Towards Practical Quantum Secure Direct Communication: A Quantum-Memory-Free Protocol and Code Design

Zhen Sun, *Student Member, IEEE,* Liyuan Song, *Student Member, IEEE,* Qin Huang, *Senior Member, IEEE,* Liuguo Yin, *Member, IEEE,* Gui-Lu Long, *Member, IEEE,* Jianhua Lu, *Fellow, IEEE,* Lajos Hanzo, *Fellow, IEEE*

***Abstract*—Quantum secure direct communication (QSDC) is capable of direct confidential communications over a quantum channel, which is achieved by dispensing with the key agreement channel of the well-known quantum key distribution (QKD). However, to make QSDC a practical reality, we have to mitigate its reliance on quantum memory, its immediate communication interruption caused by eavesdropping and its low transmission reliability due to the heavy qubit losses. Hence a new QSDC protocol is proposed based on a sophisticated coded single-photon DL04 QSDC protocol to tackle the open challenges. In particular, quantum memory is dispensed with and a high-accuracy secrecy capacity estimate is derived for this protocol by conceiving dynamic joint encryption and error-control (JEEC) coding. We demonstrate that this quantum-memory-free DL04 QSDC (QMF-DL04 QSDC) protocol inches closer to the quantum channel's capacity and significantly improves the original DL04 QSDC's robustness. Moreover, a rate-compatible low-rate JEEC coding scheme is designed for the proposed framework, and the JEEC code advocated is shown to approach the secrecy capacity, despite tolerating an extremely high loss of qubits in the time-varying wiretap channel. Our simulations and experimental results demonstrate that the QMF-DL04 QSDC scheme significantly increases both the secure information rate and the communication distance of the original DL04 protocol.**

***Index Terms*—quantum communication, quantum secure direct communication (QSDC), quantum-memory-free QSDC (QMF-QSDC) protocol, joint encryption and error-control (JEEC) coding, ultra-low-rate coding.**

This work was supported in part by the National Natural Science Foundation of China (Grant Nos. 91538203, 61871257, and 11474181), in part by the NSAF (Grant No. U1530117), in part by the National Basic Research Program of China (Grant Nos. 2017YFA0303700 and 2015CB921001) and in part by the Key R&D Program of Guangdong Province (Grant No. 2018B030325002). *(Corresponding authors: Liuguo Yin and Gui-Lu Long.)*

Zhen Sun is with the School of Information Science and Technology, Tsinghua University, and the Beijing National Research Center for Information Science and Technology, Beijing 100084, China (e-mail: sunzhen16@mails.tsinghua.edu.cn).

Liyuan Song and Qin Huang are with the School of Electronic and Information Engineering, Beihang University, Beijing 100191, China (e-mail: slybuaa@163.com; qinhuang@buaa.edu.cn).

Liuguo Yin and Jianhua Lu are with the School of Information Science and Technology, Tsinghua University, the Beijing National Research Center for Information Science and Technology, and the Frontier Science Center for Quantum Information, Beijing 100084, China (e-mail: yinlg@tsinghua.edu.cn; lhh-dee@mail.tsinghua.edu.cn).

Guilu Long is with the Department of Physics and the State Key Laboratory of Low-Dimensional Quantum Physics, Tsinghua University, and the Frontier Science Center for Quantum Information, Beijng 100084, China, and the Beijing Academy of Quantum Information Sciences, Beijing 100193, China (e-mail: gllong@mail.tsinghua.edu.cn).

Lajos Hanzo is with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, United Kingdom (e-mail: lh@ecs.soton.ac.uk).

L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/N004558/1, EP/P034284/1, EP/P034284/1, EP/P003990/1 (COALESCE), of the Royal Society's Global Challenges Research Fund Grant as well as of the European Research Council's Advanced Fellow Grant QuantCom.

Manuscript received on Sept. 9th, 2019.

I. Introduction

QUANTUM secure communication exploits the laws of quantum physics for achieving the confidentiality of messages. With the rapid development of quantum computing [1]–[3], classical encryption algorithms that are based on mathematical problems such as factorizing large numbers become vulnerable. Hence, traditional secure communication based on cryptographic encryption [4], [5] may face a serious security challenge. Nevertheless, using the principles of quantum physics, quantum secure communication is capable of eliminating any threats from quantum computers. Moreover, it is also capable of estimating the secrecy capacity of a realistic quantum channel, which is impervious to classical information theoretic security approaches. Hence, quantum cryptography has attracted wide attention [6]. The first quantum cryptographic protocol was the widely studied BB84 quantum key distribution (QKD) protocol [7], that was proposed by Bennett and Brassard in 1984. However, QKD does not rely on the transmission of a pre-determined key - it rather discusses and agrees on the keys by relying onboth a quantum channel and a classical channel. Then, the ciphertext is transmitted over another classical channel. The ciphertext can be intercepted and stored by an eavesdropper. If the keys are lost or the ciphertext is not encrypted using the one-time-pad, then there are potential security loopholes in the ciphertext. Hence, as the terminology suggests, QKD is a quantum key agreement protocol, rather than a communication protocol. By contrast, QSDC directly transmits qubits securely without the need for a prior key distribution. As a further compelling benefit, it is also capable of quantifying the amount of information that might be stolen by the eavesdropper (Eve) based on quantum mechanical principles. Therefore, the legitimate transmitter and receiver can monitor the security status of the ciphertext and detect any attacks on the communication channels. Explicitly, QSDC prevents Eve from stealing the ciphertext and promises ultimate practical security.

The idea of QSDC emerged in 2000 [8]. There have been extensive theoretical and experimental studies on QSDC in the last two decades. Its implementation can be broadly divided into two classes, depending on the types of information carriers. The first one is based on single photons, such as the DL04 protocol [9], while the other is based on entangled photons, such as the 'two-step' protocol of [8], [10], the high-dimensional protocol of [11], and the multi-step protocol

associated with the Green-Horne-Zeilinger state [12]. The QSDC dialogue [13] and measurement-device-independent QSDC [14]–[16] have further advanced the development of quantum communication. Several remarkable verification experiments have also been carried out, and these experiments demonstrated the principles of both the DL04 and the two-step QSDC schemes, [17]–[19]. Nonetheless, there are still three main challenges in practical QSDC:

1) The availability of quantum memory is vital for all existing QSDC protocols, since the carrier qubits have to wait for the result of their eavesdropping check in the memory before they are modulated with the information. Regretfully, no practical quantum memory exists that can keep photon quanta for a sufficiently long time with high fidelity [17], [20].
2) It is a challenge to quantitatively estimate the secrecy capacity of a quantum channel and to make effective use of it. Hence the secure information rate remains low. Furthermore, the communication process may be stalled or even completely stopped when Eve becomes active, even if she has a low capacity.
3) Due to the extremely high quantum channel loss and noise, the reception rate of the single-photons remains low and the error rate becomes high. Consequently, it is necessary to develop forward error correction (FEC) codes for enhancing the communication reliability.

QSDC relies on FEC coding, which is in stark contrast to classic QKD, where coding-aided post-processing is used [21]. In the pioneering contribution [22] the secrecy capacity of a practical DL04 QSDC system was estimated, while the security analysis of a two-step QSDC protocol was carried out in [23]. Based on this success, Qi *et al.* conceived an error control coding scheme based on the concatenation of low-density parity-check (LDPC) codes and pseudorandom sequences for enhancing the communication reliability [22]. However, there is still room for improvement, since the transmission rate is still far from the capacity. The class of generalized LDPC (GLDPC) codes is indeed capable of approaching the capacity in *classical* wireless communication [24]–[26], but they have not been specifically developed for QSDC systems [27]–[29].

To tackle these challenges in the implementation of practical QSDC systems, here we evolve the relevant classic information theory [30], [31] for employment in QSDC. In contrast to the QSDC implementations of [17]–[19], [22], we design a quantum-memory-free DL04 QSDC (QMF-DL04 QSDC) protocol based on dynamic joint encryption and error-control (JEEC) coding. The essential idea of QMF-DL04 QSDC is to replace the quantum memory by an FEC scheme, where the information frame is encrypted by a one-time-pad key into a ciphertext, which is further FEC-coded by a secure coding scheme and then mapped to the qubits bit-by-bit. Next the transmitter, Alice, sends the encoded qubits directly to the receiver, Bob. In this way, the use of a quantum memory will be spared. This is reminiscent of using QKD and then sending the ciphertext through a classical channel, but we will demonstrate the striking difference between these two. Because the codeword is transmitted quantum mechanically, its security is monitored. Then, a secure key will be extracted from the transmitted codeword for use in subsequent information frames. In other words, the quantum-mechanically transmitted codeword simultaneously represents the current ciphertext and the key for future employment. If Eve intercepts the QMF QSDC, we will demonstrate that this will be immediately perceived by Alice and Bob, and Eve would only be able to steal some of the codeword, but not the original information itself. The simultaneous use and updates of secret key has also been proven useful in quantum identity authentication in [32].

As a further benefit, we will demonstrate that the proposed protocol is capable of tracking and even approaching the time-varying secrecy capacity during communication. Due to the high error rate of the quantum channel, existing encryption schemes [33]–[35] may fail to guarantee a high reliability even for low-rate quantum communications. Hence we conceive and optimize a variable-rate code, the so-called rate-compatible JEEC coding scheme and design the corresponding joint decoding algorithm for the proposed protocol. More explicitly, we construct a class of low-rate GLDPC codes having flexible code parameters based on Hadamard codes [25] and repetition codes. By intrinsically amalgamating the secrecy codes of [33] and low-rate GLDPC codes, the proposed rate-compatible JEEC scheme improves the reliability vs. security trade-off [36]. The primary contributions of this paper are as follows:

1) We propose the general idea of QMF QSDC and design the QMF-DL04 QSDC protocol, which does not require quantum memory and thus it tackles one of the practical QSDC challenges.
2) The secure information rate is significantly increased, since our dynamic JEEC coding allows the system to operate close to its ultimate secrecy capacity. Quantitatively, our simulation results demonstrate that we double the secure information rate of [22].
3) Explicitly, our QMF-DL04 QSDC system realized secure transmission at 100 bps over a distance of 18.5 kilometers at a clock-rate of 1 MHz.

The rest of paper is organized as follows. Section II reviews the basic DL04 QSDC protocol and the channel model of QSDC. In Section III, we present the proposed QMF-DL04 QSDC protocol. Our rate-compatible JEEC coding structure and its joint decoding algorithm are given in Section IV, while Section V provides the simulation and experimental results. Finally, our conclusions are drawn in Section VI.

II. Preliminaries

In this section, we briefly review the original DL04 protocol [9] and the channel model of the QSDC system [22], [31]. All the abbreviations in this paper are listed in Table I.

A. DL04 QSDC Protocol

The DL04 protocol is a QSDC protocol based on single photons. It requires a quantum memory, which is shown in Fig. 1. As commonly used in quantum communication, Alice, Bob and Eve represent the transmitter, receiver and eavesdropper, respectively. In DL04, single photons (we interchangeably call

TABLE I: Abbreviations

QKD	quantum key distribution
QSDC	quantum secure direct communication
DL04	the QSDC protocol proposed by Deng and Long in 2004
LDPC	low-density parity-check
GLDPC	generalized LDPC
QMF	quantum-memory-free
QMF-DL04 QSDC	the proposed quantum-memory-free QSDC based on DL04 protocol
JEEC	joint encryption and error-control
BSC	binary symmetric channel
BEC	binary erasure channel
SPC	single parity check
GLHR	the proposed GLDPC code based on the Hadamard codes and repetition codes
VN	variable node
CN	check node
LH	A GLDPC code based on the Hadamard constraints
HCN	Hadamard-check node
LLR	log-likelihood ratio
APP	a posteriori probability
MS	min-sum
LPS	the concatenation of LDPC codes with pseudorandom sequences
PEG	progressive edge growth
BER	bit error rate
FER	frame error rate

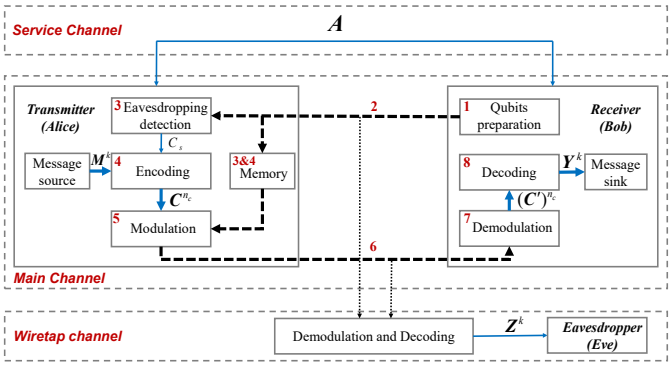

Fig. 1: Illustration of the DL04 protocol and channel model. The main channel represents a channel between the legitimate transmitter and receiver, while the wiretap channel is between the transmitter and eavesdropper. Both of them are discrete and memoryless. The classical service channel is an authenticated noiseless public channel. The black dotted lines carry qubits, and the blue lines carry classical bits.

them photons or qubits) are transmitted over the quantum channel from Bob to Alice first and then back to Bob after being modulated with the classical bit sequence $\boldsymbol{C}^{n_c}$ over the same quantum channel. Eve has to intercept the carrier qubits during both the forward and backward channel transmission, if she wants to obtain any confidential information about $\boldsymbol{C}^{n_c}$. This may change the states of the carrier qubits that Alice received from Bob due to the principles of quantum mechanics. Hence, Alice can perform sampling based detection by randomly selecting some qubits for estimating the secrecy capacity C_s [22] of the channel, while the rest of the qubits wait in the quantum memory to be modulated. Meanwhile, the associated auxiliary data and control instructions, including the result of eavesdropping detection, are transmitted through the classical service channel [1]. We assume that Eve has full access to the classical service channel, but she cannot modify the data. The same assumption is made in QKD. This will not affect the secrecy capacity C_s, because the data in the service channel have no correlation with the confidential information.

