IEEE Open Journal of Vehicular Technology

Received 26 June 2025; accepted 18 July 2025. Date of publication 21 July 2025;
date of current version 20 August 2025. The review of this article was coordinated by Editor Xiaoli Xu.

Digital Object Identifier 10.1109/OJVT.2025.3591417

Short-Block Polar-Coded Reverse and Direct Reconciliation in CV-QKD

DINGZHAO WANG (Student Member, IEEE), XIN LIU (Student Member, IEEE), CHAO XU (Senior Member, IEEE), SOON XIN NG (Senior Member, IEEE), AND LAJOS HANZO (Life Fellow, IEEE)

School of Electronics and Computer Science, University of Southampton, SO17 1BJ Southampton, U.K.

CORRESPONDING AUTHORS: DINGZHAO WANG; CHAO XU (e-mail: dw9g20@soton.ac.uk; cx1g08@soton.ac.uk).

The work of Lajos Hanzo was supported in part by Engineering and Physical Sciences Research Council (EPSRC) Projects under Grant EP/Y037243/1, Grant EP/W016605/1, Grant EP/X01228X/1, Grant EP/Y026721/1, Grant EP/W032635/1, and Grant EP/X04047X/1 and in part by European Research Council's Advanced Fellow Grant QuantCom under Grant 789028.

ABSTRACT Continuous-variable quantum key distribution (CV-QKD) is a promising technique of supporting quantum-safe wireless networks in the emerging 6 G era, mapping quantum information onto the amplitude or phase of electromagnetic waves. However, conventional CV-QKD reconciliation methods often assume ideal classical side-information channels, which is an unrealistic scenario in practical deployments. To address this critical challenge, we propose a novel protection scheme integrating Polar and low-density parity-check (LDPC) codes. Specifically, Polar codes safeguard quantum transmissions due to their superior performance for short block lengths, while LDPC codes robustly protect the classical side information exchanged over auxiliary classical channels. We further enhance the CV-QKD performance by harnessing a soft-decision Polar decoding method combined with protocols specifically tailored for reverse reconciliation (RR) and direct reconciliation (DR). In the RR scheme, conceived decoding complexity is strategically distributed: Polar decoding is performed by Alice, and LDPC decoding by Bob, hence significantly reducing the computational demands compared to traditional schemes where both decoding processes are invoked at a single node. Simulation results validate the effectiveness of our approach, demonstrating that Polar codes consistently outperform LDPC codes in quantum transmission scenarios having short block lengths under 512 bits. These findings emphasize the strong potential of Polar coding-assisted CV-QKD in achieving secure and efficient quantum-safe control information transmissions, paving the way for practical implementation in next-generation wireless networks.

INDEX TERMS Continuous-variable quantum key distribution (CV-QKD), multidimensional reconciliation, polar code, secret key rate.

NOMENCLATURE

5G	Fifth-generation.
ARQ	Automatic repeat request.
BDMC	Binary discrete memoryless channel.
BI-AWGN	Binary input additive white Gaussian noise.
BLER	Block error rate.
BP	Belief propagation.
BPL	Belief propagation list.
CN	Check node.
CRC	Cyclic redundancy check.
CV-QKD	Continuous-variable quantum key distribution.
DR	Direct reconciliation.
DV-QKD	Discrete-variable quantum key distribution.
EPR	Einstein-Podolsky-Rosen.
EXIT	Extrinsic information transfer.
FEC	Forward error correction.
FSO	Free-space optical.
LDPC	Low-density parity-check.
ML	Maximum likelihood.
mMTC	Massive machine-type communication.
OTP	One-time pad.
PCM	Parity-check matrix.

QKD	Quantum key distribution.
QRNG	Quantum random number generator.
RR	Reverse reconciliation.
SC	Successive cancellation.
SCL	Successive cancellation list.
SKR	Secret key rate.
SNR	Signal-to-noise ratio.
SNU	Shot-noise unit.
URLLC	Ultra-reliable low-latency communication.
VN	Variable node.

I. INTRODUCTION

Quantum key distribution (QKD) is a fundamental quantum communication technique, enabling legitimate users, Alice and Bob, to securely establish a shared cipher key through quantum states transmitted over a quantum channel, thereby protecting their communication against potential eavesdroppers. This shared key can facilitate secure classical communication using the proven one-time pad (OTP) encryption method. The first QKD scheme, commonly known as the BB84 protocol, was proposed by Bennett and Brassard in 1984 [1]. QKD protocols can be categorized into two main types: discrete-variable QKD (DV-QKD) [1], [2], [3], [4], [5] and continuous-variable QKD (CV-QKD) [6], [7], [8], [9], [10]. DV-QKD maps information onto discrete variables, such as the polarization or phase of a single photon, whereas CV-QKD encodes information onto continuous variables, like the quadratures of coherent states. DV-QKD typically requires costly single-photon detectors and low-temperature environments, limiting its widespread practical implementation. By contrast, CV-QKD leverages cost-effective detectors commonly used in standard telecommunication systems operating at room temperature. The security of CV-QKD against general attacks has been rigorously characterized in [11], [12], [13], [14], and successful experimental implementations often utilize integrated silicon photonic chips, demonstrating potential for low-cost, portable quantum communication solutions [15].

In the early information reconciliation schemes, the Cascade algorithm proposed by Brassard and Salvail in 1993 [28] was widely used due to its simple implementation and high efficiency. However, it requires multiple interactions, which degrades its real-time performance and increases the probability of data loss. Therefore, reducing the number of interactions is essential. The cascade protocol applies parity checking to the original key segment multiple times and uses binary search to confirm and correct errors associated with odd-numbered indices of the key [28]. A more sophisticated protocol using Hamming codes, known as WINNOW, was introduced in 2003 [29]. As a further advance, a reconciliation protocol using low-density parity-check (LDPC) codes was proposed in [30], [31].

Briefly, often an LDPC code is harnessed as a benefit of its high reconciliation efficiency [27], [32], [33], but the design of its parity-check matrix (PCM) is challenging. By contrast, polar codes are easier to construct and they perform better than LDPC codes for short blocks. Therefore, Jouguet et al [34] and Nakassis et al [16] applied Polar codes for QKD reconciliation and their simulation results demonstrated improved QKD system performance. As a further innovation, in 2018, a successive cancellation based list (SCL) decoding algorithm was conceived for Polar code based QKD reconciliation by Yan [18], resulting in an improved secret key rate (SKR). The employment of short polar codes is beneficial because the block error rate (BLER) of long codes is typically higher than that of their short counterparts. This is because the probability of quantum domain errors increases with the key-length. Explicitly, in order to ensure quantum-safe transmission for next-generation wireless networks, the impact of block length should be taken into account, when different candidate coding schemes are considered for QKD information reconciliation.

Moreover, the aforementioned schemes assume error-free side information exchange between Alice and Bob over the auxiliary classical channel. However, in practice, realistic fading and noise-contaminated communication channels degrade the overall performance of QKD [27]. In the presence of channel noise, the direct reconciliation (DR) and reverse reconciliation (RR) schemes, which generate the key at Alice's side and Bob's side, respectively yield different QKD performance. At the time of writing, the development of fifth-generation (5G)-compliant variable-length coding schemes for DR and RR, communicating over imperfect quantum and classical channels remains an open challenge. Addressing this issue is crucial for conceiving next-generation wireless QKD networks.

Against this background, we propose new Polar-coded QKD information reconciliation protocols for protecting quantum transmission. By contrast, an LDPC scheme is used for protecting the side information transmitted over classical auxiliary channels in the face of fading and noise. Our novel contributions are contrasted to the state-of-the-art in Table 1, which are elaborated on as follows:

- Firstly, the binary input additive white Gaussian noise (BI-AWGN) quantum channel [27] is assumed, complemented by a realistic fading impaired and noise-contaminated channel for side information transmission over the classical auxiliary channel [27]. For mitigating the impairments, a novel double protection scheme is proposed, where Polar codes are invoked for protecting the quantum transmission against BI-AWGN, while LDPC codes are invoked to protect the transmission of frozen bit based side information against classical channel fading and noise. Soft-decision Polar decoding is applied to the quantum key based on the frozen bits for improving the overall QKD performance.
- Secondly, to balance the forward error correction (FEC) decoding complexity between Alice and Bob, we propose a new RR protocol. In this protocol, the quantum key is generated at Bob's side, while the frozen bits of the Polar code are generated at Alice's side. Consequently, the LDPC decoder used for the side information is placed at Bob's side, while the Polar decoder protecting the

TABLE 1. Novel Contributions of This Work in Comparison to the State-of-the-Art Schemes

Contributions	This work	[16]	[17]	[18]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[26]	[27]
CV-QKD (BI-AWGN)	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Rayleigh for the classical authenticated channel	✓												✓
Double protection for reconciliation scheme	✓												✓
Soft-decoding based frozen bits index	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Balanced decoding complexity between Alice and Bob	✓												✓
Performance improvement for short blocks	✓												
Performance evaluation in terms of DR and RR	✓												

quantum key is placed at Alice's side. This approach is in contrast to the conventional schemes, where both decoding tasks are typically assumed to be performed by Alice.

- Thirdly, to support double protection, while maintaining balanced complexity for DR, we propose a new DR protocol. In this protocol, the quantum key is generated at Alice's side, and the frozen bits' index is generated at Bob's side. These are then decoded at their respective opposite sides.
- Our simulation results demonstrate that Polar codes outperform LDPC codes in assisting quantum transmission in CV-QKD, when short blocks of 512 bits or less are considered. Furthermore, DR achieves a higher SKR over short distances, while RR supports a longer secure transmission distance in both the Polar- and the LDPC-assisted schemes. These findings are instrumental for enabling quantum-safe transmissions in next-generation wireless networks.

The remainder of this paper is structured as follows. Section II provides an introduction to polar coding applied to CV-QKD systems, including the fundamental concepts of polar encoders and decoders. In Section III, the DR and RR reconciliation strategies are discussed in detail, specifically highlighting the application of polar codes in CV-QKD reconciliation processes. Following this, Section IV proposes four polar-coded reconciliation schemes (Systems A to D), which explicitly contrast the performance of polar and LDPC codes both under ideal and practical classical channel conditions. Furthermore, the trade-offs in decoding complexities shared between Alice and Bob are also explored. The corresponding security analysis of DR and RR in terms of SKR is conducted in Section V. Then, in Section VI, simulation results are presented for each proposed system, with a focus on the comparative analyses of their BLER and SKR performances for polar and LDPC codes at different code lengths. Finally, Section VII concludes the paper with a summary of the key findings and outlines future research directions. The structure of the paper is illustrated in Fig. 1.

