IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 5, 2020, accepted June 28, 2020, date of publication June 30, 2020, date of current version July 15, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3006136

Single-Photon-Memory Two-Step Quantum Secure Direct Communication Relying on Einstein-Podolsky-Rosen Pairs

DONG PAN[1,2,3], KEREN LI[4], DONG RUAN[1,2,5], SOON XIN NG[3], (Senior Member, IEEE), AND LAJOS HANZO[3], (Fellow, IEEE)

[1]State Key Laboratory of Low-Dimensional Quantum Physics, Tsinghua University, Beijing 100084, China
[2]Department of Physics, Tsinghua University, Beijing 100084, China
[3]School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K.
[4]Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen 518055, China
[5]Frontier Science Center for Quantum Information, Tsinghua University, Beijing 100084, China

Corresponding authors: Dong Ruan (dongruan@tsinghua.edu.cn) and Lajos Hanzo (lh@ecs.soton.ac.uk)

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFA0303700, in part by the Key Research and Development Program of Guangdong Province under Grant 2018B030325002, in part by the National Natural Science Foundation of China under Grant 11974205, and in part by the Beijing Advanced Innovation Center for Future Chip (ICFC). The work of Dong Pan was supported by the China Scholarship Council (CSC) under Grant 201806210237. The work of Lajos Hanzo was supported in part by the Engineering and Physical Sciences Research Council, COALESCE, under Project EP/N004558/1, Project EP/P034284/1, Project EP/P034284/1, and Project EP/P003990/1, in part by the Royal Society's Global Challenges Research Fund Grant, and in part by the European Research Council's Advanced Fellow Grant QuantCom.

ABSTRACT Quantum secure direct communication (QSDC) is an important branch of quantum communication that is capable of directly transmitting secret messages over a quantum channel. It may be viewed as a concrete realization of Wyner's wiretap channel theory, which ensures the reliable and secure communication of information in the presence of noise and eavesdropping. Hence it is a fully-fledged quantum-communications protocol, which does not require a separate secret key negotiation phase. By contrast, its quantum key distribution (QKD) counterpart represents a secret key-negotiation protocol, which has to be followed up by a separate classical communication session. The essential difference between these two modes of quantum communication lies in the employment of a block-based data transmission technique, proposed by Long and Liu in 2000. However, the original block-based data transmission requires quantum memory, which is not widely available at the time of writing. Recently, this difficulty has been overcome by using classical coding theory, which has been successfully applied to the single-qubit DL04 QSDC. Here we will present a single-photon-memory QSDC protocol based on entangled pairs of photons. We commence by comparing QSDC to QKD, followed by an example of the single-photon QSDC and single-photon QKD protocol. Then we continue by modifying the so-called two-step QSDC protocol designed for deterministic QKD by reducing the number of qubits in a block into a single one, in which Alice prepares Einstein-Podolsky-Rosen (EPR) photon pairs and partitions them into two parts: the so-called pioneer qubit and the follow-up qubit. The pioneer photon is transferred first to Bob, while the follow-up photon is used either for performing encoding or for eavesdropping detection. Bob extracts the candidate key by combining the two particles of the EPR pair to perform Bell-basis measurement. Then the protocol is transformed into a single-photon-memory QSDC using coding theory. Our theoretical analysis shows that the resultant protocol is robust to individual attacks. Additionally, a high communication efficiency is achieved.

INDEX TERMS Quantum secure direct communication, quantum key distribution, entanglement.

I. INTRODUCTION

The security of information has always been of high significance to humankind. An important subfield of secure communications is classical cryptography, which exploits the high computational complexity of certain mathematical operations, such as factorizing a large product of prime numbers. However, classical cryptosystems are facing an imminent threat with the accelerating development of quantum computers [1], [2] and powerful quantum algorithms [3]–[7], which

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Huang.

exhibit powerful computing capabilities [8], [9]. Quantum cryptography is a way of dealing with this threat.

Quantum key distribution (QKD), proposed by Bennett and Brassard in 1984 (BB84) [10], is the earliest form of quantum communication. They pointed out that the core idea in the design of QKD protocols is to use non-orthogonal quantum states to support key agreement, since quantum principles such as the collapse of measurement and the no-cloning theorem [11]–[14] guarantee its security. Since then, QKD has become one of the hottest frontiers and a large number of theoretical QKD solutions have been proposed. These protocols can be divided into discrete variable QKD (DV-QKD) [15] and continuous variable QKD (CV-QKD) [16]. The DV-QKD technique encodes the information onto the discrete degrees of freedom of a photon, such as polarization of single photons and it is suitable for long-distance communication, as represented by the BB84 [10], Ekert91 [17] and BBM92 protocols [18]. By contrast, CV-QKD [19]–[23] relies on the quadrature components of the optical field that constitute an infinite-dimensional Hilbert space. More specifically, the quadrature components of either coherent states, squeezed states, or ''non-classical'' light beams [24] are modulated by the secret key bits and then measured by high-efficiency homodyne (or heterodyne) detectors, which are compatible with off-the-shelf telecommunication technologies [23]. Hence, the latter offers a low-cost and high-secret-key-rate advantage over DV-QKD for transmission over short distances. From the first QKD experiment disseminated in [25] to the realization of an entire network [26]–[28] and to the establishment of a satellite-based quantum link [29], experimental QKD research has made a series of breakthroughs [30]–[33], which have laid down the foundations for its practical application.

Meanwhile, new research branches of quantum communications have sprung up, such as quantum teleportation [34], quantum secret sharing [35], and quantum secure direct communication (QSDC) [36]. In 2000, Long and Liu [36] put forward the first QSDC protocol, which encodes information in the EPR pair quantum states, where - in contrast to QKD solutions - secret information can be transmitted directly through a quantum channel at a high level of security. Deng *et al*. [37] invented a two-step QSDC scheme, which encodes the message in the dense coding operation. Deng and Long [38] designed a QSDC protocol in 2004 (DL04 protocol) by using a single photon for conveying information. Additionally, QSDC has also been used as a constituent protocol for constructing other quantum communication protocols, which required a high degree of security for transmission, such as quantum bidding [39], quantum dialogue [40], and so on. It is worth mentioning that due to historical reasons, the meaning of quantum key distribution is different from the key distribution process of classical cryptography. Explicitly, in the latter key distribution means the secure transmission of a pre-determined key, whereas what quantum key distribution actually accomplishes is the negotiation of a key. By contrast, QSDC succeeds in completing the task of key distribution.

With the rapid development of QSDC in terms of its theoretical characterization [41]–[46], some QSDC protocols were demonstrated in the laboratory. Notably, Hu *et al*. [47] achieved QSDC in a noisy environment based on the DL04 protocol [38] with the aid of single-photon frequency coding, demonstrating the feasibility of QSDC in the presence of loss. The efficient QSDC [36] and two-step QSDC protocol of [37] were realized using a cutting-edge atomic quantum memory, which is essential for the block transmission [48]. A transmission distance as high as 0.5 km was achieved in the entanglement-based QSDC experiment of [49]. The experimental development of QSDC is accelerating at the time of writing motivated by the ambitious objective of realizing perfectly secure communication in a metropolitan area [50], [51]. One of the last impediments hampering this process is the requirement of quantum memory. Recently, a coding technique was proposed for replacing the quantum memory [50], and this has led to the design of quantum-memory-free (QMF) QSDC protocols, hence circumventing one of the last impediments in the way of practical QSDC. We summarize the major mile-stones in the theoretical and experimental contributions to the development of QSDC in Table. 1.

Against this background, our new contribution is the conception of single-photon-memory (SPM) QSDC based on the intrinsic amalgam of the seminal QSDC protocol of [36] and of the two-step QSDC protocol of [37]. We commence with a critical appraisal of the differences between the classical cryptosystem, QKD and QSDC in Section II. We will demonstrate that the process of quantum communication relying on QSDC is more appealing than QKD-based communication system, since no key distribution, no encryption, and no decryption are necessitated. We review the operational steps of BB84 QKD protocol and DL04 QSDC protocol in Section III and Section IV, respectively. Our new protocol is conceived in Section V. The security-level of the quantum channel is quantified by randomly choosing the EPR pairs for eavesdropping detection. In Section VI, we show that any individual attack will affect the resultant error rate and hence may be readily detected. Finally, we conclude in Section VII.

II. COMPARISON OF CLASSICAL AND QUANTUM CRYPTOGRAPHY

In this section, we briefly introduce the basic characteristics of classical, QKD-based and QSDC systems, with special emphasis on their communication modality. Suffice to say at this early stage that the BB84 QKD protocol represents a secret key negotiation procedure, while QSDC constitutes a true communication technique, which dispenses with the separate key negotiation processes of QKD and of classical cryptography.

The block diagram of a classical cryptosystem is shown in Fig. 1 (a). The legitimate transmitter Alice generates the so-called plaintext and wants to send it to the authorized receiver Bob. To avoid the disclosure of the message, the plaintext is transformed into the so-called ciphertext with the aid of a secret key and an encryption algorithm. Then

TABLE 1. Timeline of important milestones in QSDC's theoretical and experimental contributions.

Theoretical proposals		Experimental demonstrations
Long *et al*. [36] proposed a high-capacity QSDC protocol.	2000	
Deng *et al*. [37] proposed a two-step QSDC protocol.	2003	
Deng *et al*. [38] created a QSDC protocol using single photons (DL04). Yan and Zhang [52] proposed a QSDC protocol using teleportation.	2004	
Wang *et al*. [53] conceived a high-dimensional two-step QSDC protocol.	2005	
Murakami *et al*. [54] proposed a QSDC scheme based on singe-qubit.	2007	
Lin *et al*. [55] designed a QSDC protocol using χ-state.	2008	
Shi *et al*. [56] proposed a QSDC scheme based on three-dimensional hyperentanglement.	2011	
Yoon *et al*. [57] used QSDC to design quantum signature.	2014	
Naseri *et al*. [58] proposed a N-users QSDC network. Cao *et al*. [59] provided a quantum secure direct communication scheme in the non-symmetric channel.	2015	
Zawadzki [60] studied the attack strategies in QSDC. Zarmehi and Houshmand [61] constructed a bidirectional QSDC network.	2016	Hu *et al*. [47] created a DL04 QSDC testbed relying on single-photon frequency coding. Lum *et al*. [62] used quantum data locking for high speed QSDC.
	2017	Zhang *et al*. [48] realized a two-step QSDC protocol with the aid of quantum memory. Zhang *et al*. [49] achieved long-distance transmission using this two-step QSDC protocol.
Zhou *et al*. [63] designed a measurement-device-independent DL04 QSDC protocol. Niu *et al*. designed a measurement-device-independent two-step QSDC protocol. Huang *et al*. [64] studies implementation vulnerabilities of QSDC.	2018	Sun *et al*. [50] reported the quantum-memory-free DL04 QSDC protocol.
Zhou *et al*. [65] proposed a device-independent two-step QSDC protocol.	2019	Qi *et al*. [51] constructed a practical QSDC system for intra-city applications. Shapiro *et al*. [66] used quantum low probability of intercept for high-rate QSDC. Massa *et al*. [67] realized a bi-directional QSDC.
	2020	Pan *et al*. [68] reported an experimental free-space QSDC.

