Quantum Frontiers
上海交通大學 SHANGHAI JIAO TONG UNIVERSITY 李政道研究所 Tsung-Dao Lee Institute

ORIGINAL ARTICLE Open Access

1002 km twin-field quantum key distribution with finite-key analysis

Yang Liu[1,2,3†], Wei-Jun Zhang[3,4†], Cong Jiang[2,3], Jiu-Peng Chen[1,2,3], Di Ma[2], Chi Zhang[1,2], Wen-Xin Pan[1], Hao Dong[1,2], Jia-Min Xiong[4], Cheng-Jun Zhang[5], Hao Li[3,4], Rui-Chun Wang[6], Chao-Yang Lu[1,3], Jun Wu[6], Teng-Yun Chen[1,3], Lixing You[3,4*], Xiang-Bin Wang[2,3,7*], Qiang Zhang[1,2,3*] and Jian-Wei Pan[1,3*]

Abstract

Quantum key distribution (QKD) holds the potential to establish secure keys over long distances. The distance of point-to-point QKD secure key distribution is primarily impeded by the transmission loss inherent to the channel. In the quest to realize a large-scale quantum network, increasing the QKD distance under current technology is of great research interest. Here we adopt the 3-intensity sending-or-not-sending twin-field QKD (TF-QKD) protocol with the actively-odd-parity-pairing method. The experiment demonstrates the feasibility of secure QKD over a 1002 km fibre channel considering the finite size effect. The secure key rate is 3.11×10^{-12} per pulse at this distance. Furthermore, by optimizing parameters for shorter fiber distances, we conducted performance tests on key distribution for fiber lengths ranging from 202 km to 505 km. Notably, the secure key rate for the 202 km, the normal distance between major cities, reached 111.74 kbps.

Keywords: Quantum key distribution, Quantum communication, Quantum optics, Quantum information

1 Introduction

Quantum key distribution (QKD) [1–7] ensures secure key distribution using the principles of quantum mechanics. An active research frontier in practical quantum cryptography is exploring the distribution distance achievable with the present technology. The main challenge in extending the distribution distance of QKD is the channel loss that occurs when transmitting single-photon level quantum signals. Unlike classical communication, quantum signals cannot be amplified, posing a significant hurdle [8]. The exponentially decreased transmission of the optical fibre channel results in a vanishing secure key rate at long distances. Importantly, the limited number of detected signals over long distances also constrains the secure key rate due to the finite-key effect.

In the quest for achieving long-distance QKD, twin-field QKD (TF-QKD) is proposed [9] recently. TF-QKD may achieve a secure key rate in spirit similar to that of a single-repeater QKD scenario, significantly increasing the ultimate distance. Within a few years, TF-QKD has already been experimentally demonstrated in lab [10–21] through up to 1002 km spooled fibre [21], and in the field test over 511 km deployed fibre across metropolitans [17]. However, the previous 1002 km distribution distance [21] was achieved under an asymptotic assumption. The longest distribution distance considering the finite size effect was reported to be 952 km [21]. The finite-size effect has to be taken into account in a practical QKD system since there are only a finite number of pulses. This consideration allows us to quantify the security level, i.e., the security coefficient; and apply the composable security framework.

*Correspondence: lxyou@mail.sim.ac.cn; xbwang@mail.tsinghua.edu.cn; qiangzh@ustc.edu.cn; pan@ustc.edu.cn
[2]Jinan Institute of Quantum Technology and CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Jinan, 250101, Shandong, China
[3]Hefei National Laboratory, University of Science and Technology of China, Hefei, 230088, Anhui, China
Full list of author information is available at the end of the article †Equal contributors

Springer

© The Author(s) 2023. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

In this work, we demonstrate TF-QKD over 1002 km fibre channel considering the finite size effect. We adopt the sending-or-not-sending (SNS) protocol [22] with advanced 3-intensity decoy-state method [23] and the actively-odd-parity-pairing (AOPP) [24, 25] to improve the distribution distance. The ultra-low-noise superconducting nanowire single-photon detectors (SNSPDs) and dual-band phase estimation method are developed to suppress the system noise, thus achieving long distribution distance. Furthermore, the system is optimized for the normal distance between major cities of a fibre distance of 202 km. A secure key rate of 111.74 kbps is achieved at this distance, better than any reported results to our best knowledge.

