

Experimental side channel secure quantum key distribution under realistic conditions

Hao Dong,^{1,2} Cong Jiang^{2,3}, Di Ma,² Chi Zhang,² Jia Huang^{2,4}, Hao Li^{2,4}, Li-Xing You,⁴ Yang Liu^{1,2,3},
Xiang-Bin Wang^{2,3,5}, Qiang Zhang^{1,2,3} and Jian-Wei Pan^{1,3}

¹*Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences,
University of Science and Technology of China, Hefei, Anhui 230026, China*

²*Jinan Institute of Quantum Technology and Hefei National Laboratory Jinan Branch, Jinan, Shandong, China*

³*Hefei National Laboratory, University of Science and Technology of China, Hefei, Anhui 230088, China*

⁴*Shanghai Key Laboratory of Superconductor Integrated Circuit Technology, Shanghai Institute of Microsystem and Information Technology,
Chinese Academy of Sciences, Shanghai 200050, China*

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



(Received 25 April 2025; accepted 23 January 2026; published 25 February 2026)

Quantum key distribution (QKD) theoretically provides unconditional security between remote parties. However, guaranteeing practical security through device characterization alone is challenging in real-world implementations due to the multidimensional spaces in which the devices may be operated. The side channel secure (SCS) QKD protocol, which only requires bounding the upper limits of the intensities for the two states, theoretically provides a rigorous solution to the challenge and achieves measurement-device-independent security in detection and security for whatever multidimensional side channel attack in the source. Here, we demonstrate a practical implementation of SCS-QKD, achieving a secure key rate of 6.67 kbps through a 50.5 km fiber and a maximum distribution distance of 101.1 km while accounting for finite-size effects. Our experiment also represents an approximately 40 times improvement over the previous experiment.

DOI: [10.1103/PhysRevResearch.8.013214](https://doi.org/10.1103/PhysRevResearch.8.013214)

I. INTRODUCTION

In theory, the quantum key distribution (QKD) generates secure keys that are information-theoretically secure [1,2], even if hackers have the most powerful attacks that physical laws permit. However, in practical implementations, components may deviate from the protocol requirements, introducing vulnerabilities that eavesdroppers (Eve) could exploit to compromise system security [3–7]. As a result, Eve could steal the secure keys without being discovered. Therefore, when designing QKD protocols, the imperfections of the practical components should be considered to guarantee practical security.

Measurement-device-independent (MDI) QKD [8,9] protocols eliminate all detection-side loopholes from theory, significantly improving practical security. Recent developments in twin-field QKD [10–15] and mode-pairing QKD [16–18] are MDI-type QKD protocols and thus inherit high practical security. The decoy-state method [19–21] was developed to counteract photon-number-splitting attack [22,23] targeting imperfect single-photon sources. This method enables practical secure QKD implementation using weak coherent pulses generated by attenuated lasers.

However, loopholes may still exist in the source. The side channel effects in multidimensional space [24], including the frequency spectrum, the emission time, the shape of the wave, etc., can leak extra information to the eavesdropper, compromising the security of practical QKD systems [2,25]. Impressively, a type of such effect in multidimensional space named time-varying encoding was experimentally demonstrated and has shown its potential to undermine the security of source sides in QKD [26]. There are several ways to solve the threat in practice. For example, we can set standards for QKD devices against all known attacks and make well calibration before deployment, but it might be impossible to defend all multidimensional side channel attacks [27–31].

The side channel secure (SCS) QKD protocol [32] is theoretically proven secure over the whole-space states, including side channels in multi-dimensional space and operational space. The original SCS-QKD protocol [32] assumes perfect vacuum states and requires that the coherent state intensities be upper-bounded to ensure security. Recent theoretical advances have addressed the imperfect vacuum [33] and established a method to calculate the secure key rate (SKR) considering finite-key length [34]. The only assumptions are that Eve cannot access inside Alice's or Bob's laboratories, and the source states of each time window prepared inside the laboratory are independent of state choice information of other time windows. The real SCS-QKD protocol with imperfect sources can be mapped to a perfect protocol with two perfect sources; the secure key rate can be calculated as if we were carrying out the perfect protocol. Importantly, through worst-case estimation for the real states in Fock space,

the SCS protocol does not need the side channel information about states in the multidimensional side channel space and thus is immune to any attacks in the multidimensional space.