Let us now introduce the DL04 protocol. The quantum state vectors of single-photon signals (qubits) are in the two-dimensional Hilbert space, represented either by the polarization states or the phase states of the photon. In free space communications typically the polarization states are used, whereas in optical fiber the phase states are employed. Here we provide a general abstract representation in terms of the Hilbert space. The state of a single photon can be described by a set of orthogonal bases, $\mathbb{Z}$:$\{|0\rangle, |1\rangle\}$ or $\mathbb{X}$:$\{|+\rangle, |-\rangle\}$, where

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad |+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad |-\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}. \tag{1}$$

The encoding operations on a single photon are the identity matrix $\mathbf{I}$ for 0, and $\mathbf{U}$ for 1, where $\mathbf{U}$ is a unitary matrix,

$$\mathbf{U} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{2}$$

The results of $\mathbf{U}$ acting on the basis states in (1) are

$$\mathbf{U}|0\rangle = -|1\rangle, \quad \mathbf{U}|1\rangle = |0\rangle, \quad \mathbf{U}|-\rangle = -|+\rangle, \quad \mathbf{U}|+\rangle = |-\rangle. \tag{3}$$

It shows that the operator $\mathbf{U}$ can change one state into another in the same basis $\mathbb{X}$ or $\mathbb{Z}$.

As Fig. 1 shows, the workflow of the DL04 QSDC protocol contains the following eight steps.

1) Bob prepares a frame of qubits in one of the four initial states in (1).
2) Then, Bob sends these qubits to Alice through the quantum channel.
3) Alice randomly selects some of the received single photons and measures them in basis $\mathbb{X}$ or $\mathbb{Z}$. She then informs Bob of the positions, the chosen basis and the measured results of the selected photons over the classical service channel. The remaining photons are stored in a quantum memory waiting for the results of the security check. Bob checks the results of Alice's measurement: if the checked photons are measured in the same basis as Bob's basis during the preparation, their results should be the same. Eve's malicious action will perturb the state of single photons, hence increasing the qubit error rate quite significantly. Here $\widetilde{e}$ to denotes the qubit error rate estimated by the eavesdropping detection. Estimating $\widetilde{e}$ allows us to determine the capacity of Eve's channel. If the error rate $\widetilde{e}$ becomes higher than a threshold, Alice

[1]Both the QSDC system and the communication system equipped with QKD need the classical channel. But there is a significant difference in the functions of the classical channel. In the communication system that uses QKD to generate and negotiate key, the classical channel is firstly used for transmitting the associated auxiliary data of the quantum key distribution, and then transmitting the classical message (ciphertext). However, in the entire communication process of QSDC, the classical channel is only used for transmitting the associated auxiliary data.

and Bob become aware of the eavesdropping and will terminate the process. Otherwise, they will continue to estimate the secrecy capacity C_s experienced by this frame, and go to the next step.

4) Once C_s has been estimated, Alice encodes the message bits $\boldsymbol{M}^k$ into the codewords $\boldsymbol{C}^{n_c}$ using a predetermined coding scheme.
5) Alice applies either the identity operator $\mathbf{I}$ or the unitary operator $\mathbf{U}$ in (2) to the stored photons to modulate them, respectively according to the bit value '0' or '1' of the $\boldsymbol{C}^{n_c}$.
6) Then Alice sends the modulated photons back to Bob.
7) Next, Bob demodulates them to obtain the received codewords $(\boldsymbol{C'})^{n_c}$.
8) Finally, Bob decodes $(\boldsymbol{C'})^{n_c}$ to obtain $\boldsymbol{Y}^k \in \{0,1\}^k$, which is the message received.

As mentioned above, the DL04 protocol provides a basic method of transmitting classical bits in a two-way single-photon system. Alice sends classical bits $\boldsymbol{C}^{n_c} \in \{0,1\}^{n_c}$, while Bob receives $(\boldsymbol{C'})^{n_c}$. After transmitting a frame of photons, Bob can estimate the qubit error rate e of the main channel. Bob can also estimate what fraction of all the qubits he has prepared was actually received by himself, denoted as Q^{Bob}. We will discuss the relationship of Q^{Bob}, e, $\widetilde{e}$ and the communication capacity between Alice and Bob in the next subsection.

B. Channel Model

Figure 1 summarizes the wiretap channel model of the QSDC system [22], [37]. There are three types of channels: the main channel, wiretap channel and service channel. All vectors in this paper are row vectors, unless stated otherwise.

After detecting the eavesdropping perturbing the quantum channel, the transmitter encodes a k-bit message $\boldsymbol{M}^k \in \{0,1\}^k$ into $\boldsymbol{C}^{n_c} \in \{0,1\}^{n_c}$, using a coding rate of $R = k/n_c$. Then, Bob's receiver obtains $(\boldsymbol{C'})^{n_c}$ from the main channel, which can be modeled as a cascaded channel consisting of a binary symmetric channel (BSC) and a binary erasure channel (BEC) concatenated in series [22]. The erasure probability of the BEC is $(1 - Q^{Bob})$, while the error probability of the BSC is e. Finally, the receiver decodes $(\boldsymbol{C'})^{n_c}$ to obtain $\boldsymbol{Y}^k \in \{0,1\}^k$. Thus, the capacity of the main channel from Alice to Bob is

$$C_m = Q^{Bob} \cdot [1 - h(e)], \tag{4}$$

where $h(e) = -e \cdot \log_2 e - (1-e) \cdot \log_2(1-e)$. Note that C_m fluctuates during a communication session vs. time, as a function of an optical channel owing to the weather, eavesdropping and other conditions, and they are reflected by the different error rates of the eavesdropping detection results of the photon blocks.

If Eve tries to intercept the message, she has to access both the backward and forward quantum channel, which will increase $\widetilde{e}$. According to [22], we can express the secrecy capacity C_s as

$$\begin{aligned} C_s &= \max\{I(A:B) - I(A:E), 0\} \\ &= \max\{C_m - C_w, 0\} \\ &= \max\{Q^{Bob} \cdot [1 - h(e)] - Q^{Eve} \cdot h(2\widetilde{e}), 0\}, \end{aligned} \tag{5}$$

TABLE II: Notations in the QMF-DL04 QSDC protocol

C_s	secrecy capacity
$\boldsymbol{M}$	the information bits
$\boldsymbol{K}$	the key taken from the key pool
m	the length of $\boldsymbol{M}$ and $\boldsymbol{K}$
$\boldsymbol{Y}$	the ciphertext, $\boldsymbol{Y} = \boldsymbol{M} \oplus \boldsymbol{K}$
k	the length of the output of the precoding module
R_P	the rate of the precoding module, $m = kR_P$
$\boldsymbol{X}$	the codeword of the precoding module, with a length of k
$\boldsymbol{X_i} \in \{0,1\}^{k_i}$	part of $\boldsymbol{X}$ or a random sequence, the input of the secure coding module in the i-th frame
R_i	the rate of the secure coding in the i-th frame
k_i	the length of $\boldsymbol{X_i}$
$\boldsymbol{C_i} \in \{0,1\}^{n_{c_i}}$	a single codeword of secure coding in the i-th frame
n_{c_i}	the length of $\boldsymbol{C_i}$
$\boldsymbol{C'_i}$	the received sequence
$\boldsymbol{S_i}$	the keys distilled from $\boldsymbol{C_i}$
$\boldsymbol{X'}$	the receiving result of $\boldsymbol{X}$
$\boldsymbol{X'_i}$	the output of the secure decoding in the i-th frame
C_{s_i}	the secrecy capacity in the i-th frame
C_{m_i}	the capacity of the main channel in the i-th frame
C_{w_i}	the capacity of the wiretap channel in the i-th frame

where $I(A:B)$ is the mutual information between Alice and Bob, and $I(A:E)$ is the mutual information between Alice and Eve, while Q^{Eve} represents the maximum reception rate of Eve. The capacity of the wiretap channel is

$$C_w = Q^{Eve} \cdot h(2\widetilde{e}). \tag{6}$$

Section V-B will highlight how to estimate Q^{Eve} in a practical system. It is widely known that the secret key rate upper bound of the BB84 protocol is

$$R = 1 - 2h(\widetilde{e}), \tag{7}$$

where $\widetilde{e}$ represents the quantum bit error rate. Thus, the threshold of $\widetilde{e}$ is 11%. As for the proposed protocol, the secrecy capacity is

$$C_s = \max\{Q^{Bob} \cdot [1 - h(e)] - Q^{Eve} \cdot h(2\widetilde{e}), 0\}, \tag{8}$$

which leads to the upper bound

$$C_{s_{max}} = 1 - h(\widetilde{e}) - h(2\widetilde{e}), \tag{9}$$

when the channels are lossless (set $e = \widetilde{e}$, $Q^{Bob} = Q^{Eve}$). Hence the threshold of $\widetilde{e}$ is about 7.6%.

The classical service channel between the transmitter and receiver is an authenticated noiseless two-way public channel. The results of the eavesdropping detection and other control signaling, labeled $\boldsymbol{A}$ in Fig. 1, are exchanged over this channel. Eve is able to fully access $\boldsymbol{A}$ but cannot modify it.

III. Quantum-Memory-Free DL04 QSDC Protocol

In this section, we conceive a new QSDC protocol, namely the QMF-DL04 QSDC, for circumventing the challenges faced by the DL04 protocol. By combining quantum mechanics and information theory, the proposed QMF-DL04 QSDC protocol can dispense with quantum memory, provide a more accurate secrecy capacity estimation, and operate at a rate close to the near-instantaneous quantum channel capacity.

We list all the notations of the QMF-DL04 QSDC protocol in Table II for readers' convenience.

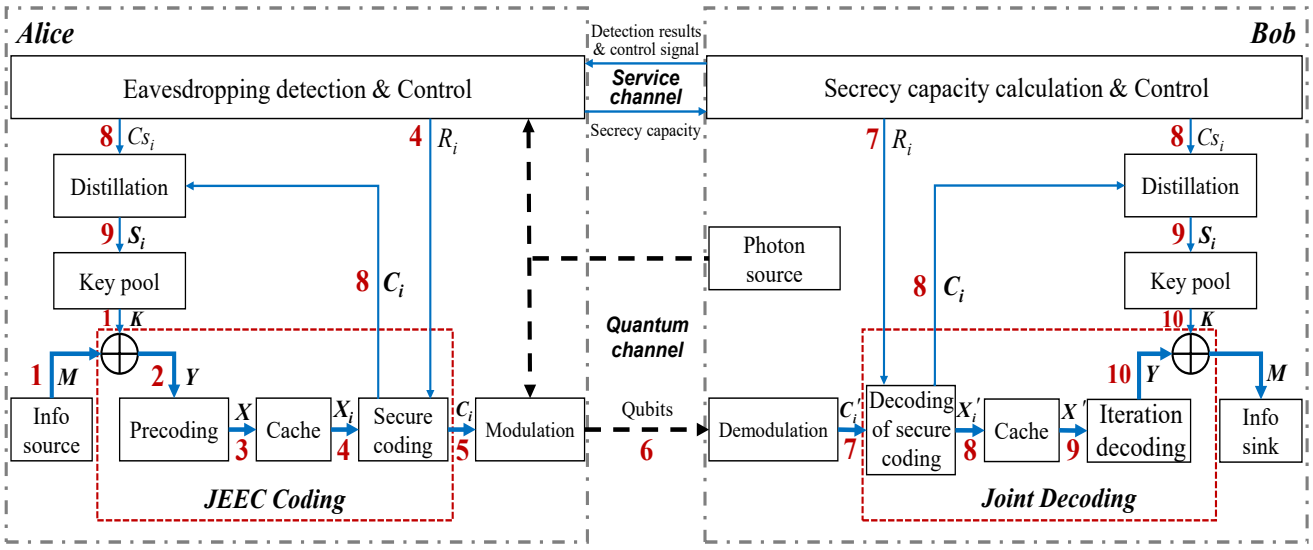

Fig. 2: Structure of the proposed QMF-DL04 QSDC protocol and the data stream of the i-th frame. The black dotted lines carry qubits, and the blue lines carry classical bits.

