

Research progress in quantum key distribution

Chun-Xue Zhang(张春雪), Dan Wu(吴丹), Peng-Wei Cui(崔鹏伟), Jun-Chi Ma(马俊驰), Yue Wang(王玥), and Jun-Ming An(安俊明)

Citation: Chin. Phys. B, 2023, 32 (**12**): 124207. DOI: 10.1088/1674-1056/acfd16
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Broadband and wide-angle plane focal surface Luneburg lens

Jue Li(李珏), Yangyang Zhou(周杨阳), and Huanyang Chen(陈焕阳)
Chin. Phys. B, 2023, 32 (**6**): 064210. DOI: 10.1088/1674-1056/ac8e9e

Optically pumped wavelength-tunable lasing from a GaN beam cavity with an integrated Joule heater pivoted on Si

Feifei Qin(秦飞飞), Yang Sun(孙阳), Ying Yang(杨颖), Xin Li(李欣), Xu Wang(王旭), Junfeng Lu(卢俊峰), Yongjin Wang(王永进), and Gangyi Zhu(朱刚毅)
Chin. Phys. B, 2023, 32 (**5**): 054210. DOI: 10.1088/1674-1056/acc05e

Four-stage cascaded variable optical attenuator with large attenuation range for quantum key distribution

Qing-Hai Liu(刘清海), Pan Pan(潘盼), Jin You(游金), Jia-Shun Zhang(张家顺), Ya Wang(汪亚),Yu-Ting Wang(王玉婷), Liang-Liang Wang(王亮亮), Jun-Ming An(安俊明),Da-Jian Cui(崔大健), Lang Zhou(周浪), and Wei Chen(陈伟)
Chin. Phys. B, 2023, 32 (**5**): 054207. DOI: 10.1088/1674-1056/ac8af6

Proof-of-principle experimental demonstration of quantum secure imaging based on quantum key distribution

Yi-Bo Zhao(赵义博), Wan-Li Zhang(张万里), Dong Wang(王东), Xiao-Tian Song(宋萧天), Liang-Jiang Zhou(周良将), Chi-Biao Ding(丁赤飚)
Chin. Phys. B, 2019, 28 (**10**): 104203. DOI: 10.1088/1674-1056/ab3e66

Effect of electromagnetic disturbance on thepractical QKD system in the smart grid

Li Fang-Yi (李芳毅), Wang Dong (王东), Wang Shuang (王双), Li Mo (李默), Yin Zhen-Qiang (银振强), Li Hong-Wei (李宏伟), Chen Wei (陈巍), Han Zheng-Fu (韩正甫)
Chin. Phys. B, 2014, 23 (**12**): 124201. DOI: 10.1088/1674-1056/23/12/124201

REVIEW

Research progress in quantum key distribution

Chun-Xue Zhang(张春雪)[1,3], Dan Wu(吴丹)[1,3], Peng-Wei Cui(崔鹏伟)[1,3], Jun-Chi Ma(马俊驰)[1,3], Yue Wang(王玥)[1], and Jun-Ming An(安俊明)[1,2,3,†]

[1] *State Key Laboratory on Integrated Optoelectronics, Institute of Semiconductors, Chinese Academy of Sciences, Beijing* 100083, *China*
[2] *Center of Materials Science and Optoelectronics Engineering, University of Chinese Academy of Sciences, Beijing* 100049, *China*
[3] *College of Materials Science and Opto-Electronic Technology, University of Chinese Academy of Sciences, Beijing* 100049, *China*

(Received 28 June 2023; revised manuscript received 4 September 2023; accepted manuscript online 26 September 2023)

Quantum key distribution (QKD) is a sophisticated method for securing information by leveraging the principles of quantum mechanics. Its objective is to establish a confidential key between authorized partners who are connected via both a quantum channel and a classical authentication channel. This paper presents a comprehensive overview of QKD protocols, chip-based QKD systems, quantum light sources, quantum detectors, fiber-based QKD networks, space-based QKD systems, as well as the applications and prospects of QKD technology.

Keywords: quantum key distribution (QKD), sources, detectors, chip

PACS: 42.82.Et, 03.67.Dd, 42.82.Bq, 03.67.Hk **DOI:** 10.1088/1674-1056/acfd16

1. Introduction

Cryptography is a discipline that studies encryption, decryption and related techniques in a number of fields, including information security, computer science and mathematics. It aims to protect the confidentiality, integrity and availability of information. In 1948, Shannon, an American communications expert, proposed the basic concept of information theory in his paper[1] that all information known to people can be transformed into the form of 0, 1 bits for storage and transmission and processing, which is important in many fields such as communications, computer science, physics and statistics. In 1976, Whitfield Diffie and Martin Hellman introduced the concept of public key encryption[2] and introduced a public key encryption algorithm based on the discrete logarithm problem. In 1978, Ron Rivest, Adi Shamir and Leonard Adleman proposed RSA encryption algorithm.[3]

Quantum cryptography is a branch of cryptography that uses the principles of quantum mechanics to secure messages. The most peculiar feature of quantum mechanics is the existence of indivisible quanta and entangled systems.[4] Unlike traditional cryptography, quantum cryptography uses quantum bits to transmit encrypted information, and its basic principle is to use the unpredictability and coherence of quantum states to ensure the confidentiality of information. Quantum cryptography consists of two main parts, quantum key distribution and quantum authentication. We focus on quantum key distribution. Charles Bennett and Gilles Brassard's paper[5] published in 1984 introduced a new concept, quantum key distribution, and proposed the BB84 protocol. The protocol uses two orthogonal bases to encode a key and achieves secure key distribution through the coherence and irreducibility of quantum states. The BB84 protocol is also known as a four-state protocol, where the four quantum states are horizontal, vertical, left-skewed and right-skewed. By using a combination of these quantum states, secure key distribution can be achieved.

Although quantum cryptography is considered to be a more secure method of cryptography in theory, there are still some technical challenges and difficulties in its practical application.

2. QKD protocols

2.1. Development process

In 1984, Charles Bennett and Gilles Brassard proposed the BB84 protocol, the first protocol for quantum key distribution and one of the most classical and practical protocols. The protocol uses two orthogonal bases to encode the key and achieves secure key distribution through the coherence and irreducibility of quantum states. In 1991, professor Ekert of the Oxford University proposed the E91 protocol,[6] which is an entanglement-based QKD protocol. In 1992, Charles H. Bennett proposed the B92 protocol,[7] a quantum authentication protocol based on single-photon polarization states, which could detect eavesdropping attacks and guarantee absolute security. In the same year, Bennett, Brassard and Mermin proposed the BBM92 protocol,[8] which aims to achieve higher efficiency and lower resource consumption by combining the advantages of BB84 and B92 protocols. Continuous-variable protocol (CV-QKD) uses an infinite-dimensional and continuous Hilbert space to encode quantum states, and the information exists in the form of continuously distributed Gaussian

†Corresponding author. E-mail: junming@semi.ac.cn

© 2023 Chinese Physical Society and IOP Publishing Ltd

random numbers. In 1999, the first CV-QKD was proposed,[9] which based on discrete modulation of Gaussian states. In 2001, CV-QKD based on continuous modulation of Gaussian states was proposed.[10] According to the different types of light sources, CV-QKD can be divided into squeezed-state protocol,[10,11] coherent-state protocol[12,13] and entangled-state protocol. In 2002, Japanese scholar Inoue first proposed the use of differential phase shift protocol (DPS),[14] which is a phase modulation-based. In 2003, Hwang proposed the idea of a decoy state,[15] and in 2005, Prof. Wang Xiangbin from Tsinghua University and H K Lo's group in Canada, Prof. Luo Kaiguang, Prof. Ma Xiongfeng and Prof. Chen Kai independently developed the decoy state quantum key distribution.[16] In 2005, Stucki proposed the COW protocol, which uses the temporal information of light pulses to encode the eavesdropping situation by randomly adding decoy states and detecting inter-pulse coherence.[17] In 2006, Antonio Acín *et al.* proposed the device-independent QKD protocol (DI-QKD), where by measuring the entangled state, both parties can generate a key that is resistant not only to eavesdroppers constrained by the laws of quantum mechanics, but also to post-quantum eavesdroppers constrained only by the assumption of the no-signal principle.[18] In 2008, the continuous-variable two-way protocol was proposed.[19] In 2012, Lo's group in Canada and Braunstein's group in UK independently proposed the measurement device independent quantum key distribution protocol (MDI-QKD),[20] which uses entanglement exchange to shut down all attacks against detectors at once. In 2014, Japanese and American scientists proposed the round-robin differential-phase-shift (RRDPS) protocol,[21] which is based on the DPS protocol and adds a variable delay line (VD). Compared with conventional QKD, it has a higher bit error threshold and is feasible in harsher circumstances with a high bit error rate and short communication time. In 2018, Lucamarini *et al.* proposed a two-field quantum key distribution protocol (TF-QKD) that breaks the PLOB boundary.[22] The TF-QKD protocol has the same level of security as the MDI-QKD protocol, with measurement device-independent security. In the same year, a variant protocol of TF-QKD was proposed by the research team of Ma Xiongfeng from Tsinghua University, which is phase-matching quantum key distribution (PM-QKD),[23] which can overcome the linear key rate constraint by matching the phases of two coherent states and encoding the key information into the common phase, and developed a quantum bit-based security proof different from the traditional one. Other variants of TF-QKD include sending or not sending TF-QKD (SNS-TF-QKD),[24] no phase post-selection TF-QKD (NPP-TF-QKD).[25] In 2022, Ma Xiongfeng's research team at Tsinghua University proposed the mode-pairing quantum key distribution protocol (MP-QKD),[26] where the encoded key bits and bases are determined during data post-processing, using conventional second-order interference, without causing global phase locking.

