The Evolution of Quantum Secure Direct Communication: On the Road to the Qinternet

Dong Pan, *Member, IEEE*, Gui-Lu Long, *Member, IEEE*, Liuguo Yin, *Senior Member, IEEE,* Yu-Bo Sheng, Dong Ruan, Soon Xin Ng, *Senior Member, IEEE*, Jianhua Lu, *Fellow, IEEE*, Lajos Hanzo, *Life Fellow, IEEE*

Abstract—Communication security has to evolve to a higher plane in the face of the threat from the massive computing power of the emerging quantum computers. Quantum secure direct communication (QSDC) constitutes a promising branch of quantum communication, which is provably secure and overcomes the threat of quantum computing, whilst conveying secret messages directly via the quantum channel. In this survey, we highlight the motivation and the status of QSDC research with special emphasis on its theoretical basis and experimental verification. We will detail the associated point-to-point communication protocols and show how information is protected and transmitted. Finally, we discuss the open challenges as well as the future trends of QSDC networks, emphasizing again that QSDC is not a pure quantum key distribution (QKD) protocol, but a fully-fledged secure communication scheme.

Index Terms—Cryptographic system, entanglement, quantum secure direct communication, quantum communication protocols, quantum communication technologies, quantum network

ABBREVIATIONS

AMZI	Asymmetric Mach-Zehnder Interferometer
Att	Attenuator
BB84	Bennett-Brassard 84
BD	Beam Displacer
BS	Beam Splitter
BSM	Bell-State Measurement
CIR	Circulator
CM	Control Mode
CNOT	Controlled-Not
CV	Continuous Variable
DI	Device-Independent
DL	Delay Line
DL04	Deng-Long 04
DQKD	Deterministic Quantum Key Distribution
DSF	Dispersion Shifted Fiber
DSQC	Deterministic Secure Quantum Communication
DWDM	Dense Wavelength Division Multiplexing
EDFA	Erbium-Doped Fiber Amplifier
ENT	a utility for evaluating random number sequences
EOM	Electro-Optical Modulator
EPC	Electronic Polarization Controller
EPR	Einstein-Podolsky-Rosen
FC	Fiber Coupler
FPGA	Field Programmable Gate Array
FR	Faraday Rotator
FSO	Free-Space Optical
GHZ	Greenberger-Horne-Zeilinger
HWP	Half Wave Plate
ILP	In-Line Polarizer
IM	Intensity Modulator
ISO	Isolator
ITU	International Telecommunication Union
LD	Laser Diode
LO	Local Oscillator
MDI	Measurement Device Independent
MOT	Magneto-Optical Trap
MZI	Mach-Zehnder Interferometer
OAM	Orbital Angular Momentum
ODL	Optical Delay Line
PBS	Polarization Beam Splitter
PC	Polariztion Controller
PM	Phase Modulation
PMCIR	Polarization-Maintaining Circulator
PMFC	Polarization Maintaining Filter Coupler
PPLN	Periodically Poled Lithium Niobate
PQC	Post-Quantum Cryptography
PQKD	Probabilistic Quantum Key Distribution
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QSDC	Quantum Secure Direct Communication
QSS	Quantum Secret Sharing
QT	Quantum Teleportation

Dong Pan and Gui-Lu Long are with the Beijing Academy of Quantum Information Sciences, Beijing 100193, China (e-mail: pandong@baqis.ac.cn; gllong@tsinghua.edu.cn). Dong Ruan and Gui-Lu Long are with the State Key Laboratory of Low-dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China (e-mail: dongruan@tsinghua.edu.cn). Yu-Bo Sheng is with the College of Electronic and Optical Engineering and College of Flexible Electronics (Future Technology), Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (email: shengyb@njupt.edu.cn). Gui-Lu Long, Liuguo Yin and Jianhua Lu are with the Beijing National Research Center for Information Science and Technology, Frontier Science Center for Quantum Information, Beijing 100084, China. Liuguo Yin and Jianhua Lu are with the School of Information Science and Technology, Tsinghua University, Beijing 100084, China (e-mail: {yinlg, lhh-dee}@tsinghua.edu.cn). Soon Xin Ng and Lajos Hanzo are with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, United Kingdom (e-mail: {sxn, lh}@ecs.soton.ac.uk).

Corresponding author: Gui-Lu Long and Lajos Hanzo

Rx	Receiver
SHA	Secure Hash Algorithm
SMZI	Sagnac-Mach-Zehnder Interferometers
SNSPD	Superconducting Nanowire Single Photon Detector
SPD	Single-Photon Detector
SR	Secure Repeater
TCSPC	Time-Correlated Single Photon Counting
TFOC	Triplet Fiber-Optic Collimator
TMSS	Two-Mode Squeezed State
Tx	Transmitter
WDM	Wavelength Division Multiplexing
WP	Wave Plate
ZXFZ	Zhu-Xia-Fan-Zhang

I. INTRODUCTION

The widespread application of communicating computers and mobile devices has changed our daily life beyond recognition. However, retaining the confidentiality of sensitive information is of crucial importance for individuals, enterprises, and governments in our information age. Cryptography is used for maintaining the confidentiality, integrity, and authenticity of information for the authorized users in the face of the malicious activities of third-party adversaries [1]. The operational cryptographic systems tend to rely on carrying out mathematical operations, that are hard to 'decypher' with the aid of state-of-the-art computers. In other words, practical computer science offers what is termed as computational security, which is practically unbreakable within a relatively short space of time by using practical computational resources. However, this conventional cryptography faces challenges imposed by the evolution of ever more powerful computing hardware.

A. Cryptosystems in the quantum world

Asymmetric cryptography[1] primarily relies on excessive-complexity calculations. Such as factoring large prime numbers in Rivest-Shamir-Adleman cryptosystems [3], and solving discrete logarithmic problems. However, at the time of writing, the security of asymmetric cryptography is facing increasing threats from quantum computers [5]–[8], which are capable of factoring large primes. In contrast to classical computers, which tend to rely on Boolean logic and on exploiting that the classical bits can only be in one of two states, namely 0 or 1, the basic variable of quantum computers - namely the qubit - exhibits entirely different properties. It is not confined to the two states, but can exist in their superposition [9]–[11]. Information encoding, storing and processing may be carried out more efficiently in quantum computers than in its classical counterpart, when relying on superimposed quantum states. Explicitly, massive parallel computations are facilitated by quantum computers. Shor's algorithm [12] shows that a quantum computer is capable of efficient factorization of large

---

[1]Asymmetric cryptography is also known as public-key cryptography, which is an approach that uses a pair of related keys called public key and private key to encrypt and decrypt a secret plaintext, respectively, which protects the plaintext from eavesdropping. Correspondingly, symmetric cryptography usually uses the same cryptographic keys for the process of encryption and decryption.

prime numbers and of solving elliptic curve based problems. Similarly, quantum annealing computers are equally powerful [13]. The noisy intermediate-scale quantum computers may challenge the Rivest-Shamir-Adleman cryptosystems by using a hybrid quantum-classical algorithm [14]. Thus, the above-mentioned commonly used cryptographic algorithms are no longer secure in the quantum era [15].

Another well-known algorithm running on a quantum computer is Grover's search algorithm [16]–[20], which is capable of finding a known entry in unsorted databases [21], [22]. Grover's algorithm is eminently suitable for analyzing symmetric encryption systems, such as the Data Encryption Standard and the Advanced Encryption Standard [2], [23]. These cryptographic protocols are generally analyzed using 'brute force' search in the space of all legitimate keys. Specifically, the 56-bit keys of the Data Encryption Standard [2] may be cracked by Grover's algorithm, which will use on the order of hundred million search steps, which is much lower than that of the number of operations to be carried out by a classical computer [24]. Furthermore, the hash function SHA-2 (Secure Hash Algorithm) and SHA-3 [2] are facing the same threats in symmetric encryption systems, since their security relies on the difficulty of finding two different messages that map to the same fixed length. However, Grover's algorithm provides an improvement to this problem [25], although an exponential speed-up in the database search problem is infeasible even for Grover's optimal algorithm [20], [26]–[28]. Cryptologists believe that the Advanced Encryption Standard, SHA-2, and SHA-3 are relatively secure even in a quantum world, but defense mechanisms should nonetheless be conceived to guard against quantum search attacks [29]. It is believed that doubling the key size of a symmetric encryption system or that of the output length of a hash function is urgently needed.

Large-scale quantum computers are expected to have far-reaching influence on the existing cryptographic solutions as reported by the National Institute of Standards and Technology [30]. Table I summarizes these impacts, indicating that the progress of quantum computation tends to threaten the security of modern cryptosystems. Although it has been argued that public-key cryptosystems will only be broken when practical quantum computers have been built for handing thousands quantum bits and can perform thousands of quantum gate operations [31]–[33], it is time for the research community to conceive new cryptosystems, which remain secure in the quantum era.

Ensuring the privacy and security of our communication in the quantum era is the major task of cryptography. There are two different alternative candidate families, namely post-quantum cryptography and quantum cryptography or quantum communication. Post-quantum cryptography is also based on solving challenging mathematical problems, but they rely on other problems than the factoring of large numbers. Instead, they rely on discrete logarithms [34], on lattice-based cryptography [35], and on code-based cryptography [36]. Quantum cryptography or quantum communication is another secure-communication solution that exploits the properties of quantum mechanics itself, which additionally has the capability of detecting eavesdropping.

Cryptosystems	Purposes	Threats	Security
Rivest-Shamir-Adleman	Key establishment and signature	Shor's algorithm	Insecure
Elliptic Curve Digital Signature Algorithm, Elliptic Curve Diffie-Hellman (Elliptic-Curve Cryptography)	Key exchange and signature		Insecure
Digital Signature Algorithm (Finite-Field Cryptography)	Key exchange and signature		Insecure
Diffie-Hellman	Key exchange		Insecure
Advanced Encryption Standard	Symmetric encryption	Grover's algorithm	Relatively secure, but large keys are needed
SHA-2, SHA-3	Hash functions		Relatively secure, but larger output needed

B. From quantum key distribution to quantum secure direct communication

The roots of quantum cryptography or quantum communication can be traced back to the idea of Wiesner in the late 1960s, who proposed the concept of unforgeable quantum money by relying on quantum physics. Similarly to many other radical concepts, he had difficulty in publishing his paper, but finally his much-delayed paper was published in 1983 [37], where he described how information may be stored and conveyed with the aid of polarized photons. In 1984 [38], enlightened by Wiesner's idea, Bennett and Brassard discovered that a pair of communicating parties can generate a cryptographic key over an insecure channel by using appropriately polarized single photons [39]. It is what we know today as the Bennett-Brassard 84 (BB84) quantum key distribution (QKD) protocol, marking the beginning of quantum cryptography. The security of quantum-domain cryptosystems is based on the laws of quantum mechanics rather than on conceiving mathematically challenging problems, which enables the legitimate commu-

nicating parties to have unconditionally secure links. As a benefit, communication systems become secure even in the presence of an eavesdropper who has unlimited computational power, which is an explicit benefit of exploiting the laws of physics.

Hence numerous quantum cryptographic or quantum communication protocols have been proposed, which can be classified into four main branches: quantum key distribution (QKD) [38], quantum teleportation [40], quantum secret sharing [41], and quantum secure direct communication (QSDC) [42], [43], as shown in Fig. 1. Bennett *et al*. [40] introduced quantum teleportation in 1993, showing how to send an unknown quantum state to a remote receiver, with the assistance of classical communication and pre-shared entangled photons. Hillery *et al*. [41] proposed quantum secret sharing in 1999, which is a scheme using entangled quantum states for sharing a random bit among several parties so that no subset of them is able to reconstruct a shared ramdom bit - all of them have to work together [44]. As a further development, in 2000, a QSDC protocol was proposed by Long and Liu [42], [43] for transmitting a predetermined information. QSDC is a beneficial secure communication technique, where secret information can be transmitted directly through the quantum channel without a pre-distributed cryptographic key.
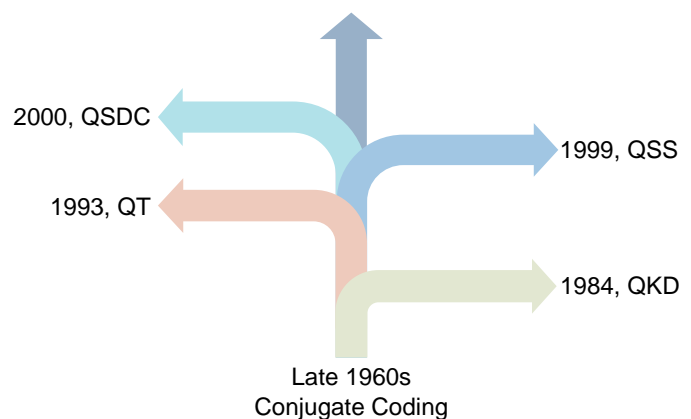

Fig. 1. The main branches of quantum communication. QKD, quantum key distribution; QT, quantum teleportation; QSS, quantum secret sharing; QSDC, quantum secure direct communication.

Fig. 2 portrays the different models of secure communications. Fig. 2 (a) highlights the secure communication structure commonly used at the time of writing. It relies on a pair of channels: the ciphertext channel and the key distribution channel. The transmitter of Alice first transforms a plaintext m into a ciphertext using a secret key k_1 and an encryption algorithm $E(m, k_1)$, and she sends the ciphertext to the receiver - namely to Bob - through the ciphertext channel. Bob uses the secret key k_2 and the decryption algorithm $D(m, k_2)$ to recover the ciphertext for accessing the plaintext m upon receipt [45]. Depending on whether the keys used by the communicating parties in Fig. 2 (a) are the same, the classical secure communication systems can be divided into two broad categories, one being symmetric

cryptosystems, typically with $k_1 = k_2$, while the other being asymmetric cryptosystems for $k_1 \neq k_2$. The ciphertext is communicated through a public channel (ciphertext channel), which is usually insecure. Hence the ciphertext can in principle be intercepted by an eavesdropper, Eve, without detection. The key is distributed through another classical channel, for example, using the asymmetric Rivest-Shamir-Adleman scheme [2], [3]. During the key distribution, the key is also encrypted and the ciphertext representing the encrypted key can also be intercepted by Eve. Key management is at the heart of this secure communication infrastructure, because the cryptographic key must be generated, exchanged, stored, and finally disposed of in a secure manner. It is clear that the adversary, Eve, can readily steal the ciphertext representing the message during its transmission over the public channel, and the ciphertext conveying the key during the key exchange process without being detected by either of the legitimate communication parties. If the key were stolen, Eve would be able to decrypt all the communications between the legitimate users.

At the time of writing, only the one-time-pad has been proven to be perfectly secure [46]. The one-time-pad protocol applies the exclusive OR logic operation between the plaintext message and a pre-shared key to generate the ciphertext. The length of the random key string has to be at least as high as that of the plaintext, and should never be reused. Even though this long key represents a 100% transmission overhead, no other cryptographic protocols relying on shorter keys have been proven to be perfectly secure. Thus, for practical applications, the repeated use of the cryptographic key in a cryptographic system should be avoided, and the length of the key should be set sufficiently high - depending on the computational power available.

The model of an unconditionally secure end-to-end cryptosystem can be constructed by combining QKD and the classical one-time pad, which is shown in Fig. 2 (b). QKD allows two parties to agree on a secret key by exchanging qubits over a quantum channel [38], [47], [48]. An authenticated public channel is also required in support of the associated sifting, parameter estimation, reconciliation, privacy amplification. More explicitly, at least one additional classical information bit is required for each qubit for key *sifting* in QKD. The malicious action of Eve would perturb the state of the qubits, hence the communicating parties can discover Eve through *parameter estimation*, for example estimating quantum bit error rate (QBER). Any potential errors imposed by imperfections of hardware and channel are mitigated by *reconciliation*. Furthermore, *privacy amplification* is used for ensuring that Eve has only negligible information about the final secret key which is achieved by compressing the key [49]. Eve has almost no information about the secret key shared between two legitimate users via QKD. In the following process, the encryption, transmission and decryption of data are identical to the aforementioned classical secure communication systems.

It is observed from Fig. 2 (c) that QSDC constitutes a new secure communication paradigm, which provides a complete confidential near - instantaneous communication solution by
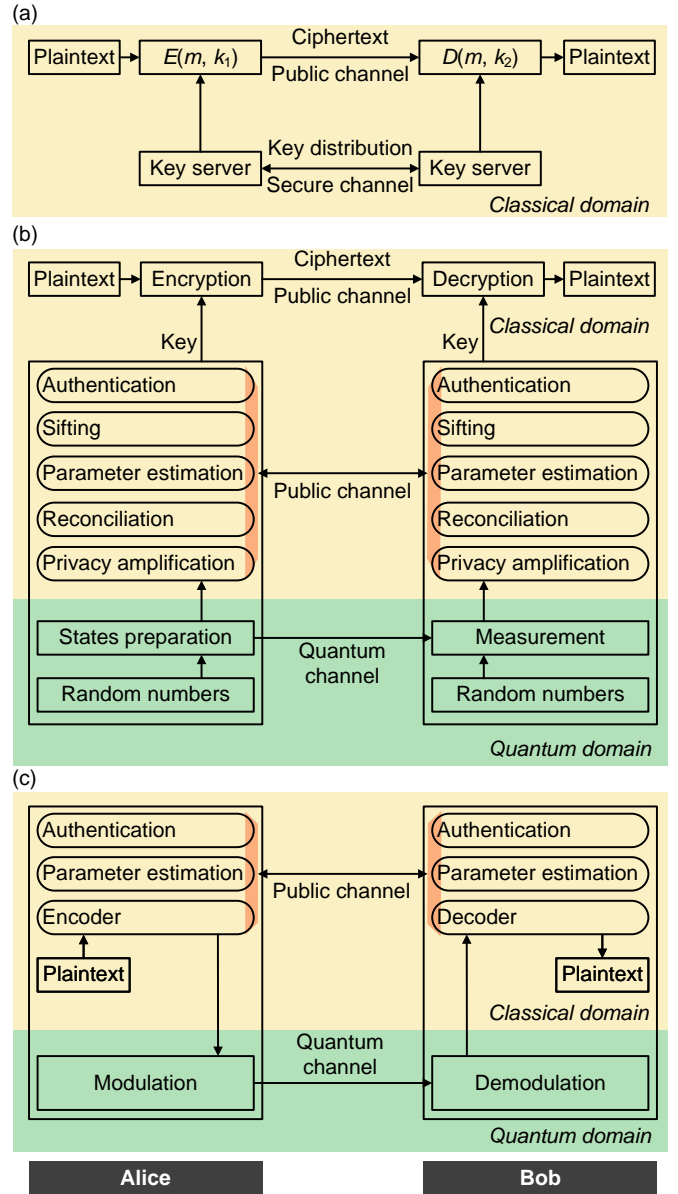

Fig. 2. Different models of communication systems: **(a) classical cryptosystem. (b) QKD system.** Key agreement is carried out by QKD, and information is transmitted via classical communication, the same as in (a); and **(c) QSDC system.** No key distribution, no key management and no ciphertext are required in QSDC.

means of transmitting the actual messages directly over a quantum channel, rather than only managing the negotiation of secret keys, as in QKD. More explicitly, the plaintext messages are mapped to quantum bits at Alice's station before transmitting them to Bob. No additional classical information is required for decoding the data. Therefore, QSDC does not use cryptographic keys, encryption algorithms, and decryption algorithms. Hence it does not have ciphertext either. Nonetheless, a classical authenticated channel is also needed in QSDC, but only for parameter estimation of detecting eavesdroppers as well as for encoder and decoder, which includes the required service communication for forward error correction and secure

coding based on the universal hashing families [50]. The encoder is composed of secure coding encoder, error correction code encoder, and anti-loss encoder, while the decoder includes secure coding decoder, error correction code decoder, and anti-loss decoder [50]. Note that the authentication seen both in Fig. 2 (b) and Fig. 2 (c) can be moved from the classical domain to the quantum domain, which has been an important research topic since its seminal source appeared [51]. This will be discussed in Section IV-C.

In general, the theoretically unbreakable classical cryptosystem developed by Shannon is based on the utilization of secret keys [46]. However, conceiving efficient key management is a challenging task. QKD provides a way for a pair of communicating parties to rely on a common secret key for supporting unconditional security, but only the key establishment takes place in the quantum domain, while the messages are sent by a conventional technique over the classical domain. A common feature of both the classical cryptosystems and of QKD seen in Fig. 2 (a) and (b), is that both of them face a security problem in terms of potential key leakage to malicious insiders and outside hackers. QSDC offers an entirely new way of solving all privacy problems. These benefits accrue from QSDC, because the process of communication takes place in the quantum domain, where the actual messages are transmitted through the quantum channel between end users. Hence no information leakage is possible, as guaranteed by applying the laws of quantum mechanics. Without relying on key encryption, no resources are required at all for key management [52].

C. Article structure

This article is organized as seen in Fig. 3. As we have discussed in Section I, quantum communication guarantees cryptographic security against quantum computation attacks, even when quantum computing becomes the norm in the post-quantum era. QSDC, as one of the prominent branches of quantum communication supports the confidential transmission of information via quantum channels. In Section II, the development of QSDC is surveyed by presenting its milestones. In Section III, we will introduce the fundamental theory and experimental techniques of quantum communication. We will only rely on modest theoretical background for understanding QSDC, followed by some practical guidelines. In Section IV, the salient QSDC protocols are introduced step by step to present the basic principles of QSDC, highlighting how the secret messages can be directly transmitted over the quantum channel. We will consider both point-to-point scenarios and networking issues. Topics such as their cryptographic applications, security proof and recent experimental advances are also covered. The long-term evolution of QSDC, its research directions and challenges are discussed in Section V. Finally, we conclude in Section VI.

II. TWENTY YEARS OF QUANTUM SECURE DIRECT COMMUNICATION

Again, QSDC was originally proposed by Long and Liu in 2000 [42], [43] and in these seminal contributions, it was
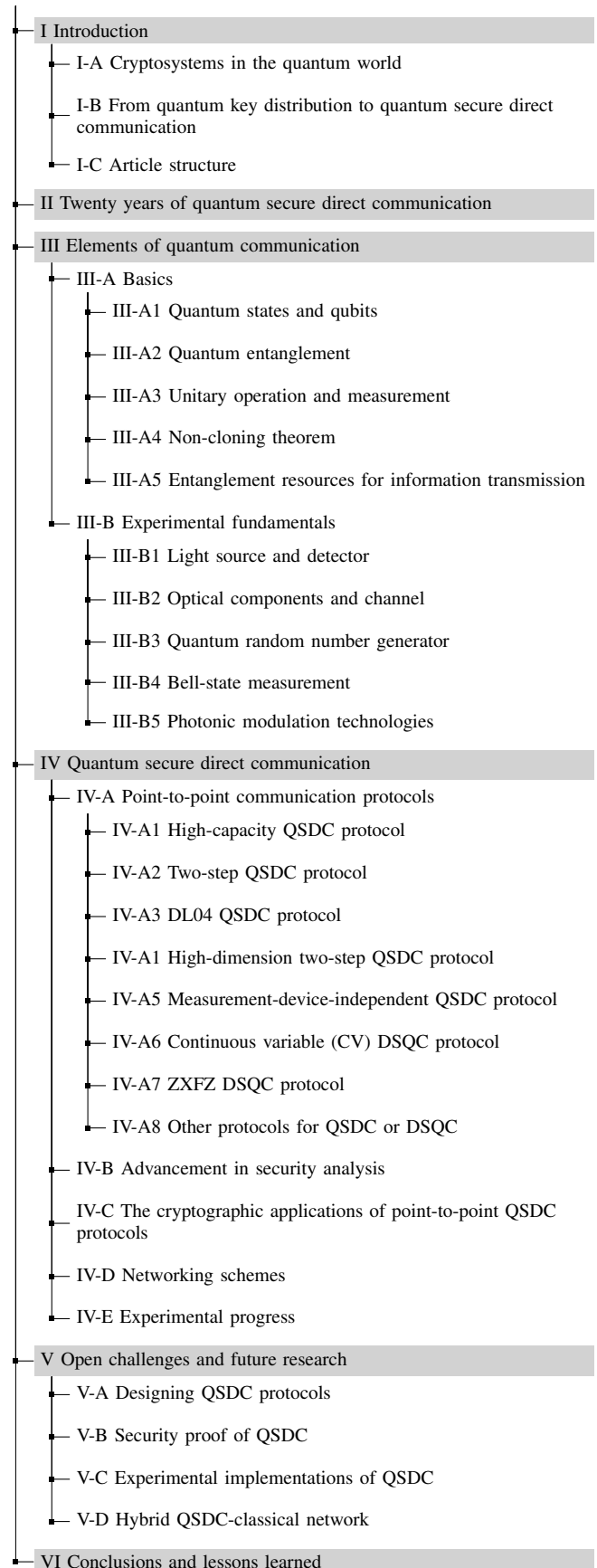
Fig. 3. The structure of this survey article.

pointed out that a key was produced by Alice before transmission took place [42] (versions 1 and 2). The terminology of 'quantum secure direct communication' was introduced for the first time in the two-step QSDC paper [53], where the definition of QSDC was also put forward. Since its conception in 2000, it has evolved into a fully-fledged communications protocol, as seen in Fig. 4 and Fig. 5. The early research of QSDC has been focused on the construction of physical schemes, and many QSDC protocols were invented for different information carriers, such as entangled states [43], [53], single photons [54], and Greenberger-Horne-Zeilinger (GHZ) states [55], [56]. Recently significant breakthroughs have been made in the experimental demonstration of QSDC protocols [57], [58], which paved the way for their practical application [59], [60].

The lack of practical quantum memory has been a serious obstacle for the evolution of quantum communication, because the employment of relaying requires memory. Hence, practical QKD has remained confined to intra-city distances. For intercity applications of QKD, so-called trusted relays are used as temporary replacements for perfectly reliable quantum repeaters. Satellite relays provide a promising technique for global quantum key distribution [99], [100]. But for QSDC even over short distances, quantum memory has remained indispensable, until quite recently, because the associated block-based transmission requires the quantum states to be stored before their security is assured. However, quite recently, a quantum-memory-free QSDC protocol [45], [80], [85] was designed, where the plaintext was encrypted using a pre-shared random key and then the ciphertext was used to distill secret keys for encrypting later message blocks. This development has finally made QSDC applicable for intercity distances [89]. Furthermore, combining QSDC and post-quantum cryptography enables the construction of a secure repeater, which can establish a large-scale quantum communication network using existing technology [91]. This approach avoids the security risks that arise from relying on trusted relays.

Many QKD protocols [38], [47], [48], [101] have a probabilistic nature, since an uncontrolled key sequence is established between two users, who randomly choose their so-called rectilinear or diagonal quantum basis to measure the qubits and the key is produced on the basis of random instances, where the pair of communicating users choose the same bases on a probabilistic basis. Here we emphasize that this probabilistic random sequence should NOT contain any meaningful information, just a sequence of random bits, not a key. It is essentially used for eavesdropper detection and if an eavesdopper is detected during its transmission, this random sequence can be discarded. There are several examples of deterministic quantum key distribution (DQKD) protocols. Briefly, DQKD is a protocol designed for handing over the above-mentioned deterministic key to the intended receiver and no basis reconciliation is required for decoding. To exemplify the DQKD protocols, Goldenberg and Vaidman proposed such a scheme in 1995 using a Mach-Zehnder interferometer [102], while Boström *et al*. [103] conceived a QKD protocol using EPR pairs, which has the fond connotation of the Ping-Pong protocol. The two-way QKD protocols

of [104]–[106] are also prominent examples of DQKD. An essential feature of QKD is that the transmitted data may become fully or partially leaked to Eve. Fortunately, QKD is capable of detecting eavesdropping, but it cannot prevent the leakage of the transmitted data. This is why QKD has to resort to the transmission of meaningless random sequences for Eve-detection, and again, if eavesdropping is detected, the transmitted data will be discarded. It is apparent that the Ping-Pong protocol [103] cannot convey secret messages over the quantum channel due to its QKD nature. Although the original Ping-pong protocol of [103] is insecure even for QKD, later it has been rendered secure and has been generalized to numerous applications [107]–[111]. As a result, a simple way of distinguishing a QSDC protocol from a DQKD protocol [112] is to check whether the transmitted data would or would not be leaked to Eve. For QSDC, the transmitted confidential information would not be leaked, because the eavesdropper would only be able to acquire completely random information, whereas the data transmitted in DQKD would be partially or completely leaked to Eve. It is worth pointing out that classical communications cannot detect eavesdropping.

There is a particular variant of DQKD, which is also mistakenly referred to as QSDC by some authors. To elaborate a little further, normally QKD is performed first to establish a shared key between Alice and Bob. The key is then used for encrypting the message into the related ciphertext, which is then transmitted through a classical channel [45]. For DQKD, the procedure can be appropriately modified, where Alice can choose a random sequence as her key to encrypt her message into the ciphertext, which is then transmitted to Bob through a quantum channel. Then they assess the grade of security during the ciphertext transmission, for example by estimating the error rate. If they are sure that the security has not been compromised, implying that tempering by Eve has not affected the ciphertext, then Alice sends the key through a classical channel to Bob. This variant of DQKD is usually termed as deterministic secure quantum communication (DSQC) [112], [113]. A simple rule to judge whether a protocol belongs to the family of DSQC is to ask the question: is there any need for classical communication for announcing the key rather than for basis choice reconciliation and eavesdropping detection in the protocol? If the answer is affirmative, we can conclude that it is indeed a DSQC protocol. In the DSQC protocol the receiver cannot directly read the secret message, unless it receives one bit of additional classical information from the transmitter for reading the secret message. In 2001, Beige *et al*. [114] proposed a DSQC protocol, which also needs additional classical communication. Their protocol became insecure, when an adversary acquired the secret information by applying a so-called quantum non-demolition measurement. As a further advance, DSQC has also been extended to entanglement distribution [115], [116] and to continuous variable based implementations [117]. Pan *et al*. [50] identified the essential characteristics that a point-to-point QSDC protocol should possess. If a protocol fails to satisfy these criterias, but nevertheless transmits information directly through a quantum channel, it is referred to as a quasi-QSDC protocol in their work.
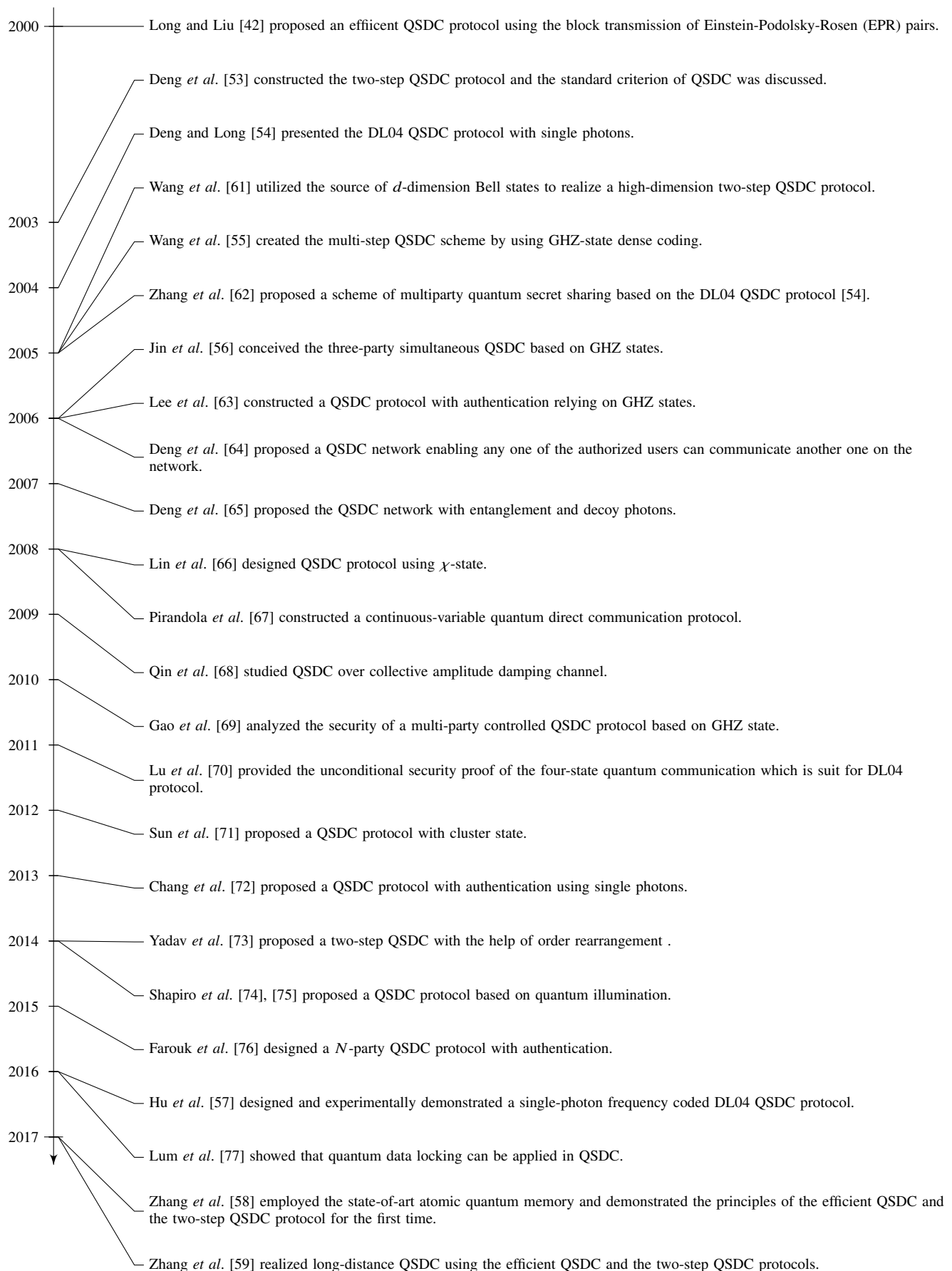
2000 — Long and Liu [42] proposed an effiicent QSDC protocol using the block transmission of Einstein-Podolsky-Rosen (EPR) pairs.

Deng *et al*. [53] constructed the two-step QSDC protocol and the standard criterion of QSDC was discussed.

Deng and Long [54] presented the DL04 QSDC protocol with single photons.

Wang *et al*. [61] utilized the source of d-dimension Bell states to realize a high-dimension two-step QSDC protocol.

2003

Wang *et al*. [55] created the multi-step QSDC scheme by using GHZ-state dense coding.

2004

Zhang *et al*. [62] proposed a scheme of multiparty quantum secret sharing based on the DL04 QSDC protocol [54].

