APPLIED PHYSICS

Simultaneous transmission of information and key exchange using the same photonic quantum states

Dong Pan[1]†, Yu-Chen Liu[1,2]†, Penghao Niu[1], Haoran Zhang[1], Feihao Zhang[1], Min Wang[1], Xiao-Tian Song[1], Xiuwei Chen[1], Chao Zheng[3], Gui-Lu Long[1,2,4,5]*

Quantum communication realizes information-theoretic security using photonic quantum states, for example, quantum secure direct communication (QSDC), which can achieve secure and reliable communication in a channel with both noise and eavesdroppers. However, QSDC suffers from large losses and short communication distances, thus being impractical for applications. Here, we have proposed a one-way quasi-QSDC protocol with single photons. This protocol enables the simultaneous transmission of information and key exchange using the same single photons and is robust against loss and error because it uses error correction and spectrum expansion techniques. In a proof-of-principle demonstration using weak coherent pulses, the system achieved a real-time secure transmission rate of 2.38 kilobits per second over a 104.8-kilometer standard telecommunication fiber, which set world records in both aspects. This system paved the way for the practical application of QSDC and offers a unique method to detect eavesdropping online, which is crucial in certain circumstances.

INTRODUCTION

Secure transmission of private data is becoming increasingly important. The rapid development of quantum computing poses an urgent threat to widely used cryptography methods such as the Rivest-Shamir-Adleman algorithm. Quantum communication (*1*–*4*), which is based on the principles of quantum mechanics, is a promising solution to this issue. There are two well-known branches of quantum communication: quantum key distribution (QKD), which realizes secure key exchange between two distant users (*1*), and quantum secure direct communication (QSDC) (*2*–*4*), which directly transmits information between two remote parties without first establishing a key. QSDC provides reliable and secure communication of information over a channel with both noise and eavesdropping and prevents an eavesdropper from obtaining useful information to decipher. QSDC is also compatible with the existing networks because it is a communication protocol. Because of its inherent low-intensity laser communication, QSDC supports covert transmission, does not require frequency licensing, and eliminates radio frequency interference. These features make QSDC a unique choice in certain applications.

In recent years, QSDC has rapidly developed. Experimental demonstrations of QSDC showed its great potential in future applications (*5*–*9*). Using Wyner's wiretap channel theory (*10*), QSDC was proven to be information-theoretically secure (*8*, *11*, *12*). Quantum data locking (*13*), quantum low probability of intercept (*14*), quantum keyless private communication (*15*), and realistic noisy entanglement-based (*16*) schemes have been used to design QSDC protocols. Measurement device–independent QSDC and device-independent protocols were recently proposed to eliminate security loopholes that are related to detectors (*17*) or all devices in QSDC systems (*18*). A prototype network using entanglement-based QSDC was demonstrated (*19*). A secure classical repeater quantum network scheme was proposed and demonstrated, in which ciphertexts of classical postquantum cryptography were transmitted using QSDC in a hop-by-hop manner (*4*). Such cryptography-assisted QSDC can also guard QSDC against potential loopholes that may arise in the late stages of the engineering process (*20*). Quantum memory–free QSDC protocols were proposed to mitigate the demand for quantum memory (*9*, *21*).

In the single-photon DL04 QSDC protocol, photons must travel back and forth between the users (*3*), which results in large losses, limits the distance of communication, and severely hinders its application. With this background, we propose a one-way single-photon practical quasi-QSDC protocol. This protocol realizes the simultaneous transmission of information and key exchange (STIKE) based on the repeatable classical one-time-pad (RECON) protocol (*22*–*25*), which was independently invented by several groups (*22*–*25*). Bennett *et al.* (*24*) developed the RECON protocol before they proposed QKD and published it in print 30 years later. RECON is considered a quasi-QSDC protocol (*20*) because it retains the transmission of information in quantum states, but it still uses a preshared key and classical one-time-pad encryption for security. In ideal conditions with no loss and no noise, the shared key can be fully replenished. However, in practice, key consumption is greater than key generation, and new keys must be added, e.g., by running the protocol as a QKD.

We designed and set up a prototype to demonstrate this principle. In the experiment, weak coherent pulses with a 1.25-GHz trigger frequency were used with the decoy-state technique. Accordingly, we achieved a real-time secure transmission rate of 2.38 kilobits per second (kbps) over a distance exceeding 100 km in a standard telecommunication fiber, which is suitable for the transmission of text, image files, and voice.

