Hindawi
Quantum Engineering
Volume 2024, Article ID 1494088, 7 pages
https://doi.org/10.1155/2024/1494088

Research Article

Quantum Enhanced Hazardous Substances Surveillance System

Peng-Hao Niu,[1] **Jian-Xing Guo**,[1] **Rui-Song Bao**,[2] **Chun-Sheng Zhang**,[1] **Wei Zhang**,[1] **and Xiu-Wei Chen**[1]

[1]*Beijing Academy of Quantum Information Sciences, Beijing, China*
[2]*Beijing National Research Center for Information Science and Technology, Beijing, China*

Correspondence should be addressed to Peng-Hao Niu; nph15@tsinghua.org.cn

Received 26 October 2023; Revised 18 December 2023; Accepted 3 January 2024; Published 8 January 2024

Academic Editor: Shi Hai Dong

Unauthorized access to hazardous substances poses a serious threat to public health. Typically, these substances, such as chemicals, are housed within warehouses or laboratory facilities, making strict control over any unauthorized entry. The control can be achieved through various measures, including access control systems, registration systems, remote inspection and surveillance, and personnel checks. Given its essential significance, the security of surveillance system data transmission plays a critical role. On the one hand, authorized entities must be capable of detecting any malicious data interception, and on the other hand, confidential information must remain safeguarded when an eavesdropper is identified. To address transmission security, we have developed a quantum-communication-based system for transmitting surveillance imagery of the hazardous chemical storage area entrance. This system effectively thwarts eavesdropping and data tampering during transmission, thereby enhancing the security of conventional monitoring systems.

1. Introduction

Scientific research and manufacturing processes frequently involve the utilization of diverse chemical agents, including explosives, inflammable substances, oxidizing agents, corrosive materials, and toxic compounds. These substances inherently pose significant hazards, necessitating stringent oversight. Typically, hazardous chemicals are securely stored in dedicated chambers, access to which is rigorously controlled.

One effective method to ensure such control is by deploying a surveillance system employing cameras and monitors to continuously oversee the entrance and exit of the chemical storage facility. Nevertheless, it is imperative to acknowledge the potential vulnerability of this system. An unauthorized individual may manipulate the transmission data between the camera and the monitoring screen, employing methodologies such as a man-in-the-middle attack, thereby falsifying the surveillance system's monitoring imagery [1]. Cryptography can potentially resolve this concern by employing data encryption to prevent tampering. However, classical cryptography relies on computational complexity. With the development of quantum computing, including the Shor algorithm and the hybrid-quantum-classical factoring algorithm [2, 3], asymmetric cryptography is under existential threat. One effective approach to address this threat is to adopt quantum communication [4–6], whose security derives from quantum principles.

Quantum secure direct communication (QSDC) is a kind of quantum communication that can transmit confidential information through the quantum channel directly. Utilizing this characteristic, employing a QSDC protocol for secure transmission of monitoring data appears to be a favorable choice.

The first QSDC protocol was proposed in 2000 [6, 7], and it has been developing fast in both theory [8–11] and experiments [12–14]. The first proof-of-principle prototype QSDC system experiment was achieved in 2019 [15], and then, a QSDC experiment over 100 km with time-bin and phase coding was achieved in 2022 [16]. Besides the fiber channel, QSDC based on free space was also completed in

2020 [17]. With the development of QSDC, many technologies are proposed to improve performance, such as quantum-memory-free (QMF) [18–20], high-loss channel coding [15, 18, 19], and INCUM coding [21]. In addition to the above achievements, safety issues stemming from device defects have also been studied, such as measurement-device-independent (MDI) QSDC [22–24] and device-independent (DI) QSDC [25]. In order to address the long-range communication needs of QSDC under current technologies, a secure repeater scheme, which can provide end-to-end secure communication based on computational security, was proposed and has been demonstrated in a principle experiment [26]. To meet the demands of QSDC networks, a QSDC networking scheme based on mesh topology has also been proposed [27].

Traditional encrypted communication requires a two-tiered structure: one layer is dedicated to transmitting keys, ensuring security, while the other handles the transmission of code words, ensuring reliability. In contrast, QSDC aims to convey information through a single quantum channel, thus concurrently achieving security and reliability. Employing QSDC for data transmission within the monitoring system offers the potential of quantum-based physical security, thereby preventing link eavesdropping and safeguarding against tampering with monitoring data, all while ensuring reliable data transmission.