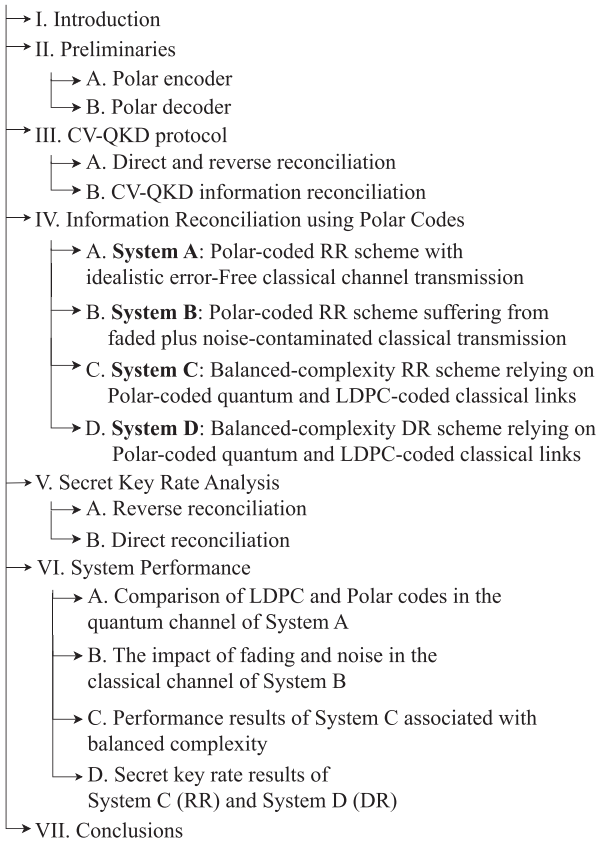

FIGURE 1. Structure of this paper.

II. PRELIMINARIES

Polar codes, invented by Arikan [35] have been shown to approach the Shannon limit in the Binary Discrete Memoryless Channel (BDMC). Compared to Turbo and LDPC codes, Polar codes have the advantage of deterministic construction, as well as lower encoding and decoding complexity. Moreover, Polar codes also have advantages in hardware implementation, since their hardware complexity increases only linearly with the code length [36].

A. POLAR ENCODER

After the polarized channel reliability estimation process, the channels will be split into K good channels and $(N-K)$ bad channels. Therefore the information bits will be transmitted over the good channels where the set of reliable channels is denoted by $\mathbf{A}$. The so-called frozen bits will be transmitted over the bad channels and $\mathbf{A}^{\mathbf{C}}$ is the complement of the set $\mathbf{A}$. Given the codeword length $\mathbf{N}$, the encoder of the Polar code is formulated as:

$$\mathbf{x}_1^N = \mathbf{u}_1^N \mathbf{G}_N, \tag{1}$$

where $\mathbf{u}_1^N$ denotes the bits to be transmitted, where both the information bits $\mathbf{u_A}$ and frozen bits $\mathbf{u_{A^C}}$ are included in $\mathbf{u}_1^N$, while $\mathbf{x}_1^N$ denotes the encoded bits. Furthermore, $\mathbf{G}_N$ denotes the Nth order generator matrix expressed as:

$$\mathbf{G}_N = \mathbf{B}_N \mathbf{F}_2^{\otimes n}, \tag{2}$$

where $\mathbf{B}_N$ denotes the bit-inverted permutation matrix, $\mathbf{F}_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ is the kernel matrix of the Kronecker product, and $\otimes^n$ denotes the n-th Kronecker power. The original codeword $\mathbf{u}_1^N$ and the generator matrix $\mathbf{G}$ can both be divided into two parts: $\mathbf{u}_1^N = (\mathbf{u_A}, \mathbf{u_{A^C}})$ and $\mathbf{G} = (\mathbf{G_A}, \mathbf{G_{A^C}})$. Thus, the encoder of the Polar code can be expressed as:

$$\mathbf{x}_1^N = \mathbf{u_A G_A} \oplus \mathbf{u_{A^C} G_{A^C}}, \tag{3}$$

where $\mathbf{u_{A^C}}$ denotes the frozen bits which are known to the decoder, while $\mathbf{G_A}$ and $\mathbf{G_{A^C}}$ are sub-matrices of the generator matrix $\mathbf{G}_N$. They contain the rows corresponding to the indices in the channel set $\mathbf{A}$ and its complement $\mathbf{A^C}$, respectively.

Finally, $\mathbf{B}_N$ of (2) is defined as:

$$\mathbf{B}_N = \mathbf{R}_N \left(\mathbf{I}_2 \otimes \mathbf{B}_{N/2} \right), \tag{4}$$

where $\mathbf{I}_2$ is an identity matrix, while $\mathbf{R}_N$ is designed to separate the odd-order and even-order elements of the input sequence. The odd-order elements are ranked first followed by the even-order elements, which can also be formulated as:

$$\begin{aligned} &(u_1, u_2, u_3, u_4, \ldots, u_N) \times \mathbf{R}_N = \\ &\quad (u_1, u_3, u_5, \cdots u_{N-1}, u_2, u_4, u_6, \ldots, u_N). \end{aligned} \tag{5}$$

B. POLAR DECODER

The low-complexity successive cancellation (SC) based decoder [35] is capable of approaching the channel capacity limit as the codeword length increases, but it exhibits relatively poor performance at short block length [35]. As a design, alternative, the SCL decoder strikes a flexible tradeoff between error-correction performance and complexity [37]. Additionally, a cyclic redundancy checking (CRC) pattern can be attached in order to check the successful decoding of the Polar codeword, which may be combined with either the SCL or belief propagation list (BPL) decoder [38]. Nonetheless, when a CRC code is concatenated, the overall throughput is reduced by both the CRC overhead and by the Polar code's frozen bits.

The SCL Polar decoding algorithm of [37], [39], was designed to enhance the performance of traditional SC decoding by exploring multiple candidate decoding paths in parallel. At each decoding step, both legitimate values (0 and 1) of an information bit are considered, effectively doubling the number of paths. To manage complexity, only the L most likely paths are retained based on a path metric, while significantly reducing the error rate. The simulation results of [39] have demonstrated that SCL decoding approaches the full-search Maximum Likelihood (ML) performance for short and moderate block lengths. For a carefully selected list size L, it becomes significantly more reliable than SC decoding. Due to its superior error correction capability and relatively low implementation complexity, SCL decoding has been widely adopted in modern communication systems, such as 5G. Explicitly it provides a compelling alternative to LDPC and Turbo codes, especially in short and moderate block-length scenarios.

III. CV-QKD PROTOCOL

The CV-QKD system connects a pair of legitimate parties, say Alice and Bob. Alice firstly prepares Gaussian-modulated coherent states and then transmits them to Bob over the quantum channel. Bob then randomly measures one of the quadratures with the aid of homodyne detection.[1] Furthermore, they both commence their classical post-processing by exchanging information over the classical public channel to extract the secret keys [27]. There are mainly two steps of the post-processing parts, namely the reconciliation and privacy amplification. For the reconciliation process, both Alice and Bob try to obtain the reconciled keys with the aid of FEC codes. After that, privacy amplification is used to further reduce the capability of eavesdropping.

A. DIRECT AND REVERSE RECONCILIATION

As an important step of post-processing, there are two types of reconciliation schemes, which are DR and RR based on the criteria that which party is viewed as the reference part. To elaborate further, for DR, Alice sends redundant side information to Bob for error correction, while keeping her data unmodified. However, DR is unable to generate a useful secure key, when the transmittance of a quantum channel is lower than 1/2 [40]. For example, Eve can effectively simulate a lossy transmission channel by capturing a portion of the light sent by Alice, while allowing the remaining portion to reach Bob with the aid of a beam splitter. In this scenario, Eve can extract a larger portion of the information destined for Bob, thereby preventing the legitimate parties from generating a secure key. This scenario is referred to as the '*3 dB loss limit*' [41] representing a transmittance of $< 1/2$.

By contrast, RR is a method conceived for overcoming the above 3 dB limit. For RR, Bob's raw key is used as the reference. He sends a key string to Alice, along with the redundant side information required for error correction. Alice then appropriately adjusts her bit string to match Bob's bit string. We will demonstrate that RR significantly extends the transmission distance. As a result, it is gradually becoming a canonical scheme in QKD.

B. CV-QKD INFORMATION RECONCILIATION

Fig. 2 portrays a CV-QKD system using a Polar code harnessed for supporting secret key distribution, which includes both quantum transmission and classical post-processing. After the quantum-domain transmission of coherent states

[1]Note that both the quadratures are needed when using heterodyne detection.

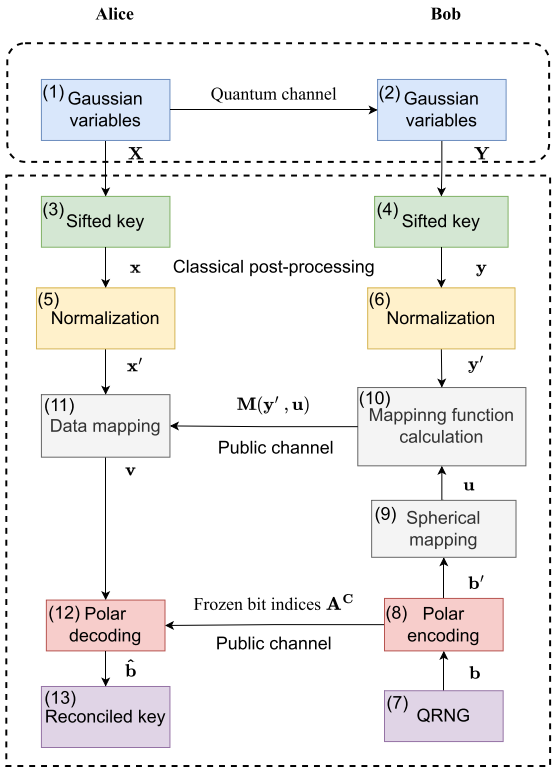

FIGURE 2. The RR based and polar coding-aided CV-QKD multidimensional reconciliation process.

conveyed by Gaussian variables from block (1) to (2), Alice and Bob sift their raw keys of blocks (3) and (4) that are correlated -i.e. similar- but potentially corrupted by channel impairments. Following this, multidimensional reconciliation is invoked between Alice and Bob relying on error correction. This step generates the reconciled key. The details of the reconciliation process are described below.