Table 1. A comparison of several protocols.

Time	Protocols	Notes	References
1984	BB84	two non-orthogonal bases	[5]
1991	E91	based on entangled photon pairs	[6]
1992	B92	two non-orthogonal states, vulnerable to PNS attacks	[7]
2002	DPS	carries key information in the phase of the quantum state	[14]
2005	COW	light pulses to encode	[17]
2005	decoy state of mind	introduces a decoy state	[16]
2012	MDI-QKD	without the need for a trusted detector	[20]
2014	RRDPS	without relying on information-disturbance trade off; higher bit error threshold	[21]
2018	TF-QKD	breaks the linear key rate boundaries	[22]
2018	PM-QKD	a protocol combining the advantages of MDI-QKD and TF-QKD	[23]
2022	MP-QKD	uses more detection events for code generation; no complex laser frequency-locking and phase-locking technology; highly resistant to environmental noise	[26]

A detailed review of protocols such as MDI-QKD and TF-QKD is as follows. MDI-QKD was first proposed in 2012,[20] with its post-processing to form a security key based on Charlie's published measurements, which are the results of Bell measurements, and Alice and Bob's determination of the correlation of the two parties' data. The eavesdropper Eve cannot know Alice's and Bob's data even if she controls Charlie, Eve can only know the correlation of the data. The first proof-of-principle experiment was subsequently reported in 2013,[27] demonstrating this new QKD method in the laboratory over more than 80 km of wound fiber and at various locations in the city of Calgary. The paper[28] provides a proof-of-principle demonstration of a polarization-encoded MDI-QKD protocol that transmits weakly coherent states over two 8.5 km long fiber-optic links. In a paper published in the same year,[29] the MDI-QKD protocol was demonstrated by developing an efficient, low-noise up conversion single photon detector that can operate at a clock rate of 2 GHz with a transmission range of over 250 km and a secure key rate of over 1 kbps at a distance of 100 km, which is immune to all hacking

strategies on detection. In 2014, the USTC extended the secure transmission distance of MDI-QKD to 200 km by developing a fully automated, highly stable system with a 75 MHz clock frequency and a superconducting nanowire single photon detector with a detection efficiency of more than 40%,[3] achieving secure key rates more than three orders of magnitude. The first implementation of polarization-encoded MDI-QKD was demonstrated at the University of Toronto.[31] By optimizing the parameters in the decoy state protocol, it was demonstrated that it is feasible to implement polarization coded MDI-QKD with existing commercial equipment. In 2015, Guo Guangcan's team at USTC proposed a phase-coded phase-reference-free experiment MDI-QKD scheme.[32] As proof, a proof-of-principle experiment using a Faraday–Michaelson interferometer is given. The experimental system operates at 1 MHz and has an average secure key rate of 8.309 bps for a fiber length of 20 km between Alice and Bob. In 2014, Pan's team at the USTC developed an automatic feedback MDI-QKD system operating at high clock rates,[33] which was field tested by deploying a total length of 30 km of fibre-optic network, achieving a secure key rate of 16.9 b/s. In 2016, the Korea Institute of Science and Technology addressed the pattern matching problem present in the system by introducing the plug-and-play concept in the MDI-QKD system.[34] In the same year, the University of Cambridge introduced a new pulsed laser seeding technique[35] to obtain high visible interference from gain-switched lasers to perform MDI-QKD at critical rates in excess of 1 Mbit/s at a finite size range never before possible. A research team from Tsinghua University proposed a four-strength decoy-state MDI-QKD protocol,[36] which greatly improved the key rate. Pan Jianwei's group at the USTC performed an experimental demonstration of MDI-QKD using an optimized four-strength decoy state method on 404 km of ultra-low-loss fibre and 311 km of standard fibre.[37] In 2017, Guangcan Guo's group demonstrated a reference-frame-independent (RFI) MDI-QKD scheme based on polarization-disruptive units,[38] which has inherent stability; thus, the final secure key rate is insensitive to polarization random perturbations and phase reference drift. In 2018, the National University of Defense Technology reported the results of reference frame-independent MDI-QKD at 160 km distance with a clock frequency of 50 MHz,[39] and experimentally implemented a four-strength RFI-MDI-QKD protocol at 100 km and 120 km transmission distances. In 2019, Pan's team reported the results of the first high-rate MDI-QKD experiment over an asymmetric channel,[40] which demonstrated a 10-fold increase in key rate over the previous MDI-QKD protocol in the large-channel asymmetric case and extended the secure transmission distance by more than 20 km–50 km in standard telecommunication fibres by using a 7-strength optimization approach. In 2020, Pan's team experimentally demonstrated a 1.25 GHz silicon photonic chip MDI-QKD system using polarization encoding,[41] achieving random modulation of polarization state and decoy strength, and demonstrating a finite key secret rate of 31 bits/s over 36 dB channel loss (or 180 km of standard fiber). In the same year, Peking University demonstrated an all-chip MDI-QKD system, including two transmitter chips and a server chip, using integrated silicon photonic technology.[42] The system is capable of producing polarization-encoded weakly coherent states with polarization extinction ratios in excess of 20 dB, sufficient for low error MDI-QKD. In proof-of-concept experiments, the chip-based MDI-QKD system produced a key rate of 2.923×10^{-6} per pulse at a distance corresponding to 50 km of standard fibre, with a detection efficiency of 25% and a predicted distance of 120 km with a detection efficiency of 85%. Pan's team developed a robust adaptive optics system for high-precision time synchronisation and frequency locking between independent photon sources far apart, achieving the first free-space MDI-QKD in a 19.2 km urban-atmosphere channel well beyond the effective atmospheric thickness,[43] and its experiments were the first step towards satellite-based MDI-QKD. In 2021, Nanjing University achieved a heterogeneously integrated superconducting silicon photonic chip,[44] using the unique high-speed properties of optical waveguide-integrated superconducting detectors. They performed the first best Bell state measurement (BSM) of time-bin encoded quantum bits generated by two independent lasers, and obtained a secure key rate of 24.0 dB loss 6.166 kbps at a clock frequency of 125 MHz, which is comparable to the experimental results of the state-of-the-art MDI-QKD at GHz clock frequency. In 2021, researchers from Nanjing University of Posts and Telecommunications demonstrated RFI-MDI-QKD over 200 km and 300 km of optical fiber.[45,46] Meanwhile, they also presented an experiment demonstration of the 5-intensity MDI-QKD, which achieved a positive secure key rate over 442 km.[47] Researchers from Beijing University of Posts and Telecommunications proposed continuous-variable MDI-QKD with one-time shot-noise unit calibration, which lays the foundation for future research.[48] In 2022, researchers from Nanjing University proposed asynchronous MDI-QKD (also called mode-pairing MDI-QKD), which can surpass the key capacity without phase tracking and phase locking.[49] Researchers from Nanjing University of Posts and Telecommunications demonstrated semi-measure-device-independent quantum state tomography.[50] In 2023, researchers from Nanjing University demonstrated the experimental implementation of asynchronous MDI-QKD in intercity networks, which is practical and efficient.[51] In 2023, the Beijing Academy of Quantum Information Sciences experimentally overcame the rate-loss limit without global phase tracking.[52] Researchers from the University of Science and

Technology of China demonstrated intercity mode-pairing MDI-QKD without global phase-locking.[53]

In 2018, Lucamarini *et al.* proposed a two-field quantum key distribution protocol that breaks the PLOB bound, twin-field quantum key distribution, TF-QKD.[22] TF-QKD protocol has the same security level as MDI-QKD protocol, with measurement-device-independent security. TF-QKD protocol involves three parties, where Alice and Bob are legitimate communication parties, and Charlie is an untrusted measurement party. Alice and Bob are both senders, each of them has a laser and an interferometer arm; Alice (Bob) phase-randomizes the light pulses, then performs phase encoding, and sends them to Charlie for interference measurement via quantum channel. The core idea of TF-QKD is to adopt a special quantum signal encoding method to reduce the threat of attack types such as PNS attack. In traditional QKD systems, a pulse is usually used to represent a quantum bit, which may result in a very close time between pulses, making it susceptible to pulse overlap attack. However, in TF-QKD, each quantum bit is split into multiple pulses, which are sent at fixed time intervals. For example, if a quantum bit is split into four pulses, the sender will send these four pulses in sequence, with the same time interval between pulses. This encoding method makes the time structure of the signal more complex, making it difficult for attackers to exploit the temporal relationship of pulses to launch attacks, such as pulse overlap attack. By using this special encoding method, TF-QKD can effectively reduce the threat of pulse overlap attack on key distribution, thus improving the security of the protocol. This encoding method design is one of the core features of the TF-QKD protocol. TF-QKD is a special type of MDI-QKD.[54] In 2018, a variant protocol of TF-QKD was proposed, PM-QKD, where researchers from the University of Waterloo used non-phase-randomized coherent states as test states to propose an improved PM-QKD protocol, and showed that PM-QKD can overcome the repeaterless bound with currently available technology.[55] In 2018, researchers from Tsinghua University proposed SNS-TF-QKD, which presents a small error rate on Z-basis because it does not request single-photon interference on this basis.[33] In 2019, researchers from the University of Science and Technology of China proposed NPP-TF-QKD, which does not require active phase randomization and post-selection, and has a higher key rate within effective distance.[34] In 2019, Spanish researchers proposed an improved TF-QKD protocol that eliminates the post-selection requirement for global phase matching, and researchers from the University of Toronto provided a proof-of-principle demonstration.[56] In 2021, researchers from Nanjing University proposed a method to increase the distance of TF-QKD by adding entangled sources,[57] in the same year, researchers from Toshiba proposed a dual-band stabilization scheme that increased the secure key rate over long distances by two orders of magnitude,[58] and researchers from University of Toronto experimentally demonstrated TF-QKD on optical channels with asymmetric loss.[59] In 2022, researchers from the University of Science and Technology of China extended the distance of TF-QKD to 830 km.[60] In the same year, researchers from Beijing University of Posts and Telecommunications proposed TF-QKD based on wavelength-division-multiplexing technology, which further increased the secret key rate of TF-QKD and its variants.[61] In 2023, researchers from Nanjing University proposed a two-photon TF-QKD protocol that eliminates the strict constraints on intensity and probability,[62] in the same year, researchers from the University of Science and Technology of China achieved 100 km TF-QKD.[63] TF-QKD is a very promising field that offers new possibilities for ultra-long-distance quantum secure communication. With the continuous development of technology, we can expect more achievements in this field in the future.