RESULTS

STIKE protocol

Figure 1 illustrates the STIKE protocol. It contains three parts: preprocessing (steps 1 to 3), prepare-and-measure (steps 4 to 6), and

[1]Beijing Academy of Quantum Information Sciences, Beijing, 100193, China. [2]State Key Laboratory of Low-dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing, 100084, China. [3]School of Energy Storage Science and Engineering, North China University of Technology, Beijing, 100144, China. [4]Frontier Science Center for Quantum Information, Beijing, 100084, China. [5]Beijing National Research Center for Information Science and Technology, Beijing, 100084, China.
*Corresponding author. Email: gllong@tsinghua.edu.cn
†These authors contributed equally to this work.

postprocessing (steps 7 to 12). Per common practice, the legitimate transmitter and receiver are named Alice and Bob, respectively. The 12 steps in the STIKE protocol are as follows.

Step 1. Alice encodes the information **m** using forward error correction (FEC) coding to obtain the codeword $\mathbf{m}_1$. The FEC includes an error correction code (ECC) encoder that overcomes errors and a spreading spectrum that handles loss.

Step 2. Alice collects a shared secure key sequence **s** with an identical length to codeword $\mathbf{m}_1$ from her secure key sink (SKS) to encrypt codeword $\mathbf{m}_1$ using an exclusive-or operation, i.e., $\mathbf{c} = \mathbf{s} \oplus \mathbf{m}_1$. This exclusive-or operation is a one-time-pad encryption. Hence, **c** is called a ciphered codeword.

Step 3. Alice uses the technique "increasing capacity using masking" (INCUM) (*26*) to mask ciphertext codeword **c**. Specifically, she uses a local random number sequence **r** with an identical length to **c** to perform the operation $\mathbf{c}_1 = \mathbf{r} \oplus \mathbf{c}$, where $\mathbf{c}_1$ is called the masked codeword.

Step 4. The masked codeword $\mathbf{c}_1$ is divided into frames as performed in classical communication, and each frame is mapped onto quantum states. Specifically, Alice randomly selects a Z or X basis to prepare the state according to the information bit in a frame. For example, states $|0\rangle$ and $|+\rangle$ carry bit 0, whereas bit 1 is mapped onto state $|1\rangle$ or $|-\rangle$. Then, she transmits the photons to Bob frame by frame. A frame is a fundamental unit of data and is used as a structure to organise, encapsulate, and transmit information. It can be customised according to specific needs.

Step 5. Bob randomly selects the Z or X basis to measure each received quantum state from Alice. Because of loss, only a fraction of the photons can be detected by Bob. Bob records the timestamps, selected basis, and measured results of the detected events. Some events are not triggered because there is a loss in transmission or the finite-efficiency detectors miss them; then, these untriggered events are treated as lost photons.

Step 6. Bob publicly announces the timestamps and basis choices of the triggered events. Alice and Bob compare their basis choices for each triggered event and maintain events in which they have selected the same basis. Next, they randomly publish some of these measured results for comparison and calculate the quantum bit error rate (QBER). If the QBER is below a predetermined threshold, they proceed to the next step; otherwise, they abort the process. Subsequently, in the case of a triggered event, if Bob and Alice select different bases, it is considered an untriggered event.

Step 7. According to the announced timestamps of the triggered events, Alice announces the corresponding local random number $\mathbf{r}_1$ for the INCUM in step (3).

Step 8. Alice and Bob share a common sequence of ciphered codewords of the triggered events. The measured results of Bob are not identical to those prepared by Alice due to channel noise and possible eavesdropping. The retained ciphered codeword of Alice is $\mathbf{c}_2$, and $\mathbf{c}_2'$ is the corresponding data held by Bob. Bob makes a copy of $\mathbf{c}_2'$ to obtain two sets of raw data.

Steps 9 and 10 read out the message.

Step 9. After receiving $\mathbf{r}_1$, Bob obtains the noisy ciphertext $\mathbf{c}'$ of the codeword by unmasking, i.e., $\mathbf{c}' = \mathbf{c}_2' \oplus \mathbf{r}_1$. Because of channel loss, noise, and Bob's random choices of a basis, the received codeword $\mathbf{c}'$ is only a fraction of **c** and contains bit errors.

