Experimental Demonstration of Fully Passive Quantum Key Distribution

Feng-Yu Lu,[1,2,*] Ze-Hao Wang,[1,2,*] Víctor Zapatero,[3,4,5,*] Jia-Lin Chen,[1,2] Shuang Wang,[1,2,6,†] Zhen-Qiang Yin,[1,2,6,‡] Marcos Curty,[3,4,5] De-Yong He,[1,2,6] Rong Wang,[7] Wei Chen,[1,2,6] Guan-Jie Fan-Yuan,[1,2] Guang-Can Guo,[1,2,6] and Zheng-Fu Han[1,2,6]

[1]*CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*
[2]*CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*
[3]*Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*
[4]*Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain*
[5]*AtlanTTic Research Center, University of Vigo, Vigo E-36310, Spain*
[6]*Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, People's Republic of China*
[7]*Department of Physics, University of Hong Kong, Hong Kong SAR, People's Republic of China*

(Received 18 May 2023; accepted 1 August 2023; published 13 September 2023)

The passive approach to quantum key distribution (QKD) consists of removing all active modulation from the users' devices, a highly desirable countermeasure to get rid of modulator side channels. Nevertheless, active modulation has not been completely removed in QKD systems so far, due to both theoretical and practical limitations. In this Letter, we present a fully passive time-bin encoding QKD system and report on the successful implementation of a modulator-free QKD link. According to the latest theoretical analysis, our prototype is capable of delivering competitive secret key rates in the finite key regime.

DOI: 10.1103/PhysRevLett.131.110802

Quantum key distribution (QKD) [1] is one of the most successful applications of quantum information science, since it allows for information-theoretically secure communications between two distant users regardless of the, potentially unlimited, computational power of an eavesdropper Eve [2–5]. However, information-theoretic security may be compromised by the presence of loopholes in the QKD equipment, which may open side channels for Eve to obtain information in unexpected ways [6–28].

Measurement-device-independent QKD [29–36] has been proposed to close all detection-related security loopholes. Thus, in recent years, more and more attention is set on the source-side loopholes [6,17–21,26,35,37,38]. For instance, Eve can obtain some modulation information with a Trojan Horse attack [37,38]. Also, the injection of bright light or external magnetic fields may damage the source-side devices [17,19,20,39]. Similarly, correlations in modulations may invalidate the independent and identically distributed assumption, opening the door to sophisticated attacks [23,26–28,40,41].

In this context, some passive schemes have been proposed to deal with source side channels. For instance, by making use of the photon-number relationship [42–48] between two pulses, Alice can deduce the photon-number distribution of one of them by detecting the other, in so passively implementing the decoy-state technique [44,49–52]. Besides, superimposing two mutually orthogonal polarizations in a polarizing beam splitter (BS) and further incorporating a postselection method, one can passively encode the four BB84 states.

However, the above passive schemes can only replace part of the active modulations, and therefore they only provide partial solutions. In spite of the considerable efforts made, passively implementing both the decoy-state choice and the BB84 encoding with linear optical components and laser sources has been a pending task for a decade. To state it shortly, the basic difficulty is dealing with the fact that the passive decoy states and the passive encoding states are correlated. Moreover, it is also a challenge to prepare and postselect the required decoy states and encoding states simultaneously, due to the large difference between passive QKD systems and traditional active QKD systems. Recently, two solutions against this elusive problem have been proposed [53,54], finally paving the way toward fully passive (FP) QKD.