2005

Jin *et al*. [56] conceived the three-party simultaneous QSDC based on GHZ states.

Lee *et al*. [63] constructed a QSDC protocol with authentication relying on GHZ states.

2006

Deng *et al*. [64] proposed a QSDC network enabling any one of the authorized users can communicate another one on the network.

2007

Deng *et al*. [65] proposed the QSDC network with entanglement and decoy photons.

2008

Lin *et al*. [66] designed QSDC protocol using χ-state.

2009

Pirandola *et al*. [67] constructed a continuous-variable quantum direct communication protocol.

2010

Qin *et al*. [68] studied QSDC over collective amplitude damping channel.

Gao *et al*. [69] analyzed the security of a multi-party controlled QSDC protocol based on GHZ state.

2011

Lu *et al*. [70] provided the unconditional security proof of the four-state quantum communication which is suit for DL04 protocol.

2012

Sun *et al*. [71] proposed a QSDC protocol with cluster state.

2013

Chang *et al*. [72] proposed a QSDC protocol with authentication using single photons.

2014

Yadav *et al*. [73] proposed a two-step QSDC with the help of order rearrangement .

Shapiro *et al*. [74], [75] proposed a QSDC protocol based on quantum illumination.

2015

Farouk *et al*. [76] designed a N-party QSDC protocol with authentication.

2016

Hu *et al*. [57] designed and experimentally demonstrated a single-photon frequency coded DL04 QSDC protocol.

2017

Lum *et al*. [77] showed that quantum data locking can be applied in QSDC.

Zhang *et al*. [58] employed the state-of-art atomic quantum memory and demonstrated the principles of the efficient QSDC and the two-step QSDC protocol for the first time.

Zhang *et al*. [59] realized long-distance QSDC using the efficient QSDC and the two-step QSDC protocols.

Fig. 4. Timeline of important milestones in quantum secure direct communication.

2018 — Zhou *et al*. [78] reported a measurement-device-independent (MDI) QSDC scheme of single photons.

Niu *et al*. proposed MDI QSDC scheme of EPR pairs [79].

Sun *et al*. [80] designed a QSDC protocol that does not require quantum mempery, overcoming a bottleneck obstacle of practical QSDC.

Qi *et al*. [60] implemented a practical QSDC system with the security analysis of the Wyner wiretap channel theory.

2019 — Shapiro *et al*. [81] proposed that the quantum low probability of perception protocol can be viewed as an example of QSDC.

Zhou *et al*. [82] proposed the device-independent QSDC protocol.

Massa *et al*. [83] experimentally demonstrated two-way QSDC [84].

2020 — Sun *et al*. [85] proposed a quantum-memory-free DL04 QSDC protocol using coding theory.

Pan *et al*. [86] reported a free-space QSDC.

Qi *et al*. [87] demonstrated a 15-user QSDC network based on entanglement distribution.

Vázquez-Castro *et al*. [88] utilized a quantum version of on-off keying modulation to directly transmit confidential information over a quantum channel.

2021 — Zhang *et al*. [89] declared breakthrough in 100 km fiber-based QSDC.

Wu *et al*. [90] proved the security of QSDC considering the finite-size effect.

Long *et al*. [91] proposed a secure repeater network and experimental demonstrated it.

2022 — Liu *et al*. [92] reported a proof-of-principle QSDC experiment over a 5 km fiber channel.

Panda *et al*. [93] presented a QSDC protocol by utilizing quantum walks on orbital angular momentum (OAM) states.

Zhou *et al*. [94] designed a device-independent (DI) QSDC scheme relying on single-photon sources.

Li *et al*. [95], [96] propounded a single-photon-memory MDI QSDC protocol and deduced its secrecy capacity. Sun *et al*. [97] relaxed the requirement for state preparation in MDI QSDC and determined the practical secrecy capacity of the protocol by integrating customized decoy-state methods.

2023 — Xu *et al*. [98] proposed a quantum blockchain scheme relying on QSDC.

Fig. 5. Timeline of important milestones in quantum secure direct communication.

Thus based on the above paragraph, it should be born in mind that the above statements regarding QSDC are not applicable to the DSQC family, whose members are essentially of DQKD nature. The nature of some of the popular communication protocols is summarized at a glance in Table II. It is clear that only QSDC is capable of avoiding the leakage of transmitted data, when Eve intercepts the transmission.

III. ELEMENTS OF QUANTUM COMMUNICATION

A. Basics

1) Quantum states and qubits: In quantum mechanics, the state of a physical system is described by a state vector in the Hilbert space $\mathscr{H}$ [118]. The so-called 'ket' notation describing a vector in the complex number space $\mathbb{C}^n$ representing a pure

TABLE II
COMPARISONS OF DIFFERENT COMMUNICATION PATTERNS. PQKD, PROBABILISTIC QKD; LEAKAGE, LEAKAGE OF TRANSMITTED DATA IF EVE INTERCEPTS.

Protocol	Deterministic	Eve detection	Leakage	Examples
Classical communication	Yes	No	Yes	Any
PQKD	No	Yes	Yes	[38]
DQKD	Yes	Yes	Yes	[102]
DSQC	Yes	Yes	Yes	[114]
QSDC	Yes	Yes	No	[42]

quantum state is mathematically denoted as

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix}, \tag{1}$$

where the symbol '$|\cdot\rangle$' is the Dirac notation [119] of a symbol ψ for a vector and we have $\alpha_n \in \mathbb{C}^n$ associated with $\sum_{i=1}^{n} |\alpha_i|^2 = 1$. The 'ket' notation simply represents the second half of the word 'Dirac-ket'. This unit vector can also be written in the form of the superposition $|\psi\rangle = \sum_{i=1}^{n} \alpha_i |\psi_i\rangle$, where α_i is the amplitude of the vector in an orthonormal basis $|\psi_i\rangle$. The conjugate transpose of $|\psi\rangle$ is $\langle\psi|$, which is called a bra vector, formulated as:

$$\langle\psi| = (|\psi\rangle)^{\dagger} = \begin{pmatrix} \alpha_1^* & \alpha_2^* & \alpha_3^* & \cdots & \alpha_n^* \end{pmatrix}. \tag{2}$$

The combined bra and ket notations $\langle\psi|\phi\rangle$, and $|\psi\rangle\langle\phi|$ represent the inner product and the outer product of the vectors, respectively. But in some cases a quantum system cannot be described by a single vector, it is rather described by a probability distribution, which may be in the state $|\phi_i\rangle$ with probability p_i. Such a quantum system is said to be in a mixed state, which corresponds to a probabilistic mixture of pure quantum states. A pure state is a particular case of a mixed state associated with $p_i = 1$ and $p_j = 0$ ($i \neq j$). A commonly adopted way of describing mixed states in quantum mechanics is to use the so-called density matrix, which is the weighted sum of pure states in the form of [120], [121]

$$\rho = \sum_{i=1}^{N} p_i |\phi_i\rangle\langle\phi_i|. \tag{3}$$

The basic element of quantum information processing is a qubit formulated in the two-dimensional Hilbert space $\mathbb{C}^2$ as [9],

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \tag{4}$$

where $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are the computational basis states, while α and β are complex numbers associated with $|\alpha|^2 + |\beta|^2 = 1$. The classical bits either assume a logical '0' or '1' value, while a qubit may be found in an arbitrary superposition of the two basis states $|0\rangle$ and $|1\rangle$. In physically tangible terms this superposition may be interpreted as a coin spinning in a box in the equi-probable superposition of 'head

and tail'. But when we lift the lid of the box and 'observe' the coin, this superposition of states 'collapses' back into one of the basis states of 'head or tail'. If the amplitudes are parameterized by $\alpha = \cos\left(\frac{\theta}{2}\right)$ and $\beta = e^{i\varphi}\sin\left(\frac{\theta}{2}\right)$, then a particularly useful form is

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle. \tag{5}$$

The state of a qubit can be geometrically represented by a vector in a Bloch sphere, shown in Fig. 6, where θ ($0 \leqslant \theta \leqslant \pi$) and φ ($0 \leqslant \varphi < 2\pi$), correspond to the polar angle and azimuthal angle, respectively. A pure qubit state can be represented by a point on the surface of the Bloch sphere, while mixed states are the points inside the Bloch sphere. The basis state $|0\rangle$ is located at the North pole, while $|1\rangle$ at the South pole. Observe from Fig. 6 that in addition to the $\{|0\rangle, |1\rangle\}$ basis, two other important states are,

$$|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$$
$$|-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right), \tag{6}$$

which are the eigenstates of σ_x, and the states

$$|R\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right), \quad |L\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - i|1\rangle\right), \tag{7}$$

which are the eigenstates of σ_y.

2) Quantum entanglement: The concept of entanglement originates from the influential argument of Einstein *et al.* [122] intended to question the completeness of quantum mechanics. Here, let us define it by using the modern terminology of qubits. Let us consider a composite Hilbert space $\mathscr{H}_A \otimes \mathscr{H}_B$. Then there is a state of the composite system, which cannot be written as a tensor product[2] of the states of the individual subsystems,

$$|\psi\rangle_{AB} \neq |\psi\rangle_A \otimes |\psi\rangle_B, \quad \forall |\psi\rangle_A \in \mathscr{H}_A, \quad \forall |\psi\rangle_B \in \mathscr{H}_B. \tag{8}$$

Such a state is called an entangled state. For example, the most commonly used entangled states are the four Bell states, also

---

[2]The tensor product $|\psi\rangle_A \otimes |\psi\rangle_B$ is often abbreviated to $|\psi\rangle_A |\psi\rangle_B$ or even more compactly as $|\psi_A \psi_B\rangle$.
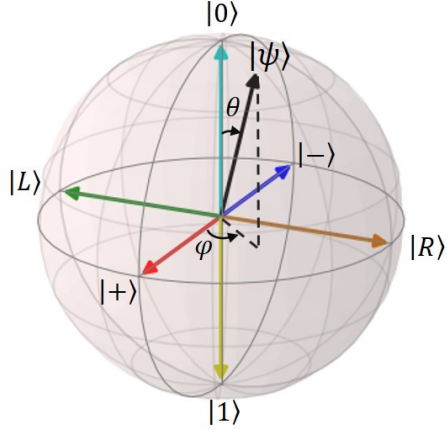
Fig. 6. Visualization of qubit states in the Bloch sphere.

their physical distance. Having said that, the speed of light cannot be exceeded, because before this 'spooky action' can take place, some preparatory classical domain operations are required, which do obey the speed of light.

3) Unitary operation and measurement: A quantum system in the process of quantum communication usually undergoes unitary operations and measurement, which carry out information/data encoding and decoding, as well as the observation of the result, respectively. The terminologies of 'observation' and 'measurement' are used as synonyms and upon measurement a qubit could be converted into a classical bit. A unitary operation is represented by a complex-valued matrix U that satisfies the condition of $U^\dagger U = I$, and transforms a state vector into another state vector, which is formulated as:

$$|\psi'\rangle = U|\psi\rangle. \tag{12}$$

It is also often written in terms of a sum-of-outer-products given by

$$U = \sum_{ij} M_{ij}|\psi_i\rangle\langle\psi_j|, \tag{13}$$

where $M_{ij} = \langle\psi_i|U|\psi_j\rangle$ is the matrix element of U between the two basis states.

The most commonly used unitary operations of the quantum cryptographic protocols, which transform single-qubit states are as follows,

$$U_0 = I = |0\rangle\langle0| + |1\rangle\langle1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$U_1 = Z = \sigma_z = |0\rangle\langle0| - |1\rangle\langle1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$U_2 = X = \sigma_x = |1\rangle\langle0| + |0\rangle\langle1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$U_3 = i\sigma_y = |0\rangle\langle1| - |1\rangle\langle0| = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$H = \frac{X+Z}{\sqrt{2}} = |+\rangle\langle0| + |-\rangle\langle1| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{14}$$

They play quite different roles. Specifically, U_0 is an identity transform that has no effect on the state, while U_1 represents the phase flip of $|0\rangle \xrightarrow{U_1} |0\rangle$, $|1\rangle \xrightarrow{U_1} -|1\rangle$. Furthermore, U_2 is the bit-flip, $|0\rangle \xrightarrow{U_2} |1\rangle$, $|1\rangle \xrightarrow{U_2} |0\rangle$ and finally, U_3 represents a simultaneous bit-flip and phase-flip, $|1\rangle \xrightarrow{U_3} |0\rangle$, $|0\rangle \xrightarrow{U_3} -|1\rangle$. Finally, H is the Hadamard transformation, which may also be represented as, $|0\rangle \xrightarrow{H} |+\rangle \xrightarrow{H} |0\rangle$, $|1\rangle \xrightarrow{H} |-\rangle \xrightarrow{H} |1\rangle$. The effects of these unitary operations can be conveniently illustrated on the Bloch Sphere of Fig. 7 for better understanding.

In entanglement-based quantum crytography, we can apply any of the operations U_0, U_1, U_2, or U_3 to one of the particles of an EPR pair while keeping the other particle untouched, the original Bell state can be turned into another Bell state. The transformation between them is described in Table III.

Quantum measurements are described by a collection of measurement operators $\{M_m\}$ that act on the quantum state, and the index m identifies one of the legitimate outcomes of the measurement. If the system to be measured is in state $|\psi\rangle$,

termed as the EPR pairs or EPR states,

$$|\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B\right),$$

$$|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right),$$

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right),$$

$$|\phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B\right). \tag{9}$$

We have no way of expressing the four Bell states as tensor products. By contrast, the state $\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B\right)$ is a separable state, because it can be written in form of the tensor product, $|0\rangle_A \otimes \frac{1}{\sqrt{2}}\left(|0\rangle_B + |1\rangle_B\right)$.

Now, the family of entangled states plays a key role both in the protocol design and in the security proof of quantum cryptography. Apart from the Bell states of Eq. (9), other members of the entangled state family include the GHZ states [123], [124] defined as:

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|00\cdots0\rangle \pm |11\cdots1\rangle\right), \tag{10}$$

and the W-state [125]

$$|\text{W}\rangle = \frac{1}{\sqrt{N}}(|00\cdots01\rangle + |00\cdots10\rangle + \cdots$$
$$+ |01\cdots00\rangle + |10\cdots00\rangle). \tag{11}$$

They have been widely used in quantum communication protocols. Loosely speaking, entangled states exhibit 'perfect' correlation, which is consistent with the nature of quantum communication, namely sending messages from the transmitter to the receiver is to correlate them [126]. Anecdotally, Einstein referred to the phenomenon of entanglement as a 'spooky action at a distance', because flipping one of the entangled bits instantaneously flips its entangled pair, regardless of
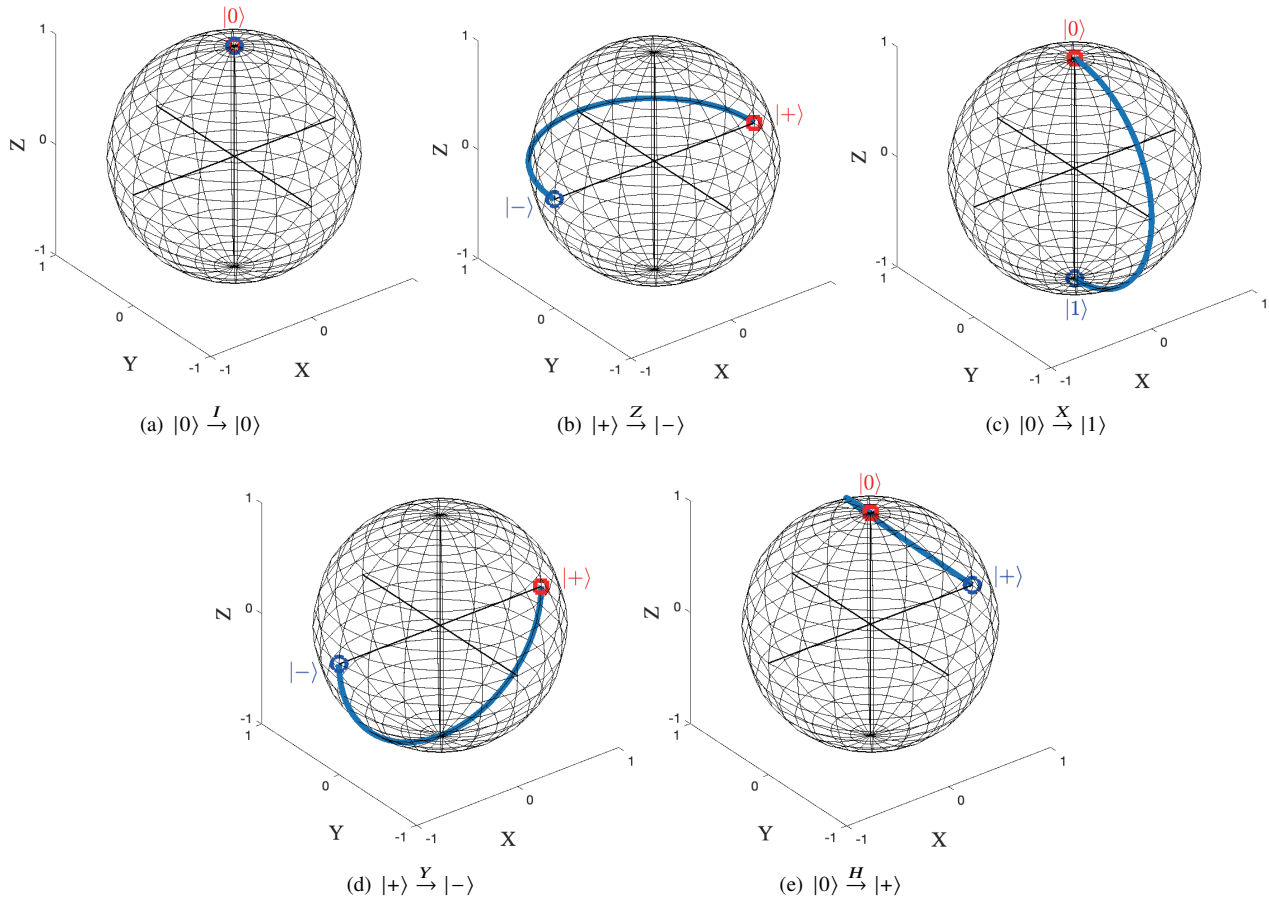
Fig. 7. The trajectory examples of quantum state under the specific unitary operation on the Bloch sphere. The red squares represent the initial states and the blue circles represent the final states, while the blue solid lines are the trajectories.

TABLE III
THE RELATIONSHIP BETWEEN THE INITIAL BELL STATES, THE FINAL
BELL STATES AND THE CORRESPONDING UNITARY OPERATOR.

Unitary operation	Initial states			
	$|\psi^+\rangle$	$|\psi^-\rangle$	$|\phi^+\rangle$	$|\phi^-\rangle$
$U_0 = I$	$|\psi^+\rangle$	$|\psi^-\rangle$	$|\phi^+\rangle$	$|\phi^-\rangle$
$U_1 = \sigma_z$	$|\psi^-\rangle$	$|\psi^+\rangle$	$|\phi^-\rangle$	$|\phi^+\rangle$
$U_1 = \sigma_x$	$|\phi^+\rangle$	$-|\phi^-\rangle$	$|\psi^+\rangle$	$-|\psi^-\rangle$
$U_3 = i\sigma_y$	$|\phi^-\rangle$	$-|\phi^+\rangle$	$|\psi^-\rangle$	$-|\psi^+\rangle$

then the probability of obtainng the result m is given by

$$p\left(m \mid |\psi\rangle\right) = \langle\psi|M_m^\dagger M_m|\psi\rangle. \quad (15)$$

After measurement, the system collapses to the state

$$|\psi'\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}. \quad (16)$$

The set of measurement operators $\{M_m\}$ must satisfy the completeness relationship of $\sum_m M_m^\dagger M_m = I$, which results from the fact that the sum of the probabilities $p\left(m \mid |\psi\rangle\right)$ is equal to 1.

When we invoke a measurement in the process of quantum communication, we always use sets composed of orthonormal computational bases and the measurement operator is constructed from them. There is a very useful rule of thumb: the measurement operators can be produced in the form of

$$M_m = |\psi_m\rangle\langle\psi_m|, \quad (17)$$

according to a set of orthonormal states $\{|\psi_m\rangle\}$ [118]. This is a special kind of projective measurement, which is also commonly referred to as the von Neumann measurement [9]. For example, when aiming for determining whether a qubit is in state $|0\rangle$ or $|1\rangle$, the corresponding measurement operators are $\{M_0 = |0\rangle\langle0|, M_1 = |1\rangle\langle1|\}$, respectively. According to Eq. (15), the result $|0\rangle$ will appear with the probability of $p(0 \mid |\psi\rangle) = (\alpha^*\langle0| + \beta^*\langle1|) |0\rangle\langle0| (\alpha|0\rangle + \beta|1\rangle) = |\alpha|^2$, while the result $|1\rangle$ will appear with probability $|\beta|^2$. The state will collapse to the new state of either $|0\rangle$ or $|1\rangle$.

The positive-operator-valued measurement defined in [9] is another commonly used notion in quantum information processing, which represents a generalized measurement, because the operators are not necessarily orthogonal. It is described by a set of positive operators $\{E_m\}$, formulated as,

$$E_m = M_m^\dagger M_m, \quad (18)$$

which satisfy the completeness condition of $\sum_m E_m = I$. Therefore, we only care about the probability of getting the

specific results m, which is given by

$$p\,(m\,|\,|\psi\rangle) = \langle\psi|E_m|\psi\rangle, \tag{19}$$

because we are unable to predict the post-measurement state of the system after carrying out the positive-operator-valued measurement. Fortunately, the post-measurement state is of limited interest in quantum information processing, since most applications are more concerned with the measurement outcomes and with their specific probabilities.

Let us briefly consider an example of using the positive-operator-valued measurement as a means of distinguishing a pair of nonorthogonal states $|0\rangle$ and $|+\rangle$. We start by constructing a positive-operator-valued measurement containing three operators $E_1 = \frac{\sqrt{2}}{1+\sqrt{2}}|1\rangle\langle1|$, $E_2 = \frac{\sqrt{2}}{1+\sqrt{2}}\frac{(|0\rangle-|1\rangle)(\langle0|-\langle1|)}{2}$, and $E_3 = I - E_1 - E_2$. Then $|0\rangle$ is easy to distinguish from $|+\rangle$ with the aid of the measurement outcomes of $\langle0|E_1|0\rangle = \langle+|E_2|+\rangle = 0$ and $\langle+|E_1|+\rangle$ as well as $\langle0|E_2|0\rangle$ being nozero: upon measuring a state $|\psi\rangle$ with the aid of E_1 and E_2, the result will be state $|0\rangle$ if the results are $\langle\psi|E_1|\psi\rangle = 0$ and $\langle\psi|E_2|\psi\rangle$ nonzero. By contrast, it will be state $|+\rangle$, if the result of $\langle\psi|E_1|\psi\rangle$ is nonzero and $\langle\psi|E_2|\psi\rangle = 0$. To elaborate, if we carry out the positive-operator-valued measurement and obtain a result for E_1, the outcome is state $|+\rangle$, while it will be state $|0\rangle$ if the result is obtained in E_2. Finally, E_3 is needed due to the completeness condition, although the mesurement result of E_3 is useless: both $\langle0|E_3|0\rangle$ and $\langle+|E_3|+\rangle$ are nozero, hence we cannot tell whether the state is $|0\rangle$ or $|+\rangle$ from the E_3 positive-operator-valued measurement. Note that the physical laws tell us that nonorthogonal quantum states cannot be distinguished with perfect reliability, but it is possible to distinguish the states some fraction of the time [127]–[129]. Therefore, both the legitimate users [130] and the attackers [131] can employ this tool for exacting information. By applying positive-operator-valued measurements to quantum cryptography, the security of QKD was analyzed in the face of certain eavedropping strategies related to positive-operator-valued measurement [132]–[134], and the maximum attainable information rate was calculated in [135], [136].

4) No-cloning theorem: In contrast to classical communication where information can in principle be copied perfectly without limits, an eavesdropper is incapable of copying quantum signals in quantum cryptography, thanks to the no-cloning theorem [137]–[139].

Let us assume that there exists a quantum cloning device capable of perfectly duplicating the arbitrary quantum states $|\psi\rangle$ and $|\phi\rangle$, where the cloning can be realized by a unitary operation

$$\begin{aligned}U_C\,(|\psi\rangle|0\rangle) &= |\psi\rangle|\psi\rangle, \\ U_C\,(|\phi\rangle|0\rangle) &= |\phi\rangle|\phi\rangle,\end{aligned} \tag{20}$$

where $|0\rangle$ is the initial state of the cloning device. The inner product between the right-hand sides of Eq. (20) is

$$\langle\phi|\langle\phi|\psi\rangle|\psi\rangle = \langle\phi|\psi\rangle\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2, \tag{21}$$

while for the left-hand side we obtain

$$\langle\phi|\langle0|U_C^\dagger U_C|\psi\rangle|0\rangle = \langle\phi|\psi\rangle\langle0|0\rangle = \langle\phi|\psi\rangle, \tag{22}$$

where the relationships of $U_C^\dagger U_C = I$ and $\langle0|0\rangle=1$ are exploited. Finally, we arrive at:

$$\langle\phi|\psi\rangle\,(\langle\phi|\psi\rangle - 1) = 0, \tag{23}$$

which implies that a cloning device can only clone $|\phi\rangle$ that is orthogonal to $|\psi\rangle$.

As a conclusion, it is claimed in [137] that unknown quantum states cannot be cloned (copied) perfectly. This argument has also been extended to mixed states in [140]. However approximate cloning, or probabilistic cloning is possible for an arbitrary state [141]–[146]. Therefore, one cannot gain full information about an unknown quantum state without perturbing it.

5) Entanglement resources for information transmission: Superdense coding [147], quantum teleportation [40], [148], and entanglement swapping [149] are important quantum-domain operations that rely on EPR pairs. These quantum techniques can be employed for the design of quantum communication protocols as exemplified in [150]–[155]. We will therefore focus our attention on the basic principles of these approaches for highlighting some of the pivotal protocols. Entanglement purification is another salient quantum communications technique conceived for mitigating the degradation of entanglement, thereby guaranteeing security.

Fig. 8 graphically illustrates *superdense coding*, as an effective means of communications, which conveys two bits of classical information from Alice to Bob by sending only a single qubit. Let us assume that the EPR pair of Fig. 8 has
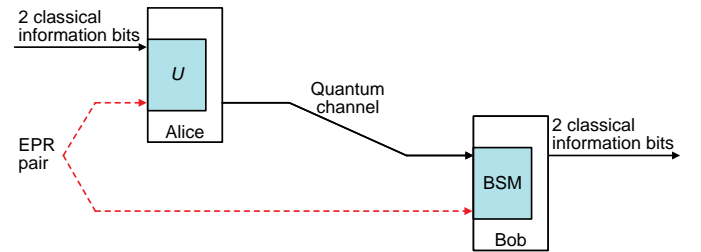

Fig. 8. Communication model of superdense coding, where the dashed line indicates entanglement and BSM represents the Bell-state measurement.

been shared by Alice and Bob, so both of them hold one of the particles representing the state $|\psi^-\rangle$. Table III suggests that all four Bell states may be gleaned from either one of them by applying only local operations to one of the particles of Bell states. Consequently, Alice is able to encode two bits of classical information onto a single qubit by applying the unitary operator U of Fig. 8 according to the following coding rules:

$$\begin{aligned}|\psi^-\rangle_{AB} &\xrightarrow[U_0=I]{00} |\psi^-\rangle_{AB}, \\ |\psi^-\rangle_{AB} &\xrightarrow[U_1=\sigma_z]{01} |\psi^+\rangle_{AB}, \\ |\psi^-\rangle_{AB} &\xrightarrow[U_2=\sigma_x]{10} -|\phi^-\rangle_{AB}, \\ |\psi^-\rangle_{AB} &\xrightarrow[U_1=i\sigma_y]{11} -|\phi^+\rangle_{AB}.\end{aligned} \tag{24}$$

She then sends her qubit to Bob through the quantum channel of Fig. 8 and Bob combines the two qubits of the EPR pair considered to perform Bell-state measurement (BSM). The pair of original classical bits of Fig. 8 are then reconstructed deterministically[3], because the measurement result will unambiguously reveal the state.
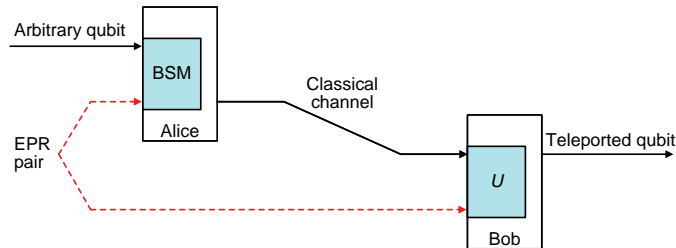

Fig. 9. Principle of quantum teleportation.

For *quantum teleportation*, the aim is to faithfully deliver an arbitrary qubit $|\psi\rangle_0 = \alpha|0\rangle + \beta|1\rangle$ between two distant parties, as seen in Fig. 9. As in the superdense coding scenario of Fig. 8, an EPR pair must be shared by Alice and Bob in advance. Without loss of generality, we assume that the shared EPR state is $|\psi^-\rangle_{AB} = 1/\sqrt{2}\,(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$. So the resultant 3-qubit state here is initially $|\psi\rangle_0|\psi^-\rangle_{AB}$, which can be regrouped and written as

$$
\begin{aligned}
|\psi\rangle_0|\psi^-\rangle_{AB} &= \frac{1}{2}\big[|\psi^-\rangle_{0A}\,(-\alpha|0\rangle - \beta|1\rangle)\big)_B \\
&+ |\psi^+\rangle_{0A}\,(-\alpha|0\rangle + \beta|1\rangle))_B \\
&+ |\phi^-\rangle_{0A}\,(\alpha|1\rangle + \beta|0\rangle))_B \\
&+ |\phi^+\rangle_{0A}\,(\alpha|1\rangle - \beta|0\rangle))_B\big].
\end{aligned}
\tag{25}
$$

If Alice performs a BSM on qubits 0 and A at her side, the measurement will project these two qubits onto one of the four Bell states of Table IV with an equal probability of 1/4. The measurement outcome is then sent to Bob over a classical channel, hence he will get to know the state of his qubit instantly. Depending on the relationship in Table IV, Bob selects the specific unitary operation that transforms the state of qubit B into the teleported state $|\psi\rangle_0$. Thus, the qubit containing the quantum information has been teleported from Alice to Bob. Observe the dual relationship between superdense coding and quantum teleportation by comparing Fig. 8 and Fig. 9. More formally, Werner's proof [157] shows that two parties can swap their equipment to convert quantum teleportation into superdense coding under certain conditions, and vice versa.

Entanglement swapping has the capability of entangling a pair of distant quantum syesems that have never been connected in the past [158]. Figure 10 shows the process of entanglement swapping. Consider a pair of entangled states $|\psi^-\rangle_{12} = 1/\sqrt{2}\,(|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2)$ and $|\psi^-\rangle_{34} = 1/\sqrt{2}\,(|0\rangle_3|1\rangle_4 - |1\rangle_3|0\rangle_4)$, which are generated simultaneously. We may then pick one photon from each of the

[3]The four Bell states encoding 2 bits of classical information can be distinguished by nonlinear optics based BSM [156].

Fig. 10. Entanglement swapping process. The BSM applied to particles 2 and 3 immediately projects particles 1 and 4 into an EPR pair.

two entangled states to make a BSM. As a result, we can immediately see in Fig. 10 that the measurement of particles 2 and 3 projects the original non-entangled particles 1 and 4 into an EPR state. This can be formally expressed as

$$
\begin{aligned}
|\psi^-\rangle_{12}|\psi^-\rangle_{34} &= \frac{1}{2}\,(|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2)\,(|0\rangle_3|1\rangle_4 - |1\rangle_3|0\rangle_4) \\
&= \frac{1}{2}(|\psi^+\rangle_{14}|\psi^+\rangle_{23} - |\psi^-\rangle_{14}|\psi^-\rangle_{23} \\
&\quad + |\phi^+\rangle_{14}|\phi^+\rangle_{23}) - |\phi^-\rangle_{14}|\phi^-\rangle_{23}).
\end{aligned}
\tag{26}
$$

Note that the state of newly generated entangled pair is decided by the measurement result, so for example, $|\phi^+\rangle_{23}$ yields $|\phi^+\rangle_{14}$.

The quality of entangled states decays exponentially upon encountering the unavoidable noise of a quantum channel. This result is absolutely against the original intention of distributing entanglement between a pair of distant nodes without contaminating them. *Entanglement purification* offers a way of mitigating this deleterious effect by extracting a small number of almost perfectly entangled pairs from many poor-quality entangled states with the aid of local operations and classical communications. Figure 11 shows the original entanglement purification scheme introduced by Bennett *et al.* [159]. Let us assume having two imperfectly entangled
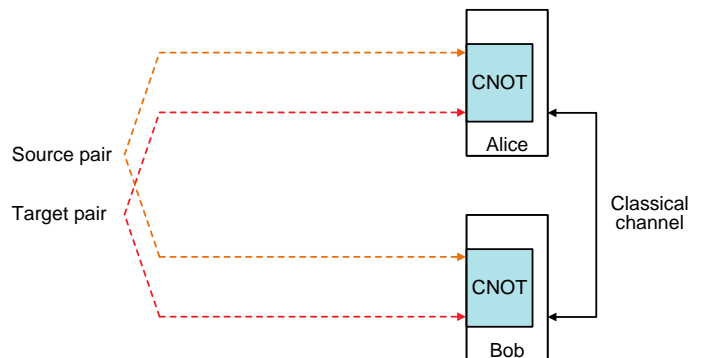

Fig. 11. The Scheme of entanglement purification by Bennett *et al* [159]. CNOT: Controlled-NOT.

pairs shared by Alice and Bob as seen in Fig. 11. One of them is the source pair, which has higher-quality entanglement

TABLE IV
TELEPORTING AN ARBITRARY QUBIT $|\psi\rangle_0 = \alpha|0\rangle + \beta|1\rangle$ WITH EPR STATE $|\psi^-\rangle_{AB}$.