2. Surveillance System with QSDC

A surveillance system typically comprises a camera device that captures images of the subject under surveillance, an image data transmission system, and a display monitor. To take advantage of quantum technology and integrate it into the surveillance system, we substitute the traditional data transfer system with a quantum terminal system utilizing the QSDC protocol, which ensures enhanced security and privacy throughout the process. The composition of the QSDC surveillance system is depicted in Figure 1. Tx and Rx are the QSDC terminals used to transmit the surveillance data. Tx represents the transmitter, and Rx represents the receiver. The camera is coupled to the transmitter by a USB-FC converter, and the screen is connected to the receiver to display the situation of the monitoring location.

The transmitter and receiver primarily comprise modules such as optical modules (OM), electrical modules (EM), and central control computers (CC). Modules communicate with each other internally via the PCIe interface, and the transmitter interconnects with the receiver through three cables. The first one is a single-mode fiber that serves as the quantum channel, linking the transmitter's optical module to the receiver's optical module. Quantum states, serving as the communication medium, are conveyed from the transmitter to the receiver, facilitating one-way communication. The second cable, also a single-mode fiber, is responsible for clock synchronization, connecting the electrical modules of the two terminals. The third one is an Ethernet cable employed to exchange essential classic interaction information, establishing connectivity between the central control computers. Upon receiving the monitoring data, the QSDC receiver will convert it into image data, subsequently transmitting it to the display screen.

The QSDC transmitter uses phases of photons to modulate the data captured by the camera, and the receiver demodulates the data utilizing the interference of photons, which is achieved by a Faraday–Michelson interferometer (FMI) [28] as shown in Figure 2. A laser diode emits weak coherent pulses, while the intensity modulator (IM) generates the three intensity decoy states [29–31]. After the beam splitter (BS), the optical circuit forms an asymmetric FMI. Phase modulation and demodulation are performed through a phase modulator (PM), and the variable optical attenuator (VOA) reduces photon pulse intensity to a single photon level. Combined with the optical circulator (CIR), the single-photon detectors (SPD) can detect the photons after interference.

The OM combined with the EM can achieve the quantum state transmission. Furthermore, software for preprocessing, encoding, and decoding monitoring data is operational on the CC.

The security of the system is ensured by the QSDC protocol. The QSDC protocol's security has been analyzed using Wyner's wiretap channel theory, and quantitative secure capacity has also been given [10, 11, 15]. Figure 3 illustrates the approximate process of an image captured by the camera being transmitted to the receiving-end screen. Initially, the image captured by the camera undergoes compression to reduce its size to a suitable level for transmission. To achieve image compression, we utilized the encoder class within Microsoft's .NET framework. Specifically, we used the quality parameter, setting it to 20. Subsequently, the image data are passed through an encoder, and the encoded codewords are modulated onto quantum states by the optical system. These modulated quantum states are then transmitted through a quantum channel and demodulated within the optical system at the receiver. The demodulated data are subsequently fed into a decoder, where it is restored to the image file and displayed on the screen. The encoder and decoder utilize a forward error correction (FEC) code based on low-density parity-check (LDPC) code and repetition code [19]. Regarding the QSDC protocol, we have devised a novel protocol inspired by the concepts introduced in [32, 33]. In brief, the existing QSDC protocols employ a bidirectional framework wherein the qubits carry the information necessitating a round trip between the sender and the receiver to transmit information. Conversely, the innovative QSDC protocol employed in this surveillance system used a unidirectional architecture, requiring merely a one-way transfer of the qubits to transmit information from the sender to the receiver. This results in a substantial reduction of the influence of transmission loss on the communication rate. The details of the novel QSDC protocol will be disclosed in a forthcoming paper, currently in the process of composition. The details of the novel QSDC protocol will be disclosed in a separate paper, currently in the process of composition.