2.2. Quantum attacks and security proofs

Here are the quantum attacks and security proofs. Although QKD has excellent potential as a secure communication technology, it also faces various challenges from quantum attacks. These attacks aim to compromise the confidentiality of communication by exploiting the characteristics of quantum communication. Here are some important types of quantum attacks and their corresponding security proofs and defense methods: common quantum attacks include photon-number-splitting attack,[64] phase-remapping attack,[65] nonrandom-phase attack,[66] Fake-state attack,[67] time-shift attack[68] and detection blinding attack,[69] etc. Security proofs include Lo–Chau security proof,[70] Shor–Preskill proof: reduction to prepare-and-measure schemes,[71] Koashi's complementarity approach[72] and entropic approach,[73] etc. Recent research progress on quantum attacks and security proofs can be seen in Ref. [74]. QKD systems can use various techniques and protocols to resist different types of quantum attacks, to improve the stability and efficiency of the system. For example, to defend against photon-number-splitting attack, single-photon sources and single-photon detectors can be used to reduce the possibility of photon splitting. To defend against phase-remapping attack, random phases can be introduced in the communication link to detect and prevent phase-remapping attack. In addition, time-based calibration and detection methods can be used to ensure that the transmitted phases are consistent and correct. Besides these technical measures, various protocols can also be used to enhance the security of QKD systems. For example, the MDI-QKD protocol aims to mitigate the threats that attackers may introduce in the measurement devices. The

security proof of MDI-QKD usually involves the untrustworthiness and asymmetry of the measurement devices. By performing measurements between different nodes on the communication link, MDI-QKD can resist various eavesdropping and tampering attempts by attackers, because attackers cannot control both communication nodes' measurements at the same time. As quantum technology continues to develop, new types of quantum attacks may emerge. The rise of quantum computing may lead to new attack methods, as the computational power of quantum computers may threaten current encryption algorithms. Attackers may use quantum computers to decrypt past communications, exposing previous keys. In addition, attackers may try to design more covert attack methods using phenomenon such as quantum entanglement. As quantum technology continues to evolve, researchers and engineers are exploring the concept of post-quantum cryptography. Post-quantum cryptography aims to develop new encryption methods that can withstand quantum computing attacks, to protect communication and data. This may involve new mathematical and physical concepts, as well as new encryption algorithms that are applicable in a quantum computing environment. However, this also brings the challenge of the transition period, i.e., how to smoothly transition to a new encryption system. Although quantum communication technologies such as QKD have high security in theory, they may be subject to limitations of physical implementation and innovative challenges from attackers in actual deployment. Losses in optical fibers, interference of photons, imperfections of devices, etc., may all lead to a decrease in the security of actual systems. Therefore, how to effectively address these issues in actual systems and ensure the security of quantum communication systems remains a challenge. As quantum communication technology develops, it will become possible to build large-scale quantum networks. However, the security issues of quantum networks will also increase accordingly. In this case, how to ensure the security of communication between multiple nodes, how to distribute and manage keys, and how to prevent potential attacks are all important issues that need to be addressed. Although quantum technology provides new possibilities for communication security, it also raises a series of new attack threats. Through continuous research and innovation, scientists and engineers will continue to improve the security of quantum communication technology, to ensure that future communication systems can withstand various potential attacks and provide reliable protection for communication confidentiality and integrity.

3. Advances in chip-based QKD research

For the silicon-based QKD chip, the first QKD transmitter to be fabricated on a standard foundry silicon photonic platform by a research team of the University of Toronto in 2016, the team designed structures integrating two identical ring modulators, a variable optical attenuator and a polarization modulator to implement BB84 polarization encoding. The work demonstrates the use of foundry silicon photonics for low-cost, wafer-scale quantum information fabrication components.[75] In the same year, the University of Bristol research team demonstrated a method to overcome the saturation and phase-dependent loss limitations of high-speed carrier depletion in standard silicon photonic fabrication using silicon photonic devices combined with high-speed, low-error quantum key distribution modulation with slow thermal optical DC deviation and fast (10 GHz bandwidth) carrier depletion modulation, and implemented the COW protocol, BB84 polarization-encoded, and BB84 time-bin coding.[76] In 2017, the Sandia National Laboratory's research team demonstrated a silicon photonic transceiver circuit for high-speed discrete variable quantum key distribution that uses a generic structure for both transmit and receive functions. When the circuit acts as a transmitter, light passes through the MZM from both arms of the MZM through a term shifter amplitude modulator and a polarization beam splitting rotator, and finally through a polarization beam splitter achieves BB84 polarization encoding and decoding.[77] In 2018, the Massachusetts Institute of Technology's research team demonstrated a silicon photonic QKD encoder in the first high-speed polarization QKD field test, designed with two MZMs and grating couplers encoder chip, demonstrating that photonic integrated circuits are a promising and scalable resource for forming future metropolitan quantum-secure communication networks.[78] In 2019, the Huawei research team introduced a time-bin approach to the silicon photonic transceiver, the silicon photonic emitter consists of three MZIs and one AMZI. The first MZI is used to generate the decoy state and the second MZI is used to balance the optical loss into the two arms of the AMZI. Through the AMZI, each laser pulse is divided into two time bins with the same intensity and a specific phase difference. The intensities of the two time-bin pulses are selectively modulated by the third MZI. As the refractive index changes when the chip temperature changes, the AMZI produces a large phase shift and the static operating point shifts, resulting in a large BER. The team designed and implemented a feedback procedure to correctly initialize and stabilize the static operating points of the two bases, thus reducing the quantum BER.[79] In 2020, Pan's team demonstrated a 1.25 GHz silicon photonic chip using a polarization encoding MDI-QKD system with light pulses generated from a laser coupled into a silicon photonic emitter chip with an integrated intensity modulator, variable optical attenuator and polarization modulator, followed by Bell testing, a study that demonstrated the miniaturization, low-cost fabrication and compatibility of silicon-

based MDI-QKD with CMOS microelectronics compatibility, among other advantages, as a promising solution for future quantum-safe networks.[41] In the same year, a research team at Peking University demonstrated a full-chip MDI-QKD system using integrated silicon photonic technology, including two transmitter chips and a server chip. For each transmitter chip, a pulse-modulated laser is coupled to a silicon waveguide via a grating coupler. The first MZI modulator generates the signal and decoy state by varying the laser intensity, and another phase modulator performs random phase modulation of the input pulse to ensure the assumption of phase randomization, which then enters the polarization modulator for modulation.[42] In 2021, an Italian research team proposed a silicon-based encoder for daylight quantum key distribution at 1550 nm.[80] Nanjing University achieved a heterogeneous integration of superconducting silicon photonic chip.[44] The Institute of Semiconductor Research, Chinese Academy of Sciences, carried out research on the application of silica AMZI in QKD coding and decoding in recent years,[81] and the optimal interferometric temperature point of single-light-level AMZI chip was obtained by using pulse self-interference method. In 2022, researchers from the University of Science and Technology of China proposed a prototype QKD transmitter by developing integrated silicon photonics and electronics technologies.[82] Researchers at the Institute of Semiconductors, Chinese Academy of Sciences proposed a simplified and reconfigurable silicon photonic encoder.[83] Researchers at the USTC used silica AMZI integrated with Faraday mirrors to improve the optimal interferometric anti-polarization performance,[84] achieving a secure key rate of 1.34 Mbps at 50 km. In 2023, the University of Science and Technology of China achieved a hundred-megabit-rate QKD by developing key technologies such as high-fidelity integrated photonic quantum state manipulation and high-count-rate superconducting single-photon detection.[85] Swiss and Italian scientists jointly developed a high-speed integrated QKD system.[86] Table 2 shows the research progress of silicon-based QKD.

Table 2. The research progress of silicon-based QKD.

Time	Clock frequency	Key rate	Bit error rate	Transmission distance	References
2016	1 GHz	0.953 kbps	5.4%	5 km	[75]
2016	1 GHz	916 kbps	1.01%	20 km	[76]
2017		1.3 Mbps	3.5%	127 km	[77]
2018	625 MHz	1.039 Mbps	2%	103.6 km	[78]
2019	100 MHz	85.7 kbps	0.84%	20 km	[79]
2019	1 MHz	0.14 kbps		100 km	[87]
2020		13.68 kbps	0.51%	20 km	[88]
2020	1.25 GHz	31 bit/s	$2.8\% \pm 0.2\%$	180 km	[41]
2020	0.5 MHz	2.923×10^{-6} per pulse	$25.6\%(x)$, $0.67\%(z)$	120 km	[42]
2020	2.54 GHz	COW: 792 kbps; DPS: 940 kbps	time 1.24%, phase 1.4/2%; DPS: phase 1.31%	20 km	[89]
2021	1 GHz	30 kbps	0.5%	145 m	[80]
2021	125 MHz	6.166 kbps	$0.25\%(x)$, close to $0(z)$	24 dB	[44]
2022		868 kbps	$1.34\%(x)$, $0.9\%(z)$	20 km	[83]
2022		42.7 kbps	0.41%	100 km	[82]
2023	2.5 GHz	115.8 Mb/s	0.61%	10 km	[85]
2023	2.5 GHz	9.4 kb/s	0.9%	202 km	[86]

4. Quantum light sources

Quantum light sources produce non-classical light states such as single photons or entangled photon pairs, which are essential for a wide range of quantum applications such as quantum key distribution, quantum computing, quantum sensing, etc. QKD systems can be divided into discrete-variable and continuous-variable protocols depending on the protocol. The light sources for both are called discrete and continuous light sources, respectively. Discrete light sources are most commonly known as single photon sources, single photon entanglement sources and weak single photon sources, while continuous light sources are most commonly known as Gaussian sources. Several quantum light sources are described next.