In this work, we experimentally demonstrated the SCS-QKD protocol [32,34] across 0–101.1 km fiber distances. Independent laser sources are stabilized locally using saturated absorption spectroscopy of acetylene as an absolute frequency reference, and real-time active phase compensation is used to improve the secure key rate. We achieve a finite-size secure key rate of 64.8 kbit/s at 0 km and 6.67 kbit/s at 50 km, which are approximately 40 times higher than the rates reported in previous work [35]. This work represents a practical implementation by eliminating the ideal vacuum and asymptotic assumptions required in the previous experiment.

II. PROTOCOL

Here, the practical two-state SCS-QKD protocol [32,34] with phase reference pulses and an active phase compensation method is used.

The protocol involves the following main steps. Alice and Bob first randomly prepare vacuum or coherent states with specific probabilities, which are called signal pulses. The prepared vacuum or coherent states can be imperfect in the whole space and different in different time windows. Alice (Bob) also prepares a strong reference pulse, time-multiplexed with the signal pulses. The phases of the reference pulses are modulated periodically, and this will be presented in detail later. No matter what she (he) decides, she (he) always sends the reference pulse to Charlie.

After receiving the signal pulses, Charlie first performs phase compensation and then an interferometry measurement at his measurement station. The measurement results will be announced to Alice and Bob. We define the effective window as the event where the right-side detector clicks and the left-side detector does not click.

After repeating the above process N times, Alice and Bob use data from effective windows for the raw bits. In the data postprocessing, they first perform error correction, and then they calculate the secure final key rate under collective attack by [34,36]

$$R_{\text{col}} = \frac{1}{N} \left\{ n_Z [1 - H(\bar{e}^{\text{ph}})] - \text{leak}_{\text{EC}} - \log_2 \frac{2}{\varepsilon_{\text{cor}}} - \log_2 \frac{1}{\varepsilon_{\text{PA}}^2} - 7 \sqrt{n_Z \log_2 \frac{2}{\bar{e}}} \right\}. \quad (1)$$

Here, leak_{EC} is the amount of information leakage during the error-correction process, and generally $\text{leak}_{\text{EC}} = f M_s H(E_Z)$, where f is the error-correction inefficiency, M_s is the number of raw keys, and E_Z is the bit-flip error rate of the raw key strings. n_Z is the number of effective windows in which only one of Alice and Bob decides to send out a coherent state pulse. $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ is the Shannon entropy, ε_{cor} is the failure probability of the error correction, ε_{PA} is the failure probability of the privacy amplification, and $\bar{e}$ is the coefficient for measuring the accuracy of estimating the smooth min-entropy. While Alice and Bob perform the privacy amplification process according to

Eq. (1), the protocol is ε_{cor} -correct and $\varepsilon_{\text{sec}} = \bar{e} + \varepsilon_{\text{PA}} + 3\xi$ -secret against collective attacks [37].

Applying the postselection technique [38,39], by shortening $2 \log_2(g_{N,x}) + 2 \log_2(1/\bar{e})$ bits of the final key against collective attack, Alice and Bob can obtain ε_{coh} -secure final key rate against coherent attack by

$$R_{\text{coh}} = R_{\text{col}} - \frac{1}{N} [2 \log_2(g_{N,x}) + 2 \log_2(1/\bar{e})], \quad (2)$$

where $g_{N,x} = \left(\frac{e^{(N+x-1)}}{x-1}\right)^{x-1}$ and $x = 64$ in the SCS protocol, and

$$\varepsilon_{\text{coh}} = \varepsilon_{\text{cor}} + g_{N,x} \left(\sqrt{8\varepsilon_{\text{sec}}} + \frac{\bar{e}}{2} \right). \quad (3)$$

In this work, we set $\varepsilon_{\text{cor}} = \varepsilon_{\text{coh}}/2$, $\sqrt{8\varepsilon_{\text{sec}}} = \bar{e}/2$, and $\bar{e} = \varepsilon_{\text{PA}} = \xi$.