1) Alice and Bob firstly normalize their sifted key at the output of blocks (3) and (4) in the form of Gaussian variables at block (5) and (6) as follows:

$$\mathbf{x}' = \frac{\mathbf{x}}{\|\mathbf{x}\|} \quad \mathbf{y}' = \frac{\mathbf{y}}{\|\mathbf{y}\|}. \tag{6}$$

2) Then Bob generates a binary bit stream $\mathbf{b}$ by the quantum random number generator (QRNG) of block (7) in Fig. 2. The bit stream $\mathbf{b}$ is then Polar encoded into $\mathbf{b}'$ in block (8) and mapped onto the unit sphere in block (9) as follows[2] [42]:

$$\mathbf{u} = \left(\frac{(-1)^{b'_1}}{\sqrt{D}}, \frac{(-1)^{b'_2}}{\sqrt{D}}, \ldots, \frac{(-1)^{b'_D}}{\sqrt{D}} \right). \tag{7}$$

[2]We note that the dimension normally takes D=1,2,4,8. It was shown in [42] that D=8 has better BLER, hence D=8 is the default choice in this paper.

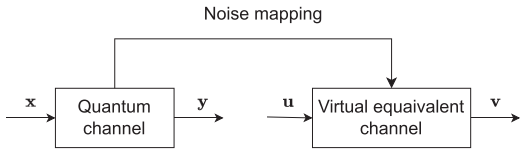

FIGURE 3. The relationship between the quantum channel and the virtual equivalent channel [27].

3) Bob generates a mapping function in block (10) based on the unit sphere $\mathbf{u}$ and its normalized Gaussian variables $\mathbf{y}'$ as follows [42]:

$$\mathbf{M}\left(\mathbf{y}', \mathbf{u}\right) = \sum_{d=1}^{D} \alpha_d \left(\mathbf{y}', \mathbf{u}\right) \mathbf{A}_d. \tag{8}$$

where we have $\alpha_d(\mathbf{y}', \mathbf{u}) = (\mathbf{A}_d \mathbf{y}')^T \mathbf{u}$ and $\mathbf{A}_d$ represents a family of D orthogonal matrices.

4) Bob shares $\mathbf{M}(\mathbf{y}', \mathbf{u})$ gleaned from block (10) with Alice together with $\mathbf{A}^{\mathbf{C}}$ of the Polar code's frozen bits prepared in block (8) as side information over the public channel.
5) Alice then applies the same mapping function in block (11) to her normalized data $\mathbf{x}'$ to get $\mathbf{v}$, which is a noisy version of $\mathbf{u}$. Based on this observation, it was demonstrated in [27] that the quantum channel of a CV-QKD system can be modelled by a BI-AWGN channel.
6) Finally, Alice carries out Polar decoding in block (12) and then obtains the reconciled key in block (13).

The relationship between the quantum channel and the equivalent channel is portrayed by Fig. 3. More explicitly, conventional QKD channel models often approximate the noise within the quantum channel as purely Gaussian, which primarily reflects quantum-domain uncertainties.

In satellite-based free-space optical (FSO) communication, quantum signals experience temperature and pressure fluctuations, leading to atmospheric turbulence. To model these realistic conditions, there is a hybrid noise model integrating quantum noise and AWGN. The received signal at the detector's input may be expressed as [43]: $Y = TX + Z$, where X denotes the modulated quantum signal received from the transmitter (Alice), T is the transmission coefficient accounting for beam spreading, scattering, and atmospheric attenuation, while Z represents the combined quantum and classical noise. This hybrid approach provides accurate modeling of practical satellite-based QKD systems, facilitating the evaluations of the SKR, channel capacity, and security analyses under realistic propagation conditions. This model is not used for simulations in our treatise, but it is worth further exploration in future research.

The aim of information reconciliation is to optimise the process of extracting the final secret key from the raw data exchanged between the legitimate parties, thus improving the SKR and increasing the transmission distance. There are two popular CV-QKD reconciliation techniques used in the DR and RR schemes, namely slice based reconciliation [44] and multidimensional reconciliation. More specifically, the

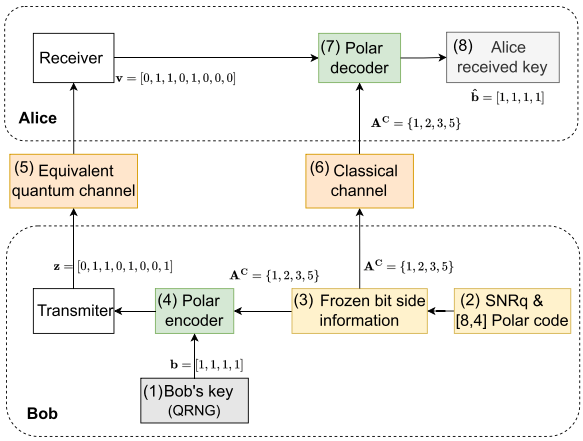

FIGURE 4. ***System A:*** **Polar-coded CV-QKD *RR* scheme, where the side information represented by the frozen bits is assumed to be *error-free* over the classical channel.**

slice based reconciliation is more suitable for relatively high signal-to-noise ratio (SNR), for example, above 0 dB (short transmission distance), while multidimensional reconciliation is popular for low SNRs spanning from −20 dB to 0 dB (long transmission distance) [45] for the AWGN channel.

Therefore, in this treatise, we consider multidimensional reconciliation based DR and RR schemes in order to achieve long-distance secret key distribution. In light of this, the associated quantum transmission is modelled by an equivalent classical BI-AWGN channel,[3] as detailed in [27], [46].

IV. INFORMATION RECONCILIATION USING POLAR CODES

In the FEC-based reconciliation part of CV-QKD systems, the main difference between the routinely used LDPC and the less well documented Polar codes is their different side information. For LDPC codes, the side information is typically the syndrome [27], while for Polar codes, it is constituted by the frozen bit information. Therefore, in this treatise, we focus our attention on the generation of frozen bit based side information for our Polar-coded reconciliation CV-QKD system, which is compared to the LDPC-coded reconciliation assisted CV-QKD benchmark system of [27], as detailed in the following performance analysis of Section VI. In order to explore a wide range of design options, we consider systems A, B, C and D exhibiting different trade-offs.

A. SYSTEM A: POLAR-CODED RR SCHEME WITH IDEALISTIC ERROR-FREE CLASSICAL CHANNEL TRANSMISSION

System A represents the SCL decoding based Polar-coded CV-QKD reconciliation scheme of Fig. 4. The error-free transmission of the side information, namely that of the frozen bit indices, is from Bob to Alice. The operation of System A is described below.

1) In block (1) of Fig. 4, Bob generates a truly random bit stream by the QRNG as the initial raw key. Here we use a simple half-rate [8,4] Polar code as our example, so Bob's initial raw key is denoted as $\mathbf{b} = [1, 1, 1, 1]$.
2) Since the equivalent channel is a BI-AWGN channel, Bob employs the Gaussian approximation method of [47] to estimate the channel reliability based on the quantum channel quality, which is characterized by SNR_q. Therefore, the information represented by SNR_q and N, K of the Polar code seen in block (2) is fed into block (3) to determine the frozen indices, which gives $\mathbf{A}^\mathbf{C} = \{1, 2, 3, 5\}$ at the output of block (3).
3) Then Bob applies Polar encoding in block (4) based on the information bits $\mathbf{b}$ at the output of block (1) and on the frozen indices $\mathbf{A}^\mathbf{C}$ output by block (3) using (1) to generate the non-systematically Polar encoded bit stream, represented as $\mathbf{z} = [0, 1, 1, 1, 1, 0, 0, 1]$.
4) Bob then transmits the bit stream $\mathbf{z} = [0, 1, 1, 1, 1, 0, 0, 1]$ to Alice through the equivalent quantum channel of block (5) in Fig. 4.
5) Furthermore, Bob also transmits the frozen bits of index $\mathbf{A}^\mathbf{C} = \{1, 2, 3, 5\}$ to Alice over the classical channel of block (6), which is assumed to be *error-free* in our System A to assist Alice in Polar decoding.
6) Alice receives a corrupted bit stream $\mathbf{v}$ from Bob via the equivalent quantum channel, which is the noisy version of $\mathbf{z}$. Observe that there is a single error in the last position, hence we have $\mathbf{v} = [0, 1, 1, 0, 1, 0, 0, 0]$. Then Alice performs Polar decoding in block (7) based on the frozen bit indices obtained through the classical channel.
7) Finally, Alice discards the frozen bits represented by the frozen bit indices and retains the remaining information bits as her key $\hat{\mathbf{b}} = [1, 1, 1, 1]$, shown at the output of block (8).

B. SYSTEM B: POLAR-CODED RR SCHEME SUFFERING FROM FADED PLUS NOISE-CONTAMINATED CLASSICAL TRANSMISSION

In practice, the classical channel is contaminated both by fading and noise, which may be mitigated by error correction coding. Therefore, we conceive System B portrayed by Fig. 5, where the separate LDPC encoder of block (9) and decoder of block (10) is used for protecting the side information transmission over the classical channel.[4] Explicitly, observe by comparing Figs. 4 and 5 that the blocks of (1)-(8) are identical,

[3]The equivalent virtual channel of the manuscript is used for performance analysis not for transmission.

[4]We note that LDPC-aided syndrome-based CV-QKD is dfferent to the LPDC-aided classical transmission. For LDPC-aided syndrome-based CV-QKD, the key and LDPC syndrome are transmitted through the quantum and classical channel, respectively. There is no correlation between the key and the syndrome, where the syndrome indicates the bit differences between the key and a legitimate LDPC codeword. In our proposed system, the LPDC code and its syndrome are replaced by a Polar code and frozen bits, respectively. By contrast, for the LDPC-aided classical transmission, a legitimate LDPC codeword is transmitted through a public channel. There is no need for any additional transmission of side information that is independent of this LDPC codeword.