4.1. Quantum dot based sources

Quantum dot (QD) light sources are semiconductor nanostructures that produce single photons through a process of radiative compounding of excitons confined within the QD. Due to their unique size dependence, quantum dots exhibit discrete energy levels that result in quantized electronic states. This quantization of energy levels allows the production of single photons with well-defined wavelengths, making QD light sources particularly suitable for quantum communication and computing applications.

Significant progress has been made in recent years in the development and optimization of QD light sources. Some of the notable advances in this area include the following aspects.

Material systems: various material systems have been

investigated to fabricate quantum dot light sources, and the choice of material system plays a critical role in determining the emission wavelength and performance of QD light sources. For example, InAs/GaAs QDs emit photons in the near-infrared region, making them suitable for telecommunication applications, and more research on InAs/GaAs QDs can be read.[90] Research has focused on optimizing growth techniques such as molecular beam epitaxy (MBE) and chemical vapour deposition (CVD)[91] to achieve high quality quantum dot structures with narrow emission linewidths, high quantum efficiencies and low multiphoton emission probabilities. Deterministic quantum dot emission: one of the main challenges for quantum dot light sources is to achieve deterministic emission of single photons with well-controlled spatial and spectral properties. Reference [92] summarizes the research progress and challenges of chip-integrated deterministic quantum light sources. Researchers have demonstrated various techniques to improve the determinism of quantum dot emission, such as cavity-enhanced QD emission[93–95] and spectral filtering.[96] Cavity-enhanced quantum dot emission relies on coupling the quantum dot to an optical cavity (e.g., a microdisk or photonic crystal cavity), thereby increasing the spontaneous emission rate and making single photon emission highly efficient and directional. Spectral filtering techniques involve the use of optical filters, such as standard fixtures or wavelength-selective couplers, to selectively transmit photons with the desired wavelength, thereby increasing the spectral purity of the emitted photons.

Integration with photonic structures: the integration of QD light sources with photonic structures such as waveguides, beam splitters and multiplexers enables the realization of complex photonic circuits for quantum information processing. Recent advances in this field include monolithic integration of QD light sources with silicon and photonic platforms based on group III–V semiconductors, as well as the development of hybrid integration techniques that combine the advantages of different materials.

QD light sources have several ideal characteristics for QKD, such as high brightness, narrow linewidth, tunable wavelength, and compatibility with fiber networks. Moreover, QD can emit entangled photon pairs, enabling more efficient and robust QKD protocols, such as the BBM92 protocol.[97] QD can also be integrated with photonic structures: integrating QD light sources with photonic structures (such as waveguides, splitters, and multiplexers) can realize complex photonic circuits for quantum information processing. The latest advances in this field include monolithic integration of QD light sources with silicon and III–V semiconductor-based photonic platforms, and the development of hybrid integration techniques that combine the advantages of different materials. The information about integration with silicon, you can read Ref. [98], which improves the performance and reliability of QD-based QKD systems.

However, QD light sources also face some challenges and limitations in QKD applications. For example, QD usually requires low temperature and complex control techniques to achieve high-quality single-photon or entangled photon emission. QDs are also affected by decoherence and noise effects, which degrade the quantum state of the emitted photons, reducing the security and key rate of QKD. In addition, QDs are sensitive to fabrication defects and environmental fluctuations, which affect their emission characteristics and stability.

Therefore, QD light sources have great potential in QKD applications, but also need further development and optimization to overcome their drawbacks. Reference [99] provides a good review of the research progress and applications of QD in QKD, and some research groups have demonstrated proof-of-principle experiments of QKD using QD light sources.[100,101] In 2022, a research group from Technische Universität Berlin reported on the first QKD testbed using a compact benchtop quantum dot single-photon source operating at telecom wavelengths.[102] Heriot–Watt University achieved asymptotic positive key rate in 175 km telecom fiber based on QD,[10] which is a step toward long-distance single-photon emission quantum networks. Sapienza University of Rome's research team implemented a quantum communication protocol during daytime for the first time using a quantum dot source.[104] But to achieve practical and robust QKD systems based on QD, more efforts are needed.

4.2. Spontaneous parameter down-conversion sources

Spontaneous parametric down-conversion (SPDC) has become an essential tool for generating entangled photon pairs, which play a significant role in quantum communication and computation. SPDC occurs when a nonlinear crystal is pumped with high-energy photons, which subsequently decay into two lower-energy photons with conservation of energy and momentum. The process can be classified into two types: type-I, where both down-converted photons have the same polarization, and type-II, where the photons have orthogonal polarizations. The entanglement of photon pairs can be established in various degrees of freedom, including polarization, spatial modes, and time-frequency domains.

The efficiency of the SPDC process depends on several factors, such as the phase-matching condition, the choice of nonlinear crystal, and the pump beam properties. Phase matching, which ensures momentum conservation, is critical for achieving high conversion efficiency. Different techniques, like birefringent phase matching and quasi-phase matching, can be employed to fulfill the phase-matching condition. More on SPDC can be found in the Ref. [105].

SPDC light sources are light sources that generate single photons or entangled photon pairs using the spontaneous parametric down-conversion process. SPDC light sources have some advantages and disadvantages in QKD applications. Advantages: SPDC single-photon sources can produce high-quality entangled photon pairs with good coherence and polarization properties;[106] SPDC single-photon sources can greatly improve the secure transmission distance in QKD applications.[107] Disadvantages: SPDC light sources require precise control of laser intensity and phase matching conditions to achieve high-quality single photon or entangled photon emission. These conditions may be affected by environmental factors such as temperature, humidity, mechanical vibration, etc., resulting in reduced stability and reliability of SPDC light sources; SPDC light sources may produce excess multi-photon pairs, which reduce the purity and fidelity of single photon or entangled photon pairs. To eliminate this effect, complex techniques such as time-division multiplexing or photon-number-resolving detectors are required; SPDC single-photon sources require complex experimental setups, including stable pump lasers, nonlinear crystals, narrow-band filters and low-noise detectors. The system's practicality is still lower than that of weak coherent source.

4.3. Four-wave mixing sources

Four-wave mixing (FWM) is a third-order nonlinear optical process that enables the generation of correlated and entangled photon pairs. FWM has attracted considerable attention due to its compatibility with integrated photonic platforms, tunability, and the potential for generating photon pairs at telecom wavelengths.

FWM arises from the interaction of multiple optical waves in a nonlinear medium, resulting in the generation of new frequency components. The process involves the mixing of three input waves with frequencies ω_1, ω_2, and ω_3 to generate a fourth wave with frequency ω_4. The energy and momentum conservation conditions must be satisfied for efficient FWM to occur.

In the context of quantum information processing, FWM is typically employed in the degenerate regime, where two pump photons at frequency ω_p interact to create signal and idler photons at frequencies ω_s and ω_i, respectively. The generated photon pairs can exhibit quantum correlations in various degrees of freedom, such as time-frequency and spatial modes.

Compared to other methods of generating entangled photons, such as SPDC or quantum dot sources, QKD based on FWM has some advantages and disadvantages. Some of the advantages are: FWM can produce high-quality, high-brightness, low-noise entangled photons, which can improve the key rate and transmission distance of QKD systems; FWM can be implemented on various platforms, such as fibers, waveguides or microresonators, which can facilitate the integration and scalability of QKD systems; FWM can generate entangled photons at telecom wavelengths, compatible with existing optical communication infrastructure and equipment. Some of the disadvantages are: FWM requires high pump power and precise phase matching conditions, which increase the complexity and cost of QKD systems; FWM is sensitive to environmental fluctuations (such as temperature or polarization changes), which degrade the quality and stability of entangled photons; FWM may suffer from crosstalk and interference from other optical signals in the same medium, which reduces the security and efficiency of QKD systems. QKD based on FWM is an active research topic in quantum communication, and some recent advances include: in 2019, a team from Singapore reported a chip-scale CV-QKD system based on silicon photonics integration.[87] They achieved a key rate of 0.14 kbit/s over 100 km fiber transmission, demonstrating the potential of low-cost and compact QKD devices. In 2020, the University of Science and Technology of China in collaboration with Tsinghua University reported a 509 km ultra-low-loss fiber transmission QKD based on an improved twin-field protocol and superconducting nanowire single-photon detectors.[108] They achieved a key rate of about 0.1 bit/s, setting a new record for discrete-variable QKD systems. In 2023, the University of Science and Technology of China reported a 1002 km point-to-point fiber transmission QKD based on low-crosstalk phase reference signal control and ultra-low-noise single-photon detectors.[63] They achieved a key rate of 0.002 bit/s, breaking the record for repeaterless fiber-based QKD.