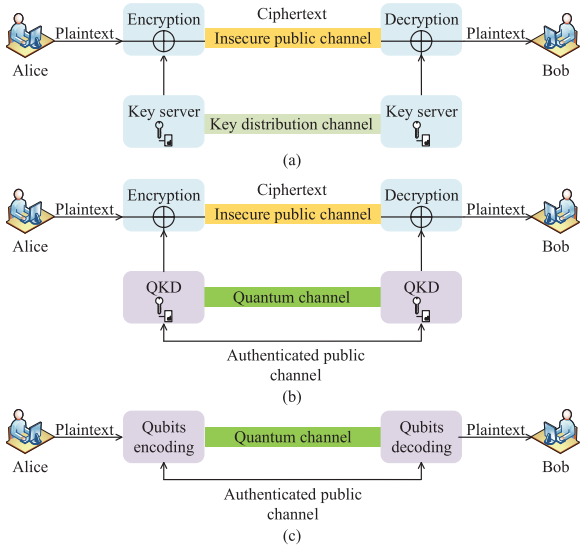

FIGURE 1. Block diagram of (a) classical cryptosystem, (b) QKD-based system and (c) QSDC system.

the ciphertext is transmitted from Alice to Bob over the insecure public channel. Upon the receipt of Alice's ciphertext, Bob translates it back into the original plaintext using the secret key and his decryption algorithm. Therefore, the key must be shared between Alice and Bob over a secure channel, as indicated in Fig. 1 (a).

However, the ciphertext transferred over the insecure public channel permits an eavesdropper Eve to intercept it and to apply a so-called ciphertext-only attack [69]. Hence using a so-called ''one-time pad'' is crucial for this system in which the plaintext is paired with a random secret key, which has at least the same length as the message [70]. Because only the one-time pad scheme has been proven to be perfectly secure [71]. Naturally, if Eve obtains the secret key, the classical cryptosystem will collapse, therefore the security of the key in both transmission and storage must be ensured. One of the inherent weaknesses of classical cryptography is its inability to detect eavesdropping. As a matter of fact, classical cryptography was designed in a way that all the ciphertext can be safely given to Eve, because she would not be able to decipher it. Hence it does not care whether the ciphertext is wiretapped or not.

By contrast, in the QKD-based communication system of Fig. 1 (b), a pair of QKD users Alice and Bob are connected both by a quantum channel and an authenticated public channel as well as an insecure public channel. A common secret key can be established over the insecure quantum channel (any qubits sent over the quantum channel can be intercepted and modified by Eve), with the aid of an additional authenticated public channel for the processes of quantum basis comparison, eavesdropping detection and error correction. This common secret key is used for one-time pad encryption, in which the procedure of encryption, ciphertext transmission, and decryption carry out the same functions to those in classical cryptosystems after key distribution. In other words, no secret message is transmitted through the quantum channel. Again, the QKD-based communication system of Fig. 1 (b) also uses an insecure public channel for transmitting the ciphertext after the key has been generated by QKD. Hence it exhibits a certain philosophical similarity with the existing classical optical communication systems. Therefore, QKD can detect eavesdropping at the key agreement whilst the ciphertext can still be intercepted without any trace.

The security of QKD is based on the no-cloning theorem and other quantum principles implying in practical terms that Eve's eavesdropping action will increase the quantum bit error rate and thus it will be discovered. For the QKD protocol of [72]–[75], the candidate keys are deterministic, which means that the users can transmit whatever deterministic candidate key they want. But the transmitted data is discarded, when tempered with by the eavesdropper. A candidate key is a random bit string that carries no information. Deterministic QKD (DQKD) cannot transmit secret information directly because it can only detect eavesdropping, but cannot prevent eavesdroppers from obtaining the transmitted data.

Finally, the procedure of QSDC is shown in Fig. 1 (c), in which the secret information is directly transmitted between Alice and Bob through an insecure quantum channel [76]. This is achieved without any key generation as well as without any encryption and decryption algorithm. The confidential information can be read directly by the legitimate user, when the information receiver receives the quantum states, and no additional classical information is needed for decoding. The authenticated public channel of Fig. 1 (c) is only used for eavesdropping detection so that legitimate users can detect the presence of an eavesdropper. The quantum states are transmitted on a block-by-block basis and the pair of legitimate users can check the confidentiality by random sampling and comparing some of the photons. In all existing secure communications, the distribution of the secret key and the communication process has been separated, as shown in Fig. 1 (a) and Fig. 1 (b). This has now been changed by QSDC. QSDC has three appealing characteristics: (1) no secret key is required, hence no need to allocate resources for key management; (2) no leakage of information occurs, even if an eavesdropper may tap into the quantum channel; (3) it does not rely on data encryption and decryption.

QSDC [36]–[38], [51] has made three profound contributions to communication and cryptography:

- Firstly, it has advanced field of classical communications from the reliable transmission of information over a noisy channel - which is guaranteed by Shannon's classical information theory [77] - to the higher plane of both reliable and secure communication over a noisy channel, even in the face of eavesdropping.
- Secondly, it may also be viewed as an explicit realization of Wyner's wiretap theory [78], hence guaranteeing both secure and reliable communication with the aid of QSDC.
- Thirdly, QSDC has advanced quantum communication from eavesdropping detection as known in QKD to joint eavesdropper detection and prevention.

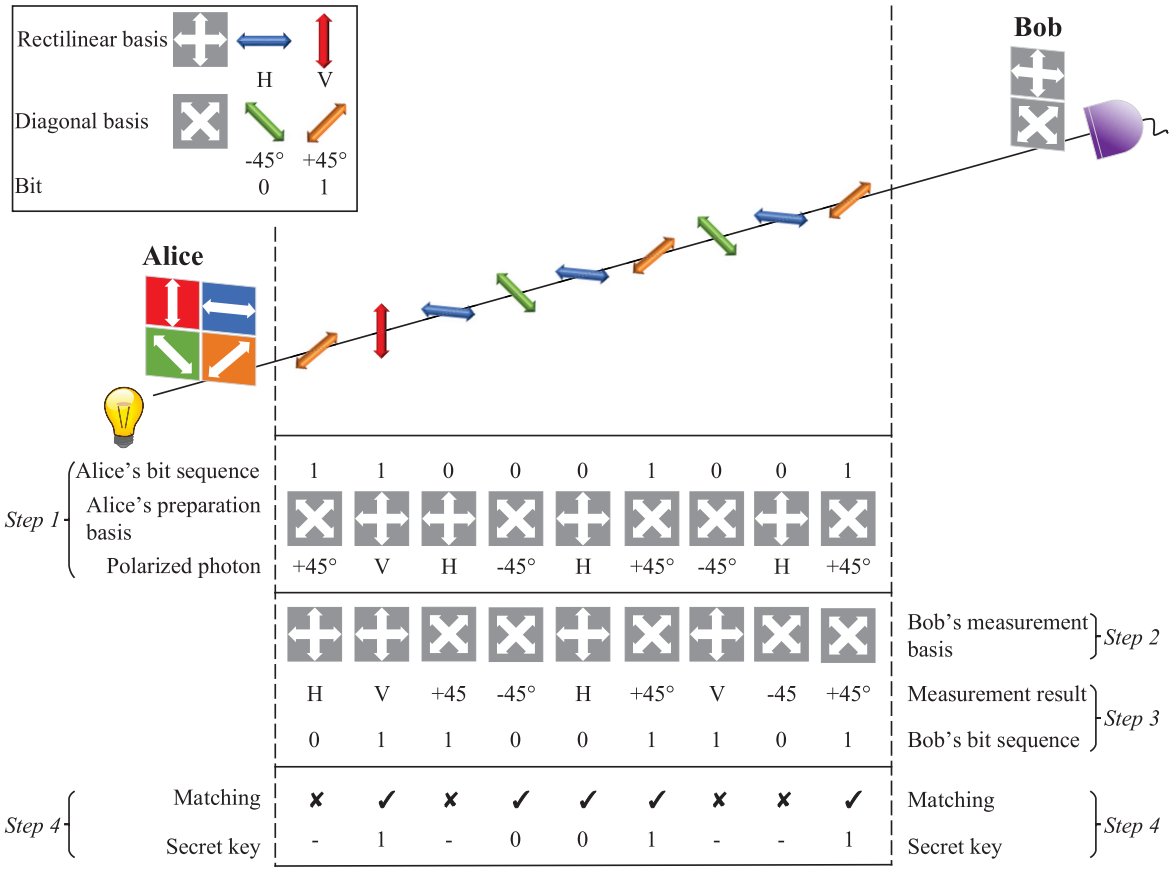

FIGURE 2. Principle of BB84 QKD protocol.

As discussed above, QSDC can directly send secret information through a quantum channel without setting up a key. Furthermore, it is capable of detecting eavesdropping and preventing information disclosure. In a nutshell, QKD-based communication systems [79]–[82] and QSDC [36]–[38] constitute perfectly secure alternative communication modalities for future classical-quantum hybrid communication networks [83].

Indeed, the QSDC philosophy is attractive, but it requires that the users have the capability of storing quantum states, which had been a challenge. Recently, this challenge has been solved with the aid of an innovative coding technique [50], where the information is encoded using a one-time-pad key and transmitted deterministically over the quantum channel. Then a new key is distilled from the transmitted ciphertext by correcting the bit errors of the ciphertext transmission. In this way, QSDC can be carried out without quantum memory, using the existing technology. The security of QSDC relies on exploiting the quantum principles, such as the no-cloning theorem, the uncertainty principle, correlation of entangled particles and nonlocality.

In the next two sections, we will review the operational steps of the BB84 QKD protocol [10] and DL04 QSDC protocol [38] for comparing these two popular quantum communication protocols. More explicitly, we will show how a secret key is distributed between two users in the BB84 protocol [10] and how secret messages can be transmitted directly over a quantum channel based on the DL04 protocol [38].

III. QUANTUM KEY DISTRIBUTION

As shown in Fig. 2, a pair of legitimate users, namely Alice (transmitter) and Bob (receiver) relying on the BB84 QKD protocol [10] agree that their photons will be polarized using conjugate bases, either a rectilinear basis $\oplus$ or a diagonal basis $\otimes$, and their correspondingly polarized photons $H/-45°$ and $V/+45°$ are used for signalling the information bit "0" and "1", respectively. The operational steps of the BB84 QKD protocol can be described as follows.