BSM outcome	State of qubit B	Operation	Teleported state
$|\psi^-\rangle_{0A}$	$-(\alpha|0\rangle + \beta|1\rangle)_B$	$U_0 = I$	$-(\alpha|0\rangle + \beta|1\rangle)_B$
$|\psi^+\rangle_{0A}$	$(-\alpha|0\rangle + \beta|1\rangle)_B$	$U_1 = \sigma_z$	$-(\alpha|0\rangle + \beta|1\rangle)_B$
$|\phi^-\rangle_{0A}$	$(\alpha|1\rangle + \beta|0\rangle)_B$	$U_2 = \sigma_x$	$(\alpha|0\rangle + \beta|1\rangle)_B$
$|\phi^+\rangle_{0A}$	$(\alpha|1\rangle - \beta|0\rangle)_B$	$U_3 = i\sigma_y$	$(\alpha|0\rangle + \beta|1\rangle)_B$

than the target pair to be purified. Both Alice and Bob apply the Controlled-NOT gate[4] to the particles in their hand. Subsequently, they both measure the qubits of the target pair using the measurement of Z and compare their measurement outcome by relying on classical communication, as seen in Fig. 11. The source pair will be retained as is, because it has a higher degree of entanglement than the original target pair, if their Controlled-NOT outputs shared over the classical channel are the same. Otherwise, the source pair will be discarded. However, since the Controlled-Not gate is difficult to realize experimentally, Pan *et al*. came up with a simpler solution by harnessing a polarizing beam splitter [160], [161]. The benefits of this solution were also demonstrated subsequently in [162]. Some further improved schemes, such as the deterministic entanglement purification protocol were proposed in [163]–[165].

B. Experimental fundamentals

1) Light source and detector: In physical implementations, qubits have been realized with the aid of many different systems [166], but for quantum communications the most popular qubit carriers are photons. However, the unconditional security of single-photon based quantum communication requires a *perfect* source [167], which is difficult to produce. In the experimental implementation, the pragmatic solution is to use a weak coherent pulse as a near-perfect practical single-photon source. The state of a photon emitted by a laser is described by the coherent state $|\alpha\rangle$, which is a superposition of Fock states $|n\rangle$ [168],

$$|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{a^n}{\sqrt{n!}} |n\rangle, \qquad (27)$$

wherein $\alpha = \sqrt{\mu}e^{i\theta}$, $\sqrt{\mu}$ represents the intensity associated with the average number of photons μ per pulse and with the phase θ. The probability that a laser pulse contains n photons obeys the Poisson distribution of $p_\mu(n) = e^{-|\alpha|^2}|\alpha|^{2n}/n! = e^{-\mu}\mu^n/n!$ [168]. In other words, the practical light source is in a mixture of states $|n\rangle$ with a probability of $p_\mu(n)$, rather than obeying the perfect desired single photon Fock state associated with $|n = 1\rangle$ (this should not be confused with one of the two states of a qubit). It is plausible that the main components of this state of the laser pulse are the zero-photon vacuum state $|n = 0\rangle$ and the single-photon state of $|n = 1\rangle$, when the intensity of the laser pulse is attenuated to be

sufficiently low. Such a practical source has also been proved secure [169]. However, the transmission distances attained remain limited, and the contributions of a fraction of the photons emitted by the laser pulses have to be deleted because they are insecure in the face of the photon number splitting attacks [170]. To elaborate a little further, in the photon number splitting attack, Eve captures a photon from each pulse that contains several photons for further eavesdropping action. The attainable distance can be substantially increased by using the so-called decoy state technique [171]–[173], which improves the overall performance of QKD systems. After the modification, this technique is also applicable to QSDC, enabling resistance to photon number splitting attack and enhancing communication performance [86], [97], [174]–[177]. Therefore, combining the weak coherent pulse based and decoy state based solution having the optimal average number of photons μ constitutes a beneficial practical method for light sources.

At the time of writing, ideal single-photon sources are not yet available [178]. Alternatively, deterministic single-photon sources and probabilistic single-photon sources are capable of dramatically reducing the relative frequency of vacuum states and multi-photons. Deterministic single-photon sources, as exemplified by quantum dots [179]–[181] and color centers as detailed in [182]–[184], usually result in a higher energy level first and then emit a single-photon. By contrast, probabilistic single-photon sources, which are also referred to as heralded single-photon sources [185], generate single photons by measuring one of the photons in an entangled photon pair, which then serves as reference for the generation of a single photon [186], [187]. These two kinds of single-photon sources have the potential of realizing higher information bit rates or longer transmission distances than the weak coherent pulse source [97].

The entangled two-photon state is the fundamental resource of many entanglement-based quantum communications techniques. The efforts of generating entanglement originally relied on the so-called atomic system concept of [188], [189]. As the developments continued, the physical process of spontaneous parametric down-conversion [190] and spontaneous four-wave mixing [190] have been frequently used as the entangled resources. Spontaneous parametric down-conversion is a process of nonlinear interaction, in which a high-frequency pump photon ω_P is converted into a pair of lower-frequency photons ω_1 and ω_2 (termed as the signal and idler photons), where the pump light illuminates a nonlinear optical crystal characterized by its second-order nonlinear susceptibility $\chi^{(2)}$ as discussed in [191]–[193], and shown in Fig. 12 (a). Various

---

[4]In the Controlled-NOT gate the target qubit will be subjected to the NOT operation if and only if the control qubit is in the state $|1\rangle$.

types of entanglement, such as OAM entanglement [194], time-energy entanglement [195], and polarization entanglement [196], can be generated with the aid of spontaneous parametric down-conversion, which constitute a popular choice for preparing entanglement, since they are relatively simple to construct and hence inexpensive. They have been used as light sources in quantum communications including QKD [197] over 140 kilometers, and even for 100+ kilometers for quantum teleportation [198], [199]. However, the energy conservation constraints of spontaneous parametric down-conversion formulated as $\hbar\omega_p = \hbar\omega_1 + \hbar\omega_2$ and the momentum conservation (also termed as phase-matching) expressed as $\hbar\boldsymbol{k}_p = \hbar\boldsymbol{k}_1 + \hbar\boldsymbol{k}_2$ results in the phenomenon that the emitted down-converted photons generated by conventional bulk crystal sources have a cone-shaped spatial multi-mode structure surrounding the pump laser. Hence it is quite challenging to collect and guide the light into single-mode fibers for quantum information processing and transmission [200]. To circumvent this problem, waveguide based spontaneous parametric down-conversion schemes [201]–[203] have also been developed.

Fig. 12. Schematic portrayal and energy-level diagram of (a) spontaneous parametric down-conversion and (b) spontaneous four-wave mixing.

The spontaneous four-wave mixing sources have also received much attention as another popular candidate for directly generating entangled photons in a single-mode waveguide [204]–[207]. As shown in Fig. 12 (b), a pair of two pump photons is annihilated and a pair of correlated photons is created in the process of spontaneous four-wave mixing by a nonlinear optical medium, characterized by its 3rd-oder nonlinear susceptablity $\chi^{(3)}$ in which both energy conservation $2\hbar\omega_p = \hbar\omega_1 + \hbar\omega_2$ and momentum conservation $2\hbar\boldsymbol{k}_p = \hbar\boldsymbol{k}_1 + \hbar\boldsymbol{k}_2$ are observed. This process has some distinct advantages over spontaneous parametric down-conversion. Firstly, the resultant entangled pairs are generated in a single spatial mode, making their collection and delivery quite efficient. Hence they can be directly integrated with existing optical-fiber communication networks [204]. Secondly, spontaneous four-wave mixing exhibits a high brightness facilitated by its long interaction duration and high transverse mode confinement as a benefit

of its limited cross-section [206]. However, spontaneous four-wave mixing requires higher pump power than spontaneous parametric down-conversion because its $\chi^{(3)}$ nonlinearity is weaker than $\chi^{(2)}$. The Raman scattering noise inflicted by its strong pump field must be mitigated in the spontaneous four-wave mixing source, for example by cooling the fiber in liquid nitrogen [208]. Thus the experimental difficulties increase accordingly.

The single-photon detector constitutes the link between the quantum domain and classical domain, which converts the quantum signals into electrical signals for information detection. At the time writting three popular detectors are used extensively in the experimental implementation of quantum communication: InGaAs avalanche photodiodes, Si avalanche photodiodes, and superconducting single-photon detectors. Six key parameters are routinely used for characterizing the performance of single-photon detectors, including their detection efficiency, dark count rate, dead time, spectral range, time jitter and the ability to distinguish the number of photons [209]. In a certain spectral range, a perfect single-photon detector must have 100% detection efficiency, the ability to determine the number of impinging photons, while having all the remaining parameters mentioned above as 0. InGaAs avalanche photodiodes are typically used for detection at telecom wavelengths [210] (typically in 1550 nm and 1310 nm). However, they tend to have a relatively low detection efficiency of around 10%. Naturally, the designer has to strike tradeoffs amongst the key parameters of practical InGaAs avalanche photodiodes. For example, increasing the bias will increase the detection efficiency, but it will also exacerbate the dark count rate [211]. Having said that, InGaAs avalanche photodiodes exceeding 50% detection efficiency are becoming available, which are capable of striking much improved performance tradeoffs [212], [213].

By contrast, Si avalanche photodiodes attain a detection efficiency of more than 60% at a low dark count rate at specific wavelengths of the visible and near-infrared domain [214], which are eminently suitable for free-space quantum communication [215], [216]. Finally, superconducting single-photon detectors also perform well in the visible to mid-infrared wavelength domain. Specifically, they exhibit a high detection efficiency (>90%) and very low dark count rate (<1 cps), low timing jitter (<100 ps) and short reset time (<100 ns) [217]. Unpon considering each of the above parameters individually an even better performance may be attained [218]–[220]. Hence they have become one of the most sought after devices for high-performance QSDC [89]. However, superconducting single-photon detector may be deemed excessively costly for conventional applications, because they must be operated at an extremely low temperature of a few Kelvin.

2) Optical components and channels: Optical components, such as beam splitters (BS), polarization beam splitters (PBS), polarization controllers, wave plates, mirrors, Faraday mirrors (FR), phase modulations (PM) and so on, are commonly used in various quantum communication systems [60], [193].

The quantum channel is a link between Alice and Bob provided for the transmission of quantum information. Basically, there are two popular choices of transmission channels, namely

optical fibers and free-space optical channels[5]. Optical fiber links have a very low channel loss of about 0.2 dB/km for photons at the 1550 nm wavelength and even 0.16 dB/km [221], [222], and approximately at 0.3 dB/km for photons at 1310 nm wavelength. QKD transmission has been demonstrated over 421 km of optical fiber [222], and it is not confined to this distance, when using new mechanisms [223]. In the absence of perfectly secure quantum repeaters, several hundreds of kilometers are feasible for single photon transmission, which is predominantly limited by the inherent path loss and by the environmental factors of temperature as well as stress.

Free-space optical (FSO) transmission is known as a very promising design alternative for quantum communications, which has a wide transmission window in the vicinity of ~800 nm, which conveniently corresponds to the detection range of efficient yet inexpensive Si-avalanche photodiode detectors [50]. Moreover, there is only negligible dispersion, but the atmospheric turbulence effects may become hostile, as detailed in [224]. Further challenges of free-space-based quantum communication are due to the scattered sunlight.

To overcome the background noise in FSO scenarios, substantial efforts have been made to use filtering techniques and optimized single-photon detection with remarkable results [225], [226]. The total attenuation α of the free-space channel can be evaluated by the contributions of two main effects: diffraction and atmospheric attenuations, including absorption, scattering, and atmospheric turbulence, which may be formulated as $\alpha_{\mathrm{atm}} = \alpha_{\mathrm{abs}} \alpha_{\mathrm{scatt}} \alpha_{\mathrm{turb}}$. As shown in Table V, several theoretical models have been established for calculating the channel loss that results from the above-mentioned effects. Diffraction, also known as geometric loss, will result in beam divergence, hence some fraction of the beam energy cannot be collected by the receiver. A plausible, but costly method of tackling this problem is to increase the telescope aperture [227], which is more realistic for the ground-station than for a compact solar-charged satellite. Nguyen *et al.* [228] applied network coding in a free-space QKD system and studied the diffraction effects. In the process of evaluating the QBER, Shapiro theoretically quantified the diffraction loss [229]. Absorption and scattering are also inevitable phenomena in the process of FSO propagation through the atmosphere, where they interact with various gasses and particles. Surprisingly, their influence on the channel attenuation tends to remain modest, apart from adverse weather conditions. The atmospheric refractive index tends to fluctuate randomly due to the temperature, pressure, and humidity variations in the air, which is the source of atmospheric turbulence. As a result, typically the probability distribution of transmittance is adopted for characterizing the beam wandering, broadening, and deformation after the laser beam undergoes atmospheric turbulence [230]–[233]. Then the mean attenuation is given by

$$\alpha_{\mathrm{turb}} = \int_0^{\eta_0} \eta^2 p(\eta) d\eta, \tag{28}$$

---

[5]It important to note that apart from these practical links, the quantum decoherence effects of quantum signal processing operations are typically modelled by a quantum depolarizing channel. This might be viewed as counterpart of the AWGN channel of classical systems, which characterizes the noise-level in the receiver.

where $\eta = \sqrt{\eta_t}$, is the intensity transmittance, η_t is the transmissivity, while the maximum value of η is η_0, and $p(\eta)$ is the probability distribution of transmittance.

3) Quantum random number generator: Truly random numbers are considered as an essential part of maintaining the security of quantum communication [238]. As for QSDC systems, the state preparation, state sampling strategies of some protocols, and classical coding [50] rely on a random number generator producing samples at a high rate and 'high-quality' randomness. Normally, the procedure of designing a quantum random number generator is divided into four steps, as seen in Table VI. First the specific source of quantum randomness will be selected, from which we can extract the raw random number sequence using measurement. The resultant raw random number sequence then undergoes postprocessing, a step of distillation, to remove the classical sources of contamination (typically appears as bias and redundancy in the sequence) that originates from the imperfection of the devices. Finally, the quality of the random number sequence will be tested either with the aid of statistical analysis or physical certification. The source of quantum randomness falls into two basic categories: discrete and continuous, which depends on the specific source of randomness. The discrete source of quantum randomness has a simple model, but its output rate is usually low. By contrast, the continuous source has a high output rate, but the inevitable classical contamination has to be carefully mitigated.

4) Bell-state measurement: This is one of the key ingredients in quantum information processing, as surveyed in Section III-A5. Entanglement generation was detailed in Section III-B1. Again, the BSM allows us to distinguish the four Bell states of Eq. (9) when we want to exploit entangled resources. If we are restricted to using only linear optical devices, such as beam splitters, polarization beam splitters and single-photon detectors, the BSM will be unable to distinguish each of the four Bell-states with 100% certainty, as shown in [261]. In other words, in this case, only two of the four Bell states $|\psi^{\pm}\rangle$ can be reliably discriminated [261]. In other words, the success rate of BSM using linear optics is limited to 50%. Although the four Bell states cannot be distinguished unambiguously by using linear optical devices, these are easier to implement than a complete BSM relying on nonlinear optical components [156]. Hence, some QSDC protocols [45], [78] tend to only choose the pair Bell state $|\psi^{\pm}\rangle_{AB}$ of Eq. (9) to transmit information for the sake of simplifing the measurement system. Let us rewrite the Bell states $|\psi^{\pm}\rangle_{AB}$ of Eq. (9) in the form of polarization-entangled photonic states, namely,

$$|\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|H\rangle_A |V\rangle_B + |V\rangle_A |H\rangle_B \right),$$

$$|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|H\rangle_A |V\rangle_B - |V\rangle_A |H\rangle_B \right). \tag{29}$$

This BSM, which purely relies on linear optical components for discriminating these two polarization-entangled photonic states is shown in Fig. 13 (a). These two devices allow us to identify the incoming Bell state by the so-called click patterns of the single-photon detectors [262]–[264], as shown

TABLE V
Major propagation phenomena characterizing the free-space channel.

Type of channel loss	References	Contributions
Diffraction	[229]	The bounds of the sift and error probabilities of a free-space QKD was deduced from the extended Huygens-Fresnel principle by considering the diffraction effects.
	[234]	The additional attenuation caused by diffraction was taken into consideration in the analysis of key-rate performance in earth-satellite QKD.
Absorption and scattering	[235], [224]	The propagation loss of adverse weathers conditions was quantified.
	[236]	A quantum theory of nonclassical light propagation under different weather conditions, including rain or haze, was developed, which agrees well with the data collected from experiments.
Atmospheric turbulence	[237]	Introducing three models to calculate the probability distribution of transmittance when facing the different propagation distances and optical turbulence strengths.

TABLE VI
The design process of quantum random number generator.

Source of quantum randomness		Detection	Postprocessing	Randomness test	
Discrete	Spatial randomness of single photons [239]–[241] Time resolution randomness of single photons [242]–[244] Attenuated coherent light [245], [246] Quantum tunneling effect [247], [248] Device-independent self-testing [249], [250]	Detection varies with dfferent quantum randomness source	Randomness extractors [259]	Statistical analysis	ENT, Diehard, National Institute of Standards and Technology statistical test suite [251], [252]
Continuous	Laser phase fluctuations [253], [254], Vacuum fluctuation [255] Shot noise [256], [257] Super-luminescent diode [258]			Physical certification	Bell's theorem [260]

in Fig. 13 (b) and (c). If two clicks happen in D_{1H} and D_{1V} or D_{2H} and D_{2V}, the measurement result is $|\psi^+\rangle_{AB}$. These two click patterns are shown in Fig. 13 (b). Furthermore, the measurement result is $|\psi^-\rangle_{AB}$ if two clicks D_{1H} and D_{2V} or D_{1V} and D_{2H} are obeserved, as shown in Fig. 13 (c).

A complete BSM is possible by using hyper-entanglement with only linear elements. Hyper-entanglement is a state that is entangled in more than one degrees of freedom and the extra degrees of freedom allows for secondary interferometry, so that the remaining two Bell states can be distinguished [265]–[267]. If nonlinear elements are added, all four Bell states can be discriminated with a success probability of 100% [156]. Additional auxiliary degrees of freedom in hyper-entanglement can also be distinguished by the nonlinearity devices of [268].

5) Photonic modulation technologies: In QSDC, the information can be conveyed by different fundamental resources, as shown in Fig. 14, namely polarization [58], [59], phase [60], [80], [85], [86], [89], time-bin [89], operation frequency [57], orbital angular momentum (OAM) [269], quadrature components [67], [270], [271], coherent optical filed [88], and spatial mode [272]. Some of these have shown promising potential QSDC. In the following, we will briefly highlight these in the context of QSDC. Some new modulation techniques of QKD will also be mentioned, in order to pave the way for their QSDC counterparts in the future. We mainly focus our attention on the field of the discrete variables, while the quadrature components of light based solutions belong to the family of continuous variables [224], [273], which will be touched upon in less detail.
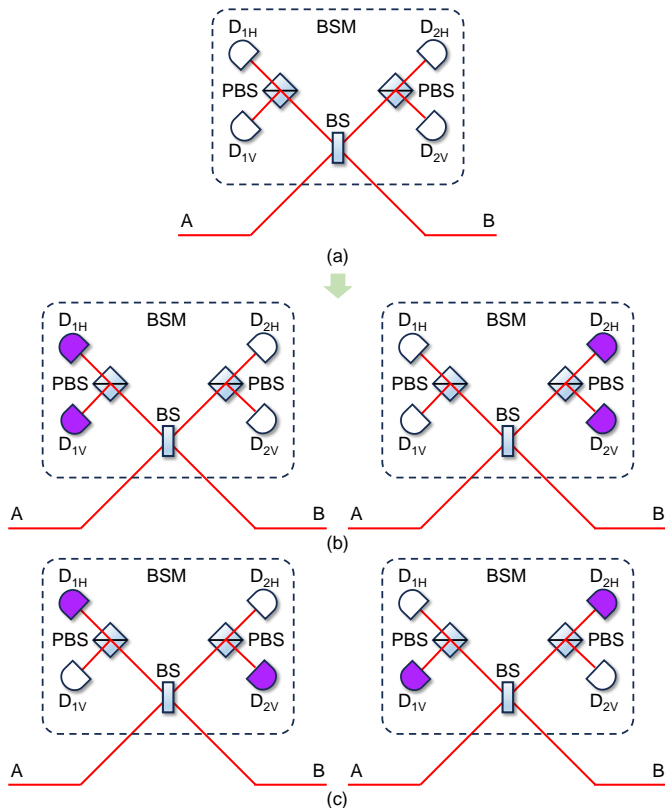
Fig. 13. (a) Setup to perform BSM; (b) The click patterns of Bell state $|\psi^+\rangle_{AB}$. (c) The click patterns of Bell state $|\psi^-\rangle_{AB}$. BS: beam splitters; PBS: polarizing beam splitters; D: single-photon detectors; the A and B represent two inputs. The single-photon detectors labeled by purple means that this detector is clicked by photons.

The **polarization** of a single-photon may be decribed by its state vector [274], [275]: the state of $|1\rangle$ stands for the vertically polarized photon $|\uparrow\rangle = |V\rangle$ also seen in the Bloch sphere of Fig. 6. Analogously, we have $|\rightarrow\rangle = |H\rangle = |0\rangle$, $|\nearrow\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|\searrow\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, $|\circlearrowright\rangle = |R\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$, and $|\circlearrowleft\rangle = |L\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$. Furthermore, for entangled states, we have $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle_A|\uparrow\rangle_B + |\uparrow\rangle_A|\rightarrow\rangle_B)$. These states represent the information carrier of the classical bits in many quantum communications protocols. They also constitute a natural choice for experimental implementations [58], [59], because they may be readily generated by the polarization based modulation of a laser source [276] or polarizing multiple lasers [216], [277][6]. Based on the characteristics of the quantum channels described in Section III-B2, we know that the polarization of photons is more suitable for FSO channels than for fiber, because the fiber channel tends to perturb the polarization of photons [278]. Furthermore, photon polarization based FSO transmission designed for satellites requires some reference frames for the accurate alignment of measurement bases [279], unless a specifically designed

---

[6]Note that this light source may raise some security concerns in quantum communication, because the laser sources cannot be exactly the same.

reference-frame-independent protocol is used [280]. At the measurement stage, the receiver can separate the orthogonal states and forward them to the single-photon detectors for determining, whether they are constituted by $|H\rangle$ or $|V\rangle$. The diagonally polarized states can also be readily identified in a similar way.

Phase encoding maps information onto the relative phase difference between two consecutive pulses. Typically, after modulation by an unbalanced Mach-Zehnder interferometer, the form of the weak coherent state becomes [281], [282]

$$\left|\sqrt{\frac{\mu}{2}}e^{i\theta}\right\rangle_s \left|\sqrt{\frac{\mu}{2}}e^{i(\theta+\varphi)}\right\rangle_l, \tag{30}$$

where μ is the average photon numbers, θ is the initial random phase, φ is the modulated phase encoding information bits. Furthermore, the subscripts s and l denote the short arm and long arm of an unbalanced Mach-Zehnder interferometer. The discrete phases of $\varphi \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ which are prepared by Alice as the initial states and then Bob randomly applies the phase shifts of either 0 or $\frac{\pi}{2}$ for performing demodulate measurement [283], [284] in BB84 QKD. This scheme may also be readily adapted for QSDC as detailed in [60], [86].
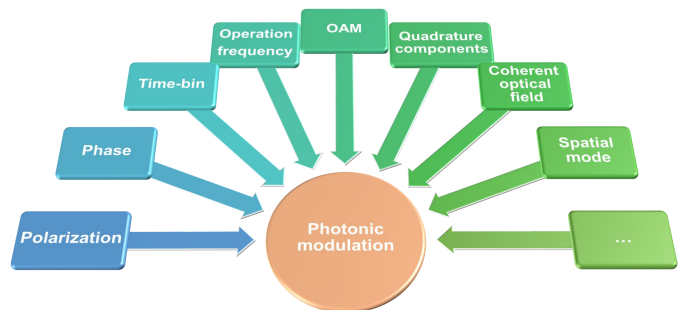

Fig. 14. Mapping qubits to physical resources using photonic modulation. OAM: orbital angular momentum.

The family of **time-bin** based methods convey the qubit states by relying on specific consecutive time intervals, written in the form of

$$|e\rangle = |\sqrt{\mu}\rangle_e|\sqrt{0}\rangle_l, \quad |l\rangle = |\sqrt{0}\rangle_e|\sqrt{\mu}\rangle_l, \tag{31}$$

where the subscripts e and l denote the temporal modes early and late, respectively. It can be prepared by emitting a pulse which has to pass through an unbalanced interferometer. Thus the computational basis $|e\rangle$ indicates that the photon takes a short path and arrive early, while $|l\rangle$ represents the long arm, hence its photon arrives late. After preparation, if this time-bin based state goes through a nonlinear crystal, eventually a time-bin entanglement can be created [285]. The phase and time-bin based qubits are more robust than the polarization based qubits, when performing quantum communication via fiber [89]. Hence the former are is popular in quantum communication.

Operation frequency based encoding applies the same unitary operation to a single-photon block periodically to encode secret messages, and the receiver of this single-photon

block is capable of decoding the secret messages through the discrete time Fourier transform [57].

Orbital angular momentum [286], [287] is another quantity that may be conveniently carried by a laser beam upon exploiting the so-called azimuthal angular dependence of $e^{-il\phi}$, where l is the azimuthal index assuming an unbounded integer and ϕ is the azimuthal angle in the beam's cross-section [288], [289]. For a given azimuthal index l, the orbital angular momentum has the discrete value of $L = l\hbar$, indicating that the beam carries $l\hbar$ amount of orbital angular momentum per photon. It has been demonstrated that orbital angular momentum states can be used for conveying information at a capacity beyond one bit per photon both for QSDC [269], [290] and DQKD [291]. Additionally, a high-dimensional system 'qudit' (a unit of information in a N dimension space) typically has a superior security level in quantum cryptography protocols [292], [293].

The QSDC scheme relying on **quadrature components** for encoding is commonly referred to as a continuous-variable protocol, which has the advantage of compatibility with existing classical communication infrastructure [294], [295], low cost, and high rate [224]. These continuous variable protocols typically employ Gaussian states [67], [270], [296] and continuous-variable entangled states [74], [75], [81], [117], [271], [297] as information carriers for secure communication. Recently, the CV QSDC experiment demonstrations were given by Paparelle et al. [298], [299].

In 2021, a protocol called quantum keyless private communication was proposed in [88], which uses the quantum-domain version of on-off keying modulation to transmit information, where the coherent state $|\alpha\rangle$ represents information bit 1 and the vacuum state $|0\rangle$ represents information bit 0. Single-photon detectors are used for detection. We refer to this as modulation based on **coherent optical fields.**

The **spatial-mode** is a frequently used degree of freedom exploited for information transfer, when combined with other degrees of freedom, it enables the design of high-capacity QSDC protocols [272], [300], [301].

The family of **hybrid methods** combining different modulation techniques which complement each other is also often used for the sake of combining their different benefits. For instance, combined polarization-orbital angular momentum states are rotationally invariant and exhibit high robustness against spatial perturbations. Hence they are eminently suitable for mitigating the frame-misalignment problems encountered in free-space quantum communication [227], [302]. Modulation techniques relying on high-dimensional states that can be used for high-rate and high-security quantum communication are also available at the time of writing, but they are limited to short distances [293], [303].

By contrast, there are many other mature modulation methods in QKD, but their feasibility in QSDC still needs to be studied. Examples of practical **phase-encoding** related QKD systems include the differential phase shift aided schemes of [304]. In differential phase shift aided QKD, the information bits are mapped to the phase difference between the adjacent pulses. It has been shown that it is feasible to realize a high-speed clock frequence of 10 GHz using the simple

experimental setup of [305], which achieves a 12.1 bit/s secure key rate over 200 km of optical fibre. In coherent one-way QKD, the bit string is carried by the coherent one-way pulse of $|0\rangle|\alpha\rangle$ for bit 0 and by $|\alpha\rangle|0\rangle$ for bit 1. Then the receiver can detect them with the aid of time-of-arrival measurements. In 2015, the coherent one way technique attained a long-distance record of 307 km for QKD [306]. Both the differential phase shift and the coherent one-way techniques use weak coherent pulses as the light source, but they are immune to photon number splitting attacks [307], [308].

A range of early contributions relied on single-sideband modulation, where the informtion bits are mapped to one of the two sidebands surrounding a central frequency [309]–[312]. Bloch et al. [313] conceived a **frequency-encoding** QKD scheme, while its improved version was proposed by Zhang et al. [314] a year later. In frequency-modulated QKD, Alice can generate four states by using the modulator, which can be formulated as follows,

$$|+;1\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0} + \frac{1}{2}|1\rangle_{\omega_0+\Omega} - \frac{1}{2}|1\rangle_{\omega_0-\Omega},$$

$$|-;1\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0} - \frac{1}{2}|1\rangle_{\omega_0+\Omega} + \frac{1}{2}|1\rangle_{\omega_0-\Omega},$$

$$|+;2\rangle = |1\rangle_{\omega_0},$$

$$|-;2\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0+\Omega} - \frac{1}{\sqrt{2}}|1\rangle_{\omega_0-\Omega}, \tag{32}$$

where $|n\rangle_\omega$ represents the number of photons in mode ω. Those four states constitute a pair of bases given by $\{|+;1\rangle, |-;1\rangle\}$ and $\{|+;2\rangle, |-;2\rangle\}$, which is equivalent to the rectilinear and diagonal orthogonal basis sets of the BB84 QKD protocol [38] and thus this modulation scheme may be readily used for implementing QKD. No unbalanced interferometers are required for frequency encoding, which has the advantage of avoiding stabilization.

The status of these photonic modulation techniques in the context of QSDC is summarized in Table. VII.

IV. QUANTUM SECURE DIRECT COMMUNICATION

A. Point-to-point communication protocols

A point-to-point QSDC protocol is defined as a sequence of steps with associated quantum operations and rules that control the communications with the goal of securing communication between two users. In this section, we will highlight some of the typical QSDC protocols step by step and show how these protocols facilitate for two parties to transmit confidential messages directly through the quantum channel [43], [53], [54], [61], [78], [117], rather than simply exchanging secret keys. We will introduce the QSDC protocol and DSQC protocol, which enable secure communication over a quantum channel. The processes of these protocols are illustrated in Fig. 15.

1) High-capacity QSDC protocol [42], [43]: Alice and Bob have the two-bit classical messages 00, 01, 10, 11 corresponding to $|\phi^+\rangle_{AB}, |\phi^-\rangle_{AB}, |\psi^+\rangle_{AB}, |\psi^-\rangle_{AB}$, respectively. An ordered set of N EPR pairs is denoted by $\{[P_1(1), P_1(2)],$ $[P_2(1), P_2(2)], \cdots, [P_i(1), P_i(2)], \cdots, [P_N(1), P_N(2)]\}$, where $P_i(1)$ is the EPR partner particle of $P_i(2)$ and vice versa. Then an ordered EPR partner particle sequence

TABLE VII
STATUS OF SOME POPULAR PHOTONIC TRANSMISSION TECHNIQUES IN
THE REALIZATION OF QSDC.

Technique	Status
Polarization	√
Phase	√
Time bin	√
Operation frequency	√
Orbital angular momentum	◯
Quadrature components	√
Coherent optical field	◯
Spatial mode	◯
Hybrid methods	◯
Differential phase shift	?
Coherent one-way	?
Frequency	?
√ There have already been experimental demonstrations. ◯ It has been proposed, but there is no experimental demonstration. ? The feasibility is uncertain at the time of writing.	

Fig. 15. The flow diagram of (a) the QSDC (high-capacity, two-step, DL04, high-dimension two-step, and MDI) and (b) DSQC protocols (continuous-variable protocol relying on two-mode squeezed states and Zhu-Xia-Fan-Zhang (ZXFZ) protocol).

$[P_1(1), P_2(1), \cdots, P_i(1), \cdots, P_N(1)]$ is generated by taking one of the EPR partner particles, say $P_i(1)$ from each EPR pair $[P_i(1), P_i(2)]$. The order of these N EPR pairs remains unchanged throughout the whole process of confidential mes-

sage transmission. They carry out the following procedures [43], which are shown in Fig. 16.

- **Step 1, state preparation**. Alice prepares an ordered set of N EPR pairs $\{[P_1(1), P_1(2)], [P_2(1), P_2(2)], \cdots, [P_i(1), P_i(2)], \cdots, [P_N(1), P_N(2)]\}$ representing her eavesdropping check bits and her confidential messages to be transmitted to Bob. The check bits are randomly selected 00, 01, 10, and 11, and they are inserted into the messages. Alice then splits the EPR pair sequence into two halves, namely into an ordered EPR partner particle sequence: $[P_1(1), P_2(1), \cdots, P_i(1), \cdots, P_N(1)]$, and into the corresponding EPR partner particle sequence: $[P_1(2), P_2(2), \cdots, P_i(2), \cdots, P_N(2)]$.

- **Step 2, first transmission**. Alice sends one of the ordered EPR partner particle sequences, say $[P_1(2), P_2(2), \cdots, P_i(2), \cdots, P_N(2)]$ to Bob and tentatively stores the other one in her quantum memory.

- **Step 3, first eavesdropping detection**. Alice randomly chooses a sufficiently large fraction of the samples representing the check bits from the EPR parter sequence stored in her memory and performs measurement on these samples by randomly using either the Z-basis or the X-basis. Naturally, she will get the result of either 0 or 1. Again, the rest of the EPR parter sequence is stored by Alice as seen in Fig. 16. She then informs Bob through an authenticated classical channel - which may of course be mapped to another wavelength in the same wavelength division multiplex aided fiber link - of the positions of the specific samples measured by her. Based on the information received from Alice, Bob measures the corresponding EPR sample particles in his hand. Then Alice and Bob publicly compare the results of their measurement to detect eavesdropping. If their results are the 'same' [42], [43], they conclude that there is no eavesdropping. If there is no eavesdropping, they proceed to the next step. Otherwise, they terminate the communication. This is the first eavesdropping detection opportunity during the transmission of $P_i(2)$. In Fig. 16, the pair of dashed hollow circles represent the checking qubits.