5. Quantum detectors

Quantum detectors play a vital role in a variety of quantum information processing applications. They are used to measure and manipulate quantum states in quantum communication systems, quantum computing architectures and quantum sensing devices. Three prominent types of quantum detectors are avalanche photodiode detectors (APD), quantum dot detectors and superconducting nanowire single photon detectors (SNSPD). The system parameters of single-photon detectors include: spectral range, dead time, dark count rate, detection efficiency, timing jitter and photon-number-resolving capability.[109]

5.1. Single-photon avalanche photodiodes

Single-photon avalanche photodiodes are semiconductor-based detectors that operate in Geiger mode. When a single incident photon triggers a carrier multiplication snow, a detectable current pulse is generated. One of the main challenges of APDs is the high dark count rate, i.e., the rate at which

the detector produces a signal without any photons. This is caused by the thermal generation of electron–hole pairs in the depletion region, which can trigger an avalanche. Various techniques have been developed to reduce the dark count rate, including cooling the APD to low temperatures, gating the APD to reduce the detection time window, and improving the quality of the diode structure to reduce the number of defect states. The advantages of APD include: high sensitivity, compact structure, high gain and high accuracy, etc., and its disadvantages include high dark count rate, high working voltage, etc. Reference [110] introduces several types of avalanche photodiode detectors made of different materials. With the advancement of research and technology, avalanche photodiodes will evolve towards higher performance, lower noise, lower cost, higher speed, etc. For example, researchers from the University of California Santa Barbara reported low dark current high gain InAs quantum dot avalanche photodetectors monolithically grown on Si.[111] The Ohio State University researchers reported high gain, low noise 1550 nm GaAsSb/AlGaAsSb avalanche photodiodes.[112] In QKD, researchers have studied the performance of differential phase shift quantum key distribution using InGaAs/InP and silicon APD.[113] Researchers will continue to explore new semiconductor materials, improve semiconductor processes, and optimize device structures and circuit designs to enhance the performance of APD.

5.2. Single-photon detectors based on quantum dots

A quantum dot detector is a device that utilizes the optoelectronic properties of quantum dots to detect infrared light. Quantum dots are semiconductor nanostructures with dimensions in the nanometer scale, with tunable energy band structure and discrete energy levels, so that selective absorption and emission of infrared light at different wavelengths can be realized. Quantum dot detectors have a wide range of applications, such as night vision, medical imaging, environmental monitoring, and quantum information.

The working principle of quantum dot detectors can be divided into two parts: photoelectric conversion and electron amplification. In the photoelectric conversion part, when a photon enters a quantum dot, it excites electrons, making the quantum dot a positively charged hole. These holes are blocked by a barrier layer to prevent them from flowing back into the quantum dot. The holes are then pushed towards the electrodes by the electric field, which in turn creates an electric current. This process is therefore the conversion of photon energy into electron energy. In the electron amplification section, a gain region is placed around the current electrode. A high voltage is applied to the gain region to create a high field. As the electrons pass through the gain region, they interact with the ions in the region, creating electron–hole pairs which continue to move and enter the current electrode to create a larger current. The process is therefore one of converting one electron into multiple electrons, resulting in the amplification of electrons. Because the process of electron amplification amplifies not only the signal current but also the noise current, quantum dot detectors are usually somewhat noisy. To reduce the noise, filters can be added to the detector or a low-noise amplifier can be used, for example.

The advantages of quantum dot detectors include high sensitivity, tunable band gap, simple fabrication and high integration, etc., and their disadvantages include poor stability, high defect density, etc. The research on quantum dot detectors has made some important progress, but also faces some challenges and problems. At present, quantum dot detectors are mainly divided into two categories: epitaxial quantum dot detectors (eQDIPs) and colloidal quantum dot detectors (cQDIPs). Epitaxial quantum dot detectors are fabricated by growing quantum dot arrays with regular arrangement and high crystalline quality on semiconductor substrates using techniques such as molecular beam epitaxy (MBE) or metal organic chemical vapor deposition (MOCVD), and then making electrodes and packaging. Colloidal quantum dot detectors are fabricated by synthesizing quantum dot particles with different compositions and sizes using solution methods, and then forming thin films or arrays by self-assembly or inkjet printing, and then making electrodes and packaging. Epitaxial quantum dot detectors have high photoelectric conversion efficiency and response speed, but also have some drawbacks, such as high growth temperature, long growth cycle, high growth cost, difficulty in wavelength tuning, low pixel density, etc. Colloidal quantum dot detectors have low production cost and high pixel density, and can achieve detection of wide-band infrared light, but also have some drawbacks, such as low carrier mobility, high defect density, poor stability, etc. In recent years, with the innovation of material synthesis and device design, the performance of quantum dot detectors has been significantly improved. For example, in the field of epitaxial quantum dot detectors, the detection of midwave infrared (MWIR) and long-wave infrared (LWIR) light was achieved by optimizing the quantum dot structure and material composition;[114] the photoelectric gain and responsivity were improved by introducing heterostructures and multilayer structures;[115] the pixel density and sensitivity were improved by using new readout circuits (ROIC).[116] In the field of colloidal quantum dot detectors, the carrier transport performance and surface passivation effect were improved by combining with materials such as metal halide perovskites, graphene, carbon nanotubes, etc.[114] The gain and response speed were improved by adopting different structures such as photodiode type, photoconductive type or field effect transistor

type; large-area infrared imaging was realized by integrating with CMOS or TFT readout circuits. Although some breakthroughs have been made in quantum dot detectors, there are still many problems and challenges to overcome: to improve the detection rate and sensitivity of quantum dot detectors. This requires further optimization of the material composition, size, morphology, structure, surface modification, etc., of quantum dots to improve their light absorption and emission efficiency, reduce defect density and Auger recombination, enhance carrier separation and transport, reduce dark current and noise, etc., to expand the detection wavelength range of quantum dot detectors. At present, most quantum dot detectors are limited to the short-wave infrared (SWIR) region, while the detection of MWIR and LWIR regions is still challenging. This requires the development of new quantum dot materials, such as lead salt, mercury telluride, indium antimonide, etc., to achieve absorption and emission of longer wavelength infrared light, and to solve the problems of stability, toxicity, processability, etc. of these materials; to reduce the fabrication cost and complexity of quantum dot detectors. At present, most quantum dot detectors rely on high-temperature, high-vacuum, high-precision equipment and processes for fabrication, which limits their scale production and application. This requires the development of new methods for quantum dot synthesis and assembly, such as liquid-phase exchange, sol-gel, spin coating, etc., to achieve high-quality quantum dot films or arrays under low-temperature, atmospheric pressure and low-cost conditions. And integrate them effectively with readout circuits to improve the stability and reliability of quantum dot detectors. At present, most quantum dot detectors show performance degradation or failure under the influence of environmental factors (such as temperature, humidity, oxygen, etc.), which affect their service life and safety. This requires improving the surface protection layer and packaging layer of quantum dots to enhance their resistance to environmental factors, and conduct systematic aging tests and fault diagnosis to evaluate their stability and reliability. Quantum dot detectors are less used in the QKD field, mainly focusing on quantum dot light sources.

5.3. Superconducting nanowire single-photon detectors

Superconducting nanowire single-photon detectors (SNSPD) are based on the principle of detecting changes in the resistance of superconducting materials caused by photon absorption. When a photon is absorbed, it creates a localized region of normal conductivity in the superconducting wire, resulting in a measurable change in resistance. Further reviews of superconducting nanowire detectors can be found in Refs. [62–64]. The advantages of SNSPD include high detection efficiency, low dark count rate, small timing jitter, short dead time and wide spectral response, etc., and its disadvantages include low working temperature, complex equipment, etc. In recent years, SNSPD technology has made great progress, constantly refreshing the performance indicators such as detection efficiency, dark count rate, timing jitter and dead time. In addition, researchers are also striving to push SNSPD technology to the next level: to achieve photon counting, fast time-tagging imaging and multi-pixel technology, and to be compatible with quantum photonic integrated circuits. The detection efficiency and time resolution of SNSPD are related to the temperature, so researchers are looking for a superconducting material that can work at high temperature to reduce the cooling cost and improve the system reliability. Researchers at the Massachusetts Institute of Technology achieved single-photon detection using high-temperature superconductors,[117] expanding the family of superconducting materials. The detection efficiency and time resolution of SNSPD are also related to the geometry and topology of the nanowire, so researchers are exploring different nanowire designs to optimize the performance of SNSPD. For example, a spiral nanowire was proposed, which can increase the probability of photon-nanowire interaction and thus improve the detection efficiency.[118] In addition, a nanowire structure based on a superconducting quantum interference device (SQUID) was proposed,[119] which can achieve photon number resolution. SQUID is an instrument that uses the characteristics of superconducting materials to detect magnetic field changes. It can be used to measure extremely weak magnetic field signals, with high sensitivity and time resolution. The application fields of SNSPD are also expanding, in addition to quantum information, bioimaging, photodetection and ranging, etc., SNSPD can also be used in astronomy, medicine, security detection and other aspects.[120] In QKD, German researchers designed a rack-sized multi-channel SNSPD system to achieve ultrafast QKD.[121] Researchers from the University of Science and Technology of China demonstrated a fiber-based dual-field QKD over 1002 km using SNSPD to suppress noise to about 0.02 Hz.[122] More research on superconducting nanowire detectors can be found in Refs. [122,123].

6. QKD based on optical fibre

6.1. QKD for telecommunication wavelengths

Telecommunication wavelengths QKD typically operate in the C-band (1530 nm–1565 nm) and L-band (1565 nm–1625 nm), where fibre transmission has minimal attenuation due to the inherent properties of silica-based fibres. These wavelengths are suitable for long distance transmission as they coincide with the lowest loss window in the fibre, which is essential for maintaining the quantum state of the photon. In addition, QKD at communication wavelengths benefits from mature and developed technologies such as high-quality

laser sources, detectors and optical fibre components designed for communication networks. In contrast, other wavelength QKD systems operate outside the traditional telecommunication wavelength range with high losses in fibre transmission, and experiments with spatial QKD are carried out in Ref. [124] using 850 nm wavelengths.