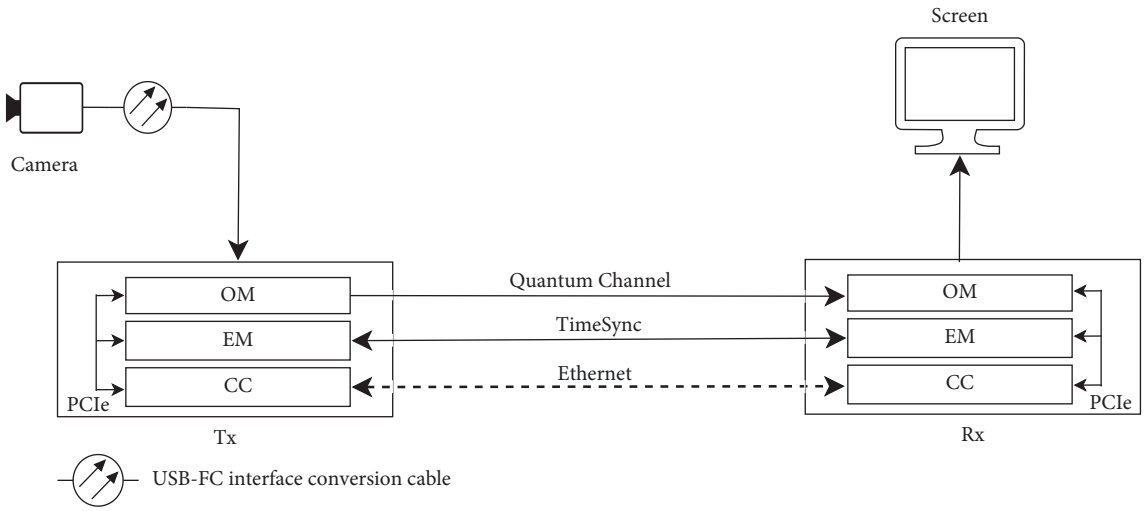

Figure 1: Composition of QSDC surveillance system. OM: optical module; EM: electrical module; CC: central control computer; Tx: transmitter; Rx: receiver; and PCIe: peripheral component interconnect express.