III. EXPERIMENT

The experimental setup is shown in Fig. 1, consisting of the legitimate users (Alice and Bob) and the measurement node (Charlie). In the laboratories of Alice and Bob, independent fiber lasers serve as the light source without any external wavelength reference. The lasers are locked to specific transitions of acetylene molecules, with a central wavelength of 1542.3837 nm. We measured the phase fluctuation rate to be approximately 0.0168 rad/ μs between the two independent lasers (see Fig. 2). We attribute this phase drift to the different environmental conditions of the acetylene cells. The acetylene-stabilized lasers ensure highly stable frequency precision without external input reference, which is typically required in an optical phase-locked loop system. Therefore, the method avoids potential loopholes associated with external light injection [40].

The light is then modulated using a series of three intensity modulators. The SCS-QKD protocol encodes information solely through the “sending” and “not sending” signals. Three cascaded intensity modulators are used to achieve the ultralow vacuum intensity required. The encoded signal is then attenuated to single-photon level at the output. Strong reference pulses are time-division multiplexed with the signal pulses to compensate for the relative phase drift [11]. (See Supplemental Material [41] for details of the signal generation, which includes Refs. [42–44].) To prevent injection attacks [45,46], e.g., the laser-seeding attack, a circulator and an optical isolator are placed immediately following the attenuator. The total isolation of the isolator, circulator, and the attenuator exceeds 169 dB.

The signals are then transmitted to Charlie’s measurement station via fiber spools with a total length from 0 to 101.1 km. Upon arrival, the light is first polarized using a polarization beam splitter (PBS). One output of the PBS is directly routed to superconducting nanowire single-photon detector, serving as the monitoring port; the other output serving as the signal port is then directed to a beam splitter (BS) for interference. From the monitoring port, the detection count is stabilized to approximately 10% of the maximum intensities, by adjusting the electrically controlled polarization controller located at Alice’s (Bob’s) side, to compensate for the polarization drift