6.2. Quantum relay technology

As the communication distance increases, the communication capability becomes worse, and currently, the maximum transmission distance of an optical fibre-based QKD system without quantum repeaters is 658 km for ultra-low loss transmission fibre transmission.[125] Instead, there are two solutions to achieve long-range communication, one is satellite-based quantum communication, and the other is to use quantum repeaters.[126] The core technologies in quantum repeaters include entanglement switching,[127] entanglement purification[128] and quantum storage,[129] and a detailed description of quantum repeaters can be found in Ref. [130]. There are several reasons that hinder the development of quantum repeater technology. Firstly, quantum repeaters: several metrics for assessing the performance of quantum machines are discussed in Ref. [131], including fidelity, efficiency, storage time, bandwidth, capacity to store multiple photons and dimensionality and wavelength.

Performance improvements remain a challenge. Atomic heterostructures, trapped ions and rare-earth ion-doped crystals, among others,[132] are among the most promising candidates for quantum memory, but each has its own set of difficulties, such as sensitivity to environmental noise, scalability and system complexity. Second, quantum entanglement generation: quantum relays rely on the distribution of entangled quantum bit pairs between distant nodes. The generation of such entangled pairs is hampered by the exponential decay of entanglement fidelity, also known as the photon loss problem, caused by fibre fading and detector inefficiencies. Third, entanglement exchange: to establish entanglement between remote nodes, entanglement exchange is required. This operation involves performing Bell state measurements (BSM) on incoming quantum bits and is technically challenging. Fourth, quantum error correction: quantum repeaters must efficiently manage the errors introduced during entanglement generation, distribution and processing. Fifth: scalability and integration: quantum repeater networks need to be scalable and interoperable with other quantum communication systems. Designing scalable and efficient quantum repeater architectures that can be integrated with existing fibre-optic networks and future quantum internet infrastructures is a complex task. Sixth, materials and fabrication challenges: implementing quantum repeater technology requires the development of suitable materials and fabrication techniques to achieve the required performance while maintaining low-loss and low-noise levels. This includes the development of low-loss waveguides, high-efficiency photonic detectors, and optimized manufacturing processes for quantum memories and other components of quantum repeater systems. The above points are also areas that researchers need to focus on.

6.3. Challenges

Signal attenuation due to fibre loss and scattering is a major challenge for fibre-based QKD systems. As the distance between communicating parties increases, the potential for photon loss also increases, resulting in a reduction in key generation rate and secure communication range. How to improve the secure communication range with low BER is a concern for fibre optic QKD systems.

7. Space QKD system

Space QKD enables secure long-range quantum communications by overcoming the distance limitations of terrestrial QKD systems that rely on fibre-optic or free-space links. By using satellites, space QKD can establish secure links between ground stations located on different continents, greatly extending the range of secure quantum communication networks. Space QKD has the following steps to achieve this. Firstly, Alice prepares a series of quantum bits, which are quantum states encoded in particles such as photons, and Alice uses a free-space optical link to send the prepared quantum bits to the satellite via the ground station. Secondly, the satellite acts as a trusted node or relay during the communication process. This step is where the space environment comes into play, as the quantum bits must travel through the Earth's atmosphere and possibly through the vacuum of space, which can introduce transmission losses, noise and other interference. Finally, the satellite receives the quantum bits and performs quantum operations on them, or simply relays them to another ground station where the second party (Bob) is located.

7.1. Satellite-based QKD

7.1.1. Mozi satellite

On 16 August 2016, China launched the world's first quantum science experiment satellite, Mozi, from the Jiuquan Satellite Launch Centre. The main objective of the satellite is to demonstrate the feasibility of using satellite links for secure long-range quantum communication. The satellite is equipped with a range of advanced quantum communication technologies, including an entangled photon source, a single photon detector and an ultrafast polarization modulator. These technologies enable Mozi to perform a variety of quantum communication experiments, including entanglement-based QKD, decoy state QKD and entanglement distribution. In 2017, Pan's team

reported the first satellite-to-ground quantum communication experiment at a distance scale of more than 1200 km using the Mozi satellite,[122] demonstrating the distribution of two entangled photons from a satellite to two ground stations separated by 1203 km, and observing the survival of entanglement and violation of Bell's inequality.[133] In 2020, entanglement-based QKD at a finite secret key rate of 0.12 bit/s between two ground stations separated by 1120 km without trusted relays being demonstrated, improving the efficiency of the link for two-photon distribution by a factor of about four compared to Ref. [134]. In 2021, a large-scale fibre-optic network of more than 700 fibre-optic QKD links and two high-speed satellite-to-ground free-space QKD links, built an integrated space-to-ground quantum communication network for the first time.[135]

7.1.2. Other satellite missions

In the field of quantum key distribution, various countries have promoted the development of space quantum communication technology. Following the success of China's Mozi satellite for satellite-based ground-based quantum key distribution, many countries and organizations have launched their own space QKD programmes. For example, the European Space Agency's SAGA project: the SAGA project aims to establish a global quantum communications network that uses satellite technology to provide high-speed, secure quantum key distribution between ground sites. The objectives of the project include research and development of quantum communication technologies applicable to satellites, determination of key performance parameters for quantum communication satellites and assessment of requirements for practical application scenarios. Canada's QEYSSAT project aims to demonstrate the application of quantum key distribution technology for secure online communications on earth.

7.2. Satellite-to-ground satellite links

Satellite–ground links refer to the establishment of quantum communication links between satellites and ground stations. The focus of research on satellite–ground links includes challenges such as overcoming atmospheric turbulence, reducing background noise and improving receiver sensitivity. In recent years, researchers have successfully solved these problems and demonstrated the feasibility of satellite–ground links.[124,133–135]

7.3. Satellite-based QKD

Satellite–satellite links refer to the technology for establishing quantum communication links in space, by transmitting quantum bits between two or more satellites in orbit. Such a link allows quantum communication on a global scale and enables complex quantum network topologies. Research on satellite–satellite links is still in its infancy. At present, the focus of research includes improving the alignment and tracking accuracy between satellites, reducing the influence of the space environment on the quantum state, and improving the stability of the link.

7.4. Intercontinental satellite links

Intercontinental satellite links are satellites that enable quantum communications between different continents. This kind of link can greatly extend the coverage of quantum communication and achieve secure communication on a global scale. The Mozi satellite has successfully realized an intercontinental quantum communication link between China and Austria.[136]

7.5. Challenge and prospects

There are the following challenges, firstly, atmospheric turbulence: atmospheric turbulence can cause photons to be deflected during transmission, thus affecting the alignment accuracy between the satellite and the ground station. Researchers need to develop stable adaptive optics to overcome the effects of atmospheric turbulence. Second, alignment and tracking: in space quantum communications, accurate alignment and tracking between satellites and ground stations is critical. High precision and high speed alignment and tracking techniques need to be developed to ensure the stability of the communication link. Thirdly, background noise: background light such as sunlight can cause interference to quantum communications and reduce communication efficiency. Solving this problem requires studying how to filter background noise and improve the sensitivity of the receiver. Fourth, signal loss: in space communication links, signal loss is a major challenge. To reduce signal loss, researchers need to optimize photon sources and improve the sensitivity of detectors and investigate more efficient quantum error correction techniques.

Global quantum communication networks: with the development of quantum communication technology in space, the future promises to enable quantum communication networks on a global scale, thus providing highly secure communication services. Satellite–satellite links: researchers will continue to explore satellite–satellite quantum communication technologies to enable more complex quantum network topologies. Intercontinental quantum communications: with advances in space quantum communication technology, quantum communications between different continents may be possible in the future, further extending the reach of quantum communications. Quantum satellite clusters: researchers may investigate the use of multiple quantum satellites to form clusters to improve communication efficiency, coverage and reliability. In conclusion, space quantum key distribution technology faces a number of challenges, but as research progresses

and technology advances, a highly secure quantum communication network on a global scale becomes possible in the future.

8. Application and prospects

8.1. Secure communications

One of the most obvious applications for QKD is secure communications, where QKD allows both parties to establish secure encryption keys that cannot be intercepted or copied by eavesdroppers. This makes it ideal for situations where secure communications are critical, such as diplomatic communications, or commercial transactions where sensitive information is shared. The stability and transmission distance limitations of quantum channels are important challenges. The fidelity of quantum bits decreases during long-distance transmission, resulting in an increase in bit error rates, which affects the security of the key. The use of quantum entangled states and quantum error-correcting codes can improve the stability of the channel. At the same time, the use of relay stations can extend the transmission distance. Relay stations can perform quantum entanglement distribution and error correction.

8.2. Financial transactions

QKD can also be used to protect financial transactions, especially those conducted over long distances. By using QKD, financial institutions can secure their transactions and protect their customers' financial information from hackers and other malicious actors. Financial transactions require high levels of security and real-time performance. Traditional QKD systems may have limitations in transmission speed and real-time performance. Developing more efficient QKD protocols, such as continuous-variable QKD, can improve transmission speed. In addition, combining classical cryptography and quantum encryption can achieve higher real-time performance while ensuring security.

8.3. Government applications

QKD has many potential applications in government environments. For example, it can be used to protect classified communications, protect critical infrastructure communications on the battlefield. Government sectors require high levels of security and need to resist various advanced attack methods, such as quantum computer attacks. Developing quantum key distribution schemes can resist known quantum attacks, such as quantum relay attacks and quantum side-channel attacks. In addition, combining traditional information protection measures, such as physical security and multi-level encryption, can provide higher levels of defense.

8.4. Internet of things security

As the internet of things becomes more widespread, there is a growing need for secure communications between devices. QKD can be used to provide secure communications between IoT devices, protecting them from hacking and other security threats. Internet of things devices have limited resources and cannot support complex encryption and decryption operations, while also ensuring low-latency and efficient communication. Developing lightweight QKD schemes suitable for IoT environments, such as those based on quantum key binding. In addition, traditional encryption techniques combined with quantum secure communication can be explored to balance security and efficiency.