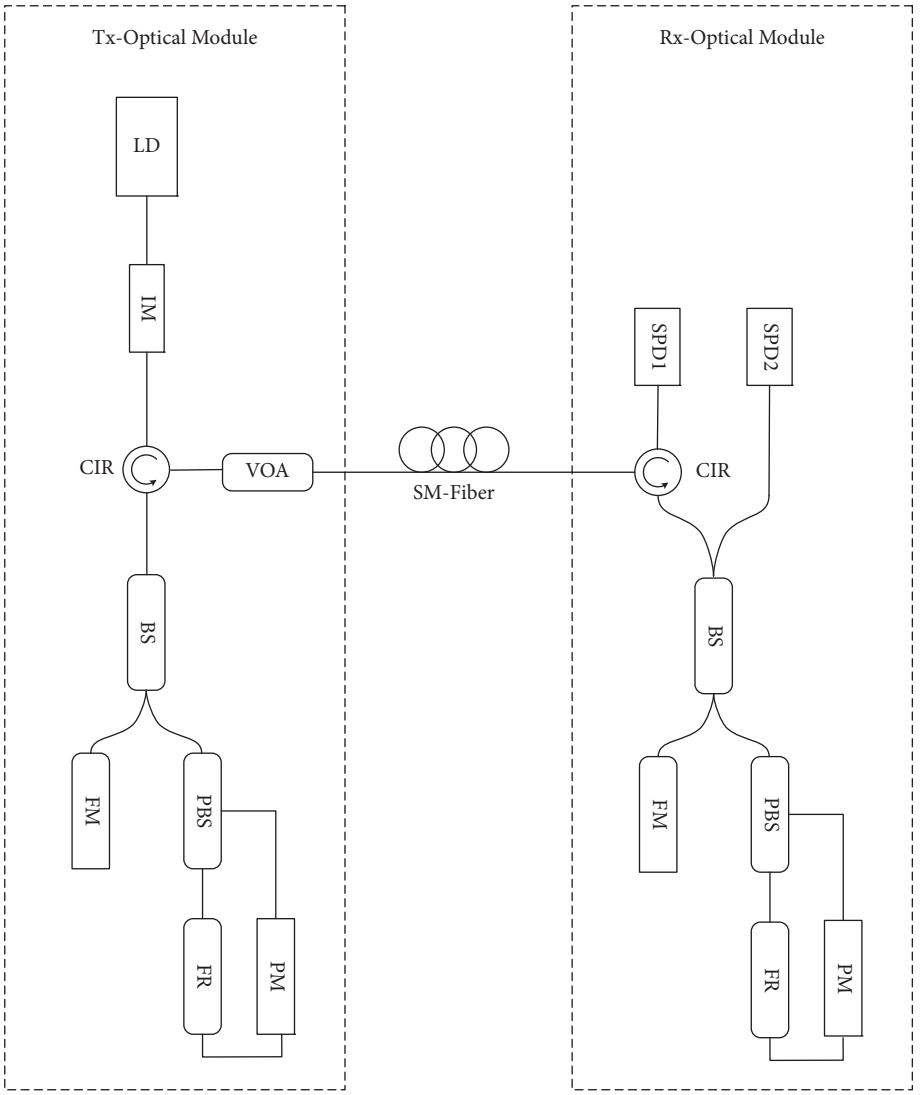

Figure 2: Schematic of the optical module. LD: laser diode, IM: intensity modulator, BS: beam splitter, PBS: polarization beam splitter, FM: Faraday mirror, FR: faraday rotator, PM: phase modulator, CIR: optical circulator, VOA: variable optical attenuator, SM: single mode, and SPD: single-photon detector.

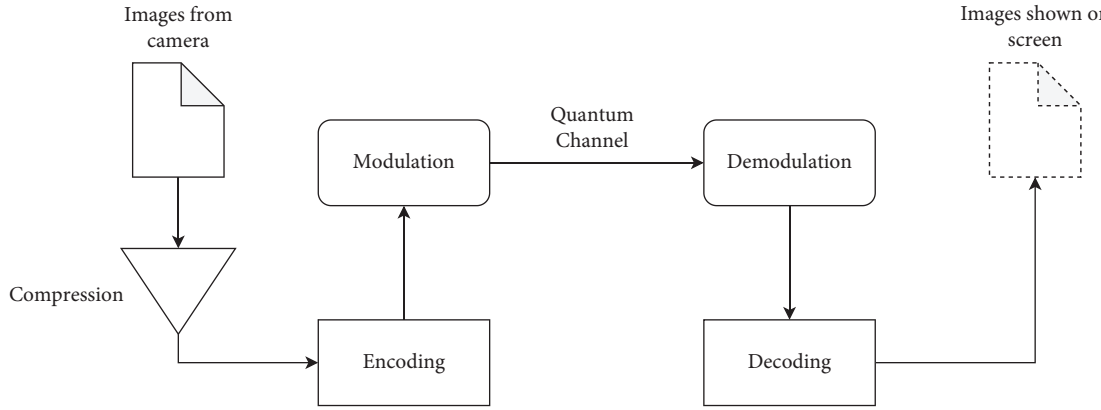

Figure 3: Process of image file transmission in the QSDC surveillance system.

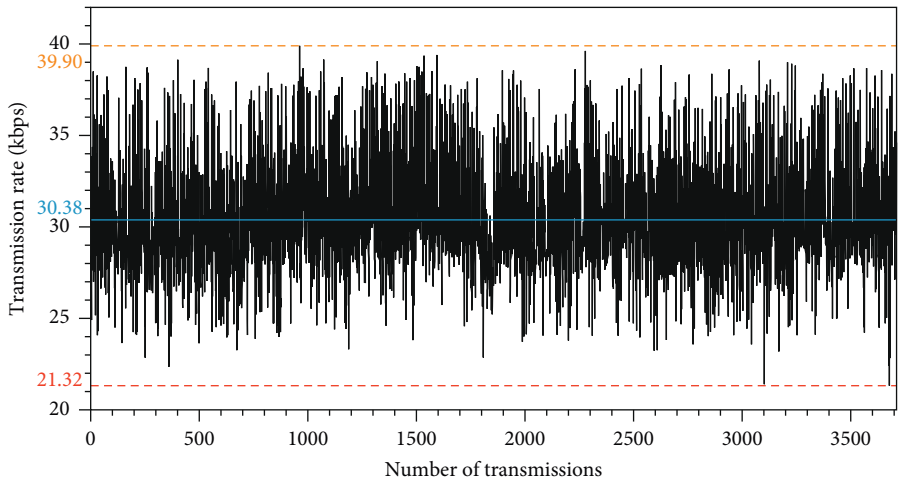

Figure 4: Transmission rate of each compressed photo in chronological order. The red and orange dashed lines denote the minimum and maximum experimental values of transmission rates, respectively. The blue solid line represents the mean transmission rate.

(a) (b)

Figure 5: Continued.

(c)

Figure 5: The images from camera to receiver. (a) The original image from the camera. (b) The compressed image. (c) The received image.