2 Results and discussion

2.1 Protocol

In this work, we adopt the 3-intensity SNS protocol developed by Wang et al. [22]. By placing the error correction process ahead of the decoy-state analysis process [23], we can utilize all the heralded time windows for decoy-state analysis, resulting in an enhanced key rate. Furthermore, we also apply the AOPP [24] method to reduce the bit-flip error rate. The source parameters are symmetric for Alice and Bob: there are three sources on each side which are the vacuum source ν, the decoy source x, and the signal source y with intensities $\mu_\nu = 0$, μ_x, μ_y and probabilities p_0, p_x, p_y respectively. In each time window, Alice (Bob) randomly prepares and sends out a pulse from the three candidate sources to Charlie who is assumed to measure the interference result of the incoming pulse pair and announce the measurement results to Alice and Bob. In this work, the raw keys in the time windows, while Alice and Bob choose the sources ν or y, are used to extract the secure keys. After Alice and Bob send N pulse pairs to Charlie, and Charlie announces all measurement results, Alice and Bob distill the secure keys according to the following formula [23, 25, 26]:

$$R = \frac{1}{N}\left\{n_1\left[1 - H\left(e_1^{ph}\right)\right] - f n_t H(E_t)\right\} - R_{\text{tail}}, \tag{1}$$

where R is the key rate of per sending-out pulse pair; n_1 is the lower bound of the number of survived untagged bits after AOPP and e_1^{ph} is the upper bound of the phase-flip error rate of those survived untagged bits after AOPP; n_t is the number of survived bits after AOPP and E_t is the corresponding bit-flip error rate in those survived bits; f is the error correction inefficiency which is set to $f = 1.16$; $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the Shannon entropy. And R_{tail} is

$$R_{\text{tail}} = \frac{1}{N}\left[2\log_2\frac{2}{\varepsilon_{\text{cor}}} + 4\log_2\frac{1}{\sqrt{2}\varepsilon_{PA}\hat{\varepsilon}} + 2\log_2(n_{vy} + n_{yv})\right], \tag{2}$$

where ε_{cor} is the failure probability of error correction, ε_{PA} is the failure probability of privacy amplification, $\hat{\varepsilon}$ is the coefficient while using the chain rules of smooth min- and max- entropy [27], and $2\log_2(n_{vy} + n_{yv})$ is the extra cost of the advanced decoy state analysis [23] (n_{vy} is the number of raw keys while Alice chooses the source ν and Bob chooses the source y, and the definition of n_{yv} is similar with that of n_{vy}).

2.2 Experiment

The experimental setup is shown in Fig. 1. The seed lasers (λ_1 = 1548.51 nm and λ_2 = 1550.12 nm) are frequency stabilized using the Pound-Drever-Hall (PDH) technique [28–30] with an ultra-stable cavity serving as the reference. The light is then sent to Alice's and Bob's stations through 450 km single-mode fibres respectively, incorporating 4 erbium-doped fibre amplifiers (EDFAs) in each path to stabilize the intensity. At Alice's (Bob's) station, the λ_1 light from Charlie is modulated to a 400 ns pulse in each 1 μs period, functioning as the "strong phase reference". The λ_2 light serves as the frequency reference for the optical phase-locked loop (OPLL). The locally produced λ_2 laser is locked to the frequency reference from Charlie, and then modulated to "dim phase reference" and "quantum signals". As shown in Fig. 2, the intensity of the 40 ms "dim phase reference" is generally higher than the 60 ms "quantum signals" light. In each 1 μs period, the pulse train is modulated to the same random pattern in the first 400 ns for Alice and Bob, serving as the "dim phase reference". In the remaining 600 ns, the pulse train is modulated to generate random quantum signals based on their respective local random numbers. Note that only the detections occurring within the first 400 ns in each 1 μs period, and within the first 40 ms in the 100 ms period, are utilized as the "dim phase reference". Similarly, the detections in the last 600 ns of each 1 μs period, and the last 60 ms of the 100 ms period, are used as the "quantum signals". For both the "strong phase reference" and "dim phase reference", the relative phases between Alice and Bob are set to four relative phases $\delta_{AB} = \{0, \pi/2, \pi, 3\pi/2\}$ within a 1 μs period.