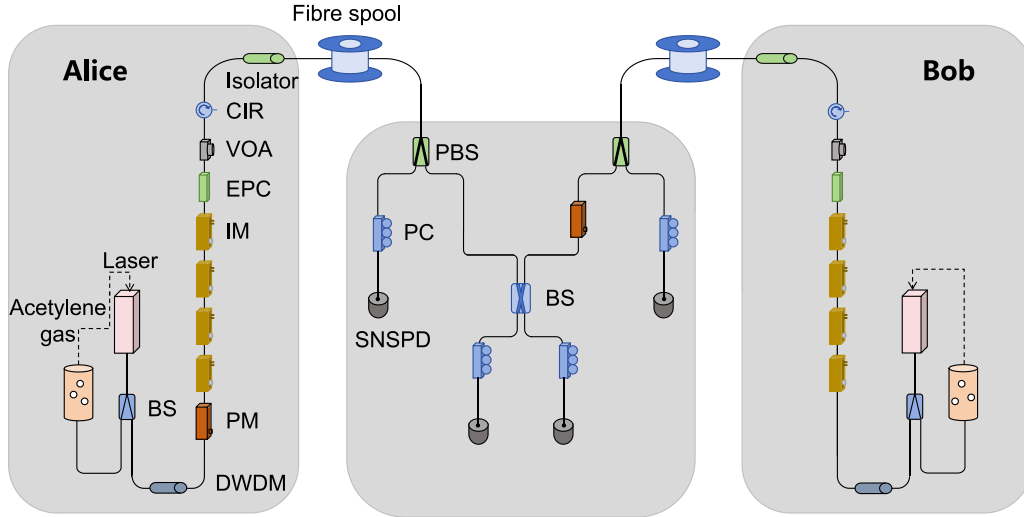


FIG. 1. Experimental setup. In Alice's and Bob's laboratories, two acetylene-stabilized lasers are employed as the light sources. First, these lasers are filtered by a dense wavelength division multiplexer (DWDM). Then, they are modulated with four intensity modulators (IMs) [and a phase modulator (PM) in Alice's laboratory] to generate a waveform pattern that time multiplexes the weak signal pulses with strong phase reference pulses and attenuates them to bring the signal pulses to the single-photon level with an attenuator (ATT). A circulator (CIR) and an optical isolator are placed immediately following the attenuator to prevent injection attacks. The prepared light pulses are finally sent to Charlie through the ultralow-loss fiber spools for detection. Charlie interferes and measures the light from Alice and Bob with superconducting nanowire single-photon detectors (SNSPDs). EPC, electric polarization controller; PC, polarization controller.

induced by the fiber channel. Consequently, the intensities of the signal port remain stable for subsequent interference.

The fast phase fluctuation induced by the channel fiber is compensated in real time with a PM positioned at the signal port of Bob's PBS. A custom-designed field-programmable gate array (FPGA) board was developed to execute the feedback. The proportional-integral-derivative (PID) algorithm was configured to stabilize the phase difference of the channel

to zero. In all experimental trials, the intensity of the reference light is set to approximately 2.5 MHz detections for the feedback. (See Supplemental Material [41] for details of the real-time feedback design.) The performance of the real-time compensation is evaluated by comparing the interference results with the feedback on and off. As shown in Figs. 3(a) and 3(b), the standard deviation of the phase fluctuation is suppressed to 0.17 rad with the real-time feedback.

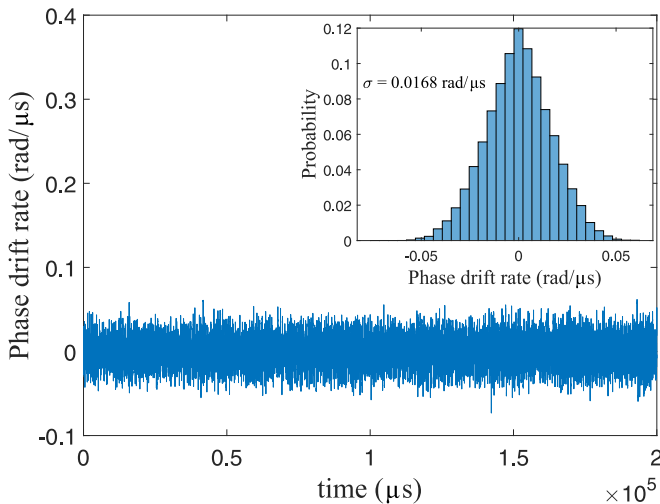


FIG. 2. Relative phase drift rate between the light sources. The interference signals from the two light sources were captured using an oscilloscope operating at a sampling rate of 1 MSA/s, with a total acquisition duration of 200 ms. A moving average filter with a 25 μ s window was applied to suppress high-frequency electrical noise. The standard deviation of the relative phase drift between the two light sources is 0.0168 rad/ μ s.

IV. RESULT

Our system operates at a repetition rate of 250 MHz with a 700 ps signal pulse width. The quantum signals are emitted in the last 40 ns of the 100 ns cycle, resulting in an effective signal frequency of 100 MHz. The extinction ratio between the signal and vacuum states is higher than 70 dB for all experimental trials. The standard deviation of the signal intensity fluctuation is approximately 0.54% of the average signal intensity. The interference results are measured with two SNSPDs and recorded by a time tagger. The detection efficiencies of the SNSPDs are 68.2% and 70.5%, with dark count rates of 8.4 and 7.5 Hz, respectively. (See Supplemental Material [41] for details of the parameters.)