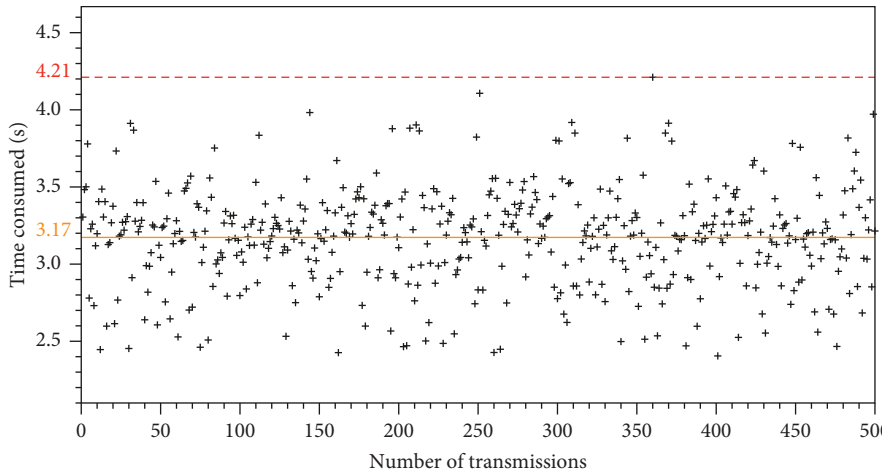

Figure 6: Time consumption of transmissions. The horizontal axis represents the sequential order of transmissions, while the vertical axis represents the time consumption for each transmission. The red dashed line indicates the maximum time consumption, and the orange solid line indicates the average time consumption.

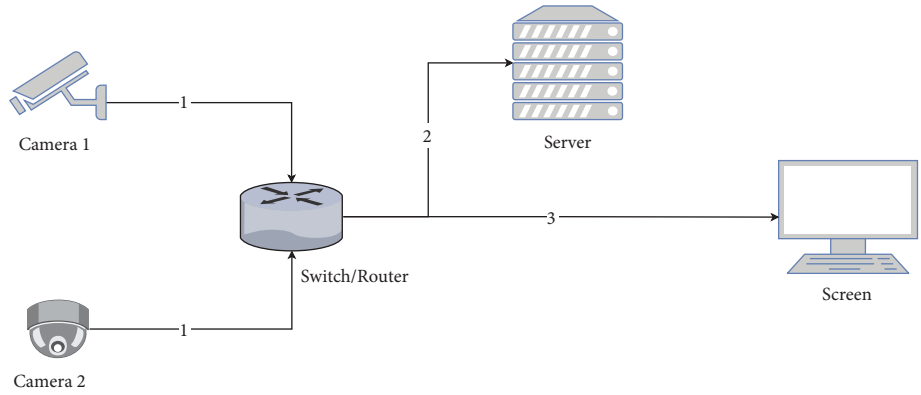

Figure 7: Diagram of a surveillance network. The numbers 1, 2, and 3 indicate links 1, 2, and 3, respectively.

3. Results and Discussion

The QSDC surveillance system is deployed in the corridor adjacent to the hazardous chemical storage room. A camera is oriented to face the entrance and captures an image every 10 seconds. Each photograph averages about 406.39 KB in size, which is subsequently compressed to an average of 11.78 KB. Then, the compressed monitoring images are encoded using an FEC code, and the resulting codewords are modulated into quantum states. The transmission distance is 50 km in a single-mode fiber. After the transmission following the QSDC protocol, the quantum states are restored

to their compressed image format and displayed on the receiver's screen.

The system operates continuously for 11.394 hours, equivalent to 11 hours, 23 minutes, and 40 seconds. The average transmission rate throughout this period is 30.38 kbps, as shown in Figure 4.

The horizontal coordinate represents the number of each transmission in chronological order, and the vertical coordinate denotes the transmission rate. The black line shows the rate for each transmission, and we can see significant fluctuations in rates per transmission. These variations can be attributed to phase drift caused by environmental factors evolving, impacting the transmission rate when the system performs the phase compensation. The dashed lines indicate the maximum and minimum transmission values, respectively, and the solid line indicates the average transmission rate.

The images captured by the camera, compressed by the transmitter, and transmitted through the quantum channel are shown in Figure 5, while some content that is not publicly available has been redacted.

It can be seen that after the compression and transmission, although a certain degree of clarity is sacrificed, the condition of the monitored object can still be recognized.