In this Letter, we propose a FP time-bin encoding QKD source and report on the first successful implementation of a FP-QKD link. Our prototype can efficiently prepare different decoy states and encoding states simultaneously, and our postselection module accurately postselects the

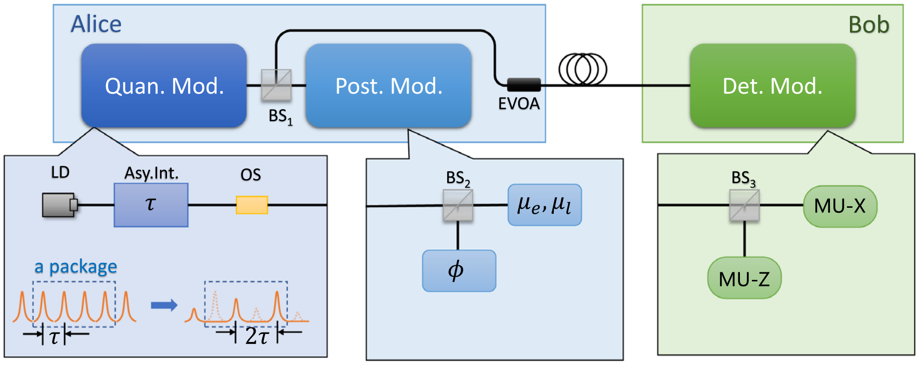


FIG. 1. Schematic diagram of our FP-QKD scheme. Quan. Mod., quantum module; Post. Mod., postselection module; Det. Mod., detection module; LD, laser diode; Asy. Int., asymmetric interferometer; OS, optical switch; BS, beam splitter; EVOA, electronic variable optical attenuator; MU-Z(X), measurement unit for measuring the Z (X) basis. τ, length difference between the two paths; $\mu_{e(l)}$, measurement of the intensity of the early (late) time bin; ϕ, measurement of the relative phase between the two time bins.

required states and ignores the undesired rounds to reduce the throughput and computation. As a result, it is capable of delivering competitive secret key rate (SKRs) in the finite key regime, following the security analysis in [55]. What is more, compared with the multilaser approach introduced in [53], the single-laser structure we deploy allows to avoid wavelength side channels. Putting it all together, the scheme is of great significance to reach higher implementation security and promote the applicability of QKD.

As illustrated in Fig. 1, our FP-QKD setup consists of three modules. In the source side, the quantum module is employed to passively and randomly generate different quantum states and intensities. Then, the postselection module locally measures the prepared states and intensities to postselect the bases, raw key bits, and decoy states. The third module is Bob's detection module.

In the quantum module, a LD generates a train of phase-randomized coherent states with a certain period, say τ. In order to obtain 4 degrees of freedom [53], we treat every four consecutive pulses as a "package,"

$$|\sqrt{\mu_{\text{in}}}e^{i\phi_1}\rangle_1|\sqrt{\mu_{\text{in}}}e^{i\phi_2}\rangle_2|\sqrt{\mu_{\text{in}}}e^{i\phi_3}\rangle_3|\sqrt{\mu_{\text{in}}}e^{i\phi_4}\rangle_4, \qquad (1)$$

where μ_{in} is the output intensity of the LD, and ϕ_1 to ϕ_4 are the phases of the four pulses. The pulse train is then fed to an asymmetric interferometer whose path difference is τ, such that adjacent pulses interfere at the output port of the interferometer. After that, an OS opens and closes with fixed period 2τ to eliminate the odd pulses, which includes the interference of $|\sqrt{\mu_{\text{in}}}e^{i\phi_2}\rangle_2$ and $|\sqrt{\mu_{\text{in}}}e^{i\phi_3}\rangle_3$ in every package, and the interference between pulses belonging to different packages. The remaining two pulses in a package constitute the late and the early time bins of an encoded state. Importantly as well, the operation of the OS is fixed and uncorrelated to the protocol settings, such that it does not constitute a side channel in this regard. Nevertheless, a practical OS with a finite extinction ratio may leak partial information about the neighboring pulses [53]. A short discussion on this potential side channel is included in Supplemental Material, Sec. III [56].