- **Step 4, second transmission, measurement, and second eavesdropping detection**. Alice sends the remaining EPR partner particle sequence $[P_1(1), P_2(1), P_3(1) \cdots, \cdots, P_N(1)]$ to Bob, which does not include the particles that have been choosen for detecting a potential eavesdropper. For instance, $P_3(1)$ in Fig. 16 has been measured by Alice and thus was not transmitted. Bob performs the BSM on every EPR pair $[P_i(1), P_i(2)]$ in order to decode the confidential message and records the measurement results after receiving the rest of the sequence from Alice. The remaining check bits are announced by Alice, whose BSM results are selected to determine whether the QSDC process is successful. As shown in Fig. 16, the EPR pair $[P_7(1), P_7(2)]$ represents the second set of check qubits. If the error rate is deemed to be below a certain

threshold, the remaining results of the BSM are deemed to represent the transmitted confidential messages. The second eavesdropping detection opportunity is included here for estimating the reliability of the communication.
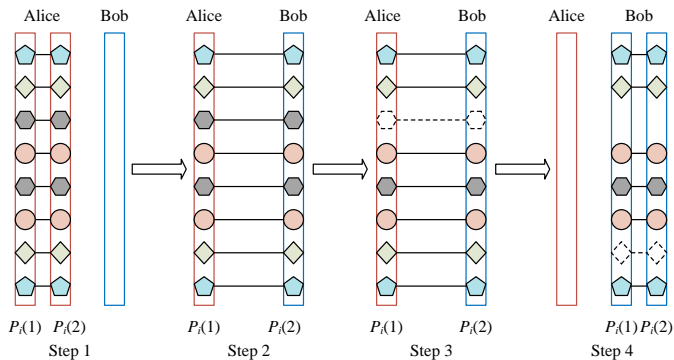

Fig. 16. Schematic illustration of the high-capacity QSDC protocol. Two symbols linked with a line are in a Bell-state. The pentagons, the rhombuses, the hexagons, and the circles represent the Bell state $|\phi^+\rangle_{AB}$, $|\phi^-\rangle_{AB}$, $|\psi^+\rangle_{AB}$, and $|\psi^-\rangle_{AB}$, respectively. The blank dashed symbols represent the state after Alice and Bob complete eavesdropping detection.

To elaborate a little further, there are two eavesdropping detections, which allows the QSDC protocol to guard against eavesdropping. On the one hand, an eavesdropper cannot steal the confidential messages without being detected, when she adopts the intercept-and-resend attack strategy. Eve has no access to both parts of the EPR pairs at the same time, since the ordered N EPR pair sequence is sent from Alice to Bob in two staggered intervals. In order to obtain the other EPR partner particle sequence $[P_1(1), P_2(1), \cdots, P_i(1), \cdots, P_N(1)]$, Eve first has to intercept the EPR partner particle sequence $[P_1(2), P_2(2), \cdots, P_i(2), \cdots, P_N(2)]$ and then a fake particle sequence $[P_1^*(2), P_2^*(2), \cdots, P_i^*(2), \cdots, P_N^*(2)]$ of her has to be sent to Bob. However, this attack can be easily detected by the above first eavesdropping detection in Step 4, because Alice randomly chooses some EPR partner particles in her hand to perform measurements and asks Bob to do the same. Alice and Bob will discover that half of their measurement results are conflicting because there is no quantum correlation between $P_i(1)$ and $P_i^*(2)$. As a further measure, the malicious nature of direct measurement by Eve may be readily spotted by the second eavesdropping detection. If Eve applies direct measurement to the EPR partner particle sequence and resends it, a high error rate will be experienced in Step 4 for the reason that the Bell states will collapse.

This is the basic principle of QSDC which has the beneficial feature of high capacity, since the four legitimate states of the EPR pair can carry two classical bits of information. This represents a higher capacity than that of other protocols that make use of EPR pairs as their information carrier [47], [48], [126]. Bob can decode the information directly without the exchange of classical bits. The protocols of [42], [43] use block transmission of quantum states to prevent the leakage of confidential messages and detect eavesdropping via random sampling tests. The idea that quantum mechanics could be beneficially exploited for direct communication over quantum channels has evolved substantially further after its conception [42], [43], which was originally proposed for deterministic key distribution. As a next evolutionary step, let us now consider the following two-step QSDC protocol.

2) Two-step QSDC protocol: The two-step QSDC protocol depicted in Fig. 17 is described as follows [53].
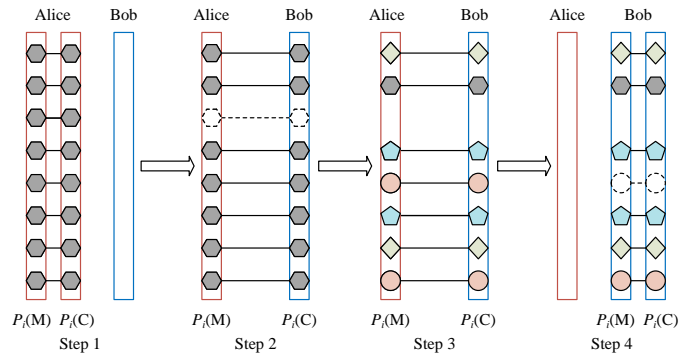

Fig. 17. The two-step QSDC protocol. Two hexagons linked with a line are in a Bell-state. The pentagons, the rhombuses, the hexagons, and the circles represent the Bell state $|\phi^+\rangle_{AB}$, $|\phi^-\rangle_{AB}$, $|\psi^+\rangle_{AB}$, and $|\psi^-\rangle_{AB}$, respectively. The blank symbols linked with a dashed line are the EPR pairs to do encoding-trick which is used for eavesdropping detection, it also in the one of the four Bell states while no secret message is carried.

- **Step 1, state preparation**. Alice and Bob agree on the specific mapping between the four Bell states $|\psi^-\rangle$, $|\psi^+\rangle$, $|\phi^-\rangle$, $|\phi^+\rangle$ and the two-bit classical information as 00, 01, 10, 11, respectively. Observe in Fig. 17 that Alice prepares an ordered sequence of N EPR pairs all in the state $|\psi\rangle_{CM} = |\psi^-\rangle = 1/\sqrt{2}(|0\rangle_C|1\rangle_M - |1\rangle_C|0\rangle_M)$, which is denoted by $[(P_1(C), P_1(M)), (P_2(C), P_2(M)), \cdots, (P_i(C), P_i(M)), \cdots, (P_N(C), P_N(M))]$. The subscript i represents the index of the EPR pair in the sequence, while C and M represent the pair of particles in the EPR pair. Alice then divides the ordered sequence of N EPR pairs into two EPR partner particle sequences. One of them is $[P_1(C), P_2(C), \cdots, P_i(C), \cdots, P_N(C)]$, which is called the checking sequence or C sequence for short. The other is the remaining EPR partner particle sequece $[P_1(M), P_2(M), P_3(M), \cdots, P_i(M), \cdots, P_N(M)]$, which is termed as the message-coding sequence or M sequence, as seen in Fig. 17.
- **Step 2, first transmission and first eavesdropping detection**. The C sequence $[P_1(C), P_2(C), P_3(C), \cdots, P_N(C)]$ of Fig. 17 is sent from Alice to Bob. Alice and Bob then detect eavesdropping through the following actions: (a) Bob randomly selects some EPR partner particles in the C sequence and tell Alice the position of these particles; (b) Bob randomly chooses one of the unitary operations $\{\sigma_x, \sigma_z\}$ to measure the EPR partner particles selected; (c) Bob tells Alice which of the two unitary operations he has performed on each particles and additionally informs her of the outcome of his measurement; (d) Alice chooses the same unitary operation as Bob to measure the corresponding EPR

partner particles in the M sequence. She will get the complete opposite results compared to Bob, provided that no eavesdropper contaminates the quantum channel: Alice gets 0 (1), Bob gets 1 (0). If the error rate is below the tolerance threshold, Alice and Bob conclude that there is no eavesdropper and proceed to next step. By contrast, in the presence of eavesdropping they curtail their communication.

- **Step 3, information encoding**. As seen in Fig. 17, Alice performs one of the four unitary operations (U_0, U_1, U_2 and U_3) on each of the particles in the M sequence to encode her confidential messages. In the process of encoding, Alice has to apply an 'encoding-trick' to the M sequence. Explicitly, she randomly chooses some EPR partner particles in the M sequence as the samples to perform one of the four unitary operations, but no valuable payload information is mapped to them. Only Alice knows the position of these particles and she keeps it secret until the M sequence is transmitted to Bob. The number of these particles must be sufficiently high for estimating the error rate, and all the remaining particles are used for encoding confidential payload messages.

- **Step 4, second transmission, measurement, and second eavesdropping detection**. Once Bob receives the M sequence, Alice tells him the position of the samples and the specific unitary operations applied to them. Bob performs the BSM on each and every EPR pair $[P_i\,(\mathrm{C})\,,\,P_i\,(\mathrm{M})]$ to decode the confidential payload messages. By checking the measurement results, Bob will then get an estimate of the error rate within the current M sequence transmission. In fact, Eve is capable of perturbing the qubits, but cannot steal the confidential payload messages because she can only get one of the partner particles from an EPR pair in the second transmission. If the error rate of the Eve-checking pairs is reasonably low, Alice and Bob can then trust the process, and may proceed to correct the errors in the confidential payload messages using a classical-domain error correction method. Otherwise, they have to abandon this particular transmission session and go back to Step 1 of Fig. 17.

Let us now continue our journey through QSDC history by considering the DL04 protocol.

3) DL04 QSDC protocol: As Fig. 18 shows, single photons are used as carriers of confidential messages in the DL04 protocol, which relies on the following two steps [54].

- **Step 1, the secure postal pigeon sending stage**. As seen in Fig. 18, N single photons are prepared by Bob and each of them is randomly mapped to one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, as shown in Table VIII. These single photons are called B-batch photons, and they are transmitted directly to Alice after preparation. Upon receiving the batch of single photons, Alice and Bob check the presence of eavesdropping by the following actions: (a) Sufficient single photon samples are picked randomly from the B batch. This fraction is termed as the C_1 batch, which is marked in gray in Table VIII, leaving behind the other photons forming the B batch having a cardinality

of $A = B - C_1$; (b) Alice randomly chooses either the measurement basis Z or X for measuring each photon in the C_1 batch and then publishes both the position of these photons as well as the measurement bases applied to them and the measurement results; (c) Bob then calculates the error rate to estimate the probability of eavesdropping. More specifically, Bob compares the measurement results of Alice to his original quantum states to obtain the error rate, when Alice has chosen the same measurement basis as the preparation basis of Bob. If the error rate is lower than a pre-determined threshold, the transmission of the B batch through the quantum forward channel is considered to be secure and they proceed to the next step. Otherwise, the communication is aborted.

- **Step 2, the message coding and postal pigeon returning stage**. Alice decides either to perform the operation $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ to encode the information 0 or to perform the operation $U = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ to encode the message 1[7]. Observe that the unitary operation U acts as flipping the state in both measuring bases, hence we can obtain

$$U|0\rangle = -|1\rangle, \ U|1\rangle = |0\rangle, \tag{33}$$

and

$$U|+\rangle = |-\rangle, \ U|-\rangle = -|+\rangle. \tag{34}$$

This operation offers the option of deterministically detecting confidential messages for Bob. To guarantee the security of the second transmission, Alice has to randomly choose some photons in the A-batch as Eve-checking samples. We refer to them as the C_2-batch and Alice maps random bits to them. These instances are marked in gray in Table VIII. She publicly announces the positions of these photons and of the coded random bits after Bob receiving the returned photons. Armed with the knowledge of his preparation bases and original quantum states, Bob directly decodes the confidential payload messages and random bits by using the same preparation bases to measure the returned photons. Then the error rate is estimated to assess if there has been any eavesdropping attack from Eve.

By now the confidential payload messages have been transmitted directly over the quantum channel. In addition to the capability of detecting the presence of an eavesdropper, the communicating parties must ensure that the secret messages are unlikely to be leaked to an eavesdropper before she is detected. Therefore, eavesdropping detection is necessary before mapping the secret messages to the single photons. Although the eavesdropper can intercept the quantum states carrying the confidential messages in the second transmission, she can only infer random results by measuring them, since she is unaware of the original quantum state. Alice encodes the confidential message in Step 2 just like in the one-time pad encryption. The quantum batch C_2 is then inserted

---

[7]This is a process of quantum one-time pad, because it relies on inserting some decoy photons into the message photons and only Alice knows the positions of these decoy photons.
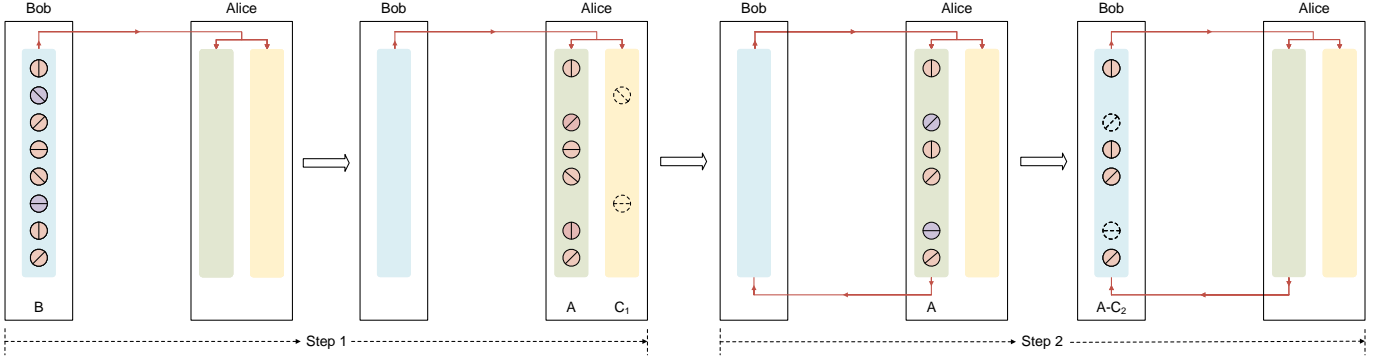
Fig. 18. Illustrating of DL04 QSDC protocol. The circles having vertical, horizontal, diagonal, and backslash lines correspond to the quantum state $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$, respectively. To distinguish the Eve-checking samples from the confidential messages, the checking samples are denoted by the purple circles although they are also in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

TABLE VIII
DL04 QSDC PROTOCOL EXAMPLE CORRESPONDING TO FIG:18.

Step 1									
Bob	Preparation bases	Z	X	X	Z	X	Z	Z	X
	Original quantum states (A-batch)	$|0\rangle$	$|-\rangle$	$|+\rangle$	$|1\rangle$	$|-\rangle$	$|1\rangle$	$|0\rangle$	$|+\rangle$
Alice	Eavesdropping detection		X				X		
	Quantum states detected		$|-\rangle$				$|+\rangle$		
Step 2									
Alice	Encoding operations	I		I	U	U		U	I
	Quantum sates after encoding (B-batch)	$|0\rangle$		$|+\rangle$	$|0\rangle$	$|+\rangle$		$|1\rangle$	$|+\rangle$
	Secret message bits or random number bits	0		0	1	1		1	0
Bob	Measurement bases	Z		X	Z	X		Z	X
	Decoding Results	0		0	1	1		1	0

randomly into the secret message encoding sequence in this QSDC protocol, which encrypts the transmitted messages to ciphertext. A QSDC protocol relying on single photons was presented in [272], where every qubit can carry 2 bits of information, as the transmitter can map messages both to the polarization states and to the spatial-mode states of single photons completely independently.

4) High-dimensional two-step QSDC protocol: Consider a quantum system relying on a d-dimensional Hilbert space [315], where a set of maximally d-dimensional Bell states can be defined as follows

$$|\Psi_{nm}\rangle = \sum_j e^{2\pi ijn/d}|j\rangle \otimes |j \oplus m\rangle/\sqrt{d}, \quad (35)$$

where we have $n, m, j = 0, 1, \cdots, d - 1$, $j \oplus m = (j + m) \bmod d$. The unitary transformation of

$$U_{nm} = \sum_j e^{2\pi ijn/d}|j \oplus m\rangle\langle j| \quad (36)$$

can map the Bell state $|\Psi_{00}\rangle = \sum_j |j\rangle \otimes |j\rangle/\sqrt{d}$ to the Bell state $|\Psi_{nm}\rangle$, formulated as

$$U_{nm}|\Psi_{00}\rangle = |\Psi_{nm}\rangle. \quad (37)$$

Now, let us describe the detailed steps of the high-dimensional two-step QSDC protocol of [61] with the aid of Fig. 19.
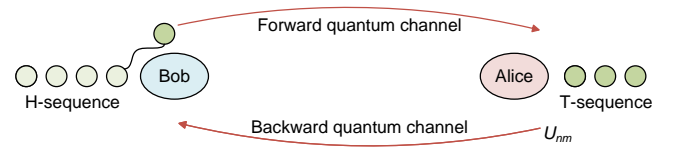

Fig. 19. Scheme showing principles involved in the high-dimension two-step QSDC of [61]. The connected circles represent an EPR pair. The bottle green circle is the EPR partner particle that belongs to what we refer to as T-sequence, while the light green one belongs to the H-sequence. U_{nm} is the unitary transformation used for encoding.

- **Step 1, state preparation**. Bob prepares a sequence of d-dimensional Bell states $|\Psi_{00}\rangle_{HT}$. The subscripts H and T serve as the labels of the two particles in the EPR pairs. Explicitly, H represents the home particle of Bob while the T-particle will be transmitted by Alice to Bob and returned to Alice later. Bob selects one of the particles in each EPR pair to construct a partner particle queue, i.e., $[P_1(H), P_2(H), P_3(H), \cdots, P_N(H)]$, termed as the home sequence or H-sequence for short. Thus the other new queue of $[P_1(T), P_2(T), P_3(T), \cdots, P_N(T)]$ is composed of the remaining partner particles of each and every EPR

pair. This queue may be referred to as the travel sequence or T-sequence. The subscript N refers to the EPR pair index in the sequence.

- **Step 2, first transmission and first eavesdropping detection**. Bob sends the T-sequence to Alice, and then they carry out the following substeps to finish the first eavesdropping detection. (a) Alice randomly selects one of several conjugate single-particle measurement bases to measure each of the sample particles, which are randomly picked from the T-sequence; (b) Alice then publishes the index of sample particles and also the choice of the measurement bases applied to them; (c) Bob applies measurements to the EPR partner particles of those that are Alice's sample particles; (d) both Alice and Bob disclose their own measurement results, hence Bob compares his measurement results to those of Alice to check whether or not an eavesdropper attack perturbs the quantum states. If their results are highly correlated, they continue to the next step. Otherwise, the first transmission of particles is insecure and they have to abandon this communication session and restart from Step 1.
- **Step 3, information encoding**. Alice maps her secret message bits to the photons of the T-sequence with the aid of the unitary operation U_{nm}, but excludes the specific sample particles that have been chosen in Step 2. In addition, Alice and Bob have to detect the presence of the eavesdropper by comparing their appropriately selected particles for estimating the error rate. To do this, Alice randomly chooses some photons of the T-sequence for conveying random bits during the process of secret message encoding. She will not expose the position and the encoding bases U_{mn} of these sample particles before Bob receives the T-sequence. Since the encoding bases of the secret message and random bits are U_{mn}, the eavesdropper does not know, which particles carry the message and which convey random bits. This is beneficial for confidentiality.
- **Step 4, measurement**. Bob applies a joint BSM to every EPR pair after receiving the T-sequence from Alice. At this time, he has both the H-sequence and T-sequence again, except for the sample particles that have been used for the first eavesdropping detection.
- **Step 5, second eavesdropping detection**. After Alice sends the index of the sample particles and the type of unitary operation in Step 4 as classical information to Bob, he carries out the second eavesdropping detection by combining his own measurement results. If the error rate is too high, Alice and Bob must abandon this transmission session and restart it from the beginning.

As discussed in Ref. [316], the high-dimensional two-step QSDC provides better security than that obtainable with the aid of two-dimensional Bell states [53]. Furthermore, the protocol has the advantage of high capacity [317], where a particle can carry $\log_2 d^2$ bits of classical information.

5) Measurement-device-independent QSDC protocol: In theory, the quantum cryptographic protocols are unconditionally secure as guaranteed by the laws of quantum physics. However, the practical devices suffer from inevitable imperfec-

tions that can be exploited by the eavesdropper to infer some confidential information, especially when using single-photon detectors. For example, Huang *et al.* [318] showed that QSDC systems may be compromised by detector blinding attacks [319]. As a remedy, measurement-device-independent (MDI) protocols were proposed for protecting practical quantum cryptographic systems against the detector side channel attacks [78], [79]. In the MDI protocol, the measurement-device is under the control of an untrusted party called Charlie who performs a BSM. Note that even if an adversary controls the measurement-device, he would not gain any useful information about the confidential message. Hence MDI protocols can remove all security loopholes from the measurement unit. More significantly, the realization of MDI protocols is entirely feasible at the time of writing. Recently, Gao *et al.* [320] proposed a long-distance MDI QSDC protocol by relying on ancillary entangled sources, which were located in the middle of the link by adding an extra relay node.

The measurement-device-independent QSDC protocol is illustrated in Fig. 20, which relies on both single-photon states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and Bell states $\{|\psi^+\rangle, |\psi^-\rangle, |\phi^+\rangle, |\phi^-\rangle\}$. It may be summarized in the following steps [78].
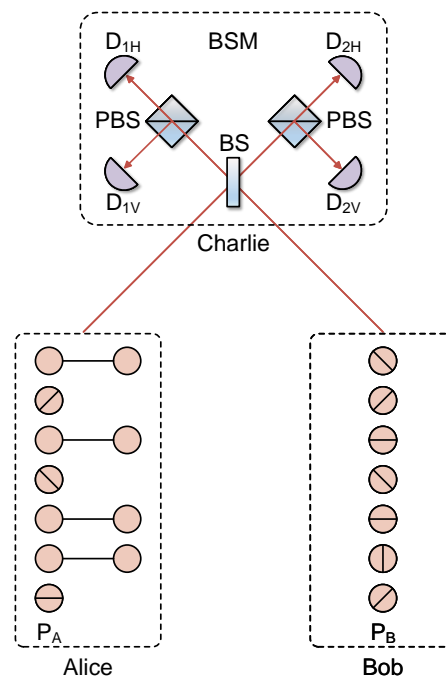

Fig. 20. The MDI QSDC protocol. Two circles linked with a line denote the Bell state $|\psi^-\rangle$. The circles having vertical, horizontal, diagonal, and backslash represent the single photons $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$, respectively. BS: beam splitter, PBS: polarization beam splitter, D: single photon detector, BSM: Bell-state measurement.

- **Step 1, state preparation**. Alice prepares a queue of $N + t_0$ EPR pairs, all of which are in the state $|\psi^-_{12}\rangle$. Then the EPR pair sequence is separated into two parts: S_{Ah} and S_{At}, each of which includes one of the particles in the EPR pair. She also generates a sequence of t_1 single photons, each randomly representing one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. These single photons are then randomly inserted into the EPR partner particle sequence

S$_{At}$. Therefore an ordered qubit sequence P$_A$ is prepared by Alice, as seen in Fig. 20. In the meantime, Bob produces a sequence of $N + t_0 + t_1$ single photons, which are randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. This sequence is denoted by P$_B$ in Fig. 20.

- **Step 2, qubit transmission and measurement**. Alice sends the sequence P$_A$ to an untrusted relay termed as Charlie and located in the middle, while Bob sends the sequence P$_B$ to Charlie. Charlie then performs a BSM that projects the incoming qubits into a Bell state, and he publishes the measurement results. Once a partner particle from an EPR pair of P_A and a single photon from P_B are projected into a Bell state, the other partner particle of Alice is instantaneously collapsed into one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ with equal probabilities[8], as shown in Table IX. The state after BSM can be deduced by Bob according to Table IX, but it is unknown to anyone else. For example, Alice's state is $|0\rangle_1$ for $|\psi_{12}^-\rangle|1\rangle_3$ if the BSM result of Charlie is $|\phi_{23}^+\rangle$.

- **Step 3, eavesdropping detection**. To proceed further, Alice announces publicly the index and states of the t_1 single photons. Bob also publishes the state of the corresponding single photon in the sequence P_B. They then compare the BSM results, where they employ the same bases. The method of eavesdropping detection is identical to that in the MDI QKD [321]. A BSM will project the incoming two photons that were prepared by the same two bases into one of the two Bell states, formulated as,

$$|+\rangle_1|+\rangle_3 = \frac{1}{\sqrt{2}} \left(|\phi^+\rangle_{13} + |\psi^+\rangle_{13} \right), \tag{38}$$

$$|+\rangle_1|-\rangle_3 = \frac{1}{\sqrt{2}} \left(|\phi^-\rangle_{13} - |\psi^-\rangle_{13} \right), \tag{39}$$

$$|0\rangle_1|0\rangle_3 = \frac{1}{\sqrt{2}} \left(|\phi^+\rangle_{13} + |\phi^-\rangle_{13} \right), \tag{40}$$

$$|0\rangle_1|1\rangle_3 = \frac{1}{\sqrt{2}} \left(|\psi^+\rangle_{13} + |\psi^-\rangle_{13} \right). \tag{41}$$

Charlie has a 50% probability to obtain the other two Bell-states in the face of eavesdropping attacks, so the error rate is increased. Nonethless, if the error rate remains below the maximum tolerable level, they proceed to the next step. Otherwise, they decide to abort the communication session.

- **Step 4, confidential message encoding**. As her next action, Alice applies one of two unitary operators $\{I, i\sigma_y\}$ to the particles in her hand where the unitary operation $U_m = I$ represents 0 and the operation $U_m = i\sigma_y$ corresponds to 1. To provide an integrity check for the confidential message, t_0 EPR pair partner particles are randomly positioned to encode random bits. Then Bob publishes his preparation bases of the remaining single photons.

- **Step 5, qubit transmission and measurement**. Alice

[8]This is actually a process of quantum teleportation carried out in a more complicated manner, in which Bob's state associated with a unitary operation U_T ($U_T = I$ or $U_T = i\sigma_y$) is teleported to Alice. U_T is only known by Bob.

sends the qubits to Charlie after encoding. Charlie measures the qubits by using the bases that Bob has published in Step 4 and announces the measurement results.

- **Step 6, decoding and integrity check**. Bob decodes Alice's bits by combining his initial states with the measurement results of Step 2 and Step 5. Alice discloses the index of the t_0 EPR pair partner particles selected as well as the random bits mapped to them. If no perturbation is imposed by Eve and the direct communication is deemed to be secure, the error rate will be below the maximum tolerable threshold. Then Bob obtains the confidential payload message bits.

TABLE IX
THE CORRESPONDENCE AMONG BOB'S STATE, CHARLIE'S BSM RESULT AND ALICE'S STATE.

		Charlie's BSM results			
		$|\phi_{23}^+\rangle$	$|\phi_{23}^-\rangle$	$|\psi_{23}^+\rangle$	$|\psi_{23}^-\rangle$
Bob's state	$|0\rangle_3$	$-|1\rangle_1$	$-|1\rangle_1$	$|0\rangle_1$	$-|0\rangle_1$
	$|1\rangle_3$	$|0\rangle_1$	$-|0\rangle_1$	$-|1\rangle_1$	$-|1\rangle_1$
	$|+\rangle_3$	$|-\rangle_1$	$-|+\rangle_1$	$|-\rangle_1$	$-|+\rangle_1$
	$|-\rangle_3$	$-|+\rangle_1$	$|-\rangle_1$	$|+\rangle_1$	$-|-\rangle_1$

The MDI QSDC protocol has the same security level as the MDI QKD protocol in Step 3 and the teleportation process of Bob's state is also secure after the eavesdropping detection. Firstly, Alice sends two kinds of photons to Charlie, but they have the same density matrix, $Tr_1 \left(|\psi_{12}^-\rangle\langle\psi_{12}^-| \right) = I/2$ for the EPR pairs and $\frac{|0\rangle\langle 0|}{4} + \frac{|1\rangle\langle 1|}{4} + \frac{|+\rangle\langle +|}{4} + \frac{|-\rangle\langle -|}{4} = I/2$ for single photons. Hence Eve cannot differentiate between the EPR pair particles and single photons. Secondly, Bob knows the initial state $|q\rangle_3$, but it is sealed to others, so only he can infer the unitary encoding operation U_m of Alice, even though both Alice and Charlie know the result of $U_m|q\rangle_3$.

6) Continuous variable DSQC protocol: The DSQC protocol has also been extended to the continuous-variable (CV) domain related to infinite-dimensional Hilbert spaces [67], [117], [224], [270], [273]. The continuous variable DSQC scheme uses the squeezing phase of a two-mode squeezed state, as detailed in [117]. The characteristics of the two-mode squeezed state are eminently suitable for quantum direct communication and the associated communication protocol is shown in Fig. 21. The whole process can be divided into the following 6 steps:

- **Step 1, state preparation and transmission**. Alice generates and distributes the two-mode squeezed state, keeping one of the modes at her side and sending the other mode to Bob over a quantum channel as indicated by Fig. 21. A coherent-state local oscillator LO$_2$ is also sent to Bob by Alice together with the transmitted mode by using a polarizing beam splitter for combining them.

- **Step 2, encoding**. Alice mapps the confidential messages to her part of the two-mode squeezed state by imposing a phase shift on the LO$_1$ and then carries out homodyne detection. She also inserts check bits at random time slots throughout the message encoding process, so that the communicating parties can detect eavesdropping.
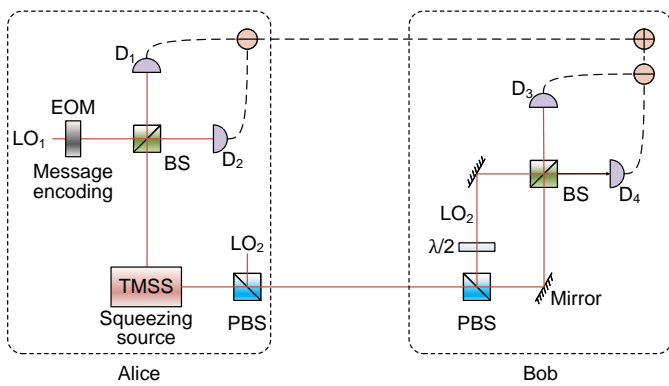
Fig. 21. Schematic of the CV DSQC protocol using two-mode squeezed states. LO: local oscillator, EOM: electro-optical modulator, BS: beam splitter, TMSS: two-mode squeezed state, PBS: polarizing beam splitter, D: photodetector, $\lambda/2$: half wave plate.

- **Step 3, measurement**. Bob splits the incoming beam in half at his polarizing beam splitter, which are then distributed to the separate parties, namely to LO_2 and to the squeezed mode. Then, they are combined in a balanced beam splitter to perform homodyne detection and the phase of LO_2 is kept constant during the measurement.
- **Step 4, repeated transmission**. Alice and Bob repeat Step 1 to Step 3 until the secret messages have been completely encoded.
- **Step 5, eavesdropping detection**. Alice informs Bob of the time slot of her Eve-check bits and of the corresponding measurement results. Alice and Bob publicly compare the Eve-check bits to evaluate the error rate and confirm whether an eavesdropper is present. If the channel's integrity has been verified, they continue to the next step. Otherwise, they restart their communication session over a different quantum channel.
- **Step 6, message decoding**. Alice sends the measurement results of the confidential messages to Bob. Once the two local measurement results are combined by Bob, he will have a signal whose variance fluctuates between two different levels, which represent the confidential information of Alice. Hence, Bob can retrieve the entire confidential message.

This protocol is immune to the intercept and resends attacks. Eve may intercept the mode sent to Bob. If this occurs, then she can extract the information of squeezing degree and she can then resend a new mode at the same squeezing degree to Bob. This fraudulent action can be easily detected from the new mode sent by Eve, because it is not entangled with the mode retained by Alice. More explicitly, this will result in increased noise and no pair of distinct variance in the combined signal of Bob. As for the partial interception strategy, Eve can acquire part of the beam and combine it with the published measurement results of Alice to steal information. However, this will result in a reduction of the squeezing degree, making it easy to detect.

7) ZXFZ DSQC protocol: In 2003, a specific encryption scheme was invented [322], which was subsequently adopted

also to design a DSQC protocol by Zhu, Xia, Fan, and Zhang (ZXFZ) [116], [323]. Below we summarize the ZXFZ DSQC protocol, which is based on a secret transmission order of EPR pairs [116]. To elaborate, Alice and Bob exploit that the unitary operations of $U_0 = I = |0\rangle\langle0| + |1\rangle\langle1|$, $U_1 = \sigma_z = |0\rangle\langle0| - |1\rangle\langle1|$, $U_2 = \sigma_x = |1\rangle\langle0| + |0\rangle\langle1|$, and $U_3 = i\sigma_y = |0\rangle\langle1| - |1\rangle\langle0|$ are used for conveying two bits of confidential information 00, 11, 01, and 10, respectively.

- **Step 1, state preparation**. Alice prepares an EPR pair sequence, where $[P_1(1,1'), P_2(2,2'), \cdots, P_i(i,i'), \cdots, P_N(N,N')]$, each pair is in the same state of $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_i|1\rangle_{i'} - |1\rangle_i|0\rangle_{i'})$. A sufficiently large subset is selected for the Eve-checking set (C set) and the rest of the EPR pairs serve as the confidential message set (M set). The basic elements of the C set or M set are EPR pairs, rather than being a single photon of an EPR pair. Alice uses the above four unitary operations for encoding the confidential message onto the M set, while random bits are mapped to the C set. Taking the C set as an example, Alice's random bits are $(0100101101\cdots)$ and she chooses the first 50 EPR pairs as the C set. So she maps 01 to $P_1(1,1')$, 00 to $P_2(1,1')$, 10 to $P_3(3,3'),\cdots$, by applying the four unitary operations to one of the particles in each EPR pair.
- **Step 2, transmission**. Given a secret transmit order of particles, Alice sends these particles to Bob one by one. A partner particle in the EPR pair is taken as the minimal transmitted unit. For instance, Alice sends the particles in the order of $S_1(2)$, $S_2(1)$, $S_3(51)$, $S_4(5')$, $S_5(2')$, $S_6(60)$, $S_7(10)$, $S_8(1')$, $\cdots$, $S_j(x)$, $\cdots$, $S_k(x')$, $\cdots$, $S_{2N}(y)$, where $S_j(i), (j \in \{1,2,\cdots,2N\}, i \in \{1,2,\cdots,N\})$. This means that Alice sends the original particle i at the $j-$th output index.
- **Step 3, announcing correlation**. Bob confirms to Alice that he has recieved all the $2N$ particles. Alice then announces the exact quantum correlation of two particles that pertain to the C set over a public channel as exemplified by $S_2 \sim S_8$, $S_1 \sim S_5$, $\cdots$, $S_j \sim S_k$, $\cdots$.
- **Step 4, eavesdropping detection**. Bob performs a BSM based on the pairs Alice has told him, and then the measurement results are published subsequently. Upon comparing the measurement results with her original information, Alice estimates the error rate and detects the presence or absence of eavesdroppers.
- **Step 5, announcing correlation**. When Alice can ascertain that no eavesdropper is present, she classically informs Bob of the matching information of two particles in the M set. If Alice finds an unacceptably high error rate, she curtails the communication session and starts a new one from the Step 1.
- **Step 6, measurement**. Finally, Bob decodes the confidential messages by performing the BSM.

