Received 9 March 2024; accepted 24 March 2024. Date of publication 27 March 2024; date of current version 17 April 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.3382225

The Road to Near-Capacity CV-QKD Reconciliation: An FEC-Agnostic Design

XIN LIU (Graduate Student Member, IEEE), CHAO XU (Senior Member, IEEE), YASIR NOORI (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 AUTHOR: L. HANZO (e-mail: lh@ecs.soton.ac.uk)

The work of Lajos Hanzo was supported in part by the Engineering and Physical Sciences Research Council under Project EP/W016605/1, Project EP/X01228X/1, Project EP/Y026721/1, and Project EP/W032635/1; and in part by the European Research Council's Advanced Fellow Grant QuantCom under Grant 789028.

ABSTRACT New near-capacity continuous-variable quantum key distribution (CV-QKD) reconciliation schemes are proposed, where both the authenticated classical channel (ClC) and the quantum channel (QuC) for QKD are protected by separate forward error correction (FEC) coding schemes. More explicitly, all of the syndrome-based QKD reconciliation schemes found in literature rely on syndrome-based codes, such as low-density parity-check (LDPC) codes. Hence at the current state-of-the-art the channel codes that cannot use syndrome decoding such as the family of convolutional codes (CCs) and polar codes cannot be directly applied. Moreover, the ClC used for syndrome transmission in these schemes is generally assumed to be idealistically error-free, where the realistic additive white Gaussian noise (AWGN) and Rayleigh fading of the ClC have not been taken into account. To circumvent this limitation, a new codeword-based - rather than syndrome-based - QKD reconciliation scheme is proposed, where Alice sends an FEC-protected codeword to Bob through a ClC, while Bob sends a separate FEC protected codeword to Alice through a QuC. Upon decoding the codeword received from the other side, the final key is obtained by applying a simple modulo-2 operation to the local codeword and the decoded remote codeword. As a result, **first of all**, the proposed codeword-based QKD reconciliation system ensures protection of both the QuC and of the ClC. **Secondly**, the proposed system has a similar complexity at both sides, where both Alice and Bob have an FEC encoder and an FEC decoder. **Thirdly**, the proposed system makes QKD reconciliation compatible with a wide range of FEC schemes, including polar codes, CCs and irregular convolutional codes (IRCCs), where a near-capacity performance can be achieved for both the QuC and for the ClC. Our simulation results demonstrate that thanks to the proposed regime, the performance improvements of the QuC and of the ClC benefit each other, hence leading to an improved secret key rate (SKR) that inches closer to both the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound and to the maximum achievable rate bound.

INDEX TERMS Continuous variable quantum key distribution (CV-QKD), multidimensional reconciliation, low-density parity check (LDPC) codes, irregular convolutional codes (IRCC), secret key rate (SKR), near-capacity codes.

NOMENCLATURE

List of Abbreviations

5G	Fifth Generation
6G	Sixth Generation
AES	Advanced Encryption Standard
AWGN	Additive White Gaussian Noise
B5G	Beyond 5G
B92	Bennett-92
BB84	Bennett-Brassard-1984
BBM92	Bennett-Brassard-Mermin-1992
BCH	Bose-Chaudhuri-Hocquenghem
BER	Bit Error Rate

BF	Bit-Flipping
BI-AWGN	Binary-Input Additive White Gaussian Noise
BLER	Block Error Rate
BP	Belief Propagation
BPSK	Binary Phase-Shift Keying
BSC	Binary Symmetric Channel
CC	Convolutional Code
CK	Classical key
ClC	Classical Channel
CM	Covariance Matrix
CN	Check Node
CV-QKD	Continuous Variable Quantum Key distribution
D2D	Device-to-device
DES	Data Encryption Standard
DH	Diffie-Hellman
DR	Direct Reconciliation
DV-QKD	Discrete Variable Quantum Key distribution
E91	Ekert-91
ECDH	Elliptic-Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EPR	Einstein-Podolsky-Rosen
EXIT	Extrinsic Information Transfer
FEC	Forward Error Correction
GG02	Grosshans-Grangier-2002
IRCC	Irregular Convolutional Code
LDPC	Low Density Parity-check
LG09	Leverrier-Grangier-2009
LLR	Log-likelihood Ratio
MI	Mutual Information
MIMO	Multiple-Input Multiple-Output
NG	Next-generation
OFDM	Orthogonal Frequency Division Multiplexing
OTP	One-Time Pad
PCM	Parity-Check Matrix
PLOB	Pirandola-Laurenza-Ottaviani-Banchi
PM	Phase-matching
QK	Quantum key
QKD	Quantum Key Distribution
QRNG	Quantum Random Number Generator
QuC	Quantum channel
RR	Reverse Reconciliation
RSA	Rivest-Shamir-Adleman
SARG04	Scarani-Acién-Ribordy-Gisin-2004
SHA	Secure Hash Algorithm
SKR	Secret Key Rate
SNR	Signal-to-Noise Ratio
SPA	Sum-Product Algorithm
TF	Twin-Field
THz	Terahertz
UAV	Unmanned Aerial Vehicle
URC	Unitary Rate Code
VN	Variable Node

List of Key Variables

α	the attenuation of a single-mode optical fibre
β	the reconciliation efficiency
χ_{BE}	the Holevo information between Bob and Eve
η	the homodyne detector efficiency
$\hat{\mathbf{b}}$	the decoded bit stream of $\mathbf{b}$
$\hat{X}_A$	the quadrature component transmitted by Alice
$\hat{X}_B$	the quadrature component transmitted by Bob
$\hat{X}_E$	the excess noise quadrature component introduced by Eve
$\mathbf{b}$	the random bit stream
$\mathbf{b}'$	the random bit stream after interleaving
$\mathbf{M}(\mathbf{y}', \mathbf{u})$	the mapping function sent from Bob to Alice
$\mathbf{s}$	the syndrome side information
$\mathbf{u}$	the spherical codes of $\mathbf{b}'$
$\mathbf{x}$	the rest of raw data of Alice
$\mathbf{x}'$	the normalized version of $\mathbf{x}$
$\mathbf{y}$	the rest of raw data of Bob
$\mathbf{y}'$	the normalized version of $\mathbf{y}$
$\tilde{\mathbf{u}}$	the noisy version of $\mathbf{u}$
ξ_{ch}	the excess noise
$I_{A,B}$	the mutual information between Alice and Bob
K	the information length of LDPC codes
K_f	the SKR
N	the codeword length of LDPC codes
P_B	the BLER in the reconciliation
V_s	the variance of Gaussian signals transmitted over QuC
v_{el}	the electronic noise

I. INTRODUCTION

GIVEN the increasing penetration of commercial fifth generation (5G) services, since 2020 researchers have embarked on the exploration of future wireless systems such as beyond 5G (B5G) and sixth generation (6G) communication. In this context, quantum science has the promise of supporting a range of appealing application scenarios [1], [2], [3], [4]. More explicitly, on one hand, quantum computing provides revolutionary acceleration in the information processing speed, which is envisioned to substantially improve the computing efficiency in B5G applications and to facilitate powerful new solutions for optimizing next-generation (NG) systems [5]. However, the commercialization of quantum computing may also impose a threat to the conventional cryptosystems [6], [7], [8], [9], [10], [11], [12], [13], [14]. These classical cryptography algorithms can provide computational security, which is practically unbreakable within a relatively short period of time when using state-of-the-art computational sources. However, conventional cryptography may be endangered by the progress in advanced quantum computing techniques. More explicitly, Shor's powerful algorithm that is capable of efficiently factorizing large prime numbers and of solving elliptic curve problems can impose a serious threat on the classic asymmetric cryptography [15]. Similarly, Grover's search algorithm will also make symmetric cryptography insecure [16], [17]. Hence, a quantum-safe cryptosystem is needed to tackle this threat. Against this backdrop, quantum

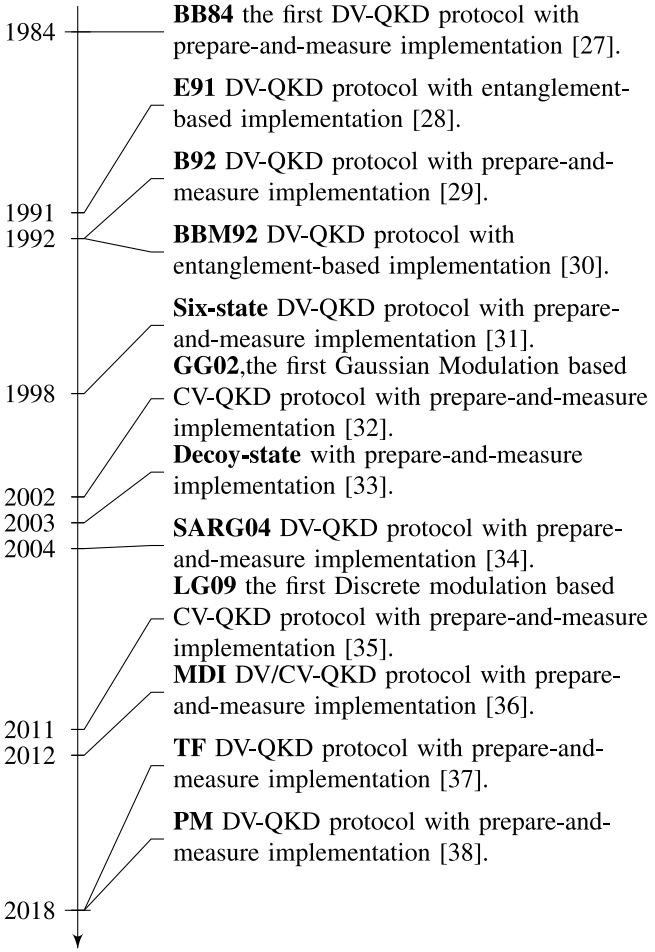


FIGURE 1. State-of-the-art QKD protocols.

key distribution (QKD) as one of the promising technologies can play an important role in providing sufficiently secure and reliable data transmission for next-generation communication systems [18], [19], [20], [21], [22], [23], [24], [25]. More explicitly, a QKD scheme instructs both the transmitter Alice and the receiver Bob to encrypt their confidential messages with the reconciled keys generated at both sides. This so-called one-time pad (OTP) system has been proven by Shannon to be information-theoretically secure [26]. Furthermore, the QKD-based cryptosystem possesses the capability of eavesdropping detection based on the no-cloning theorem and Heisenberg's uncertainty principle.