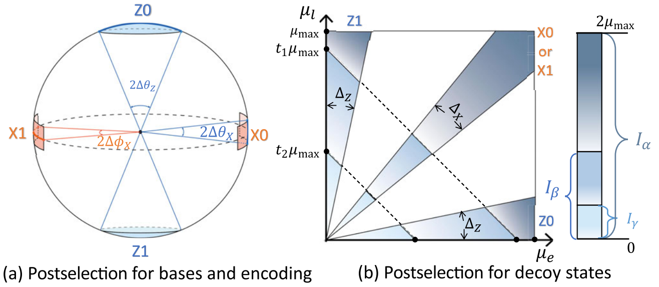
The output of the quantum module is unevenly split: most of the intensity is sent to the postselection module for Alice's local measurement, and the remaining part is attenuated to the single-photon level and sent to Bob. This can be expressed as

$$\begin{aligned}&|\sqrt{\mu_{\max}}(e^{i\phi_1}+e^{i\phi_2})/2\rangle_e|\sqrt{\mu_{\max}}(e^{i\phi_3}+e^{i\phi_4})/2\rangle_l\\&=|\sqrt{\mu_e}e^{i\phi_e}\rangle_e|\sqrt{\mu_l}e^{i\phi_l}\rangle_l,\end{aligned} \qquad (2)$$

where $\mu_{\max}=2\mu_{\text{in}}\eta_S$ stands for the maximum intensity in each time bin, η_S denoting the total attenuation of the source-side devices. Similarly, $\mu_e=\mu_{\max}[1+\cos(\phi_1-\phi_2)]/2$ and $\mu_l=\mu_{\max}[1+\cos(\phi_3-\phi_4)]/2$ denote the respective intensities of the early time bin and the late time bin, while $\phi_e=(\phi_1+\phi_2)/2$ and $\phi_l=(\phi_3+\phi_4)/2$ denote their phases. Hence, defining $\phi_G=\phi_e$, $\phi=\phi_l-\phi_e$, $\mu=\mu_e+\mu_l$, and $\theta=2\arccos\sqrt{\mu_e/\mu}$, respectively, as the global phase, the relative phase, the intensity, and the polar angle of the time-bin state. The corresponding single-photon state can be expressed as $\cos(\theta/2)|e\rangle+e^{i\phi}\sin(\theta/2)|l\rangle$, where $|e\rangle=|1\rangle_e\otimes|0\rangle_l$ ($|l\rangle=|0\rangle_e\otimes|1\rangle_l$) denotes the early (late) time-bin single-photon state.

In the detection module, Bob passively selects the Z or the X basis to measure the received states, publicly announces if a successful detection event occurs in the measurement unit (MU), and records his raw key bits and bases according to the outcomes of the MUs. For those rounds where a successful event is announced, Alice records (or discards) her raw key bits, bases, and decoy settings according to the postselection method depicted in Fig. 2. A complete description of the postselection is presented in Supplemental Material, Sec. I [56].

Once the quantum communication ends, Alice and Bob reveal their basis choices for sifting, and disclose parts of their raw key data for the estimation of the secret key



(a) Postselection for bases and encoding (b) Postselection for decoy states

FIG. 2. Schematic illustration of the postselection. (a) Postselection of bases and bit values. $\Delta\theta_Z$, $\Delta\theta_X$, and $\Delta\phi_X$ are predecided thresholds that characterize the acceptance regions. The areas Z0 and Z1 (X0 and X1) define the key (test) basis, while the blank area corresponds to the rejected data. (b) Postselection of decoy states. The horizontal (vertical) axis denotes the intensity $\mu_{e(l)}$ of the early (late) time bin, and the total intensity at any point of the graph is $\mu = \mu_e + \mu_l$. As stated in the main text, $\mu_{\max}$ denotes the maximum intensity in each time bin. On the other hand, Δ_Z and Δ_X are threshold values related to $\Delta\theta_Z$, $\Delta\theta_X$, and $\Delta\phi_X$, and t_1 and t_2 are predecided thresholds that define the decoy-state intervals. Specifically, overlapping intensity intervals are used in the experiment (see Supplemental Material, Sec. I [56]).

length. The details of the parameter estimation method are summarized in Supplemental Material, Sec. II [56], sticking to the finite-key analysis provided in [55].