We experimentally demonstrated SCS-QKD over fiber lengths from 0 to 101.1 km between Alice and Bob. The average attenuation of the fibers is 0.168 dB/km. The finite size effect is taken into consideration for all experimental tests to ensure the composable security under any coherent attack. In the calculation, the upper bound of the signal intensity is set to 102.15% of the average signal intensity, considering 4 times the standard deviation of the signal fluctuation. The error-correction inefficiency is set to $f = 1.16$, the statistics block size is set to the complete length of the test, and the security coefficient under coherent attack is $\epsilon_{\text{coh}} = 2 \times 10^{-10}$.

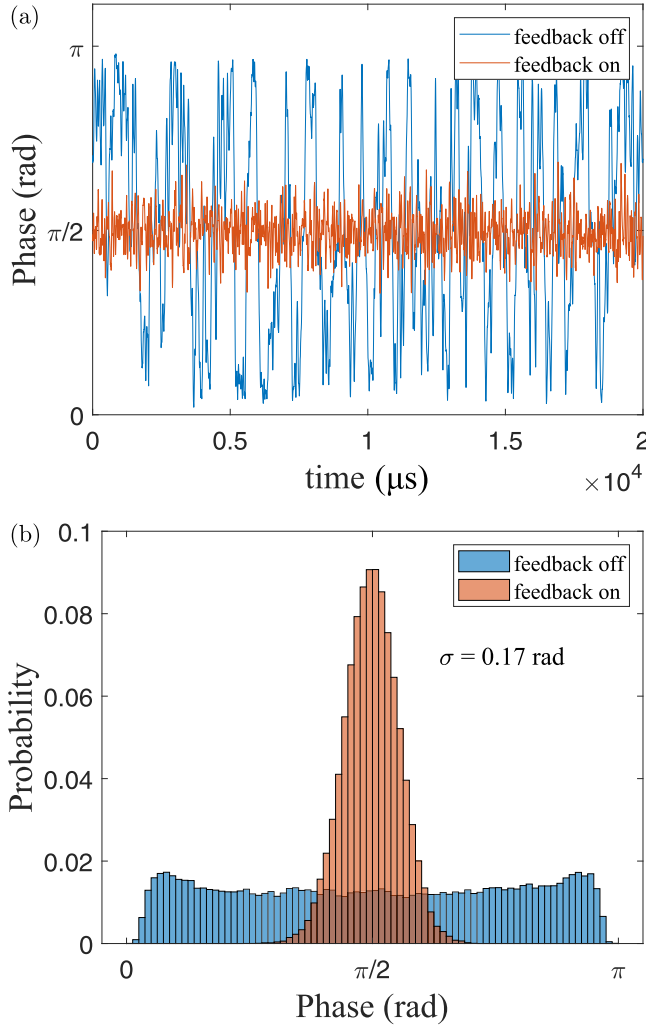


FIG. 3. (a) Phase drift compensation with the feedback on and off. The optical output power as a function of time measured at one output of Charlie's beam splitter is shown. (b) Phase distribution with the feedback on and off. The standard deviation of the phase fluctuation is 0.88 rad when the feedback is off, and 0.17 rad when the feedback is on.

For the 0 and 50.5 km cases, we set the fiber length of the Alice-Charlie and Bob-Charlie paths to be the same. However, the additional PM in Bob's path introduced a 3.05 dB higher insertion loss for Bob's path. To compensate for this imbalance, we optimized the transmitter's optical intensity (see Supplemental Material [41] for details of the parameters) to maximize the key rate. The total number of pulses sent by Alice and Bob is set to 3.63×10^{11} , corresponding to 1.01 h experimental time. The achieved secure key rate is 64.8 kbps for 0 km and 6.67 kbps for 50.5 km, as summarized in Fig. 4. The quantum bit error rates (QBERs) are 1.95% and 2.47%, respectively. Note that these secure key rates represent an $\sim 40\times$ improvement over the previous SCS-QKD experiment [35].