The earliest QKD protocol can be traced back to 1984, which is the Bennett-Brassard-1984 (BB84) protocol [27]. Since then, a variety of QKD protocols have been proposed, which can be divided into two types, i.e., discrete variable QKD (DV-QKD) and continuous variable QKD (CV-QKD). The state-of-the-art of DV-QKD and CV-QKD schemes is summarized at a glance in Fig. 1. More specifically, the landmark BB84 protocol [27] has spawned the family of DV-QKD exemplified by the Ekert-91 (E91) [28], Bennett-Brassard-Mermin-1992 (BBM92) [30], Bennett-92 (B92) [29], six-state [31], decoy-state [33], Scarani-Acién-Ribordy-Gisin-2004 (SARG04) [34], Twin-field (TF) [37], and phase-matching (PM) [38] protocols. Furthermore, the first CV-QKD protocol was the Gaussian modulation assisted Grosshans-Grangier-2002 (GG02) protocol [32], which was followed by the discrete modulation based CV-QKD Leverrier-Grangier-2009 (LG09) [35] protocol. A comprehensive overview of QKD protocols can be found in [39], [40], [41], [42], [43].

TABLE 1. Comparisons between two types of QKD.

	DV-QKD	CV-QKD
Light source	Single photon or attenuated laser	Coherent state or squeezed state
Modulation	Polarization or phase	Quadrature components of electromagnetic fields
Detection	Single-photon detection	Homodyne or Heterodyne detection

Table 1 offers a comparison between the two types of QKD. First of all, for light sources, typically the single photon or the attenuated laser source is utilized in DV-QKD, whilst the coherent state or squeezed state solution is used for CV-QKD. Secondly, the DV-QKD modulates or maps information onto the discrete degrees of freedom of a single photon, such as its polarization or phase. By contrast, the CV-QKD information is modulated or mapped onto the quadrature components of electromagnetic fields [19]. Finally, single-photon detection is required for DV-QKD, which is expensive to implement and yet has a low key rate. By contrast, for CV-QKD either homodyne or heterodyne detection is utilized, which has convenient compatibility with the operational network infrastructure [19], [44].

Recently, some authors have studied the feasibility of CV-QKD for NG wireless communication systems operating at microwave and terahertz (THz) frequencies [45], [46], [47], [48]. More explicitly, multiple-input multiple-output (MIMO) and orthogonal frequency division multiplexing (OFDM) air interface techniques have been utilized for increasing the limited secure transmission distance caused by the high path loss of the THz band [49], [50], [51], [52], [53], [54], [55], [56]. Furthermore, some recent achievements in THz hardware implementations such as detectors, power-efficient sources and antennas [57], [58], [59], [60], can facilitate the practical implementation of CV-QKD in NG communication systems. Therefore, this paper mainly focuses on the study of CV-QKD.

As an important step of classical post-processing in QKD, reconciliation plays an pivotal role in ensuring that both the transmitter and the receiver rely on the same bit stream and use it as the reconciled key. More explicitly, the reconciliation process is based on error correction used for mitigating the deleterious effects of noise and interference imposed by Eve [61]. For instance, a simple Hamming code was utilized in the reconciliation step to correct the bit errors in the raw key string shared by the satellite and the ground station for the experimental satellite-to-ground QKD system used in the *Micius* experiment [62]. Inspired by this development,

some more advanced forward error correction (FEC) codes have also been investigated, such as low-density parity-check (LDPC) codes [13], [63], [64], [65], [66], [67], [68], polar codes [55], [69], [70], [71], rateless codes [72], [73], and their diverse variants. As a further advance, instead of using a fixed FEC code rate, adaptive-rate reconciliation schemes were proposed in [74], [75], [76], where the secret key rate (SKR) and the secure transmission distance were optimized for different signal-to-noise ratios (SNRs). Moreover, a Raptor-like LDPC code was harnessed for QKD in [75], where the rate-compatible nature of the raptor code was exploited for reducing the cost of constructing new matrices for low-rate LDPC codes harnessed at low SNRs. In contrast to the conventional CV-QKD reconciliation, where a so-called single decoding attempt based algorithm was used, a multiple decoding attempt based method was adopted in [68] to improve the SKR performance. Furthermore, a large block length based LDPC coded scheme was analyzed in [77], where a near-capacity performance was achieved for transmission over the quantum channel (QuC).

A list of LDPC coded QKD reconciliation schemes is seen at a glance in Table 2. In a nutshell, there are two main types of reconciliation methods, namely the multidimensional [78], [79] and the slice-based reconciliation method [80], [81]. The former achieves better performance in the low-SNR region, which is suitable for long-range CV-QKD transmission, while the latter in the high-SNR domain, which is suitable for short-distance CV-QKD systems.[1] The soft-decision LDPC decoding adopted for QKD in [13], [83] outperforms the hard-decision decoding algorithm of [81], but at the cost of a higher complexity. **However**, a major issue is that all the existing studies assume that the classical channel (ClC) used for syndrome transmission is error-free. In practice, the ClC is contaminated both by fading and noise, hence error correction is required for both the QuC and the classical syndrome-feedback channel. Consequently, for the multidimensional reconciliation scheme, the receiver has to perform two separate FEC decoding actions, namely one for the QuC and one for the ClC.[2] This creates an imbalance in terms of the reconciliation complexity, heavily burdening one side. Furthermore, the classic syndrome-based QKD reconciliation system is limited to syndrome-based codes such as LDPC codes, while the family of convolutional codes (CCs) that are often included in communication standards [84], [85] have not been used in the open literature. Against this background, the novel contributions of this work are as follows:

- Firstly, the block error rate (BLER) performance is analyzed in the context of syndrome-based reconciliation systems, where the ClC is initially assumed to be error-free, and both the bit-flipping (BF) and belief propagation (BP) based decoding algorithms are harnessed. More explicitly, we revise Gallager's sum-product algorithm (SPA) for LDPC codes using BP, where both the codeword transmitted through the QuC and the side information conveying the syndrome through the authenticated ClC can be accepted as the input of the modified SPA. Our performance results confirm that the revised BP decoder substantially outperforms the conventional BF decoder in terms of the secret key rate (SKR) of the QKD system.
- Secondly, for the first time in the literature, the effect of a realistic imperfect ClC is characterized for syndrome transmission from Bob to Alice, where reverse reconciliation (RR) is considered and the effects of both fading as well as of noise are taken into account. We demonstrate that the QKD system requires error correction for both the quantum and ClC. Consequently, the receiver has to perform FEC decoding of the potentially corrupted encoded syndrome for transmission over the ClC, and FEC decoding of the corrupted reference key sent from Bob over the ClC, making the decoding complexity unbalanced that burdens the receiver side. This calls for clean-slate considerations for a new QKD system design.
- Thirdly, a new bit-difference based CV-QKD reconciliation scheme is proposed, where Bob transmits the key through the QuC to Alice, and Alice carries out decoding with the aid of the bit-difference side information sent by Bob through the ClC to Alice. The bit-difference side information is constituted by the vector of bit differences between the key and a legitimate LDPC codeword. This regime allows us to use any arbitrary FEC codes. Our performance results confirm that for a specific FEC this new system has the same performance as the conventional syndrome-based CV-QKD [61], but again, it is compatible with any FEC schemes, including polar codes, CCs and irregular convolutional codes (IRCCs).
- Since the bit-difference vector based CV-QKD system still requires Alice to perform FEC decoding for both the QuC and ClC, a new codeword-based QKD reconciliation system is proposed. In this system, Alice sends a FEC-protected classical key (CK) to Bob through the ClC, while Bob sends a separate FEC protected quantum

[1] As for the multidimensional reconciliation, it attains higher reconciliation efficiency than slice based reconciliation due to the fact that there is no quantization process, which can cause performance degradation, and also that the capacity of the virtual established channel gets closer to the capacity of additive white Gaussian noise (AWGN) channel at a low SNR [82]. However, its throughput is limited to 1 bit, hence making it more suitable for long-range CV-QKD transmission system. By contrast, the slice based reconciliation, especially the multilevel coding and multistage decoding aided slice based reconciliation, has the capability of extracting more than 1 bit of information per channel use (bpcu), especially for higher SNRs. This is achieved at the cost of poor quantization performance in the low SNR region, making it more suitable for a short range CV-QKD transmission system.

[2] Note that the QuC and ClC of CV-QKD will be detailed in Section II-B.

key (QK) to Alice through the QuC.[3] Upon a FEC decoding performed at both sides, the final key to be used for the message encryption is the modulo-2 sum of the CK and QK.[4] As a result, for the first time in the open literature, our proposed codeword-based CV-QKD system achieves the following novelties. **Firstly**, the proposed scheme ensures protection of both the QuC and the ClC by FECs. **Secondly**, the system conceived has a symmetric complexity, where both Alice and Bob have an FEC encoder and an FEC decoder. **Thirdly**, the proposed QKD reconciliation scheme is compatible with a wide range of FEC schemes, including polar codes, CCs and IRCCs, where a near-capacity performance can be achieved for both the QuC and for the ClC.

- Our performance results demonstrate that with the aid of IRCCs, near-capacity performance can be achieved for both the quantum and the ClC, which leads to an improved SKR that inches closer to both the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [86] and the maximum achievable rate bound [87]. Therefore, the proposed codeword-based QKD reconciliation system facilitates flexible FEC deployment and it is capable of increasing the secure transmission distance.

The rest of this paper is structured as follows. Section II describes one of the classic CV-QKD protocols [13], [61], relying on a commonly utilized reconciliation scheme. Furthermore, some LDPC basics are introduced together with the modified BP[5] decoding algorithm used in the reconciliation schemes. Following this, different system designs are proposed and compared in Section III. The corresponding security analysis in terms of SKR is conducted in Section IV. Then, Section V presents the BLER and BER performance of different systems, where the performance of the proposed FEC aided CV-QKD is analyzed. Finally, Section VI provides our main conclusions and future research ideas. The structure of this paper is shown in Fig. 2.

Notations: In this paper, bold uppercase and lowercase represent matrices and vector, respectively; $\|\cdot\|$ denotes the Frobenius norm, and $(\cdot)^T$ denotes the transpose operation. A list of abbreviations and a list of variables are offered in the beginning of our paper.

[3]Note that in our proposed codeword-based reconciliation system the QK is defined as the specific part of the key that is transmitted through the QuC, while the CK is defined as the remaining part of the key that is transmitted through the ClC. This is different from the terminology of key used in Systems A-C, where the key is only transmitted through the QuC with the aid of some side information.

[4]We note that in the conventional syndrome-based QKD [61], even if Eve infers the syndrome from the ClC, she still cannot extract the QK from the QuC. Similarly, in the proposed system, even if Eve obtains the CK that is suitable for any FEC codes, she still cannot acquire the QK from the QuC. The QKD's Heisenberg's uncertainty principle remains valid for the quantum transmission. As a benefit, the SKR will be improved by using our powerful IRCC FEC schemes for both the ClC and the QuC despite considering realistic imperfect channels.

[5]The modified BP decoding algorithm is different from the original BP decoding algorithm, because the check node update BP contains a sign flipping term that depends on the syndrome information. The revised Gallager SPA is summarized in Algorithm 1.