We also measured the time consumption of each transmission, a factor that affects the timeliness of detecting changes in the monitored objects. As shown in Figure 6, the time consumption of the initial 500 transmissions is presented. The time consumption refers to the duration from the moment of the camera capturing until the decoder at the receiver completes all decoding for the current transmission. The maximum recorded time consumption stands at 4.21 seconds, while the average time consumption amounts to 3.17 seconds, which implies that duty personnel can detect changes in the monitored object in approximately 4 seconds.

In a more complex complicated scenario, such as a surveillance network comprising multiple cameras, the above surveillance system can still be applied to enhance the security of the surveillance network infrastructure. As shown in Figure 7, cameras positioned at multiple locations transmit images via link 1 to the router, which has the capability to relay the monitoring data to the server through link 2, or directly to the screen for real-time viewing via link 3. With the characteristics of our system, the QSDC surveillance system can be mounted using existing links for integration, endowing links 1, 2, or 3 with the operational capacity to switch to quantum transmission, thereby enhancing the security of the surveillance network.

4. Conclusions

We have implemented a surveillance system based on quantum communication in this article. The system employs QSDC to transmit images captured by cameras, providing secure transmission for monitoring data. We performed tests to assess the system's performance, revealing that with a 50 km fiber connection between the transmitter and receiver, the system achieved an average transmission rate of 30.38 kbps, with an average transmission time of 3.17 seconds. Based on these results, we conclude that this system is appropriate for monitoring hazardous substances storage facilities.

In complex monitoring scenarios, reducing transmission time will be an area for improvement in the future. The current factors that affect transmission time in the system are mainly image compression, information encoding, and decoding processes. These issues can be resolved by replacing compression algorithms, using more efficient channel coding, and optimizing encoders. As the QSDC system continues to evolve, higher secure transmission rates are expected to be achieved in the future, which may support real-time video monitoring applications.

It is worth pointing out that the QSDC protocol provides a quantum physics-based secure transmission channel between two legitimate users. It can transmit ciphertext data encrypted by the users and allows them to recover plaintext data using their preferred encryption system. This feature provides flexibility for integrating our scheme into practical systems, expanding its potential application scenarios.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This research was supported by the National Natural Science Foundation of China under (Grant no. 11974205), Beijing Advanced Innovation Center for Future Chip (ICFC), and Tsinghua University Initiative Scientific Research Program.

References

[1] N. Kalbo, Y. Mirsky, A. Shabtai, and Y. Elovici, "The security of IP-Based video surveillance systems," *Sensors*, vol. 20, no. 17, p. 4806, 2020.

[2] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, IEEE, Santa Fe, NM, USA, November 1994.

[3] B. Yan, Z. Tan, S. Wei et al., "Factoring integers with sublinear resources on a superconducting quantum processor," 2022, https://arxiv.org/abs/2212.12372.

[4] 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, January 1984.

[5] L. C. Kwek, L. Cao, W. Luo et al., "Chip-based quantum key distribution," *AAPPS Bulletin*, vol. 31, no. 1, p. 15, 2021.

[6] G.-L. Long and X.-S. Liu, "Theoretical efficient high capacity quantum key distribution scheme," 2000.

[7] G. L. Long and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Physical Review A*, vol. 65, no. 3, Article ID 032302, 2002.

[8] F.-G. Deng, G.-L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Physical Review A*, vol. 68, no. 4, Article ID 042317, 2003.

[9] F.-G. Deng and G.-L. Long, "Secure direct communication with a quantum one-time pad," *Physical Review A*, vol. 69, no. 5, Article ID 052319, 2004.

[10] J.-W. Wu, Z.-S. Lin, L.-G. Yin, and G.-L. Long, "Security of quantum secure direct communication based on Wyner's wiretap channel theory," *Quantum Engineering*, vol. 1, no. 4, p. e26, 2019.

[11] J. Wu, G.-L. Long, and M. Hayashi, "Quantum secure direct communication with private dense coding using a general preshared quantum state," *Physical Review Applied*, vol. 17, no. 6, Article ID 064011, 2022.

[12] J.-Y. Hu, B. Yu, M.-Y. Jing et al., "Experimental quantum secure direct communication with single photons," *Light: Science & Applications*, vol. 5, no. 9, Article ID e16144, 2016.

[13] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, and G.-C. Guo, "Quantum secure direct communication with quantum memory," *Physical Review Letters*, vol. 118, no. 22, Article ID 220501, 2017.