For the 25.3 and 75.7 km cases, we set the fiber length asymmetry to be approximately 25 km, and placed a 1.2 dB attenuator on Bob's side to balance the total loss, including Charlie's optics for Alice's and Bob's paths. The total number

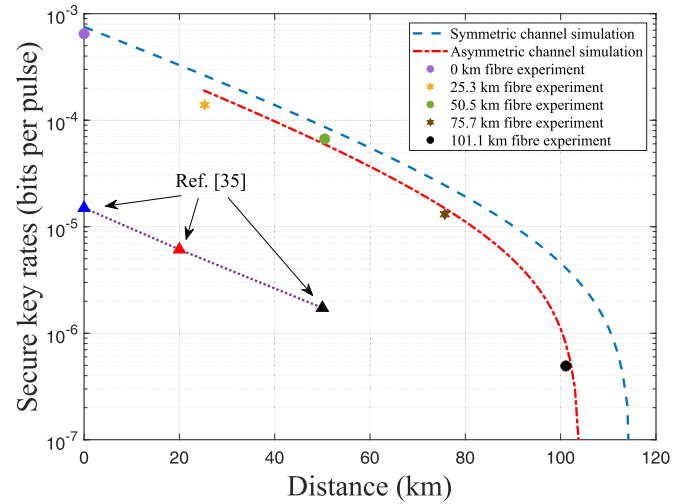


FIG. 4. Simulated and experimental secure key rates. Experimental results are shown for (1) symmetric fiber lengths: 0 km (purple dot), 50.5 km (green dot), and 101.1 km (black dot); and (2) asymmetric fiber lengths: 25.3 km (yellow star) and 75.7 km (brown star). Theoretical simulations are illustrated as dashed curves: blue for optimized symmetric channels and red for optimized asymmetric channels. Previous experimental SCS-QKD results from Ref. [35] are shown as triangles for comparison.

of pulses sent is 3.63×10^{11} , the same as in the 0 and 50.5 km cases. The achieved secure key rate is 13.9 kbps for 25.3 km and 1.31 kbps for 75.7 km, with QBERs of 2.99% and 2.48%.

For the 101.1 km fiber length, the fiber length is set to be symmetric. Additionally, we set a 600 ps width detection window to filter noise during data processing. This retains approximately 79% of the detections as valid events, decreasing the effective detection efficiency to about 55%. The number of quantum pulses sent is increased to 1.126×10^{12} , enabling us to collect a statistically reliable measurement dataset for evaluating finite-size effects. The achieved secure key rate is 49.3 bps.

In conclusion, we have experimentally demonstrated the SCS-QKD protocol. Compared with the previous experiment, our work addresses security, considering imperfect vacuum states and coherent attacks with finite pulse numbers. The results of our experiment are secure under whatever side channels in multidimensional space, such as the frequency spectrum, the emission time, and so on. The experiment achieves superior key rates and extends the maximum secure transmission distance to over 100 km. The achieved SKR below 100 km is comparable to that of previous MDI-QKD experiments [2]. We note that MDI-QKD holds a significant advantage in terms of distance; the SKR is about 15%–35% of the theoretically optimized MDI-QKD when intensity fluctuations are neglected and is comparable to MDI-QKD when considering the same level of intensity fluctuations. Although the SCS protocol already possesses a high level of security, there are still some issues that remain to be addressed in the future. From the theoretical perspective, the theory of statistical fluctuations in parameter characterization on security and safety factors is lacking. The security assumption in the source side, e.g., the independent state preparation

assumption, should be studied; the security and the performance of using sharper concentration inequalities designed for i.i.d. variables should be investigated. On the experimental side, the demonstration of longer transmission distances is possible with better noise performance. The prevention of eavesdroppers from stealing information inside the laboratory is also one of the future tasks.

ACKNOWLEDGMENTS

This work was supported by Innovation Program for Quantum Science and Technology (2021ZD0300700), Quantum Science and Technology-National Science and Technology Major Project (No. 2023ZD0300100), the Key R&D Plan of Shandong Province (Grant No. 2021ZDPT01), the National Natural Science Foundation of China (Grants No. T2125010,

No. 12174215, No. 12374470, and No. 12374473), Shandong Provincial Natural Science Foundation Grants No. ZR2021LLZ007 and No. ZR2024LLZ007, and the Chinese Academy of Sciences. C.J., X.-B.W., and Q.Z. acknowledge support from the Taishan Scholar Program of Shandong Province. Q.Z. was supported by the New Corner Stone Science Foundation through the Xplorer Prize.