A. The QMF-DL04 QSDC Protocol

A detailed description of the proposed QMF-DL04 QSDC protocol is now given as follows, where Alice and Bob communicate over the quantum channel and with the aid of the classical service channel. As depicted in Fig. 2, the transmitter has an eavesdropping detection module, system control module, key distillation module, JEEC encoding module, modulator, key pool and the information source. The receiver includes the C_s-calculation module, system control module, key distillation module, joint decoding module, demodulator, key pool and the information sink.

The symbols in the data stream are defined as follows: $\boldsymbol{M} \in \{0,1\}^m$ is the information bit sequence encoded by the JEEC coding module; $\boldsymbol{K}$ is the key needed for JEEC encoding and decoding, which is taken from the key pool and has the same length, m, as $\boldsymbol{M}$. The sequence $\boldsymbol{Y}$ represents the ciphertext, which is the input of the precoding module, $\boldsymbol{Y} = \boldsymbol{M} \oplus \boldsymbol{K}$. A (k, kR_p) LDPC encoder of code length k and rate R_p is a good choice for the precoding module, where $m = kR_P$. A codeword $\boldsymbol{X}$ of the (k, kR_p) LDPC code with length k is the output of the precoding module formulated by encoding the input sequence $\boldsymbol{Y}$. The sequence $\boldsymbol{X_i} \in \{0,1\}^{k_i}$ is part of $\boldsymbol{X}$ or a random bit sequence, which is the input of the secure coding module in the i-th frame. Let R_i be the rate of the secure coding in the i-th frame. Details of R_i and k_i will be given later. Let us assume that $\boldsymbol{C_i} \in \{0,1\}^{n_{c_i}}$ is a single codeword produced by encoding $\boldsymbol{X_i}$, i.e. the output of the secure coding module of Fig. 2. Then, $\boldsymbol{C_i}$ is transmitted to Bob over the quantum channel.

After the transmission of $\boldsymbol{C_i}$, Alice and Bob can infer C_m, C_w and C_s of the system during the period in which the i-th frame is sent; we denote them as C_{m_i}, C_{w_i} and C_{s_i}, respectively. The received sequence $\boldsymbol{C_i'}$ is decoded by an iterative decoding algorithm. Let $I_{\max}$ be the maximum number of iterations. When the set $I_{\max}$ is reached, and not all check sums of the decoding result of $\boldsymbol{C_i}$ multiplying the transpose of associated parity-check matrix are equal to 0, a decoding failure is reported to Alice through the classical service channel. Then, the system has to re-transmit the corresponding message by using a new secret key from the key pool. If however all check sums are equal to 0, we exit the decoding and output the decoded sequence $\boldsymbol{X_i'}$, namely the secure decoding result. Then, $\boldsymbol{X_i'}$ is successively stored in the cache.

If Bob decodes $\boldsymbol{C_i'}$ correctly and flawlessly recovers $\boldsymbol{X_i}$ and $\boldsymbol{C_i}$, Alice and Bob can distill a common secret key $\boldsymbol{S_i}$ from $\boldsymbol{C_i}$, according to the secrecy capacity C_{s_i}. After all parts of $\boldsymbol{X}$ have been transmitted, if Bob cannot correctly decode $\boldsymbol{C_i'}$ in several frames, the sequence $\boldsymbol{X'} = \{\boldsymbol{X_i'}\}$ in the cache is further decoded based on the precoding LDPC code. If $\boldsymbol{X'}$ is decoded correctly to obtain both $\boldsymbol{X}$ and the ciphertext $\boldsymbol{Y}$, Bob can recover all transmitted codewords even if several received sequences $\boldsymbol{C_i'}$ are decoded incorrectly. The distillation module of Fig. 2 makes use of the universal hashing procedure [38] for extracting the key [39], [40]. Alice and Bob can use the same Toeplitz matrix for distilling a $(n_{c_i} \cdot C_{s_i})$-bit secret key $\boldsymbol{S_i}$ from $\boldsymbol{C_i} \in \{0,1\}^{n_{c_i}}$. For ensuring that Alice and Bob always keep the same key pool, it can be designed as a first-in first-out (FIFO) memory. The modulator and demodulator module simply follow the DL04 protocol.

The basic quantum processes of communication and eavesdropping detection are the same as those of the DL04 scheme. It is worth mentioning that the role of the secure coding module is vital for approaching the secrecy capacity. Furthermore, the accurate estimation of the secrecy capacity after the transmission allows us to distill a new key sequence from the received codeword for later use. If the system transmits $\boldsymbol{X}$ directly, namely without secure coding, the secrecy capacity cannot be approached. As a consequence, Alice and Bob cannot distill keys according to the measurement of the C_s. This results in a sharp reduction in the number/length of keys and we are unable to ascertain, how many keys we can

distill. Hence, although $\boldsymbol{X}$ is already encrypted by the keys, the system still needs the secure coding module for protecting $\boldsymbol{X}$ transmitted over the quantum channel, whose secrecy capacity varies.

Let us now concentrate on the three different phases of the proposed QMF-DL04 QSDC protocol. As mentioned above, we denote each frame transmitted over the quantum channel as $\boldsymbol{C_i}$ ($i = 1, 2, 3, \ldots$). Additionally, $\boldsymbol{C_i}$ is constituted of n_{c_i} bits. Then, we have the corresponding parameters given by $\boldsymbol{X_i}$, k_i, R_i, $\boldsymbol{C_i'}$, $\boldsymbol{S_i}$, C_{m_i}, C_{w_i} and C_{s_i}. Referring now to Fig. 2, when Alice is going to send the i-th frame $\boldsymbol{C_i}$:

- If $i = 1$, the key pool is empty: the precoding module simply does not work, and $\boldsymbol{X_i}$ is constituted by random bits using a random number generator [41], [42]. Alice and Bob should select the appropriate values of C_{w_0}, k_1, R_1 and C_{m_0} to meet (10). After Alice sends $\boldsymbol{C_1}$ to Bob correctly, they can obtain C_{m_1}, C_{w_1}. If (10) is satisfied, then they can obtain the same new key $\boldsymbol{S_1}$ by distilling $\boldsymbol{C_1}$. The length of $\boldsymbol{S_1}$ is $n_{c_1} \cdot C_{s_1}$. Note that C_{w_0} and C_{m_0} can also glean prior knowledge from the preceding channel estimation.
- If $i > 1$ and there is insufficient keys for encrypting a m-bit $\boldsymbol{M}$ (the length of the keys in the pool is shorter than m), then the precoding module also fails and $\boldsymbol{X_i}$ is a random bit sequence. Then, the secure coding module requires

$$\frac{k_i}{n_{c_i}} \leq R_i - C_{w_{i-1}}, \quad R_i < C_{m_{i-1}}, \tag{10}$$

  where $C_{w_{i-1}}$ is the wiretap channel capacity of the $(i-1)$-th frame, which is used as an estimate of C_{w_i} and it is defined by

$$C_{w_{i-1}} = Q_{i-1}^{Eve} \cdot h(2\widetilde{e}_{i-1}) = g \cdot Q_{i-1}^{Bob} \cdot h(2\widetilde{e}_{i-1}), \tag{11}$$

  where $g = Q^{Eve}/Q^{Bob}$ for convenience. After Alice sends $\boldsymbol{C_i}$ to Bob correctly, they can obtain C_{m_i}, C_{w_i} and C_{s_i}. If C_{m_i} and C_{w_i} satisfy (10), then they can obtain the common new key $\boldsymbol{S_i}$ by distilling the $\boldsymbol{C_i}$. The length of $\boldsymbol{S_i}$ is $n_{c_i} \cdot C_{s_i}$.
- If $i > 1$ and there is enough key to encrypt $\boldsymbol{M}$, then the workflow contains the following ten steps, as seen in Fig. 2:
  1) Alice uses $\boldsymbol{K} \in \{0,1\}^{k'}$ to encrypt $\boldsymbol{M} \in \{0,1\}^{k'}$: $\boldsymbol{Y} = \boldsymbol{M} \oplus \boldsymbol{K}$.
  2) $\boldsymbol{Y}$ is precoded to produce $\boldsymbol{X} \in \{0,1\}^{k}$.
  3) Then, $\boldsymbol{X}$ is stored in a cache.
  4) Alice chooses a k_i-bit sequence from the cache to carry out secure coding. Note that k_i and R_i also have to satisfy (10).
  5) Alice modulates the carrier qubits and then sends them over the quantum channel to Bob.
  6) Bob demodulates the received qubits.
  7) Bob decodes the secure coding of Step 4.
  8) After Bob receives $\boldsymbol{C_i}$ correctly, both Alice and Bob can obtain C_{m_i}, C_{w_i} and C_{s_i}.
  9) If C_{m_i} and C_{w_i} satisfy (10), Alice and Bob are capable of obtaining the same new key $\boldsymbol{S_i}$ by distilling $\boldsymbol{C_i}$. The length of $\boldsymbol{S_i}$ is $n_{c_i} \cdot C_{s_i}$. Now we repeat Steps 4 to 9 until all parts of $\boldsymbol{X}$ are transmitted. If Bob fails to correctly receive $\boldsymbol{C_i}$ in several frames, the decoded sequence $\boldsymbol{X'} = \{\boldsymbol{X_i'}\}$ in the cache is further decoded to obtain both $\boldsymbol{X}$ and those previously incorrectly received codewords $\boldsymbol{C_i}$.
  10) Finally, Bob uses the same $\boldsymbol{K}$ to decrypt $\boldsymbol{Y}$: $\boldsymbol{M} = \boldsymbol{Y} \oplus \boldsymbol{K} = \boldsymbol{M} \oplus \boldsymbol{K} \oplus \boldsymbol{K} = \boldsymbol{M}$. However, if $\boldsymbol{X'} = \{\boldsymbol{X_i'}\}$ cannot be correctly decoded, Bob informs Alice over the classical service channel as to which received codewords $\boldsymbol{C_i'}$ are incorrect.

  The precoding, secure coding and their decoders of Fig. 2 will be discussed in the next section.

The main novelty of this contribution hinges on dispensing with the use of quantum memory in QSDC and on optimizing the performance attained. There are significant differences between our QMF QSDC and QKD, although they both use similar information theoretic security techniques, such as for example the key distillation. QKD distills the key from transmitted random bits and then sends the ciphertext in a separate classical communications phase. In QMF QSDC, the key is distilled from the transmitted codewords, which encode and protect the ciphertext. The transmitted codewords simultaneously represent both the coded ciphertext and the raw key to be distilled for subsequent transmissions. Hence QSDC relies on a single transmission phase instead of the two separate transmission phases of QKD. More explicitly, QSDC succeeds in this because it can monitor the transmission of the codewords, followed by the accurate estimation of the number/length of keys that can be distilled from the transmitted codewords. Furthermore, QSDC is also capable of performing the task of distributing keys.

B. Secure Information-Rate Improvement

In this protocol, the confidentiality of $\boldsymbol{M}$ is guaranteed with the aid of the one-time pad. Moreover, secure coding is used for protecting the codewords $\boldsymbol{C_i}$ from Eve by taking advantage of the gap between C_{m_i} and C_{w_i}. Thus, we can distill the secret key $\boldsymbol{S_i}$ from $\boldsymbol{C_i}$.

Proposition 1: The proposed QMF-DL04 QSDC protocol is capable of increasing the practical secure information transmission rate by the amount of $\delta_i = C_{m_i} - R_i$ in the i-th frame, over and above the original DL04 protocol.

Proof: Based on the QMF-DL04 QSDC protocol of Section II-A, we can obtain a longer key after the transmission of the i-th frame:

$$s_i = n_{c_i} \cdot C_{s_i} = n_{c_i} \cdot (C_{m_i} - C_{w_i}) > n_{c_i} \cdot (R_i - C_{w_i}) = k_i, \tag{12}$$

where k_i is the maximum number of information bits in the i-th frame in Ref. [22]. Because the length of the information word is equal to the length of the key in this proposed protocol, the increment of the secure information rate of the i-th frame is given by

$$\delta_i = (s_i - k_i)/n_{c_i} = C_{m_i} - R_i, \tag{13}$$

which is exactly the gap between the capacity of the main channel and the rate of the codes. This proves our proposition. ■

As a result, the proposed QMF-DL04 QSDC protocol approaches the secure capacity C_s more closely than the original protocol of [22].