Step 1: Alice randomly chooses either the basis $\oplus$ or $\otimes$ for preparing polarized photons and then transmits them to Bob over an insecure quantum channel. Fig. 2 shows an example of Alice's bit sequence and the correspondingly polarized photons.

Step 2: Bob randomly exploits either the basis $\oplus$ or $\otimes$ to measure the received polarized photons.

Step 3: Only some of the polarized photons can be detected by Bob using his measurements due to the intrinsic loss of photons during their passage through the quantum channel and owing to the imperfections of the optical components. Bob then transmits the position of successful detection events

back to Alice over the classical authenticated channel of Fig. 1 (b) and then Alice stores the corresponding data. This process could be realized as follows, assuming that there is bit-based time synchronization between Alice and Bob for every transmitted qubit in the experimental implementation. If nothing is detected by Bob in a specific time window that corresponds to the photon emitted from Alice, we regard it as an unsuccessful detection event, which means that the photon has been emitted by Alice but not be received by Bob due to optical loss. Note that the example of Fig. 2 has omitted the photons which have been obliterated by optical loss.

Step 4: Alice and Bob compare their preparation and measurement basis, respectively. Explicitly, if Bob's measurement basis is the same as Alice's preparation basis used in *Step 1*, he will detect all the transmitted polarized photons correctly. Again, they store the qubits conveyed under the same preparation and measurement basis, which are ticked in the specific line indicating Matching in Fig. 2. The benefit of this particular procedure is that only the specific index of the identical bases is transmitted over the authenticated public channel of Fig. 1 (b), but the actual quantum state is not divulged to Eve. For example, only Alice and Bob know whether the quantum state is H (bit 0) or V (bit 1). Although Eve knows that both Alice and Bob use the same basis $\bigoplus$ by monitoring the authenticated public channel, yet Eve cannot infer the transmitted bit. It does not make sense for Eve to carry out a full search to find out the secret key, since there are 2^N possible results for a secret key of a length N. This process is formally called sifting [15]. By contrast, if Alice and Bob know that the measurement basis disagrees with the preparation basis by publicly discussing over the authenticated classical channel, they will discard the corresponding of transmitted photons, since the received polarized photon will be randomly changed to one of the legitimate polarization states of the measurement basis. To be more specific, if for example an H or V polarized photon is expected according to Alice's preparation basis, but $+45^\circ$ or -45° is obtained by Bob, then the measurement basis is claimed to be different from the preparation basis, which is indicated by the cross in the third position from the left in the last-but-one line of Fig. 2.

Step 5: Then a sufficiently high number of bits, which are randomly selected from the sifted data of *Step 3* are compared for statistically estimating the quantum bit error rate (QBER). Note that this process has to publicly compare the specific quantum states (secret bits) of Alice and Bob to be sure that these states were not perturbed by eavesdropping. Since Alice and Bob have publicly announced them, they cannot be the final secret key. If the QBER is below a pre-determined threshold, Alice and Bob proceed to the next step by assuming that no eavesdropper has tampered with their information. Otherwise, they abort this QKD transmission and return to *Step 1* owing to the risk of tampering. More explicitly, an eavesdropper can be readily detected during this step, because her eavesdropping action will perturb the transmitted qubit, as indicated by the postulates of quantum mechanics [16], [80]. Hence the qubits prepared and detected within the same basis by Alice and Bob will be different.

Step 6: In case of mild impairments, Alice and Bob may be able to correct the errors inflicted by the channel/device imperfections using error correction. In order to ensure that Eve has only negligible information about the final secret key, the so-called privacy amplification process [15], [84], [85] is invoked. To elaborate a little further, Alice randomly chooses a hash function from the universal hash function family of [86] and forwards the description of the selected hash function to Bob over the authenticated public channel. Then, Alice and Bob can use this hash function for mapping the reconciled secret key strings to a final secret key. However, this step has not been presented in the example of Fig. 2.

Therefore, by exploiting the quantum-physical properties of the photons, *eavesdropping can indeed be detected in QKD. However, QKD fails to prevent eavesdropping*. Therefore, to mitigate the risk, QKD always transmits a potential candidate key string which is initially meaningless before it is elevated to the status of a raw key later. If eavesdropping is detected, QKD discards the candidate key and the entire process is resumed from the beginning, which leads to its relatively low key rate. If however no eavesdropping is detected, the candidate key is elevated to the raw key.

IV. QUANTUM SECURE DIRECT COMMUNICATION

The first QSDC protocol is based on EPR pairs with the block data transmission technique in 2000 [36]. The information is encoded in the quantum states and transmitted in two steps. In 2003, a two-step QSDC protocol [37] was proposed where information is encoded using the dense coding operations. The first sing-photon based QSDC protocol [38] was proposed in 2004, to compare the QKD and QSDC, we concentrate on the DL04 QSDC protocol, which is based on single photons, like BB84 QKD [10]. The DL04 QSDC protocol is shown in Fig. 1 (c), which is a solution conceived for directly transmitting secret messages with the aid of a single-photon block [38]. The QSDC procedure is illustrated in Fig. 3. We would like to mention that ''Alice'' and ''Bob'' represent the qubit transmitter and qubit receiver, respectively, in line with the role definition of the BB84 QKD protocol. However, the DL04 QSDC protocol is still quite different, since some qubits traverse the quantum channel twice. Although Bob represents the legitimate information receiver, he also transmits his own prepared qubits to Alice (the legitimate information transmitter). Recall that in the BB84 QKD-based system the legitimate receiver Bob also acted as a transmitter by sending back the index of the successfully detected qubits to Alice, but instead of the quantum channel, over the authenticated classical channel of Fig. 1 (b). The DL04 QSDC protocol can be described as follows.

Step 1: Bob (information receiver) randomly chooses either the basis $\bigoplus$ or $\bigotimes$ for preparing a sequence of polarized photons. Each photon is randomly in one of the four legitimate polarizations $\{H, V, +45^\circ, -45^\circ\}$. Then, this photon sequence will be transmitted from Bob (information

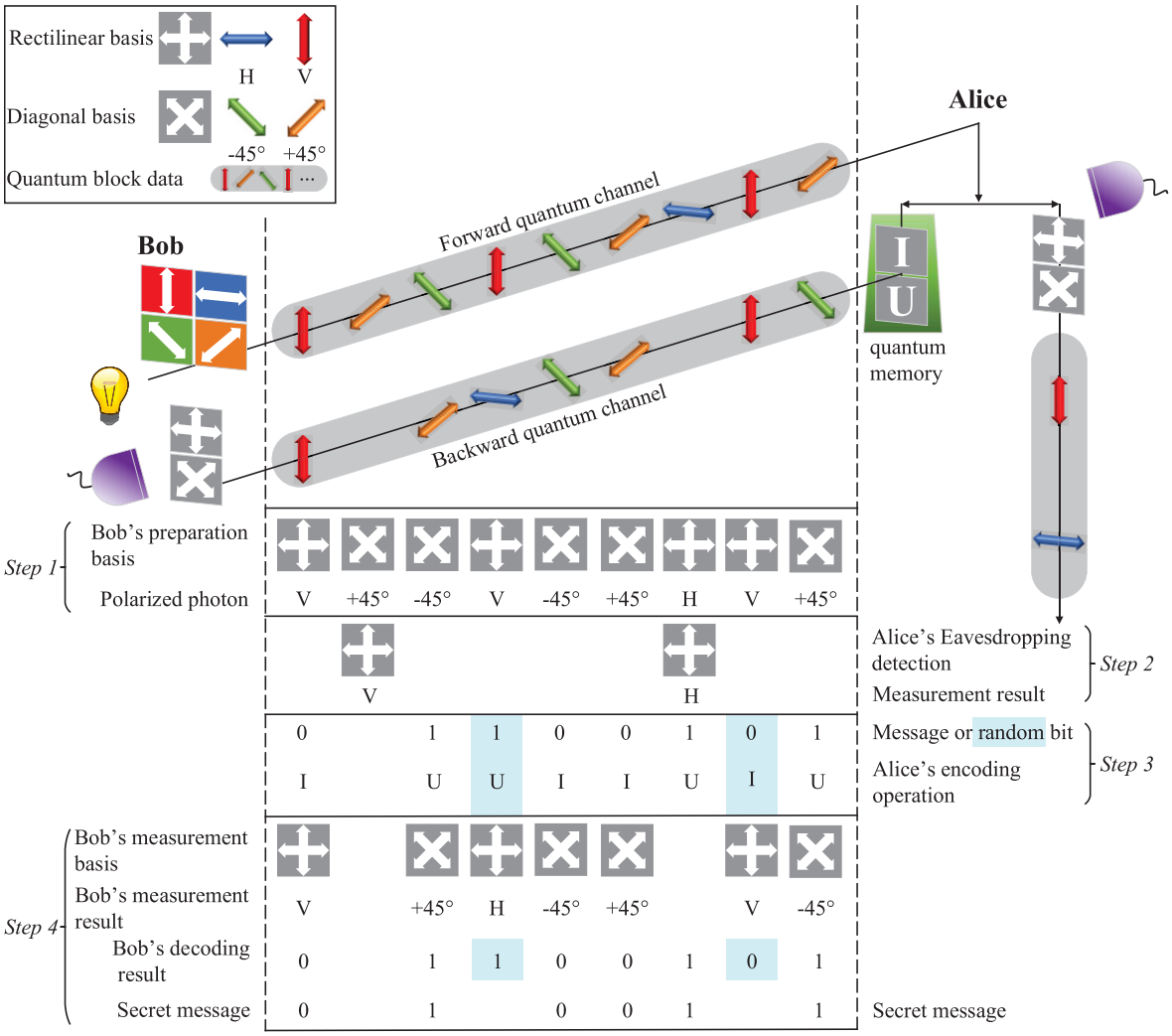

FIGURE 3. Principle of DL04 QSDC protocol.

receiver) to Alice (information transmitter) using a process called block transmission [36] over the quantum channel of Fig 1 (c). This block has been marked by a gray cylinder in Fig. 3, which was not part of the QKD procedure of Fig. 2.

Step 2: After receiving this block, Alice (information transmitter) randomly selects a sufficiently large set of the received photons and measures them. Indeed, Alice (information transmitter) would get Bob's (information receiver) legitimate polarized photons, provided that no eavesdropping perturbs their quantum states and if she has used the same basis to measure the photons as Bob's preparation basis. To ascertain whether an eavesdropper has tempered with the photons during their flight over the quantum channel, the QBER is estimated by comparing the qubits via the authenticated classical channel seen in Fig. 1 (c). For example, in the second position of Fig. 3 Alice and Bob have different bases, but in the 7th position they coincide, where a "1" is detected. If the comparison confirms that the transmission is secure, i.e. free from eavesdropping by Eve, they proceed to the next step. This eavesdropping detection of the forward quantum channel of Fig. 3 is identical to *Step 1*, *Step 2*, and *Step 5* of the BB84 QKD protocol of Fig. 2, thus QSDC has the same level of security as the BB84 QKD during its forward transmission from Bob to Alice.