The experimental setup is illustrated in Fig. 3. A gain-switched LD driven by a homemade circuit generates pulse trains with 200 ps pulse width and 5 ns interval, and the phase of each pulse is randomized due to the amplified spontaneous emission process [64]. By carefully tuning the temperature-electronic control in the LD, the central wavelength of the LD is locked at 1550.12 nm. An EDFA is employed to amplify the intensity, and a VOA is employed to protect Alice's local PDs. The pulses are fed to an asymmetric AMZI whose path difference is 5 ns to generate random intensities. A 5 GSa/s arbitrary waveform generator connected to a radio-frequency amplifier produces a 100 MHz square-wave periodic signal to drive a $\mathrm{LiNbO_3}$ OS to eliminate the odd pulses. The interval between the early and late time bins is 10 ns and the interval between two time-bin states is 20 ns, meaning that our system works at 50 MHz period. The 1:99 BS $\mathrm{BS_1}$ sends 99% of the intensity to the postselection module for Alice's local measurement and, as mentioned above, the remaining 1% is attenuated to a single-photon level by an EVOA with attenuation ratio η_A, to be ultimately sent to Bob through a fiber quantum channel.

At the detection side, Bob passively selects the Z or the X basis to measure the received time-bin states. The detection module consists of a BS ($\mathrm{BS_3}$) and two MUs. MU-Z is the unit for measuring the Z basis, and it consists of a 50:50 BS ($\mathrm{BS_4}$) and two homemade SPDs. The two SPDs work on the gated mode [65] and respectively open their gates at the early and the late time bins. That is to say, Bob records bit 0 (1) in the Z basis when SPD_e ($\mathrm{SPD_l}$) clicks. Analogously, MU-X measures the X basis and consists of a FMI ($\mathrm{FMI_2}$) and two homemade SPDs (SPD_c and SPD_d). The path difference of the $\mathrm{FMI_2}$ is 10 ns, such that the adjacent pulses interfere in its output port. SPD_c and SPD_d are connected to the two outputs of