Proposition 2: The QMF-DL04 QSDC has the capability of key accumulating, and enables secure communication even if the secure capacity C_s becomes zero for a short time, provided that there are enough keys in the pool.

Proof: Without loss of generality, we assume that j frames are transmitted and that $C_{m_i} > C_{w_i}$, for $1 \le i \le j$. Then the total length of the keys entered into the key pool is

$$s_{in} = \sum_{i=1}^{j} [n_{c_i} \cdot (C_{m_i} - C_{w_i})]. \tag{14}$$

To transmit the $(j+1)$-st frame, the maximum total length of the keys used by all the $(j+1)$ frames is

$$s_{out} = \sum_{i=1}^{j+1} [R_p \cdot n_{c_i} \cdot (R_i - C_{w_{i-1}})], \tag{15}$$

where $R_i > C_{w_{i-1}}$, for $1 \le i \le j$, according to the proposed protocol. Hence, the total length of the keys left in the pool is

$$\begin{aligned}
s &= s_{in} - s_{out} \\
&= \sum_{i=1}^{j} \{n_{c_i} \cdot [C_{m_i} - C_{w_i} - R_p \cdot (R_i - C_{w_{i-1}})]\} - R_p \cdot n_{c_{j+1}} \cdot (R_{j+1} - C_{w_j}) \\
&> n_c^{\min} \cdot \sum_{i=1}^{j} (C_{m_i} - C_{w_i} - R_i + C_{w_{i-1}}) - R_p \cdot n_{c_{j+1}} \cdot (R_{j+1} - C_{w_j}) \\
&= n_c^{\min} [(C_{m_j} - C_{w_j}) + (C_{w_0} - R_1) + \sum_{i=1}^{j-1} (C_{m_i} - R_{i+1})] - R_p \cdot n_{c_{j+1}} \cdot (R_{j+1} - C_{w_j}) \\
&> n_c^{\min} [(C_{m_j} - C_{w_j}) + (C_{w_0} - R_1) + \sum_{i=1}^{j-1} (C_{m_i} - R_{i+1})] - n_{c_{j+1}} (R_{j+1} - C_{w_j})
\end{aligned} \tag{16}$$

where $n_c^{\min}$ is the minimum value of $\{n_{c_i}\}, i = 1, 2, \cdots, j$. In a practical QSDC system, we can let $n_c^{\min} = n_{c_{j+1}} = n_c$. Then

$$\begin{aligned}
s &> n_c \cdot [(C_{m_j} - C_{w_j}) + (C_{w_0} - R_1) + \sum_{i=1}^{j-1} (C_{m_i} - R_{i+1}) - R_{j+1} + C_{w_j}] \\
&= n_c \cdot [\sum_{i=1}^{j} (C_{m_i} - R_{i+1}) + (C_{w_0} - R_1)].
\end{aligned} \tag{17}$$

According to (10), $R_{i+1} < C_{m_i}$. In addition, C_{w_0} and R_1 are chosen by the system itself. Obviously it is plausible that in most cases,

$$s > 0, \tag{18}$$

which indicates that the $(j+1)$-th frame is capable of conveying secure information bits even if $C_{s_{j+1}} < 0$. This proves the proposition. ■

According to Proposition 2, our QMF-DL04 QSDC protocol is capable of improving the system's robustness over that of [22], because in [22] communications will inevitably be interrupted, when C_s becomes zero.

IV. Dynamic Joint Encryption and Error-Control Coding

In this section, we design and optimize the JEEC coding scheme of Fig. 2 for the QMF-DL04 QSDC protocol. A range of impressive secrecy codes have been proposed in [33]–[35], [43], [44], striving for a compelling trade-off between security and reliability [36] for transmission over a wiretap channel. There also have been some researches on the joint encryption and error-control coding in the wireless communication [45]–[47]. However, the received photon-count reduction in quantum communication is tremendous. For example, the reception rate Q^{Bob} of Bob may become lower than 0.0035 in a practical QSDC system [37]. Thus, these existing coding schemes may suffer from severe performance loss in quantum communications, and they can not be used in our protocol directly.

Here, we propose to extend the traditional secrecy-LDPC codes [33]–[35], which randomly select a single codeword from the coset of a LDPC code, to the new class of low-rate secrecy-GLDPC codes which we define in this section. Then, a rate-compatible low-rate JEEC coding scheme is designed based on the proposed secrecy-GLDPC codes for enhancing the reliability and for achieving an increased secure information rate of QSDC. The new class of low-rate JEEC coding schemes is designed by replacing the single parity check (SPC) codes at the check nodes (CNs) of a secrecy-LDPC code by Hadamard codes [25] and concatenated repetition codes. The proposed *GLDPC code based on the Hadamard codes and repetition codes* (GLHR) allows us to appropriately choose the length of the repetition codes. Furthermore, we can use low-complexity Hadamard codes and still achieve good performance.

Before we present the low-rate JEEC coding scheme, we define and list all notations which will be used in the next sections in Table III.

A. Low-Rate JEEC Coding Structure

A detailed description of the JEEC coding scheme based on the GLHR codes which is designed for the protocol proposed in Section III is given as follows. The entire structure of the proposed JEEC coding is shown in Fig. 3. Recall the precoding module defined in Section III. The (k, kR_p) LDPC code C is considered as the coding scheme in the precoding module, and the output $\boldsymbol{X}$ is a single codeword of C. The codeword $\boldsymbol{X}$ is divided into N parts, $\boldsymbol{X_i} \in \{0,1\}^{k_i}$, and stored in the cache, where $1 < i \le (N+1)$. Then, each part $\boldsymbol{X_i}$ is successively input into the secure coding module, as shown in Fig. 2, in the i-th frame.

Let us select the first $m_1^{(i)}$ rows of the matrix $\mathbf{B}$ to form the parity-check matrix $\mathbf{H}_1^{(i)}$ with a constant row weight ρ. Then, the above submatrix of $\mathbf{H}_1^{(i)}$, $\mathbf{H}_2^{(i)}$, is an $m_2^{(i)} \times n$ parity-check matrix with a constant row weight ρ, whose null space defines the $(n, k_2^{(i)})$ LDPC code $C_2^{(i)}$. For transmitting each vector $\boldsymbol{X_i}$ of length k_i, Alice first randomly chooses a codeword $\mathbf{c}^{(i)}$

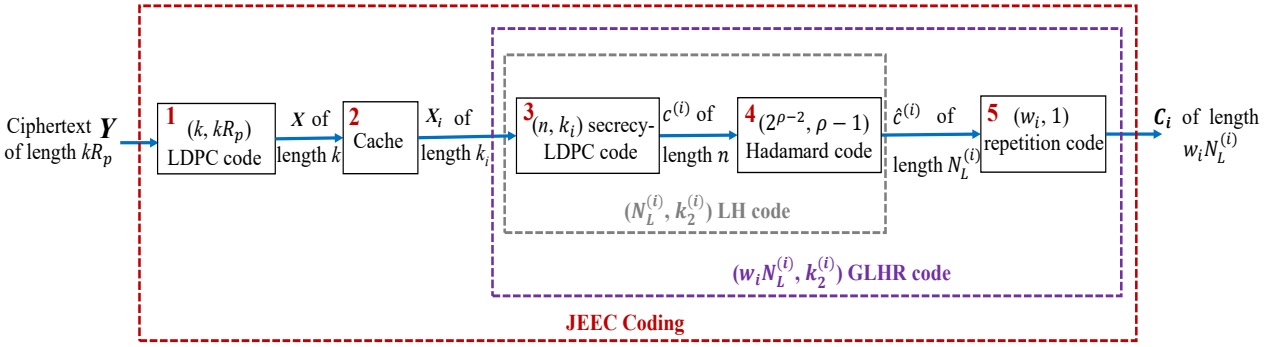

Fig. 3: Entire structure of the proposed JEEC coding

of the LDPC code $C_2^{(i)}$ if $\mathbf{c}^{(i)}$ is a solution of the following equation [33]:

$$\mathbf{H}_1^{(i)}(\mathbf{c}^{(i)})^T = \begin{bmatrix} \mathbf{H}_2^{(i)} \\ \tilde{\mathbf{H}}_2^{(i)} \end{bmatrix} (\mathbf{c}^{(i)})^T = [\underbrace{0 \ldots 0}_{n-k_2^{(i)}} X_i]^T, \tag{19}$$

where the j-th codeword bit $c_j^{(i)}$ of $\mathbf{c}^{(i)}$ is associated with the j-th variable node (VN) of $C_2^{(i)}$, $1 < i \leq N+1$ and $0 \leq j < n$. Each check node (CN) having the degree-ρ of the standard LDPC code $C_2^{(i)}$ can be considered as a $(\rho, \rho-1)$ SPC code. Then, Alcie uses the variable codeword bits of the randomly chosen codeword $\mathbf{c}^{(i)}$ for encoding various low-rate linear codes so that she can obtain a codeword of the low-rate GLHR code.

To construct the low-rate GLHR code, first the SPC constraints imposed on the CNs of the standard LDPC code $C_2^{(i)}$ are replaced by the constraints based on other linear codes, such as Hadamard codes and BCH codes. Again, we consider the family of Hadamard codes for constructing the *GLDPC code subject to the Hadamard constraints*, which were hence termed as LH codes in [25] [2], where the SPC code used at each CN in a standard LDPC code is replaced by a Hadamard constituent code. A CN obeying the Hadamard constraints of the LH code is termed as a Hadamard-check node (HCN).

For constructing the $(N_L^{(i)}, k_2^{(i)})$ LH code $\hat{C}_2^{(i)}$, all CNs of $C_2^{(i)}$ are replaced by HCNs. For $0 \leq l < m_2^{(i)}$, the first $\rho-1$ codeword bits $c_j^{(i)}$'s corresponding to the first $\rho-1$ VNs connected to the l-th CN of $C_2^{(i)}$, $j \in N_l \backslash j_l$, are encoded into the codeword $\mathbf{a}_l^{(i)}$ of a $(2^r, r+1)$ systematic Hadamard code with the order of $r = \rho-2$ [25]. Thus, each bit $c_j^{(i)}$, $j \in N_l \backslash j_l$, is equal to the codeword bit $a_{l,t}^{(i)}$ of $\mathbf{a}_l^{(i)}$ at the l-th HCN for $t \in \{0, 1, 2, 4, \ldots, 2^{r-1}\}$, respectively, which are termed as the information bits. The other $2^r - (\rho-1)$ codeword bits of $\mathbf{a}_l^{(i)}$ are considered to be parity bits. It has been proven that the last parity bit $a_{l,2^r-1}^{(i)}$ is equal to the bit $c_{j_l}^{(i)}$ associated with the last VN_{j_l} connected to CN_l [25], if r is even. Thus, the l-th HCN of $\hat{C}_2^{(i)}$ connects two types of VNs, if the row weight ρ is even. The VNs of the first one are the original ρ VNs connected to the l-th CN of $C_2^{(i)}$, and those of the second one are new VNs of degree-1 that correspond to the first $2^r - r - 2$ parity bits of the encoded codeword $\mathbf{a}_l^{(i)}$ of the $(2^r, r+1)$ Hadamard code. The SPC constraint is also satisfied in an HCN, if it is based on a Hadamard code with an even order. For an HCN based on an odd-order Hadamard code, the SPC constraint is also satisfied by using a nonsystematic Hadamard code (which is not considered in this paper).

Then, a codeword $\hat{\mathbf{c}}^{(i)} = (\hat{c}_0^{(i)}, \hat{c}_1^{(i)}, \ldots, \hat{c}_{N_L^{(i)}-1}^{(i)})$ of the LH code $\hat{C}_2^{(i)}$ is formed by the chosen codeword $\mathbf{c}^{(i)}$ of the LDPC code $C_2^{(i)}$ and the parity bit sequences, $\mathbf{b}_l^{(i)}$, of all HCNs, i.e., $\hat{\mathbf{c}}^{(i)} = (\mathbf{c}^{(i)}, \mathbf{b}_0^{(i)}, \mathbf{b}_1^{(i)}, \ldots, \mathbf{b}_{m_2^{(i)}-1}^{(i)})$, where $0 \leq l < m_2^{(i)}$. The parity-check matrix $\hat{\mathbf{H}}_2^{(i)}$ of $\hat{C}_2^{(i)}$ is given in (20), where $t \in \Lambda^{\complement}$, $\mathbf{h}_{l,j}$ is an all-zero column vector of length $2^r - r - 1$ if the (l, j)-th element $h_{l,j}$ in $\mathbf{H}_2^{(i)}$ is zero; otherwise, $\mathbf{h}_{l,j}$ is equal to the x-th column of $\mathbf{H}_{h,r}$ for $x \in \Lambda$, $0 \leq l < m_2^{(i)}$ and $0 \leq j < n$.