Step 3: Then Alice (information transmitter) applies a pair of unitary operations I and $U = i\sigma_y$ to the remaining photons, for example, photons 1, 3, 4, 5, 6, 8 and 9 in Fig. 3 - namely to those that were not chosen for performing eavesdropping detection - in order to convey the secret information bit "0" and "1", respectively. More explicitly, the unitary operation I keeps the photons unchanged, while U flips the photon state that belongs to the same basis, which is formulated as:

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

and

$$U|+\rangle = |-\rangle, \quad U|-\rangle = -|+\rangle, \tag{2}$$

where the states $|0\rangle$, $|1\rangle$, $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$, and $|-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$ represent the polarized photons H, V, $+45°$, and $-45°$, respectively. This action may be observed by comparing the 2nd and 8th rows of Fig. 3 in their photon-positions 1, 3, 4, 5, 6, 8 and 9. This operation enables Bob (information receiver) to deterministically decode the secret message bits, since he has the knowledge of the initial states' preparation basis seen in these photon-positions of Fig. 3 in row 1. Additionally, Alice (information transmitter) randomly chooses some photons as test photons for conveying random bits so as to guarantee the security of her second transmission, which are represented by the shaded boxes of Fig. 3. Both types of photons, namely those carrying genuine secret messages and those conveying the random test bits are transmitted to Bob. More explicitly, the photon sequence returned from Alice to Bob is a mixture of random test photons and message carriers, hence Eve does not know, which photon represents the desired secret message and which conveys only a random bit.

Step 4: Finally, Bob (information receiver) measures the returned photons using the same basis he used for preparing them. In this case, he can deterministically decode the encoded bits without requiring a classical channel. Then Alice (information transmitter) and Bob (information receiver) publicly compare the decoded test photons in positions 4 and 8 of line 8 in Fig. 3 for determining whether Eve has or has not intercepted the photons during their transmission from Alice to Bob.

V. A SINGLE-PHOTON-MEMORY QSDC PROTOCOL BASED ON EPR PAIRS

Against the above background, in this section, we present first a new QSDC scheme requiring no block transmission and mitigating the requirement of quantum memory, as inspired by the seminal QSDC protocol of [36] and by the two-step QSDC protocol of [37]. This new SPM QSDC protocol is evolved from the two-step DQKD protocol by reducing the number of particles in a block to just 1 in the two-step QSDC protocol of [37] and by appropriately adaption the coding-technique proposed in [50]. Historically speaking, the two-step DQKD protocol is a simplified version of the two-step QSDC of [37]. Here only two EPR states $|\psi^-\rangle$ and $|\psi^+\rangle$ are used. The reason for using these two Bell-basis states is that they can be measured with the aid of linear optics [87], [88], which is more easily implemented than a complete four-Bell-state measurement, since the latter requires nonlinear optics [89]. The procedure of two-step DQKD is depicted in Fig. 4, and the detailed steps are as follows.

An EPR pair represents one of the four Bell states [37], [90]

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle),$$
$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle),$$

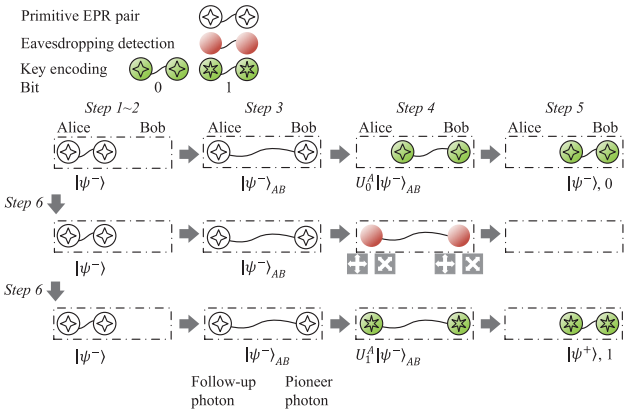

FIGURE 4. Illustration of the DQKD protocol. The subscript *AB* of an entangled state $|\psi^-\rangle_{AB}$ represents that this state is shared by Alice and Bob, i.e., they respectively hold one of the particles of an entangled state. If there is no subscript, this means that either Alice or Bob holds the entangled state in its entirety. Furthermore, the superscript *A* in a quantum operation indicates that the operation is performed by Alice.

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle),$$
$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle). \quad (3)$$

Step 1: Alice and Bob agree prior to their actual communication that each of the two Bell-basis states can carry one bit of classical information and they map 0 and 1 onto $|\psi^-\rangle$ and $|\psi^+\rangle$, respectively, as seen at the top left corner of Fig. 4.

Step 2: Alice prepares an EPR pair in the Bell state $|\psi^-\rangle$, as seen in Fig. 4.

Step 3: Alice sends one of the photons in the EPR-pair to Bob, which we refer to as the *pioneer photon.*

Step 4: After waiting for a transmission time of t, which is the time it takes for the photon to reach Bob, Alice applies either an eavesdropping detection measurement or an encoding operation to the *follow-up photon*, and then sends either a classical message through the authenticated classical channel or the follow-up photon to Bob. At the time t, Bob receives the pioneer photon and keeps it at hand. The encoding operations are

$$U_0^A = I = |0\rangle\langle 0| + |1\rangle\langle 1| \quad (4)$$

and

$$U_1^A = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \quad (5)$$

respectively, which transforms the state $|\psi^-\rangle$ into $|\psi^-\rangle$ and $|\psi^+\rangle$, and represent bit "0" and "1", respectively. Some of these encoded bits are used as test bits to estimate the bit error rate of the follow-up photon transmission. The capacity of this protocol can be further increased by using four unitary operations as in [37], [91].

Step 5: At time $2t$, either the classical bit or the follow-up qubit reaches Bob. If the classical bit is received, Bob measures his pioneer photon using either $\{|0\rangle, |1\rangle\}$ basis or $\{|+\rangle, |-\rangle\}$ basis, and announces his measurement basis

as well as the measurement result through the authenticated public channel. If Bob receives the follow-up photon, he combines it with the pioneer photon to perform Bell-basis measurement.

Step 6: After sufficient EPR pairs have been transmitted, Alice and Bob can estimate the QBER of the received pioneer photons by comparing the eavesdropping detection measurements at the photon-positions, where they chose the same basis. Then they continue by estimating the QBER of the follow-up photons by comparing some of the EPR pairs to the encoded test bits. If the error rates are below a certain acceptable threshold, Bob and Alice may conclude that there are no eavesdroppers, and they continue the steps from *Step 2* to *Step 6* until sufficient candidate keys have been generated. Then they go to *Step 7*. Otherwise, Alice and Bob must discard the key that they have communicated and terminate the process.

Step 7: Finally, Alice and Bob acquire the final key by utilizing error correction and privacy amplification.

At this stage, it is worth mentioning that in BB84 QKD Alice and Bob cannot decide in advance what the candidate key-encoding sequence would be and thus it is referred to as probabilistic QKD (PQKD), since they randomly choose the basis used for measuring the transmitted qubits. A specific disadvantage of this is that a lot of qubits must be discarded during the information reconciliation, thus resulting in a low key bit transmission efficiency (discussed later), as exemplified in Fig. 2. By contrast, the deterministic QKD (DQKD) of Fig. 4 has the benefit that Alice can distribute her pre-determined candidate key sequence, hence no qubits have to be discarded [72], [74] so that having a higher key bit transmission efficiency.

In a nutshell, we have accomplished the distribution of candidate key after the transmission of each EPR pairs. Let us now briefly elaborate on the important quantity of the waiting time t in *Step 4*, which critically depends on the distance between Alice and Bob. It must be long enough for transmitting a photon to Bob. Assuming that their distance is L, the waiting time must satisfy $t > L/c$, in order to leave sufficient time for the pioneer photon to reach Bob. So that Eve could not get the two photons of an EPR without violating the relativity. The reason we call this protocol as two-step DQKD protocol is that the particles pioneer photon and follow-up photon in EPR pairs are transmitted from Alice to Bob in two steps *Step 3* and *Step 4*, rather than there are only two operational steps in this protocol.

Let us now deal with another salient benefit of the proposed protocol, namely its ability to mitigate the need for quantum memory. To elaborate a little further, the entanglement-based QSDC schemes of [36], [37] rely on the block-based transmission of photons and are capable of detecting eavesdropping with the aid of random sampling tests. Unfortunately, however, N-photon quantum memory with long decoherence time is needed for storing a batch of quantum states in pure block-based transmission. In the light of this, it is a substantial benefit of the proposed DQKD protocol that it lends itself to convenient implementation as a benefit of dispensing with block-based transmission, albeit this is achieved at the cost of transmitting a deterministic key, instead of genuine secret messages.

Note that a single-photon storage is required in *Step 3* (*Step 5*) for the follow-up (pioneer photon) photon when the pioneer photon (follow-up) is transmitted over the quantum channel. This scenario is similar to entanglement-based QKD protocols, such as the Ekert91 [17], the BBM92 [18] and the ping-pong protocol [72]. The storage of a single-photon in the EPR pair can be realized by a low-cost optical fiber delay line [92] instead of a genuine N-photon quantum memory [93], which has a long decoherence time. By contrast, genuine quantum memory is necessary for the original two-step QSDC protocol due to the block-based transmission of quantum states [37], [48].

The DQKD protocol can be transformed into a QMF QSDC protocol by using the quantum-memory-free technique proposed in [50], which has successfully transformed the DL04 QSDC protocol [38] into the QMF DL04 QSDC protocol of [94]. Here we briefly describe the idea of QMF. Let us commence by recalling that in the original DL04 QSDC protocol of [38] the message block is only encoded after it has been ascertained that the block of information was not tampered with. Similarly, in the two-step QSDC protocol of [37] the message block is only encoded after it has been confirmed that the pioneer block of photons has not been tampered with. Thus, QSDC is capable of not only eavesdropping detection, but also of eavesdropping prevention. However, to ensure the security of the pioneer sequence or the block of information carriers before their encoding, quantum memory is required for storing them until the discussions of their security check are completed. Otherwise, Eve could steal the information. Although this could indeed be detected, but only retrospectively.