DATA AVAILABILITY

The data that support the findings of this article are not publicly available upon publication because it is not technically feasible and/or the cost of preparing, depositing, and hosting the data would be prohibitive within the terms of this research project. The data are available from the authors upon reasonable request.

-
- [1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, edited by G. R. Blakley and D. Chaum (IEEE, New York, 1984), pp. 175–179.
 - [2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* **92**, 025002 (2020).
 - [3] 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).
 - [4] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, *Nat. Photon.* **4**, 686 (2010).
 - [5] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, Laser damage helps the eavesdropper in quantum cryptography, *Phys. Rev. Lett.* **112**, 070503 (2014).
 - [6] K.-i. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, and A. Tomita, Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses, *npj Quantum Inf.* **4**, 8 (2018).
 - [7] Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Hacking the quantum key distribution system by exploiting the avalanche-transition region of single-photon detectors, *Phys. Rev. Appl.* **10**, 064062 (2018).
 - [8] S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, *Phys. Rev. Lett.* **108**, 130502 (2012).
 - [9] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
 - [10] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, *Nature (London)* **557**, 400 (2018).
 - [11] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental twin-field quantum key distribution through sending or not sending, *Phys. Rev. Lett.* **123**, 100505 (2019).
 - [12] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km, *Phys. Rev. Lett.* **124**, 070501 (2020).
 - [13] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas, *Nat. Photon.* **15**, 570 (2021).
 - [14] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, D.-F. Zhao, W.-J. Zhang, F.-X. Chen, H. Li, L.-X. You, Z. Wang, Y. Chen, X.-B. Wang, Q. Zhang, and J.-W. Pan, Quantum key distribution over 658 km fiber with distributed vibration sensing, *Phys. Rev. Lett.* **128**, 180502 (2022).
 - [15] 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, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental twin-field quantum key distribution over 1000 km fiber distance, *Phys. Rev. Lett.* **130**, 210801 (2023).
 - [16] P. Zeng, H. Zhou, W. Wu, and X. Ma, Mode-pairing quantum key distribution, *Nat. Commun.* **13**, 3903 (2022).
 - [17] H.-T. Zhu, Y. Huang, H. Liu, P. Zeng, M. Zou, Y. Dai, S. Tang, H. Li, L. You, Z. Wang, Y.-A. Chen, X. Ma, T.-Y. Chen, and J.-W. Pan, Experimental mode-pairing measurement-device-independent quantum key distribution without global phase locking, *Phys. Rev. Lett.* **130**, 030801 (2023).
 - [18] H.-T. Zhu, Y. Huang, W.-X. Pan, C.-W. Zhou, J. Tang, H. He, M. Cheng, X. Jin, M. Zou, S. Tang, X. Ma, T.-Y. Chen, and J.-W. Pan, Field test of mode-pairing quantum key distribution, *Optica* **11**, 883 (2024).
 - [19] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
 - [20] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).
 - [21] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).