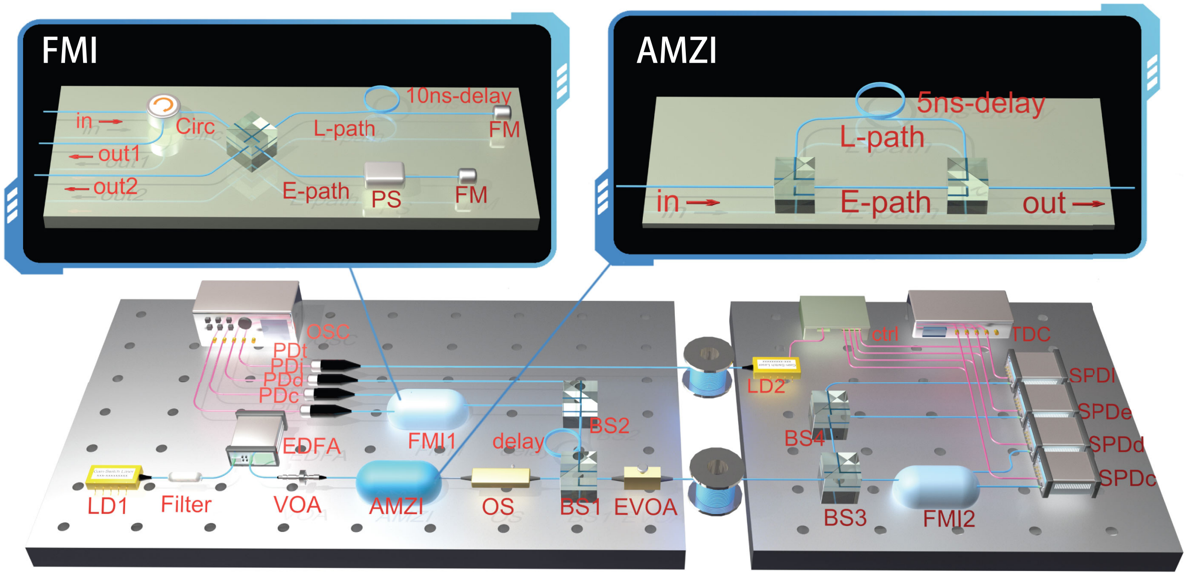


FIG. 3. Depiction of the experimental setup. Devices in the main setup: LD, laser diode; VOA, variable optical attenuator; EDFA, erbium-doped fiber amplifier; AMZI, asymmetric Mach-Zehnder interferometer; FMI, Faraday-Michelson interferometer; OS, optical switch; BS, beam splitter; EVOA, electronic variable optical attenuator; SPD, single-photon detector; PD, photon diode; TDC, time-digital converter; OSC, oscilloscope; ctrl, computer and field-programmable gate array. Devices in FMI and AMZI: PS, phase shifter; FM, Faraday mirror; Circ, circulator; L(E)-path, "late" ("early") path of the FMI and the AMZI.

the FMI$_2$ to measure constructive and destructive interference, respectively. These two SPDs also work on the gated mode, with a 50 MHz frequency to filter the dark counts and the interference between different packages. We observe a dark count rate of 6×10^{-7} in the detection module, while its overall detection efficiency is 12.5%. As for the detection events, Bob records bit 0 (1) in the X basis when SPD$_c$ (SPD$_d$) clicks. The output signals of each SPD are copied by a homemade circuit. Bob sends one of the copies to the time-digital converter for his raw key bit generation, and the other copy is sent to a homemade AND-logic circuit accompanied by a homemade electrical-to-optical converter. A click from any of the SPDs triggers the converter to generate a light pulse to be sent to Alice. When Alice receives this pulse, she measures and records the corresponding μ_e, μ_l, and ϕ using her postselection module.

In Alice's postselection module, the pulses are evenly split by BS$_2$. The first part is measured by a 20-GHz bandwidth high-speed photon diode PD$_i$ and the other part is fed to FMI$_1$, whose path difference is 10 ns. The early and the late time-bin pulses interfere at the output port of FMI$_1$, and the constructive and destructive interference results are respectively detected by two 20-GHz bandwidth high-speed PDs, PD$_c$ and PD$_d$. The outputs of the three PDs are monitored by a 20-GSa/s high-speed oscilloscope and stored if Bob announces a successful event, or discarded otherwise. If stored, Alice calculates the intensities I_e and I_l according to the measurement results of PD$_i$ [28], and the intensities I_c and I_d according to the respective measurement results of PD$_c$ and PD$_d$, I_e (I_l) denoting the intensity of the early (late) time bin. Here, I_c and I_d stand for the constructive and the destructive interference results, respectively. The central parameters for Alice's postselection are calculated as $\mu_{e(l)} = I_{e(l)}\eta_A t_{B_1}/[h\nu t_{B_2}(1 - t_{B_1})]$ and $\phi = \pi \pm \arccos[1 - 2I_c/(I_c + I_d)]$, where $t_{B_{1(2)}}$ is the transmittance of BS$_{1(2)}$, h is the Planck constant, and $\nu = 1550.12$ nm is the central wavelength. According to the postselection rule, Alice deduces and records her basis, raw key bit, and decoy setting.

We successfully proved the feasibility of FP-QKD in three different scenarios: at 6 dB of channel loss with $N = 10^{10}$ transmitted signals (experiment 1), at 10 dB of channel loss with $N = 10^{10}$ transmitted signals (experiment 2), and at 6 dB of channel loss with $N = 10^9$ transmitted signals (experiment 3). In all three of them, the postselection thresholds—presented in Fig. 2—are set to $\Delta\theta_Z = 0.6135$, $\Delta\theta_X = 0.1002$, $\Delta\phi_X = 0.6435$, $t_2 = 0.15$, and $t_1 = 0.55$. The test-basis probability of Bob's passive module is $q_X = 0.25$, and the value of $\mu_{\max}$ is determined to be 0.359 in the first experiment and 0.254 in the other two. Lastly, the finite key parameter introduced in Supplemental Material, Sec. II [56] is set to $\epsilon = 10^{-20}$ for illustration purposes, leading to an overall secrecy parameter of $\epsilon_{\text{sec}} \approx 4 \times 10^{-10}$ and a correctness parameter of $\epsilon_{\text{cor}} = 10^{-20}$.