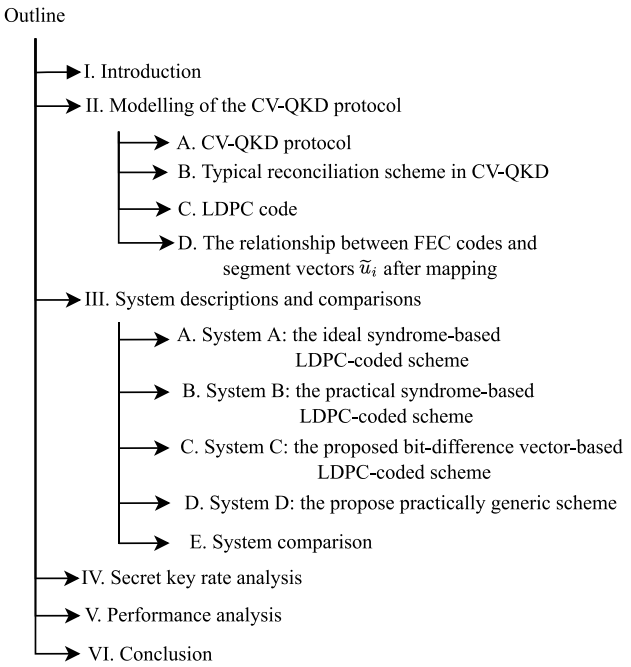


FIGURE 2. Structure of this paper.

II. MODELLING OF THE CV-QKD PROTOCOL

In this section, a general CV-QKD scheme[6] is modelled, which contains both the quantum transmission and classical post-processing. Following this, the important post-processing step of multidimensional reconciliation is detailed. Finally, the modified BP decoding is conceived for the reconciliation scheme.

A. CV-QKD PROTOCOL

The basic QKD protocol is shown in Fig. 3(a), which has a quantum processing part and a classical post-processing part. As for the quantum processing part, Alice prepares Gaussian-modulated coherent states for transmission to Bob. After receiving the signal, Bob makes a measurement relying either on homodyne or on heterodyne detection. This is followed by the classical post-processing part. Explicitly, the signal $\mathbf{y}$ of Fig. 3(a) is a sifted and potentially channel-infested version of $\mathbf{x}$, which suffers from the hostile action of the QuC. Observe in the figure that the post-processing part contains four steps, namely the sifting, parameter estimation, reconciliation, and privacy amplification.

1) QUANTUM TRANSMISSION PART

Firstly, Alice generates a pair of independent Gaussian distributed random variables, denoted as $q_A, p_A \sim \mathcal{N}(0, V_s)$, where V_s is the variance of the initial Gaussian signal. Then she uses the random variables q_A, p_A to generate a coherent state $|\alpha\rangle$ associated with $\alpha = q_A + jp_A$ for transmission. As for Eve, we consider an optimal eavesdropping attack,

[6]In this paper, the Gaussian modulated coherent state based CV-QKD protocol is considered.

TABLE 2. Novel contributions of this work in comparison to the state-of-the-art schemes.

Contributions	**This work**	[78]	[13]	[83]	[63]	[64]	[65]	[66]	[67]	[68]	[88]	[75]	[77]	[81]
DV-QKD(BSC)											✓			
CV-QKD(AWGN)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	
Hard-decoding	✓													✓
Soft-decoding incorporates syndromes	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
AWGN/Rayleigh for the classical authenticated channel	✓													
Balanced decoding complexity for Alice and Bob	✓													
Compatible application with LDPC, CC, polar codes, IRCC	✓													
Near-capacity for both classical & quantum part	✓													

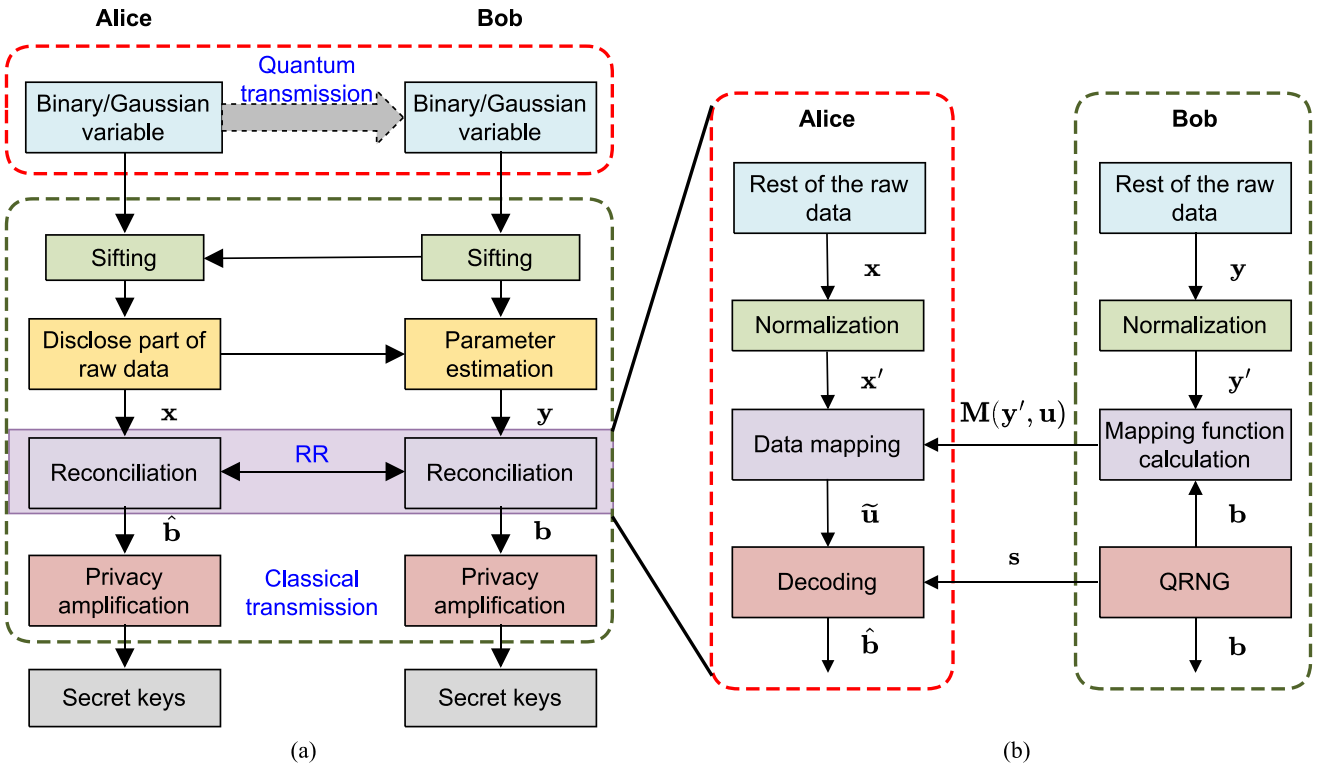


FIGURE 3. (a) Schematic diagram of a QKD protocol. Note that a binary variable is utilized in DV-QKD systems, whilst a Gaussian variable is utilized in CV-QKD systems. Moreover, as for the quantum transmission shown here, it contains the process of converting the binary/Gaussian variable to quantum states and that of converting the quantum states to binary/Gaussian variable, which is the quantum measurement. (b) Schematic of the multidimensional RR scheme in QKD, where x and y are two correlated Gaussian sequences, while x′ and y′ represent their normalized counterparts; M(y′, u) represents the mapping function sent from Bob to Alice; b denotes the initial sequence generated by QRNG; $\mathbf{u} = (\frac{(-1)^{b'(1)}}{\sqrt{8}}, \frac{(-1)^{b'(2)}}{\sqrt{8}}, \ldots, \frac{(-1)^{b'(8)}}{\sqrt{8}})$ denotes the spherical codes of b′, which is the interleaved bit stream of b; ũ is the sequence before decoding and b̂ is the decoding result that is equal to b when the decoding is successful; s denotes the additional side information, which is normally the syndrome calculated based on Bob's bit stream. Note that the dimensionality D is set 8.

namely the so-called Gaussian collective attack that can be implemented by the Gaussian entangling cloner attack, where Eve has full control over the channel [89]. Generally, Eve prepares the ancilla modes, which are two-mode squeezed states also known as Einstein-Podolsky-Rosen (EPR) states, with variance W. The modes of the EPR states can be described by the operators $\hat{E}$ and $\hat{E}''$, where Eve keeps one of the modes such as $\hat{E}''$ and injects the other mode $\hat{E}$ into the channel. After the interaction with Alice's state Eve gets the output result $\hat{E}'$. Eve then collectively detects both modes of $\hat{E}'$ and $\hat{E}''$, gathered from each run of the protocol, in a final coherent measurement. Based on this, the output mode at Bob's side can be expressed as

$$\hat{a}_B = \sqrt{T}\hat{a}_A + \sqrt{1-T}\hat{a}_E, \tag{1}$$

where $\sqrt{T}$ represents the transmission coefficient of the link between Alice and Bob, $\hat{a}_A$ and $\hat{a}_E$ respectively represent the transmitted mode of Alice associated with the coherent state

$|\alpha\rangle$ and the injected Gaussian mode of Eve, and $\sqrt{1-T}\hat{a}_E$ can be considered as a noise term.

For each of the received modes, Bob applies homodyne measurement to one of the randomly chosen quadratures, i.e., the Q or the P quadrature. After the measurement, the input-output relationship between Alice and Bob is given by

$$\hat{X}_B = \sqrt{T}\hat{X}_A + \sqrt{1-T}\hat{X}_E, \tag{2}$$

and the input-output relationship of Eve's ancilla mode is

$$\hat{X}_{E'} = -\sqrt{1-T}\hat{X}_A + \sqrt{T}\hat{X}_E, \tag{3}$$

where $\hat{X}_B$ is the received quadrature component, which is measured at Bob, $\hat{X}_A$ is the quadrature component transmitted by Alice, $\hat{X}_E$ is the excess noise quadrature component introduced by Eve, and $\hat{X}_{E'}$ is the ancilla quadrature component stored in Eve's quantum memory. Note that the variable $\hat{X}$ corresponds to one of the two quadrature components $\{\hat{q}, \hat{p}\}$, so that we have $\hat{X} \in \{\hat{q}, \hat{p}\}$, which is held for $\hat{X}_A, \hat{X}_B$, $\hat{X}_E$ and $\hat{X}_{E'}$. The variance of Alice's transmitted mode is $V_A = V_s + V_0$, where V_s is the variance of the initial Gaussian signal and V_0 is the variance of the vacuum state, and $V_E = W$ is the variance of the excess noise injected by Eve. The variance of the vacuum state can be expressed as

$$V_0 = 2\bar{n} + 1, \tag{4}$$

where $\bar{n} = [\exp(hf_c/K_B T_e) - 1]^{-1}$ while h is Planck's constant, k_B is Boltzmann's constant and T_e is the environmental temperature in Kelvin.