The security of this protocol is ensured by the secret order of the particles. Even if Eve captures all the particles, she cannot glean any useful message without knowing the correct order. But this scheme becomes insecure, if an eavesdropper

steals the secret message by relying on Trojan horse attack strategies, hence it has been improved in Ref [324].

8) Other protocols for QSDC or DSQC: As detailed above, numerous theoretical proposals have been conceived for QSDC or DSQC, in which the communication security is guaranteed by encrypting information using quantum states [67], [77], [270], [325] or by denying eavesdroppers access to the entirety of correlated quantum states [75], [81]. To achieve confidential direct communication, Alice can also map the secret message to a coherent state $|\alpha_M\rangle$ and add a random amplitude α_R chosen from a Gaussian-distribution for ensuring that an encrypted quantum state of $|\alpha_M + \alpha_R\rangle$ is used for conveying confidential information along with random bits, which will be revealed to Bob for assisting his message decoding via the classical authentication channel [67], [270]. The technique of quantum data locking [77] provides a new way of realizing QSDC under the realistic practical assumption that Eve can only access quantum memories having limited coherence time. The secret messages are encoded onto a quantum state and locked by a random unitary operation applied to it. Then the locked quantum state containing messages is transmitted from Alice to Bob. Bob can unlock the original message by using an inverse unitary operation. The choice of the unitary operations between Alice and Bob depends on a pre-shared key, which could be generated using QKD. Both the protocols in [67], [270] and in [77] required only the transmission of quantum states over a quantum channel once, thus they were less corrupted by channel impairments. By contrast, a pair of transmission is required in conventional QSDC protocols [42], [53], [54], [61].

Additionally, both the quantum illumination [74], [75] and quantum low probability of intercept techniques [81] exhibit impressive potential for realizing QSDC at Gigabits per second communication rates only using single-wavelength operations over metropolitan-area fiber channels. In these two schemes, a spontaneous parametric down-conversion operation emits entangled signals and idler beams. Then the signal beam is transmitted to the transmitter of information for message encoding, while the idler beam is retained by the receiver of information. The receiver can recover transmitter's message by combining her idler beam and the returned signal beam as a benefit of their initial entanglement.

The above examples of QSDC or DSQC protocols include both discrete variable and continuous variable systems, proposing new techniques for realizing point-to-point quantum communication, where confidential messages can be transmitted directly through the quantum link between a pair of legitimate users. The most striking contrast is in the additional classical communication step of Fig 15. Explicitly, DSQC protocols need the transmitter's additional classical information for message decoding, whereas for QSDC there is no need to do this. This transmission from Step 6 of the continuous variable DSQC protocol relies on two-mode squeezed states, where Alice reveals her measurement results, and she also announces the matching information in Step 5 of the ZXFZ DSQC protocol.

While still relying on the basic principles of the earliest QSDC schemes, we can choose different physical entities to implement QSDC [55], [56], [66], [71], [75], [269], [290], [300], [326]–[333]. There are three fundamental features of a peer-to-peer QSDC protocol [50]:

- (a) QSDC enables secure communication without the need for pre-distributed secret keys.
- (b) The encoded information can be read out deterministically by the receiver without a basis reconciliation step, and hence in principle there is no additional classical bit exchange between the transmitter and the receiver, except for the process of eavesdropping detection and error rate estimation.
- (c) Eve will be detected by the legitimate users in real-time.

Protocols that do not meet the above three characteristics are typically referred to as quasi-QSDC protocols [50].

The most appealing feature of QSDC protocols is that a pair of legitimate users can prevent information leakage before eavesdropper detection. The eavesdropper can be detected by sampling the measurements of quantum cryptographic protocols, but information leakage cannot be avoided. To elaborate a little further, QKD is developed for transmitting a cryptographic key. If the eavesdropping detection of QKD discovers the presence of Eve, even if the encoded information has already been unveiled to Eve, the key is simply discarded. However, when the confidential message itself is transmitted directly, the legitimate users cannot throw away the message. Thus some new concepts were created:

block based transmission and transmission order rearrangement.

In block based transmission, Alice and Bob have to transmit a batch of quantum states and for the sake of preventing the leakage of a secret message they must carry out an Eve-check procedure to ascertain the absence or presence of an eavesdropper. By contrast, in case of order rearrangement Alice first encodes the confidential message and then reorganizes the position of the particles within a block, while keeping the order secret. However, the secret transmit order of particles may be announced publicly, provided that security of the channel has been confirmed. The above block transmission and order rearrangement methods are popularly used for constructing quantum communication protocols [73], [324], [334]–[338].

B. Advances in security analysis

Classified by Eve's powers, three different types of attacks are commonly considered in QSDC's security analysis:

- **individual attack**: Eve prepares separate ancilla states, each of which is used as a probe to interact independently with qubits and these probes are measured one after the other;
- **collective attack**: Eve independently attaches probes to each qubit, but she stores these ancilla states in the quantum memory to perform an optimal collective measurement at any later time;
- **coherent attack**: Eve prepares a global ancilla state to be used as a probe for interacting with all qubits. Then the ancilla state is stored and collectively measured. This is the strongest class of attacks that Eve could carry out.

Individual attacks are the only ones that are feasible with the aid of existing quantum technologies, while both collective attacks and coherent attacks rely on quantum memories having long coherence time and coherent quantum operations associated with high fidelity, which are unavailable at the time of writing. However, despite the unavailability of quantum memory, the eavesdropper is assumed to have full access to the quantum channel and have all quantum technologies - some of which are unavailable at the time of writing - at her disposal, while operating without violating the laws of quantum mechanics. Cleraly, sustaining confidentiality even under these worst-case assumptions would make the security of quantum communication 'unconditional'. Additionally, it is assumed that Eve can monitor the classical authentication channel, but cannot tamper with it. A quantum communication scheme cannot be generally regarded as being information-theoretically secure until it is proven to be secure against coherent attacks [170].

The security proof of QSDC protocols is still considered to be work in progress. The challenge in this context is that Eve can attack the qubits traveling along the two-way channel. Similarly, the above three different types of attacks can also be considered in the security analysis QSDC. The security analysis of the initial QSDC protocols focused on tackling individual attacks was given in [53], followed by that of collective attacks in [60].

QSDC protocols can be changed to the DQKD protocols, when dispensing with block transmissions, that is, when the number of qubits N is reduced to 1. The paradigmatic examples of DQKD are the Ping-Pong protocol of [103] and the LM05 protocol of [105]. In [105], Bob randomly produces a photon polarized in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and he transmits it to Alice. When this particle reaches Alice, she measures it with a probability of c with the objective of eavesdropping detection (checking mode), or she uses it for conveying a secret key bit with probability $1 - c$ (encoding mode). After encoding the particle it is sent back to Bob. The above steps are repeated until all key bits are transmitted. Then Bob can deterministically access the secret key as well as an estimate of the error rate experienced during transmission over the forward quantum channel (Bob-Alice) after Alice revealing the index of Eve-checking bits. Alice will also publish some part of the key bits for estimating the error rate in the backward quantum channel (Alice-Bob). If entanglement is used, one particle of the entangled state will travel in a forward-backward manner for supporting the information flow [103]. There is no block based transmission in DQKD protocols, so they are similar to the DL04 or to the two-step QSDC protocol when $N = 1$. The security of DQKD protocols has been analyzed in [70], [339]–[348]. Some of them are analyzed under the scenario of Alice and Bob using QSDC protocols to distribute the cryptographic key, but they are appropriate for the security analysis of QSDC. To elaborate a little further, diverse individual attack strategies are discussed in Ref. [344] and the upper bound of the amount of information stolen by Eve has also been given. A pair of legitimate communication parties can also benefit from encountering a scenario in that Eve attacks both the forward and the backward channel, because these correlated attacks may be more easily detected [345]. Eve can only access the confidential information probabilistically by combining a photon number splitting attack with methods of state discrimination, even if a weak coherent pulse source is adopted [339], [348]. In 2011, Lu *et al.* [70] proved that the DL04 protocol is secure against collective attacks, when the secret key is transmitted by QSDC while relying on idealized perfect devices. In their proof, Eve attaches separable ancilla states to each qubit and applies a unitary operation to the joint state. She keeps the ancilla states in a quantum memory until receiving the qubit from Alice after encoding. In order to infer the maximal possible amount of information from a secret message, the optimal measurement is performed by combining the encoded state and her ancilla state. The the joint state of Bob's initial state, Alice's encoded state, and Eve's attack were used for estimating the maximal possible amount of information that Eve can extract. On this basis, Lu *et al.* [342] assumed that Eve controls the detector and performs measurements by exploiting the measurement bases Bob has passed to her. The results showed that all detector-side-channel attacks are futile in the channel of Alice-Bob. Moreover, Beaudry *et al.* [343] and Henao *et al.* [347] also gave the security proof of two-way protocol.

In the framework of taking collective attacks into consideration, the security of practical QSDC systems may be analyzed from an information theoretical point of view by relying on Wyner's wiretap channel theory [349]. The mutual information $I(A:B)$ quantifies the information rate at which Bob can reliably receive from Alice. By comparison, the channel quality of the eavesdropper link and the maximum attainable information rate of a malicious Eve is given by $I(A:E)$. The lower bound of the secrecy capacity of the DL04 protocol can be expressed as [60], [86], [350]

$$
\begin{aligned}
C_s &= \max_{\{p\}} \{I(A:B) - I(A:E)\} \\
&= Q_{\text{Bob}}[1 - h(e)] - Q_{\text{Eve}}h(e_x + e_z) \\
&= Q_{\text{Bob}}[1 - h(e) - gh(e_x + e_z)],
\end{aligned} \tag{42}
$$

where Q_{Bob} is the reception rate of Bob, Q_{Eve} is the maximum rate Eve can access the qubits, e is the quantum bit error rate, e_x and e_z is the error rate under X-basis and Z-basis of the first eavesdropping-check, g is the gap between Q_{Eve} and Q_{Bob}, and finally $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function. By contrast, the lower bound of the secrecy capacity of the two-step protocol is given by [350]

$$
C_s = Q_{\text{Bob}}[2 - h_4(\mathbf{e})] - Q_{\text{Eve}}[h(e_x) + h(e_z)], \tag{43}
$$

where $h_4(\mathbf{e})$ is the 'four-array' Shannon entropy and $\mathbf{e}$ is error distribution.

A promising solution capable of increasing the channel capacity using masking was proposed in [351], where Eve's effective reception rate is limited to $Q_{\text{Eve}} = Q_{\text{Bob}}$, namely $g = 1$. Therefore, the secrecy capacity limits the maximum rate at which Alice can directly convey confidential messages to Bob through the quantum channel under the guarantee that Eve has no useful information about the confidential

message. The secrecy capacity of MDI QSDC was given in [96], [97], [352]. In addition, the finite-length security analysis of QSDC is currently under investigation [90]. In order to obtain the real-life secrecy capacity of QSDC, some of its practical influencing factors are starting to be taken into account, such as the detector efficiency mismatch [353], side-channel effects [353], source imperfections [97], [353], and so on.

C. The cryptographic applications of point-to-point QSDC protocols

The blueprint of managing security in communication has been proposed in [354], where end-users of communications networks utilize specific quantum communication systems having different security levels. QSDC constitutes an important fundamental communication protocol capable of supporting high-level security. Hence, numerous quantum cryptographic solutions have been derived from QSDC, as seen in Table X and Table XI. Based on the DL04 QSDC protocol, a single photon is harnessed by Alice and Bob during their one-way [355] or two-way transmission [356], where both of them deduce their secret messages after the announcement of measurement results. The role of Alice and Bob is symmetric. Explicitly, when Bob receives the sequence of M photons, as shown in Fig.17 of the two-step QSDC protocol, Alice and Bob hold half of every EPR pair in the state $|\psi^-\rangle$. They both are able to encode their secret messages and speak to each other (dialogue) [357]. This makes it natural to apply QSDC for the design of the quantum dialogue protocols of [337], [358].

In 2005, the new concept of quantum secret sharing under QSDC was presented in Ref. [62], where the advantages of both QSDC and quantum secret sharing are combined. This allows Alice to transmit a secret message to different agents, where no single person is capable of reconstructing the complete original message, unless the users cooperate. Such protocols can be classified based on their information carriers. Some of them are based on single photons [62], [360]–[362] and rely on the character of 'DL04'. Others employ entangled states [363], [364] and exhibit a 'two-step' or 'high-dimensional' character. In the protocols using a single photon, a batch of N initial single photons is prepared by the first agent, and then the next agents apply the unitary operations[9] to each and every photon to encrypt them. These photons will be transmitted to Alice after the last agent completes the encryption. Then eavesdropping detection and the encoding of secret messages is carried out followed by return to the last agent. If all agents act in concert, all of them can acquire the secret message by applying their repective preparation bases and encryption operations. However, the process is slightly different, when it comes to entanglement-based protocols, where Alice first prepares an EPR photon pair sequence according to her secret message and randomly

inserts some checking photon pairs into it. A partner EPR particle sequence is encrypted by the agents alternately, and Alice sends the retained sequence to the last agent for their cooperation to decrypt the secret message in the event of having no eavesdroppers.

QSDC schemes associated with authentication are composed of two parts: one of them is for an authentication process and the other is for direct communication [63], [365], [366], [388]. These protocols are able to resist man-in-the-middle attacks. Commencing from the principles of three-party QSDC associated with GHZ states [56], the authors of [367]–[370] put forward the concept of quantum sealed-bid auction. The auctioneer, say Alice, prepares a set of M groups of n-particle GHZ states and then she distributes each n-particle GHZ state to n bidders. These bidders encode their own bid information and return the corresponding particles to Alice for an n-particle GHZ-basis measurement. After this, the winner of the auction will be revealed to all bidders. Of course, both EPR pairs [371], [372] and single-photon schemes [373] can also be used as the basic resources of quantum sealed-bid auction.

By combining the two-step QSDC protocol and ping-pong protocol, the quantum steganography philosophy was is proposed in [374], [375]. Explicitly, a pair of users employ block transmission to prevent information disclosure. Accordingly, first Bob prepares a large number of entangled states. Then the first layer of secret information is transmitted in the same way as in the ping-pong protocol, but auxiliary Bell states are introduced for capacity improvement. Then two adjacent BSM results are picked by Alice to act as the second secret information, which can be read out by the process of entanglement swapping as detailed in [374], [375]. This is how the hidden secret message is embedded. As a further advance, another 'hidden rule' was conceived based on the tensor product of Bell states and unitary transformations for employment in quantum steganography [376]. Inspired by quantum steganography, the hidden layer of secret messages was also exploited for quantum watermaking [377], [378]. The covert quantum channel is established by changing the secret message encoding rule of QSDC, which can also be used for the transmission of confidential messages [379].

In the protocol of quantum domain anonymous ranking, each user can acquire the correct rankings of his/her data, but nobody else can infer it [380]. An ordered sequence of N two-qudit entangled pairs is grouped into a pair of sequences and one of the sequences will visit the station of every users one by one to register their data, while the other sequence is kept at its source. According to the measurement results announced in the final stage, each of the N users can get anonymously the ranking of his/her own data. Decoy qudits are required in some random positions of the photon sequence for detecting eavesdroppers and hence to secure the quantum channel. In [381], [382], the decoy photons are randomy inserted into the sequence of photons of the GHZ states similarly to the procedure of quantum one-time pad in DL04, where the decoy photons are prepared for authenticating users, while the GHZ states can be used for QSDC broadcasting to N-receivers.

In [383], the authors proposed a quantum version of the process of arbitrated signature between two users and a trust

---

[9]The unitary operation set is different from that of the encoding operation set in the QSDC protocol. For instance, an additional Hadamard gate operator is brought into the original encoding operation set. It is carefully picked by the agents for avoiding that a single agent intercepts and recovers the whole message independently.

TABLE X
AN OVERVIEW OF THE STUDIES ON DIFFERENT TYPES OF QUANTUM CRYPTOGRAPHIC PROTOCOLS BASED ON QSDC.

Primitive QSDC protocol	Different types of quantum cryptographic tasks	Design objective	Related references (studies)
DL04	Quantum dialogue	To realize bidirectional QSDC, in which both legitimate users are the sender of the secret message as well as the receivers, and their secret message can be exchanged simultaneously.	[355], [356]
Two-step			[358], [359]
DL04	Quantum secret sharing of secure direct communication	A dealer wants to share his secret message directly with a group of agents, but the secret message can only be obtained by all the agents if they collaborate.	[62], [360], [361], [362]
Two-step			[363]
High-dimension two-step			[364]
QSDC with GHZ states [63]	Quantum authentication	Verifying the identity of communication participants to prevent a malicious eavesdropper from pretending to be a legitimate user, where a sender can simultaneously transmit a secret message over the quantum channel to the receiver.	[63]
Two-step			[365]
DL04			[366]
Three-party QSDC with GHZ states [56]	Quantum sealed-bid auction	Allowing all bidders to submit their own bids, where the auctioneer makes all the bids public and determines the winning bidder. The honesty of auction must be pledged, and no malicious bidders can collide with the auctioneers.	[367], [368], [369], [370]
Two-step			[371], [372]
DL04			[373]
Two-step	Quantum steganography	Embedding the secret message into another innocent-looking quantum carrier for secure transmission of the secret messages.	[374], [375], [376]
Two-step	Quantum watermarking	Quantum watermarking is utilized to embed owner identification into quantum multimedia, which is difficult to remove.	[377], [378]
High-dimension two-step	Quantum covert channel	To send secret messages over a covert channel which is established within the normal quantum channel.	[379]
Two-step	Quantum anonymous ranking	To allow users to attend a privacy-preserving ranking activity whereby each of the participants involved can anonymously infer his/her ranking information, but cannot get that of others.	[380]
DL04	Quantum broadcast communication	Transmitting secret messages from a sender to a dynamically changing group of receivers, where only the authenticated users can decode the relevant information and others obtain nothing.	[381], [382]

TABLE XI
AN OVERVIEW OF THE STUDIES ON DIFFERENT TYPES OF QUANTUM CRYPTOGRAPHIC PROTOCOLS BASED ON QSDC.

Primitive QSDC protocol	Different types of quantum cryptographic tasks	Design objective	Related references (studies)
Two-step	Quantum signature	To guarantee the security of digital signatures for two participants, so that the message cannot be forged by the receiver or a possible attacker.	[383]
Two-step	Quantum key agreement	To permit each participant to equally contribute to the generation of a shared key, which cannot be determined fully by any of the parties alone. Hence others cannot get the key through illegal means.	[384], [385]
Three-party QSDC with GHZ states [56]			[386], [387]

center. Accordingly, the users sign the public message by using a pre-shared key[10] and the unitary operation of a quantum search algorithm [16], [20]. Then the signed message qubits are transmitted by two-step QSDC. By this means, the message receiver can confirm that the transmitter signed the message legitimately, while the attacker cannot identify the signature and cannot forge it, because QSDC secures the quantum channel. Similarly, if the particles of each entangled states are held by two different users [384] or even more than two users [385]–[387], then every one in the group has the right to modify a key by applying his/her operation to the qubits in hand and the final key is jointly determined by all members.

As seen from the literature, QSDC is indeed capable of high-security communication. Thus QSDC is eminently suitable for a wide variety of quantum cryptographic tasks, which require a direct transport of deterministic information over the quantum channel. Both block transmission and the random decoy photon insertion techniques constitute powerful countermeasures against eavesdropping attacks.

D. Networking schemes

The topology of a hypothetical any-to-any multi-user QSDC system can be of a loop or star structure as shown in Fig. 22, similar to QKD networks [389], [390]. The nodes assume one of three roles: the server, the transmitter (Tx) and receiver (Rx). The server prepares qubits and receives classical requests from all the users on the network. It responds to them over the quantum channel and the classical channel in a different slot. Controllable switches are used for constructing the quantum link between a pair of communicating parties [391].

A multi-user QSDC network can be reduced to that seen in Fig. 23. If two users are not in the same loop or branch, the server of the loop supporting a Tx or Rx will carry out the tasks of qubit preparation, while the other servers will offer the quantum link for their communication. In this case, we assume that only a single subsystem can use the same

[10]The key is generated by QKD, thus this protocol assumes that the key is secure.

quantum channel and classical channel simultaneously [64], [392]. The server prepares a set of EPR pairs in the same quantum state $|\psi^-\rangle_{TR}$, and divides them into two parts, S_T and S_R. The S_T sequence is composed of all the particles marked by T and R in every EPR pair $|\psi^-\rangle_{TR}$, respectively. They will be distributed to two different users. Then a subset of particles is selected randomly to detect eavesdroppers by applying the unitary operation σ_x or σ_z to them, similarly to the process in the two-step QSDC protocol [53]. If the transmission of qubits is deemed to be secure, the transmitter maps its secret message onto the particles of the sequence S_T by applying one of the unitary operations $\{U_0, U_1, U_2, U_3\}$, and then randomly picks some particles for the next eavesdropping detection action. The receiver also uses the sequence S_R for conveying information, where all bit values are randomly set to 0 or 1. The transmitter and receiver transmit the sequence S_T and S_R respectively back to the server. The server applies the BSM to each and every EPR pair received and publishes the outcomes given by $U_A = U_T \otimes U_R$. Then the receiver checks the security and deduces the transmitter's secret messages by applying $U_T = U_A \otimes U_R$. At this stage communication between the network users is completed.

Diverse QSDC networks relying on entanglement [64], [65], [393], on single photon based regimes [394], and on hyper-entanglement [395]–[397] have been conceived, providing an important step forward in terms of achieving any-to-any multi-users QSDC connectivity. Furthermore, the authentication process or identity verification between a quantum server and the users can be validated by entangled EPR pairs and controlled NOT gates [76]. Some of the QSDC features have also been introduced into classical optical virtual private networks and into quantum virtual private networks with the objective of enhancing the security of passive optical networks [398]. To fit into the operational mobile communication framework and allow telecom companies to provide secure communication, a controlled bidirectional QSDC protocol based on the properties of GHZ-states was invented and applied in mobile networks [399]. Some techniques of the network layer, such as quantum multiple access techniques and routing have also
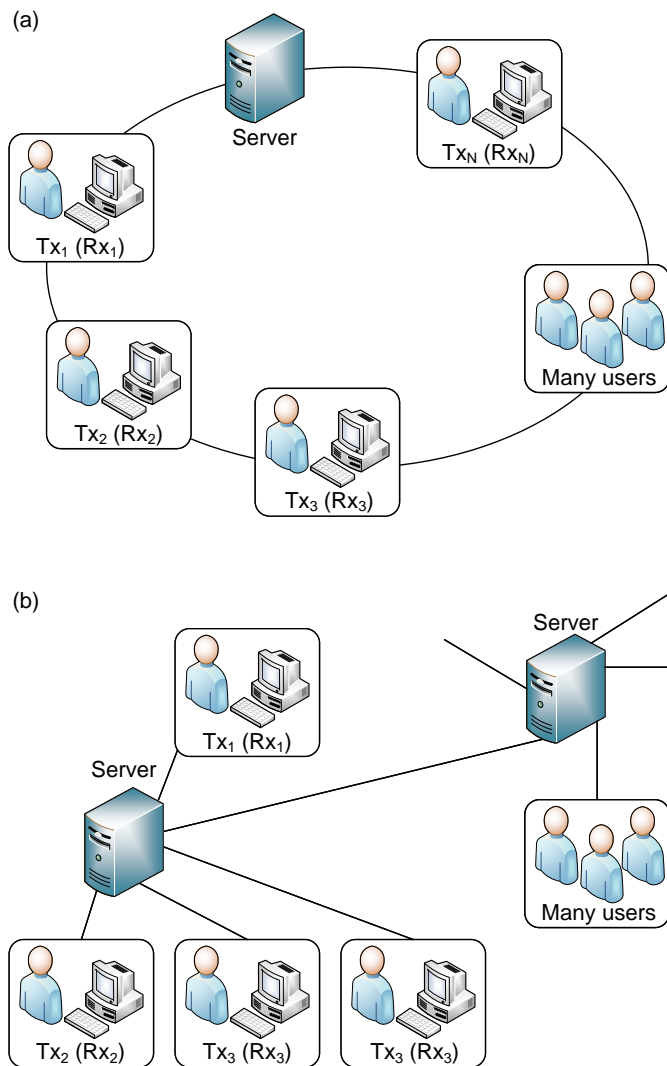
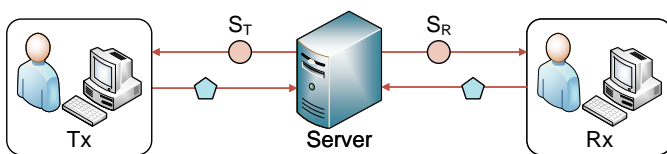Fig. 22. Multi-user network configurations for QSDC. (a) loop-configuration, (a) star-configuration.

Fig. 23. The subsystem of the QSDC network. The pair of circles represent the state $|\psi^-\rangle_{TR}$, while the pair of pentagons denote the state $|\phi^+\rangle_{TR}$.

been considered in multi-user QSDC networks [400], [401]. Indeed, we may view the overall communication networks as a hybrid one relying on a quantum and a classical channel, where the confidential messages are transmitted directly over the quantum channels and the classical channels simply assist in eavesdropping detection.

Constrained by the capabilities of the state-of-the-art technologies at the time of writing, quantum communication relies on classical trusted nodes in networking applications [402]–

[407], which have to be hosted in secure premises. Unless these premises are protected from potential eavesdroppers, the information security at the relay nodes potentially faces challenges. The secure repeaters of the near future will have to utilize QSDC and post-quantum cryptography for hop-by-hop relaying, while ensuring reliable and secure information transfer even in the presence of realistic eavesdropping-infested quantum channels, while protecting the information security at the classical relay nodes using post-quantum cryptography [91]. Hence again, the relay nodes are not required to be trusted, as shown in Fig. 24. This dual protection scheme solves a major challenge in quantum communication and networking. This approach enhances the transmission distance of QSDC, potentially supporting large-scale secure networking applications, while additionally promoting the organic fusion of quantum communications and post-quantum cryptography. A secure relay has been experimentally characterized by combining 10 kilometers of optical fiber and short-distance free-space transmission for supporting relay-based image transmission [91]. This near-term quantum network supports both connection-oriented and connectionless network protocols in classical networks. A seven-stage evolutionary roadmap of constructing a perfectly quantum Internet based on secure relays has been proposed in [91], but again, the ultimate solution hinges on the introduction of fully-fledged entanglement-based relaying.

E. Experimental progress

Substantial efforts have been invested into realizing DQKD [210], [408]–[412], which has the potential of preparing the groundwork for QSDC experiments. At the time of writing QSDC has evolved from its theoretical protocol development phase to experimental demonstrations over the past few years. Both the DL04 [57], [60] and the two-step QSDC protocol [58], [59] have been realized by dedicated experimentalists. Below, the associated experimental results are reviewed in a little more detail. Table XII and Table XIII provide a summary of the most representative QSDC experiments (N.A. represents not available). These experiments were conducted to demonstrate and test a range of QSDC protocols in real-world conditions.

The information carriers inevitably suffer from the impairments of the quantum channel, such as its thermal effects, nonlinearities and dispersion. Therefore, quantum error correction codes [413], [414] and the decoherence-free subspace technique [415]–[417] have been developed for protecting QSDC. In 2016, Hu et al. [57] proposed the so-called single-photon frequency coding technique for the DL04 protocol, which is different from the frequency encoding technique of Section III-B5. The receiver of the resultant single-photon block is capable of detecting the confidential messages by the discrete time Fourier transform. Even if not all the photons can be detected by the receiver owing to optical loss and due to the limited quantum efficiency of the associated single photon detector, reliable information transimission may still be achieved at a low signal-to-noise ratio.

Figure 25 (a) shows the fiber-optic QSDC system designed by Hu et al [57]. Their system had an operating frequency
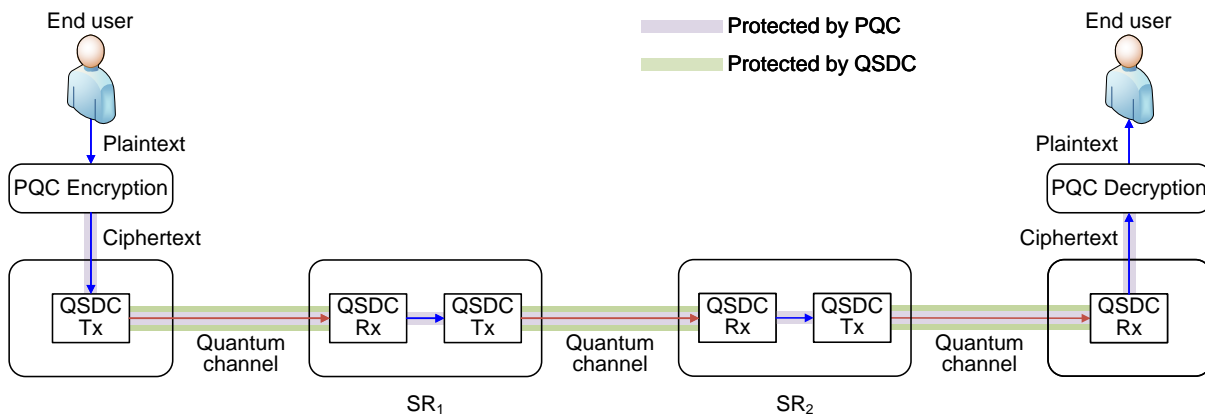
Fig. 24. A secure repeater network. PQC, post-quantum cryptography; SR, secure repeater.

TABLE XII
SUMMARY OF REPRESENTATIVE QSDC EXPERIMENTS BASED ON SINGLE PHOTON.

Group & year	Hu *et al.*, 2016 [57]	Qi *et al.*, 2019 [60]	Sun *et al.*, 2020 [85]	Pan *et al.*, 2020 [86]	Zhang *et al.*, 2022 [89]	Liu *et al.*, 2022 [92]
Protocol	DL04					
Information carrier	Single photon					
Encoding	Operation frequency	Phase	Phase	Phase	Phase and time-bin	Phase
Wavelength	1550 nm	1550 nm	1550 nm	1550 nm	1550 nm	1550 nm
Channel	Fiber	Fiber	Fiber	Free space	Fiber	Fiber
Repetition rate	10 MHz	1 MHz	1 MHz	16 MHz	50 MHz	50 MHz
Distance	N.A.	1.5 km	18.5 km	10 m	100 km	5 km
Error rate	N.A.	0.6%	0.96%	0.49%±0.27%	2.5%	0.42%±0.05%
Rate	4 kbps	50 bps	100 bps	500 bps	0.54 bps	3.43 kbps

range spanning from 25 to 400 kHz and a channel spacing of 25 kHz. So there are 16 frequency bands and an information transmission rate of 4 kbps was achieved. Both the common intercept-resend attack [170] and photon-number-splitting attack [101] were considered in this experiment, when calculating the number of secure information bits versus the communication distance.

Qi *et al.* [60] described the practical QSDC of Fig. 25 (b), including both its optical and electronic part. Motivated readers are referred to [60] for the detailed portrayal of this practical circuit. The QSDC system of Fig. 25 (b) was also concatenated with a low-density parity check coding scheme [60] for enhancing its performance. This practical QSDC experiment conducted over 1.5 km fiber attained a secure communication rate of 50 bps at a quantum bit error rate of 0.6%, and both pictures and audio were successfully transmitted by this system. Nonetheless, the rate vs. distance performance of the system requires further improvement.

The full implementation of typical QSDC protocols [43], [53], [54], [61], [78], [116] requires block-based transmission, where a large number of quantum states have to be processed, which requires quantum memory. However, at the time of writing quantum memory has a rather limited coherence time. A compelling solution is to use an ingenious coding method

to reduce the reliance on quantum memory [80], [85], which was hence termed as quantum-memory-free scheme.

In quantum-memory-free QSDC [80], [85], the forward error correction codeword is divided into several data frames for transmission, as seen in Fig. 25 (c). Alice extracts a secure sequence from the previously sent data frame and encrypts the current secret message by using this sequence to obtain the ciphertext. Then, she utilizes the channel's secrecy capacity estimated during the previously sent data frames as the upper limit of the encoding rate representing the maximum normalized throughput for transmitting the current data frame, encoding the ciphertext into a forward-error-correction codeword. This system achieved an information transmission rate of 100 bps over an 18.5 km optical fiber channel.

Pan *et al.* [86] experimentally demonstrated single-photon based QSDC in a free-space channel, for a transmission over a distance of 10 m at an information transmission rate of 500 bps. In 2022, the communication distance of QSDC was extended to 100 km [89]. Hence QSDC is indeed capable of supporting an entire metropolitan area, providing secure communication. As a further advance, Liu *et al.* [92] constructed a robust optical fiber QSDC system successfully operating without active polarization compensation.

Experimentalists often store the photons by using a delay

TABLE XIII
SUMMARY OF REPRESENTATIVE QSDC EXPERIMENTS BASED ON ENTANGLEMENT. ITU, INTERNATIONAL TELECOMMUNICATION UNION

Group & year	Zhang et al., 2017 [58]	Zhu et al., 2017 [59]	Qi et al., 2021 [87]
Protocol	Two-step		
Information carrier	Entangled photon		
Encoding	Polarization	Polarization	Polarization
Wavelength	795 nm	1549.32 nm	30 ITU channels
Channel	Free space	Fiber	Fiber
Repetition rate	N.A.	N.A.	N.A.
Distance	N.A.	0.5 km	40 km
Error rate	10%	N.A.	0.13%
Rate	2.5 bps	N.A.	1 kbps
Fidelity	90%	91%, 88%	>95%

line, such as a fiber loop [408], [418] and optical fiber delay line [57], [59], [60], [409] as a simple design alternative. As a further advance, Zhang et al. [58] opened the door for storing the entangled photons in QSDC using state-of-the-art atomic quantum memory. The detailed components of the QSDC system relying on quantum memory are shown in Fig. 26 (a). A bit rate of 2.5 bps was achieved at the error rate of 10% in this quantum-memory-assisted QSDC system.

Additionally, another practical challenge in the implementation of entanglement-based QSDC is to perform high-fidelity Bell-state discrimination. Zhang et al. [58] applied so-called quantum state tomography [9] to discriminate the polarization of entangled states instead of applying the BSM mentioned above. Zhu et al. [59] replaced the quantum state tomography by the BSM using only linear optical elements. In their experiment the Bell states $|\psi^+\rangle$ and $|\psi^-\rangle$ were discriminated successfully with a fidelity of 88% and 91%, respectively. Fig. 26 (b) shows their experimental setup, where the communicating parties are linked by 0.5 km of optical fiber. The entangled photons were generated by spontaneous four-wave mixing [419], and this fiber-based source is conveniently compatibile with the transmission medium. Recently, Qi et al. [87] experimentally demonstrated a 15-user QSDC network based on entanglement distribution, achieving an information transmission rate of 1 kbps between any pair of users separated by a distance as high as 40 km.