Step 10. Bob takes the secure key sequence from his SKS. According to the announced timestamps of the triggered events, the corresponding secure key sequence $\mathbf{s}_1$ of the triggered events is extracted from the SKS to decrypt $\mathbf{c}'$ via $\mathbf{m}_1' = \mathbf{s}_1 \oplus \mathbf{c}'$. $\mathbf{m}_1'$ is a partial sequence of $\mathbf{m}_1$ and has bit errors. However, because the FEC is capable of error correction and loss resistance, Bob can decode $\mathbf{m}_1'$ to obtain the secret message **m** as long as the QBER is below the predetermined threshold.

Step 11. Alice returns the secure key sequence at timestamps that correspond to the untriggered events to the SKS. These secure keys are masked by the local random numbers, which are only known to Alice and Bob and will never be revealed to any other parties. Thus, they can be reused. As Fig. 1 shows, **s** is the secure key sequence for information encryption, and $\mathbf{s}_1$ is the secure key bits on the photon that corresponds to the triggered events. The secure key sequence for the untriggered events, which is $\mathbf{s} - \mathbf{s}_1$, is obtained by sequentially removing all key bits in $\mathbf{s}_1$ from **s** according to the timestamps and subsequently returning the remaining bits as a new key sequence to the SKS.

Step 12. For another copy of the raw data, Alice and Bob perform the error correction and privacy amplification in the same manner as in the standard QKD to obtain a secure key sequence $\mathbf{s}_n$ to replenish their respective SKSs.

In step 5, Bob randomly selects the Z or X basis to measure the received quantum states. Compared with Alice's preparation basis,

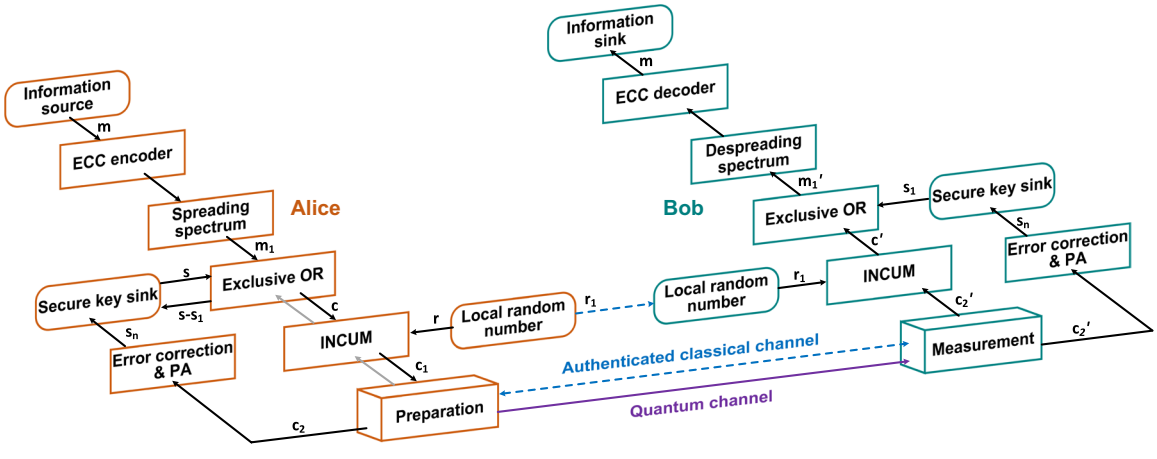

Fig. 1. Schematic of one-way quasi-QSDC. ECC, error correction code; INCUM, increase capacity using masking; PA, privacy amplification.

Bob has a 50% probability of selecting the wrong basis for measurement. The results from incorrect basis selections are discarded as outlined in step 6. The results from correct selections are retained for information recovery. Consequently, Bob's random choice of the Z or X basis for measurement introduces an attenuation of approximately 3 dB. This additional loss and the channel loss are tolerable in our protocol due to the cascade of ECC and spreading spectrum.

STIKE differs from the quantum key recycling protocols (*22*–*25*) in the following manners: (i) the spreading spectrum technique is used to overcome the loss; (ii) the INCUM technique is used to increase the capacity and reduce the consumption of shared keys; (iii) the basis is not synchronised; (iv) the decoy-state method can be incorporated into the prepare-and-measure phase of the STIKE protocol, which enables the use of weak coherent pulses instead of ideal single photons.