We implemented the 3-intensity SNS-TF-QKD protocol in the experiment. The λ_2 quantum signals are modulated to 3 intensities with 16 different phases using intensity modulators (IMs) and phase modulators. The IMs are stabilized at Alice's (Bob's) station to ensure the quantum signals' intensities are stable. The λ_1 "strong phase reference" is then filtered and combined with the quantum

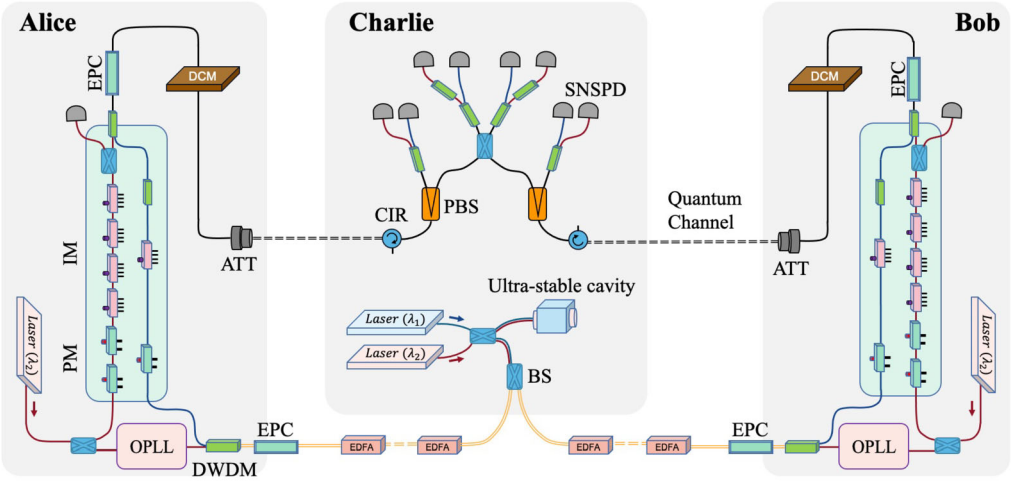


Figure 1 Experimental setup. The seed lasers (λ_1 = 1548.51 nm and λ_2 = 1550.12 nm) for the phase reference and quantum signal are distributed from Charlie to Alice and Bob through 900 km single mode fibre spools. The locally generated λ_2 light is frequency locked to the seed laser with an optical phase-locked loop (OPLL), and modulated to quantum signals. The "dim phase reference" is generated by time-multiplexing with the quantum signal. The λ_1 light is modulated to "strong phase reference", and then combined with the quantum signals by wavelength-multiplexing. The quantum signals are transmitted through the quantum channel and interfered at Charlie. The interference results are detected with SNSPDs. The local intensity monitors at Alice and Bob, the polarization and the relative delay at Charlie, and the "strong phase reference" signals are also detected with SNSPDs. BS, beam splitter; PBS, polarization beam splitters; IM, intensity modulator, PM, phase modulator; ATT, attenuator; DWDM, dense wavelength division multiplexing; CIR, optical circulator; EDFA, erbium-doped fibre amplifier; DCM, dispersion compensation module; EPC, electronic polarization controller

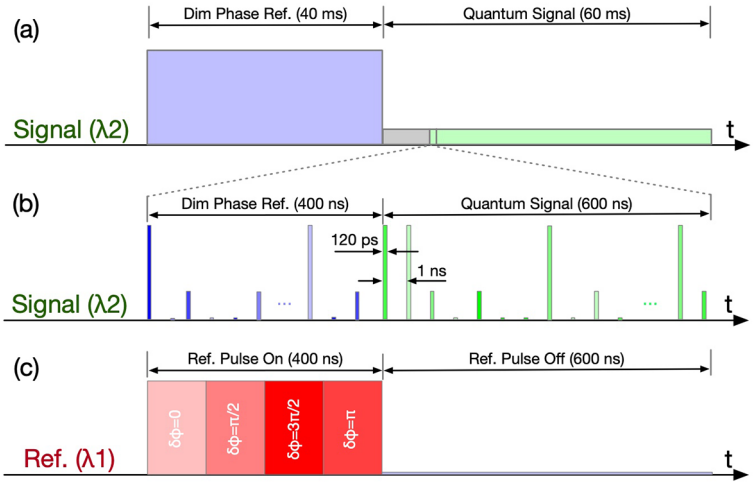


Figure 2 Time sequence of the quantum signals and the reference signals: (a) The λ_2 light is modulated to a 100 ms period, including 40 ms "dim phase reference", and 60 ms "quantum signals". (b) The λ_2 light is modulated to a 1 GHz pulse train in each 1 μs period: in the first 400 ns, Alice and Bob modulate the pulses to the same intensity pattern, with four relative phases between them, as the "dim phase reference"; in the remaining 600 ns, they modulate random "quantum signals" based on Alice's/Bob's random numbers, respectively. (c) The λ_1 "strong phase reference" light is modulated to a 400 ns pulse in each 1 μs period, with four relative phases between Alice and Bob

signals. An electronic polarization controller is installed within the secure zone to control the polarization drift. A dispersion compensation module is employed to pre-compensate for the chromatic dispersion of the fibre channel. The signals are then attenuated to the predetermined intensities and subsequently transmitted to Charlie via the quantum channels.