- [22] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on practical quantum cryptography, *Phys. Rev. Lett.* **85**, 1330 (2000).
- [23] N. Lütkenhaus, Security against individual attacks for realistic quantum key distribution, *Phys. Rev. A* **61**, 052304 (2000).
- [24] A. Navarrete, M. Pereira, M. Curty, and K. Tamaki, Practical quantum key distribution that is secure against side channels, *Phys. Rev. Appl.* **15**, 034072 (2021).
- [25] A. Huang, S.-H. Sun, Z. Liu, and V. Makarov, Quantum key distribution with distinguishable decoy states, *Phys. Rev. A* **98**, 012330 (2018).
- [26] A. Gnanapandithan, L. Qian, and H.-K. Lo, Hidden multi-dimensional modulation side channels in quantum protocols, *Phys. Rev. Lett.* **134**, 130802 (2025).
- [27] G. Currás-Lorenzo, M. Pereira, G. Kato, M. Curty, and K. Tamaki, Security framework for quantum key distribution with imperfect sources, *Optica Quantum* **3**, 525 (2025).
- [28] V. Zapatero, Á. Navarrete, and M. Curty, Implementation security in quantum key distribution, *Adv. Quantum Technol.* **8**, 2300380 (2025).
- [29] D. Tupkary, S. Nahar, P. Sinha, and N. Lütkenhaus, Phase error rate estimation in QKD with imperfect detectors, *Quantum* **9**, 1937 (2025).
- [30] S. Nahar, D. Tupkary, and N. Lütkenhaus, Imperfect detectors for adversarial tasks with applications to quantum key distribution, [arXiv:2503.06328](https://arxiv.org/abs/2503.06328).
- [31] G. Currás-Lorenzo, M. Pereira, S. Nahar, and D. Tupkary, Security of quantum key distribution with source and detector imperfections through phase-error estimation, [arXiv:2507.03549](https://arxiv.org/abs/2507.03549).
- [32] X.-B. Wang, X.-L. Hu, and Z.-W. Yu, Practical long-distance side-channel-free quantum key distribution, *Phys. Rev. Appl.* **12**, 054034 (2019).
- [33] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, Side-channel-secure quantum key distribution with imperfect vacuum sources, *Phys. Rev. Appl.* **19**, 064003 (2023).
- [34] C. Jiang, X.-L. Hu, Z.-W. Yu, and X.-B. Wang, Side-channel security of practical quantum key distribution, *Phys. Rev. Res.* **6**, 013266 (2024).
- [35] C. Zhang, X.-L. Hu, C. Jiang, J.-P. Chen, Y. Liu, W. Zhang, Z.-W. Yu, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental side-channel-secure quantum key distribution, *Phys. Rev. Lett.* **128**, 190503 (2022).
- [36] C. Jiang, X.-L. Hu, Z.-W. Yu, H. Xu, and X.-B. Wang, Side-channel-secure quantum key distribution with state-dependent correlated errors and Trojan-horse attack, *Opt. Express* **33**, 51715 (2025).
- [37] L. Sheridan, T. P. Le, and V. Scarani, Finite-key security against coherent attacks in quantum key distribution, *New J. Phys.* **12**, 123019 (2010).
- [38] M. Christandl, R. König, and R. Renner, Postselection technique for quantum channels with applications to quantum cryptography, *Phys. Rev. Lett.* **102**, 020504 (2009).
- [39] S. Nahar, D. Tupkary, Y. Zhao, N. Lütkenhaus, and E. Y.-Z. Tan, Postselection technique for optical quantum key distribution with improved de Finetti reductions, *PRX Quantum* **5**, 040315 (2024).
- [40] Q. Peng, J.-P. Chen, T. Xing, D. Wang, Y. Wang, Y. Liu, and A. Huang, Practical security of twin-field quantum key distribution with optical phase-locked loop under wavelength-switching attack, *npj Quantum Inf.* **11**, 7 (2025).
- [41] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/fxxb-9y8n> for the details of the signal generation, real-time feedback design, and experimental parameters.
- [42] V. Scarani and R. Renner, Security bounds for quantum cryptography with finite resources, in *Workshop on Quantum Computation, Communication, and Cryptography* (Springer, Berlin, Heidelberg, 2008), pp. 83–95.
- [43] 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, and Z.-F. Han, Intensity modulator for secure, stable, and high-performance decoy-state quantum key distribution, *npj Quantum Inf.* **7**, 75 (2021).
- [44] G. L. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution, *Opt. Lett.* **43**, 5110 (2018).
- [45] V. Lovic, D. Marangon, P. Smith, R. Woodward, and A. Shields, Quantified effects of the laser-seeding attack in quantum key distribution, *Phys. Rev. Appl.* **20**, 044005 (2023).
- [46] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Practical security bounds against the Trojan-horse attack in quantum key distribution, *Phys. Rev. X* **5**, 031030 (2015).