At the time of writing many of the grave QSDC impediments have indeed been overcome, despite relying on off-the-shelf optoelectronic devices. An information rate of a few dozens of kbps has been achieved over several tens of kilometers, impressive achievement likely to be followed by more practical high-performance implementations in the near future.
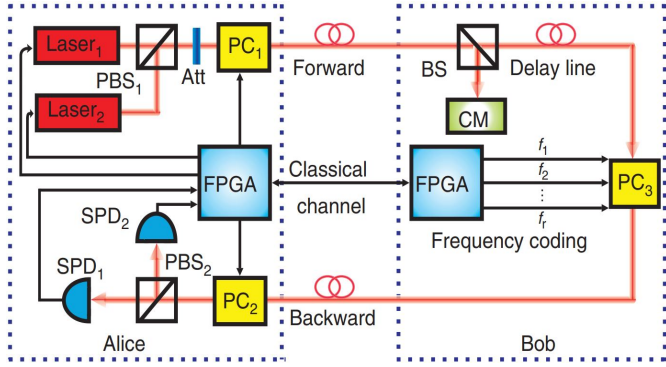
V. OPEN CHALLENGES AND FUTURE RESEARCH

Looking back over the twenty year history of QSDC, several stages of development appear prominently before our eyes, as seen in Fig. 27. From these the following lessons can be derived.

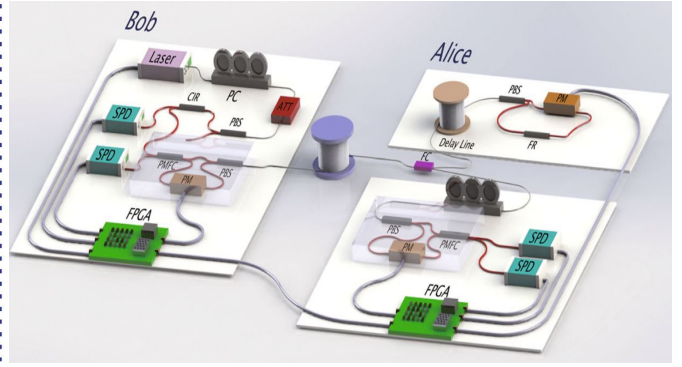Starting from 2000 when the QSDC philosophy was conceived, researchers have endeavoured to construct point-to-point communication protocols. Then the early QSDC protocols were further developed for solving diverse quantum cryptographic tasks, including quantum dialogues, quantum signatures, and quantum steganography, which opened the way for the extensive application of QSDC. The security of QSDC is provable in theory: the QSDC protocols are information-theoretically secure. Recent engineering efforts completed the proof-of-principle experiment and took a step toward practical field-operation. Nonetheless, numerous open problems and challenges exist, hence substantial further research is needed.
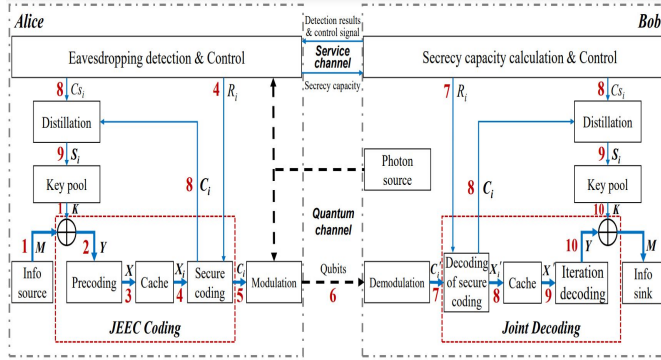
A. Designing QSDC protocols

As it transpires from the literature we have reviewed, QSDC protocols have mainly been studied in the discrete variable domain. But, the continuous-variable schemes are potentially more compatible with current telecom equipment, and have the advantage of cost-effective detectors, as well as higher rates than discrete-variable protocols. Hence there have been some initial QSDC studies in the continuous-variable domain [67], [117], [270], [325]. However, all of them belong to the family of DSQC or quasi-QSDC [50], because additional communication is a prerequisite for the final information decoding, which reduces the efficiency of communication. Thus, one of the open problems is that of designing the family of continuous-variable QSDC protocols, whose receiver can detect information without the assistance of additional communication. Traditional QSDC protocols require round-trip transmission of quantum states. Designing one-way QSDC protocols would be beneficial both in terms of reducing channel losses and system complexity. The rate vs. distance performance has to be improved by harnessing novel physical resources [223], for breaking the theoretical limits [420]. In the transmission of confidential information over quantum channels with noise, loss, and eavesdropping, excellent forward error correction codes are required [50], such as polar codes [421], low density parity check codes [60], and so on. A particularly promising technique is to design error correction codes for QSDC schemes.
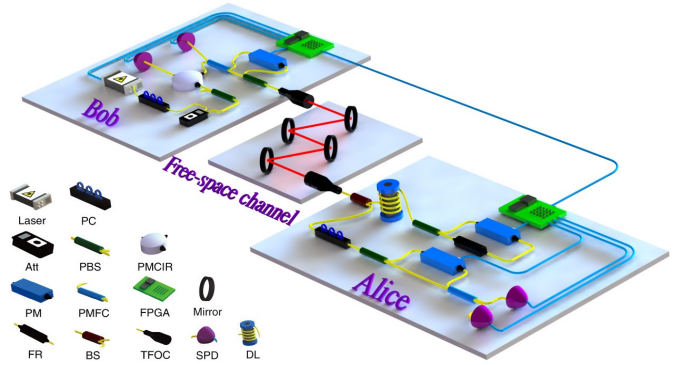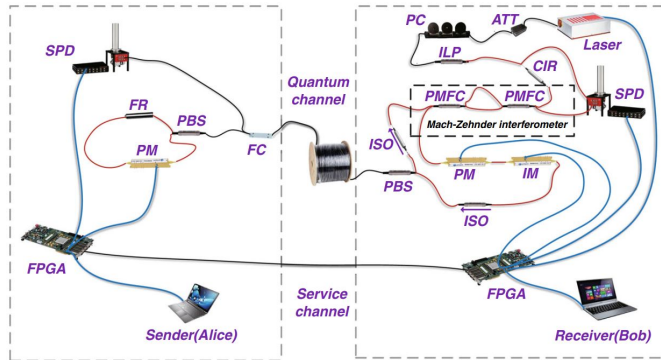
(a) operation frequency encoding [57].

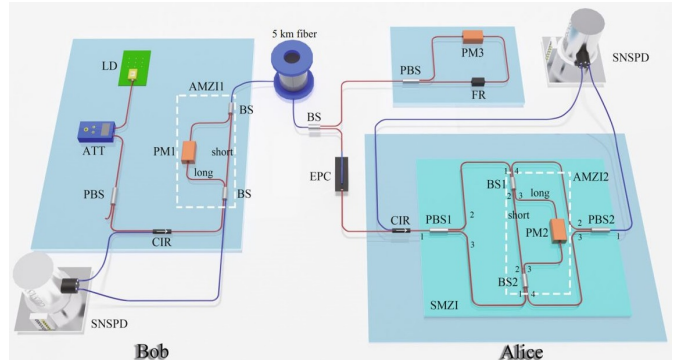(b) QSDC system over 1.5 km fiber channel [60].

(c) quantum-memory-free coding [85].

(d) free-space QSDC system [86].

(e) QSDC over 100 km fiber [89].

(f) QSDC without active polarization compensation [92].

Fig. 25. Experimental progress of DL04 QSDC protocol. In the figures: Att, attenuator; AMZI, asymmetric Mach-Zehnder interferometer; BS, beam splitter; CIR, circulator; CM, control mode; DL, delay line; EPC, electronic polarization controller; FC, fiber coupler; FPGA, field programmable gate array; FR, Faraday Rotator; ILP, in-line polarizer; IM, intensity modulator; ISO, isolator; LD, laser diode; PBS, polarization beam splitter; PC, polarization controller; PM, phase modulator; PMCIR, polarization-maintaining circulator; PMFC, polarization maintaining filter coupler; SMZI, Sagnac-Mach-Zehnder interferometers; SNSPD, superconducting nanowire single photon detector; SPD, single-photon detector; TFOC, triplet fiber-optic collimator.

B. Security proof of QSDC

Historically speaking, the security proof of BB84 QKD has been carried out from a range of different perspectives [422]–[425]. The security proof QSDC still requires further research. One of the challenges is that the two-way transmission is vulnerable to attacks by quantum hackers. The security analysis of imperfect devices is also urgently needed. The secrecy capacity considering finite-length effects and practical system parameters has to be determined.

C. Experimental implementations of QSDC

Optimizing the parameters of devices and improving the performance of practical QSDC systems represents ongoing challenges on the experimental side. Intuitively, the communication distance of single-photon QSDC may approach a half of QKD's distance at the same information rate, bearing in mind that QSDC requires two-way block based transmission. Combining quantum memory with QSDC is conducive to the further improvement of the communication distance and in support of QSDC with block based transmission [58]. Furthermore, the investigation of free-space optical QSDC

(a) QSDC with the quantum memory [58]

(b) entanglement-based long-distance QSDC [60].
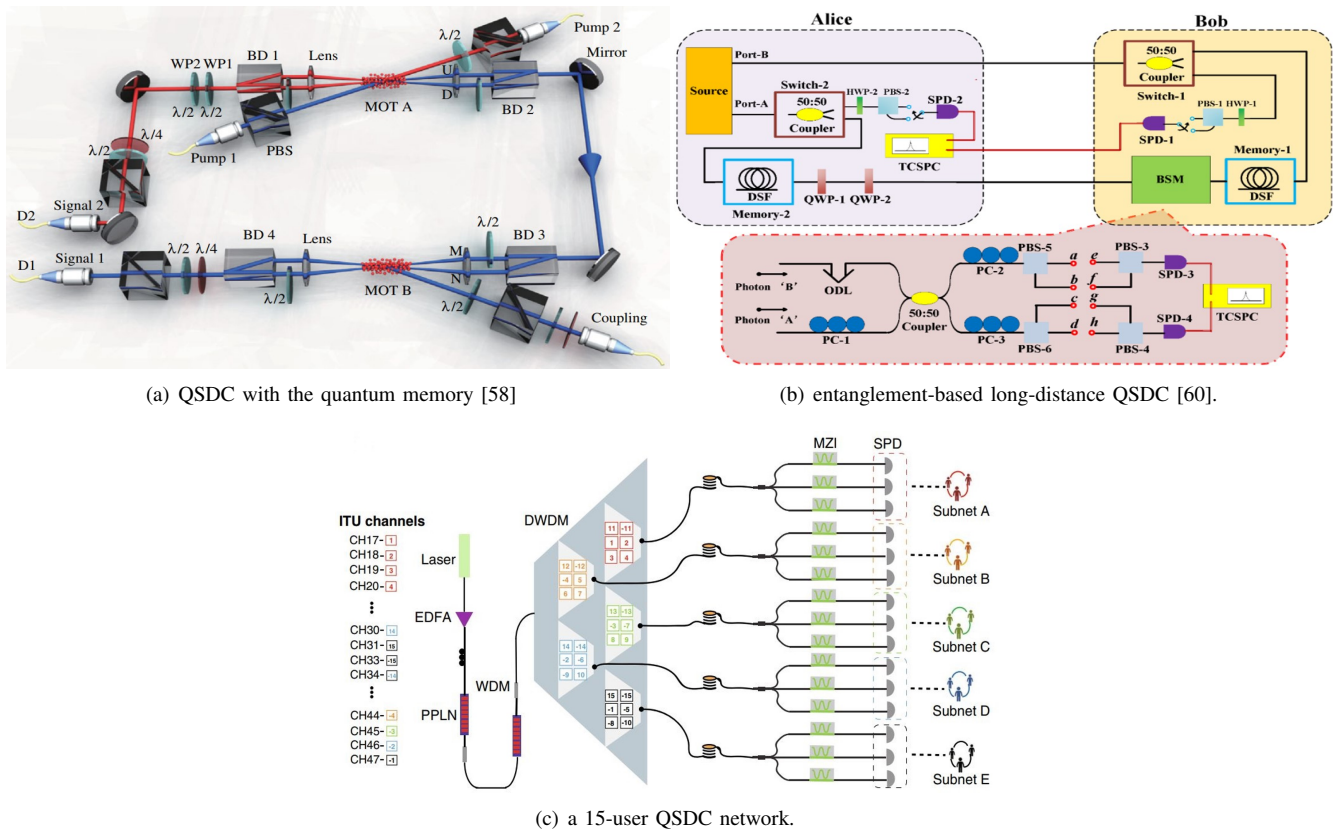
(c) a 15-user QSDC network.

Fig. 26. Demonstration of Two-step QSDC protocol. In the figures: BD1, BD2, BD3 and BD4, beam displacer; D1 and D2, single photon detector; DWDM, dense wave-length division multiplexing; DSF, dispersion shifted fiber; EDFA, erbium-doped fiber amplifier; $\lambda/2$, half-wave plate; HWP, half wave plate; ITU, International Telecommunication Union; MOT A and MOT B, magneto-optical trap; MZI, Mach–Zehnder interferometer; ODL, optical delay line; PBS, polarization beam splitter; PC, polarization controller; PPLN, periodically poled lithium niobate; $\lambda/4$, quarter-wave plate; SPD, single-photon detector; TCSPC, time-correlated single photon counting; U, D, M, and N, path; WDM, wavelength division multiplexing; WP1 and WP2, half-wave plate.
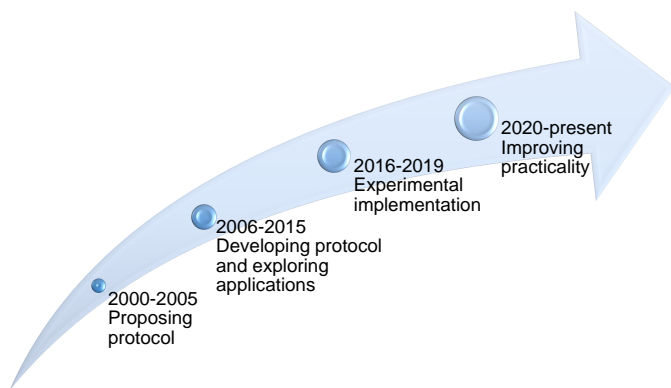

Fig. 27. Development and outlook of QSDC

would contribute to the future implementation of satellite-based QSDC networks.

D. Hybrid QSDC-classical network

In closing we note that most of the cryptographic tasks considered operated in the quantum domain. However, it is also feasible to integrate QSDC into high-security classical communication network. Specially, the secure repeater network is compatible with the existing Internet [91], but additional efforts are needed to design its architecture and establish the interface with the classical network. The classical-cryptography assured imperfect device QSDC proposed in [50] combines classical cryptographic techniques with QSDC using existing technology, enabling confidential communication at an improved security level.

VI. CONCLUSIONS AND LESSONS LEARNED

Following our tour of quantum signal processing with a view to inspire a community-wide effort in the interest of filling the open challenges detailed in the previous section, we conclude by listing a few crisp lessens learned:

- The main benefit of communicating in the quantum-domain is that eavesdropping may be detected, which is not the case in the classical domain. Hence if a QKD process is perturbed by an eavesdropper, any further proceedings are curtailed and the key-negotiation is recommended. Once the key is determined, it may be used exactly in the same way as in classic encryption.
- In contrast to the family of QKD solutions, which constitute a family of pure secret key-negotiation protocols, QSDC supports secure communication without requiring a cryptographic key for encryption and decryption.

- Dispensing with a secret key is possible, because in QSDC the confidential messages are directly embedded into the quantum system and transmitted between the communicating parties via a quantum channel.
- The QSDC protocols are also eminently suitable for diverse cryptographic tasks, and a large number of cryptographic protocols beyond QSDC have been constructed.
- The recent experimental progress was reviewed in Section IV-E highlighting the associated technological challenges. It is clear that the performance of QSDC in terms of its information rate and communication distance is still very limited at the time of writing.
- In conclusion, there are significant untapped opportunities and numerous open problems for a strongly interdisciplinary research community to solve, including numerous open problems in quantum information and communication theory, in quantum physics, in numerous aspects of quantum engineering. These include, but are no means limited to quantum error mitigation, quantum coding, quantum channel modelling and transmission techniques.
- A compelling direction is to further explore the potential of wireless QSDC both in the context of free-space optical satellite communication and terrestrial scenarios relying on both visible-light communications and potentially even on THz wireless communications.
- **Join this exhilarating research momentum valued Colleague!**

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept. 2016.

[2] Y. Lindell and J. Katz, *Introduction to modern cryptography*. Chapman and Hall/CRC, 2014.

[3] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[4] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[5] P. Benioff, "The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines," *J. Stat. Phys.*, vol. 22, no. 5, pp. 563–591, May 1980.

[6] I. Yuri, "Manin. vychislimoe i nevychislimoe," *Sov. Radio*, pp. 13–15, 1980.

[7] R. P. Feynman, "Simulating physics with computers," *Int. J. Theor. Phys.*, vol. 21, no. 6-7, pp. 467–488, May 1982.

[8] D. Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer," *Proc. R. Soc. Lond. A*, vol. 400, no. 1818, pp. 97–117, Jul. 1985.

[9] M. A. Nielsen and I. Chuang, *Quantum computation and quantum information*, U.K.: Cambridge Univ. Press, 2000.

[10] S.-S. Li, G.-L. Long, F.-S. Bai, S.-L. Feng, and H.-Z. Zheng, "Quantum computing," *Proc. Natl. Acad. Sci.*, vol. 98, no. 21, pp. 11847–11848, Sep. 2001.

[11] P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, "Quantum search algorithms for wireless communications," *IEEE Commun. Surv. Tut.*, vol. 21, no. 2, pp. 1209–1242, Nov. 2018.

[12] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Nov. 1994, pp. 124–134.

[13] W. Peng, B. Wang, F. Hu, Y. Wang, X. Fang, X. Chen, and C. Wang, "Factoring larger integers with fewer qubits via quantum annealing with optimized parameters," *Sci. China Phys., Mech. Astron.*, vol. 62, no. 6, Art. no. 60311, Jan. 2019.

[14] B. Yan, Z. Tan, S. Wei, H. Jiang, W. Wang, H. Wang, L. Luo, Q. Duan, Y. Liu, W. Shi, Y. Fei, X. Meng, Y. Han, Z. Shan, J. Chen, X. Zhu, C. Zhang, F. Jin, H. Li, C. Song, Z. Wang, Z. Ma, H. Wang, G.-L. Long, "Factoring integers with sublinear resources on a superconducting quantum processor," *arXiv preprint arXiv:2212.12372*, 2022.

[15] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the internet of things in a quantum world," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, Feb. 2017.

[16] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput*. Philadelphia, PA, USA, May 1996, pp. 212–219.

[17] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett.*, vol. 79, pp. 325–328, Jul. 1997.

[18] L. K. Grover, "Quantum computers can search rapidly by using almost any transformation," *Phys. Rev. Lett.*, vol. 80, no. 19, pp. 4329–4332, May 1998.

[19] G. L. Long, Y. S. Li, W. L. Zhang, and L. Niu, "Phase matching in quantum searching," *Phys. Lett. A*, vol. 262, no. 1, pp. 27–34, Oct. 1999.

[20] G.-L. Long, "Grover algorithm with zero theoretical failure rate," *Phys. Rev. A*, vol. 64, no. 2, p. Art. no. 022307, Jul. 2001.

[21] P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design," *IEEE Access*, vol. 1, pp. 94–122, May 2013.

[22] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, "Iterative quantum-assisted multi-user detection for multi-carrier interleave division multiple access systems," *IEEE Trans. Commun.*, vol. 63, no. 10, pp. 3713–3727, Oct. 2015.

[23] Ze. Wang, S. Wei, G.-L. Long and L. Hanzo, "Variational quantum attacks threaten advanced encryption standard based symmetric cryptography," *Sci. China Inf. Sci.*, vol. 65, no. 10, Jul. 2022, Art. no. 200503.

[24] G. Brassard, "Searching a quantum phone book," *Science*, vol. 275, no. 5300, pp. 627–628, Jan. 1997.

[25] G. Brassard, P. Høyer, and A. Tapp, "Quantum cryptanalysis of hash and claw-free functions," in *Proc. Latin Amer. Symp. Theor.*, Apr. 1998, pp. 163–169.

[26] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1510–1523, Oct. 1997.

[27] F. Toyama, W. Van Dijk, and Y. Nogami, "Quantum search with certainty based on modified grover algorithms: optimum choice of parameters," *Quantum Inf. Process.*, vol. 12, no. 5, pp. 1897–1914, Oct. 2013.

[28] G. Castagnoli, "Highlighting the mechanism of the quantum speedup by time-symmetric and relational quantum mechanics," *Found. Phys.*, vol. 46, no. 3, pp. 360–381, Nov. 2016.

[29] W. Buchanan and A. Woodward, "Will quantum computers be the end of public key encryption?" *J. Cyber Secur. Technol.*, vol. 1, no. 1, pp. 1–22, Sep. 2016.

[30] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, *Report on post-quantum cryptography*, US Department of Commerce, National Institute of Standards and Technology, Apr. 2016.

[31] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," *Quantum Inf. Comput.*, vol. 3, no. 4, pp. 317–344, Jul. 2003.

[32] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, "Quantum resource estimates for computing elliptic curve discrete logarithms," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security*, Nov. 2017, pp. 241–270.

[33] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, Apr. 2021, Art. no. 433.

[34] D. J. Bernstein, *Introduction to post-quantum cryptography*, Springer, 2009.

[35] D. Micciancio and O. Regev, "Lattice-based cryptography," *Post-quantum cryptography*, Springer, pp. 147–191, 2009.

[36] N. Sendrier, "Code-based cryptography: State of the art and perspectives," *IEEE Secur. Priv.*, vol. 15, no. 4, pp. 44–50, Aug. 2017.

[37] S. Wiesner, "Conjugate coding," *ACM Sigact News*, vol. 15, no. 1, pp. 78–88, 1983.

[38] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proc. Int. Conf. Comput. Syst. Signal Process.*, Dec. 1984, pp. 175–179.

[39] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, Jan. 1992.

[40] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, no. 13, pp. 1895–1899, Mar. 1993.

[41] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, no. 3, pp. 1829–1834, Jun. 1999.

[42] G. L. Long and X. S. Liu, "Theoretical efficient high capacity quantum key distribution scheme," *arXiv preprint quant-ph/0012056*, 2000.

[43] G.-L. Long and X.-S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Phys. Rev. A*, vol. 65, no. 3, Feb. 2002, Art. no. 032302.

[44] L. Xiao, G. L. Long, F.-G. Deng, and J.-W. Pan, "Efficient multiparty quantum-secret-sharing schemes," *Phys. Rev. A*, vol. 69, no. 5, May 2004, Art. no. 052307.

[45] D. Pan, K. Li, D. Ruan, S. X. Ng, and L. Hanzo, "Single-photon-memory two-step quantum secure direct communication relying on Einstein-Podolsky-Rosen pairs," *IEEE Access*, vol. 8, pp. 121146–121161, Jun. 2020.

[46] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[47] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.

[48] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, no. 5, p. 557–559, Feb. 1992.

[49] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[50] D. Pan, X.-T. Song, and G.-L. Long, "Free-space quantum secure direct communication: basics, progress, and outlook," *Adv. Devices Instrum.*, vol. 4, Feb. 2023, Art. no. 0004.

[51] M. Dušek, O. Haderka, M. Hendrych, and R. Myška, "Quantum identification system," *Phys. Rev. A*, vol. 60, no. 1, pp. 149–156, Jul. 1999.

[52] B. S. Dhillon and M. J. Nene, "QSDC: Future of quantum communication a study," in *2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, 2021, pp. 77–83.

[53] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Phys. Rev. A*, vol. 68, no. 4, Oct. 2003, Art. no. 042317.

[54] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A*, vol. 69, no. 5, May 2004, Art. no. 052319.

[55] C. Wang, F. G. Deng, and G. L. Long, "Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state," *Opt. Commun.*, vol. 253, no. 1-3, pp. 15–20, Sep. 2005.

[56] X.-R. Jin, X. Ji, Y.-Q. Zhang, S. Zhang, S.-K. Hong, K.-H. Yeon, and C.-I. Um, "Three-party quantum secure direct communication based on GHZ states," *Phys. Lett. A*, vol. 354, no. 1-2, pp. 67–70, May 2006.

[57] J.-Y. Hu, B. Yu, M.-Y. Jing, L.-T. Xiao, S.-T. Jia, G.-Q. Qin, and G.-L. Long, "Experimental quantum secure direct communication with single photons," *Light-Sci. Appl.*, vol. 5, Apr. 2016, Art. no. e16144.

[58] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, and G.-C. Guo, "Quantum secure direct communication with quantum memory," *Phys. Rev. Lett.*, vol. 118, no. 22, May 2017, Art. no. 220501.

[59] F. Zhu, W. Zhang, Y. Sheng, and Y. Huang, "Experimental long-distance quantum secure direct communication," *Sci. Bull.*, vol. 62, no. 22, pp. 1519–1524, Nov. 2017.

[60] R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G.-L. Long, "Implementation and security analysis of practical quantum secure direct communication," *Light-Sci. Appl.*, vol. 8, Feb. 2019, Art. no. 22.

[61] C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, and G. L. Long, "Quantum secure direct communication with high-dimension quantum superdense coding," *Phys. Rev. A*, vol. 71, no. 4, Apr. 2005, Art. no. 044305.

[62] Z.-j. Zhang, Y. Li, and Z.-x. Man, "Multiparty quantum secret sharing," *Phys. Rev. A*, vol. 71, no. 4, Apr. 2005, Art. no. 044301.

[63] H. Lee, J. Lim, and H. Yang, "Quantum direct communication with authentication," *Phys. Rev. A*, vol. 73, no. 4, Apr. 2006, Art. no. 042305.

[64] F.-G. Deng, X.-H. Li, C.-Y. Li, P. Zhou, and H.-Y. Zhou, "Quantum secure direct communication network with Einstein–Podolsky–Rosen pairs," *Phys. Lett. A*, vol. 359, no. 5, pp. 359–365, Dec. 2006.

[65] F.-G. Deng, X.-H. Li, C.-Y. Li, P. Zhou, and H.-Y. Zhou, "Quantum secure direct communication network with superdense coding and decoy photons," *Phys. Scr.*, vol. 76, no. 1, pp. 25–30, Jun. 2007.

[66] S. Lin, Q.-Y. Wen, F. Gao, and F.-C. Zhu, "Quantum secure direct communication with χ-type entangled states," *Phys. Rev. A*, vol. 78, no. 6, Dec. 2008, Art. no. 064304.

[67] S. Pirandola, S. L. Braunstein, S. Mancini, and S. Lloyd, "Quantum direct communication with continuous variables," *Europhys. Lett.*, vol. 84, no. 2, Oct. 2008, Art. no. 20013.

[68] S. Qin, Q. Wen, L. Meng, and F. Zhu, "Quantum secure direct communication over the collective amplitude damping channel," *Sci. China Ser. G: Phys., Mech. Astron.*, vol. 52, no. 8, pp. 1208–1212, May 2009.

[69] F. Gao, S.-J. Qin, Q.-Y. Wen, and F.-C. Zhu, "Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilinger state," *Opt. Commun.*, vol. 283, no. 1, pp. 192–195, Jan. 2010.

[70] H. Lu, C.-H. F. Fung, X. Ma, and Q.-Y. Cai, "Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel," *Phys. Rev. A*, vol. 84, no. 4, Oct. 2011, Art. no. 042344.

[71] Z.-W. Sun, R.-G. Du, and D.-Y. Long, "Quantum secure direct communication with two-photon four-qubit cluster states," *Int. J. Theor. Phys.*, vol. 51, no. 6, pp. 1946–1952, Jan. 2012.

[72] Y. Chang, C. Xu, S. Zhang, and L. Yan, "Quantum secure direct communication and authentication protocol with single photons," *Chin. Sci. Bull.*, vol. 58, no. 36, pp. 4571–4576, Nov. 2013.

[73] P. Yadav, R. Srikanth, and A. Pathak, "Two-step orthogonal-state-based protocol of quantum secure direct communication with the help of order-rearrangement technique," *Quantum Inf. Process.*, vol. 13, no. 12, pp. 2731–2743, Sep. 2014.

[74] J. H. Shapiro, Z. Zhang, and F. N. Wong, "Secure communication via quantum illumination," *Quantum Inf. Process.*, vol. 13, pp. 2171–2193, Nov. 2014.

[75] Q. Zhuang, Z. Zhang, J. Dove, F. N. Wong, and J. H. Shapiro, "Ultrabroadband quantum-secured communication," *arXiv preprint arXiv:1508.01471*, 2015.

[76] A. Farouk, M. Zakaria, A. Megahed, and F. A. Omara, "A generalized architecture of quantum secure direct communication for N disjointed users with authentication," *Sci. Rep.*, vol. 5, Nov. 2015, Art. no. 16080.

[77] D. J. Lum, J. C. Howell, M. Allman, T. Gerrits, V. B. Verma, S. W. Nam, C. Lupo, and S. Lloyd, "Quantum enigma machine: Experimentally demonstrating quantum data locking," *Phys. Rev. A*, vol. 94, no. 2, Aug. 2016, Art. no. 022315.

[78] Z. Zhou, Y. Sheng, P. Niu, L. Yin, G. Long, and L. Hanzo, "Measurement-device-independent quantum secure direct communication," *Sci. China Phys., Mech. Astron.*, vol. 63, Mar. 2020, Art. no. 230362. arXiv preprint arXiv:1805.07228, 2018.

[79] 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," *Sci. Bull.*, vol. 63, no. 20, pp. 1345–1350, Oct. 2018.

[80] Z. Sun, R. Qi, Z. Lin, Z. Yin, G. Long, and J. Lu, "Design and implementation of a practical quantum secure direct communication system," in *2018 IEEE Globecom Workshops (GC Wkshps)*, IEEE, Dec. 2018, pp. 1–6.

[81] J. H. Shapiro, D. M. Boroson, P. B. Dixon, M. E. Grein, and S. A. Hamilton, "Quantum low probability of intercept," *JOSA B*, vol. 36, no. 3, pp. B41–B50, Mar. 2019.

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

[83] F. Massa, A. Moqanaki, Ä. Baumeler, F. Del Santo, J. A. Kettlewell, B. Dakić, and P. Walther, "Experimental two-way communication with one photon," *Adv. Quantum Technol.*, vol. 2, no. 11, Sep. 2019, Art. no. 1900050.

[84] F. Del Santo and B. Dakić, "Two-way communication with a single quantum particle," *Phys. Rev. Lett.*, vol. 120, Feb. 2018, Art. no. 060503.

[85] Z. Sun, L. Song, Q. Huang, L. Yin, G. Long, J. Lu, and L. Hanzo, "Toward practical quantum secure direct communication: a quantum-memory-free protocol and code design," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5778–5792, Sep. 2020.

[86] D. Pan, Z. Lin, J. Wu, H. Zhang, Z. Sun, D. Ruan, L. Yin, and G. L. Long, "Experimental free-space quantum secure direct communication and its security analysis," *Photonics Res.*, vol. 8, no. 9, pp. 1522–1531, Sep. 2020.

[87] Z. Qi, Y. Li, Y. Huang, J. Feng, Y. Zheng, and X. Chen, "A 15-user quantum secure direct communication network," *Light-Sci. Appl.*, vol. 10, Sep. 2021, Art. no. 183.

[88] A. Vázquez-Castro, D. Rusca, and H. Zbinden, "Quantum keyless private communication versus quantum key distribution for space links," *Phys. Rev. Appl*, vol. 16, no. 1, Jul. 2021, Art. no. 014006.

[89] H. Zhang, Z. Sun, R. Qi, L. Yin, G.-L. Long, and J. Lu, "Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states," *Light-Sci. Appl.*, vol. 11, Apr. 2022, Art. no. 83.

[90] J. Wu, G.-L. Long, and M. Hayashi, "Quantum secure direct communication with private dense coding using a general preshared quantum state," *Phys. Rev. Appl*, vol. 17, Jun. 2022, Art. no. 064011.

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

[92] X. Liu, D. Luo, G. Lin, Z. Chen, C. Huang, S. Li, C. Zhang, Z. Zhang, and K. Wei, "Fiber-based quantum secure direct communication without active polarization compensation," *Sci. China Phys., Mech. Astron.*, vol. 65, no. 12, Nov. 2022, Art. no. 120311.

[93] S. S. Panda, P. A. Yasir, and C. Chandrashekar, "Quantum direct communication protocol using recurrence in k-cycle quantum walks," *Phys. Rev. A*, vol. 107, no. 2, Feb. 2023, Art. no. 022611.

[94] L. Zhou, B.-W. Xu, W. Zhong, and Y.-B. Sheng, "Device-independent quantum secure direct communication with single-photon sources," *Phys. Rev. Appl*, vol. 19, no. 1, Jan. 2023, Art. no. 014036.

[95] X.-J. Li, D. Pan, G.-L. Long, and L. Hanzo, "Single-photon-memory measurement-device-independent quantum secure direct communication—part I: Its fundamentals and evolution," *IEEE Commun. Lett.*, vol. 27, no. 4, pp. 1055–1059, Apr. 2023.

[96] X.-J. Li, D. Pan, G.-L. Long, and L. Hanzo, "Single-photon-memory measurement-device-independent quantum secure direct communication—part II: A practical protocol and its secrecy capacity," *IEEE Commun. Lett.*, vol. 27, no. 4, pp. 1060–1064, Apr. 2023.

[97] Z.-Z. Sun, D. Pan, D. Ruan, and G.-L. Long, "One-sided measurement-device-independent practical quantum secure direct communication," *J. Lightwave Technol.*, Feb. 2023, early Access.

[98] M. Xu, X. Ren, D. Niyato, J. Kang, C. Qiu, Z. Xiong, X. Wang, and V. C. M. Leung, "When quantum information technologies meet blockchain in web 3.0," *IEEE Netw.*, 2023, early Access.

[99] L. Bacsardi, "On the way to quantum-based satellite communication," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 50–55, Aug. 2013.

[100] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, and J.-W. Pan, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, Aug. 2017.

[101] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Phys. Rev. A*, vol. 51, no. 3, pp. 1863–1869, 1995.

[102] L. Goldenberg and L. Vaidman, "Quantum cryptography based on orthogonal states," *Phys. Rev. Lett.*, vol. 75, no. 7, pp. 1239–1243, Aug. 1995.