The polarization of different wavelengths may evolute differently. At Charlie's measurement station, a polarization feedback algorithm is utilized to optimize the λ_1 de-

tections to between 75 kHz and 300 kHz, while minimizing the λ_2. The relative delay between Alice's and Bob's signals is monitored and compensated using the rising edges of the λ_1 pulses. The light from Alice and Bob is interfered at the beam splitter and subsequently demultiplexed to λ_1 and λ_2 wavelengths. This light is then filtered by DWDMs, measured with SNSPDs, and recorded with a Time Tagger. The recorded signals are categorized into the "strong phase reference", "dim phase reference" and the quantum signal for subsequent data processing.

The ultra-low loss fibre is utilized to minimize channel loss. The fibre is manufactured with "pure silica core" technology to reduce the doped Ge in the core and with decreased fictive temperature. The average attenuation of the fibres is measured to be less than 0.157 dB/km.

The ultra-low dark count SNSPDs are developed to reduce detection-related noise. The noise suppression includes stages of filtering. The long-wavelength (>2 μm) filtering is achieved using the 28 mm diameter fibre coils at the 40 K cold plate. Narrowband wavelength filtering is carried out utilizing a cryogenic bandpass filter (BPF) with a 5 nm bandwidth and an 85% transmittance at 2.2 K cold plate [31]. The dark count rate is measured to be as low as 0.02 Hz. Additionally, the detection efficiency is optimized to be around 60% with a distributed Bragg reflector (DBR) based optical cavity [32].

The time-multiplexed dual-band stabilization method is employed to reduce the re-Rayleigh scattering noise induced in previously reported time-multiplexed phase estimation procedures. With dual-band stabilization, the wavelength of the "strong phase reference" of λ_1 is different from the quantum signal of λ_2. The induced re-Rayleigh scattering is filtered with DWDMs. Furthermore, circulators are implemented in Charlie to eliminate noise resulting from the SNSPDs. Additionally, the λ_1 "strong phase reference" is time-multiplexed with the quantum signal, effectively mitigating disturbance caused by spontaneous Raman scattering noise induced by the strong phase reference light. The combination of wavelength- and time-multiplexing ensures that the noise introduced by the strong phase reference signal is less than 0.01 Hz. Moreover, the intensity of the weak "dim phase reference" signal, which is also time-multiplexed with the quantum signal, remains low enough to not generate perceptible noise.

The data post-processing-based phase estimation method [21] is adopted. First, the phase drift of the λ_1 wavelength is estimated using the "strong phase reference". Then, the wavelength difference is taken into account to estimate the phase of the λ_2 light, with the accumulated phase drift of the "strong phase reference". Lastly, the initial phase difference $\phi_s(0) - \phi_r(0)$ is computed using the phase difference between the "dim phase reference" and the "strong phase reference". In the experiment, this phase

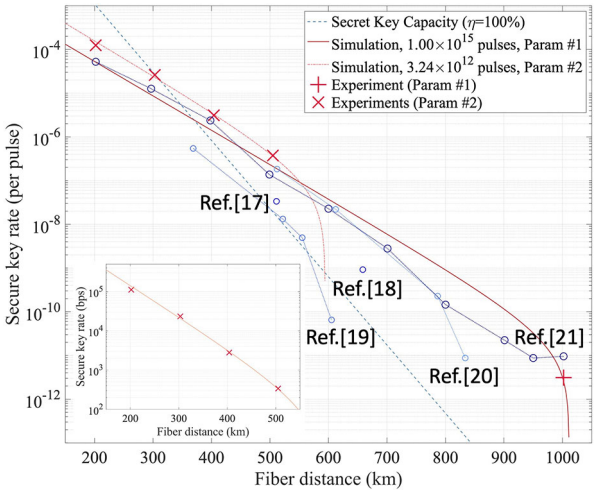


Figure 3 Simulations and experimental results of the secure key rates. The "+"-shape points are experimental results using the long-distance optimized parameter (Parameter #1), and the "×"-shape points are experimental results using the short-distance optimized parameter (Parameter #2). The solid curve is the simulation results with Parameter #1. The red dashed curve is the simulation result with Parameter #2. All simulations and experimental results considered the finite size effect. The circle markers indicates the state-of-the-art TF-QKD results reported in Ref. [17–21]. The blue dashed line shows the secret key capacity, i.e., the PLOB bound. Insert: the secure key rate per second in short distances