Next, each codeword bit in the codeword $\hat{\mathbf{c}}^{(i)}$ of the LH code $\hat{C}_2^{(i)}$ is respectively mapped into a codeword of the $(w_i, 1)$ repetition code to generate a sequence $\boldsymbol{C_i} = (\boldsymbol{C_{i,0}}, \boldsymbol{C_{i,1}}, \ldots, \boldsymbol{C_{i,N_L^{(i)}-1}})$. For $0 \leq j < N_L^{(i)}$, the j-th codeword bit $\hat{c}_j^{(i)}$, '0' or '1', in $\hat{\mathbf{c}}^{(i)}$ is mapped to $\mathbf{R}_0^{(i)}$ or $\mathbf{R}_1^{(i)}$, respectively, i.e., if $\hat{c}_j^{(i)} = 0$, $\boldsymbol{C_{i,j}} = \mathbf{R}_0^{(i)}$; otherwise, $\boldsymbol{C_{i,j}} = \mathbf{R}_1^{(i)}$. The resultant sequence $\boldsymbol{C_i}$ of length $n_{c_i} = w_i N_L^{(i)}$ is a codeword of the $(n_{c_i}, k_2^{(i)})$ GLHR code $\tilde{C}_2^{(i)}$. Then, the codeword $\boldsymbol{C_i}$ is the output of the secure coding module of Fig. 2 in the i-th frame. The parity-check matrix $\tilde{\mathbf{H}}_2^{(i)}$ of the GLHR code $\tilde{C}_2^{(i)}$ is a $(n_{c_i} - k_2^{(i)}) \times n_{c_i}$ matrix. The bipartite Tanner graph representation of a GLHR code based on a standard LDPC code having a constant row weight ρ and a constant column weight γ is shown in Fig. 4. Finally, Alice transmits the coded sequence $\boldsymbol{C_i}$ to Bob over the main quantum channel. The rate of secure coding based on the GLHR code in the i-th frame is given as follows:

$$R_i = R_{\text{GLHR}}^{(i)} = k_2^{(i)}/n_{c_i} = k_2^{(i)}/[w_i \cdot (n + m_2^{(i)}(2^{\rho-2} - \rho)], \tag{21}$$

and the actual rate of the message vector $\mathbf{X}_i$ passed through the secure coding module is

$$R_{x_i} = k_i/n_{c_i} = [k_2^{(i)} - k_1^{(i)}]/[w_i(n + m_2^{(i)}(2^{\rho-2} - \rho)], \tag{22}$$

where $1 < i \leq N+1$. If we have $0 < R_i < C_{m_{i-1}}$ and

$$R_{e_i} = k_1^{(i)}/n_{c_i} = k_1^{(i)}/[w_i(n + m_2^{(i)}(2^{\rho-2} - \rho)] \geq C_{w_{i-1}}, \tag{23}$$

[2] A GLDPC code which is subject to the Hadamard constraints at each of its CN is called as the LH code in this paper.

$$\hat{\mathbf{H}}_2^{(i)} = \left[\begin{array}{cccc|ccc} \mathbf{h}_{0,0} & \mathbf{h}_{0,1} & \cdots & \mathbf{h}_{0,n-1} & \mathbf{p}_3 \cdots \mathbf{p}_t \cdots \mathbf{p}_{2^r-2} & & \\ \mathbf{h}_{1,0} & \mathbf{h}_{1,1} & \cdots & \mathbf{h}_{1,n-1} & & \mathbf{p}_3 \cdots \mathbf{p}_t \cdots \mathbf{p}_{2^r-2} & \\ \vdots & & \ddots & \vdots & & & \ddots \\ \mathbf{h}_{m_2^{(i)}-1,0} & \mathbf{h}_{m_2^{(i)}-1,1} & \cdots & \mathbf{h}_{m_2^{(i)}-1,n-1} & & & \mathbf{p}_3 \cdots \mathbf{p}_t \cdots \mathbf{p}_{2^r-2} \end{array}\right] \tag{20}$$

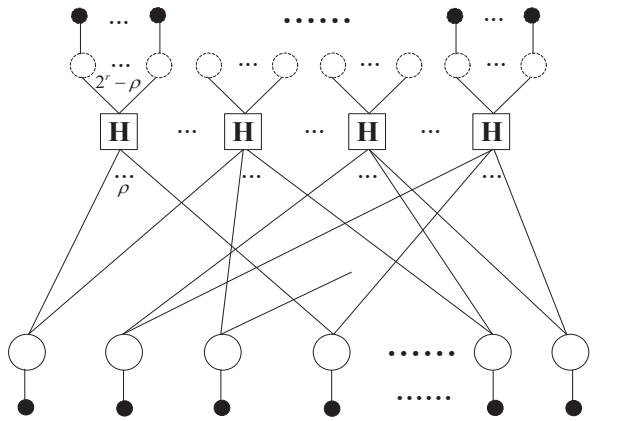

Fig. 4: Bipartite Tanner graph representation of a GLHR code with Hadamard constraints and repetition codes.

then it may be deduced that we have to satisfy that $R_{x_i} \leq R_i - R_{e_i} \leq R_i - C_{w_{i-1}} \leq C_{s_i}$ so that the message vector $\boldsymbol{X}_i$ is transmitted securely and reliably according to (10). The total secure information rate R of the data stream $\boldsymbol{M}$, which is transmitted by N frames, is given as follows:

$$R = \frac{R_p \sum_{i=2}^{N+1} k_i}{\sum_{i=2}^{N+1} n_{c_i}} = \frac{R_p \sum_{i=2}^{N+1} (k_2^{(i)} - k_1^{(i)})}{\sum_{i=2}^{N+1} w_i [n + m_2^{(i)}(2^{\rho-2} - \rho)]}, \tag{24}$$

where R_p is the code rate of the LDPC code C used in the precoding module of Fig. 2.

The entire encoding process of the proposed JEEC coding scheme is summarized in Algorithm 1. In conclusion, we have constructed a new class of low-rate JEEC codes having flexible code parameters based on secrecy-LDPC codes and the proposed GLHR codes.

Algorithm 1 Encoding of the constructed JEEC codes

1: The ciphertext $\boldsymbol{Y}$ is encoded into the codeword $\boldsymbol{X}$ of the LDPC code C.
2: For $1 < i \leq N+1$, the i-th part $\boldsymbol{X_i}$ of $\boldsymbol{X}$ is encoded one randomly selected codeword $\mathbf{c}^{(i)}$ of the LDPC code $C_2^{(i)}$ satisfying (19).
3: For $1 < i \leq N+1$ and $0 \leq l < m_2^{(i)}$, the first $\rho - 1$ codeword bits connected with each CN of the LDPC code $C_2^{(i)}$ is encoded into one codeword $\mathbf{a}_l^{(i)}$ of a $(2^r, r+1)$ systematic Hadamard code with the order of $r = \rho - 2$. Then, parity bit sequence $\mathbf{b}_l^{(i)}$ of $\mathbf{a}_l^{(i)}$ is successively attached to $\mathbf{c}^{(i)}$ to obtain the codeword $\hat{\mathbf{c}}^{(i)} = (\hat{c}_0^{(i)}, \hat{c}_1^{(i)}, \ldots, \hat{c}_{N_L^{(i)}-1}^{(i)}) = (\mathbf{c}^{(i)}, \mathbf{b}_0^{(i)}, \mathbf{b}_1^{(i)}, \ldots, \mathbf{b}_{m_2^{(i)}-1}^{(i)})$.
4: For $1 < i \leq N+1$ and $0 \leq j < N_L^{(i)}$, if $\hat{c}_j^{(i)} = 0$, $\hat{c}_j^{(i)}$ is mapped to $\mathbf{R}_0^{(i)}$; otherwise $\hat{c}_j^{(i)}$ is mapped to $\mathbf{R}_1^{(i)}$, to generate the codeword $\boldsymbol{C_i} = (\boldsymbol{C_{i,0}}, \boldsymbol{C_{i,1}}, \ldots, \boldsymbol{C_{i,N_L^{(i)}-1}})$ of the GLHR code $\tilde{C}_2^{(i)}$.
5: For $1 < i \leq N+1$, each encoded result $\boldsymbol{C_i}$ of the JEEE coding scheme is transmitted to Bob, successively.

B. Joint Decoding of the Proposed JEEC Codes

Given the hostile nature of the quantum channel, only a fraction of the photons associated with each transmitted sequence $\boldsymbol{C_i}$ can be received by Bob, and the received photons may also have errors. Recall that the reception rate Q^{Bob} of Bob as well as the bit-error rate e between Alice and Bob was defined in Section II. Bob successively receives N sequences of $\boldsymbol{C_i'} = (\boldsymbol{C'_{i,0}}, \boldsymbol{C'_{i,1}}, \ldots, \boldsymbol{C'_{i,N_L^{(i)}-1}})$ from the demodulator, where we have $1 < i \leq N+1$. The detailed description of the joint decoding algorithm conceived for our proposed JEEC code is given as follows.

First, Bob successively decodes each received sequence $\boldsymbol{C_i'}$ to obtain the decoded message sequence $\boldsymbol{X_i'}$ of $\boldsymbol{X_i}$ for $1 < i \leq N+1$. Since $\boldsymbol{C_i}$ is obtained by mapping each codeword bit $\hat{c}_j^{(i)}$ in $\hat{\mathbf{c}}^{(i)} = (\hat{c}_0^{(i)}, \hat{c}_1^{(i)}, \ldots, \hat{c}_{N_L^{(i)}-1}^{(i)})$ to a single codeword of the $(w_i, 1)$ repetition code, the original log-likelihood ratio (LLR) sequence $\mathbf{U}_i = (U_{i,0}, U_{i,1}, \ldots, U_{i,N_L^{(i)}-1})$ of the corresponding $\hat{\mathbf{c}}^{(i)}$ is expressed as

$$U_{i,j} = \ln \frac{\Pr(\boldsymbol{C'_{i,j}} | \hat{c}_j^{(i)} = 0)}{\Pr(\boldsymbol{C'_{i,j}} | \hat{c}_j^{(i)} = 1)} = \ln \frac{(1-e)^{t_{0,j}} \cdot e^{t_{1,j}}}{(1-e)^{t_{1,j}} \cdot e^{t_{0,j}}} = (t_{0,j} - t_{1,j}) \ln \frac{1-e}{e}, \tag{25}$$

where $1 < i \leq N+1$ and $0 \leq j < N_L^{(i)}$. The LLR sequence $\mathbf{U}_i$ represents the reliability of the original messages invoked for decoding the codeword $\hat{\mathbf{c}}^{(i)}$ of the $(N_L^{(i)}, k_2^{(i)})$ LH code during the i-frame. The LDPC-Hadamard decoder designed for decoding the LH code is presented in [25], which iteratively uses the message-passing algorithm at the VN update and the *a posteriori probability* (APP) decoding of the Hadamard codes at the HCN update. By using the LDPC-Hadamard decoder presented in [25] and the LLR sequence $\mathbf{U}_i$, Bob extracts the decoded sequence $z^{(i)}$ corresponding to Alice's randomly chosen codeword $\mathbf{c}^{(i)}$ of the LDPC code $C_2^{(i)}$, where $1 < i \leq N+1$.