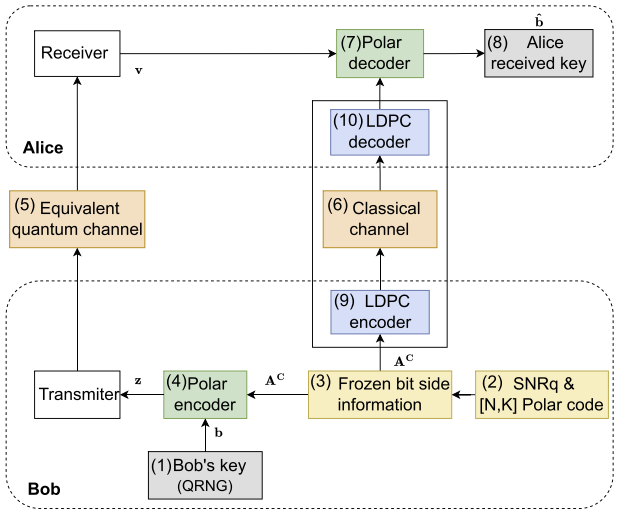

FIGURE 5. *System B:* **Polar-coded CV-QKD *RR* scheme, where LDPC is used to protect side information in *realistic classical channel with fading and noise*.**

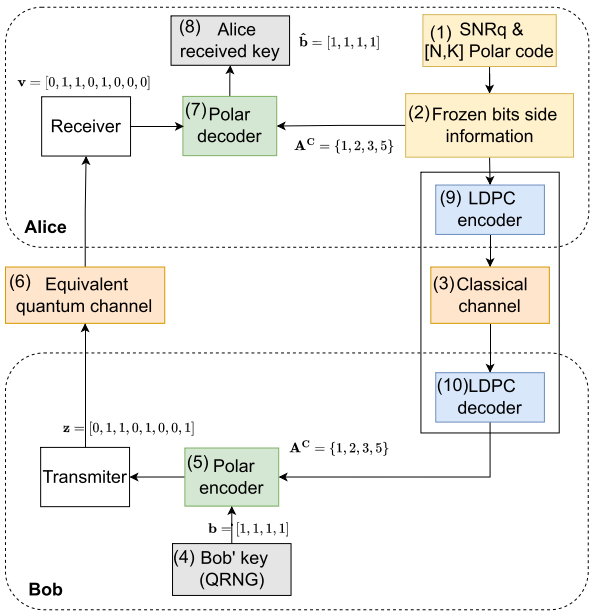

FIGURE 6. *System C:* **Polar-coded CV-QKD *RR* scheme with *double protection and balanced complexity*.**

but System B has the extra LDPC encoder and decoder of blocks (9) and (10) for protecting the realistic classical channel. In order to represent and transmit the frozen bit indices, each of them requires 10 bits for an $N = 1024$-bit codeword, which would require an excessive number of $10 \cdot 512 = 5120$ bits for a half-rate Polar code. Given that Polar codes require a block length which is an integer of power 2, LDPC codes are more flexible.

LDPC codes are a class of linear block codes characterized by a sparse PCM $\mathbf{H}$ of size $(N - K) \times N$, where N represents the block length and K denotes the number of information bits. The code rate is defined as $R = K/N$. For a regular LDPC code, each row of $\mathbf{H}$ contains exactly d_c ones, which corresponds to the check node (CN) degree, while each column has exactly d_v ones, representing the variable node (VN) degree. The PCM can be visualized as a bipartite Tanner graph [48], consisting of two distinct node sets: CNs and VNs. An edge connects VN v_j to CN c_i if and only if the matrix element $H_{i,j} = 1$. For example, consider a regular (10,5) LDPC code with VN degree $d_v = 2$ and CN degree $d_c = 4$. The corresponding PCM is given by:

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}. \quad (9)$$

We note that the PCMs used as benchmark of this work are constructed based on [49].

C. SYSTEM C: BALANCED-COMPLEXITY RR SCHEME RELYING ON POLAR-CODED QUANTUM AND LDPC-CODED CLASSICAL LINKS

To achieve a more balanced complexity and latency distribution between Alice and Bob, a more sophisticated scheme is conceived in Fig. 6, where a Polar code is harnessed for protecting the quantum link and an LDPC scheme protects the classical channel to achieve balanced complexity. Explicitly, in System C, Bob generates the key, which is protected by a Polar code for transmission over quantum channels, while Alice produces frozen-bit based side information, which is protected by a separate LDPC code for transmission over classical channel. This enables Alice and Bob to perform polar decoding and LDPC decoding separately, instead of both being performed on Alice's side, as in System B.

1) Firstly, Alice obtains the frozen bit indices $\mathbf{A}^{\mathbf{C}} = \{1, 2, 3, 5\}$ from block (2) based on the estimated channel SNR_q and on the N, K information defining the Polar code, as provided by block (1), using method of [47]. The frozen bit indices are first LDPC-encoded in block (9) and then transmitted to Bob through the realistic error-infested classical channel of block (3). Additionally, the frozen bit indices are also used to assist the Polar decoder at Alice's side in block (7). Note that, similarly to System B of Fig. 5, System C also has the extra LDPC encoder and decoder of blocks (9) and (10) of Fig. 6 for protecting the classical channel.
2) Bob generates the key $\mathbf{b} = [1, 1, 1, 1]$ by the true random QRNG in block (4) and forwards it to the Polar encoder. Bob then applies the Polar encoder of block (5) based on both the side information $\mathbf{A}^{\mathbf{C}}$ recovered after LDPC decoding in block (10) and the information bits

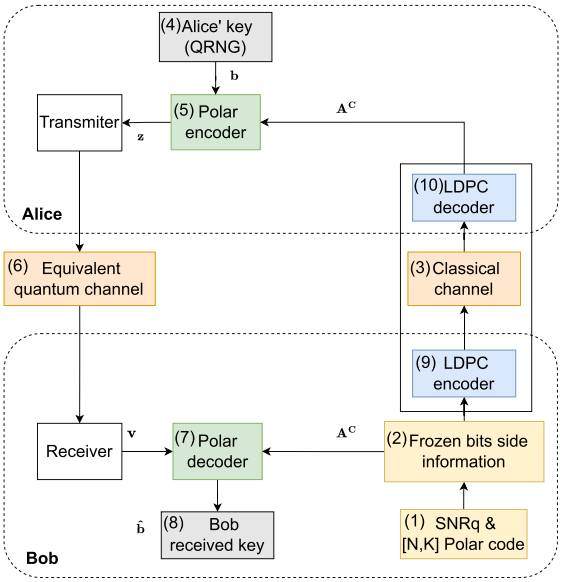

FIGURE 7. ***System D:*** **Polar-coded CV-QKD *DR* scheme with *double protection and balanced complexity*.**

b of block (4) using (1) to generate the Polar encoded bit stream of $\mathbf{z} = [0, 1, 1, 1, 1, 0, 0, 1]$.

3) Bob then transmits the bit stream $\mathbf{z} = [0, 1, 1, 1, 1, 0, 0, 1]$ to Alice through the equivalent quantum channel of block (6) in Fig. 6.
4) Furthermore, Alice performs Polar decoding of the received bit stream **v** in block (7) with the aid of the frozen bit indices passed onto her from block (2).
5) Finally, Alice discards the frozen bits based on the side information and retains the rest of the information bits as her key $\hat{\mathbf{b}} = [1, 1, 1, 1]$ in block (8).

D. SYSTEM D: BALANCED-COMPLEXITY DR SCHEME RELYING ON POLAR-CODED QUANTUM AND LDPC-CODED CLASSICAL LINKS

An alternative to the RR of Systems A to C, namely the DR based scheme is conceived in System D, which is portrayed in Fig. 7. Explicitly in contrast to RR, the key is generated by Alice for DR in Fig. 7. We will demonstrate in our simulation results of Section VI that DR exhibits better performance at low SNR than its RR counterpart. The steps in System D of Fig. 7 are described as follows:

1) Bob generates the frozen bit indices $\mathbf{A^C}$ in block (2) based on SNR_q and on N, K of the Polar code provided for block (2) by block (1). These are then encoded by the LDPC encoder of block (9) and transmitted to Alice over the classical channel of block (3).
2) Alice performs LDPC decoding in block (10) and obtains the side information constituted by the frozen bit index $\mathbf{A^C}$.
3) Alice then generates the key **b** by her QRNG of block (4), and then encodes the key to construct **z** by the Polar encoder of block (5) based on the recovered frozen bit indices $\mathbf{A^C}$ and on the key of block (4). Alice transmits the encoded key **z** to Bob through the equivalent quantum channel of block (6).
4) Bob performs Polar decoding in block (7) with aid of the frozen bit information $\mathbf{A^C}$ in order to recover the key $\hat{\mathbf{b}}$ in block (8), given that the frozen bits are known locally.

V. SECRET KEY RATE ANALYSIS

A. REVERSE RECONCILIATION

Since collective attacks[5] and finite-length codes are considered, the SKR of a CV QKD system using RR is defined as [27]:

$$K^{RR} = \gamma\,(1-\theta)\,[\beta I_{AB} - \chi_{BE} - \Delta n]\,, \tag{10}$$

where γ denotes the specific fraction of successful key extractions by Eve, normalized by the total number of data exchanged by Alice and Bob. Furthermore, θ represents the BLER estimated during the reconciliation step. Still referring to (10), I_{AB} is Shannon's classical mutual information between Alice and Bob based on their shared correlated data, and χ_{BE} represents the Holevo information [54] that Eve can extract from Bob. Finally, Δn represents the SKR-reduction owing to using a finite block-length.

The finite-size offset factor $\Delta(n)$ characterizes the statistical deviation induced by finite-length effects in parameter estimation. As established in [55], for block sizes satisfying $n > 10^4$, this term can be simplified as:

$$\Delta(n) \approx 7\sqrt{\frac{\log_2\left(\frac{2}{\epsilon}\right)}{n}}, \tag{11}$$

where ϵ is the protocol's security failure probability and its value is chosen to be $\epsilon = 10^{-10}$, which is widely used in the literature [55]. Our framework employs $n = 10^{12}$, which is a value chosen in most of the literature, as in the benchmark [27].

The reconciliation efficiency β in (10) is calculated based on [56]:

$$\beta = \frac{R}{C} = \frac{R}{0.5\log_2(1+\text{SNR})} = \frac{R}{0.5\log_2(1+\frac{E_S}{E_N})}, \tag{12}$$

where R represents the coding rate of the error correction code used, C is the Shannon capacity, E_S is the average power of the transmitted signal, and E_N is the Gaussian noise power in the receiver [22].