2) CLASSICAL POST-PROCESSING PART

- *Sifting:* In the sifting step of Fig. 3(a), both Alice and Bob retain the data associated with those specific states, whose preparation and measurement basis happen to be the same, given that both their bases are randomly chosen. More explicitly, in the BB84 DV-QKD example, Bob randomly chooses one of two legitimate polarization bases to measure his data received from Alice. Then they both publicly communicate with each other to agree about the particular bit-indices, where the measurement basis of Bob is the same as the preparation basis of Alice.
- *Parameters estimation:* In this step of Fig. 3(a), Alice and Bob will reveal and compare a random subset of the data, which allows them to estimate some parameters, such as the transmissivity (pathloss coefficient), excess noise, and the SNR of the channel. Then the mutual information (MI) between them is calculated to judge whether this channel is secure enough for supporting their communication. If the MI between Alice and Bob is higher than Eve's information concerning the key, the channel is deemed to be secure enough for supporting secret keys transmission, otherwise, the transmission aborts and a new random process is initiated.
- *Reconciliation:* The reconciliation step of Fig. 3(a) relies on error correction. There are two styles of reconciliation, namely direct reconciliation (DR) and RR. As for DR, Bob corrects his data according to Alice's data, while Alice's data remains unmodified. By contrast, in RR, Alice corrects her data according to Bob's data and Bob's data remains unmodified. Usually, RR is preferred since it can provide longer secure transmission distance than that of DR. More explicitly, in DR, the channel's transmission coefficient must be above 0.5 to provide a non-zero SKR, while there is no such limitation in the RR case [48], [90].
- *Privacy amplification:* Finally, the last step of Fig. 3(a) is privacy amplification harnessed for reducing Eve's probability of successfully guessing (a part of) the keys, since Eve has a certain amount of information concerning the key. A hashing function may be used for privacy amplification. For example, a universal hashing function can be used to complete the privacy amplification via turning the reconciled key stream into a shorter-length final key stream. As for the amount by which the reconciled key is shortened, this depends on how much information Eve has gained about the key.

B. TYPICAL RECONCILIATION SCHEME IN CV-QKD

Again, a multidimensional reconciliation method is considered, since it exhibits better performance in the lower SNR region, which may translate into a longer secure transmission distance [78]. The multidimensional reverse reconciliation process is shown in Fig. 3(b). After the disclosure of the raw data to be used for parameter estimation, as seen in Fig. 3(a), the rest of their raw data $x := \hat{X}'_A$ and $y := \hat{X}'_B$ is constituted by a pair of correlated Gaussian distributed sequences, where $x \sim \mathcal{N}(0, \sigma_x^2)$, and $y = x+n$, $n \sim \mathcal{N}(0, \sigma_n^2)$. Then both Alice and Bob choose D for representing the number of dimensions in the multidimensional reconciliation, which defines how the sequence of transmit data is partitioned into shorter segments. It was shown in [78] that the mapping function used in the multidimensional reconciliation process only exists in $\mathbb{R}, \mathbb{R}^2, \mathbb{R}^4, \mathbb{R}^8$ dimensions, which corresponds to $D = 1, 2, 4, 8$, due to its algebraic structure as proven by [78, Th. 2]. Moreover, it was demonstrated in [13], [67], [72], [78] that an eight-dimensional reconciliation scheme ($D = 8$) outperformed the schemes associated with $D = 1, 2, 4$ in terms of the BLER performance attained. Therefore, usually the eight-dimensional ($D = 8$) reconciliation scheme is adopted for practical CV-QKD systems [13], [72], [78]. The main steps of multidimensional RR can be described as follows.

1) Firstly, the rest of the raw data of Alice and Bob, can be viewed as a pair of sequences, denoted as $\mathbf{x}$ and $\mathbf{y}$. The length of the two sequences is set to the FEC codeword length N. Then they are partitioned into $I = N/8$ number of shorter segments, denoted as $\mathbf{x} = [\mathbf{x}_1; \mathbf{x}_2; \cdots; \mathbf{x}_I]$ and $\mathbf{y} = [\mathbf{y}_1; \mathbf{y}_2; \cdots; \mathbf{y}_I]$, where $\mathbf{x}_i$, $\mathbf{y}_i$, $i = 1, 2, \ldots, I$, are 8×1 column vectors.
2) Both Alice and Bob will normalize each 8-element segment of $\mathbf{x}$ and $\mathbf{y}$ in order to get a uniformly distributed

8-element vector, which is reminiscent of producing equi-probable 2^8-ary symbols. To elaborate on the resultant eight-dimensional reconciliation scheme, the normalized data in the form of the vectors $\mathbf{x}'_i$ and $\mathbf{y}'_i$ can be obtained by $\mathbf{x}'_i = \frac{\mathbf{x}_i}{\|\mathbf{x}_i\|}$ and $\mathbf{y}'_i = \frac{\mathbf{y}_i}{\|\mathbf{y}_i\|}$, where we have $\|\mathbf{x}_i\| = \sqrt{\langle \mathbf{x}_i, \mathbf{x}_i \rangle} = \sqrt{\sum_{d=1}^{8} \mathbf{x}_i(d)^2}$ and $\|\mathbf{y}_i\| = \sqrt{\langle \mathbf{y}_i, \mathbf{y}_i \rangle} = \sqrt{\sum_{d=1}^{8} \mathbf{y}_i(d)^2}$. Hence, both the normalized vectors $\mathbf{x}'_i$ and $\mathbf{y}'_i$ are uniformly distributed on the surface of the 8-dimensional unit-radius sphere. Therefore, spherical codes [78], where all codewords lie on a sphere centered on 0 can play the same role for CV-QKD as binary codes for DV-QKD.

3) Bob randomly generates a binary stream $\mathbf{b}$ using a quantum random number generator (QRNG),[7] whose length is the same as the FEC codeword length N. Then, the random bit sequence $\mathbf{b}$ will be interleaved into $\mathbf{b}'$ and the resultant sequence $\mathbf{b}'$ is partitioned into $\mathbf{b}' = [\mathbf{b}'_1; \mathbf{b}'_2; \cdots; \mathbf{b}'_I]$, where $\mathbf{b}'_i$ is an 8-element binary column vector. Then each segment $\mathbf{b}'_i$, $i = 1, 2, \ldots, I$, will be mapped to the 8-dimensional unit-radius sphere of $\mathbf{u}_i = (\frac{(-1)^{\mathbf{b}'_i(1)}}{\sqrt{8}}, \frac{(-1)^{\mathbf{b}'_i(2)}}{\sqrt{8}}, \ldots, \frac{(-1)^{\mathbf{b}'_i(8)}}{\sqrt{8}})$.
4) Bob calculates the mapping function for each segment based on the vectors $\mathbf{u}_i$ and $\mathbf{y}'_i$. This mapping function is used to map $\mathbf{y}'_i$ to $\mathbf{u}_i$ so as to find the relationship between the normalized Gaussian vector $\mathbf{y}'_i$ and the modulated stream $\mathbf{u}_i$, which is represented by a phase rotation between $\mathbf{y}'_i$ and $\mathbf{u}_i$ in the case of $D = 2$, as can seen in Fig. 4. More details about how the mapping function works for our scheme can be seen in our following discourse. On the other hand, Bob also has to calculate the side information represented by the syndrome $\mathbf{s}$ used for assisting the decoding process. This side-information decoding is slightly different for different reconciliation schemes. To elaborate further, initially we assume that LDPC codes are adopted in the reconciliation scheme considered in this paper. However, it is not necessary to encode $\mathbf{b}$ using LDPC codes, where the side information $\mathbf{s}$ could be the syndrome calculated from $\mathbf{b}$. But again, the side information is not necessarily constituted by the syndromes in other application scenarios. For example, frozen bits are used as side information in polar code-based reconciliation schemes [55], [76]. Then Bob publicly transmits both the mapping function $\mathbf{M}_i(\mathbf{y}'_i, \mathbf{u}_i)$ and the syndrome $\mathbf{s}$ to Alice through the classical communication channel. The details of the mapping function calculation can be found in [78] and are also shown in the Appendix.
5) Alice then applies the same mapping function to her normalized segment $\mathbf{x}'_i$ in order to map the Gaussian variables to $\widetilde{\mathbf{u}}_i = \mathbf{M}_i(\mathbf{y}'_i, \mathbf{u}_i)\mathbf{x}'_i$, which is actually the noisy version of $\mathbf{u}_i$. Hence, the difference between the variable $\mathbf{u}_i$ and its noisy version $\widetilde{\mathbf{u}}_i$ can reflect the quality of the QuC. Hence it may be exploited for eavesdropping detection.
6) After the mapping operation harnessed for each segment at Alice's side, she then concatenates all the segments into a sequence $\widetilde{\mathbf{u}} = [\widetilde{\mathbf{u}}_1; \widetilde{\mathbf{u}}_2; \cdots; \widetilde{\mathbf{u}}_I]$ having the length of N. Furthermore, the sequence $\widetilde{\mathbf{u}}$ is turned into $\widetilde{\mathbf{u}}'$ after deinterleaving. She finally carries out the decoding of $\widetilde{\mathbf{u}}'$ with the aid of the syndrome $\mathbf{s}$ calculated by Bob and obtains the secret key $\hat{\mathbf{b}}$.

[7]Note that the QRNG generates classical random numbers.

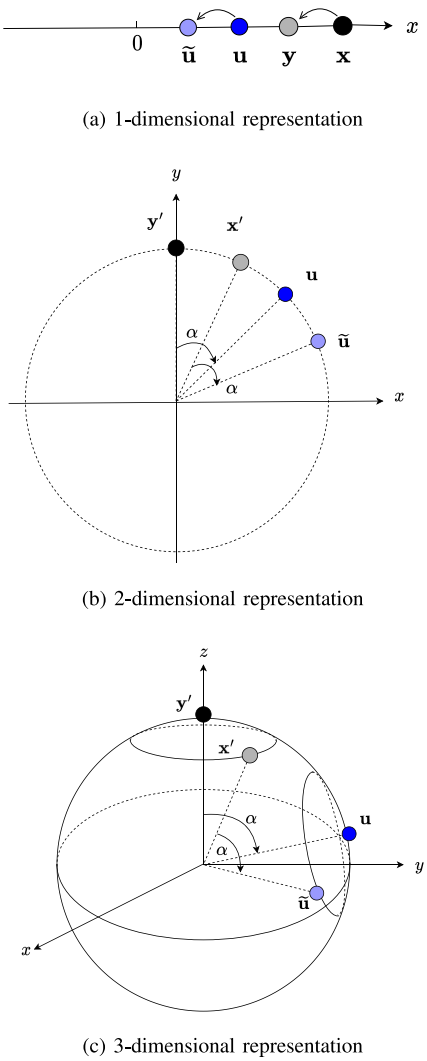


FIGURE 4. The representation of the noise conversion process for $D = 1,2$ and 3 based on [78].