The information transmission is secured by the one-time pad of the shared secure key sequence. The loss of the quantum channel is very high, e.g., 20 dB in a standard optical fiber over 100 km. These untriggered events are also encrypted by the secure key sequence and cause a huge consumption of secure keys in the SKS. By masking the transmitted bits, the INCUM technique limits Eve's ability to obtain information or encryption keys from lost photons, which reduces the burden of key consumption, as described in step 11. For the triggered event, step 12 distills new keys and adds them to the SKS. These two steps greatly alleviate the secure key consumption. The masked codeword that Alice emits is entirely random due to the masking by locally generated random numbers. This condition severs all potential correlations between bits in an information frame or across different frames, which enhances the security of information transmission and generation of fresh keys from the transmitted codeword.

The proposed protocol is universal for both fiber and free-space transmission. However, in free-space communication scenarios, FEC coding can be optimized on the basis of the particular channel characteristics. As a communication protocol, this quasi-QSDC protocol is compatible with the existing network and can cooperate with various applications for enhanced security (*4*). When this protocol is incorporated into the existing network, it is only necessary to add communication terminals that run this protocol at the link ends, where optical-fiber amplifiers are not present. This protocol can also be implemented using quantum states on the future quantum internet.

Performance analysis of STIKE

According to Wyner's wiretap channel theory (*8*, *10*–*12*), the secure channel capacity of STIKE is

$$C_s = C_m - C_w \tag{1}$$

where C_m and C_w are the channel capacities of the main and wiretap channels, respectively. C_s is given by

$$C_s = 1 - H_2(\delta_p) - H_2(\delta_b) \tag{2}$$

where δ_p and δ_b are the phase error rate and bit error rate, respectively. Equation 2 is exactly the key rate of the BB84 QKD protocol. C_s is greater than zero if QBER is below the threshold value of 11%. In this case, one is assured that there exist classical codes that can realize the secure and reliable communication of information at a rate no greater than the secure channel capacity.

To distill a secure key from the ciphertext, let us observe the following facts. The key exchange, which includes the prepare-and-measure steps and step 12, is identical to the standard BB84 QKD process. Ciphered codewords **c** are simply random numbers to all entities except Alice and Bob. Therefore, the key exchange is a BB84 QKD process. Hence, we can distill a secure key from the received ciphertext **c′** at the maximum rate in Eq. 2.

Combined with the decoy-state method (*27*–*29*), the secrecy capacity of STIKE with one signal and two decoy intensities is bounded by (*28*).

$$C_s = qQ_\mu\{-fH_2(E_\mu) + \Delta_1[1 - H_2(e_1)]\} \tag{3}$$

where $q = 1/2$ with the BB84 prepare-and-measure processing (*1*); Q_μ is the overall gain of the signal states; μ is the mean photon number of the signal state; f is the error correction efficiency; E_μ is the overall QBER; $\Delta_1 = Q_1/Q_\mu$ is the ratio of the single-photon gain to the overall gain; e_1 is the error rate caused by single photons (see the Supplementary Materials for more details).

The security of information in STIKE is guaranteed by the one-time pad in step 2. Therefore, the communication capacity can be larger than the secure channel capacity as long as it can reliably transmit information, i.e.

$$C_r = C_m = qQ_\mu[1 - fH_2(E_\mu)] \tag{4}$$

where C_m is the channel capacity of the main channel. According to Shannon's theory, as long as C_r is greater than zero, one can always find an FEC scheme for reliable transmission.

Our secrecy capacity was derived in an asymptotic scenario, where we assumed that the number of transmitted qubits approached infinity. However, we must consider the finite length of coding for practical implementation, which implies that the number of transmitted qubits is finite. In this case, the secrecy capacity and maximum secure transmission distance will decrease. Further investigation is required to calculate the completeness, reliability, and secrecy parameters considering the finite-length effects based on the wiretap channel theory (*12*). This calculation is necessary to derive the practical secrecy capacity.

Experimental results

Figure 2 shows the information transmission rate and QBER of this system during a testing period of 168 hours (1 week) to transmit image files over a distance of 104.8 km. The average information transmission rate and the average QBER were 2.38 kbp and 3.60%, respectively. We also tested the communication performance at 50.3 and 81.1 km. During a 1-hour transmission, the average information transmission rate and average QBER were 34.08 kbp and 2.94% at 50.3 km and changed to 11.36 kbp and 3.20% at 81.1 km, respectively. Our system enables real-time functionality, so all results represent real-time communication rates.