[103] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Phys. Rev. Lett.*, vol. 89, no. 18, Oct. 2002, Art. no. 187902.

[104] F.-G. Deng and G. L. Long, "Bidirectional quantum key distribution protocol with practical faint laser pulses," *Phys. Rev. A*, vol. 70, no. 1, Jul. 2004, Art. no. 012311.

[105] M. Lucamarini and S. Mancini, "Secure deterministic communication without entanglement," *Phys. Rev. Lett.*, vol. 94, no. 14, Apr. 2005, Art. no. 140501.

[106] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, "Continuous-variable quantum cryptography using two-way quantum communication," *Nat. Phys.*, vol. 4, no. 9, pp. 726–730, Jul. 2008.

[107] A. Wójcik, "Eavesdropping on the "ping-pong" quantum communication protocol," *Phys. Rev. Lett.*, vol. 90, no. 15, Apr. 2003, Art. no. 157901.

[108] Z. Zhang, Z. Man, and Y. Li, "Improving wójcik's eavesdropping attack on the ping–pong protocol," *Phys. Lett. A*, vol. 333, no. 1-2, pp. 46–50, Nov. 2004.

[109] Q.-y. Cai, "The ping-pong protocol can be attacked without eavesdropping," *arXiv preprint quant-ph/0402052*, 2004.

[110] M. Pavičić, "In quantum direct communication an undetectable eavesdropper can always tell ψ from ϕ Bell states in the message mode," *Phys. Rev. A*, vol. 87, no. 4, Apr. 2013, Art. no. 042326.

[111] J. Li, L. Li, H. Jin, and R. Li, "Security analysis of the "ping–pong" quantum communication protocol in the presence of collective-rotation noise," *Phys. Lett. A*, vol. 377, no. 39, pp. 2729–2734, Nov. 2013.

[112] G.-L. Long, F.-G. Deng, C. Wang, X.-H. Li, K. Wen, and W.-Y. Wang, "Quantum secure direct communication and deterministic secure quantum communication," *Front. Phys. China*, vol. 2, no. 3, pp. 251–272, 2007.

[113] G. Long, C. Wang, F. Deng, and W. Wang, "Quantum direct communication, advances in lasers and electro optics," *Rijeka, Croatia: InTech*, 2010.

[114] A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, "Secure communication with a publicly known key," *arXiv preprint quant-ph/0111106*, 2001.

[115] F. Yan and X. Zhang, "A scheme for secure direct communication using EPR pairs and teleportation," *Eur. Phys. J. B, Condens. Matter Complex Syst.*, vol. 41, pp. 75–78, Sep. 2004.

[116] A.-D. Zhu, Y. Xia, Q.-B. Fan, and S. Zhang, "Secure direct communication based on secret transmitting order of particles," *Phys. Rev. A*, vol. 73, no. 2, p. 022338, Feb. 2006.

[117] A. M. Marino and C. Stroud Jr, "Deterministic secure communications using two-mode squeezed states," *Phys. Rev. A*, vol. 74, no. 2, Aug. 2006, Art. no. 022315.

[118] S. Imre and F. Balazs, *Quantum Computing and Communications: an engineering approach*, John Wiley & Sons, 2005.

[119] P. A. M. Dirac, *The principles of quantum mechanics*, Oxford university press, 1981.

[120] J. A. Jones and D. Jaksch, *Quantum information, computation and communication*, Cambridge University Press, 2012.

[121] L. Gyongyosi, S. Imre, and H. V. Nguyen, "A survey on quantum channel capacities," *IEEE Commun. Surv. Tut.*, vol. 20, no. 2, pp. 1149–1205, Jan. 2018.

[122] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Phys. Rev.*, vol. 47, no. 10, pp. 777–780, May 1935.

[123] D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Bell's theorem, quantum theory, and conceptions of the universe," 1989.

[124] Z.-Z. Li, G. Xu, X.-B. Chen, X. Sun, and Y.-X. Yang, "Multi-user quantum wireless network communication based on multi-qubit GHZ state," *IEEE Commun. Lett.*, vol. 20, no. 12, pp. 2470–2473, Sep. 2016.

[125] W. Dür, G. Vidal, and J. I. Cirac, "Three qubits can be entangled in two inequivalent ways," *Phys. Rev. A*, vol. 62, no. 6, Nov. 2000, Art. no. 062314.

[126] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Rev. Mod. Phys.*, vol. 81, no. 2, pp. 865–942, Jun. 2009.

[127] B. Huttner, A. Muller, J.-D. Gautier, H. Zbinden, and N. Gisin, "Unambiguous quantum measurement of nonorthogonal states," *Phys. Rev. A*, vol. 54, no. 5, pp. 3783–3789, Nov. 1996.

[128] Y. C. Eldar and G. D. Forney, "On quantum detection and the square-root measurement," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 858–872, Mar. 2001.

[129] Y. Sun, J. A. Bergou, and M. Hillery, "Optimum unambiguous discrimination between subsets of nonorthogonal quantum states," *Phys. Rev. A*, vol. 66, no. 3, Sep. 2002, Art. no. 032315.

[130] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.

[131] B. A. Slutsky, R. Rao, P.-C. Sun, and Y. Fainman, "Security of quantum cryptography against individual attacks," *Phys. Rev. A*, vol. 57, no. 4, pp. 2383–2398, Apr. 1998.

[132] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, "Eavesdropping on quantum-cryptographical systems," *Phys. Rev. A*, vol. 50, no. 2, pp. 1047–1056, Aug. 1994.

[133] N. Lütkenhaus, "Security against eavesdropping in quantum cryptography," *Phys. Rev. A*, vol. 54, no. 1, pp. 97–111, Jul. 1996.

[134] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, "Security of quantum key distribution against all collective attacks," *Algorithmica*, vol. 34, no. 4, pp. 372–388, Nov. 2002.

[135] C. A. Fuchs and A. Peres, "Quantum-state disturbance versus information gain: Uncertainty relations for quantum information," *Phys. Rev. A*, vol. 53, no. 4, pp. 2038–2045, Apr. 1996.

[136] C. A. Fuchs, "Nonorthogonal quantum states maximize classical information capacity," *Phys. Rev. Lett.*, vol. 79, no. 6, pp. 1162–1165, Aug. 1997.

[137] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.

[138] D. Dieks, "Communication by EPR devices," *Phys. Lett. A*, vol. 92, no. 6, pp. 271–272, Nov. 1982.

[139] P. W. Milonni and M. Hardies, "Photons cannot always be replicated," *Phys. Lett.;(Netherlands)*, vol. 92, no. 7, Nov. 1982.

[140] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, "Noncommuting mixed states cannot be broadcast," *Phys. Rev. Lett.*, vol. 76, no. 15, pp. 2818–2821, Apr. 1996.

[141] V. Bužek and M. Hillery, "Quantum copying: Beyond the no-cloning theorem," *Phys. Rev. A*, vol. 54, no. 3, pp. 1844–1852, Sep. 1996.

[142] N. Gisin and S. Massar, "Optimal quantum cloning machines," *Phys. Rev. Lett.*, vol. 79, no. 11, pp. 2153–2156, Sep. 1997.

[143] R. F. Werner, "Optimal cloning of pure states," *Phys. Rev. A*, vol. 58, no. 3, pp. 1827–1832, Sep. 1998.

[144] N. J. Cerf, "Pauli cloning of a quantum bit," *Phys. Rev. Lett.*, vol. 84, no. 19, pp. 4497–4500, May 2000.

[145] M. Lemm and M. M. Wilde, "Information-theoretic limitations on approximate quantum cloning and broadcasting," *Phys. Rev. A*, vol. 96, no. 1, Jul. 2017, Art. no. 012304.

[146] L.-M. Duan and G.-C. Guo, "Probabilistic cloning and identification of linearly independent quantum states," *Phys. Rev. Lett.*, vol. 80, no. 22, pp. 4999–5002, Jun. 1998.

[147] C. H. Bennett and S. J. Wiesner, "Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.*, vol. 69, no. 20, pp. 2881–2884, Nov. 1992.

[148] A. S. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, "When entanglement meets classical communications: Quantum teleportation for the quantum internet," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3808–3833, Jun. 2020.

[149] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, ""event-ready-detectors" Bell experiment via entanglement swapping," *Phys. Rev. Lett.*, vol. 71, pp. 4287–4290, Dec. 1993.

[150] Y.-B. Zhan, L.-L. Zhang, and Q.-Y. Zhang, "Quantum secure direct communication by entangled qutrits and entanglement swapping," *Opt. Commun.*, vol. 282, no. 23, pp. 4633–4636, Dec. 2009.

[151] X.-H. Li, B.-K. Zhao, Y.-B. Sheng, F.-G. Deng, and H.-Y. Zhou, "Fault tolerant quantum key distribution based on quantum dense coding with collective noise," *Int. J. Quantum Inf.*, vol. 7, no. 08, pp. 1479–1489, Sep. 2009.

[152] T. Hwang, C. Hwang, and C. Tsai, "Quantum key distribution protocol using dense coding of three-qubit W state," *Eur. Phys. J. D*, vol. 61, no. 3, pp. 785–790, Feb. 2011.

[153] S. Bandyopadhyay, "Teleportation and secret sharing with pure entangled states," *Phys. Rev. A*, vol. 62, no. 1, Jun. 2000, Art. no. 012308.

[154] N. Zhou, L. Wang, L. Gong, X. Zuo, and Y. Liu, "Quantum deterministic key distribution protocols based on teleportation and entanglement swapping," *Opt. Commun.*, vol. 284, no. 19, pp. 4836–4842, Sep. 2011.

[155] S.-T. Cheng, C.-Y. Wang, and M.-H. Tao, "Quantum communication for wireless wide-area networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 7, pp. 1424–1432, Jul. 2005.

[156] Y.-H. Kim, S. P. Kulik, and Y. Shih, "Quantum teleportation of a polarization state with a complete bell state measurement," *Phys. Rev. Lett.*, vol. 86, no. 7, pp. 1370–1373, Feb. 2001.

[157] R. F. Werner, "All teleportation and dense coding schemes," *J. Phys. A: Math. Gen.*, vol. 34, no. 35, pp. 7081–7094, Aug. 2001.

[158] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, "Experimental entanglement swapping: entangling photons that never interacted," *Phys. Rev. Lett.*, vol. 80, no. 18, pp. 3891–3894, May 1998.

[159] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Phys. Rev. Lett.*, vol. 76, no. 5, pp. 722–725, Jan. 1996.

[160] J.-W. Pan, C. Simon, Č. Brukner, and A. Zeilinger, "Entanglement purification for quantum communication," *Nature*, vol. 410, no. 6832, pp. 1067–1070, Apr. 2001.

[161] C. Simon and J.-W. Pan, "Polarization entanglement purification using spatial entanglement," *Phys. Rev. Lett.*, vol. 89, no. 25, Dec. 2002, Art. no. 257901.

[162] J.-W. Pan, S. Gasparoni, R. Ursin, G. Weihs, and A. Zeilinger, "Experimental entanglement purification of arbitrary unknown states," *Nature*, vol. 423, no. 6938, pp. 417–422, May 2003.

[163] Y.-B. Sheng, F.-G. Deng, and H.-Y. Zhou, "Efficient polarization-entanglement purification based on parametric down-conversion sources with cross-kerr nonlinearity," *Phys. Rev. A*, vol. 77, no. 4, Apr. 2008, Art. no. 042308.

[164] Y.-B. Sheng and F.-G. Deng, "Deterministic entanglement purification and complete nonlocal Bell-state analysis with hyperentanglement," *Phys. Rev. A*, vol. 81, no. 3, Mar. 2010, Art. no. 032307.

[165] Y.-B. Sheng, G. L. Long, and F.-G. Deng, "One-step deterministic multipartite entanglement purification with linear optics," *Phys. Lett. A*, vol. 376, no. 4, pp. 314–319, Jan. 2012.

[166] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," *Nature*, vol. 464, no. 7285, pp. 45–53, Mar. 2010.

[167] D. Mayers, "Unconditional security in quantum cryptography," *J. ACM*, vol. 48, no. 3, pp. 351–406, 2001.

[168] D. Walls and G. J. Milburn, *Quantum Optics*, Springer, 1994.

[169] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Inf. Comput.*, vol. 4, no. 5, pp. 325–360, Sep. 2004.

[170] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, p. 145, 2002.

[171] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, Aug. 2003, Art. no. 057901.

[172] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, no. 23, Jun. 2005, Art. no. 230503.

[173] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, Jun. 2005, Art. no. 230504.

[174] L. Yang, J. Wu, Z. Lin, L. Yin, and G. Long, "Quantum secure direct communication with entanglement source and single-photon measurement," *Sci. China Phys., Mech. Astron.*, vol. 63, no. 11, Aug. 2020, Art. no. 110311.

[175] X. Liu, Z. Li, D. Luo, C. Huang, D. Ma, M. Geng, J. Wang, Z. Zhang, and K. Wei, "Practical decoy-state quantum secure direct communication," *Sci. China Phys., Mech. Astron.*, vol. 64, no. 12, Oct. 2021, Art. no. 120311.

[176] J. Park, B. Kim, and J. Heo, "Statistical fluctuation analysis for quantum secure direct communication with entanglement source and single-photon measurement," in *2022 13th Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, IEEE, Nov. 2022, pp. 332–334.

[177] J. Park, B. Kim, and J. Heo, "Statistical fluctuation analysis for decoy-state quantum secure direct communication," *Quantum Inf. Process.*, vol. 22, Feb. 2023, Art. no. 112.

[178] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, "Invited review article: Single-photon sources and detectors," *Rev. Sci. Instrum.*, vol. 82, no. 7, Jul. 2011, Art. no. 071101.

[179] D. Fattal, E. Diamanti, K. Inoue, and Y. Yamamoto, "Quantum teleportation with a quantum dot single photon source," *Phys. Rev. Lett.*, vol. 92, no. 3, Jan. 2004, Art. no. 037904.

[180] D. Bimberg, E. Stock, A. Lochmann, A. Schliwa, J. A. Tofflinger, W. Unrau, M. Munnix, S. Rodt, V. A. Haisler, A. I. Toropov, A. Bakarov, and A. K. Kalagin, "Quantum dots for single-and entangled-photon emitters," *IEEE Photon. J.*, vol. 1, no. 1, pp. 58–68, Jun. 2009.

[181] X. Sun, P. Wang, T. Wang, D. Li, Z. Chen, L. Chen, K. Gao, M. Li, J. Zhang, W. Ge, Y. Arakawa, B. Shen, M. Holmes, and X. Wang, "Single photon source based on an ingan quantum dot in a site-controlled optical horn structure," *Appl. Phys. Lett.*, vol. 115, no. 2, Jul. 2019, Art. no. 022101.

[182] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, "Single photon quantum cryptography," *Phys. Rev. Lett.*, vol. 89, no. 18, Oct. 2002, Art. no. 187901.

[183] R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle, J.-P. Poizat, and P. Grangier, "Experimental open-air quantum key distribution with a single-photon source," *New J. Phys.*, vol. 6, no. 1, Jul. 2004, Art. no. 92.

[184] M. Leifgen, T. Schröder, F. Gädeke, R. Riemann, V. Métillon, E. Neu, C. Hepp, C. Arend, C. Becher, K. Lauritsen, and O. Benson, "Evaluation of nitrogen-and silicon-vacancy defect centres as single photon sources in quantum key distribution," *New J. Phys.*, vol. 16, no. 2, 2014, Art. no. 023021.

[185] S. Castelletto and R. Scholten, "Heralded single photon sources: a route towards quantum communication technology and photon standards," *Eur. Phys. J-Appl. Phys.*, vol. 41, no. 3, pp. 181–194, Apr. 2008.

[186] A. Trifonov and A. Zavriyev, "Secure communication with a heralded single-photon source," *J. Opt. B: Quantum Semiclassical Opt.*, vol. 7, no. 12, pp. S772–S777, Nov. 2005.

[187] Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo, and A. Karlsson, "Experimental decoy-state quantum key distribution with a sub-poissionian heralded

single-photon source," *Phys. Rev. Lett.*, vol. 100, no. 9, Mar. 2008, Art. no. 090501.

[188] C. A. Kocher and E. D. Commins, "Polarization correlation of photons emitted in an atomic cascade," *Phys. Rev. Lett.*, vol. 18, no. 15, pp. 575–577, Dec. 1967.

[189] S. J. Freedman and J. F. Clauser, "Experimental test of local hidden-variable theories," *Phys. Rev. Lett.*, vol. 28, no. 14, pp. 938–941, Apr. 1972.

[190] A. Migdall, S. V. Polyakov, J. Fan, and J. C. Bienfang, *Single-photon generation and detection: physics and applications*, Academic Press, 2013.

[191] C. Hong and L. Mandel, "Theory of parametric frequency down conversion of light," *Phys. Rev. A*, vol. 31, no. 4, pp. 2409–2418, Apr. 1985.

[192] M. H. Rubin, D. N. Klyshko, Y. Shih, and A. Sergienko, "Theory of two-photon entanglement in type-II optical parametric down-conversion," *Phys. Rev. A*, vol. 50, no. 6, pp. 5122–5133, Dec. 1994.

[193] T. S. Humble, "Quantum security for the physical layer," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 56–62, Aug. 2013.

[194] Z. Wang, R. Malaney, and J. Green, "Satellite-based entanglement distribution using orbital angular momentum of light," in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, Jul. 2020, pp. 1–6.

[195] S. Rogers, D. Mulkey, X. Lu, W. C. Jiang, and Q. Lin, "High visibility time-energy entangled photons from a silicon microdisk resonator," in *2016 Conference on Lasers and Electro-Optics (CLEO)*, 2016, pp. 1–2.

[196] E. Ji, Q. Liu, X. Fu, P. Du, M. Nie, F. Zhang, and M. Gong, "High-brightness semiconductor laser-pumped 1.56 μ m polarization-entangled photon pairs," *IEEE J. Quantum Electron.*, vol. 53, no. 2, pp. 1–6, 2017.

[197] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," *Nat. Phys.*, vol. 3, no. 7, pp. 481–486, Jun. 2007.

[198] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, "Quantum teleportation over 143 kilometres using active feed-forward," *Nature*, vol. 489, no. 7415, pp. 269–273, Sep. 2012.

[199] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, K.-X. Yang, X. Han, Y.-Q. Yao, J. Li, H.-Y. Wu, S. Wan, L. Liu, D.-Q. Liu, Y.-W. Kuang, Z.-P. He, P. Shang, C. Guo, R.-H. Zheng, K. Tian, Z.-C. Zhu, N.-L. Liu, C.-Y. Lu, R. Shu, Y.-A. Chen, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, no. 7670, pp. 70–73, Aug. 2017.

[200] F. A. Bovino, P. Varisco, A. M. Colla, G. Castagnoli, G. Di Giuseppe, and A. V. Sergienko, "Effective fiber-coupling of entangled photons for quantum communication," *Opt. Commun.*, vol. 227, no. 4-6, pp. 343–348, Nov. 2003.

[201] K. Banaszek, A. B. U'Ren, and I. A. Walmsley, "Generation of correlated photons in controlled spatial modes by downconversion in nonlinear waveguides," *Opt. Lett.*, vol. 26, no. 17, pp. 1367–1369, Sep. 2001.

[202] K. Sanaka, K. Kawahara, and T. Kuga, "New high-efficiency source of photon pairs for engineering quantum entanglement," *Phys. Rev. Lett.*, vol. 86, no. 24, pp. 5620–5623, Jun. 2001.

[203] M. C. Booth, M. Atatüre, G. Di Giuseppe, B. E. Saleh, A. V. Sergienko, and M. C. Teich, "Counterpropagating entangled photons from a waveguide with periodic nonlinearity," *Phys. Rev. A*, vol. 66, no. 2, Aug. 2002, Art. no. 023815.

[204] M. Fiorentino, P. L. Voss, J. E. Sharping, and P. Kumar, "All-fiber photon-pair source for quantum communications," *IEEE Photon. Technol. Lett.*, vol. 14, no. 7, pp. 983–985, Jul. 2002.

[205] H. Takesue and K. Inoue, "Generation of 1.5- μ m band time-bin entanglement using spontaneous fiber four-wave mixing and planar light-wave circuit interferometers," *Phys. Rev. A*, vol. 72, no. 4, Oct. 2005, Art. no. 041804.

[206] J. Fan and A. Migdall, "A broadband high spectral brightness fiber-based two-photon source," *Opt. Express*, vol. 15, no. 6, pp. 2915–2920, Mar. 2007.

[207] J. W. Silverstone, D. Bonneau, K. Ohira, N. Suzuki, H. Yoshida, N. Iizuka, M. Ezaki, C. M. Natarajan, M. G. Tanner, R. H. Hadfield, V. Zwiller, G. D. Marshall, J. G. Rarity, J. L. O'Brien, and M. G.

[208] H. Takesue and K. Inoue, "1.5-μm band quantum-correlated photon pair generation in dispersion-shifted fiber: suppression of noise photons by cooling fiber," *Opt. Express*, vol. 13, no. 20, pp. 7832–7839, Oct. 2005.

[209] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nat. Photonics*, vol. 3, no. 12, pp. 696–705, 2009.

[210] R. Kumar, M. Lucamarini, G. Di Giuseppe, R. Natali, G. Mancini, and P. Tombesi, "Two-way quantum key distribution at telecommunication wavelength," *Phys. Rev. A*, vol. 77, no. 2, Feb. 2008, Art. no. 022304.

[211] M. A. Itzler, R. Ben-Michael, C.-F. Hsu, K. Slomkowski, A. Tosi, S. Cova, F. Zappa, and R. Ispasoiu, "Single photon avalanche diodes (SPADs) for 1.5 μ m photon counting applications," *J. Mod. Opt.*, vol. 54, no. 2-3, pp. 283–304, Jan. 2007.

[212] A. Restelli, J. C. Bienfang, and A. L. Migdall, "Single-photon detection efficiency up to 50% at 1310 nm with an InGaAs/InP avalanche diode gated at 1.25 GHz," *Appl. Phys. Lett.*, vol. 102, no. 14, Apr. 2013, Art. no. 141104.

[213] L. C. Comandar, B. Fröhlich, J. F. Dynes, A. W. Sharpe, M. Lucamarini, Z. Yuan, R. V. Penty, and A. J. Shields, "Gigahertz-gated InGaAs/InP single-photon detector with detection efficiency exceeding 55% at 1550 nm," *J. Appl. Phys.*, vol. 117, no. 8, Feb. 2015, Art. no. 083109.

[214] O. Thomas, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, "Efficient photon number detection with silicon avalanche photodiodes," *Appl. Phys. Lett.*, vol. 97, no. 3, Jul. 2010, Art. no. 031102.

[215] W. Buttler, R. Hughes, P. Kwiat, S. Lamoreaux, G. Luther, G. Morgan, J. Nordholt, C. Peterson, and C. Simmons, "Practical free-space quantum key distribution over 1 km," *Phys. Rev. Lett.*, vol. 81, no. 15, pp. 3283–3286, Oct. 1998.

[216] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New J. Phys.*, vol. 4, no. 1, 2002, Art. no. 43.

[217] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, "Detecting single infrared photons with 93% system efficiency," *Nat. Photonics*, vol. 7, no. 3, pp. 210–214, Mar. 2013.

[218] K. Smirnov, A. Divochiy, Y. Vakhtomin, P. Morozov, P. Zolotov, A. Antipov, and V. Seleznev, "NbN single-photon detectors with saturated dependence of quantum efficiency," *Supercond. Sci. Technol.*, vol. 31, no. 3, Feb. 2018, Art. no. 035011.

[219] H. Shibata, K. Shimizu, H. Takesue, and Y. Tokura, "Ultimate low system dark-count rate for superconducting nanowire single-photon detector," *Opt. Lett.*, vol. 40, no. 14, pp. 3428–3431, Jul. 2015.

[220] B. Korzh, Q.-Y. Zhao, J. P. Allmaras, S. Frasca, T. M. Autry, E. A. Bersin, R. M. Beyer, Andrew D. ad Briggs, B. Bumble, M. Colangelo, G. M. Crouch, A. E. Dane, T. Gerrits, A. E. Lita, F. Marsili, G. Moody, C. Peña, E. Ramirez, J. D. Rezac, N. Sinclair, M. J. Stevens, A. E. Velasco, V. B. Verma, E. E. Wollman, S. Xie, D. Zhu, P. D. Hale, M. Spiropulu, K. L. Silverman, R. P. Mirin, S. W. Nam, A. G. Kozorezov, M. D. Shaw, and K. K. Berggren, "Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector," *Nat. Photonics*, vol. 14, no. 4, pp. 250–255, Apr. 2020.

[221] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, no. 19, Nov. 2016, Art. no. 190501.

[222] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, no. 19, Nov. 2018, Art. no. 190502.

[223] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, May 2018.

[224] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Commun. Surv. Tut.*, vol. 21, no. 1, pp. 881–919, Aug. 2018.

[225] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan, W. Chen, Y.-H. Gong, Y. Li, Z.-H. Lin, G.-S. Pan, J. S. Pelc, M. M. Fejer, W.-Z. Zhang, W.-Y. Liu, J. Yin, J.-G. Ren, X.-B. Wang, Q. Zhang, C.-Z. Peng, and J.-W. Pan, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nat. Photonics*, vol. 11, no. 8, pp. 509–513, Jul. 2017.

[226] A. Restelli, J. C. Bienfang, C. W. Clark, I. Rech, I. Labanca, M. Ghioni, and S. Cova, "Improved timing resolution single-photon detectors in daytime free-space quantum key distribution with 1.25 GHz transmission rate," *IEEE J. Sel. Topics Quantum Electron.*, vol. 16, no. 5, pp. 1084–1090, Sept.-Oct. 2010.

[227] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, "Free-space quantum key distribution by rotation-invariant twisted photons," *Phys. Rev. Lett.*, vol. 113, no. 6, Aug. 2014, Art. no. 060503.

[228] H. V. Nguyen, P. V. Trinh, A. T. Pham, Z. Babar, D. Alanis, P. Botsinis, D. Chandra, S. X. Ng, and L. Hanzo, "Network coding aided cooperative quantum key distribution over free-space optical channels," *IEEE Access*, vol. 5, pp. 12301–12317, Jun. 2017.

[229] J. H. Shapiro, "Near-field turbulence effects on quantum-key distribution," *Phys. Rev. A*, vol. 67, no. 2, Feb. 2003, Art. no. 022309.

[230] D. Y. Vasylyev, A. Semenov, and W. Vogel, "Toward global quantum communication: beam wandering preserves nonclassicality," *Phys. Rev. Lett.*, vol. 108, no. 22, Jun. 2012, Art. no. 220501.

[231] D. Vasylyev, A. Semenov, and W. Vogel, "Atmospheric quantum channels with weak and strong turbulence," *Phys. Rev. Lett.*, vol. 117, no. 9, Aug. 2016, Art. no. 090501.

[232] D. Vasylyev, W. Vogel, and A. Semenov, "Theory of atmospheric quantum channels based on the law of total probability," *Phys. Rev. A*, vol. 97, no. 6, Jun. 2018, Art. no. 063852.

[233] P. V. Trinh, T. V. Pham, N. T. Dang, H. V. Nguyen, S. X. Ng, and A. T. Pham, "Design and security analysis of quantum key distribution protocol over free-space optics using dual-threshold direct-detection receiver," *IEEE Access*, vol. 6, pp. 4159–4175, Jan. 2018.

[234] L. Moli-Sanchez, A. Rodriguez-Alonso, and G. Seco-Granados, "Performance analysis of quantum cryptography protocols in optical earth-satellite and intersatellite links," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1582–1590, Dec. 2009.

[235] H. Kaushal and G. Kaddoum, "Optical communication in space: challenges and mitigation techniques," *IEEE Commun. Surv. Tut.*, vol. 19, no. 1, pp. 57–96, Aug. 2017.

[236] D. Vasylyev, A. Semenov, W. Vogel, K. Günthner, A. Thurn, Ö. Bayraktar, and C. Marquardt, "Free-space quantum links under diverse weather conditions," *Phys. Rev. A*, vol. 96, no. 4, Oct. 2017, Art. no. 043856.

[237] D. Vasylyev, A. Semenov, and W. Vogel, "Characterization of free-space quantum channels," in *Quantum Communications and Quantum Imaging XVI*, vol. 10771, SPIE, Sep. 2018, pp. 133–148.

[238] A. Trushechkin, P. Tregubov, E. Kiktenko, Y. V. Kurochkin, and A. Fedorov, "Quantum-key-distribution protocol with pseudorandom bases," *Phys. Rev. A*, vol. 97, no. 1, Jan. 2018, Art. no. 012311.

[239] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Rev. Sci. Instrum.*, vol. 71, no. 4, pp. 1675–1680, Apr. 2000.

[240] P. Wang, G. Long, and Y. Li, "Scheme for a quantum random number generator," *J. Appl. Phys.*, vol. 100, no. 5, Sep. 2006, Art. no. 056107.

[241] E. de Jesus Lopes Soares, F. A. Mendonca, and R. V. Ramos, "Quantum random number generator using only one single-photon detector," *IEEE Photon. Technol. Lett.*, vol. 26, no. 9, pp. 851–853, May 2014.

[242] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, "Photon arrival time quantum random number generation," *J. Mod. Opt.*, vol. 56, no. 4, pp. 516–522, Mar. 2009.

[243] H. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," *Opt. Express*, vol. 18, no. 12, pp. 13029–13037, Jun. 2010.

[244] Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, "Practical and fast quantum random number generation based on photon arrival time relative to external reference," *Appl. Phys. Lett.*, vol. 104, no. 5, Feb. 2014, Art. no. 051110.

[245] W. Wei and H. Guo, "Bias-free true random-number generator," *Opt. Lett.*, vol. 34, no. 12, pp. 1876–1878, Jun. 2009.

[246] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, "Quantum random-number generator based on a photon-number-resolving detector," *Phys. Rev. A*, vol. 83, no. 2, Dec. 2011, Art. no. 023820.

[247] H. Zhou, J. Li, D. Pan, W. Zhang, and G. Long, "Quantum random number generator based on quantum tunneling effect," *arXiv preprint arXiv:1711.01752*, 2017.

[248] H. Zhou, J. Li, W. Zhang, and G.-L. Long, "Quantum random-number generator based on tunneling effects in a Si diode," *Phys. Rev. Appl*, vol. 11, no. 3, Mar. 2019, Art. no. 034060.

[249] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan, H. Li, W. J. Munro, Z. Wang, L. You, J. Zhang, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, "Device-independent quantum random-number generation," *Nature*, vol. 562, no. 7728, pp. 548–551, Sep. 2018.

[250] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm, "Experimentally generated randomness certified by the impossibility of superluminal signals," *Nature*, vol. 556, no. 7700, pp. 223–226, Apr. 2018.

[251] J. Liu, J. Yang, Z. Li, Q. Su, W. Huang, B. Xu, and H. Guo, "117 Gbits/s quantum random number generation with simple structure," *IEEE Photon. Technol. Lett.*, vol. 29, no. 3, pp. 283–286, Dec. 2017.

[252] F.-X. Wang, C. Wang, W. Chen, S. Wang, F.-S. Lv, D.-Y. He, Z.-Q. Yin, H.-W. Li, G.-C. Guo, and Z.-F. Han, "Robust quantum random number generator based on avalanche photodiodes," *J. Lightwave Technol.*, vol. 33, no. 15, pp. 3319–3326, May 2015.

[253] H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," *Phys. Rev. E*, vol. 81, no. 5, 2010, Art. no. 051137.

[254] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations," *Rev. Sci. Instrum.*, vol. 86, no. 6, Jun. 2015, Art. no. 063105.

[255] Q. Zhou, R. Valivarthi, C. John, and W. Tittel, "Practical quantum random-number generation based on sampling vacuum fluctuations," *Quantum Eng.*, vol. 1, no. 1, Mar. 2019, Art. no. e8.

[256] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," *Nat. Photonics*, vol. 4, no. 10, pp. 711–715, Aug. 2010.

[257] Y. Shen, L. Tian, and H. Zou, "Practical quantum random number generator based on measuring the shot noise of vacuum states," *Phys. Rev. A*, vol. 81, no. 6, Jun. 2010, Art. no. 063814.

[258] Y. Liu, M. Zhu, B. Luo, J. Zhang, and H. Guo, "Implementation of 1.6 tb s- 1 truly random number generation based on a super-luminescent emitting diode," *Laser Phys. Lett.*, vol. 10, no. 4, Feb. 2013, Art. no. 045001.

[259] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," *Phys. Rev. A*, vol. 87, no. 6, Jun. 2013, Art. no. 062327.

[260] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," *Nature*, vol. 464, no. 7291, pp. 1021–1024, Apr. 2010.

[261] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, "Bell measurements for teleportation," *Phys. Rev. A*, vol. 59, no. 5, pp. 3295–3300, May 1999.

[262] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, "Long-distance Bell-state analysis of fully independent polarization weak coherent states," *J. Lightwave Technol.*, vol. 31, no. 17, pp. 2881–2887, Jul. 2013.

[263] R. Valivarthi, I. Lucio-Martinez, A. Rubenok, P. Chan, F. Marsili, V. B. Verma, M. D. Shaw, J. A. Stern, J. A. Slater, D. Oblak, S. W. Nam, and W. Tittel, "Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors," *Opt. Express*, vol. 22, no. 20, pp. 24497–24506, Sep. 2014.

[264] L. Yu, C. M. Natarajan, T. Horikiri, C. Langrock, J. S. Pelc, M. G. Tanner, E. Abe, S. Maier, C. Schneider, S. Höfling, M. Kamp, R. H. Hadfield, M. M. Fejer, and Y. Yamamoto, "Two-photon interference at telecom wavelengths for time-bin-encoded single photons from quantum-dot spin qubits," *Nat. Commun.*, vol. 6, Nov. 2015, Art. no. 8955.

[265] P. G. Kwiat and H. Weinfurter, "Embedded Bell-state analysis," *Phys. Rev. A*, vol. 58, no. 4, pp. R2623–R2626, Oct. 1998.

[266] S. Walborn, S. Pádua, and C. Monken, "Hyperentanglement-assisted Bell-state analysis," *Phys. Rev. A*, vol. 68, no. 4, Oct. 2003, Art. no. 042313.

[267] C. Schuck, G. Huber, C. Kurtsiefer, and H. Weinfurter, "Complete deterministic linear optics Bell state analysis," *Phys. Rev. Lett.*, vol. 96, no. 19, 2006, Art. no. 190501.

[268] Y.-B. Sheng, F.-G. Deng, and G. L. Long, "Complete hyperentangled-Bell-state analysis for quantum communication," *Phys. Rev. A*, vol. 82, no. 3, Sep. 2010, Art. no. 032318.