In summary, the core idea of multidimensional reconciliation is to convert the noise in the QuC to the ClC via using the specific mapping functions $\mathbf{M}_i(\mathbf{y}'_i, \mathbf{u}_i)$. As a consequence, the noisy version $\widetilde{\mathbf{u}}$ of $\mathbf{b}$ is obtained, hence the family of commonly used FEC schemes can be applied to CV-QKD. More specifically, Fig. 4 demonstrates this conversion

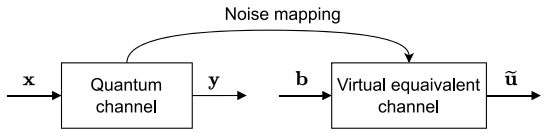


FIGURE 5. The relationship between the QuC and the virtual equivalent channel.

process from three different dimensionalities,[8] that are D=1, 2, 3, respectively. In Fig. 4(a), the noisy version $\tilde{\mathbf{u}}$ of $\mathbf{u} = +1$ can be obtained based on the proportion of $\mathbf{y}$ to $\mathbf{x}$ in a 1-dimensional case. Note that the values of $\mathbf{x}$ and $\mathbf{y}$ are not normalized in the 1-dimensional case. As for the 2-dimensional case of Fig. 4(b), the normalized vectors $\mathbf{y}'$ and $\mathbf{x}'$ are on the unit-circle, and we have $\mathbf{u} = [\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}]^T$. Firstly, Bob calculates the mapping function between $\mathbf{y}'$ and $\mathbf{x}'$, corresponding to α, which physically represents the phase rotation operation. After Alice receives the mapping function, she uses it to get the noisy version $\tilde{\mathbf{u}}$ of $\mathbf{u}$ by rotating $\mathbf{x}'$ with the same angle α. Similarly, for the 3-dimensional case seen in Fig. 4(c), the mapping function can be calculated based on $\mathbf{y}'$ and $\mathbf{u}$ on the surface of the unit-radius sphere. Then the noisy version of $\mathbf{u}$, namely $\tilde{\mathbf{u}}$ can be obtained by applying the same mapping function to $\mathbf{x}'$. As for how strong the noise is, it depends on the quality of the QuC, which is modelled by a virtual equivalent binary-input AWGN (BI-AWGN) ClC characterized in Fig. 5. This is reminiscent of classical modulation and transmission through the AWGN channel [78]. After that, FEC decoding can be applied and finally the reconciled key is generated.

To elaborate a little further, the 2-dimensional reconciliation of a segment is exemplified to illustrate this process. Firstly, after Alice and Bob finish their quantum-domain transmission and detection, sifting and parameter estimation, as well as normalization, they have two sequences, which are $\mathbf{x}'_1 = [0.8865, -0.4626]^T$, $\mathbf{y}'_1 = [0.9748, -0.229]^T$. Let us assume that the random bit stream after interleaving at Bob's side is $\mathbf{b}'_1 = [0, 0]^T$ along with the corresponding $\mathbf{u}_1 = [0.7071, 0.7071]^T$. Then the resultant mapping matrix can be calculated as $\mathbf{M_1}(\mathbf{y}'_1, \mathbf{u}_1) = \begin{bmatrix} -0.7618 & -0.6479 \\ 0.6479 & -0.7618 \end{bmatrix}$, where $\mathbf{M}_1(\mathbf{y}'_1, \mathbf{u}_1) = \sum_{d=1}^{2} \alpha_1^d \mathbf{A}_2^d$. Note that the pair of orthogonal matrices used in this 2-dimensional scheme are $\mathbf{A}_2^1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\mathbf{A}_2^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Furthermore, α_1^d is the specific element of $\boldsymbol{\alpha}_1(\mathbf{y}'_1, \mathbf{u}_1) = (\mathbf{A}_2^1\mathbf{y}'_1, \mathbf{A}_2^2\mathbf{y}'_1)^T \cdot \mathbf{u}_1$, which is the coordinate of the vector $\mathbf{u}_1$ under the orthonormal basis $(\mathbf{A}_2^1\mathbf{y}'_1, \mathbf{A}_2^2\mathbf{y}'_1)$ [78]. Based on this, the sequence $\tilde{\mathbf{u}}_1$ at Alice's side after data mapping becomes $\tilde{\mathbf{u}}_1 = \mathbf{M}(\mathbf{y}'_1, \mathbf{u}_1)\mathbf{x}'_1 = [0.8632, 0.5049]^T$, which is a noisy version of $\mathbf{u}_1$. Furthermore, the noise in $\tilde{\mathbf{u}}_1$ is capable of reflecting the noise level of the quantum transmission between Alice and Bob. Therefore, in our ensuing discourse, the QuC is modelled by an equivalent BI-AWGN ClC.

[8] As stated that the dimensionality of multidimensional reconciliation can be chosen to be 1, 2, 4 and 8. Here for convenience we exemplify this process via using visible 1, 2 and 3 dimensionalities.

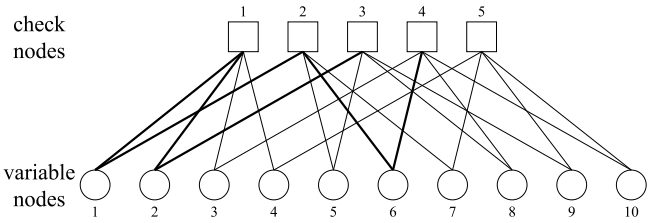


FIGURE 6. The Tanner graph for the code given in Eq. (5).

C. LDPC CODE

LDPC codes constitute a class of linear block codes defined by a sparse parity-check matrix (PCM) $\mathbf{H}$ of size $(N-K) \times N$, $K \leq N$, where N is the number of columns in $\mathbf{H}$ and it is also known as the block length, while $(N-K)$ is the rank of $\mathbf{H}$. Hence, the code rate is $R = K/N$. A $[N, K]$-regular LDPC code is defined as the null space of a sparse PCM, where each row of $\mathbf{H}$ contains exactly d_c ones, which is also called the degree d_c of check nodes (CNs). Each column of $\mathbf{H}$ contains exactly d_v ones, which is also called the degree d_v of variable nodes (VNs). Both the degrees of CNs and VNs are small compared to the number of rows in $\mathbf{H}$. An LDPC code is classified as being irregular if the row weight d_c and column weight d_v are not constant. It is often helpful to use the so-called Tanner graph to represent the PCM $\mathbf{H}$ [91]. In the Tanner graph representation, there are two types of nodes, which are the VNs (or code-bit nodes) and CNs (or constraint nodes), respectively. If an element of $\mathbf{H}_{i,j}$ is equal to one, then CN i denoted as c_i is connected by an edge to VN j denoted as v_j in the Tanner graph. Otherwise, there is no connection between them. The notion of degree distribution is used for characterizing the check and variable node degrees [92]. For example, as shown in Fig. 6, for the first VN, there are two edge connections seen in bold lines with the first and second CN. In a similar fashion, the second VN is connected with the first and third CN. The corresponding PCM $\mathbf{H}$ is formulated as

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{10\times 5}, \tag{5}$$

which is a [10, 5]-regular LDPC code having the code length of $N = 10$ and code rate of $R = 0.5$, the row weight is $d_c = 4$ and the column weight is $d_v = 2$. The notation of $[N, K]$-regular LDPC code used from now on to represent regular LDPC codes having a code length of N, and information length of K.

LDPC decoding is popularly performed using the BP algorithm [93], which is an iterative message-passing algorithm commonly used for inference based on graphical

Algorithm 1 The Modified Sum-Product Algorithm of Gallager

1: **Initialization:** Initialize LLR at each VN, $v = 1, 2, ..., n$ for the appropriate channel model. Then, for all i, j for which $h_{i,j} = 1$, set $L^{l}_{v\to c} = L^{0}_{v\to c}$.

2: **CN update:** Compute outgoing CN messages $L_{c\to v}$ for each CN using

$$L^{t}_{c\to v} = (-1)^{\mathbf{s}_B(c)} \cdot 2\tanh^{-1}\left(\prod\nolimits_{v'\in V_c\backslash v}\tanh\left(\frac{L^{t-1}_{v'\to c}}{2}\right)\right),$$

and then transmit to the VN.

3: **VN update:** Compute outgoing VN messages $L_{v\to c}$ for each VN using

$$L^{t}_{v\to c} = \begin{cases} L^{0}_{v\to c} \\ L^{0}_{v\to c} + \sum_{c'\in C_v\backslash c} L^{t}_{c'\to v} \end{cases} \quad \text{if } t \geq 1,$$

and then transmit to the CN.

4: **LLR total:** For $v = 1, 2, ..., n$ compute

$$L^{total}_{v} = L^{0}_{v\to c} + \sum\nolimits_{c'\in C_v} L^{t}_{c'\to v}.$$

5: **Stopping criterion:** Hard decision and early termination check:

$$\hat{C}^{(t)}_{v} = \begin{cases} 0, & L^{total}_{v} \geq 0 \\ 1, & \text{otherwise} \end{cases}.$$

If $\hat{\mathbf{C}}\mathbf{H}^T = \mathbf{s}_B$ or the number of affordable iterations reaches the maximum limit, stop; else, go to step 2.

models such as factor graphs [94]. In the context of LDPC codes, the decoding procedure attempts to find a valid codeword by iteratively exchanging the probabilistic information represented by the log-likelihood ratio (LLR) between the CN and VN along the edges of the Tanner graph until the parity-check condition is satisfied or the maximum affordable number of iterations is reached. More explicitly, we modify the classic Gallager SPA [93] for QKD systems, as seen in Algorithm 1, where both the codeword transmitted through the QuC and the side information constituted by the syndrome transmitted through the authenticated ClC are the inputs of the modified SPA.

In Algorithm 1, Step 1 prepares the LLR input values at each VN. All VN-to-CN messages arriving from VN v to CN c are initialized to the received LLR, denoted as $L^{0}_{v\to c}$ at the output of the channel before the first message-passing iteration. Then, Step 2 to Step 5 illustrate the process of finding the most likely codeword by iterative soft information exchange between CN and VN, until the syndrome defined by $\hat{\mathbf{C}}\mathbf{H}^T$ becomes zero, or the maximum affordable number of decoding iterations is reached. To elaborate further, in Step 2, $L^{t}_{c\to v}$ is the message arriving from CN to VN in iteration t, and $C_v\backslash c$ denotes all the CNs connected to VN v, except for CN c. In Step 3, $L^{t}_{v\to c}$ is the message coming from VN to CN in iteration t, and $V_c\backslash v$ is the set of VNs connected to CN c, except for VN v.

In contrast to the conventional SPA decoding algorithm, both the contaminated codeword received from the QuC and the side information received from the ClC are entered into the modified SPA of Algorithm 1. Normally, the side information refers to the syndrome calculated by Bob in the context of LDPC codes. Hence, the SPA decoding algorithm has to be modified. Specifically, we have to change the CN update operation, which is Step 2 in Algorithm 1, based on the syndrome $\mathbf{s}_B$ from Bob received by Alice. The modified CN update operation can be formulated as [13]

$$L^{t}_{c\to v} = (-1)^{\mathbf{s}_B(c)} \cdot 2\tanh^{-1}\left(\prod_{v'\in V_c\backslash v}\tanh\left(\frac{L^{t-1}_{v'\to c}}{2}\right)\right), \quad (6)$$

where $\mathbf{s}_B(c) \in \{0, 1\}$ represents the parity value at index c. It is plausible that if the syndrome is $\mathbf{s}_B(c) = 0$, the CN update operation remains the same as that of the conventional SPA. Otherwise, for $\mathbf{s}_B(c) = 1$, the CN update operation would flip the sign of the outgoing messages.