Figure 3 shows the communication performances of the STIKE protocol, indicating that it could maintain a highly reliable communication rate over long distances. The secrecy capacities of our experimental system at communication distances of 81.1 and 104.8 km exceeded the acievable upper limit of a two-way QSDC (*9*). Compared with previous experimental results of two-way QSDC (*9*), the secrecy capacity of this experimental system increased by three orders of magnitude at a communication distance of approximately

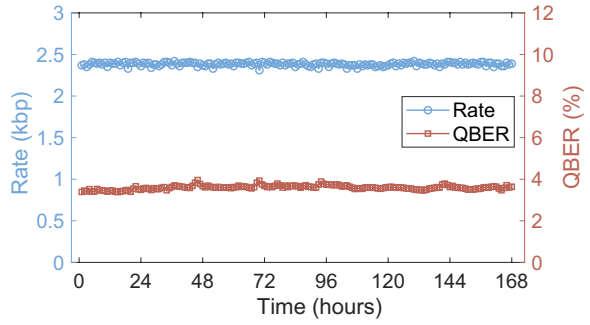

Fig. 2. Information transmission rate and QBER versus time at a transmission distance of 104.8 km during 1 week of data collection. Each point represents the average value over 1 hour of data.

80 km. With our experimental device parameters, the distance of communication can exceed 150 km, which will be interesting to verify in future experiments.

DISCUSSION

We proposed the STIKE protocol using single photons and extended it to weak coherent lasers using a decoy-state technique. Notably, we experimentally demonstrated the protocol with a system that operated at a repetition rate of 1.25 GHz over a communication distance of 104.8 km in a standard telecommunication fiber. This protocol paves the way for practical long-distance quasi-QSDC, which is crucial for building a space-air-ground-sea integrated secure communication network using quantum states.

The proposed STIKE one-way quasi-QSDC is different from QKD. In the ideal case with no errors and no loss, the rates of consumption and generation of the secure keys are identical to each other as if a preshared key can be perpetually reused. In practice, key consumption is commonly greater than key generation. It requires additional key negotiation to compensate for the reduction of keys in the SKS. The STIKE system has different modes of operation. In one extreme, STIKE can only be used to perform key exchange, where Alice sends random numbers without encrypting them with the shared keys, which we call the full key exchange (FKE) mode. In the other extreme, STIKE can only be used to realize communications, where it consumes the secure key in the SKS and does not distill new keys. In this case, STIKE aims to reliably transmit information, so the QBER can be larger than the predetermined threshold, which is commonly 11%. We call this case the full-communication (FC) mode. The FC mode is useful when there is eavesdropping in the channel, but the communication task is too urgent to wait for the eavesdroppers to clear. The FC mode will stop once the keys in the SKS have been exhausted.

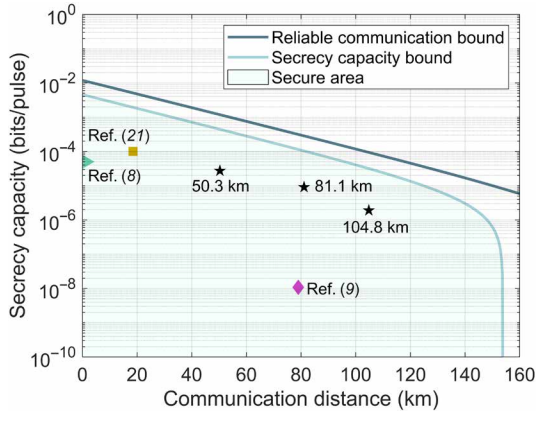

Fig. 3. Simulation (lines) and experimental (symbols) results of the secrecy capacity. The pentagram symbols represent the experimental results of this system at different communication distances.

The issure of greater key consumption than key generation can be addressed using the sustained mode. When a frame of bits is generated for transmission, a fixed length in the frame is designated as a masked codeword, whereas a specific length is entirely allocated for the quantum key exchange using random numbers. This approach reduces the communication bandwidth while dedicating a portion of the bandwidth for the quantum key exchange to balance between key consumption and generation. Normally, one can run STIKE with a predetermined QBER to simultaneously transmit information and distill new keys, which we call the standard mode. In the standard mode, because of channel loss and noise, fewer keys are replenished than consumed. Therefore, when the number of keys in the SKS reaches an alarming level, the users can change STIKE to the FKE mode to add keys to the SKS. When the STIKE system is not in use for communication, it can work in the FKE mode to negotiate keys and fill the SKS. A detailed strategy for real applications is an interesting subject of future study.