The QMF concept hinges on letting Alice encrypt the message using a one-time-pad and then mapping the ciphertext onto the photons in a block, *which are sent to Bob one by one.* Bob receives the encoded photons and decodes the ciphertext as well as assesses the degree of eavesdropping tampering with the transmitted ciphertext by estimating the QBER of the transmission. Then Bob calculates the secrecy capacity [51]. Given this, Alice and Bob can distill a new secret key from the ciphertext, and these keys will be used for protecting the ensuing transmission of information. To start with, Alice and Bob can pre-share a common one-time-pad key, or they can run the protocol as a DQKD procedure to produce some initial keys. Again, we note that this genuine quantum communications protocol is totally different from a QKD-based system, because instead of simply negotiating/distributing a key it carries out simultaneous key agreement and ciphertext transmission. As a further benefit, no classical ciphertext transmission is performed.

Given the QMF concept, the DQKD protocols can now be transformed into QMF QSDC [50]. However, the single-photon memory is required in the entanglement-based

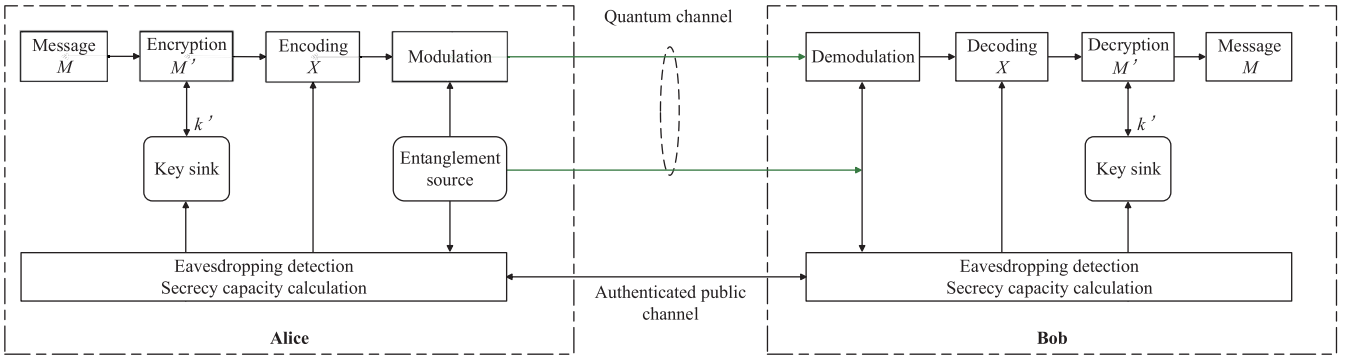

FIGURE 5. The block diagram of the proposed SPM QSDC protocol based on [50].

DQKD, which could be realized by using the fiber delay lines. Hence, the proposed entanglement-based protocol is called SPM QSDC. The operational steps of this SPM QSDC protocol are nearly identical to the two-step DQKD protocol of Fig. 4, apart from the fact that they are intrinsically amalgamated with an extra classical coding technique to conceive a compelling SPM QSDC protocol. Below we continue by discussing the details of the SPM QSDC protocol based on EPR pairs. For the sake of bold and explicit exposition, we will introduce it step by step, again emphasizing the some of the steps are identical to the two-step DQKD protocol of Fig. 4. Hence the identical steps ***Step X*** of the DQKD protocol of Fig. 4 will be copied directly from above, while the different steps will be described using ***Step Xb***. The resultant SPM QSDC protocol relies on combining Fig. 4 and Fig. 5.

Step 1: Alice and Bob agree prior to their actual communication that each of the two Bell-basis states can carry one bit of classical information and they map 0 and 1 onto $|\psi^-\rangle$ and $|\psi^+\rangle$, respectively. As seen at the top left corner of Fig. 4.

Step 2: Alice prepares an EPR pair in the Bell state $|\psi^-\rangle$, as seen in Fig. 4.

Step 3: Alice sends one of the photons in the EPR-pair to Bob, which we refer to as the *pioneer photon*, as shown in Fig. 4.

Step 4b: Both Alice and Bob rely on a quantum/to-classical (Q/C) converter for converting the optical signals to classical bits for extracting a key and then temporarily storing it in the *sink* found in the classical encoding/decoding scheme of Fig. 5. The corresponding classical electronics is part of Alice' and Bob's classical computers. The Q/C converter may be for example a single-photon detector, converting an optical signal to an electronic signal. If there are insufficient random key bits shared between Alice and Bob, Alice chooses a string M of random bits. By contrast, if there are sufficient random key bits shared between them, then Alice chooses a string of message bits and uses a string of secret key bits stored by the sink in the classical coding scheme of Fig. 5 for encrypting them utilizing a one-time-pad, generating the encrypted string M'. Hence as usual, the length of the stored key is the same as that of the secret message (plaintext) and as always, the ''one-time pad'' requires that the key would only be used once. The duration of key storage is only required to be long enough for the transmission of a single secret message. Alice then chooses a classical code C for encoding the encrypted string M', representing either a random binary string or a message string into the codewords X of Fig. 5. The classical coding rate is given by m/N_c, where m is the length of the message frame and N_c is the length of the encoded codeword.

To elaborate a little further, the above-mentioned process is based on a classical encryption or coding process, where no photons or optical signals are involved. To provide a simple example, if Alice wants to transmit the secret message string of M ''0011'' to Bob, she might opt for using a key ''1010'' to encrypt it. The string M is then encrypted using their modulo-two connection into M' ($M' = 1001 = 0011$ mod 1010). The encrypted string M' ''1001'' is then encoded for example into a codeword X ''10000011010100100'', which is finally mapped onto photons using quantum-domain operations.

After waiting for a transmission time of t, Alice modulates the follow-up photons with the codewords X, using U_0^A and U_1^A as the coding bit of 0 and 1, respectively, as seen in Fig. 5. She also inserts some test bits into the codewords and then she sends the test bit positions and the encoded follow-up photons to Bob. Furthermore, Alice randomly chooses some follow-up photons for performing eavesdropping detection using either the $\{|0\rangle, |1\rangle\}$ basis or the $\{|+\rangle, |-\rangle\}$ basis, whose position indices will be conveyed to Bob. In a nut-shell, apart from the employment of the classical coding schemes of Fig. 5 this step is also similar to *Step 4* of Fig. 4.

Step 5: At time $2t$, either the classical bit transmitted over the classical channel of Fig. 1 or the follow-up photon reaches Bob.

If the classical bit is received, Bob measures the associated pioneer photon using either the $\{|0\rangle, |1\rangle\}$ basis or the $\{|+\rangle, |-\rangle\}$ basis, and announces his measurement basis as well as the measurement result through the authenticated public channel.

By contrast, if Bob receives the follow-up photon, he combines it with the associated pioneer photon to perform Bell-basis measurement, similarly to *Step 5* of Fig. 4.

Step 6b: Bob then decodes the codewords using the classical decoding scheme of Fig. 5 representing the message Alice has encoded. They also estimate the secrecy capacity using the QBERs of both the pioneer- and follow-up photon transmissions. Finally, Alice and Bob distill a secure key k' from the ciphertext. They insert k' into their classical key sinks respectively, as shown in Fig. 5.

Step 7b: They continue to send the next frame of information by repeating all the steps commencing from *Step 2* until they complete the transmission of the entire message.

In closing we note that the details of the classical code design will be similar to those in [50] and will be further elaborated on in a follow-on paper [94]. Compared to QSDC critically relying on the availability of quantum memory, only a single classical key sequence has to be stored by the *classical sink* of Fig. 5 for the transmission of a single secret message in the proposed SPM QSDC. More explicitly, it is necessary to store a single key having the same length as the secret message in the classical sink for the transmission duration of single ciphertext message, whilst no key storage is necessitated by QSDC relying on quantum memory. The ciphertext is transmitted over the quantum channel, which is protected by the postulates of quantum physics. In the next phase a new key may be readily distilled from the very same ciphertext, because the presence or absence of eavesdropping is perpetually monitored. The resultant key is then used immediately for encoding the subsequent message. In QKD, DQKD or PQKD, the transmitted bits must be discarded if they happen to be tampered with, which leads to a potentially low effective throughput. By contrast, in SPM QSDC, the transmitted data does not have to be discarded even in the presence of eavesdropping, because the information is protected by the above-mentioned one-time pad in the ciphertext.

In conclusion, there is a trade-off between QSDC relying on quantum memory and mitigating the requirement of quantum memory. Explicitly, the former requires no key distribution, no key storage and no ciphertext. By contrast, although the proposed SPM QSDC requires both secure key agreement as well as the storage of a key for the duration of a single secret frame's transmission, it eliminates one of the last impediments in the way of practical QSDC, because it only requires a fiber delay line for single-photon storage and it minimizes the leakage of ciphertext.

VI. SECURITY LEVEL AND EFFICIENCY OF THE SPM QSDC PROTOCOL

A. IDENTIFICATION OF THE LEGITIMATE PARTIES WITH THE AID OF ENTANGLEMENTS

In many quantum communication protocols, it is assumed that the participants are honest, albeit this not so in the real world. To guarantee secure communications, mutual partner-identification is necessary. The quantum identification techniques of [95]–[97] relying on entanglements can be used in our protocol to guard against insider attacks. In these schemes, the underlying assumption is that a pair of legitimate users have previously established entangled states or that there exists a trusted authority. They can use their entangled states to complete the procedure of identity authentication, since Eve has no qubits entangled with legitimate users. In the proposal of [96], Alice and Bob share some entangled states $|\psi^-\rangle$. Then Bob randomly selects I or σ_x for operating on the photons in his hand and then sends them to Alice. If no eavesdropping takes place, Alice should only get either the state $|\psi^-\rangle$ or $|\phi^-\rangle$. The man-in-the-middle attack issue raised in [98] by Desurvire would disappear if the communicating parties could pre-share a sequence of entangled states, as pointed out by Long in [99]. This concept has also been used in [100], [101].

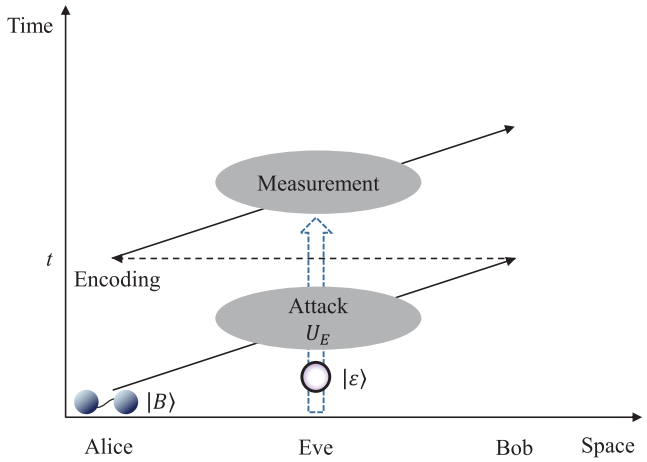

FIGURE 6. The process of Eve's individual attack, whose $|\varepsilon\rangle$ is the probe of Eve, $|B\rangle$ is the photon state sent by Alice, while U_E represents Eve's unitary operation in her attack. Finally, t is the waiting time in the *Step 4* of Fig. 4.