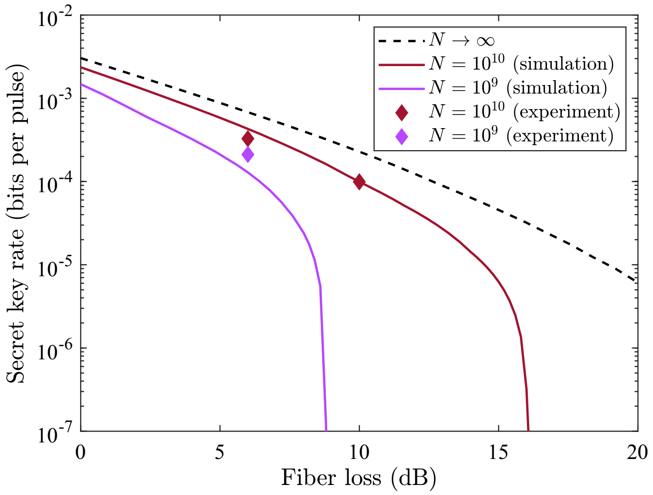


FIG. 4. Experimental and simulated performance of our FP-QKD system as a function of the fiber loss. The dashed line represents the simulated SKR in the asymptotic limit, while the solid lines represent the simulated SKRs with data sizes $N = 10^{10}$ and 10^9, as indicated in the legend. Lastly, the diamond-shaped points denote the experimental SKRs with data sizes $N = 10^{10}$ and 10^9, respectively. In the simulations, the value of $\mu_{\max}$ is optimized as a function of the channel loss, while all other settings are fixed as in the experiments.

As shown in Fig. 4, the extractable SKR is about 3.3×10^{-4} (9.9×10^{-5}) bits per pulse in experiment 1 (2), and 2.1×10^{-4} in experiment 3. In addition, in Table I we show the sifted-key length (M_α^Z), the lower bound on the number of key-basis single-photon counts ($M_{Z,1}^{\text{L}}$), the upper bound on the phase-error rate ($e_1^{(\text{ph})U}$) and the error rate in the key basis (e_Z). In the simulations, the error correction (EC) leakage is modeled as $\lambda_{\text{EC}} = 1.16 M_\alpha^Z h(e_Z)$, meaning that we assume an error-correction efficiency of 1.16 and a perfect knowledge of the bit-error rate for simplicity. In this regard, we remark that the more sensitive approach of setting a prefixed threshold bit-error rate to assure the robustness of the EC would only have a negligible impact on the SKR, due to the fairly large numbers of signals transmitted in the experiments. In addition, this issue is independent of the correctness of the protocol, which can be guaranteed by simply performing an error verification step after EC.

The experimental results are greatly consistent with our simulation results. In particular, we note that the experiment with $N = 10^9$ signals outperforms the simulated SKR

TABLE I. Results of the experiments.

f. loss	N	M_α^Z	$M_{Z,1}^{\text{L}}$	$e_1^{(\text{ph})U}$	e_Z	K
6 dB	10^{10}	1.4×10^7	1.0×10^7	6.2%	3.4%	3.3×10^{-4}
10 dB	10^{10}	4.0×10^6	3.2×10^6	7.1%	3.4%	9.9×10^{-5}
6 dB	10^9	1.0×10^6	7.7×10^5	7.6%	3.4%	2.1×10^{-4}

to some extent. This is so because, compared to the simulated observables, the set of actually observed key-basis measure counts leads to a slightly tighter confidence interval for the number of single-photon counts $M_{Z,1}$.