Under current technological conditions, the integration of this communication capability into classical networks for practical applications is worth exploring, particularly when a small quantity of highly sensitive information in is transmitted, e.g., in national security protection and financial information safeguarding. Outlining a feasible roadmap to enhance the performance under current conditions can involve focusing on higher-performance devices and optimizing the codes. Such high-performance devices may include high–repetition rate light sources and high-efficiency single-photon detectors. Accordingly, constructing more efficient error-correction codes and optimizing the spreading ratio to adapt to channel losses will improve the communication performance. These improvements will address the existing limitations and broaden potential applications. With the enhanced point-to-point system performance, this approach can be extended to free-space communication and multiuser network scenarios.

METHODS

We completed a proof-of-principle demonstration experiment to demonstrate the feasibility of the proposed protocol. We constructed a Faraday-Michelson system (*30*), as shown in Fig. 4. This phase encoding infrastructure realized the prepare-and-measure process in Fig. 1 and avoided the influence of birefringence in the transmission path on phase modulation, dispensed the need for an additional polarisation calibration module, and achieved highly stable interference. Signal pulses at a 1550-nm wavelength were prepared at Alice's site with a repetition rate of 1.25 GHz and a pulse width of 50 ps. The delay of the Faraday-Michelson interferometer was 400 ps. The system used two decoy-state intensities with the mean photon number of the signal state $\mu = 0.6$, decoy state $\nu_1 = 0.2$, and decoy state $\nu_2 = 0$ (the vacuum). A laser was followed by an intensity modulator, which

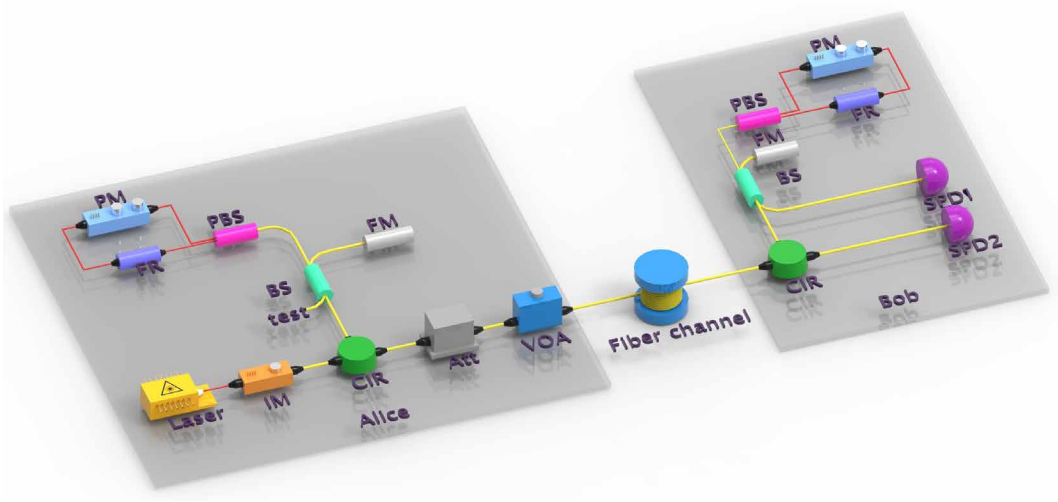

Fig. 4. Schematic of our experimental setup. IM, intensity modulator; CIR, circulator; BS, beam splitter; FM, Faraday mirror; PBS, polarisation beam splitter; FR, Faraday rotator; PM, phase modulator; Att, attenuator; VOA, variable optical attenuator; SPD, single-photon detector.

modulated the pulses into two different intensities and served as the signal states and decoy states. The vacuum state was prepared by not triggering the laser. Then, the modulated laser pulses were attenuated by a fixed attenuator and a variable optical attenuator to the desired mean photon number levels. The fiber channel distance between Alice and Bob was 104.8 km when a standard telecommunication fiber that exhibited a loss of 0.2 dB/km was used. Bob recorded the received photons using two InGaAs/InP single-photon detectors, which had a detection efficiency of 20% and a dark count rate of 1.2×10^{-6}. There was an optical loss of 6.5 dB at Bob's end due to the loss in the optical devices.