B. ROBUSTNESS AGAINST ATTACKS

If Eve intercepts only one of the photons in the EPR pairs, she is unable to infer valid information [17], [18], [36], since $\rho_A^{\pm} = \mathrm{tr}_B(|\psi^{\pm}\rangle\langle\psi^{\pm}|) = \mathrm{tr}_B(|\phi^{\pm}\rangle\langle\phi^{\pm}|)$. Furthermore, the act of eavesdropping will be discovered by Alice and Bob. Similar to the security of the original QSDC proposal by Long and Liu [36], our QSDC protocol is secure against the act of direct measurement as well as against the "intercept-resend" attack and against the "opaque attack" strategy of [36]. The security of QSDC based on EPR pairs has been formally proved in [102].

In order to glean information about Alice's message, Eve will have to take advantage of the individual attack strategy of Fuchs and Peres [103]. To achieve this, Eve prepares a pure state $|\varepsilon\rangle$ as the probe and arranges for it to interact with the photon state $|B\rangle$ that was sent from Alice to Bob in the first transmission. Subsequently, Eve applies the unitary attack operation U_E to the joint state of $|\varepsilon\rangle$ and $|B\rangle$, and extracts valuable information after Alice completed the secret key encoding, as seen from Fig. 6 and detailed below.

Let us consider the maximum amount of information that Eve can acquire. After Eve's attack operation U_E, the system

can be described as [104]

$$\begin{aligned} U_E|0\rangle|\varepsilon\rangle &= \alpha|0\rangle|\varepsilon_{00}\rangle + \beta|1\rangle|\varepsilon_{01}\rangle \\ &= \alpha|0,\varepsilon_{00}\rangle + \beta|1,\varepsilon_{01}\rangle, \\ U_E|1\rangle|\varepsilon\rangle &= \beta|0\rangle|\varepsilon_{10}\rangle + \alpha|1\rangle|\varepsilon_{11}\rangle \\ &= \beta|0,\varepsilon_{10}\rangle + \alpha|1,\varepsilon_{11}\rangle, \end{aligned} \tag{6}$$

where $|\varepsilon\rangle$ is Eve's probe and the four states $|\varepsilon_{00}\rangle$, $|\varepsilon_{01}\rangle$, $|\varepsilon_{10}\rangle$, and $|\varepsilon_{11}\rangle$ belong to the Hilbert space of Eve's probe. Unitarity and symmetry requires that the four state must satisfy [15]

$$\begin{aligned} |\langle\varepsilon_{00}|\varepsilon_{00}\rangle|^2 &= |\langle\varepsilon_{11}|\varepsilon_{11}\rangle|^2 = |\alpha|^2, \\ |\langle\varepsilon_{01}|\varepsilon_{01}\rangle|^2 &= |\langle\varepsilon_{10}|\varepsilon_{10}\rangle|^2 = |\beta|^2, \\ |\alpha|^2 + |\beta|^2 &= 1, \\ \langle\varepsilon_{00}|\varepsilon_{01}\rangle &= \langle\varepsilon_{11}|\varepsilon_{10}\rangle = 0. \end{aligned} \tag{7}$$

Without loss of generality, we assume that the photon state Alice sends to Bob is $|1\rangle$. From Eq. (6) we know that the joint state is

$$|\psi\rangle = U_E|1\rangle|\varepsilon\rangle = \beta|0,\varepsilon_{10}\rangle + \alpha|1,\varepsilon_{11}\rangle. \tag{8}$$

During detecting eavesdropping, as seen in *Step 4* of our proposed protocol of Fig. 4, Bob randomly selects one of the two sets of measurement bases ($\sigma_z = \{|0\rangle, |1\rangle\}$ and $\sigma_x = \{|+\rangle, |-\rangle\}$) to measure the photon in his possession and Alice chooses the same measurement basis as Bob to measure the corresponding photon. If there is no eavesdropper, they will arrive at the opposite results. Thus the eavesdropping detection probability or quantum bit error rate for Eve's attack is $D = |\beta|^2$.

By contrast, if the EPR pair is used for secret key encoding instead of eavesdropping detection, the joint density matrix after Eve's attack becomes

$$\begin{aligned} \rho = |\psi\rangle\langle\psi| &= |\beta|^2|0,\varepsilon_{10}\rangle\langle 0,\varepsilon_{10}| \\ &+ |\alpha|^2|1,\varepsilon_{11}\rangle\langle 1,\varepsilon_{11}| + \alpha^*\beta|0,\varepsilon_{10}\rangle\langle 1,\varepsilon_{11}| \\ &+ \alpha\beta^*|1,\varepsilon_{11}\rangle\langle 0,\varepsilon_{10}|. \end{aligned} \tag{9}$$

This can also be modeled by

$$\rho = \begin{pmatrix} |\beta|^2 & \alpha^*\beta \\ \alpha\beta^* & |\alpha|^2 \end{pmatrix}. \tag{10}$$

After Alice performs the unitary operations U_0 and U_1 with probabilities of $p_0 = 1/2$ and $p_1 = 1/2$, respectively, the joint state becomes:

$$\begin{aligned} \rho' &= p_0 U_0 \rho U_0^\dagger + p_1 U_1 \rho U_1^\dagger \\ &= \begin{pmatrix} |\beta|^2 & (p_0 - p_1)\alpha^*\beta \\ (p_0 - p_1)\alpha\beta^* & |\alpha|^2 \end{pmatrix} \\ &= \begin{pmatrix} D & 0 \\ 0 & F \end{pmatrix}, \end{aligned} \tag{11}$$

where F represents the fidelity. As discussed in [15], the value of F can be formulated as:

$$F = \frac{1 + \langle\varepsilon_{01}|\varepsilon_{10}\rangle}{2 - \langle\varepsilon_{00}|\varepsilon_{11}\rangle + \langle\varepsilon_{01}|\varepsilon_{10}\rangle} = \frac{1 + \cos x}{2 - \cos y + \cos x}, \tag{12}$$

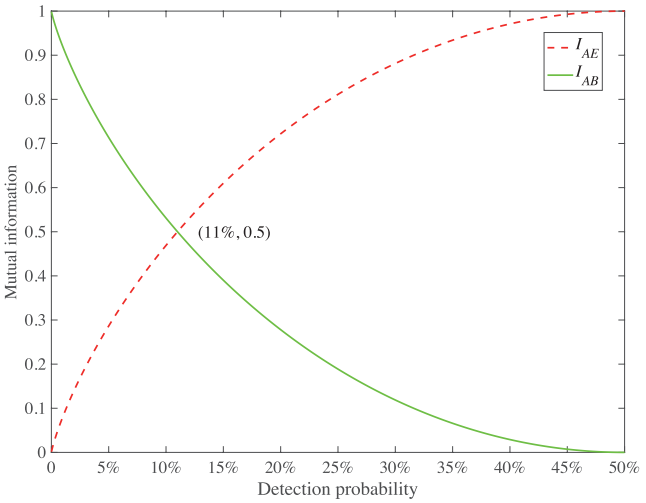

FIGURE 7. Eve's maximal information and the mutual Shannon information of Alice and Bob vs the eavesdropping detection probability.

where x and y represent the angle of nonorthogonal vectors, associated with $0 \leqslant x, y \leqslant \frac{\pi}{2}$ [74].

According to the Holevo bound [105], an upper bound on the amount of information accessible for Eve is

$$\begin{aligned} I \leqslant S(\rho') - \sum_x p_x S(\rho_x{}') &= -\mathrm{tr}(\rho'\log_2\rho') \\ &= -D\log_2 D - F\log_2 F. \end{aligned} \tag{13}$$

The information gleaned by Eve is maximal when $x = y$ [15]. Hence both Eve's maximal information I_{AE} and the mutual Shannon information I_{AB} between Alice and Bob only depend on the eavesdropping detection probability of:

$$\begin{aligned} I_{AE} &= -D\log_2 D - (1-D)\log_2(1-D) \\ I_{AB} &= 1 + D\log_2 D + (1-D)\log_2(1-D). \end{aligned} \tag{14}$$

If the state of the photon Alice sent to Bob is assumed to be $|0\rangle$, the same conclusions are arrived at.

Eve's maximal inferred information and the mutual Shannon information of the Alice-Bob link are plotted in Fig. 7. Clearly, the higher information gained by Eve, the higher eavesdropping detection probability becomes, and ultimately it would reach 50.0% when Eve gets all the information. Furthermore, Eve is unable to steal any information at the eavesdropping detection probability of $D = 0$. The pair of mutual information curves cross at the specific eavesdropping detection probability of 11.0%. If the detection probability is higher than 11.0%, the information Eve can steal becomes higher than the mutual information between Alice and Bob, which implies that the secrecy capacity becomes zero. Hence, the error threshold guarding against individual attack for the proposed QSDC protocol is 11.0%.

This protocol may also be conveniently interpreted in the context of Wyner's wiretap theory. Let us assume that I_{AB} represents the channel capacity of the main channel and I_{AE} is that of the wire-tap channel, where the latter cannot be readily

estimated in classical communication. Given these definitions, $\mathrm{Max}\{I_{AB} - I_{AE}, 0\}$ quantifies the secrecy capacity. If it is higher than zero, then Wyner's wiretap theory guarantees the existence of a coding scheme having a code-rate equal to or lower than the secrecy channel capacity, which facilitates both the reliable and secure transmission of information over a noisy channel even in the face of eavesdropping.

C. SECRET BIT TRANSMISSION EFFICIENCY

It has been pointed out our SPM QSDC can be also used as a DQKD. In this aspect, it is worthwhile to compare the bit transmission efficiency defined in [106]

$$\mathcal{E} = \frac{b_s}{q_t + b_t}, \tag{15}$$

where b_s is the number of secret bits received by Bob, q_t is the number of qubits transmitted in the quantum channel and b_t is the number of classical bits exchanged between a pair of correspondents. The number of classical bits used for eavesdropping detection may be deemed negligible [106]. No classical bits are needed for key generation in our scheme. Accordingly, we have $b_t = 0$, $b_s = 1$ and $q_t = 2$ in Eq. (15), which provides an efficiency of approximately $\mathcal{E} = 50\%$. This efficiency is higher than some of the schemes listed in [106], namely that of the BB84 (25%), B92 (<25%) and GV (33%) protocols. This efficiency may potentially be improved to exceed 50% using the four unitary operations of [37] to encode bits, as mentioned in Section V. However, the channel's transmittance [107] such as exponential photon loss from the fiber also has to be considered in order to calculate the practical efficiency of all QKD schemes. If $\mathcal{T}$ is the channel's transmission efficiency of the qubit over a distance of L, the overall transmittance of the qubits over a distance of L from Alice to Bob is $\mathcal{T}^2\mathcal{T}^2 = \mathcal{T}^4$ in our protocol, when fiber-based delay lines are considered. Then, the practical efficiency can be formulated as $\mathcal{E}' = \mathcal{E}\mathcal{T}^4 = \mathcal{T}^4$.