8.5. Quantum internet

QKD is also a key technology for the development of the quantum internet. The quantum internet will be a network of interconnected quantum computers and other devices that can share information in a completely secure and hacker-proof manner. Building a large-scale quantum internet requires highly reliable quantum nodes and complex quantum communication architectures, as well as efficient quantum routing and management. Developing scalable quantum network architectures, utilizing quantum relay stations to connect different nodes, enables the achievement of quantum communication across larger distances. At the same time, efficient quantum routing algorithms and network management strategies must be developed to ensure the stability and reliability of communication.

9. Conclusion and perspectives

We have summarized the research progress in QKD. For QKD protocols, quantum light sources and quantum detectors, the research focuses on improving the security of QKD. The trend of chip-based QKD is to continuously improve its key rate and transmission distance, as well as to reduce the BER. Fiber-based QKD and spatial QKD are also evolving and the application of QKD is very important. In addition, QKD is developing towards intelligence and network. Machine learning methods are expected to improve the performance of QKD systems to better meet the needs of secure communication. Machine learning methods can use historical data and real-time data to predict phase changes and zero-phase voltages in QKD systems and control the corresponding devices in real time, thereby improving the stability and efficiency of the system;[137] machine learning methods can use LSTM networks to learn the data change rules in QKD systems and adjust the network parameters and structure dynamically according to environmental factors and device characteristics, thereby improving the intelligence and flexibility of

the system;[138] machine learning methods can combine other coding schemes and QKD protocols to design more suitable features and labels, thereby improving the security and fault tolerance of the system. These methods need to be combined with in-depth quantum physics and cryptography expertise to fully exploit their potential and ensure system security. QKD networking can improve the interoperability, scalability, flexibility and robustness of quantum networks, as well as exploit the advantages of different QKD protocols, such as high key rates, high security, long distance transmission, etc. QKD networking requires solving some challenging problems, such as protocol conversion,[139] resource allocation, node architecture, network management, etc., and it can also be combined with other quantum communication technologies, such as quantum secure direct communication (QSDC) and quantum teleportation (QST), to achieve higher-level quantum information services.

Future research and development will continue to promote the advancement of QKD technology so that it can be more widely applied to practical networks and communication systems. This development trend is expected to bring significant improvements to the field of information security, ensuring the privacy and integrity of communication data. Despite some progress, QKD also has many challenges. One of the main difficulties is to ensure security from the theory, and another difficulty is to ensure security from the device. Although the road of QKD development is full of challenges, its application prospect is still bright.

Acknowledgments

Project supported by the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300701), the National Key Research and Development Program of China (Grant No. 2018YFA0306403), and the Strategic Priority Research Program of Chinese Academy of Sciences (Grant No. XDB43000000).

References

[1] Shannon C E 1948 *Bell Syst. Tech. J.* **27** 379
[2] Hellman M 1976 *IEEE Trans. Inf. Theory* **22** 644
[3] Rivest R L, Shamir A and Adleman L 1978 *Commun. ACM* **21** 120
[4] Guo H 2016 *Quantum Cryptography* (Beijing: National Defense Industry Press) (in Chinese)
[5] Bennett C H and Brassard G 2020 *Theor. Comput. Sci.* **560** 7
[6] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[7] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[8] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[9] Ralph T C 1999 *Phys. Rev. A* **61** 010303
[10] Cerf N J, Levy M and Van A G 2001 *Phys. Rev. A* **63** 052311
[11] García-Patrón R and Cerf N J 2009 *Phys. Rev. Lett.* **102** 130501
[12] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[13] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 *Phys. Rev. Lett.* **93** 170504
[14] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902
[15] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[16] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[17] Stucki D, Brunner N, Gisin N, Scarani V and Zbinden H 2005 *Appl. Phys. Lett.* **87** 194108
[18] Acin A, Massar S and Pironio S 2006 *New J. Phys.* **8** 126
[19] Pirandola S, Mancini S, Lloyd S and Braunstein S L 2008 *Nat. Phys.* **4** 726
[20] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[21] Bouchard F, Sit A, Heshami K, Fickler R and Karimi E 2018 *Phys. Rev. A* **98** 010301
[22] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[23] Ma X, Zeng P and Zhou H 2018 *Phys. Rev. X* **8** 031043
[24] Wang X B, Yu Z W and Hu X L 2018 *Phys. Rev. A* **98** 062323
[25] Cui C, Yin Z Q, Wang R, Chen W, Wang S, Guo G C and Han Z F 2019 *Phys. Rev. Appl.* **11** 034053
[26] Zeng P, Zhou H, Wu W and Ma X 2022 *Nat. Commun.* **13** 3903
[27] Rubenok A, Slater J A, Chan P, Lucio-Martinez I and Tittel W 2013 *Phys. Rev. Lett.* **111** 130501
[28] Da Silva T F, Vitoreti D, Xavier G, Do Amaral G, Temporão G and Von Der Weid J 2013 *Phys. Rev. A* **88** 052303
[29] Liu Y, Chen T Y, Wang L J, Liang H, Shentu G L, Wang J and Pan J W 2013 *Phys. Rev. Lett.* **111** 130502
[30] Tang Y L, Yin H L, Chen S J, *et al.* 2014 *Phys. Rev. Lett.* **113** 190501
[31] Tang Z, Liao Z, Xu F, *et al.* 2014 *Phys. Rev. Lett.* **112** 190503
[32] Wang C, Song X T, Yin Z Q, *et al.* 2015 *Phys. Rev. Lett.* **115** 160502
[33] Tang Y L, Yin H L, Chen S J, *et al.* 2014 *IEEE J. Sel. Top. Quantum Electron.* **21** 116
[34] Choi Y, Kwon O, Woo M, Oh K, Han S W, Kim Y S and Moon S 2016 *Phys. Rev. A* **93** 032319
[35] Comandar L, Lucamarini M, Fröhlich B, Dynes J, Sharpe A, Tam S B, Yuan Z, Penty R and Shields A 2016 *Nat. Photonics* **10** 312
[36] Zhou Y H, Yu Z W and Wang X B 2016 *Phys. Rev. A* **93** 042324
[37] Yin H L, Chen T Y, Yu Z W, Liu H, You L X, Zhou Y H, Chen S J, Mao Y, Huang M Q and Zhang W 2016 *Phys. Rev. Lett.* **117** 190501
[38] Wang C, Yin Z Q, Wang S, Chen W, Guo G C and Han Z F 2017 *Optica* **4** 1016
[39] Liu H, Wang J, Ma H and Sun S 2018 *Optica* **5** 902
[40] Liu H, Wang W, Wei K, *et al.* 2019 *Phys. Rev. Lett.* **122** 160501
[41] Wei K, Li W, Tan H, *et al.* 2020 *Phys. Rev. X* **10** 031030
[42] Cao L, Luo W, Wang Y, *et al.* 2020 *Phys. Rev. Appl.* **14** 011001
[43] Cao Y, Li Y H, Yang K X, *et al.* 2020 *Phys. Rev. Lett.* **125** 260503
[44] Zheng X, Zhang P, Ge R, *et al.* 2021 *Adv. Photonics* **3** 055002
[45] Zhou X Y, Ding H J, Sun M S, *et al.* 2021 *Phys. Rev. Appl.* **15** 064016
[46] Liu J Y, Zhou X Y, Zhang C H, *et al.* 2021 *J. Light. Technol.* **39** 5486
[47] Liu J Y, Ma X, Ding H J, Zhang C H, Zhou X Y and Wang Q 2023 *Phys. Rev. A* **108** 022605
[48] Huang L, Zhang Y and Yu S 2021 *Chin. Phys. Lett.* **38** 040301
[49] Xie Y M, Lu Y, Weng C X, Cao X, Jia Z Y, Bao Y and Chen Z B 2022 *PRX Quantum* **3** 020315
[50] Li J, Zhu J L, Gao J, Pang Z G and Wang Q 2022 *Chin. Phys. Lett.* **39** 070303
[51] Xie Y M, Bai J L, Lu Y S, *et al.* 2023 *Phys. Rev. Appl.* **19** 054070
[52] Zhou L, Lin J, Xie Y M, Lu Y S, Jing Y, Yin H L and Yuan Z 2023 *Phys. Rev. Lett.* **130** 250801
[53] Zhu H T, Huang Y, Liu H, Zeng P, Zou M, Dai Y and Pan J W 2023 *Phys. Rev. Lett.* **130** 030801
[54] Yin H and Fu Y 2019 *Sci. Rep.* **9** 3045
[55] Lin J and Lütkenhaus N 2018 *Phys. Rev. A* **98** 042332
[56] Zhong X, Hu J, Curty M, Qian L and Lo H K 2019 *Phys. Rev. Lett.* **123** 100506
[57] Li B H, Xie Y M, Li Z, Weng C X, Li C L, Yin H L and Chen Z B 2021 *Opt. Lett.* **46** 5529
[58] Pittaluga M, Minder M, Lucamarini M, Sanzaro M, Woodward R I, Li M J and Shields A J 2021 *Nat. Photonics* **15** 530
[59] Zhong X, Wang W, Qia L and Lo H K 2021 *NPJ Quantum Inf.* **7** 8
[60] Wang S, Yin Z Q, He D Y, *et al.* 2022 *Nat. Photonics* **16** 154
[61] Han Y, Sun Z, Dou T, *et al.* 2022 *Chin. Phys. Lett.* **39** 070301
[62] Xie Y M, Weng C X, Lu Y S, Fu Y, Wang Y, Yin H L and Chen Z B 2023 *Phys. Rev. A* **107** 042603
[63] Liu Y, Zhang W J, Jiang C, Chen J P, Zhang C, Pan W X and Pa J W 2023 *Phys. Rev. Lett.* **130** 210801
[64] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330