We used a low-density parity check (LDPC) code based on (*21*) and a generous spreading ratio of 1:3840 for the communication distance of 104.8 km to combat the effect of channel loss. The spreading ratios for communication distances of 81.1 and 50.3 km were set to 1:768 and 1:192, respectively. The spread-spectrum ratio is correlated with the channel loss, where a higher channel loss necessitates a larger spread-spectrum multiple. To achieve stable and reliable communication over extended periods, we determined relatively generous spread-spectrum ratios for the aforementioned distances in our experiments. Consequently, there is potential for further optimization. The system implements communication using frame-by-frame transmission. Each frame consists of 125 bytes: 1 byte for the frame type, 3 bytes for the total frame count, 3 bytes for the current frame number, 1 byte for the current frame length, and the remaining 117 bytes reserved for the masked codeword $\mathbf{c}_1$ to be transmitted.

A rate-adaptive LDPC code based on the progressive edge growth method was used for error correction (*31*) to negotiate a secure key sequence. Privacy amplification was achieved using a universal class of hash functions with an optimised multiplication algorithm, which enabled the length adaptability and accelerates processing (*32*). The error correction efficiency f was 1.05.

Supplementary Materials

This PDF file includes:

Supplementary Text
Table S1
References

REFERENCES AND NOTES

1. C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, paper presented at the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984.
2. G.-L. Long, X.-S. Liu, Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **65**, 032302 (2002).
3. F.-G. Deng, G. L. Long, Secure direct communication with a quantum one-time pad. *Phys. Rev. A* **69**, 052319 (2004).
4. G.-L. Long, D. Pan, Y.-B. Sheng, Q. Xue, J. Lu, L. Hanzo, An evolutionary pathway for the quantum internet relying on secure classical repeaters. *IEEE Netw.* **36**, 82–88 (2022).
5. J.-Y. Hu, B. Yu, M.-Y. Jing, L.-T. Xiao, S.-T. Jia, G.-Q. Qin, G.-L. Long, Experimental quantum secure direct communication with single photons. *Light Sci. Appl.* **5**, e16144 (2016).
6. W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, G.-C. Guo, Quantum secure direct communication with quantum memory. *Phys. Rev. Lett.* **118**, 220501 (2017).
7. F. Zhu, W. Zhang, Y. Sheng, Y. Huang, Experimental long-distance quantum secure direct communication. *Sci. Bull.* **62**, 1519–1524 (2017).
8. R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, G.-L. Long, Implementation and security analysis of practical quantum secure direct communication. *Light Sci. Appl.* **8**, 22 (2019).
9. H. Zhang, Z. Sun, R. Qi, L. Yin, G.-L. Long, J. Lu, Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. *Light Sci. Appl.* **11**, 83 (2022).
10. A. D. Wyner, The wire-tap channel. *Bell Syst. Tech. J.* **54**, 1355–1387 (1975).
11. J. Wu, Z. Lin, L. Yin, G.-L. Long, Security of quantum secure direct communication based on Wyner's wiretap channel theory. *Quantum Eng.* **1**, e26 (2019).
12. J. Wu, G.-L. Long, M. Hayashi, Quantum secure direct communication with private dense coding using a general preshared quantum state. *Phys. Rev. Appl.* **17**, 064011 (2022).
13. D. J. Lum, J. C. Howell, M. Allman, T. Gerrits, V. B. Verma, S. W. Nam, C. Lupo, S. Lloyd, Quantum enigma machine: Experimentally demonstrating quantum data locking. *Phys. Rev. A* **94**, 022315 (2016).
14. J. H. Shapiro, D. M. Boroson, P. B. Dixon, M. E. Grein, S. A. Hamilton, Quantum low probability of intercept. *J. Opt. Soc. Am. B* **36**, B41–B50 (2019).
15. A. Vázquez-Castro, D. Rusca, H. Zbinden, Quantum keyless private communication versus quantum key distribution for space links. *Phys. Rev. Appl.* **16**, 014006 (2021).
16. D. Chandra, A. S. Cacciapuoti, M. Caleffi, L. Hanzo, Direct quantum communications in the presence of realistic noisy entanglement. *IEEE Trans. Commun.* **70**, 469–484 (2021).
17. Z. Zhou, Y. Sheng, P. Niu, L. Yin, G. Long, L. Hanzo, Measurement-device-independent quantum secure direct communication. *Sci. China Phys. Mech.* **63**, 230362 (2020).
18. L. Zhou, Y.-B. Sheng, G.-L. Long, Device-independent quantum secure direct communication against collective attacks. *Sci. Bull.* **65**, 12–20 (2020).
19. Z. Qi, Y. Li, Y. Huang, J. Feng, Y. Zheng, X. Chen, A 15-user quantum secure direct communication network. *Light Sci. Appl.* **10**, 183 (2021).
20. D. Pan, X.-T. Song, G.-L. Long, Free-space quantum secure direct communication: Basics, progress, and outlook. *Adv. Devices Instrum.* **4**, 0004 (2023).