The mutual information I_{AB} attained upon using homodyne detection is given by [57]:

$$I_{AB} = \frac{1}{2}\log_2(1+\text{SNR}) = \frac{1}{2}\log_2\left(\frac{V+\xi_{total}}{1+\xi_{total}}\right), \tag{13}$$

where V represents the variance of Alice's initially transmitted signals and given by $V = V_S + 1$, while V_S represents the

[5]In the security analysis of CV-QKD protocols, the collective Gaussian attacks [50] constitute the most important family, permitted by quantum mechanics [51]. The general framework for a collective Gaussian attack is detailed explicitly in [52], [53].

variance of the Gaussian signals used in the modulator of CV-QKD [27]. Moreover, ξ_{total} is the total amount of noise imposed on the receiver, which can be expressed as

$$\xi_{total} = \xi_{line} + \frac{\xi_{hom}}{T_{ch}}, \tag{14}$$

where $\xi_{hom} = \frac{1+v_{el}}{\eta} - 1$ is the homodyne detector's noise and v_{el} stands for the electronic noise caused by the detector, while η represents the detection efficiency. Furthermore, $\xi_{line} = (\frac{1}{T_{ch}} - 1) + \varepsilon$ represents the noise, where T_{ch} is the channel transitivity and ε is the excess noise (e.g., modulation noise, phase-recovery noise, Raman noise, etc [57]). The excess noise parameter is a critical performance indicator in CV-QKD systems, since all realizations, regardless of the specific protocol employed, exhibit sensitivity to noise. Here ε is quantified in terms of shot-noise units (SNU), which is normalized with respect to the shot-noise power [58]. A single-mode fiber is assumed with an attenuation of $\alpha = 0.2$ dB/km, where the distance-dependent path-loss of the channel is $T_{ch} = 10^{-\alpha d/10}$, with d denoting the distance between the two parties.

Furthermore, the Holevo information between Bob and Eve can be calculated as follows [57]:

$$\chi_{BE} = S_E - S_{(E|B)} = S_{AB} - S_{(E|B)}, \tag{15}$$

where S is the von Neumann entropy defined in [54]. For Gaussian states, the von Neumann entropy can be expressed in terms of its symplectic eigenvalues [59] as follows:

$$S = \sum_f h(f), \tag{16}$$

where we have:

$$h(f) = \left(\frac{f+1}{2}\right)\log_2\left(\frac{f+1}{2}\right) - \left(\frac{f-1}{2}\right)\log_2\left(\frac{f-1}{2}\right). \tag{17}$$

In order to calculate the von Neumann entropy of S_E and $S_{(E|A)}$, the general calculation of sympletic eigenvalues using the covariance matrix is shown below. Firstly, a covariance matrix is used in the following block form:

$$\Xi = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}. \tag{18}$$

Then the symplectic eigenvalue of the covariance matrix Ξ can be calculated using the following formula [57]

$$f = |i\Omega\Xi|, f \geq 1, \tag{19}$$

where Ω defines the symplectic form given by

$$\Omega := \bigoplus_{m=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{20}$$

where the notation $\oplus$ represents the direct sum that adds matrices on the block diagonal. Then the symplectic eigenvalues can be written by

$$f = \sqrt{\frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4\det\Xi}\right)}, \tag{21}$$

where $\det\Xi$ is the determinant of the covariance matrix Ξ and we have $\Delta = \det\mathbf{A} + \det\mathbf{B} + 2\det\mathbf{C}$.

Therefore, the covariance matrix Ξ_{AB} can be expressed as

$$\begin{aligned}\Xi_{AB} &= \begin{pmatrix} V\mathbf{I} & \sqrt{T\left(V^2-1\right)}\mathbf{Z} \\ \sqrt{T\left(V^2-1\right)}\mathbf{Z} & [(1-T)W + TV]\mathbf{I} \end{pmatrix} \\ &= \begin{pmatrix} a\mathbf{I} & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I} \end{pmatrix},\end{aligned} \tag{22}$$

where T is defined by $T = T_{ch}\eta$, W is the variance of the Einstein-Podolsky-Rosen (EPR) entangled Gaussian states, which are related to the optimal collective Gaussian attack by Eve [60]. On the other hand, W is given by [59][57]

$$W = 1 + \frac{T\sigma}{1-T}, \sigma = \varepsilon + \frac{v_{el}}{T}, \tag{23}$$

where

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{24}$$

are a pair of Pauli matrices. Hence, the required symplectic eigenvalues of Ξ_{AB} are given by

$$f_{1,2}^{\mathrm{RR}2} = \frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4D^2}\right), \tag{25}$$

where we have:

$$\begin{aligned}\Delta &= a^2 + b^2 - 2c^2, \\ D &= ab - c^2.\end{aligned} \tag{26}$$

As for the symplectic eigenvalue of $S_{(E|B)}$, it can be shown that:

$$f_3^{\mathrm{RR}} = \sqrt{a\left(a - \frac{c^2}{b}\right)}. \tag{27}$$

Hence, the Holevo information can be calculated as

$$\chi_{BE} = h\left(f_1^{\mathrm{RR}}\right) + h\left(f_2^{\mathrm{RR}}\right) - h\left(f_3^{\mathrm{RR}}\right), \tag{28}$$

where f_1^{RR}, f_2^{RR} and f_3^{RR} are symplectic eigenvalues. Upon substituting (13) and (28) into (10), the corresponding SKR can be obtained.

B. DIRECT RECONCILIATION

The SKR of our CV QKD system using DR is defined as:

$$K^{DR} = \gamma\left(1-\theta\right)\left[\beta I_{AB} - \chi_{AE} - \Delta n\right], \tag{29}$$

where χ_{AE} represents the Holevo information [54] that Eve can extract from the information of Alice. The other parameters are the same as in the RR SKR (10).

The Holevo information between Alice and Eve can be calculated as follows,

$$\chi_{AE} = S_E - S_{(E|A)}. \tag{30}$$

The corresponding covariance matrices as Ξ_E and $\Xi_{(E|A)}$ can be found in [59] as

$$\Xi_E = \begin{pmatrix} ([1-T]V + TW)\cdot \mathbf{I} & \sqrt{T(W^2-1)}\cdot \mathbf{Z} \\ \sqrt{T(W^2-1)}\cdot \mathbf{Z} & W\cdot \mathbf{I} \end{pmatrix}. \quad (31)$$

Hence, Eve's symplectic eigenvalues f_1^{DR} and f_2^{DR} can be obtained using (21), while $\Xi_{(E|A)}$ is shown below

$$\Xi_{(E|A)} = \begin{pmatrix} \mathbf{D} & \mathbf{E} \\ \mathbf{E}^T & \mathbf{F} \end{pmatrix}, \quad (32)$$

where we have:

$$\mathbf{D} = \begin{pmatrix} \frac{(1-T)(VV_S - V^2+1)}{V} + TW & 0 \\ 0 & (1-T)V + TW \end{pmatrix},$$
$$\mathbf{E} = \sqrt{T(W^2-1)}\cdot \mathbf{Z},$$
$$\mathbf{F} = W\cdot \mathbf{I}. \quad (33)$$

Then the symplectic eigenvalues f_3^{DR} and f_4^{DR} of $\Xi_{(E|A)}$ can also be obtained by using (21).

Finally, the Holevo information can be calculated as

$$\chi_{AE} = h\left(f_1^{\mathrm{DR}}\right) + h\left(f_2^{\mathrm{DR}}\right) - h\left(f_3^{\mathrm{DR}}\right) - h\left(f_4^{\mathrm{DR}}\right), \quad (34)$$

where f_1^{DR}, f_2^{DR}, f_3^{DR} and f_4^{DR} are symplectic eigenvalues. Upon substituting (13) and (34) into (29), the corresponding SKR of DR can be obtained.

VI. SYSTEM PERFORMANCE

A. COMPARISON OF LDPC AND POLAR CODES IN THE QUANTUM CHANNEL OF SYSTEM A

Fig. 8 compares the BLER performance of LDPC and Polar codes at the same coding rate of $R = 0.5$ for different block lengths spanning from $N = 64$ to $N = 1024$ in the equivalent BI-AWGN quantum channel. Again, the classical channel harnessed for side information transmission is considered *ideal* in System A. As expected, when the block length increases, both codes exhibit improved performance. However, the LDPC codes represented by dashed lines demonstrate superior performance at a longer block length of $N = 1024$, whereas Polar codes marked by continuous lines exhibit better performance at the short block lengths of 512 bits and below. Polar codes have been proven to be able to achieve a better performance than LDPC for short block length [61]. For this reason, Polar codes have been adopted for 5G Ultra-reliable low-latency communication (URLLC) and Massive machine-type communication (mMTC) standardizations [62]. Our simulation results of Fig. 9 confirm its superior performance in short-block CV-QKD systems as well.

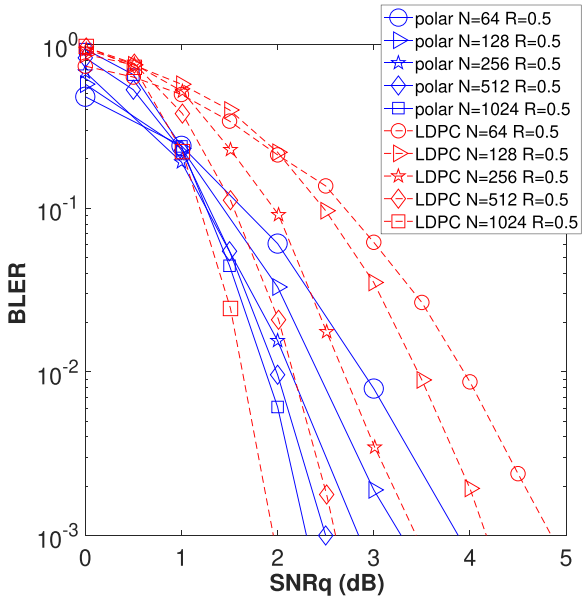

FIGURE 8. BLER performance comparison between LDPC and Polar code for different block lengths, where the LDPC decoder uses belief propagation (BP) decoding and the Polar code uses SCL ($L = 16$) decoding.

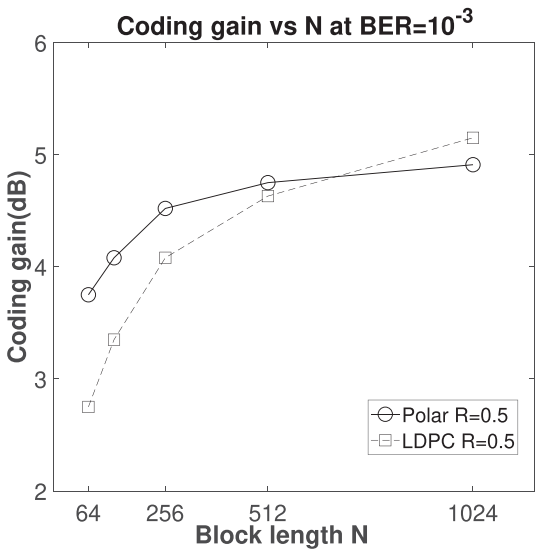

FIGURE 9. Coding gain of Polar and LDPC codes at the BER of 10^{-3}.