difference is computed and refreshed every 500 ms, to circumvent any accumulation of errors stemming from inaccurate wavelength settings, high-order residual phase errors, and errors in phase estimation.

Result We first test the performance of 1002 km fibres (the "+"-shape points in Fig. 3). The fibre distances between Alice-Charlie and Bob-Charlie are measured to be 500 km and 502 km. The decoy intensities are optimized as $\mu_x = 0.08$, $\mu_y = 0.445$, with the time ratios $p_{\text{vac}} = 0.52$, $p_x = 0.28$, $p_y = 0.20$ (Parameter #1). The finite size effect [26] is taken into consideration for all the experimental tests, considering composable security under any coherent attack [26, 33]. The error correction inefficiency is set to $f = 1.16$ in the calculation; the failure probability of Chernoff bound in finite-size estimation is set to $\varepsilon = 10^{-10}$; the failure probability of the error correction, and the privacy amplification is set to $\varepsilon_{\text{cor}} = \varepsilon_{PA} = 10^{-10}$; the coefficient of the chain rules of smooth min- and max- entropies is set to $\hat{\varepsilon} = 10^{-10}$.

The system frequency is set to 1 GHz, with the signal pulse width set to 120 ps. The quantum signals are sent in the last 600 ns of the 1 μs period where the "strong phase reference" is switched off. The quantum signals are time-multiplexed with the "dim phase reference" in the last 60 ms of the 100 ms period. The detections near the strong

Table 1 Experimental results for fibre lengths between 202 km and 1002 km. L: total fibre distance, η: total fibre transmittance, N: total signal pulses Alice and Bob sent, n_1: untagged bits after AOPP, e_1^{ph}: phase-flip error rate after AOPP, n_t: survived bits after AOPP, E_t: bit-flip error rate after AOPP, E_x: X-basis QBER of the raw bits, R: secure key rate per pulse, R (bps): secure key rate per second

L	202 km	303 km	404 km	505 km	1002 km
η	31.6 dB	46.9 dB	62.9 dB	78.6 dB	156.5 dB
N	3.24×10^{12}	3.24×10^{12}	3.24×10^{12}	3.24×10^{12}	1.00×10^{15}
n_1	7.92×10^{8}	1.56×10^{8}	2.25×10^{7}	3.29×10^{6}	39454
e_1^{ph}	10.24%	9.17%	10.31%	13.24%	17.05%
n_t	2.17×10^{9}	4.27×10^{8}	6.22×10^{7}	9.41×10^{6}	111671
E_t	3.88×10^{-4}	4.28×10^{-4}	2.28×10^{-3}	1.88×10^{-3}	9.44×10^{-3}
E_x	4.25%	3.63%	3.76%	3.62%	4.20%
R	1.24×10^{-4}	2.60×10^{-5}	3.11×10^{-6}	3.76×10^{-7}	3.11×10^{-12}
R (bps)	111,735	23,438	2,797	338	0.0011

light are also dropped to avoid potential noises. As a result, the effective signal frequency is 351 MHz for the long-distance scenario.

The total noises in the λ_2 are measured to be 0.019 Hz and 0.035 Hz in the working conditions. We attribute the noise mainly contributed by the SNSPD dark count and the spontaneous Raman scattering noise induced by the λ_1 light. The SNSPD detection efficiencies are measured to be 60% and 55%. The additional optical losses in Charlie are measured to be around 1.4 dB. In data processing, a 200 ps window is defined to filter out noises, with an efficiency of about 65%.

Owing to the significant optical attenuation experienced over long-distance fibre, it is necessary to send a larger number of quantum signals in order to generate secure keys considering the finite size effect. A total of 1.00×10^{15} quantum signal pulses are dispatched, resulting in 9.81×10^5 valid detections that fall within the effective window. The quantum bit error rate (QBER) in Z basis is measured to be 9.44×10^{-3} after AOPP; the QBER in X basis is measured to be 4.20%. The final secure key is 3.11×10^{-12}, which equates to 0.0011 bps considering the effective signal frequency. A total of 3112 bits of final secure keys are accumulated during the test. The detailed experimental results are summarized in Table 1 and Fig. 3. See Additional file 1 for the full experimental results.