[269] S. Mi, T.-j. Wang, G.-s. Jin, and C. Wang, "High-capacity quantum secure direct communication with orbital angular momentum of photons," *IEEE Photon. J.*, vol. 7, no. 5, Oct. 2015, Art. no. 7600108.

[270] S. Pirandola, S. L. Braunstein, S. Lloyd, and S. Mancini, "Confidential direct communications: a quantum approach using continuous variables," *IEEE J. Sel. Topics Quantum Electron.*, vol. 15, no. 6, pp. 1570–1580, Jul. 2009.

[271] Z. Cao, L. Wang, K. Liang, G. Chai, and J. Peng, "Continuous-variable quantum secure direct communication based on gaussian mapping," *Phys. Rev. Appl*, vol. 16, no. 2, Aug. 2021, Art. no. 024012.

[272] D. Liu, J.-L. Chen, and W. Jiang, "High-capacity quantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom," *Int. J. Theor. Phys.*, vol. 51, no. 9, pp. 2923–2929, May 2012.

[273] S. L. Braunstein and P. Van Loock, "Quantum information with continuous variables," *Rev. Mod. Phys.*, vol. 77, no. 2, pp. 513–577, Jun. 2005.

[274] C. H. Bennett and P. W. Shor, "Quantum information theory," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2724–2742, Oct. 1998.

[275] S. Imre, "Quantum communications: Explained for communication engineers," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 28–35, Aug. 2013.

[276] P. D. Townsend, "Experimental investigation of the performance limits for first telecommunications-window quantum cryptography systems," *IEEE Photon. Technol. Lett.*, vol. 10, no. 7, pp. 1048–1050, Jul. 1998.

[277] J.-S. Choe, H. Ko, B.-S. Choi, K.-J. Kim, and C. J. Youn, "Silica planar lightwave circuit based integrated 1×4 polarization beam splitter module for free-space BB84 quantum key distribution," *IEEE Photon. J.*, vol. 10, no. 1, Jan. 2018, Art. no. 7600108.

[278] J. Breguet, A. Muller, and N. Gisin, "Quantum cryptography with polarized photons in optical fibres: Experiment and practical limits," *J. Mod. Opt.*, vol. 41, no. 12, pp. 2405–2412, Mar. 1994.

[279] C. Bonato, M. Aspelmeyer, T. Jennewein, C. Pernechele, P. Villoresi, and A. Zeilinger, "Influence of satellite motion on polarization qubits in a space-earth quantum communication link," *Opt. Express*, vol. 14, no. 21, pp. 10050–10059, Oct. 2006.

[280] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, "Reference-frame-independent quantum key distribution," *Phys. Rev. A*, vol. 82, no. 1, Jul. 2010, Art. no. 012304.

[281] H.-K. Lo and J. Preskill, "Security of quantum key distribution using weak coherent states with nonrandom phases," *Quantum Inf. Comput.*, vol. 7, no. 5, pp. 431–458, Jul. 2007.

[282] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Source attack of decoy-state quantum key distribution using phase information," *Phys. Rev. A*, vol. 88, no. 2, Aug. 2013, Art. no. 022308.

[283] C. Gobby, Z. Yuan, and A. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Appl. Phys. Lett.*, vol. 84, no. 19, pp. 3762–3764, Apr. 2004.

[284] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, ""plug and play" systems for quantum cryptography," *Appl. Phys. Lett.*, vol. 70, no. 7, pp. 793–795, Feb. 1997.

[285] I. Marcikic, H. De Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, "Distribution of time-bin entangled qubits over 50 km of optical fiber," *Phys. Rev. Lett.*, vol. 93, no. 18, Oct. 2004, Art. no. 180502.

[286] Z.-Y. Zhou, Y. Li, D.-S. Ding, W. Zhang, S. Shi, B.-S. Shi, and G.-C. Guo, "Orbital angular momentum photonic quantum interface," *Light-Sci. Appl.*, vol. 5, no. 1, Jan. 2016, Art. no. e16019.

[287] M. Erhard, R. Fickler, M. Krenn, and A. Zeilinger, "Twisted photons: new quantum perspectives in high dimensions," *Light-Sci. Appl.*, vol. 7, no. 3, Mar. 2018, Art. no. 17146.

[288] L. Allen, M. W. Beijersbergen, R. Spreeuw, and J. Woerdman, "Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes," *Phys. Rev. A*, vol. 45, no. 11, pp. 8185–8189, Jun. 1992.

[289] I. B. Djordjevic, "Integrated optics modules based proposal for quantum information processing, teleportation, QKD, and quantum error correction employing photon angular momentum," *IEEE Photon. J.*, vol. 8, no. 1, Feb. 2016, Art. no. 6600212.

[290] Z.-R. Jian, G.-S. Jin, and T.-J. Wang, "Efficient quantum secure direct communication using the orbital angular momentum of single photons," *Int. J. Theor. Phys.*, vol. 55, no. 3, pp. 1811–1819, Mar. 2016.

[291] F. Farman, S. Tofighi, and A. Bahrampour, "Ping-pong protocol based on the orbital angular momentum of light," *JOSA B*, vol. 35, no. 10, pp. 2348–2355, Oct. 2018.

[292] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," *Phys. Rev. Lett.*, vol. 88, no. 12, Mar. 2002, Art. no. 127902.

[293] I. B. Djordjevic, "Multidimensional QKD based on combined orbital and spin angular momenta of photon," *IEEE Photon. J.*, vol. 5, no. 6, Nov. 2013, Art. no. 7600112.

[294] B. Qi, "Simultaneous classical communication and quantum key distribution using continuous variables," *Phys. Rev. A*, vol. 94, no. 4, Oct. 2016, Art. no. 042340.

[295] D. Pan, S. X. Ng, D. Ruan, L. Yin, G. Long, and L. Hanzo, "Simultaneous two-way classical communication and measurement-device-independent quantum key distribution with coherent states," *Phys. Rev. A*, vol. 101, no. 1, Jan. 2020, Art. no. 012343.

[296] S. Srikara, K. Thapliyal, and A. Pathak, "Continuous variable direct secure quantum communication using gaussian states," *Quantum Inf. Process.*, vol. 19, Mar. 2020, Art. no. 132.

[297] G. Chai, Z. Cao, W. Liu, M. Zhang, K. Liang, and J. Peng, "Novel continuous-variable quantum secure direct communication and its security analysis," *Laser Phys. Lett.*, vol. 16, no. 9, Aug. 2019, Art. no. 095207.

[298] I. Paparelle, M. Paris, and A. Zavatta, "Implementation and security analysis of continuous variable quantum secure direct communication protocols," *Il nuovo cimento C*, vol. 45, no. 6, pp. 1–4, Sep. 2022.

[299] I. Paparelle, F. Mousavi, F. Scazza, A. Bassi, M. Paris, and A. Zavatta, "Practical quantum secure direct communication with squeezed states," *arXiv preprint quant-ph/2306.14322*, 2023.

[300] T.-J. Wang, T. Li, F.-F. Du, and F.-G. Deng, "High-capacity quantum secure direct communication based on quantum hyperdense coding with hyperentanglement," *Chin. Phys. Lett.*, vol. 28, no. 4, Apr. 2011, Art. no. 040305.

[301] X.-D. Wu, L. Zhou, W. Zhong, and Y.-B. Sheng, "High-capacity measurement-device-independent quantum secure direct communication," *Quantum Inf. Process.*, vol. 19, p. 354, Sep. 2020.

[302] V. D'ambrosio, E. Nagali, S. P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci, and F. Sciarrino, "Complete experimental toolbox for alignment-free quantum communication," *Nat. Commun.*, vol. 3, Jul. 2012, Art. no. 961.

[303] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "High-dimensional intracity quantum cryptography with structured photons," *Optica*, vol. 4, no. 9, pp. 1006–1010, Aug. 2017.

[304] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 89, no. 3, Jun. 2002, Art. no. 037902.

[305] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," *Nat. Photonics*, vol. 1, no. 6, pp. 343–348, Jun. 2007.

[306] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nat. Photonics*, vol. 9, no. 3, pp. 163–168, Feb. 2015.

[307] K. Inoue and T. Honjo, "Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack," *Phys. Rev. A*, vol. 71, no. 4, 2005, Art. no. 042305.

[308] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Appl. Phys. Lett.*, vol. 87, no. 19, Nov. 2005, Art. no. 194108.

[309] J.-M. Merolla, Y. Mazurenko, J.-P. Goedgebuer, and W. T. Rhodes, "Single-photon interference in sidebands of phase-modulated light for quantum cryptography," *Phys. Rev. Lett.*, vol. 82, no. 8, pp. 1656–1659, Feb. 1999.

[310] L. Duraffourg, J.-M. Merolla, J.-P. Goedgebuer, Y. Mazurenko, and W. T. Rhodes, "Compact transmission system using single-sideband modulation of light for quantum cryptography," *Opt. Lett.*, vol. 26, no. 18, pp. 1427–1429, Sep. 2001.

[311] J.-M. Merolla, L. Duraffourg, J.-P. Goedgebuer, A. Soujaeff, F. Patois, and W. Rhodes, "Integrated quantum key distribution system using single sideband detection," *Eur. Phys. J. D*, vol. 18, no. 2, pp. 141–146, Feb. 2002.

[312] O. L. Guerreau, J.-M. Mérolla, A. Soujaeff, F. Patois, J.-P. Goedgebuer, and F. J. Malassenet, "Long-distance qkd transmission using single-sideband detection scheme with wdm synchronization," *IEEE J. Sel. Topics Quantum Electron.*, vol. 9, no. 6, pp. 1533–1540, Nov.-Dec. 2003.

[313] M. Bloch, S. W. McLaughlin, J.-M. Merolla, and F. Patois, "Frequency-coded quantum key distribution," *Opt. Lett.*, vol. 32, no. 3, pp. 301–303, Feb. 2007.

[314] T. Zhang, Z.-Q. Yin, Z.-F. Han, and G.-C. Guo, "A frequency-coded quantum key distribution scheme," *Opt. Commun.*, vol. 281, no. 18, pp. 4800–4802, Sep. 2008.

[315] X. Liu, G. Long, D. Tong, and F. Li, "General scheme for superdense coding between multiparties," *Phys. Rev. A*, vol. 65, no. 2, Jan. 2002, Art. no. 022304.

[316] H. Bechmann-Pasquinucci and A. Peres, "Quantum cryptography with 3-state systems," *Phys. Rev. Lett.*, vol. 85, no. 15, pp. 3313–3316, 2000.

[317] M. Krenn, M. Huber, R. Fickler, R. Lapkiewicz, S. Ramelow, and A. Zeilinger, "Generation and confirmation of a (100× 100)-dimensional entangled quantum system," *Proc. Natl. Acad. Sci.*, vol. 111, no. 17, pp. 6243–6247, Mar. 2014.

[318] A. Huang, S. Barz, E. Andersson, and V. Makarov, "Implementation vulnerabilities in general quantum cryptography," *New J. Phys.*, vol. 20, no. 10, Oct. 2018, Art. no. 103016.

[319] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nat. Photonics*, vol. 4, no. 10, pp. 686–689, Aug. 2010.

[320] Z. Gao, T. Li, and Z. Li, "Long-distance measurement-device–independent quantum secure direct communication," *Europhys. Lett.*, vol. 125, no. 4, Mar. 2019, Art. no. 40004.

[321] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130503.

[322] F.-G. Deng and G.-L. Long, "Controlled order rearrangement encryption for quantum key distribution," *Phys. Rev. A*, vol. 68, no. 4, Oct. 2003, Art. no. 042315.

[323] J. Wang, Q. Zhang, and C.-j. Tang, "Quantum secure direct communication based on order rearrangement of single photons," *Phys. Lett. A*, vol. 358, no. 4, pp. 256–258, Oct. 2006.

[324] X.-H. Li, F.-G. Deng, and H.-Y. Zhou, "Improving the security of secure direct communication based on the secret transmitting order of particles," *Phys. Rev. A*, vol. 74, no. 5, Nov. 2006, Art. no. 054302.

[325] G. He, J. Zhu, and G. Zeng, "Quantum secure communication using continuous variable Einstein-Podolsky-Rosen correlations," *Phys. Rev. A*, vol. 73, no. 1, Jan. 2006, Art. no. 012314.

[326] J. Wang, Q. Zhang, and C.-j. Tang, "Multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilinger state," *Opt. Commun.*, vol. 266, no. 2, pp. 732–737, Oct. 2006.

[327] Z.-X. Man, Y.-J. Xia, and N. B. An, "Quantum secure direct communication by using GHZ states and entanglement swapping," *J. Phys. B: At., Mol. Opt. Phys.*, vol. 39, no. 18, pp. 3855–3863, Sep. 2006.

[328] X.-B. Chen, Q.-Y. Wen, F.-Z. Guo, Y. Sun, G. Xu, and F.-C. Zhu, "Controlled quantum secure direct communication with W state," *Int. J. Quantum Inf.*, vol. 6, no. 04, pp. 899–906, Aug. 2008.

[329] A. Chamoli and C. Bhandari, "Secure direct communication based on ping–pong protocol," *Quantum Inf. Process.*, vol. 8, no. 4, pp. 347–356, Apr. 2009.

[330] C.-Y. Lu, S.-A. Wang, Y.-J. Cheng, and S.-Y. Kuo, "Quantum secure direct communication with a constant number of EPR pairs," *Int. J. Quantum Inf.*, vol. 8, no. 08, pp. 1355–1371, Dec. 2010.

[331] Z. Liu, H. Chen, W. Liu, J. Xu, D. Wang, and Z. Li, "Quantum secure direct communication with optimal quantum superdense coding by using general four-qubit states," *Quantum Inf. Process.*, vol. 12, no. 1, pp. 587–599, Apr. 2013.

[332] B.-C. Ren, H.-R. Wei, M. Hua, T. Li, and F.-G. Deng, "Photonic spatial Bell-state analysis for robust quantum secure direct communication using quantum dot-cavity systems," *Eur. Phys. J. D*, vol. 67, no. 2, Mar. 2013, Art. no. 30.

[333] A. Meslouhi and Y. Hassouni, "A quantum secure direct communication protocol using entangled modified spin coherent states," *Quantum Inf. Process.*, vol. 12, no. 7, pp. 2603–2621, Mar. 2013.

[334] Y. Xia and H.-S. Song, "Controlled quantum secure direct communication using a non-symmetric quantum channel with quantum superdense coding," *Phys. Lett. A*, vol. 364, no. 2, pp. 117–122, Mar. 2007.

[335] L. Dong, X.-M. Xiu, Y.-J. Gao, Y.-P. Ren, and H.-W. Liu, "Controlled three-party communication using GHZ-like state and imperfect Bell-state measurement," *Opt. Commun.*, vol. 284, no. 3, pp. 905–908, Feb. 2011.

[336] G. Gao, "Secure multiparty quantum secret sharing with the collective eavesdropping-check character," *Quantum Inf. Process.*, vol. 12, no. 1, pp. 55–68, Jan. 2013.

[337] T.-Y. Ye and L.-Z. Jiang, "Quantum dialogue without information leakage based on the entanglement swapping between any two Bell states and the shared secret Bell state," *Phys. Scr.*, vol. 89, no. 1, Dec. 2013, Art. no. 015103.

[338] Y. Cao, A.-M. Wang, X.-S. Ma, and N.-B. Zhao, "Multi-particle and high-dimension controlled order rearrangement encryption protocols," *Eur. Phys. J. D*, vol. 44, no. 3, pp. 607–617, Jul. 2007.

[339] S. Lin, Q.-Y. Wen, F. Gao, and F.-C. Zhu, "Eavesdropping on secure deterministic communication with qubits through photon-number-splitting attacks," *Phys. Rev. A*, vol. 79, no. 5, May 2009, Art. no. 054303.

[340] H. Lu, "Upper bound on key generation rate of quantum key distribution with two-way or two-step quantum channels," *Opt. Commun.*, vol. 284, no. 8, pp. 2254–2256, Apr. 2011.

[341] C.-H. F. Fung, X. Ma, H. Chau, and Q.-y. Cai, "Quantum key distribution with delayed privacy amplification and its application to the security proof of a two-way deterministic protocol," *Phys. Rev. A*, vol. 85, no. 3, Mar. 2012, Art. no. 032308.

[342] H. Lu, C.-H. F. Fung, and Q.-y. Cai, "Two-way deterministic quantum key distribution against detector-side-channel attacks," *Phys. Rev. A*, vol. 88, no. 4, Oct. 2013, Art. no. 044302.

[343] N. J. Beaudry, M. Lucamarini, S. Mancini, and R. Renner, "Security of two-way quantum key distribution," *Phys. Rev. A*, vol. 88, no. 6, Dec. 2013, Art. no. 062302.

[344] M. Lucamarini and S. Mancini, "Quantum key distribution using a two-way quantum channel," *Theor. Comput. Sci.*, vol. 560, pp. 46–61, 2014.

[345] J. S. Shaari, M. Lucamarini, and S. Mancini, "Checking noise correlations for safer two-way quantum key distribution," *Quantum Inf. Process.*, vol. 13, no. 5, pp. 1139–1153, Dec. 2014.

[346] H. Lu, "Two-way deterministic quantum key distribution against passive detector side channel attacks in the forward line," *Quantum Inf. Process.*, vol. 14, no. 10, pp. 3827–3834, Aug. 2015.

[347] C. I. Henao and R. M. Serra, "Practical security analysis of two-way quantum-key-distribution protocols based on nonorthogonal states," *Phys. Rev. A*, vol. 92, no. 5, Nov. 2015, Art. no. 052317.

[348] H. Lu, "Ambiguous discrimination among linearly dependent quantum states and its application to two-way deterministic quantum key distribution," *JOSA B*, vol. 36, no. 3, pp. B26–B30, Mar. 2019.

[349] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

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

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

[352] P.-H. Niu, J.-W. Wu, L.-G. Yin, and G.-L. Long, "Security analysis of measurement-device-independent quantum secure direct communication," *Quantum Inf. Process.*, vol. 19, no. 10, Sep. 2020, Art. no. 356.

[353] Z.-D. Ye, D. Pan, Z. Sun, C.-G. Du, L.-G. Yin, and G.-L. Long, "Generic security analysis framework for quantum secure direct communication," *Front. Phys.*, vol. 16, Dec. 2021, Art. no. 21503.

[354] M. Niemiec and A. R. Pach, "Management of security in quantum cryptography," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 36–41, Aug. 2013.

[355] J. Xin and Z. Shou, "Secure quantum dialogue based on single-photon," *Chin. Phys.*, vol. 15, no. 7, pp. 1418–1420, Jul. 2006.

[356] G.-F. Shi, X.-Q. Xi, M.-L. Hu, and R.-H. Yue, "Quantum secure dialogue by using single photons," *Opt. Commun.*, vol. 283, no. 9, pp. 1984–1986, May 2010.

[357] A. Pathak, *Elements of quantum computation and quantum communication*, CRC Press, 2013.

[358] C. Zheng and G. Long, "Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs," *Sci. China Phys., Mech. Astron.*, vol. 57, no. 7, pp. 1238–1243, Apr. 2014.

[359] G. Gao, "Two quantum dialogue protocols without information leakage," *Opt. Commun.*, vol. 283, no. 10, pp. 2288–2293, May 2010.

[360] F.-G. Deng, X.-H. Li, H.-Y. Zhou, and Z.-j. Zhang, "Improving the security of multiparty quantum secret sharing against Trojan horse attack," *Phys. Rev. A*, vol. 72, no. 4, Oct. 2005, Art. no. 044302.

[361] L.-F. Han, Y.-M. Liu, J. Liu, and Z.-J. Zhang, "Multiparty quantum secret sharing of secure direct communication using single photons," *Opt. Commun.*, vol. 281, no. 9, pp. 2690–2694, May 2008.

[362] R. Du, Z. Sun, B. Wang, and D. Long, "Quantum secret sharing of secure direct communication using one-time pad," *Int. J. Theor. Phys.*, vol. 51, no. 9, pp. 2727–2736, Apr. 2012.

[363] Z.-J. Zhang, "Multiparty quantum secret sharing of secure direct communication," *Phys. Lett. A*, vol. 342, no. 1-2, pp. 60–66, Jul. 2005.

[364] X. Wang, Y.-M. Liu, L.-F. Han, and Z.-J. Zhang, "Multiparty quantum secret sharing of secure direct communication with high-dimensional quantum superdense coding," *Int. J. Quantum Inf.*, vol. 6, no. 06, pp. 1155–1163, Dec. 2008.

[365] Y.-G. Yang, J. Tian, J. Xia, and H. Zhang, "Quantum authenticated direct communication using Bell states," *Int. J. Theor. Phys.*, vol. 52, no. 2, pp. 336–344, Sep. 2013.

[366] C.-H. Yu, G.-D. Guo, and S. Lin, "Quantum secure direct communication with authentication using two nonorthogonal states," *Int. J. Theor. Phys.*, vol. 52, no. 6, pp. 1937–1945, Sep. 2013.

[367] M. Naseri, "Secure quantum sealed-bid auction," *Opt. Commun.*, vol. 282, no. 9, pp. 1939–1943, May 2009.

[368] Y.-G. Yang, M. Naseri, and Q.-Y. Wen, "Improved secure quantum sealed-bid auction," *Opt. Commun.*, vol. 282, no. 20, pp. 4167–4170, Oct. 2009.

[369] Z. Zhao, M. Naseri, and Y. Zheng, "Secure quantum sealed-bid auction with post-confirmation," *Opt. Commun.*, vol. 283, no. 16, pp. 3194–3197, Aug. 2010.

[370] Y. Luo, Z. Zhao, Z. Zhao, H. Long, W. Su, and Y. Yang, "The loophole of the improved secure quantum sealed-bid auction with post-confirmation and solution," *Quantum Inf. Process.*, vol. 12, no. 1, pp. 295–302, Jan. 2013.

[371] Z.-Y. Wang, "Quantum secure direct communication and quantum sealed-bid auction with EPR pairs," *Commun. Theor. Phys.*, vol. 54, no. 6, pp. 997–1002, Dec. 2010.

[372] W.-J. Liu, F. Wang, S. Ji, Z.-G. Qu, and X.-J. Wang, "Attacks and improvement of quantum sealed-bid auction with EPR pairs," *Commun. Theor. Phys.*, vol. 61, no. 6, pp. 686–690, Jun. 2014.

[373] R. Zhang, R.-h. Shi, J.-q. Qin, and Z.-w. Peng, "An economic and feasible quantum sealed-bid auction protocol," *Quantum Inf. Process.*, vol. 17, no. 2, Jan. 2018, Art. no. 35.

[374] Z.-G. Qu, X.-B. Chen, X.-J. Zhou, X.-X. Niu, and Y.-X. Yang, "Novel quantum steganography with large payload," *Opt. Commun.*, vol. 283, no. 23, pp. 4782–4786, Dec. 2010.

[375] Z.-G. Qu, X.-B. Chen, M.-X. Luo, X.-X. Niu, and Y.-X. Yang, "Quantum steganography with large payload based on entanglement swapping of χ-type entangled states," *Opt. Commun.*, vol. 284, no. 7, pp. 2075–2082, Apr. 2011.

[376] S. Xu, X. Chen, X. Niu, and Y. Yang, "High-efficiency quantum steganography based on the tensor product of Bell states," *Sci. China Phys., Mech. Astron.*, vol. 56, no. 9, pp. 1745–1754, Jul. 2013.

[377] N. Fatahi and M. Naseri, "Quantum watermarking using entanglement swapping," *Int. J. Theor. Phys.*, vol. 51, no. 7, pp. 2094–2100, Feb. 2012.

[378] J. Mo, Z. Ma, Y. Yang, and X. Niu, "A quantum watermarking protocol based on Bell dual basis," *Int. J. Theor. Phys.*, vol. 52, no. 11, pp. 3813–3819, Jun. 2013.

[379] S.-J. Xu, X.-B. Chen, X.-X. Niu, and Y.-X. Yang, "A novel quantum covert channel protocol based on any quantum secure direct communication scheme," *Commun. Theor. Phys.*, vol. 59, no. 5, pp. 547–553, May 2013.

[380] W. Huang, Q.-Y. Wen, B. Liu, Q. Su, S.-J. Qin, and F. Gao, "Quantum anonymous ranking," *Phys. Rev. A*, vol. 89, no. 3, Mar. 2014, Art. no. 032325.

[381] C. Yan, X. Chun-Xiang, Z. Shi-Bin, and Y. Li-Li, "Quantum broadcast communication and authentication protocol with a quantum one-time pad," *Chin. Phys. B*, vol. 23, no. 1, Dec. 2013, Art. no. 010305.

[382] Y. Cao and F. Gao, "Cryptanalysis of quantum broadcast communication and authentication protocol with a one-time pad," *Chin. Phys. B*, vol. 25, no. 11, Sep. 2016, Art. no. 110305.

[383] C. S. Yoon, M. S. Kang, J. I. Lim, and H. J. Yang, "Quantum signature scheme based on a quantum search algorithm," *Phys. Scr.*, vol. 90, no. 1, Dec. 2014, Art. no. 015103.

[384] W. Huang, Q.-Y. Wen, B. Liu, F. Gao, and Y. Sun, "Quantum key agreement with EPR pairs and single-particle measurements," *Quantum Inf. Process.*, vol. 13, no. 3, pp. 649–663, Mar. 2014.

[385] Z. Sun, J. Yu, and P. Wang, "Efficient multi-party quantum key agreement by cluster states," *Quantum Inf. Process.*, vol. 15, no. 1, pp. 373–384, Jan. 2016.

[386] G.-J. Zeng, K.-H. Chen, Z.-H. Chang, Y.-S. Yang, and Y.-H. Chou, "Multiparty quantum key agreement based on quantum secret direct communication with GHZ states," *arXiv preprint arXiv:1602.00832*, 2016.

[387] Y.-H. Chou, G.-J. Zeng, Z.-H. Chang, and S.-Y. Kuo, "Dynamic group multi-party quantum key agreement," *Sci. Rep.*, vol. 8, no. 1, Mar. 2018, Art. no. 4633.

[388] Z.-W. Sun, R.-G. Du, and D.-Y. Long, "Quantum secure direct communication with quantum identification," *Int. J. Quantum Inf.*, vol. 10, no. 01, Feb. 2012, Art. no. 1250008.

[389] S. J. Phoenix, S. M. Barnett, P. D. Townsend, and K. Blow, "Multi-user quantum cryptography on optical networks," *J. Mod. Opt.*, vol. 42, no. 6, pp. 1155–1163, Jun. 1995.

[390] M. Razavi, "Multiple-access quantum key distribution networks," *IEEE Trans. Commun.*, vol. 60, no. 10, pp. 3071–3079, Oct. 2012.

[391] 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 Eng.*, vol. 2022, Aug. 2022, Art. no. 6345981.

[392] F.-G. Deng, X.-S. Liu, Y.-J. Ma, L. Xiao, and G.-L. Long, "A theoretical scheme for multi-user quantum key distribution with N Einstein-Podolsky-Rosen pairs on a passive optical network," *Chin. Phys. Lett.*, vol. 19, no. 7, pp. 893–896, Feb. 2002.

[393] X.-H. Li, P. Zhou, Y.-J. Liang, C.-Y. Li, H.-Y. Zhou, and F.-G. Deng, "Quantum secure direct communication network with two-step protocol," *Chin. Phys. Lett.*, vol. 23, no. 5, pp. 1080–1083, May 2006.

[394] F.-G. Deng, X.-H. Li, C.-Y. Li, P. Zhou, and H.-Y. Zhou, "Economical quantum secure direct communication network with single photons," *Chin. Phys.*, vol. 16, no. 12, pp. 3553–3559, 2007.

[395] B. Gu, Y.-G. Huang, X. Fang, and Y.-L. Chen, "Bidirectional quantum secure direct communication network protocol with hyperentanglement," *Commun. Theor. Phys.*, vol. 56, no. 4, pp. 659–663, Oct. 2011.

[396] C. H. Hong, J. Heo, J. I. Lim, and H. J. Yang, "Quantum secure direct communication network with hyperentanglement," *Chin. Phys. B*, vol. 23, no. 9, Jul. 2014, Art. no. 090309.

[397] K. Kim, B. Kim, and J. Heo, "Security analysis of one-step qsdc protocol with hyperentanglement," in *2022 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*, Oct. 2022, pp. 155–159.

[398] L.-H. Gong, Y. Liu, and N.-R. Zhou, "Novel quantum virtual private network scheme for PON via quantum secure direct communication," *Int. J. Theor. Phys.*, vol. 52, no. 9, pp. 3260–3268, Sep. 2013.

[399] Y.-H. Chou, G.-J. Zeng, F.-J. Lin, C.-Y. Chen, and H.-C. Chao, "Quantum secure communication network protocol with entangled photons for mobile communications," *Mobile Netw. Appl.*, vol. 19, no. 1, pp. 121–130, Feb. 2014.

[400] S.-A. Wang and C.-Y. Lu, "Quantum secure direct communication network," in *Nanotechnology (IEEE-NANO), 2013 13th IEEE Conference on*. IEEE, 2013, pp. 752–755.

[401] F. Zarmehi and M. Houshmand, "Controlled bidirectional quantum secure direct communication network using classical XOR operation and quantum entanglement," *IEEE Commun. Lett.*, vol. 20, no. 10, pp. 2071–2074, Jul. 2016.

[402] C. Elliott, "The DARPA quantum network," *arXiv preprint quant-ph/0412029*, 2004.

[403] A. Poppe, M. Peev, and O. Maurhart, "Outline of the secoqc quantum-key-distribution network in vienna," *Int. J. Quantum Inf.*, vol. 6, no. 02, pp. 209–218, Apr. 2008.

[404] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Metropolitan all-pass and inter-city quantum communication network," *Opt. Express*, vol. 18, no. 26, pp. 27217–27225, Dec. 2010.

[405] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Express*, vol. 19, no. 11, pp. 10387–10409, May 2011.

[406] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, "Field and long-term demonstration of a wide area quantum key distribution network," *Opt. Express*, vol. 22, no. 18, pp. 21739–21756, Sep. 2014.

[407] Y. Cao, Y. Zhao, J. Zhang, Q. Wang, D. Niyato, and L. Hanzo, "From single-protocol to large-scale multi-protocol quantum networks," *IEEE Netw.*, vol. 36, no. 5, pp. 14–22, Nov. 2022.

[408] M. Ostermeyer and N. Walenta, "On the implementation of a deterministic secure coding protocol using polarization entangled photons," *Opt. Commun.*, vol. 281, no. 17, pp. 4540–4544, Sep. 2008.

[409] H. Chen, Z.-Y. Zhou, A. J. J. Zangana, Z.-Q. Yin, J. Wu, Y.-G. Han, S. Wang, H.-W. Li, D.-Y. He, S. K. Tawfeeq, B.-S. Shi, G.-C. Guo, W. Chen, and Z.-F. Han, "Experimental demonstration on the deterministic quantum key distribution based on entangled photons," *Sci. Rep.*, vol. 6, Feb. 2016, Art. no. 20962.

[410] A. Cere, M. Lucamarini, G. Di Giuseppe, and P. Tombesi, "Experimental test of two-way quantum key distribution in the presence of controlled noise," *Phys. Rev. Lett.*, vol. 96, no. 20, May 2006, Art. no. 200501.

[411] M. F. A. Khir, M. A. M. Zain, S. Saharudin, S. Soekardjo, and S. B. H. Shaari, "Implementation of two-way free space quantum key distribution," *Opt. Eng.*, vol. 51, no. 4, 2012, Art. no. 045006.

[412] M. F. Abdul Khir, M. N. Mohd Zain, Iskandar Bahari, Suryadi and S. Shaari, "Implementation of two way quantum key distribution protocol with decoy state," *Opt. Commun.*, vol. 285, no. 5, pp. 842–845, Mar. 2012.

[413] K. Wen and G. L. Long, "One-party quantum-error-correcting codes for unbalanced errors: principles and application to quantum dense coding and quantum secure direct communication," *Int. J. Quantum Inf.*, vol. 8, no. 04, pp. 697–719, Jun. 2010.

[414] N. Zamir, M. F. U. Butt, Z. Babar, and S. X. Ng, "Secure quantum turbo coded superdense coding scheme," in *2018 IEEE 29th Annual Int. Symp. on Personal, Indoor and Mobile Radio Commun. (PIMRC)*, IEEE, 2018, pp. 1–5.

[415] Y.-B. Li, T.-T. Song, W. Huang, and W.-W. Zhan, "Fault-tolerant quantum secure direct communication protocol based on decoherence-free states," *Int. J. Theor. Phys.*, vol. 54, no. 2, pp. 589–597, Jul. 2015.

[416] S.-J. Qin, F. Gao, Q.-Y. Wen, and F.-C. Zhu, "Robust quantum secure direct communication over collective rotating channel," *Commun. Theor. Phys.*, vol. 53, no. 4, pp. 645–647, Apr. 2010.

[417] Z. Gao, M. Ma, T. Liu, J. Long, T. Li, and Z. Li, "Free-space quantum secure direct communication based on decoherence-free space," *JOSA B*, vol. 37, no. 10, pp. 3028–3033, Oct. 2020.

[418] T. Pittman, B. Jacobs, and J. Franson, "Single photons on pseudodemand from stored parametric down-conversion," *Phys. Rev. A*, vol. 66, no. 4, Oct. 2002, Art. no. 042303.

[419] F. Zhu, W. Zhang, and Y. Huang, "Fiber-based frequency-degenerate polarization entangled photon pair sources for information encoding," *Opt. Express*, vol. 24, no. 22, pp. 25619–25628, Oct. 2016.

[420] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nat. Commun.*, vol. 8, no. 1, Apr. 2017, Art. no. 15043.

[421] H. Zhou, B.-Y. Tang, S.-C. Li, W.-R. Yu, H. Chen, H.-C. Yu, and B. Liu, "Appending information reconciliation for quantum key distribution," *Phys. Rev. Appl*, vol. 18, no. 4, Oct. 2022, Art. no. 044022.

[422] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, 2000.

[423] M. Koashi, "Unconditional security of quantum key distribution and the uncertainty principle," in *J. Phys., Conf. Ser*, vol. 36, no. 1, pp. 98–102, Apr. 2006.

[424] R. Renner, "Security of quantum key distribution," *Int. J. Quantum Inf.*, vol. 6, no. 01, pp. 1–127, Feb. 2008.

[425] M. Koashi, "Simple security proof of quantum key distribution based on complementarity," *New J. Phys.*, vol. 11, no. 4, Apr. 2009, Art. no. 045018.