The computational complexities of LDPC and Polar codes quantified in terms of the total number of real-valued additions/multiplications are portrayed in Fig. 10[6]. The computational complexity of Polar codes is given by [63]:

$$L\cdot N\cdot \log_2(N) + L\cdot (N-1) + 2K\cdot L\cdot \log_2(2L), \quad (35)$$

[6]We note that as demonstrated in [39], L=16 is sufficient for polar code to approach the ML performance, while typically 50 iterations are assumed for LDPC decoders, as seen in [27]. Our work demonstrates that with short block length, Polar codes achieve better performance than LDPC, despite the lower decoding complexity.

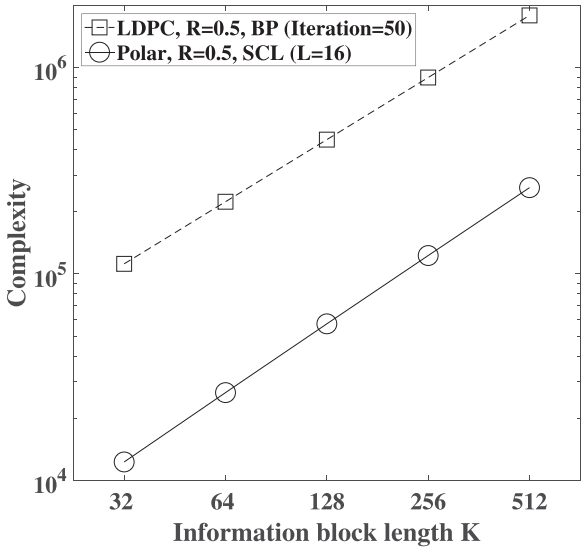

FIGURE 10. Computational complexity versus information block length for the LDPC and Polar decoders having a coding rate of $R = 1/2$.

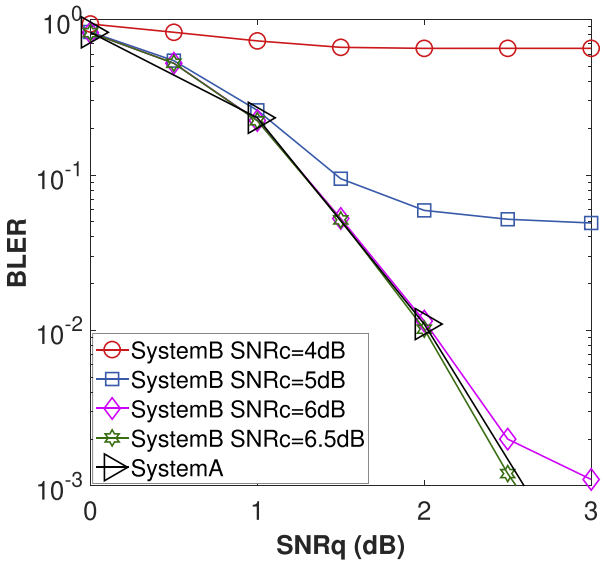

FIGURE 11. BLER performance comparison using System B. The code length and coding rate of the Polar code are 512 and 0.5 respectively. SCL decoding with $L = 16$ is used. The classical channel is assumed to be a Rayleigh fading channel.

where N is the block length, L is the list size, and K represents the number of information bits. By contrast, the total complexity associated with one iteration of LDPC's BP requires $11NJ - 9N$ real multiplications, $N(J + 1)$ real divisions, and $N(3J + 1)$ real additions [64]. Here J denotes the number of ones in each of the columns of the PCM, where $J = 3$ in our case. It can be seen in Fig. 10 that the Polar decoding complexities are substantially lower than those of their LDPC counterparts.

B. THE IMPACT OF FADING AND NOISE IN THE CLASSICAL CHANNEL OF SYSTEM B

Fig. 11 portrays the BLER performance of quantum transmission in System B, when the classical channel is modelled by Rayleigh fading associated with different SNRs. The code length of $N = 512$ and coding rate of $R = 0.5$ are employed. The term SNR_c denotes the SNR of the classical channel. When SNR_c is low, System B experiences an error floor. This error floor is reduced as SNR_c increases. As SNR_c reaches a sufficiently high value, the BLERs of the quantum transmission converge to those of System A of Fig. 8, where the classical channel used for side information transmission is assumed to be ideal. Fig. 12 demonstrates our BLER comparison between the Polar and LDPC codes for System B, where the benchmark of LDPC aided CV-QKD characterized in [27] utilizes the syndrome as side information. It can be seen in Fig. 12 that the Polar code aided CV-QKD consistently outperforms LDPC assisted CV-QKD for short block lengths up to $N = 512$.

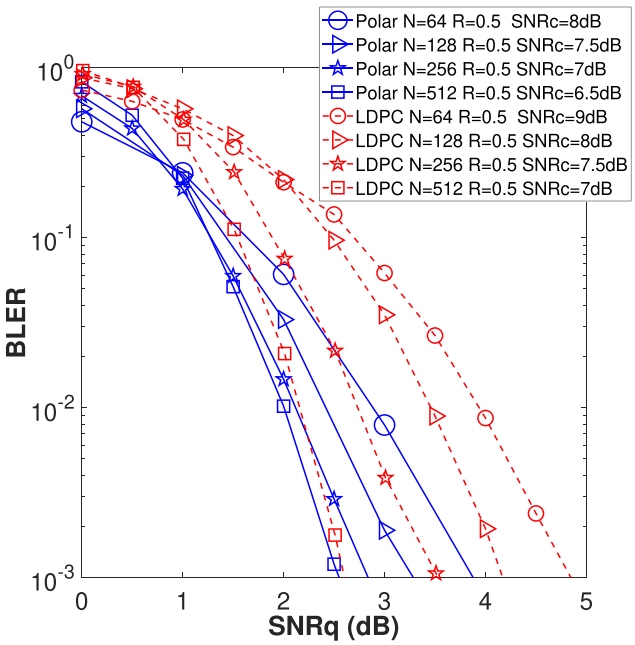

FIGURE 12. BLER performance comparison in System B. Polar and LDPC codes are used here, where the classical channel is assumed to be a Rayleigh fading channel.

C. PERFORMANCE RESULTS OF SYSTEM C ASSOCIATED WITH BALANCED COMPLEXITY

Fig. 13 portrays the BLER results of System C having balanced FEC decoding complexity, where a Polar decoder and an LDPC decoder are employed at Alice's and Bob's sides, respectively. The benchmark in [27] employs an LDPC code for both quantum transmission and for syndrome transmission over the classical channel. It can be seen in Fig. 13 that Polar coding assisted CV-QKD consistently outperforms its LDPC counterpart of [27], when short block lengths of up to $N = 512$ are considered.

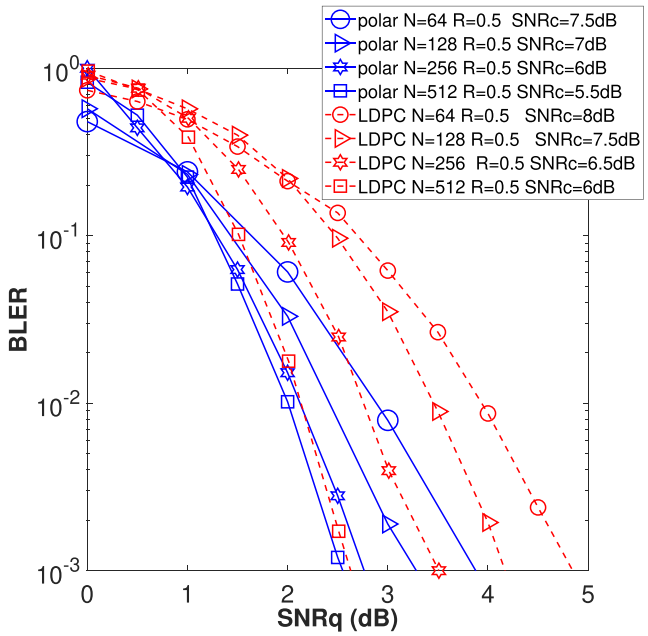

FIGURE 13. BLER performance comparison in System C. Polar and LDPC codes are used here, where the classical channel is assumed to be a Rayleigh fading channel.

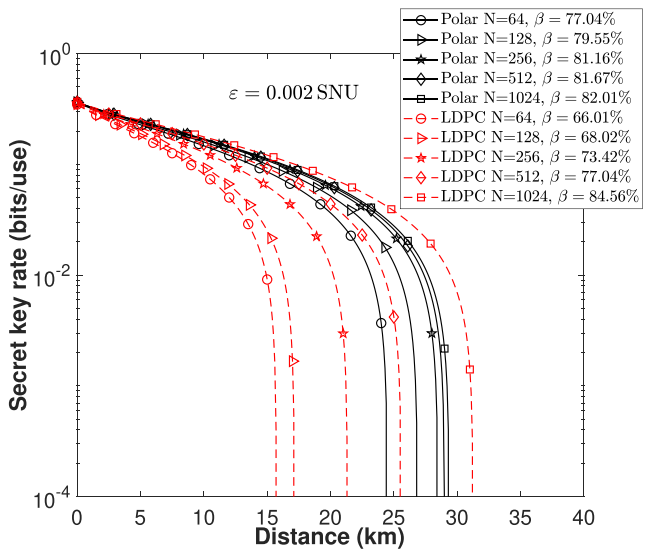

FIGURE 14. SKR of System C using RR. LDPC and Polar code are used with different block length. The efficiency of the homodyne detector is $\eta = 0.98$, and the electric noise is $v_{el} = 0.01$ SNU. The values of different reconciliation efficiency are calculated based on the corresponding SNR at BLER equals to 0.1, while the excess noise ε is set as 0.002 SNU.

D. SECRET KEY RATE RESULTS OF SYSTEM C (RR) AND SYSTEM D (DR)

Fig. 14 portrays our SKR comparison between Polar and LDPC codes for System C, which confirms that Polar-coded CV-QKD systems exhibit longer secure distance than their LDPC counterparts for a short block length of $N \leq 512$.