[14] F. Zhu, W. Zhang, Y.-B. Sheng, and Y.-D. Huang, "Experimental long-distance quantum secure direct communication," *Science Bulletin*, vol. 62, no. 22, pp. 1519–1524, 2017.

[15] R.-Y. Qi, Z. Sun, Z.-S. Lin et al., "Implementation and security analysis of practical quantum secure direct communication," *Light: Science & Applications*, vol. 8, no. 1, p. 22, 2019.

[16] H.-R. Zhang, Z. Sun, R.-Y. Qi, L.-G. Yin, G.-L. Long, and J.-H. Lu, "Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states," *Light: Science & Applications*, vol. 11, no. 1, p. 83, 2022.

[17] D. Pan, Z.-S. Lin, J.-W. Wu et al., "Experimental free-space quantum secure direct communication and its security analysis," *Photonics Research*, vol. 8, no. 9, pp. 1522–1531, 2020.

[18] Z. Sun, R.-Y. Qi, Z.-S. Lin, L.-G. Yin, G.-L. Long, and J.-H. Lu, "Design and implementation of a practical quantum secure direct communication system," in *Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps)*, IEEE, Abu Dhabi, United Arab Emirates, December 2018.

[19] Z. Sun, L.-Y. Song, Q. Huang et al., "Toward practical quantum secure direct communication: a quantum-memory-free protocol and code design," *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5778–5792, 2020.

[20] D. Pan, K. Li, D. Ruan, S. X. Ng, and L. Hanzo, "Single-photon-memorytwo-step quantum secure direct communication relying on einstein-podolsky-rosen pairs," *IEEE Access*, vol. 8, pp. 121146–121161, 2020.

[21] G.-L. Long and H.-R. Zhang, "Drastic increase of channel capacity in quantum secure direct communication using masking," *Science Bulletin*, vol. 66, no. 13, pp. 1267–1269, 2021.

[22] P.-H. Niu, Z.-R. Zhou, Z.-S. Lin, Y.-B. Sheng, L.-G. Yin, and G.-L. Long, "Measurement-device-independent quantum communication without encryption," *Science Bulletin*, vol. 63, no. 20, pp. 1345–1350, 2018.

[23] Z.-R. Zhou, Y.-B. Sheng, P.-H. Niu, L.-G. Yin, G.-L. Long, and L. Hanzo, "Measurement-device-independent quantum secure direct communication," *Science China Physics, Mechanics & Astronomy*, vol. 63, no. 3, Article ID 230362, 2020.

[24] P.-H. Niu, J.-W. Wu, L.-G. Yin, and G.-L. Long, "Security analysis of measurement-device-independent quantum secure direct communication," *Quantum Information Processing*, vol. 19, no. 10, p. 356, 2020.

[25] L. Zhou, Y.-B. Sheng, and G.-L. Long, "Device-independent quantum secure direct communication against collective attacks," *Science Bulletin*, vol. 65, no. 1, pp. 12–20, 2020.

[26] G.-L. Long, D. Pan, Y.-B. Sheng, Q.-K. Xue, J.-H. Lu, and L. Hanzo, "An evolutionary pathway for the quantum internet relying on secure classical repeaters," *IEEE Network*, vol. 36, no. 3, pp. 82–88, 2022.

[27] P.-H. Niu, F.-H. Zhang, X.-W. Chen, M. Wang, and G.-L. Long, "QNUS: reducing terminal resources in quantum secure direct communication network using switches," *Quantum Engineering*, vol. 2022, Article ID 6345981, 6 pages, 2022.

[28] S. Wang, W. Chen, Z.-Q. Yin et al., "Practical gigahertz quantum key distribution robust against channel disturbance," *Optics Letters*, vol. 43, no. 9, p. 2030, 2018.

[29] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Physical Review Letters*, vol. 91, no. 5, Article ID 057901, 2003.

[30] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Physical Review Letters*, vol. 94, no. 23, Article ID 230503, 2005.

[31] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical Review Letters*, vol. 94, no. 23, Article ID 230504, 2005.

[32] K. Wen, F.-G. Deng, and G.-L. Long, "Reusable vernam cipher with quantum media," 2007, https://arxiv.org/abs/0711.1632.

[33] F.-G. Deng and G.-L. Long, "Repeatable classical one-time-pad crypto-system with quantum mechanics," 2019, https://arxiv.org/abs/1902.04218.