D. THE RELATIONSHIP BETWEEN FEC CODES AND SEGMENT VECTORS $\tilde{\mathbf{U}}_I$ AFTER MAPPING

Once an equivalent ClC has been setup for the QuC, an FEC scheme is needed to proceed. Therefore, in this section, we aim for clarifying how to connect the segment vectors $\tilde{\mathbf{u}}_i$ after mapping with FEC codes.

In Fig. 7, we consider 2-dimensional reconciliation and a [10,5] LDPC code. The PCM of Eq. (5), is used for illustrating the relationship between the FEC codes and segmented vectors $\mathbf{u}_i$. In Fig. 7, the dashed box at the left represents the relationship between the pair of Gaussian sequences, namely $\mathbf{y}$ and $\mathbf{x}$. Since we consider a [10, 5] LDPC code and a 2-dimensional reconciliation scheme ($D = 2$), each of the pair of Gaussian sequences of length $N = 10$, is divided into $I = N/D = 5$ segments, yielding $\mathbf{x} = [\mathbf{x}_1; \mathbf{x}_2; \mathbf{x}_3; \mathbf{x}_4; \mathbf{x}_5]$ and $\mathbf{y} = [\mathbf{y}_1; \mathbf{y}_2; \mathbf{y}_3; \mathbf{y}_4; \mathbf{y}_5]$, each of which contains 2 Gaussian elements, i.e., $\mathbf{x}_i = [\mathbf{x}^1_i, \mathbf{x}^2_i]$ for $i = 1, 2, \ldots, 5$ and $\mathbf{y}_i = [\mathbf{y}^1_i, \mathbf{y}^2_i]$ for $i = 1, 2, \ldots, 5$. Furthermore, it is assumed that within each segment the channel's fading coefficients remain constant. For example, we have $\mathbf{h}_1 = [\mathbf{h}^1_1; \mathbf{h}^2_1] = [h_1, h_1]$. On the other hand, the bit stream $\mathbf{b}$ generated by Bob's QRNG seen in Fig. 3(b) is correspondingly divided into 5 segments, i.e., $\mathbf{b} = [\mathbf{b}_1; \mathbf{b}_2; \mathbf{b}_3; \mathbf{b}_4; \mathbf{b}_5]$, each of which contains two elements, i.e., $\mathbf{b}_i = [\mathbf{b}^1_i, \mathbf{b}^2_i]$ for $i = 1, 2, \ldots, 5$. After interleaving, the new bit stream $\mathbf{b}'$ is obtained, which is also partitioned into 5 segments, i.e., $\mathbf{b}' = [\mathbf{b}'_1; \mathbf{b}'_2; \mathbf{b}'_3; \mathbf{b}'_4; \mathbf{b}'_5]$, where $\mathbf{b}'_i = [\mathbf{b}'^1_i, \mathbf{b}'^2_i]$ for $i = 1, 2, \ldots, 5$. In light of this, the affect of the channel's fading coefficient $\mathbf{h} = [\mathbf{h}_1; \mathbf{h}_2; \mathbf{h}_3; \mathbf{h}_4; \mathbf{h}_5]$ and noise $\mathbf{n} = [\mathbf{n}_1; \mathbf{n}_2; \mathbf{n}_3; \mathbf{n}_4; \mathbf{n}_5]$ in the QuC are used for representing the relationship between the modulated sequences $\mathbf{u} = [\mathbf{u}_1; \mathbf{u}_2; \mathbf{u}_3; \mathbf{u}_4; \mathbf{u}_5]$ based on $\mathbf{b}'$ and $\tilde{\mathbf{u}} = [\tilde{\mathbf{u}}_1; \tilde{\mathbf{u}}_2; \tilde{\mathbf{u}}_3; \tilde{\mathbf{u}}_4; \tilde{\mathbf{u}}_5]$. Note that it is assumed that the fading coefficients are known at both sides, and the noise variances of $\mathbf{n} = [\mathbf{n}_1; \mathbf{n}_2; \mathbf{n}_3; \mathbf{n}_4; \mathbf{n}_5]$ and $\mathbf{n}' = [\mathbf{n}'_1; \mathbf{n}'_2; \mathbf{n}'_3; \mathbf{n}'_4; \mathbf{n}'_5]$ are the same even thought the exact value of noise $\mathbf{n}'$ is not the same as $\mathbf{n}$ in the QuC. After deinterleaving, a

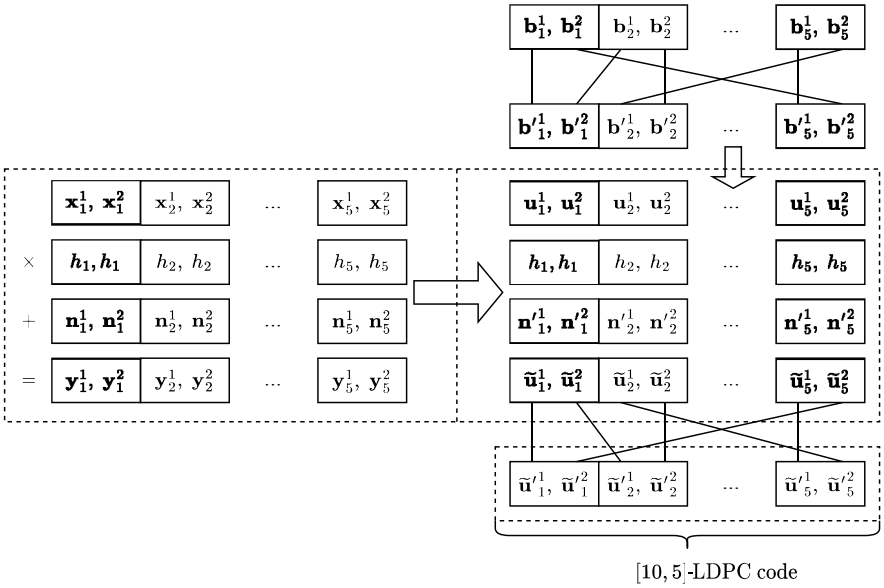


FIGURE 7. The relationship between FEC codes and segmented vectors. Note that a [10,5] LDPC code is applied and 2-dimensional reconciliation is adopted. Correspondingly, $N = 10$, $D = 2$, and $I = N/D = 5$.

reordered sequence $\widetilde{\mathbf{u}}' = [\widetilde{\mathbf{u}}'_1; \widetilde{\mathbf{u}}'_2; \widetilde{\mathbf{u}}'_3; \widetilde{\mathbf{u}}'_4; \widetilde{\mathbf{u}}'_5]$ of $\widetilde{\mathbf{u}}$ is derived, which represents the corrupted sequences of $\mathbf{b}$. Therefore, the sequence $\widetilde{\mathbf{u}}'$ of length 10 will be fed into the [10,5] LDPC decoder.

III. SYSTEM DESCRIPTIONS AND COMPARISONS

In this section, our new codeword-based reconciliation system will be proposed, following the critical appraisal of the state-of-the-art. More explicitly, four reconciliation systems will be presented in this section. In a nutshell,

1) *System A* represents the conventional LDPC-coded reconciliation scheme relying on the idealistic simplifying assumption that the ClC used for syndrome transmission is error-free.
2) *System B* takes into account the fading and noise effects of the ClC, where a separate LDPC code is required for both the QuC and the ClC. Note that System B is a practical version of System A.
3) *System C* is proposed to demonstrate that the bit-difference vector-based side information can play the same role as the syndrome of Systems A and B. Hence System C has the same performance as System A and System B.
4) *System D* represents the proposed codeword-based reconciliation scheme suitable for any arbitrary FEC code. Hence the family of powerful IRCCs can also be applied to achieve a near-capacity performance for both the QuC and ClC.

Note that the following reconciliation systems mainly focus on the details of the reconciliation step within the QKD protocol. More specifically, the BI-AWGN equivalent QuC of Fig. 5 is used here for the description of the reconciliation post-processing step.

A. SYSTEM A: THE IDEAL SYNDROME-BASED LDPC-CODED SCHEME

System A: The first reconciliation system shown in Figure 8 is the BF/BP decoding algorithm based LDPC-coded CV-QKD reconciliation scheme, where the ClC used for syndrome transmission is assumed to be error-free. The algorithmic steps are described as follows.

(a) Bob randomly generates a bit stream $\mathbf{C}$ using a QRNG, and we view this as the initial raw key $\mathbf{b}$ at his side. Note that, the QRNG generates classical random numbers. The length of this is determined by the codeword length of the predefined PCM $\mathbf{H}$. The PCM is known at both sides. Note that, the bit stream $\mathbf{b}$ at Bob's side does not have to be a legitimate codeword, because the final objective is to obtain a reconciled key. More specifically, in the reverse reconciliation scheme, the bit stream generated at Bob's side is the reference key, and Alice has to acquire this as the final key. Let us consider the single-error correcting [7,4,1] Bose-Chaudhuri-Hocquenghem (BCH) code as our rudimentary example, and assume that the bit stream generated by the QRNG in block (1) of Fig. 8 is $\mathbf{C} = [1111010]$. Then Bob treats this random bit stream as the initial key $\mathbf{b} = [1111010]$ in block (2) of Fig. 8.

(b) Bob transmits this bit stream $\mathbf{b} = [1111010]$ through a QuC to Alice, which is modelled by the equivalent ClC constructed in Fig. 5 and represented by block (3) of Fig. 8. The channel-contaminated sequence received by Alice is denoted by $\widetilde{\mathbf{b}} = [1111011]$ in block (4), which is corrupted in the last bit position.

