. Sun, W.-L. Wang, Y. Liu, F. Zhou, J. S. Pelc, M. Fejer, C.-Z. Peng, X. Chen, X. Ma, Q. Zhang *et al.*, Laser Phys. Lett. **11**, 085202 (2014).

[27] S.-H. Sun, G.-Z. Tang, C.-Y. Li, and L.-M. Liang, Phys. Rev. A **94**, 032324 (2016).

[28] Y. Zhang, S. Wang, Z.-Q. Yin, W. Chen, W.-Y. Liang, H.-W. Li, G.-C. Guo, and Z.-F. Han, Chin. Phys. B **21**, 100307 (2012).

[29] C. Li, C. Hu, W. Wang, R. Wang, and H.-K. Lo, arXiv: 2212.01876.

[30] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, Nat. Photonics **10**, 312 (2016).

[31] Z. L. Yuan, B. Fröhlich, M. Lucamarini, G. L. Roberts, J. F. Dynes, and A. J. Shields, Phys. Rev. X **6**, 031044 (2016).

[32] Z. Yuan, M. Lucamarini, J. Dynes, B. Fröhlich, A. Plews, and A. Shields, Appl. Phys. Lett. **104**, 261112 (2014).

[33] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.131.110801 for experimental details, postselection strategy, decoy-state analysis and key rate formula, detailed results, and fiber test.

[34] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[35] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[36] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[37] E. Moschandreou, J. I. Garcia, B. J. Rollick, B. Qi, R. Pooser, and G. Siopsis, J. Lightwave Technol. **36**, 3752 (2018).

[38] 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.*, Phys. Rev. Lett. **117**, 190501 (2016).

[39] Y. Lo, R. Woodward, N. Walk, M. Lucamarini, I. De Marco, T. Paraïso, M. Pittaluga, T. Roger, M. Sanzaro, Z. Yuan *et al.*, APL Photonics **8**, 036111 (2023).

[40] F.-Y. Lu, Z.-H. Wang, J.-L. Chen, S. Wang, Z.-Q. Yin, D.-Y. He, R. Wang, W. Chen, G.-J. Fan-Yuan, G.-C. Guo *et al.*, following Letter, Phys. Rev. Lett. **131**, 110802 (2023).