21. Z. Sun, L. Song, Q. Huang, L. Yin, G. Long, J. Lu, L. Hanzo, Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design. *IEEE Trans. Commun.* **68**, 5778–5792 (2020).
22. F.-G. Deng, G. L. Long, Repeatable classical one-time-pad crypto-system with quantum mechanics. arXiv:1902.04218 [quant-ph] (2019).
23. K. Wen, F. G. Deng, G. L. Long, Secure reusable base-string in quantum key distribution. arXiv:0706.3791 [quant-ph] (2007).
24. C. H. Bennett, G. Brassard, S. Breidbart, Quantum cryptography II: How to re-use a one-time pad safely even if P= NP. *Nat. Comput.* **13**, 453–458 (2014).
25. D. Leermakers, B. Škorić, Quantum Alice and silent Bob: Qubit-based quantum key recycling with almost no classical communication. *Quantum Inf. Comput.* **21**, 1–18 (2021).
26. G.-L. Long, H. Zhang, Drastic increase of channel capacity in quantum secure direct communication using masking. *Sci. Bull.* **66**, 1267–1269 (2021).
27. W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
28. H.-K. Lo, X. Ma, K. Chen, Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
29. X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
30. X.-F. Mo, B. Zhu, Z.-F. Han, Y.-Z. Gui, G.-C. Guo, Faraday–Michelson system for quantum cryptography. *Opt. Lett.* **30**, 2632–2634 (2005).
31. M. Li, C.-M. Zhang, Z.-Q. Yin, W. Chen, C. Wang, Z.-F. Han, Simple rate-adaptive LDPC coding for quantum key distribution. arXiv:1505.06423 [quant-ph] (2015).
32. C.-M. Zhang, M. Li, J.-Z. Huang, P. Treeviriyanupab, H.-W. Li, F.-Y. Li, C. Wang, Z.-Q. Yin, W. Chen, K. Sripimanwat, Z.-F. Han, Fast implementation of length-adaptive privacy amplification in quantum key distribution. *Chin. Phys. B* **23**, 090310 (2014).
33. X. Ma, B. Qi, Y. Zhao, H.-K. Lo, Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).

Acknowledgments: We thank LetPub for its linguistic assistance during the preparation of this manuscript. **Funding:** D.P. was funded by the National Natural Science Foundation of China grant 12205011, G.-L.L. was funded by the National Natural Science Foundation of China grant 62471046, D.P. and G.-L. L. were funded by the Open Research Fund Program of the State Key Laboratory of Low-Dimensional Quantum Physics grant KF202205, and M.W. was funded by the Young Elite Scientists Sponsorship Program by CAST grant 2022QNRC001. All authors were funded by the Beijing Advanced Innovation Center for Future Chip (ICFC). **Author contributions:** G.-L.L. devised the research and conceived the theoretical protocol. D.P., Y.-C.L., P.N., H.Z., F.Z., M.W., X.C., and C.Z. participated in the refinement of the protocol design. D.P., P.N., X.-T.S., and G.-L.L. constructed the experimental system. D.P. completed the experimental tests and analyzed the data. D.P. and G.-L.L. completed the simulation. All authors discussed the experimental and simulation results. G.-L.L. and D.P. wrote the paper with contributions from all authors. G.-L.L. supervised the entire project. **Competing interests:** G.-L.L., D.P., P.N., H.Z., F.Z, M.W., C.Z., and X.C. are inventors on a US patent related to this work (the current patent status is pending; the applicant is Beijing Academy of Quantum Information Sciences, the application date is 24 March 2023, and the patent publication number is US 2024/0322914 A1). The authors declare that they have no other competing interests. **Data and materials availability:** All data needed to evaluate the conclusions in the paper are present in the paper and/or the Supplementary Materials. The data and code used to generate the figures in this manuscript have been deposited in the Dryad database at https://doi.org/10.5061/dryad.n2z34tn70 LWVGJ8lEDps6RGNs6jX6Q-yWyQ2SKt7h3Sevgh3v8Rs.

Submitted 26 September 2024
Accepted 22 January 2025
Published 21 February 2025
10.1126/sciadv.adt4627