(c) Meanwhile, based on the QRNG output Bob calculates the syndrome, say $\mathbf{s} = [100]$ in block (5) and transmits it as side information to Alice through the

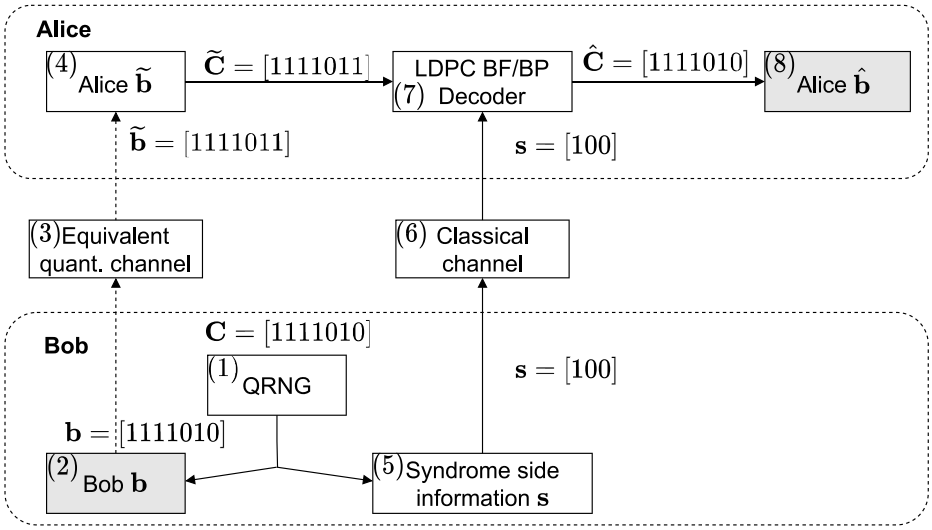


FIGURE 8. ***System A*** **- the ideal LDPC-coded syndrome-based reconciliation scheme in the CV-QKD system relying on the BF/BP decoding algorithm. Note that, the dashed arrow represents the bit stream sent from Bob to Alice through the equivalent QuCs as illustrated in Section II-B.**

authenticated ClC of block (6), which is assumed to be perfectly *noiseless and error-free*.

(d) Alice takes the bit stream $\widetilde{\mathbf{b}}$ inferred at the output of the QuC, which may or may not be a legitimate codeword, and forwards it as namely $\widetilde{\mathbf{C}} = [1111011]$ to the decoder. Decoding is carried out by the corresponding FEC decoder with the aid of the syndrome bits she received through the ClC (6) and gets the decoded result of $\hat{\mathbf{C}} = [1111010]$ at the output of block (7). Based on this, Alice gets the decoded codeword as the final reconciled key, which is $\hat{\mathbf{b}} = [1111010]$ shown in block (8). Observe that this is the same as Bob's bit stream $\mathbf{b}$, provided that there are no decoding errors. This is the case, if the QuC inflicts no more than a single error, since the [7,4,1] code can only correct a single error. It is important to mention here that if the classical syndrome-transmission channel inflicts errors, this would results in catastrophic corruption of the QuCs' output. This issue will be addressed by System B.

B. SYSTEM B: THE PRACTICAL SYNDROME-BASED LDPC-CODED SCHEME

System B: Following the above rudimentary BCH-coded example to introduce how System A works, let us now detail a practical LDPC code based scheme. System B of Fig. 9 represents the BP decoding algorithm based CV-QKD reconciliation scheme. In contrast to System A, System B no longer assumes that the ClC is error-free. Hence both the classical and the QuC require error correction. Let us consider a [1024,512] LDPC code as our example to introduce System B. More explicitly, the operational steps of System B are

(a) Bob randomly generates a 1024-bit stream using the QRNG of Fig. 9, and views this as the initial key $\mathbf{b}$ at his side. Note that, the QRNG generates classical random numbers. Again, the length of this is determined by the codeword length of the predefined LDPC PCM $\mathbf{H}$, which is known to both sides.

(b) Bob transmits this bit stream $\mathbf{b}$ through the equivalent QuC to Alice, who receives the bit stream as $\widetilde{\mathbf{b}}$.

(c) Meanwhile, Bob calculates the syndrome based on the QRNG output - namely $\mathbf{b}$ - as the side information $\mathbf{s}$ and transmits it to Alice through the authenticated ClC protected by the LDPC encoder in block (6) of Fig. 9. *Note that*, the rectangular frame shown in Fig. 9 that encompasses blocks (6)-(8), constitutes a separate FEC-aided data protection for the ClC, which relies on the LDPC 1 code. The dimensionality of the PCM of such LDPC codes in our example is 512×1024, and hence the syndrome $\mathbf{s} = \mathbf{H} \cdot \mathbf{b}$ calculated from Bob has the length of 512 bits. After the FEC scheme applied to the syndrome protection, which is protected by another [1024, 512] LDPC code, the encoded syndrome has the length of 1024 bits. Then, after being decoded at Alice's side by the LDPC 1 decoder (8), the syndrome $\mathbf{s}$ having 512 bits is recovered. In the literature [13], [63], [64], [65], [66], [67], [75], [77], [78], [81], [83], [88], the ClC is assumed to be *noiseless and error-free*, but a realistic ClC tends to inflict both fading and noise. Hence the ClC's LDPC 1 scheme of Fig. 9 may not be able to eliminate all errors imposed on the syndrome. Therefore, the performance of practical FEC schemes in the classical syndrome-transmission channel is taken into account in System B.

(d) Then Alice carries out *BP* decoding of the information received over the QuC with the aid of the syndrome bits to get $\hat{\mathbf{b}}$, as seen in block (9).

Note that, the syndrome-based scheme is limited to FEC codes that rely on syndromes, whereas other codes such as

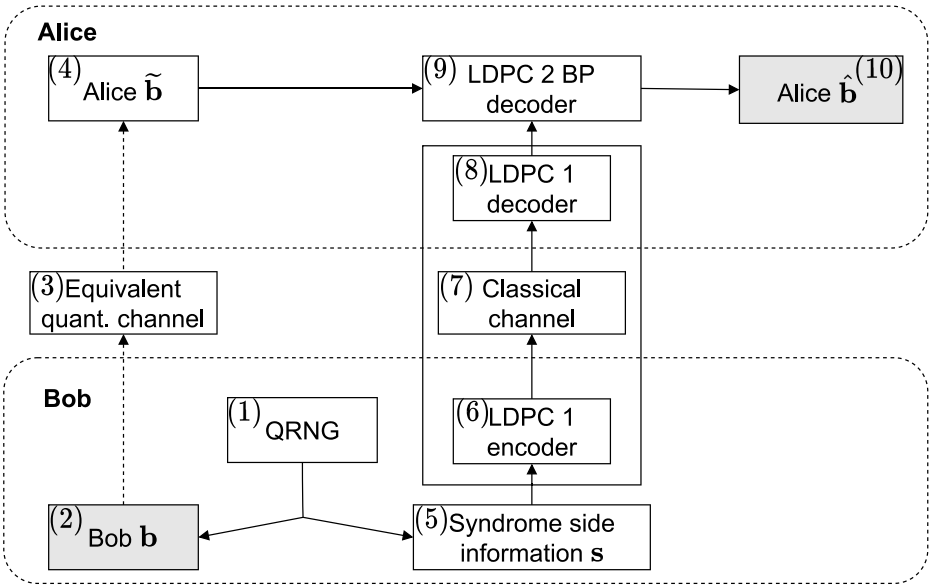


FIGURE 9. *System B* - the practical LDPC-coded syndrome-based reconciliation scheme in the CV-QKD system with BP decoding algorithm. Compared to System A, System B no longer assumes that the CIC is error-free, where both CIC and QuC require data protection by error correction.

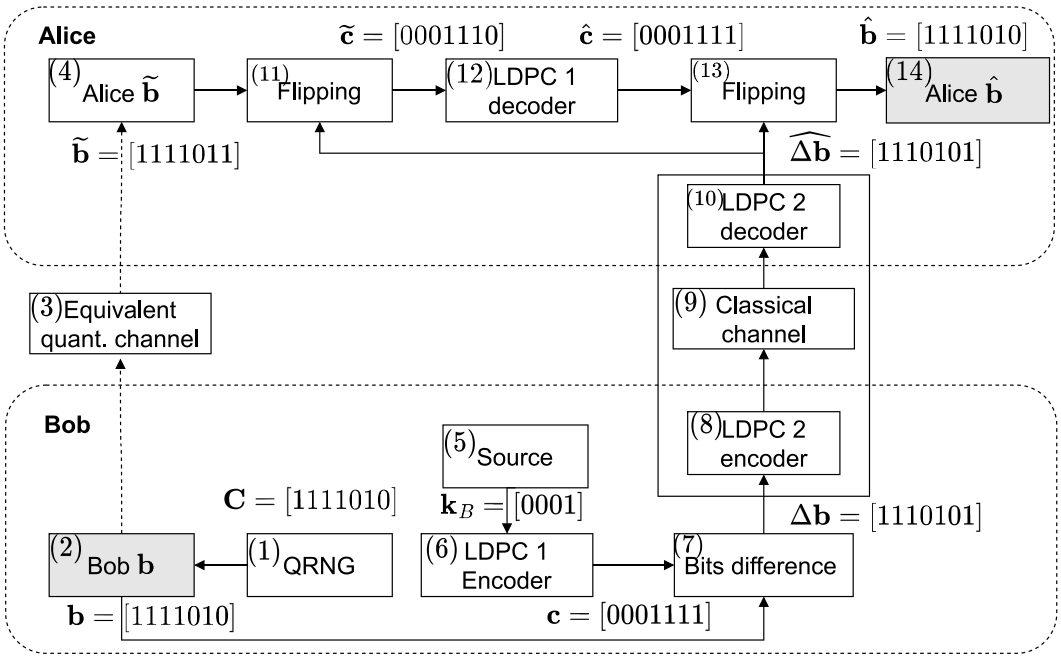


FIGURE 10. *System C* - the LDPC-coded bit-difference vector-based reconciliation scheme designed for CV-QKD systems and using the BP decoding algorithm.

polar codes and CCs cannot be applied. Therefore, the bit-difference vector-based scheme (System C) is proposed to tackle this issue, which is described as follows.

C. SYSTEM C: THE PROPOSED BIT-DIFFERENCE VECTOR-BASED LDPC-CODED SCHEME

System C of Figure 10, is our proposed scheme, where the final key generated by the QRNG is transmitted through the QuC and the syndromes of System B are replaced by the bit-difference vector. For convenience, both the QuC and the ClC may adopt the same kind of FEC codes, albeit they may have different length. The corresponding steps are described as follows.

(a) The functions of block (1) to (4) in Fig. 10 are the same as described in System A. Here, again a simple [7,4,1] BCH code is used as our rudimentary example. Specifically, the bit stream $\mathbf{b} = [1111010]$ may be obtained from the QRNG, which generates a bit stream C=[1111010], and it is transmitted from Bob to Alice through the QuC, resulting the corrupted bit stream $\widetilde{\mathbf{b}} = [1111011]$ at Alice's side. This has a single error in the last position.