Next, we test the performance of fibre distances between 202 km and 505 km (the "×"-shape points in Fig. 3). The intensities of the decoy states are optimized for short distances as $\mu_x = 0.05$, $\mu_y = 0.482$, with the time ratios $p_{\text{vac}} = 0.68$, $p_x = 0.04$, $p_y = 0.28$ (Parameter #2). The "strong phase reference" period is reduced to 100 ns in the 1 μs signal period; the intensity of the "dim phase reference" is set to the same as the quantum signal through the 100 ms period. As a result, the effective signal frequency is increased to 900 MHz. Besides, we used SNSPDs with >80% detection efficiency and a relatively higher dark count rate of about 10 Hz. The time window in data processing is set to 500 ps, yielding an almost unity efficiency.

A total of 3.24×10^{12} quantum signal pulses are sent for each distance, which equals to one hour of experimental time. The secure key rate is measured to be 1.24×10^{-4}, 2.60×10^{-5}, 3.11×10^{-6}, and 3.76×10^{-7} which corresponds to 111.74 kbps, 23.44 kbps, 2.80 kbps, and 338 bps for the 202 km, 303 km, 404 km, and 505 km fibre distances, respectively. The secure key rates exceed the absolute PLOB bound [34] for the tests with the fibre distances equal to or longer than 404 km, where the PLOB bound is calculated as $-\log_2(1-\eta)$ with the optical and detection efficiency in Charlie set to $\eta_{\text{opt}} = 100\%$.

3 Conclusion

In conclusion, we have demonstrated the first experiment of SNS-TF-QKD over a remarkable distance of 1002 km, while considering the finite size effect. The result has been made possible by employing several key components, including the ultra-low-loss fiber, ultra-low-noise SNSPD, dual-band phase stabilization method, and moderate data size. The achieved secure key rates over fiber distances ranging from 202 km to 505 km were highly practical, indicating the potential for supporting a wide range of applications. In addition to improving the performance, TF-QKD is also expected to be implemented in chip-scale systems in the future, based on recent advancements in chip-scale systems implementing BB84 and MDI-QKD protocols [35–38].

Supplementary information

Supplementary information accompanies this paper at https://doi.org/10.1007/s44214-023-00039-9.

Additional file 1. (PDF 68 kB)

Acknowledgements
Not applicable.

Funding
Open access funding provided by Shanghai Jiao Tong University. This work was supported by the Key R&D Plan of Shandong Province (Grant No.

2021ZDPT01, 2020CXGC010105), the National Key Research and Development (R&D) Plan of China (Grant No. 2020YFA0309800), the Innovation Program for Quantum Science and Technology (2021ZD0300700), the National Natural Science Foundation of China (Grant Nos. T2125010, 12174215, 61971409 and 61971408), the Chinese Academy of Sciences, Shandong Provincial Natural Science Foundation (Grant Nos. ZR2020YQ45, ZR2022LLZ011). Y.L. and Q.Z. acknowledge support from the Taishan Scholar Program of Shandong Province, W.-J.Z. acknowledges support from the Youth Innovation Promotion Association (No. 2019238).

Availability of data and materials
The data that support the findings of this study are available from the corresponding author on reasonable request.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
CYL and QZ are editorial board members for Quantum Frontiers and was not involved in the editorial review, or the decision to publish, this article. All authors declare that there are no competing interests.

Author contributions
YL and W-JZ contribute equally. X-BW, QZ and J-WP conceived the research. YL, CJ, X-BW, QZ and J-WP designed the experiment. YL, DM, CZ, HD, build the optical and the software system. J-PC build the ultra-stable laser and the OPLL system. W-XP build the polarization feedback system. W-JZ, J-MX, C-JZ, HL and LY build the ultra-low noise SNSPD. R-CW and JW fabricated the ultra-low-loss fiber. CJ and X-BW performed the theoretical analysis. YL, CJ, J-PC, DM, CZ, W-XP, HD, C-YL, T-YC, X-BW, QZ and J-WP contributed to the data analysis and revision of the manuscript. The author(s) read and approved the final manuscript.