In summary, we have experimentally demonstrated FP-QKD exploiting very recent theoretical achievements, and solving the difficulty of designing a stable FP transmitter and an efficient local postselection system. Our single-laser structure allows to avoid wavelength side channels, and our time-bin encoding approach benefits from a high stability in the fiber and a simpler experimental layout. What is more, our postselection method can accurately select the required states and ignore the undesired rounds to reduce the throughput. On top of it, we have assessed the finite-key scenario, which implies that our results are of immediate practical relevance.

In view of the fact that FP-QKD eliminates all modulator side channels, our work promotes the practical security of QKD and might play a central role in its way to standardization.

This work has been supported by the National Natural Science Foundation of China (Grants No. 62271463, No. 62171424, and No. 62105318), the China Postdoctoral Science Foundation (No. 2022M723064, No. 2021M693098), and the Anhui Initiative in Quantum Information Technologies. M. C. and V. Z. acknowledge support from Cisco Systems Inc., the Galician Regional Government (consolidation of Research Units: AtlantTIC), the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through Grant No. PID2020-118178RB-C21, MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1) and the Galician Regional Government with own funding through the "Planes Complementarios de I + D + I con las Comunidades Autónomas" in Quantum Communication, the European Union's Horizon Europe Framework Programme under the Marie Sklodowska-Curie Grant No. 101072637 (Project QSI), and the project "Quantum Security Networks Partnership" (QSNP, Grant Agreement No. 101114043).

Note added.—Recently, we have become aware of a related work [57].

[*] These authors contributed equally to this work.

[†] wshuang@ustc.edu.cn

[‡] yinzq@ustc.edu.cn

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, Bangalore, India, 1984), pp. 175–179.

[2] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[5] R. Renner, Int. Symp. Inf. Theor. **6**, 1 (2008).

[6] N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).

[7] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73 (2007).

[8] V. Makarov, New J. Phys. **11**, 065003 (2009).

[9] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).

[10] Y. Zhao, C. H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).

[11] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[12] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. **107**, 110501 (2011).

[13] S. Sajeed, A. Huang, S. Sun, F. Xu, V. Makarov, and M. Curty, Phys. Rev. Lett. **117**, 250505 (2016).

[14] Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. Appl. **10**, 064062 (2018).

[15] W.-T. Liu, S.-H. Sun, L.-M. Liang, and J.-M. Yuan, Phys. Rev. A **83**, 042326 (2011).

[16] L. O. Mailloux, D. D. Hodson, M. R. Grimaila, R. D. Engle, C. V. Mclaughlin, and G. B. Baumgartner, IEEE Access **4**, 2188 (2016).

[17] A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, Phys. Rev. Appl. **12**, 064043 (2019).

[18] K. Tamaki, M. Curty, and M. Lucamarini, New J. Phys. **18**, 065008 (2016).

[19] 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).

[20] A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, and V. Makarov, Phys. Rev. Appl. **13**, 034017 (2020).

[21] G. Zhang, I. W. Primaatmaja, J. Y. Haw, X. Gong, C. Wang, and Charles Ci Wen Lim, PRX Quantum **2**, 030304 (2021).

[22] A. Mizutani, G. Kato, K. Azuma, M. Curty, R. Ikuta, T. Yamamoto, N. Imoto, H.-K. Lo, and K. Tamaki, npj Quantum Inf. **5**, 8 (2019).

[23] V. Zapatero, Á. Navarrete, K. Tamaki, and M. Curty, Quantum **5**, 602 (2021).

[24] Y. Nagamatsu, A. Mizutani, R. Ikuta, T. Yamamoto, N. Imoto, and K. Tamaki, Phys. Rev. A **93**, 042325 (2016).

[25] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, Appl. Phys. Lett. **117**, 144003 (2020).

[26] 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).

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

[28] 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).