Next, Bob computes the product

$$\boldsymbol{X_i'} = \tilde{\mathbf{H}}_2^{(i)} (z^{(i)})^T \tag{26}$$

for obtaining the estimated $\boldsymbol{X_i'}$ of the message $\boldsymbol{X}_i$, where $1 < i \leq N+1$. Finally, Bob decodes the sequence $\boldsymbol{X'} = (\boldsymbol{X_2'}, \boldsymbol{X_3'}, \ldots, \boldsymbol{X'_{N+1}})$ of length k for recovering the ciphertext

TABLE III: All notations in the proposed JEEC coding scheme

C	(k, kR_p) LDPC code of code length k, information length kR_p and code rate R_p
$\mathbf{H}$	$(k - kR_p) \times k$ parity-check matrix of C
$\boldsymbol{X}$	one codeword of C and $\boldsymbol{X}$ is divided into N parts
$\boldsymbol{X_i}$	the i-th part of $\boldsymbol{X}$ for $1 < i \leq (N+1)$
k_i	length of $\boldsymbol{X_i}$, $\sum_{i=2}^{N+1} k_i = k$
$\mathbf{B}$	$m_r \times n$ parity-check matrix of a rate-compatible LDPC code with row weight ρ
$\mathbf{H}_1^{(i)} = \begin{bmatrix} \mathbf{H}_2^{(i)} \\ \bar{\mathbf{H}}_2^{(i)} \end{bmatrix}$	$m_1^{(i)} \times n$ submatrix of $\mathbf{B}$, $k_i < m_1^{(i)} \leq m_r$
$\mathbf{H}_2^{(i)}$	$m_2^{(i)} \times n$ above submatrix of $\mathbf{H}_1^{(i)}$, $m_2^{(i)} = m_1^{(i)} - k_i$
$\bar{\mathbf{H}}_2^{(i)}$	$k_i \times n$ below submatrix of $\mathbf{H}_1^{(i)}$
$k_1^{(i)}$	$k_1^{(i)} = n - m_1^{(i)}$
$k_2^{(i)}$	$k_2^{(i)} = n - m_2^{(i)} = k_i + k_1^{(i)}$
$\mathbf{h}_l = (h_{l,0}, h_{l,1}, \ldots, h_{l,n-1})$	the l-th row of $\mathbf{H}_2^{(i)}$, $0 \leq l < m_2^{(i)}$
$N_l = \{j : 0 \leq j < n, h_{l,j} \neq 0\}$	index set for each row l of $\mathbf{H}_2^{(i)}$, $0 \leq l < m_2^{(i)}$
j_l	maximum value in N_l, i.e., the last index in N_l
ρ	constant row weight of $\mathbf{H}_2^{(i)}$
$C_2^{(i)}$	$(n, k_2^{(i)})$ LDPC code defined by the null space of $\mathbf{H}_2^{(i)}$
$\mathbf{c}^{(i)} = (c_0^{(i)}, c_1^{(i)}, \ldots, c_{n-1}^{(i)})$	one codeword of $C_2^{(i)}$
r	$r = \rho - 2$
$\mathbf{a}_l^{(i)} = (a_{l,0}^{(i)}, a_{l,1}^{(i)}, \ldots, a_{l,2^r-1}^{(i)})$	one codeword of a $(2^r, r+1)$ systematic Hadamard code with the order of r
$\mathbf{b}_l^{(i)}$	parity bit sequence including all parity bits (except the last parity bit $a_{l,2^r-1}^{(i)}$) in $\mathbf{a}_l^{(i)}$
$\mathbf{H}_{h,r} = [\mathbf{p}_0, \mathbf{p}_1, \ldots, \mathbf{p}_{2^r-1}]$	$(2^r - r - 1) \times 2^r$ parity-check matrix of a $(2^r, r+1)$ systematic Hadamard code
$\Lambda = \{0, 1, 2, 4, \ldots, 2^{r-1}, 2^r - 1\}$	index set of $\lvert\Lambda\rvert = r + 2$ elements
$\Lambda^{\complement} = \{0, 1, 2, 3, \ldots, 2^r - 1\} \backslash \Lambda$	index set of $\lvert\Lambda^{\complement}\rvert = 2^r - r - 2$ elements
$N_L^{(i)}$	$N_L^{(i)} = n + m_2^{(i)}(2^r - r - 2)$
$\hat{C}_2^{(i)}$	$(N_L^{(i)}, k_2^{(i)})$ GLDPC code formed by $C_2^{(i)}$ and $(2^r, r+1)$ Hadamard codes
$\hat{\mathbf{H}}_2^{(i)}$	$m_2^{(i)}(2^r - r - 1) \times N_L^{(i)}$ parity-check matrix of $\hat{C}_2^{(i)}$
$\hat{\mathbf{c}}^{(i)} = (\hat{c}_0^{(i)}, \hat{c}_1^{(i)}, \ldots, \hat{c}_{N_L^{(i)}-1}^{(i)})$	one codeword of $\hat{C}_2^{(i)}$
$\mathbf{R}_0^{(i)} = (R_{0,0}^{(i)}, R_{0,1}^{(i)}, \ldots, R_{0,w_i-1}^{(i)})$	all zero codeword of the $(w_i, 1)$ repetition code, i.e., $R_{0,t}^{(i)} = 0$ for $0 \leq t < w_i$
$\mathbf{R}_1^{(i)} = (R_{1,0}^{(i)}, R_{1,1}^{(i)}, \ldots, R_{1,w_i-1}^{(i)})$	all one codeword of the $(w_i, 1)$ repetition code, i.e., $R_{1,t}^{(i)} = 1$ for $0 \leq t < w_i$
n_{c_i}	$n_{c_i} = w_i N_L^{(i)}$
$\tilde{C}_2^{(i)}$	$(n_{c_i}, k_2^{(i)})$ GLHR code of code length n_{c_i} and rate $R_{\text{GLHR}}^{(i)} = k_2^{(i)}/n_{c_i}$
$\tilde{\mathbf{H}}_2^{(i)}$	parity-check matrix of $\tilde{C}_2^{(i)}$
$\boldsymbol{C_i} = (\boldsymbol{C_{i,0}}, \boldsymbol{C_{i,1}}, \ldots, \boldsymbol{C_{i,N_L^{(i)}-1}})$	one codeword of $\tilde{C}_2^{(i)}$
$\boldsymbol{C_i}' = (\boldsymbol{C'_{i,0}}, \boldsymbol{C'_{i,1}}, \ldots, \boldsymbol{C'_{i,N_L^{(i)}-1}})$	received sequence of length n_{c_i} from the demodulator in the i-th frame
$\boldsymbol{C'_{i,j}} = (y_{j,0}^{(i)}, y_{j,1}^{(i)}, \ldots, y_{j,w_i-1}^{(i)})$	$y_{j,t}^{(i)}$ is equal to 0, ? or 1, with "?" representing an erasure for $0 \leq t < w_i$
$t_{0,j} \triangleq \lvert\{y_{j,t}^{(i)} = 0 \lvert 0 \leq t < w_i\}\rvert$	the number of "0" values in $\boldsymbol{C'_{i,j}}$
$t_{1,j} \triangleq \lvert\{y_{j,t}^{(i)} = 1 \lvert 0 \leq t < w_i\}\rvert$	the number of "1" values in $\boldsymbol{C'_{i,j}}$
$\mathbf{U}_i = (U_{i,0}, U_{i,1}, \ldots, U_{i,N_L^{(i)}-1})$	original log-likelihood ratio sequence of the corresponding $\hat{\mathbf{c}}^{(i)}$
$\boldsymbol{z}^{(i)}$	decoding result of $\mathbf{c}^{(i)}$
$\boldsymbol{X}' = (\boldsymbol{X_2}', \boldsymbol{X_3}', \ldots, \boldsymbol{X'_{N+1}})$	$\boldsymbol{X_i'}$ is decoding result of $\boldsymbol{X_i}$ for $1 < i \leq N+1$
$\boldsymbol{X}'' = (\boldsymbol{X_2}'', \boldsymbol{X_3}'', \ldots, \boldsymbol{X''_{N+1}})$	decoding result of $\boldsymbol{X}$

TABLE IV: Code parameters of all codes in the simulation examples

Parameters	N	k	R_p	n	k_2	w_i	w_p	w_i'
Example 1	100	50000	0.985	1000	500	63	384	64
Example 2	25	50000	0.985	4000	2000	61	372	
						131	792	
Example 3			1	4000	2000			

$\boldsymbol{Y}$ based on the (k, kR_p) LDPC code C by the scaling Min-Sum (MS) algorithm of [48]. The entire joint decoding of the proposed JEEC coding scheme is summarized in Algorithm 2.

Algorithm 2 Decoding of the constructed JEEC codes

1: For $1 < i \leq N+1$, initialize the original LLR sequence $\mathbf{U}_i$ using (25).
2: For $1 < i \leq N+1$, each LLR sequence $\mathbf{U}_i$ is decoded by using the LDPC-Hadamard decoder [25] to obtain the decoded sequence $\boldsymbol{z}^{(i)}$.
3: For $1 < i \leq N+1$, if $\boldsymbol{z}^{(i)}(\mathbf{H}_2^{(i)})^T = \mathbf{0}$, let $f_i = 1$; otherwise $f_i = 0$.
4: For $1 < i \leq N+1$, compute $\boldsymbol{X_i'}$ using (26) to obtain the decoded sequence $\boldsymbol{X}' = (\boldsymbol{X_2'}, \boldsymbol{X_3'}, \ldots, \boldsymbol{X'_{N+1}})$.
5: If $\boldsymbol{X}'\mathbf{H}^T = \mathbf{0}$, exit decoding and output the ciphertext $\boldsymbol{Y}$; otherwise, go to Step 6.
6: Decode $\boldsymbol{X}' = (\boldsymbol{X_2'}, \boldsymbol{X_3'}, \ldots, \boldsymbol{X'_{N+1}})$ by using the scaling Min-Sum algorithm [48] to obtain the decoded sequence $\boldsymbol{X}'' = (\boldsymbol{X_2''}, \boldsymbol{X_3''}, \ldots, \boldsymbol{X''_{N+1}})$ of $\boldsymbol{X}'$.
7: For $1 < i \leq N+1$, if $f_i = 1$, let $\boldsymbol{X_i''} = \boldsymbol{X_i'}$.
8: If $\boldsymbol{X}''\mathbf{H}^T = \mathbf{0}$, exit decoding and output the ciphertext $\boldsymbol{Y}$; otherwise, exit decoding and indicate failure.

V. Simulation and System Implementation

In this section, we compare the reliability and secure information rate of the proposed low-rate JEEC codes to those of the scheme conceived in [22]. We will show that our JEEC coding scheme significantly improves both the reliability and the communication distance of QSDC compared to those of other low-rate codes. Moreover, the experimental results characterize the proposed QSDC framework.

A. Simulation Results

For the sake of convenience, in this section, we assume that the capacities C_{m_i} and C_{w_i} of each frame are the same as C_m and C_w. A time-varying C_{w_i} will be considered in a practical system experiment later in more detail for each frame according to a different $\widetilde{e}$. The parameters of all codes in the next examples are listed in Table IV.

First, we only compare the reliability of the proposed JEEC coding scheme to that of other low-rate codes of similar code rates and lengths, such as the *concatenation of LDPC codes with pseudorandom sequences* (LPS) used in [22]. Simulations are conducted for transmission over the cascaded channel model consisting of a BEC and a BSC, which is considered to be a realistic main quantum channel model for the QSDC system defined in Section II. Let Q^{Bob} be the reception rate of

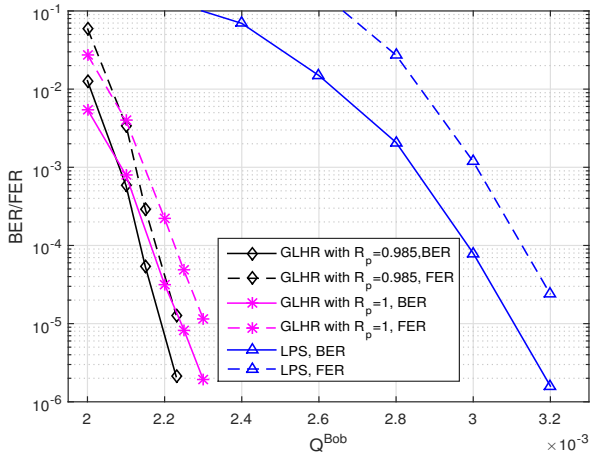

Fig. 5: BERs/FERs of the GLHR code with $R_p = 0.985$, the GLHR code with $R_p = 1$ and the LPS code.

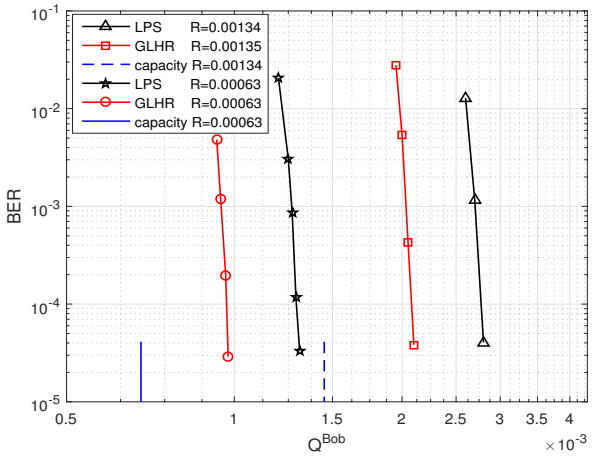

Fig. 6: BERs of the constructed GLHR and LPS codes with various code parameters.

Bob; then, the erasure probability of the BEC is $1-Q^{Bob}$. The error probability e of the BSC is set to 0.01 in the simulations. Let us furthermore use $k_2 = k_2^{(i)} = k_i = k/N$, and let the code length n_{c_i} of each sequence $\boldsymbol{C}_i$ transmitted over the main quantum channel be equal to the same value n_c. Then, the total information rate R of the data stream $\boldsymbol{M}$ transmitted through the proposed QSDC framework is equal to $R = \frac{R_p k}{N n_c} = \frac{R_p k_2}{n_c}$.