Author details
[1]Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences, University of Science and Technology of China, Hefei, 230026, Anhui, China. [2]Jinan Institute of Quantum Technology and CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Jinan, 250101, Shandong, China. [3]Hefei National Laboratory, University of Science and Technology of China, Hefei, 230088, Anhui, China. [4]State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai, 200050, China. [5]Photon Technology (Zhejiang) Co. Ltd., Jiaxing, 314100, Zhejiang, China. [6]State Key Laboratory of Optical Fibre and Cable Manufacture Technology, Yangtze Optical Fibre and Cable Joint Stock Limited Company, Wuhan, 430073, Hubei, China. [7]State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing, 100084, China.

Received: 10 October 2023 Revised: 10 October 2023
Accepted: 1 November 2023 Published online: 24 November 2023

References

1. Bennett CH, Brassard G (1984) Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE international conference on computers, systems, and signal processing, pp 175–179
2. Ekert AK (1991) Quantum cryptography based on bell's theorem. Phys Rev Lett 67(6):661
3. Gisin N, Ribordy G, Tittel W, Zbinden H (2002) Quantum cryptography. Rev Mod Phys 74(1):145
4. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M (2009) The security of practical quantum key distribution. Rev Mod Phys 81(3):1301
5. Gisin N (2015) How far can one send a photon? Front Phys 10:100307
6. Xu F, Ma X, Zhang Q, Lo H-K, Pan J-W (2020) Secure quantum key distribution with realistic devices. Rev Mod Phys 92(2):025002
7. Pirandola S, Andersen UL, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C et al (2020) Advances in quantum cryptography. Adv Opt Photonics 12(4):1012–1236
8. Wootters WK, Zurek WH (1982) A single quantum cannot be cloned. Nature 299(5886):802–803
9. Lucamarini M, Yuan ZL, Dynes JF, Shields AJ (2018) Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature 557(7705):400
10. Minder M, Pittaluga M, Roberts G, Lucamarini M, Dynes J, Yuan Z, Shields A (2019) Experimental quantum key distribution beyond the repeaterless secret key capacity. Nat Photonics 13(5):334
11. Wang S, He D-Y, Yin Z-Q, Lu F-Y, Cui C-H, Chen W, Zhou Z, Guo G-C, Han Z-F (2019) Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system. Phys Rev X 9(2):021046
12. Liu Y, Yu Z-W, Zhang W, Guan J-Y, Chen J-P, Zhang C, Hu X-L, Li H, Jiang C, Lin J et al (2019) Experimental twin-field quantum key distribution through sending or not sending. Phys Rev Lett 123(10):100505
13. Zhong X, Hu J, Curty M, Qian L, Lo H-K (2019) Proof-of-principle experimental demonstration of twin-field type quantum key distribution. Phys Rev Lett 123:100506
14. Fang X-T, Zeng P, Liu H, Zou M, Wu W, Tang Y-L, Sheng Y-J, Xiang Y, Zhang W, Li H et al (2020) Implementation of quantum key distribution surpassing the linear rate-transmittance bound. Nat Photonics 14(7):422–425
15. Chen J-P, Zhang C, Liu Y, Jiang C, Zhang W, Hu X-L, Guan J-Y, Yu Z-W, Xu H, Lin J et al (2020) Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km. Phys Rev Lett 124(7):070501
16. Liu H, Jiang C, Zhu H-T, Zou M, Yu Z-W, Hu X-L, Xu H, Ma S, Han Z, Chen J-P et al (2021) Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km. Phys Rev Lett 126(25):250502
17. Chen J-P, Zhang C, Liu Y, Jiang C, Zhang W-J, Han Z-Y, Ma S-Z, Hu X-L, Li Y-H, Liu H et al (2021) Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. Nat Photonics 15:570
18. Chen J-P, Zhang C, Liu Y, Jiang C, Zhao D-F, Zhang W-J, Chen F-X, Li H, You L-X, Wang Z, Chen Y, Wang X-B, Zhang Q, Pan J-W (2022) Quantum key distribution over 658 km fiber with distributed vibration sensing. Phys Rev Lett 128:180502
19. Pittaluga M, Minder M, Lucamarini M, Sanzaro M, Woodward RI, Li M-J, Yuan Z, Shields AJ (2021) 600 km repeater-like quantum communications with dual-band stabilisation. Nat Photonics 15:530
20. Wang S, Yin Z-Q, He D-Y, Chen W, Wang R-Q, Ye P, Zhou Y, Fan-Yuan G-J, Wang F-X, Chen W, Zhu Y-G, Morozov PV, Divochiy AV, Zhou Z, Guo G-C, Han Z-F (2022) Twin-field quantum key distribution over 830-km fibre. Nat Photonics 16(2):154
21. Liu Y, Zhang W-J, Jiang C, Chen J-P, Zhang C, Pan W-X, Ma D, Dong H, Xiong J-M, Zhang C-J et al (2023) Experimental twin-field quantum key distribution over 1000 km fiber distance. Phys Rev Lett 130(21):210801
22. Wang X-B, Yu Z-W, Hu X-L (2018) Twin-field quantum key distribution with large misalignment error. Phys Rev A 98(6):062323
23. Hu X-L, Jiang C, Yu Z-W, Wang X-B (2022) Universal approach to sending-or-not-sending twin field quantum key distribution. Quantum Sci Technol 7(4):045031
24. Xu H, Yu Z-W, Jiang C, Hu X-L, Wang X-B (2020) Sending-or-not-sending twin-field quantum key distribution: breaking the direct transmission key rate. Phys Rev A 101:042330
25. Jiang C, Hu X-L, Xu H, Yu Z-W, Wang X-B (2020) Zigzag approach to higher key rate of sending-or-not-sending twin field quantum key distribution with finite-key effects. New J Phys 22(5):053048
26. Jiang C, Hu X-L, Yu Z-W, Wang X-B (2021) Composable security for practical quantum key distribution with two way classical communication. New J Phys 23(6):063038
27. Vitanov A, Dupuis F, Tomamichel M, Renner R (2013) Chain rules for smooth min-and max-entropies. IEEE Trans Inf Theory 59(5):2603–2612
28. Pound RV (1946) Electronic frequency stabilization of microwave oscillators. Rev Sci Instrum 17(11):490–505
29. Drever R, Hall JL, Kowalski F, Hough J, Ford G, Munley A, Ward H (1983) Laser phase and frequency stabilization using an optical resonator. Appl Phys B 31(2):97–105
30. Clivati C, Meda A, Donadello S, Virzì S, Genovese M, Levi F, Mura A, Pittaluga M, Yuan Z, Shields AJ et al (2022) Coherent phase transfer for real-world twin-field quantum key distribution. Nat Commun 13(1):157