[65] Fung C H F, Qi B, Tamaki K and Lo H K 2007 *Phys. Rev. A* **75** 032314
[66] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[67] Makarov V and Hjelme D R 2005 *J. Mod. Opt.* **52** 691
[68] Qi B, Fung C H F, Lo H K and Ma X 2005 arXiv: quant-ph/0512080
[69] Makarov V 2009 *New J. Phys.* **11** 065003
[70] Lo H K and Chau H F 1999 *Science* **283** 2050
[71] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[72] Koashi M 2009 *New J. Phys.* **11** 045018
[73] Renner R, Gisin N and Kraus B 2005 *Phys. Rev. A* **72** 012332
[74] Xu F, Ma X, Zhang Q, Lo H K and Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
[75] Ma C, Sacher W D, Tang Z, Mikkelsen J C, Yang Y, Xu F, Thiessen T, Lo H and Poon J K 2016 *Optica* **3** 1274
[76] Sibson P, Kennard J E, Stanisic S, Erven C, O'Brien J L and Thompson M G 2017 *Optica* **4** 172
[77] Cai H, Long C M, DeRose C T, *et al.* 2017 *Opt. Express* **25** 12282
[78] Bunandar D, Lentine A, Lee C, *et al.* 2018 *Phys. Rev. X* **8** 021009
[79] Geng W, Zhang C, Zheng Y, He J, Zhou C and Kong Y 2019 *Opt. Express* **27** 29045
[80] Avesani M, Calderaro L, Schiavon M, *et al.* 2021 *NPJ Quantum Inf.* **7** 93
[81] Li X, Ren M, Zhang J, Wang L, Chen W, Wang Y, Yin X J and An J M 2021 *Photonics Res.* **9** 222
[82] Zhu C X, Chen Z Y, Li Y, *et al.* 2022 *Phys. Rev. Appl.* **17** 064034
[83] Zhang G, Zhao Z, Dai J, Yang S, Fu X and Yang L 2022 *J. Light. Technol.* **40** 2052
[84] Zhang G W, Chen W, Fan-Yuan G J, *et al.* 2022 *Sci. China Inf. Sci.* **65** 200506
[85] Li W, Zhang L, Tan H, *et al.* 2023 *Nat. Photonics* **17** 416
[86] Sax R, Boaron A, Boso G, Atzeni S, Crespi A, Grünenfelder F and Zbinden H 2023 *Photonics Res.* **11** 1007
[87] Zhang G, Haw J Y, Cai H, *et al.* 2019 *Nat. Photonics* **13** 839
[88] Kong L, Li Z, Li C, Cao L, Xing Z, Cao J, Wang Y, Cai X and Zhou X 2020 *Opt. Express* **28** 18449
[89] Dai J, Zhang L, Fu X, Zheng X and Yang L 2020 *Opt. Lett.* **45** 2014
[90] Senellart P, Solomon G and White A 2017 *Nat. Nanotechnol.* **12** 1026
[91] Arakawa Y and Holmes M J 2020 *Appl. Phys. Rev.* **7** 021309
[92] Wang X, Zhu Y, Jin T, Ou W, Ou X and Zhang J 2022 *Chip* **1** 100018
[93] Pelton M, Santori C, Vucković J, Zhang B, Solomon G S, Plant J and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 233602
[94] Englund D, Faraon A, Fushman I, Stoltz N, Petroff P and Vučković J 2007 *Nature* **450** 857
[95] Reitzenstein S and Forchel A 2010 *J. Phys. D: Appl. Phys.* **43** 033001
[96] Ates S, Agha I, Gulinatti A, Rech I, Badolato A and Srinivasan K 2013 *Sci. Rep.* **3** 1397
[97] Schimpf C, Reindl M, Huber D, Lehner B, Covre Da Silva S F, Manna S and Rastelli A 2021 *Sci. Adv.* **7** eabe8905
[98] Cao V, Park J S, Tang M, Zhou T, Seeds A, Chen S and Liu H 2022 *Front. Phys.* **10** 839953
[99] Vajner D A, Rickert L, Gao T, Kaymazlar K and Heindel T 2022 *Adv. Quantum Technol.* **5** 2100116
[100] Rau M, Heindel T, Unsleber S, Braun T, Fischer J, Frick S and Weinfurter H 2014 *New J. Phys.* **16** 043003
[101] Bozzio M, Vyvlecka M, Cosacchi M, Nawrath C, Seidelmann T, Loredo J C and Walther P 2022 *NPJ Quantum Inf.* **8** 104
[102] Gao T, Rickert L, Urban F, Große J, Srocka N, Rodt S and Heindel T 2022 *Appl. Phys. Rev.* **9** 011412
[103] Morrison C L, Pousa R G, Graffitti F, Koong Z X, Barrow P, Stoltz N G and Fedrizzi A 2023 *Nat. Commun.* **14** 3573
[104] Basset F B, Valeri M, Neuwirth J, Polino E, Rota M B, Poderini D and Trotta R 2023 *Quantum Sci. Technol.* **8** 025002
[105] Zhang C, Huang Y F, Liu B H, Li C F and Guo G C 2021 *Adv. Quantum Technol.* **4** 2000132
[106] Euler S, Fitzke E, Nikiforov O, Hofmann D, Dolejsky T and Walther T 2021 *Eur. Phys. J.: Spec. Top.* **230** 1073
[107] Meng J, Xun L C, Zhang C J, Zhang C H and Wang Q 2022 *Acta Phys. Sin.* **71** 170304 (in Chinese)
[108] Chen J P, Zhang C, Liu Y, Jiang C, Zhang W, Hu X L and Pan J W 2020 *Phys. Rev. Lett.* **124** 070501
[109] Hadfield R H 2009 *Nat. Photonics* **3** 696
[110] Hall D, Liu Y H and Lo Y H 2015 *Nanophotonics* **4** 397
[111] Chen B, Wan Y, Xie Z, Huang J, Zhang N, Shang C and Bowers J E 2020 *ACS Photonics* **7** 528
[112] Lee S, Jin X, Jung H, Lewis H, Liu Y, Guo B and Krishna S 2023 *Optica* **10** 147
[113] Sharma V and Bhardwaj A 2022 *International Conference on Numerical Simulation of Optoelectronic Devices (NUSOD)* pp. 17–18
[114] Xu K, Zhou W and Ning Z 2020 *Small* **16** 2003397
[115] García de Arquer F P, Talapin D V, Klimov V I, Arakawa Y, Bayer M and Sargent E H 2021 *Science* **373** eaaz8541
[116] Chen N, Zhang J Q, Mao W B, Li X J, Song L W, Gao L and Yao L B 2022 *Infrared Laser Eng.* **51** 20210821
[117] Charaev I, Bandurin D A, Bollinger A T, *et al.* 2023 *Nat. Nanotechnol.* **18** 343
[118] Chen C, Zhao B, Wang R, *et al.* 2022 *Adv. Mater.* **34** 2206364
[119] Kleiner R, Koelle D, Ludwig F and Clarke J 2004 *Proc. IEEE* **92** 1534
[120] Zadeh I E, Chang J, Los J W, Gyger S, Elshaari A W, Steinhauer S, Dorenbos S N and Zwiller V 2021 *Appl. Phys. Lett.* **118** 190502
[121] Terhaar R, Rödiger J, Häußler M, *et al.* 2023 *Opt. Express* **31** 2675
[122] You L 2020 *Nanophotonics* **9** 2673
[123] Natarajan C M, Tanner M G and Hadfield R H 2012 *Supercond. Sci. Technol.* **25** 063001
[124] Liao S K, Cai W Q, Liu W Y, *et al.* 2017 *Nature* **549** 43
[125] Chen J P, Zhang C, Liu Y, *et al.* 2022 *Phys. Rev. Lett.* **128** 180502
[126] Briegel H J, Dür W, Cirac J I and Zoller P 1998 *Phys. Rev. Lett.* **81** 5932
[127] Pan J W, Bouwmeester D, Weinfurter H and Zeilinger A 1998 *Phys. Rev. Lett.* **80** 3891
[128] Pan J W, Simon C, Brukner Č and Zeilinger A 2001 *Nature* **410** 1067
[129] Bao X H, Reingruber A, Dietrich P, Rui J, Dück A, Strassel T, Li L, Liu N L, Zhao B and Pan J W 2012 *Nat. Phys.* **8** 517
[130] Wei S H, Jing B, Zhang X Y, *et al.* 2022 *Laser & Photonics Rev.* **16** 2100219
[131] Simon C, Afzelius M, Appel J, *et al.* 2010 *Eur. Phys. J. D* **58** 1
[132] Heshami K, England D G, Humphreys P C, Bustard P J, Acosta V M, Nunn J and Sussman B J 2016 *J. Mod. Opt.* **63** 2005
[133] Yin J, Cao Y, Li Y H, *et al.* 2017 *Science* **356** 1140
[134] Yin J, Li Y H, Liao S K, *et al.* 2020 *Nature* **582** 501
[135] Chen Y A, Zhang Q, Chen T Y, *et al.* 2021 *Nature* **589** 214
[136] Liao S K, Cai W Q, Handsteiner J, *et al.* 2018 *Phys. Rev. Lett.* **120** 030501
[137] Liu J, Jiang Q, Ding H, *et al.* 2023 *Sci. China Inf. Sci.* **66** 189402
[138] Liu J Y, Ding H J, Zhang C M, Xie S P and Wang Q 2019 *Phys. Rev. Appl.* **12** 014059
[139] Cao Y, Zhao Y, Zhang J, Wang Q, Niyato D and Hanzo L 2022 *IEEE Netw.* **36** 14