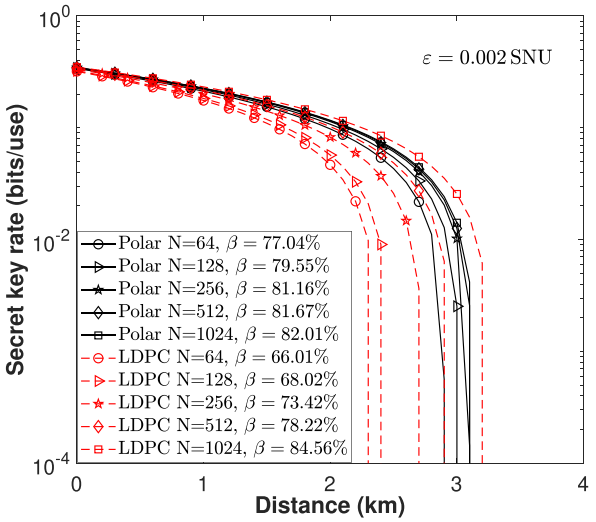

FIGURE 15. SKRs of System D using DR. LDPC and Polar code are used with different block length. The efficiency of the homodyne detector is $\eta = 0.98$, and the electric noise is $v_{el} = 0.01$ SNU. The values of different reconciliation efficiency are calculated based on the corresponding SNR at BLER equals to 0.1, excess noise ε is set as 0.002 SNU.

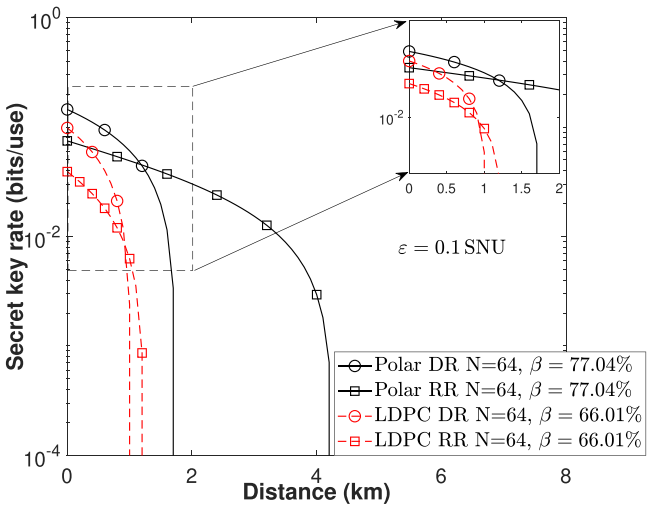

FIGURE 16. SKR comparison between RR and DR. LDPC and Polar code are used with same block length. The efficiency of the homodyne detector is $\eta = 0.98$, and the electric noise is $v_{el} = 0.01$ SNU. The values of reconciliation efficiency are calculated based on the corresponding SNR at BLER equals to 0.1, while the excess noise ε is set as 0.1 SNU.

Fig. 15 demonstrates the SKR of System D using DR, when Polar and LDPC codes are invoked for quantum transmission. It can be seen in Fig. 15 that again, LDPC codes perform better for a long frame length of $N = 1024$, while the Polar code assisted schemes perform better for a short block length of $N = 512$ and below.

Finally, the SKRs of DR and RR are compared in Fig. 16, where both LDPC and Polar codes having a short block length of $N = 64$ are considered for protecting the quantum transmission. The CV-QKD system utilizing short Polar codes is capable of transmitting over greater distances than the LDPC codes, irrespective of whether the DR or RR protocols are

applied. Additionally, when the excess noise is increased from $\varepsilon = 0.002$ in Figs. 14 and 15 to $\varepsilon = 0.1$ in Fig. 16, both the DR and RR distances decrease, with the reduction being more pronounced for the RR protocol, as evidenced by comparing Figs. 14 and 16. For distances up to approximately 1.3 km, the DR protocol yields a higher SKR compared to the RR protocol, when Polar codes are used. However, for LDPC codes, the DR protocol generally outperforms RR. Having said that, the difference in achievable distances between the two LDPC-based DR and RR protocols is not substantial.

VII. CONCLUSION

A set of four Polar coding assisted CV-QKD systems were investigated. **Firstly**, System A employed Polar codes for protecting quantum transmission in RR, where the frozen bit based side information was transmitted over an idealistic error-free classical channel. **Secondly**, System B communicated over a realistic fading classical channel, where LDPC coding was employed for protecting the side information. **Thirdly**, System C aimed for achieving a balanced FEC decoding complexity, where Polar decoding was performed at Alice's side, while LDPC decoding was employed at Bob's side. **Finally**, System D relied on the DR protocol that also ensured protection of both the quantum and classical channels, where the FEC decoding complexity was balanced following the same philosophy as System C. Our simulation results demonstrated that Polar coding aided quantum transmission is capable of achieving better BLER and SKR than its LDPC counterpart, when short block lengths of $N = 512$ and below are considered. By contrast, for block lengths longer than $N = 512$, LDPC coding aided quantum transmission [27] can be used. Further research is required for CV-QKD schemes relying on both variable-rate and variable-length coding schemes relying Extrinsic Information Transfer (EXIT) chart based near-capacity schemes [65]. Furthermore, Automatic Repeat Request (ARQ) based multiple component turbo codes are worth considering, which have both a variable block-length and variable code rate, as detailed in [66].

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014.

[2] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, 1992, Art. no. 3121.

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

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

[5] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error," *Phys. Rev. A*, vol. 98, no. 6, 2018, Art. no. 062323.

[6] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, 2002, Art. no. 057902.

[7] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," *Phys. Rev. Lett.*, vol. 93, no. 17, 2004, Art. no. 170504.

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

[9] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, "Continuous-variable measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 89, no. 5, 2014, Art. no. 052301.

[10] I. B. Djordjevic, "Optimized-eight-state CV-QKD protocol outperforming Gaussian modulation based protocols," *IEEE Photon. J.*, vol. 11, no. 4, Aug. 2019, Art. no. 4500610.

[11] A. Leverrier and P. Grangier, "Simple proof that Gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a Gaussian modulation," *Phys. Rev. A*, vol. 81, no. 6, 2010, Art. no. 062314.

[12] C. Ottaviani, S. Mancini, and S. Pirandola, "Two-way Gaussian quantum cryptography against coherent attacks in direct reconciliation," *Phys. Rev. A*, vol. 92, no. 6, 2015, Art. no. 062323.

[13] C. Ottaviani and S. Pirandola, "General immunity and superadditivity of two-way Gaussian quantum cryptography," *Sci. Rep.*, vol. 6, no. 1, pp. 1–8, 2016.

[14] A. Leverrier, "Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction," *Phys. Rev. Lett.*, vol. 118, no. 20, 2017, Art. no. 200501.

[15] G. Zhang et al., "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," *Nature Photon.*, vol. 13, no. 12, pp. 839–842, 2019.

[16] A. Nakassis and A. Mink, "Polar Codes in a QKD Environment," *Proc. SPIE*, vol. 9123, 2014, Art. no. 912305.

[17] S. Lee and J. Heo, "Efficient reconciliation protocol with polar codes for quantum key distribution," in *Proc. 10th Int. Conf. Ubiquitous Future Netw.*, 2018, pp. 40–43.

[18] S. Yan, J. Wang, J. Fang, L. Jiang, and X. Wang, "An improved polar codes-based key reconciliation for practical quantum key distribution," *Chin. J. Electron.*, vol. 27, no. 2, pp. 250–255, 2018.

[19] S. Zhao, Z. Shen, H. Xiao, and L. Wang, "Multidimensional reconciliation protocol for continuous-variable quantum key agreement with polar coding," *Sci. China Phys., Mechan. Astron.*, vol. 61, no. 9, 2018, Art. no. 090323.

[20] M. Zhang, H. Hai, Y. Feng, and X.-Q. Jiang, "Rate-adaptive reconciliation with polar coding for continuous-variable quantum key distribution," *Quantum Inf. Process.*, vol. 20, pp. 1–17, 2021.

[21] M. Zhang, Y. Dou, Y. Huang, X.-Q. Jiang, and Y. Feng, "Improved information reconciliation with systematic polar codes for continuous variable quantum key distribution," *Quantum Inf. Process.*, vol. 20, pp. 1–16, 2021.

[22] C. Zhou, X. Wang, Y. Zhang, Z. Zhang, S. Yu, and H. Guo, "Continuous-variable quantum key distribution with rateless reconciliation protocol," *Phys. Rev. Appl.*, vol. 12, no. 5, 2019, Art. no. 054013.

[23] Y. Kim, C. Suh, and J.-K. K. Rhee, "Reconciliation with polar codes constructed using Gaussian approximation for long-distance continuous-variable quantum key distribution," in *Proc. 2017 Int. Conf. Inf. Commun. Technol. Convergence*, 2017, pp. 301–306.

[24] Z. Cao, X. Chen, G. Chai, K. Liang, and Y. Yuan, "Rate-adaptive polar-coding-based reconciliation for continuous-variable quantum key distribution at low signal-to-noise ratio," *Phys. Rev. Appl.*, vol. 19, no. 4, 2023, Art. no. 044023.

[25] X. Wang, H. Wang, C. Zhou, Z. Chen, S. Yu, and H. Guo, "Continuous-variable quantum key distribution with low-complexity information reconciliation," *Opt. Exp.*, vol. 30, no. 17, pp. 30455–30465, 2022.

[26] M. Zhang, Q. Wang, T. Son, and S. Kim, "Evaluation of adaptive reconciliation protocols for CV-QKD using systematic polar codes," *Quantum Inf. Process.*, vol. 23, no. 157, pp. 1–17, 2024.

[27] X. Liu, C. Xu, Y. Noori, S. X. Ng, and L. Hanzo, "The road to near-capacity CV-QKD reconciliation: An FEC-agnostic design," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 2089–2112, 2024.

[28] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Proc. Workshop Theory Appl. Cryptographic Techn.*, 1993, pp. 410–423.

[29] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. Nickel, C. Donahue, and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," *Phys. Rev. A*, vol. 67, no. 5, 2003, Art. no. 052303.

[30] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *Proc. 2009 IEEE Int. Symp. Inf. Theory*, 2009, pp. 1879–1883.