31. Zhang W, Yang X, Li H, You L, Lv C, Zhang L, Zhang C, Liu X, Wang Z, Xie X (2018) Fiber-coupled superconducting nanowire single-photon detectors integrated with a bandpass filter on the fiber end-face. Supercond Sci Technol 31(3):035012
32. Zhang W, You L, Li H, Huang J, Lv C, Zhang L, Liu X, Wu J, Wang Z, Xie X (2017) Nbn superconducting nanowire single photon detector with efficiency over 90% at 1550 nm wavelength operational at compact cryocooler temperature. Sci China, Phys Mech Astron 60(12):120314
33. Jiang C, Yu Z-W, Hu X-L, Wang X-B (2019) Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses. Phys Rev Appl 12(2):024061
34. Pirandola S, Laurenza R, Ottaviani C, Banchi L (2017) Fundamental limits of repeaterless quantum communications. Nat Commun 8:15043
35. Paraiso TK, Roger T, Marangon DG, De Marco I, Sanzaro M, Woodward RI, Dynes JF, Yuan Z, Shields AJ (2021) A photonic integrated quantum secure communication system. Nat Photonics 15(11):850–856
36. Zhu C-X, Chen Z-Y, Li Y, Wang X-Z, Wang C-Z, Zhu Y-L, Liang F-T, Cai W-Q, Jin G, Liao S-K et al (2022) Experimental quantum key distribution with integrated silicon photonics and electronics. Phys Rev Appl 17(6):064034
37. Wei K, Li W, Tan H, Li Y, Min H, Zhang W-J, Li H, You L, Wang Z, Jiang X et al (2020) High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. Phys Rev X 10(3):031030
38. Cao L, Luo W, Wang Y, Zou J, Yan R, Cai H, Zhang Y, Hu X, Jiang C, Fan W et al (2020) Chip-based measurement-device-independent quantum key distribution using integrated silicon photonic systems. Phys Rev Appl 14(1):011001

Publisher's Note

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

Submit your manuscript to a SpringerOpen journal and benefit from:

- ► Convenient online submission
- ► Rigorous peer review
- ► Open access: articles freely available online
- ► High visibility within the field
- ► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com