VII. CONCLUSIONS

In this paper, we compared the basic structure of a classical cryptosystem, of QKD and of QSDC as seen in Fig. 1. The specific operational steps of probabilistic and deterministic QKD as well as of QSDC were also detailed and compared. It can be seen that QKD exploits the laws of quantum mechanics to generate a shared cryptographic key for encryption and decryption. The QKD of Fig. 1 (b) still uses a public classical channel to transmit the ciphertext, making it to some extent similar to the classical cryptosystem. In contrast to QKD, QSDC can send secret information directly through a quantum channel without setting up a key. This communication model relies on the block transmission of quantum states, which requires quantum memory. There has been substantial progress toward the realization of quantum memory [48], [93], but there are still substantial challenges. Hence, conceiving QSDC protocols without quantum memory is a pressing issue for practical QSDC. Remarkably, the QMF QSDC protocol has been invented in [50]. Quantum memory can be dispensed with classical coding. The single-photon based QMF DL04 has been designed [50].

We conceived a new SPM QSDC scheme based on a two-step QSDC protocol. The protocol uses two Bell-basis states which can be measured using linear optics with present-day technology. In the security analysis of this scheme, we considered the families of direct measurement attacks, the intercept-resend attack, and the opaque attack strategy, but none of them constitute a threat. Moreover, our protocol has been proved to be secure against individual attacks.

In closing it is worth pointing out that all QSDC protocols become equivalent to deterministic QKD protocols, if the number of qubits in a block is reduced to a single one [36]–[38]. They all may be transformed to quantum-memory-free or single-photon-memory QSDC using the coding technique proposed in [50]. Thus, at the current state-of-the-art QSDC can be realized for convenient practical applications using block-based data transmission, whilst relying on classical coding techniques.

REFERENCES

[1] 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.
[2] R. P. Feynman, "Simulating physics with computers," *Int. J. Theor. Phys.*, vol. 21, nos. 6–7, pp. 467–488, Jun. 1982.
[3] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput. (STOC)*, 1996, pp. 212–219.
[4] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, Jan. 1999.
[5] G. L. Long, "Grover algorithm with zero theoretical failure rate," *Phys. Rev. A, Gen. Phys.*, vol. 64, no. 2, Jul. 2001, Art. no. 022307.
[6] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O'Brien, "A variational eigenvalue solver on a photonic quantum processor," *Nature Commun.*, vol. 5, no. 1, p. 4213, Sep. 2014.
[7] S. Wei, H. Li, and G. Long, "A full quantum eigensolver for quantum chemistry simulations," *Research*, vol. 2020, Mar. 2020, Art. no. 1486935.
[8] 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. Surveys Tuts.*, vol. 21, no. 2, pp. 1209–1242, 2nd Quart., 2019.
[9] Y. Zhang and Q. Ni, "Recent advances in quantum machine learning," *Quantum Eng.*, vol. 2, no. 1, p. e34, Mar. 2020.
[10] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Bangalore, India, Dec. 1984, pp. 175–179.
[11] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.
[12] D. Dieks, "Communication by EPR devices," *Phys. Lett. A*, vol. 92, no. 6, pp. 271–272, Nov. 1982.
[13] M. Wang and Q. Cai, "Duplicating classical bits with universal quantum cloning machine," *Sci. China Phys., Mech. Astron.*, vol. 62, no. 3, p. 30312, Mar. 2019.
[14] S. Xue, J. Wu, P. Xu, and X. Yang, "Optimal subsystem approach to multi-qubit quantum state discrimination and experimental investigation," *Sci. China Phys., Mech. Astron.*, vol. 61, no. 2, Feb. 2018, Art. no. 020313.
[15] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, p. 145, Mar. 2002.
[16] 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. Surveys Tuts.*, vol. 21, no. 1, pp. 881–919, 1st Quart., 2019.

[17] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, p. 661, 1991.
[18] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett*, vol. 68, no. 5, p. 557, 1992.
[19] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A, Gen. Phys.*, vol. 61, no. 1, Dec. 1999, Art. no. 010303.
[20] M. Hillery, "Quantum cryptography with squeezed states," *Phys. Rev. A, Gen. Phys.*, vol. 61, no. 2, Jan. 2000, Art. no. 022309.
[21] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, Jan. 2002, Art. no. 057902.
[22] I. B. Djordjevic, "On the discretized Gaussian modulation (DGM)-based continuous variable-QKD," *IEEE Access*, vol. 7, pp. 65342–65346, 2019.
[23] 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, Gen. Phys.*, vol. 101, no. 1, Jan. 2020, Art. no. 012343.
[24] K. Wang, D.-S. Ding, W. Zhang, Q.-Y. He, G.-C. Guo, and B.-S. Shi, "Experimental demonstration of Einstein-Podolsky-Rosen entanglement in rotating coordinate space," *Sci. Bull.*, vol. 65, no. 4, pp. 280–285, Feb. 2020.
[25] 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.
[26] P. D. Townsend, "Quantum cryptography on multiuser optical fibre networks," *Nature*, vol. 385, no. 6611, pp. 47–49, 1997.
[27] M. Sasaki, M. Fujiwara, H. Ishizuka, and W. Klaus, "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Express*, vol. 19, no. 11, pp. 10387–10409, 2011.
[28] Y. Zhang and Q. Ni, "Design and analysis of random multiple access quantum key distribution," *Quantum Eng.*, vol. 2, no. 1, p. e31, Mar. 2020.
[29] S.-K. Liao, W. Q. Cai, W. Y. Liu, L. Zhang, Y. Li, J. G. Ren, and J. Yin, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, p. 43–47, Aug. 2017.
[30] A. Müller, 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, 1997.
[31] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, pp. 238–241, Jan. 2003.
[32] X.-F. Mo, B. Zhu, Z.-F. Han, Y.-Z. Gui, and G.-C. Guo, "Faraday–Michelson system for quantum cryptography," *Opt. Lett.*, vol. 30, no. 19, pp. 2632–2634, 2005.
[33] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 112, no. 19, May 2014, Art. no. 190503.
[34] 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, p. 1895, Mar. 1993.
[35] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A, Gen. Phys.*, vol. 59, no. 3, p. 1829, 1999.
[36] G. L. Long and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 3, Feb. 2002, Art. no. 032302.
[37] 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, Gen. Phys.*, vol. 68, no. 4, Oct. 2003, Art. no. 042317.
[38] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A, Gen. Phys.*, vol. 69, no. 5, May 2004, Art. no. 052319.
[39] M. Naseri, "Secure quantum sealed-bid auction," *Opt. Commun.*, vol. 282, no. 9, pp. 1939–1943, May 2009.
[40] 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.
[41] X.-L. Zhao, J.-L. Li, P.-H. Niu, H.-Y. Ma, and D. Ruan, "Two-step quantum secure direct communication scheme with frequency coding," *Chin. Phys. B*, vol. 26, no. 3, Mar. 2017, Art. no. 030302.
[42] R. He, J.-G. Ma, and J. Wu, "A quantum secure direct communication protocol using entangled beam pairs," *EPL (Europhys. Lett.)*, vol. 127, no. 5, p. 50006, Oct. 2019.
[43] Z. Gao, T. Li, and Z. Li, "Long-distance measurement-device–independent quantum secure direct communication," *EPL (Europhys. Lett.)*, vol. 125, no. 4, p. 40004, 2019.
[44] L. Li, J. Li, C. Li, H. Li, Y. Tian, Y. Zheng, and Y. Yang, "Deterministic quantum secure direct communication protocol based on omega state," *IEEE Access*, vol. 7, pp. 6915–6921, 2019.
[45] J.-Y. Hu, L. Yang, S.-X. Wu, R.-Y. Chen, G.-F. Zhang, C.-B. Qin, L.-T. Xiao, and S.-T. Jia, "Security proof of the two-way quantum secure direct communication with channel loss and noise," *EPL (Europhys. Lett.)*, vol. 129, no. 1, p. 10004, Feb. 2020.
[46] 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, 2020, Art. no. 110361.
[47] 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, no. 9, Sep. 2016, Art. no. e16144.
[48] 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.
[49] 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.
[50] Z. Sun, R. Qi, Z. Lin, L. Yin, G. Long, and J. Lu, "Design and implementation of a practical quantum secure direct communication system," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–6.
[51] 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, no. 1, p. 22, Dec. 2019.
[52] F. L. Yan and X. Q. Zhang, "A scheme for secure direct communication using EPR pairs and teleportation," *Eur. Phys. J. B*, vol. 41, no. 1, pp. 75–78, Sep. 2004.
[53] 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, Gen. Phys.*, vol. 71, no. 4, Apr. 2005, Art. no. 044305.
[54] Y. Murakami, M. Nakanishi, S. Yamashita, Y. Nakashima, and M. Hagiwara, "A quantum secure direct communication protocol for sending a quantum state and its security analysis," in *Proc. 6th WSEAS Int. Conf. Inf. Secur. Privacy*, 2007, pp. 91–97.
[55] S. Lin, Q.-Y. Wen, F. Gao, and F.-C. Zhu, "Quantum secure direct communication with χ-type entangled states," *Phys. Rev. A, Gen. Phys.*, vol. 78, no. 6, 2008, Art. no. 064304.
[56] S. Jin, G. Yan-Xiao, X. Ping, Z. Shi-Ning, and Z. You-Bang, "Quantum secure direct communication by using three-dimensional hyperentanglement," *Commun. Theor. Phys.*, vol. 56, no. 5, p. 831, 2011.
[57] C. S. Yoon, M. S. Kang, J. I. Lim, and H. J. Yang, "Quantum signature scheme based on a quantum search algorithm," *Phys. Scripta*, vol. 90, no. 1, Jan. 2015, Art. no. 015103.
[58] M. Naseri, M. A. Raji, M. R. Hantehzadeh, A. Farouk, A. Boochani, and S. Solaymani, "A scheme for secure quantum communication network with authentication using GHZ-like states and cluster states controlled teleportation," *Quantum Inf. Process.*, vol. 14, no. 11, pp. 4279–4295, Nov. 2015.
[59] Z.-W. Cao, X.-Y. Feng, J.-Y. Peng, G.-H. Zeng, and X.-F. Qi, "Quantum secure direct communication scheme in the non-symmetric channel with high efficiency and security," *Int. J. Theor. Phys.*, vol. 54, no. 6, pp. 1871–1877, Jun. 2015.
[60] P. Zawadzki, "Eavesdropping on quantum secure direct communication in quantum channels with arbitrarily low loss rate," *Quantum Inf. Process.*, vol. 15, no. 4, pp. 1731–1741, Apr. 2016.
[61] 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, Oct. 2016.
[62] D. J. Lum, J. C. Howell, M. S. 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, Gen. Phys.*, vol. 94, no. 2, Aug. 2016, Art. no. 022315.
[63] 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, no. 3, Mar. 2020, Art. no. 230362.