[31] D. Elkouss, J. Martinez-Mateo, and V. M. Ayuso, "Information reconciliation for quantum key distribution," *Quantum Inf. Comput.*, vol. 11, no. 3/4, 2011, pp. 226–238.
[32] D. Lin, D. Huang, P. Huang, J. Peng, and G. Zeng, "High performance reconciliation for continuous-variable quantum key distribution with LDPC code," *Int. J. Quantum Inf.*, vol. 13, no. 2, 2015, Art. no. 1550010.
[33] X. Wang, Y.-C. Zhang, Z. Li, B. Xu, S. Yu, and H. Guo, "Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution," *Quantum Inf. Comput.*, vol. 17, no. 13/14, pp. 1123–1134, 2017.
[34] P. Jouguet and S. Kunz-Jacques, "High performance error correction for quantum key distribution using polar codes," *Quantum Inf. Comput.*, vol. 14, no. 3/4, pp. 329–338, 2014.
[35] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.
[36] C. Leroux, A. J. Raymond, G. Sarkis, I. Tal, A. Vardy, and W. J. Gross, "Hardware implementation of successive-cancellation decoders for polar codes," *J. Signal Process. Syst.*, vol. 69, pp. 305–315, 2012.
[37] A. Balatsoukas-Stimming, M. B. Parizi, and A. Burg, "LLR-based successive cancellation list decoding of polar codes," *IEEE Trans. Signal Process.*, vol. 63, no. 19, pp. 5165–5179, Oct. 2015.
[38] K. Niu and K. Chen, "CRC-aided decoding of polar codes," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1668–1671, Oct. 2012.
[39] I. Tal and A. Vardy, "List decoding of polar codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2213–2226, May 2015.
[40] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, "Quantum cryptography approaching the classical limit," *Phys. Rev. Lett.*, vol. 105, no. 11, 2010, Art. no. 110501.
[41] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous variable quantum cryptography: Beating the 3 dB loss limit," *Phys. Rev. Lett.*, vol. 89, no. 16, 2002, Art. no. 167901.
[42] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 77, no. 4, 2008, Art. no. 042325.
[43] M. Chakraborty, A. Mukherjee, I. Krikidis, A. Nag, and S. Chandra, "A hybrid noise approach to modelling of free-space satellite quantum communication channel for continuous-variable QKD," *IEEE Trans. Green Commun. Netw.*, early access, Jan. 2, 2025, doi: 10.1109/TGCN.2024.3525297.
[44] G. Van Assche, J. Cardinal, and N. J. Cerf, "Reconciliation of a quantum-distributed Gaussian key," *IEEE Trans. Inf. Theory*, vol. 50, no. 2, pp. 394–400, Feb. 2004.
[45] S.-S. Yang, Z.-G. Lu, and Y.-M. Li, "High-speed post-processing in continuous-variable quantum key distribution based on FPGA implementation," *J. Lightw. Technol.*, vol. 38, no. 15, pp. 3935–3941, Aug. 2020.
[46] X. Liu, C. Xu, S. X. Ng, and L. Hanzo, "OTFS-based CV-QKD systems for doubly selective THz channels," *IEEE Trans. Commun.*, early access, Jan. 29, 2025, doi: 10.1109/TCOMM.2025.3535889.
[47] D. Wu, Y. Li, and Y. Sun, "Construction and block error rate analysis of polar codes over AWGN channel based on Gaussian approximation," *IEEE Commun. Lett.*, vol. 18, no. 7, pp. 1099–1102, Jul. 2014.
[48] R. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, 2003.
[49] W. Ryan and S. Lin, *Channel Codes: Classical and Modern*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
[50] M. Navascués, F. Grosshans, and A. Acín, "Optimality of Gaussian attacks in continuous-variable quantum cryptography," *Phys. Rev. Lett.*, vol. 97, Nov. 2006, Art. no. 190502.
[51] R. Renner and J. I. Cirac, "De Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," *Phys. Rev. Lett.*, vol. 102, Mar. 2009, Art. no. 110504.
[52] S. Pirandola, S. L. Braunstein, and S. Lloyd, "Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography," *Phys. Rev. Lett.*, vol. 101, Nov. 2008, Art. no. 200504.
[53] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Commun. Surveys. Tuts.*, vol. 21, no. 1, pp. 881–919, firstquarter 2019.
[54] F. Laudenbach et al., "Continuous-variable quantum key distribution with Gaussian modulation—The theory of practical implementations," *Adv. Quantum Technol.*, vol. 1, no. 1, 2018, Art. no. 1800011.
[55] A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," *Phys. Rev. A—At., Mol., Opt. Phys.*, vol. 81, no. 6, 2010, Art. no. 062343.
[56] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," *Phys. Rev. A—At., Mol., Opt. Phys.*, vol. 84, no. 6, 2011, Art. no. 062317.
[57] C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-variable quantum key distribution using thermal states," *Phys. Rev. A—At., Mol., Opt. Phys.*, vol. 86, no. 2, 2012, Art. no. 022318.
[58] D. Milovančev, N. Vokić, F. Laudenbach, C. Pacher, H. Hübel, and B. Schrenk, "High rate CV-QKD secured mobile WDM fronthaul for dense 5G radio networks," *J. Lightw. Technol.*, vol. 39, no. 11, pp. 3445–3457, Jun. 2021.
[59] C. Liu, C. Zhu, X. Liu, M. Nie, H. Yang, and C. Pei, "Multicarrier multiplexing continuous-variable quantum key distribution at terahertz bands under indoor environment and in inter-satellite links communication," *IEEE Photon. J.*, vol. 13, no. 4, Aug. 2021, Art. no. 7600113.
[60] R. García-Patrón and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," *Phys. Rev. Lett.*, vol. 97, no. 19, 2006, Art. no. 190503.
[61] H. Gamage, N. Rajatheva, and M. Latva-Aho, "Channel coding for enhanced mobile broadband communication in 5G systems," in *Proc. 2017 Eur. Conf. Netw. Commun.*, 2017, pp. 1–6.
[62] A. Sharma and M. Salim, "Polar code: The channel code contender for 5G scenarios," in *Proc. 2017 Int. Conf. Comput., Commun. Electron.*, 2017, pp. 676–682.
[63] R. G. Maunder, "On the hardware implementation of channel decoders for short block lengths," AccelerComm, Reno, Nevada, USA, Tech. Rep. R1-1612306, Nov. 2016.
[64] M. P. Fossorier, M. Mihaljevic, and H. Imai, "Reduced complexity iterative decoding of low-density parity check codes based on belief propagation," *IEEE Trans. Commun.*, vol. 47, no. 5, pp. 673–680, May 1999.
[65] L. Hanzo, T. H. Liew, and B. L. Yeap, *Turbo Coding, Turbo Equalisation and Space-Time Coding*. Hoboken, NJ, USA: Wiley, 2002.
[66] H. Chen, R. G. Maunder, and L. Hanzo, "A survey and tutorial on low-complexity turbo coding techniques and a holistic hybrid ARQ design example," *IEEE Commun. Surveys. Tuts.*, vol. 15, no. 4, pp. 1546–1566, fourthquarter 2013.

DINGZHAO WANG (Student Member, IEEE) received the B.E. degree from the Xi'an University of Posts & Telecommunications, Xi'an, China, in 2020, and the B.Eng. degree from Staffordshire University, Staffordshire, U.K., in 2020 and the M.Sc. degree with Distinction from the University of Southampton, Southampton, U.K., in 2021. He is currently working toward the Ph.D. degree with the Next Generation Wireless Group, University of Southampton, Southampton, U.K. His research interests include quantum communications, channel coding.

XIN LIU (Student Member, IEEE) received the B.E. degree from the Wuhan University of Technology, Wuhan, China, in 2017, the M.S. degree from the Huazhong University of Science and Technology, Wuhan, China, in 2020, and the Ph.D degree from the University of Southampton, Southampton, U.K., in 2025. He is currently a Research Fellow with the Next Generation Wireless Group, University of Southampton. His research interests include quantum communications, channel coding, and wireless communications.

CHAO XU (Senior Member, IEEE) received the B.Eng. degree in telecommunications from the Beijing University of Posts and Telecommunications, Beijing, China, the B.Sc. (Eng.) degree (with First Class Hons.) in telecommunications from the Queen Mary, University of London, London, U.K., through a Sino-U.K. joint degree Program in 2008, and the M.Sc. degree (with Distinction) in radio frequency communication systems and the Ph.D. degree in wireless communications from the University of Southampton, Southampton, U.K., in 2009 and 2015, respectively. He is currently a Senior Lecturer with Next Generation Wireless Research Group, University of Southampton. His research interests include index modulation, reconfigurable intelligent surfaces, noncoherent detection, and turbo detection. He was the recipient of the Best M.Sc. Student in Broadband and Mobile Communication Networks by the IEEE Communications Society U.K. and Republic of Ireland Chapter in 2009, 2012 Chinese Government Award for Outstanding Self-Financed Student Abroad, 2017 Dean's Award, Faculty of Physical Sciences and Engineering, University of Southampton, 2023 Marie Sklodowska-Curie Actions Global Postdoctoral Fellowships with the highest evaluation score of 100/100.

SOON XIN NG (Senior Member, IEEE) received the B.Eng. degree (First class) in electronic engineering and the Ph.D. degree in telecommunications from the University of Southampton, Southampton, U.K., in 1999 and 2002, respectively. From 2003 to 2006, he was a Postdoctoral Research Fellow working on collaborative European research projects known as SCOUT, NEWCOM and PHOENIX. Since 2006, he has been a member of academic staff in the School of Electronics and Computer Science, University of Southampton. He was involved in the OPTIMIX and CONCERTO European Projects as well as IU-ATC and UC4G Projects. He was the Principal Investigator of an EPSRC Project on "Cooperative Classical and Quantum Communications Systems". He is currently a Professor of next generation communications with the University of Southampton. He has authored or coauthored more than 300 papers and co-authored two John Wiley/IEEE Press books in this field. His research interests include adaptive coded modulation, coded modulation, channel coding, space-time coding, joint source and channel coding, iterative detection, OFDM, MIMO, cooperative communications, distributed coding, quantum communications, quantum error correction codes, joint wireless-and-optical-fibre communications, game theory, artificial intelligence and machine learning. He is a Fellow of the Higher Education Academy in the U.K., a Chartered Engineer and a Fellow of the IET. He acted as TPC/track/workshop chairs for various conferences. He was an Editor of Quantum Engineering. He was the Guest Editor for the special issues in IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATION and Editors of IEEE ACCESS and *KSII Transactions on Internet and Information Systems*. He is one of the Founders and Officers of IEEE Quantum Communications & Information Technology Emerging Technical Subcommittee (QCIT-ETC).

LAJOS HANZO (Life Fellow, IEEE) received the Doctorates (Hons.) degree from the Technical University of Budapest, Budapest, Hungary, in 2009 and Edinburgh University, Edinburgh, Scotland, (2015). He is a Foreign Member of the Hungarian Science-Academy, Fellow of the Royal Academy of Engineering (FREng), of the IET, of EURASIP and holds the IEEE Eric Sumner Technical Field Award. For further details please see: http://www-mobile.ecs.soton.ac.uk , https://en.wikipedia.org/wiki/Lajos_Hanzo