[29] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[30] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[31] C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, Phys. Rev. Lett. **115**, 160502 (2015).

[32] Z. Tang, K. Wei, O. Bedroya, L. Qian, and H.-K. Lo, Phys. Rev. A **93**, 042308 (2016).

[33] X.-B. Wang, X.-L. Hu, and Z.-W. Yu, Phys. Rev. Appl. **12**, 054034 (2019).

[34] Á. Navarrete, M. Pereira, M. Curty, and K. Tamaki, Phys. Rev. Appl. **15**, 034072 (2021).

[35] F.-Y. Lu, Z.-H. Wang, Z.-Q. Yin, S. Wang, R. Wang, G.-J. Fan-Yuan, X.-J. Huang, D.-Y. He, W. Chen, Z. Zhou *et al.*, Optica **9**, 886 (2022).

[36] F.-Y. Lu, P. Ye, Z.-H. Wang, S. Wang, Z.-Q. Yin, R. Wang, X.-J. Huang, W. Chen, D.-Y. He, G.-J. Fan-Yuan *et al.*, Optica **10**, 520 (2023).

[37] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).

[38] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Phys. Rev. X **5**, 031030 (2015).

[39] H. Tan, W.-Y. Zhang, L. Zhang, W. Li, S.-K. Liao, and F. Xu, Quantum Sci. Technol. **7**, 045008 (2022).

[40] M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki, Sci. Adv. **6**, eaaz4487 (2020).

[41] X. Sixto, V. Zapatero, and M. Curty, Phys. Rev. Appl. **18**, 044069 (2022).

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

[43] M. Curty, X. Ma, H.-K. Lo, and N. Lütkenhaus, Phys. Rev. A **82**, 052325 (2010).

[44] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. Lett. **99**, 180503 (2007).

[45] X. Ma and H.-K. Lo, New J. Phys. **10**, 073018 (2008).

[46] W. Mauerer and C. Silberhorn, Phys. Rev. A **75**, 050305(R) (2007).

[47] S. Krapick, M. S. Stefszky, M. Jachura, B. Brecht, M. Avenhaus, and C. Silberhorn, Phys. Rev. A **89**, 012329 (2014).

[48] Q. Wang, C.-H. Zhang, and X.-B. Wang, Phys. Rev. A **93**, 032312 (2016).

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

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

[51] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

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

[53] W. Wang, R. Wang, C. Hu, V. Zapatero, L. Qian, B. Qi, M. Curty, and H.-K. Lo, Phys. Rev. Lett. **130**, 220801 (2023).

[54] V. Zapatero, W. Wang, and M. Curty, Quantum Sci. Technol. **8**, 025014 (2023).

[55] V. Zapatero and M. Curty, arXiv:2308.02376.

[56] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.131.110802 for more details about the postselection and the finite-key analysis, which includes Refs. [23,26–28,35,57–63].

[57] C. Hu, W. Wang, K.-S. Chan, Z. Yuan, and H.-K. Lo, preceding Letter, Phys. Rev. Lett. **131**, 110801 (2023).

[58] X. Kang, F.-Y. Lu, S. Wang, J.-L. Chen, Z.-H. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, G.-J. Fan-Yuan, G.-C. Guo *et al.*, J. Lightwave Technol. **41**, 75 (2023).

[59] G. Kato, arXiv:2002.04357.

[60] Á. Navarrete and M. Curty, Quantum Sci. Technol. **7**, 035021 (2022).

[61] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A **90**, 052314 (2014).

[62] Z.-Q. Yin, C. H. F. Fung, X. Ma, C.-M. Zhang, H.-W. Li, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **88**, 062322 (2013).

[63] R. J. Serfling, Ann. Stat. **2**, 39 (1974).

[64] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan *et al.*, Nat. Photonics **17**, 416 (2023).

[65] D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, Y.-J. Qian, Z. Zhou, G.-C. Guo, and Z.-F. Han, Appl. Phys. Lett. **110**, 111104 (2017).