[64] 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.
[65] 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, Jan. 2020.
[66] 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, 2019.
[67] 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, 2019, Art. no. 1900050.
[68] D. Pan, Z. Lin, J. Wu, Z. Sun, D. Ruan, L. Yin, and G. Long, "Experimental free-space quantum secure direct communication and its security analysis," 2020, *arXiv:2005.05102*. [Online]. Available: https://arxiv.org/abs/2005.05102
[69] C. Swenson, *Modern Cryptanalysis: Techniques for Advanced Code Breaking*. Hoboken, NJ, USA: Wiley, 2008.
[70] J. Buchmann, *Introduction to Cryptography*. New York, NY, USA: Springer, 2004.
[71] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[72] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Phys. Rev. Lett.*, vol. 89, no. 18, Oct. 2002, Art. no. 187902.
[73] F.-G. Deng and G. L. Long, "Bidirectional quantum key distribution protocol with practical faint laser pulses," *Phys. Rev. A, Gen. Phys.*, vol. 70, no. 1, Jul. 2004, Art. no. 012311.
[74] M. Lucamarini and S. Mancini, "Secure deterministic communication without entanglement," *Phys. Rev. Lett.*, vol. 94, no. 14, Apr. 2005, Art. no. 140501.
[75] H. Lu, C.-H.-F. Fung, and Q.-Y. Cai, "Two-way deterministic quantum key distribution against detector-side-channel attacks," *Phys. Rev. A, Gen. Phys.*, vol. 88, no. 4, Oct. 2013, Art. no. 044302.
[76] L. Yin, D. Pan, and G. L. Long, "Quantum secure direct communication: A survey of basic principle and recent development," *J. Fizik Malaysia*, vol. 39, no. 2, pp. 2–7, 2018.
[77] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul./Oct. 1948.
[78] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[79] 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, 2017.
[80] 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, 2018.
[81] H. Wang, Y. Zhao, X. Yu, A. Nag, Z. Ma, J. Wang, L. Yan, and J. Zhang, "Resilient quantum key distribution (QKD)-integrated optical networks with secret-key recovery strategy," *IEEE Access*, vol. 7, pp. 60079–60090, 2019.
[82] Z.-X. Cui, W. Zhong, L. Zhou, and Y.-B. Sheng, "Measurement-device-independent quantum key distribution with hyper-encoding," *Sci. China Phys., Mech. Astron.*, vol. 62, no. 11, Nov. 2019, Art. no. 110311.
[83] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, and L. Gyongyosi, "Wireless myths, realities, and futures: From 3G/4G to optical and quantum wireless," *Proc. IEEE*, vol. 100, pp. 1853–1888, May 2012.
[84] B. Kraus, N. Gisin, and R. Renner, "Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication," *Phys. Rev. Lett.*, vol. 95, no. 8, Aug. 2005, Art. no. 080501.
[85] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the Internet of Things: Authentication and key generation," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 92–98, Oct. 2019.
[86] H. Krawczyk, "LFSR-based hashing and authentication," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1994, pp. 129–139.
[87] L. Yang, H.-Y. Ma, C. Zheng, X.-L. Ding, J.-C. Gao, and G.-L. Long, "Quantum communication scheme based on quantum teleportation," *Acta Phys. Sinica*, vol. 66, no. 23, 2017, Art. no. 230303.
[88] L. Yang, Y.-C. Liu, and Y.-S. Li, "Quantum teleportation of particles in an environment," *Chin. Phys. B*, vol. 29, no. 6, Jun. 2020, Art. no. 060301.
[89] 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, p. 1370, 2001.
[90] D. Bohm, *Quantum Theory*. Chelmsford, MA, USA: Courier Corporation, 2012.
[91] Q.-Y. Cai and B.-W. Li, "Improving the capacity of the Boström-Felbinger protocol," *Phys. Rev. A, Gen. Phys.*, vol. 69, no. 5, 2004, Art. no. 054301.
[92] 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, no. 1, p. 20962, Aug. 2016.
[93] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Rev. Mod. Phys.*, vol. 83, no. 1, p. 33, 2011.
[94] Z. Sun, L. Song, Q. Huang, L. Yin, G.-L. Long, J.-H. Lu, and L. Hanzo, "Towards practical quantum secure direct communication: A quantum memory-free protocol and code design," to be published.
[95] H. N. Barnum, "Quantum secure identification using entanglement and catalysis," 1999, *arXiv:quant-ph/9910072*. [Online]. Available: https://arxiv.org/abs/quant-ph/9910072
[96] B.-S. Shi, J. Li, J.-M. Liu, X.-F. Fan, and G.-C. Guo, "Quantum key distribution and quantum authentication based on entangled state," *Phys. Lett. A*, vol. 281, nos. 2–3, pp. 83–87, Mar. 2001.
[97] T. Mihara, "Quantum identification schemes with entanglements," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 5, May 2002, Art. no. 052326.
[98] E. Desurvire, *Classical and Quantum Information Theory: An Introduction for the Telecom Scientist*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
[99] G.-L. Long, "On the man-in-the-middle attack in quantum communication," *Mod. Phys.*, to be published.
[100] H. Sun, S. Liu, W. Lin, K. Y. Zhang, W. Lv, X. Huang, F. Huo, H. Yang, G. Jenkins, Q. Zhao, and W. Huang, "Smart responsive phosphorescent materials for data recording and security protection," *Nature Commun.*, vol. 5, no. 1, pp. 1–9, May 2014.
[101] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens," in *Advances in Cryptology*. Boston, MA, USA: Springer, 1983, pp. 267–275.
[102] J. Wu, Z. Lin, L. Yin, and G. Long, "Security of quantum secure direct communication based on Wyner's wiretap channel theory," *Quantum Eng.*, vol. 1, no. 4, p. e26, Dec. 2019.
[103] C. A. Fuchs and A. Peres, "Quantum-state disturbance versus information gain: Uncertainty relations for quantum information," *Phys. Rev. A, Gen. Phys.*, vol. 53, no. 4, p. 2038, 1996.
[104] H. Inamori, L. Rallan, and V. Vedral, "Security of EPR-based quantum cryptography against incoherent symmetric attacks," *J. Phys. A, Math. Gen.*, vol. 34, no. 35, p. 6913, 2001.
[105] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2010.
[106] A. Cabello, "Quantum key distribution in the Holevo limit," *Phys. Rev. Lett.*, vol. 85, no. 26, p. 5635, 2000.
[107] I. Degiovanni, I. R. Berchera, S. Castelletto, M. L. Rastello, F. Bovino, A. Colla, and G. Castagnoli, "Quantum dense key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 69, no. 3, 2004, Art. no. 032310.

DONG PAN received the B.S. degree from Northwest University, Xi'an, China, in 2016. He is currently pursuing the Ph.D. degree with Tsinghua University, Beijing, China. From 2018 to 2019, he was a Visiting Student with the University of Southampton, Southampton, U.K. His current research interest includes quantum information.

KEREN LI received the bachelor's degree in applied physics from the Beijing University of Posts and Telecommunications, in 2014, and the Ph.D. degree in physics from Tsinghua University, in 2019, supervised by Prof. G. Long. He is currently an Assistant Professor with the Peng Cheng Laboratory, Shenzhen, China. From 2015 to 2017, he has visited the IQC, University of Waterloo, for NMR quantum computing experiments supervised by R. Laflamme. He has published 20 articles on quantum information experiments, quantum control, and quantum machine learning. His studies are mainly on quantum control and quantum machine learning. He also does quantum computing experiments on spin-based quantum systems.

DONG RUAN was born in 1970. He received the Ph.D. degree from Tsinghua University, Beijing, in 1997. He is currently a Professor with Tsinghua University. His research interests include quantum computing, quantum physics, and mathematical physics. He is the Deputy Chair of the Department of Physics, Tsinghua University, the Deputy Chair of the National College Steering Committee on Physics Major Teaching, MOE, and the Vice President of the Beijing Physical Society.

SOON XIN NG (Senior Member, IEEE) received the B.Eng. degree (Hons.) in electronics engineering and the Ph.D. degree in telecommunications from the University of Southampton, Southampton, U.K., in 1999 and 2002, respectively. From 2003 to 2006, he was a postdoctoral research fellow, working on collaborative European research projects known as SCOUT, NEWCOM, and PHOENIX. Since August 2006, he has been a member of academic staff with the School of Electronics and Computer Science, University of Southampton. He is currently an Associate Professor in telecommunications with the University of Southampton. He was involved in the OPTIMIX and CONCERTO European projects as well as the IU-ATC and UC4G projects. He was the principal investigator of an EPSRC project on cooperative classical and quantum communications systems. He has published over 250 articles and coauthored two John Wiley/IEEE Press books in his research field. His research interests include adaptive coded modulation, coded modulation, channel coding, space-time coding, joint source and channel coding, iterative detection, OFDM, MIMO, cooperative communications, distributed coding, quantum communications, quantum error correction codes, and joint wireless-and-optical-fiber communications. He is a Chartered Engineer and a Fellow of the Higher Education Academy, U.K.

LAJOS HANZO (Fellow, IEEE) received the master's and Ph.D. degrees from the Technical University (TU) of Budapest, in 1976 and 1983, respectively, and the Doctor of Sciences degree by the University of Southampton, in 2004, and the Honorary Doctorates by the TU of Budapest, in 2009, and by the University of Edinburgh, in 2015. He is a Foreign Member of the Hungarian Academy of Sciences and a former Editor-in-Chief of the IEEE PRESS. He has served several terms as Governor of both IEEE ComSoc and of VTS. He has published 1900+ contributions at IEEE Xplore, 19 Wiley-IEEE Press books and has helped the fast-track career of 123 Ph.D. students. Over 40 of them are Professors at various stages of their careers in academia and many of them are leading scientists in the wireless industry. He is a Fellow of the Royal Academy of Engineering (FREng), of the IET and of EURASIP. (http://www-mobile.ecs.soton.ac.uk, https://en.wikipedia.org/wiki/Lajos_Hanzo).