Example 1: Let $k = 50,000$ and $N = 100$. Thus, $k_2^{(i)} = k_2 = k_i = 500$. Let the $(n, k_2^{(i)})$ LDPC code $C_2^{(i)}$ defined in Section IV be a $(1000, 500)$ LDPC code of code rate 0.5 and a constant row weight 6, which is constructed by using the progressive edge growth (PEG) algorithm [49]. Let the LDPC code C in the precoding module be a $(50000, 49250)$ LDPC code of rate $R_p = 0.985$ and a constant column weight 3 using the PEG algorithm. The LDPC code $C_2^{(i)}$ is extended to the GLHR code in each frame. The order of the Hadamard codes in the GLHR code constructed is equal to 4, and the length w_i of the repetition codes is set to 63. Hence, the codeword length of the constructed GLHR code in each frame is equal to 378,000. The actual message rate R of the JEEC code based on the GLHR code and the precoding code C is 0.001303. Finally we set the maximum number $I_{\max}$ of iterations for the LDPC-Hadamard decoder to 50 for decoding the GLHR code and the $I_{\max}$ of the scaling MS algorithm [48] to 90 for decoding the precoding code.

In this example, we further consider the JEEC coding scheme without the precoding module, i.e., the rate R_p is equal to 1. For comparison, the LDPC code $C_2^{(i)}$ is respectively extended to a LPS code based on pseudorandom sequences of length $w_p = 384$ and one GLHR code based on Hadamard codes of order 4 and repetition codes of length $w_i^{'} = 64$ in each frame. The codeword lengths of both these two codes are 384,000. Hence, the actual information rates R of the proposed JEEC codes (without precoding) based on the GLHR code and on the LPS code are both 0.001302. Let us use $I_{\max} = 50$ for the LDPC-Hadamard decoder for decoding this GLHR code. The LPS code is decoded by the scaling MS algorithm using $I_{\max} = 100$. As shown in Fig. 5, the GLHR code conceived with precoding outperforms the GLHR code without it at the bit error rate (BER) of 10^{-6} and the frame error rate (FER) of 10^{-5}. Moreover, both GLHR codes have better performance than the LPS code.

Example 2: Let $N = 25$ and the precoding code C be a $(50000, 49250)$ LDPC code of rate $R_p = 0.985$ identical to that constructed in Example 1, using the parameters of Table IV. Let us also consider a $(4000, 2000)$ random MacKay LDPC code [50] of rate 0.5 with column weight 3 and row weight 6 [50] as the LDPC code $C_2^{(i)}$. This LDPC code is used for constructing the GLHR and LPS codes, respectively. The lengths w_i of the repetition codes are chosen to be 61 and 131 to construct the $(1464000, 2000)$ GLHR code of rate 0.00137 and the $(3144000, 2000)$ GLHR code of rate 0.00064, respectively. Hence, the actual information rates R of the proposed JEEC codes with precoding based on the $(1464000, 2000)$ GLHR code and the $(3144000, 2000)$ GLHR code are 0.00135 and 0.00063, respectively. The lengths w_p of the pseudorandom sequences are chosen to be 372 and 792 for constructing the $(1488000, 2000)$ LPS code (without precoding) of rate $R = 0.00134$ and the $(3168000, 2000)$ LPS code (without precoding) of rate $R = 0.00063$, respectively. We set $I_{\max} = 30$ for the LDPC-Hadamard decoder for decoding the GLHR code and $I_{\max} = 30$ for the scaling MS algorithm [48] for decoding the precoding code C. We set $I_{\max} = 65$ for the scaling MS algorithm for decoding the LPS codes. As expected, the proposed GLHR codes perform better than the LPS codes for similar codeword lengths and rates as seen in Fig. 6. Moreover, our JEEC codes based on the GLHR codes are capable of operating close to the corresponding channel capacity of the main channel at these low code rates.

Next, we consider the secure information rate of the proposed JEEC coding scheme for transmission over a practical quantum channel, which has been considered in [22]. The parameters of this quantum channel are the same as those in [22]: the initial total channel loss is 24.5 dB at a distance of a 0 kilometer fiber with an initial received rate Q^{Bob} of 0.00345 at Bob's side. And the gap between Q^{Bob} and Q^{Eve} is set to 2.4. Each kilometer of increased distance corresponds to 0.4

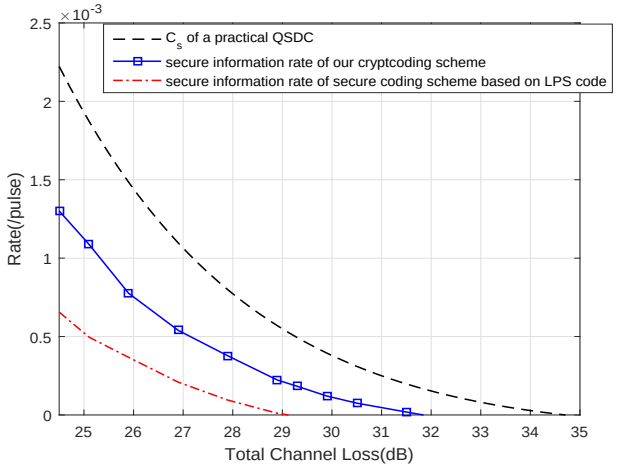

Fig. 7: Secure information transmission rates of the proposed JEEC coding scheme and the secure coding based on LPS codes for a practical QSDC system, without the consideration of the loss caused by the delay fiber.

dB of increased total channel loss imposed by the concatenated forward and backward quantum channel transmission between Alice and Bob. The bit-error rate e between Alice and Bob over this quantum channel is usually approximately 0.6% [22]. In our simulations, the bit-error rate e is set to 1%. The capacity of the wiretap channel C_w is given by (11). Let $k_2^{(i)} = k_2$, $k_1^{(i)} = k_1$, and $k_i = k_2 - k_1$ in our JEEC coding scheme. The code length n_{c_i} of each transmitted sequence $\boldsymbol{C}_i$ over the main channel is equal to the same value n_c. According to (21) and (23), it is necessary that we have $R_i = \frac{k_2}{n_c} < C_m$ and $R_{e_i} = \frac{k_1}{n_c} \geq C_w$ for maintaining the desired security vs reliability trade-off. According to (24), the secure information rate R of our scheme is equal to

$$R = R_p(k_2 - k_1)/n_c. \tag{27}$$

Example 3: We compare the secure information rate of our proposed JEEC coding scheme and the secure coding based on the LPS codes presented in [22] for transmission over the above practical QSDC system, using the parameters of Table IV. In this example, the precoding rate R_p of the (k, kR_p) LDPC code C is set to 1. The secure coding module of the proposed JEEC coding scheme is constructed based on a rate-compatible LDPC code of a constant block length 4000 and row weight 6. We fix the value of k_2 to 2000 for the various reception rates Q^{Bob}, so the LDPC code $C_2^{(i)}$ is a $(4000, 2000)$ LDPC code of rate 0.5 and row weight 6. We set $I_{\max} = 50$ for the LDPC-Hadamard decoder. The optimal lengths of the repetition codes used in the JEEC coding scheme are separately obtained by computer search for various Q^{Bob} values when the BER of the LDPC-Hadamard decoding is about 10^{-5}.

The secure coding based on LPS codes [22] is constructed based on the $(4000, 2000)$ random MacKay LDPC code [50] of rate 0.5 used in Example 2 of Table IV. We set $I_{\max} = 65$ for the scaling MS algorithm for decoding the LPS codes. The optimal lengths of the pseudo-random sequences invoked for the secure coding based on LPS codes are also obtained by a computer search for various Q^{Bob} values when the BER of the MS decoding is about 10^{-5}. As shown in Fig. 7, the secure information rate area of the proposed JEEC coding scheme is much larger than that of the secure coding in [22]. The secure information rate of our coding scheme is always higher than 0, if the total channel loss is lower than 32 dB. Hence, our scheme is capable of reliable and secure communication for a maximum communication distance of approximately 19 kilometers (km), while that of the coding scheme in [22] is only about 10 km. Furthermore, the difference between secrecy capacity and secure information rate decreases as the communication distance increases. For example, it is about 9×10^{-4} bit/pulse at 0 km (total loss 24.3 dB) and 2.5×10^{-4} bit/pulse at 14 km (total loss 29.9 dB). But the ratio of secure information rate and secrecy capacity also decreases as the communication distance increases. For example, it is about 0.591 at 0 km and 0.375 at 14 km.

B. System Implementation

We have implemented a verification experiment on the basis of the proposed protocol in an optical fiber system. We summarize the key experimental parameters in Table V and discuss them below. Meanwhile, the performance of our system has also been compared to [22].

An optical fiber based system is used for supporting the basic measurements and operations in the original DL04 scheme, which is an improved version of our previous work [22]. The main benefit of our new optical system is that we do not need a storage-delay line (quantum memory). The method of modulating a '0' or '1' bit onto a photon is based on the time-bin coding of [51]. We use a weak coherent pulse source having a wave length 1550 nm as the single-photon source. The pulse repetition frequency f of the laser can be set to less than 16 MHz. The attenuator sets the mean photon count to 0.1. A commercial fiber channel is used both for transmitting the quantum signal, with a loss of 0.2 dB/km, and the classical signals of the service channel between Alice and Bob. However, the service channel carries a classical optical signal, while the quantum channel carries single photons.

In a practical system, there is a time-varying C_w for each frame $\boldsymbol{C_i}$ according to the different $\widetilde{e}$ representing the qubit error rate of the eavesdropping detection module of Fig. 2. The average channel parameters associated with different communication distances (d km) are shown in Table V. The average secrecy capacity can be obtained from (5) and (11). The initial total loss at a distance of 0 km is 24.3 dB. We define the variable g as the ratio of $g = Q^{Eve}/Q^{Bob}$ for characterizing the channel, which can be determined by accounting for the losses in the system using the following equation,

$$g = 10^{L_B/10} = 10^{(L_{SPD}+L_f+L_b)/10} = 10^{[1.5+2.3+(0.2\times d)]/10}, \tag{28}$$

where L_B is the total loss of the quantum channel between Alice and Bob at a distance of d km. When the modulated photons are conveyed from Alice to Bob over the quantum channel, Eve is assumed to be as close to Alice as possible. Thus, g also depends on L_B, as seen in (28). $L_{SPD} = 1.5$ dB is the loss of the superconducting nanowire single-photon

TABLE V: Performance Comparison of Our QSDC Experiment System and the System in [22]

Experiment Systems	f (MHz)	d (km)	g	$\overline{e}$	$\overline{2\overline{e}}$	$\overline{Q^{Bob}}$	$\overline{C_s}$	$\overline{C_w}$	$\overline{R}$	$\overline{R_M}$ (bps)
DL04 System	1	1.5	2.57	0.0060	0.0165	0.00291	0.00184	0.00091	0.00005	50
QMF-DL04 System	1	1.5	2.57	0.0029	0.0070	0.00320	0.00261	0.00049	0.00177	1770
		6.0	3.16	0.0039	0.0081	0.00210	0.00157	0.00045	0.00102	1020
		13.0	4.37	0.0072	0.0087	0.00110	0.00069	0.00035	0.00043	430
		18.5	5.62	0.0096	0.0123	0.00068	0.00026	0.00037	0.00010	100

$\overline{*}$ represents the average value of "*".
The BER of information is required to be less than 1×10^{-5} in these two systems.

detector used in the system, $L_{\mathrm{f}} = 2.3$ dB is the fixed loss of the optical component and L_{b} is the loss of the optical fiber. In this experiment, the secure coding of the JEEC coding scheme is constructed based on a rate-compatible LDPC code having a constant block length of 4000 and a row weight 6 to match the varying C_{w_i}. The precoding rate R_p is 1. We set $I_{\max} = 50$ for the LDPC-Hadamard decoder.

This experimental system is capable of successfully transmitting voice, images, text and so on. The performance attained by our experimental system and by the system presented in [22] at different distances is shown in Table V. To demonstrate the advantages of the proposed QSDC framework, the pulse repetition frequency of the laser was set to $f = 1$ MHz, which is the same as that in [22]. Let us denote the actual average secure information rate by $\overline{R}$, while $\overline{R_M} = \overline{R} \cdot f$ is the message bits transmission rate per second on average. In [22], when $d = 1.5$ km, $\overline{R}$ is equal to 0.00005, while $\overline{C_s}$ is equal to 0.00184. Hence, there is a ratio of 0.00184/0.00005 = 36.8 between the information rate and secrecy capacity. Our experimental system achieves a maximum communication distance of approximately $d = 18.5$ km. In our system, when $d = 1.5$ km, we have $\overline{R} = 0.00177$ and $\overline{C_s} = 0.00261$. Hence, the rate-ratio is only 0.00261/0.00177 = 1.47, indicating that the proposed system approaches the secrecy capacity more closely. Moreover, the gain in terms of the secure information rate at 1.5 km between our system and the system in [22] is approximately 1770/50 = 35.4. We have also increased f to 16 MHz, and the information rate attained is in excess of 27 kbps at a distance of 1.5 km. Additionally, the pulse repetition frequency of the laser, f, can be further increased to 100 MHz and above. Last but not least, although [22] verifies the feasibility of a QSDC system, it is still a major challenge to implement a practical system relying on a quantum memory. Beneficially, this QSDC system dispenses with the dependence on quantum memory for the first time.

However, the secure information rate is still rather low - on the order of kbps. As mentioned above, the small Q^{Bob} is the real bottleneck, which results in a low capacity for the main channel. There are three main factors:

1) It results in many empty pulses (more than 90 %) by replacing the single-photon source with a weak coherent pulse source.
2) The optical components used for measurement introduce a further attenuation.
3) The qubits are attenuated by the fiber channel by 0.2 dB/km.

Fortunately, Q^{Bob} could be substantially improved by more efficient optical devices and simpler optical processing.

VI. Conclusions

A quantum-memory-free DL04 QSDC protocol has been proposed. This has solved one of the main obstacles in the way of the practical implementation of QSDC at the time of writing. The analysis indicates that our QMF-DL04-QSDC protocol is capable of improving the secure information rate, whilst enhancing the system's robustness. The design and optimization of this new rate-compatible low-rate JEEC coding scheme was detailed. It was shown to be approaching the secrecy capacity and be able to tolerate an extremely high loss of qubits. It is also adaptive to the time-varying nature of the wiretap quantum channel. Our numerical simulations revealed that the QMF-DL04-QSDC protocol relying on the dynamic JEEC coding scheme enhances the reliability of QSDC. Explicitly, it achieves a higher secure information rate as well as longer communication distance. In conclusion, we have demonstrated that practical QSDC is feasible for a practical long distance without the use of quantum memory.

Again, QKD requires both a quantum channel and a classical channel for key agreement, where information is transmitted in the form of ciphertext by relying on another classical communication session. By contrast, QSDC systems transmit their information directly over the quantum channel. Moreover, QSDC is capable of performing key distribution and lends itself to the design of other cryptographic protocols. Our numerical results reveal that the QMF QSDC protocol using the proposed dynamic JEEC coding scheme substantially improves the reliability of QSDC, whilst increasing the secure information rate as well as the communication distance.

Finally, we suggest several important tasks for future studies. First, we should improve the optical system design to reduce the deleterious channel effects. For instance, we should reduce the number of optical components to reduce the intrinsic attenuation caused by these components. Second, a higher pulse repetition frequency is required for increasing the secure information rate of the QSDC system. Third, there is still room for designing better coding schemes for further reducing the gap between the secure information rate and secrecy capacity.

Acknowledgements

The authors are very grateful to Editor and Reviewers for their comments and constructive suggestions, which help to enrich the content and improve the presentation of this paper. Helpful discussions with Dr. Ruoyang Qi are gratefully acknowledged.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Foundations of Computer Science*. IEEE, 1994, pp. 124–134.

[2] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett.*, vol. 79, no. 2, pp. 325–328, 1997.

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

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

[5] 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, 1978.

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

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *IEEE Int. Conf. Computers, Systems, Signal Processing.*, 1984.

[8] G. Long and X. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Phys.Rev. A*, vol. 65, no. 3, p. 032302, 2002; also see arXiv preprint quant-ph/0012056, 2000.

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

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

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

[12] 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, 2005.

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

[14] P. Niu, Z. Zhou, Z. Lin, Y. Sheng, L. Yin, and G. Long, "Measurement-device-independent quantum communication without encryption," *Sci. Bull.*, vol. 63, no. 20, pp. 1345–1350, 2018.

[15] Z. Zhou, Y. Sheng, P. Niu, L. Yin, G. Long, and L. Hanzo, "Measurement-device-independent quantum secure direct communication," *Sci. ChinaâĂŘPhys. Mech. Astron.*, vol. 63, no. 3, p. 230362, 2020.

[16] Z. Gao, T. Li, and Z. Li, "Long-distance measurement-device–independent quantum secure direct communication," *EPL (Eurpphys Lett.)*, vol. 125, no. 4, p. 40004, 2019.

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

[18] 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, 2017.

[19] J. Hu, B. Yu, M. Jing, L. Xiao, S. Jia, G. Qin, and G. Long, "Experimental quantum secure direct communication with single photons," *Light Sci. Appl.*, vol. 5, no. 9, p. e16144, 2016.

[20] Y. F. Pu, N. Jiang, W. Chang, H. X. Yang, C. Li, and L. M. Duan, "Experimental realization of a multiplexed quantum memory with 225 individually accessible memory cells," *Nat. Commun.*, vol. 8, p. 15359, 2017.

[21] E. O. Kiktenko, A. S. Trushechkin, C. C. W. Lim, Y. V. Kurochkin, and A. K. Fedorov, "Symmetric blind information reconciliation for quantum key distribution," *Phys. Rev. Applied*, vol. 8, no. 4, p. 044017, 2017.

[22] R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G. Long, "Implementation and security analysis of practical quantum secure direct communication," *Light Sci. Appl.*, vol. 8, no. 1, p. 22, 2019.

[23] 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, p. e26, 2019.

[24] I. B. Djordjevic, O. Milenkovic, and B. Vasic, "Generalized low-density parity-check codes for optical communication systems," *J. Lightw. Technol.*, vol. 23, no. 5, pp. 1939–1946, 2005.

[25] G. Yue, L. Ping, and X. Wang, "Generalized low-density parity-check codes based on Hadamard constraints," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1058–1079, 2007.

[26] Q. Li, X. Qu, L. Yin, and J. Lu, "Generalized Low-Density Parity-Check coding scheme with partial-band jamming," *Tsinghua Sci. Technol.*, vol. 19, no. 2, pp. 203–210, 2014.

[27] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Fifteen years of quantum LDPC coding and improved decoding strategies," *IEEE Access*, vol. 3, pp. 2492–2519, 2015.

[28] N. Bonello, S. Chen, and L. Hanzo, "Design of low-density parity-check codes," *IEEE Veh. Technol. Mag.*, vol. 6, no. 4, pp. 16–23, 2011.

[29] Z. Babar, S. X. Ng, and L. Hanzo, "Near-capacity code design for entanglement-assisted classical communication over quantum depolarizing channels," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 4801–4807, 2013.

[30] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, 1948.

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

[32] Z. Zhang, G. Zeng, N. Zhou, and J. Xiong, "Quantum identity authentication based on ping-pong technique for photons," *Phys. Lett. A*, vol. 356, no. 3, pp. 199–205, 2006.

[33] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.

[34] A. Subramanian, A. Thangaraj, M. Bloch, and S. W. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 585–594, Sep 2011.

[35] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Performance analysis and design of two edge-type LDPC codes for the BEC wiretap channel," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1048–1064, 2013.

[36] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215–228, 2014.

[37] 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 Conf. Wkshps*. IEEE, 2018, pp. 1–6.

[38] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J.Computer and System Sciences*, vol. 18, no. 2, pp. 143–154, 1979.

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

[40] H. Tyagi and A. Vardy, "Universal hashing for information-theoretic security," *Proc. IEEE*, vol. 103, no. 10, pp. 1781–1795, 2015.

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

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

[43] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using Polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, 2011.

[44] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1250–1276, 2002.

[45] L. Yin, C. Jiang, C. Jiang, N. Ge, L. Kuang, and M. Guizani, "A communication framework with unified efficiency and secrecy," *IEEE Wirel. Commun.*, vol. 26, no. 4, pp. 133–139, 2019.

[46] L. Yin and W. Hao, "Code-hopping based transmission scheme for wireless physical-layer security," *Wirel. Commin. Mob. Com.*, vol. 2018, 2018.

[47] Z. Chen, L. Yin, Y. Pei, and J. Lu, "Codehop: physical layer error correction and encryption with ldpc-based code hopping," *Sci. China-Inform. Sci*, vol. 59, no. 10, p. 102309, 2016.

[48] X.-Y. Hu, E. Eleftheriou, D.-M. Arnold, and A. Dholakia, "Efficient implementations of the sum-product algorithm for decoding LDPC codes," in *Proc. IEEE GlobeCom Conf.*, vol. 2. IEEE, 2001, pp. 1036–1036E.

[49] X. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth Tanner graphs," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 386–398, 2005.

[50] D. J. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 399–431, 1999.

[51] I. Marcikic, H. de Riedmatten, V. Scarani, H. Zbinden, N. Gisin *et al.*, "Femtosecond time-bin entangled qubits for quantum communication," *arXiv preprint quant-ph/0205144*, 2002.

Zhen Sun received his B.E. degree in electronic information science and technology from Tsinghua University (THU), Beijing, China, in 2016. Since 2016, he has been working towards the Ph.D. degree at the Department of Electronic Engineering, School of Information Science and Technology in Tsinghua University, Beijing, China. His research interests include error control codes and quantum secure communication systems.

Liyuan Song received the B.S. degree from Beiyou University (BUPT), Beijing, China, in 2014, in electronic and information engineering. Since 2014, she has been working towards the Ph.D. degree at the School of Electronic and Information Engineering, Beihang University (BUAA), Beijing, China. Her research interests are error-control codes of storage and communication systems.

Qin Huang received the B.E. and M.E. degrees in electrical engineering from Southeast University, Nanjing, China, in 2005 and 2007, respectively, and the Ph.D. degree in electrical engineering from the University of California at Davis, Davis, CA, USA, in 2011. He joined Link-A-Media Devices Corporation, Santa Clara, CA, USA, in 2011. He is currently a Professor at the School of Electronic and Information Engineering, Beihang University (BUAA), Beijing, China. He currently serves as an Associate Editor for the IEEE Transactions on Communications. His research interests include classical and modern coding theory, signal processing, and their applications on communications and storage systems.

Liuguo Yin (S'01-M'05) received the MEng and PhD degrees from Tsinghua University, Beijing, China, in 2002 and 2005, respectively. From March 2005 to March 2007, he was a research assistant with the School of Aerospace, Tsinghua University. From April 2007 to March 2008, he was an ERCIM postdoctoral fellow with the Norwegian University of Science and Technology (NTNU), Trondheim, Norway. Since 2009, he has been with the School of Information Science and Technology, Tsinghua University, where he is currently a professor. His research interests include channel coding, joint source-channel coding, aerospace communications, wireless multimedia communication systems, and quantum secure direct communications. He is a member of the IEEE communications society.

Gui-Lu Long is a professor at Tsinghua University. He received his B.S. degree from Shandong University in 1982 and his Ph.D. degree from Tsinghua University in 1987, and since then has been working in Tsinghua University. During 1989 and 1993, he was research fellow in the University of Sussex, UK. Notably among his various contributions, he proposed the theory of quantum secure direct communication in 2000, which one of the three major quantum secure communication theories; constructed a quantum exact search algorithm, sometimes called Grover-Long algorithm; and established the linear combination unitaries (LCU) method, which is widely used in quantum algorithm designs. He published more than 300 papers in refereed international journals. He is fellow of IoP (UK), fellow of APS (US). He served as President of Associations of Asian Pacific Physical Societies (2017âĂŞ2019), and Vice-chair of C13 of IUPAP (2015âĂŞ2017). His research interests include quantum communication and computing and optical microcavity.

Jianhua Lu (M'98-SM'07-F'15) received his B.S. and M.S. degrees from Tsinghua University, Beijing, China, in 1986 and 1989, respectively, and his Ph.D. degree in Electrical & Electronic Engineering from the Hong Kong University of Science & Technology, Hong Kong, China, in 1998. Since 1989, he has been with the Department of Electronic Engineering, Tsinghua University, where he currently serves as a professor. He is now a vice president of the National Natural Science Foundation of China. His research interests include broadband wireless communications, multimedia signal processing, and satellite communications. He has authored/co-authored over 300 referred technical papers published in international renowned journals and conferences and over 80 Chinese invention patents. He was also a recipient of the Best Paper Awards at the IEEE ICCCS 2002, China Comm. 2006, IEEE Embedded-Com 2012, IEEE WCSP 2015, IEEE IWCMC 2017 and IEEE ICNC 2019. Prof. Lu served as an Editor for IEEE Transactions on Wireless Communications from 2008 to 2011, and Program Committee Co-Chair, as well as, TPC member of many international conferences. He is now the Editor-in-Chief of China Communications. He is a member of Chinese Academy of Sciences, and a Fellow of IEEE.

Lajos Hanzo (http://www-mobile.ecs.soton.ac.uk, https://en.wikipedia.org/wiki/Lajos_Hanzo) (FIEEE'04, Fellow of the Royal Academy of Engineering (FREng), of the IET and of EURASIP) received his Master degree and Doctorate in 1976 and 1983, respectively from the Technical University (TU) of Budapest. He was also awarded the Doctor of Sciences (DSc) degree by the University of Southampton (2004) and Honorary Doctorates by the TU of Budapest (2009) and by the University of Edinburgh (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 PhD 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.