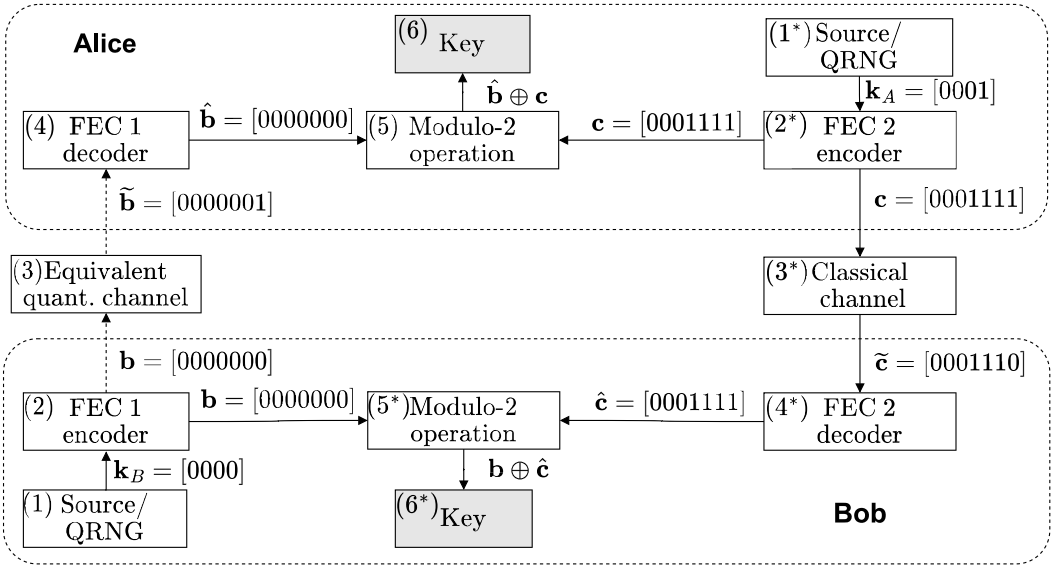


FIGURE 11. *System D* - the proposed practically generic reconciliation scheme designed for CV-QKD systems.

(b) In contrast to the way of calculating the syndrome in Systems A and B, a legitimate codeword $\mathbf{c} = [0001111]$ is required for deriving the bit-difference vector $\Delta\mathbf{b} = [1110101]$ based on blocks (5) to (7) in Fig. 10, where $\mathbf{k}_B = [0001]$ represents the corresponding random information bits used to obtain $\mathbf{c}$.

(c) Based on the received and protected bit-difference vector $\widehat{\Delta\mathbf{b}} = [1110101]$ at the output of block (10) in Fig. 10, Alice flips the bits of $\widetilde{\mathbf{b}}$ in those specific positions, where a logical 1 occurs in $\widehat{\Delta\mathbf{b}}$ at the output of block (3) in Fig. 10 to arrive at $\widetilde{\mathbf{c}} = [0001110]$ at the output of (11) before decoding.

(d) Alice then decodes the bit stream $\widetilde{\mathbf{c}} = [0001110]$ to arrive at $\hat{\mathbf{c}} = [0001111]$ after (12) to get the key $\hat{\mathbf{b}} = [1111010]$ at the output of block (13), which is ideally the same as $\mathbf{b}$ at Bob's side.

Observe in Fig. 9 (System B) and Fig. 10 (System C) that there are two LDPC decoders at Alice's side. By contrast, there is merely a single LDPC encoder and a low-complexity syndrome calculation scheme at Bob's side in System B, while two LDPC encoders are required at Bob's side in System C. Since Alice has to perform computationally demanding LDPC decoding twice in order to infer the final key, this is not a balanced-complexity system.[9] In light of these considerations, the new codeword-based reconciliation System D was proposed for arriving at a solution having a balanced-complexity, where Alice and Bob have a similar complexity, as required in device-to-device (D2D) systems for example [97], [98], which is described as follows.

[9]Even though System C is not a balanced-complexity system, there are practical scenarios, where having a balanced complexity is not imperative, such as in ground station to unmanned aerial vehicle (UVA) quantum communication [95], [96], etc.

D. SYSTEM D: THE PROPOSED PRACTICALLY GENERIC SCHEME

System D of Figure 11, is our proposed scheme that utilizes a pair of FEC codes to protect both the QuC and the classical authenticated channel. For convenience, both the QuC and the ClC may adopt the same kind of FEC codes. The corresponding steps are described as follows.

(a) Both Bob and Alice generate a legitimate codeword based on a pair of predefined PCMs $\mathbf{H}_1$ and $\mathbf{H}_2$, which are $\mathbf{b}$ and $\mathbf{c}$. Consider again a simple [7,4,1] BCH code as our rudimentary example, where the pair of legitimate codewords are $\mathbf{b} = [0000000]$ and $\mathbf{c} = [0001111]$, respectively, as indicated in Fig. 11. The corresponding uncoded information bits are for example $\mathbf{k}_B = [0000]$ and $\mathbf{k}_A = [0001]$, respectively.

(b) Bob transmits his legitimate codeword $\mathbf{b}$ through the QuC, which is modelled again by the equivalent ClC of Fig. 5. On the other hand, Alice transmits her legitimate codeword $\mathbf{c}$ through the ClC, which may inflict errors. Note that, the 2 LDPC codes in Fig. 11 do not have to be exactly the same code, whose PCMs are the same. However, for convenience, in our study, it is assumed that both QuC and ClC may adopt the same kind of FEC codes, which have exactly the same PCM. The codewords transmission over both the QuC and the ClC is independent. More specifically, the codeword $\mathbf{c}$ is transmitted the same as that in conventional wireless communication, whilst the codeword $\mathbf{b}$ is transmitted with the aid of the equivalent QuC of Fig. 5, where the relationship between the Gaussian signals transmitted over the QuC and the random bit stream generated by QRNG is leveraged as can be seen in Fig. 3(b).

TABLE 3. Comparisons between four different systems.

	System A	System B	System C	System D
Equivalent QuC	BI-AWGN channel			
ClC	Error-free	Noise and fading		
QK	Bob→Alice	Bob→Alice	Bob→Alice	Bob→Alice
Side information (CK)	Syndromes (Bob→Alice)		Bit-difference (Bob→Alice)	CK (Alice→Bob)
FEC types	Only LDPC	Only LDPC	Any	Any
Improvements over syndrome-based CV-QKD [61]	-	-	Near-capacity, compatible to any FEC	Near-capacity, balanced complexity, compatible to any FEC

(c) Both Alice and Bob carry out LDPC BP decoding to get $\hat{\mathbf{b}} = [0000000]$ and $\hat{\mathbf{c}} = [0001111]$, respectively.[10]
(d) Furthermore, Modulo-2 operation is carried out at both sides to obtain the final key for both Alice and Bob, which are $\hat{\mathbf{b}} \oplus \mathbf{c}$ and $\mathbf{b} \oplus \hat{\mathbf{c}}$, respectively.

The proposed System D is summarized in Algorithm 2.

As a benefit of this design, first of all, the proposed codeword-based - rather than syndrome-based - QKD reconciliation scheme protects both the QuC and ClC. Secondly, the system has a similar complexity for both Alice and Bob, each of whom has a FEC encoder and a FEC decoder. Thirdly, System D makes QKD reconciliation compatible with a wide range of FEC, including polar codes and the family of CCs. We will demonstrate in Section V that this design allows us to achieve a near-capacity performance for both the QuC and for the ClC.

Algorithm 2 Description of *System D*

1: **Codeword generation:**
Both Alice and Bob generate a legitimate codeword, which are $\mathbf{c}$ and $\mathbf{b}$.
2: **Codeword transmission:**
Bob transmits his legitimate codeword $\mathbf{b}$ through the equivalent QuC, which is the same process as in the System A, B and C. Meanwhile, Alice transmits her legitimate codeword $\mathbf{c}$ through the ClC.
3: **Decoding:**
Both Alice and Bob carry out FEC decoding.
4: **Modulo-2 operation:**
Modulo-2 operation is implemented at both sides to obtain the final key for both Alice and Bob, which are $\hat{\mathbf{b}} \oplus \mathbf{c}$ and $\mathbf{b} \oplus \hat{\mathbf{c}}$, respectively.

E. SYSTEMS COMPARISON

In summary, the comparisons between System A (ideal syndrome-based CV-QKD), System B (practical syndrome-based CV-QKD), System C (practical bit-difference vector based CV-QKD) and System D (codeword-based CV-QKD) are summarized in Table 3. More specifically, all four systems use the same equivalent QuC, but in System A we assume that the ClC is error-free, while in Systems B, C and D we consider realistic noise and fading in the ClC. Secondly, as for the side information, syndromes are transmitted from Bob to Alice through the ClC in both System A and System B. By contrast, instead of using the syndrome, System C transmits the bit-difference vector from Bob to Alice through the ClC, making the system compatible with any FEC. Furthermore, System D transmits the CK from Alice to Bob through the ClC, making the FEC decoding complexity balanced between both sides. Lastly, only LDPC codes can be applied to both System A and System B, while any kinds of FEC codes can be applied to System C and D. We opted for powerful IRCCs to achieve near-capacity performance.

[10]As for handling decoding failures, it is assumed to be identical to that in the conventional LDPC-based reconciliation scheme of [66], which is based on the classic cyclic redundancy check. Specifically, the system opts for discarding the sifted keys, if decoding failure occurs. Yet, a slight difference is that our codeword-based reconciliation needs two separate steps to check whether decoding is successful or not. We can only proceed to the next step when both parts are correct.

IV. SECRET KEY RATE ANALYSIS

Note that the security level of the proposed System C and D is the same as that of System A and B, since the difference between them only lies in the side information. More specifically, we can only proceed with the reconciliation steps of Fig. 3, when the QK is securely received through the QuC, which obeys the Heisenberg's uncertainty principle. Therefore, even if Even steals the side information from the ClC, the final key still cannot be recovered. This is true for Systems A-D. Nonetheless, there are three distinct advantages for the proposed System D. Firstly, it is compatible with any FEC code, rather than being limited to LDPC codes. Secondly, it has a balanced complexity for Alice and Bob, which is particularly favourable in wireless device-to-device scenarios. Lastly, it exhibits near-capacity performance, where the SKR is close to the PLOB. This is achieved by using IRCCs for protecting both the QuC and ClC, making the SNRs required for error-free quantum and classical transmissions near-optimal.

The SKR is defined as [67]

$$K_f = \gamma(1 - P_B)\left[\beta I_{AB} - \chi_{BE} - \Delta\left(N_{\text{privacy}}\right)\right], \tag{7}$$

where γ denotes the proportion of the key extractions in the total number of data exchanged by Alice and Bob, while P_B represents the BLER in the reconciliation step. Furthermore, I_{AB} is the classical MI between Alice and Bob based on their shared correlated data, and χ_{BE} represents the Holevo information [61] that Eve can extract from the information of Bob. Finally, $\Delta(N_{\text{privacy}})$ represents the finite-size offset factor with the finite-size N_{privacy}.[11] It was proven in [99] that when $N_{\text{privacy}} > 10^4$, this factor can be simplified as

$$\Delta\big(N_{\text{privacy}}\big) \approx 7\sqrt{\frac{\log_2(2/\epsilon)}{N_{\text{privacy}}}}, \tag{8}$$

where ϵ represents the security parameter[12] for the protocol. As for $\beta \in [0, 1]$, it represents the reconciliation efficiency, which is defined as [61], [75]

$$\beta = \frac{R}{C} = \frac{R}{0.5\log_2(1+\text{SNR})}, \tag{9}$$

where R represents the transmission rate, and C is referred to as the one-dimensional Shannon capacity [93], [100], which is given by the MI as follows [67]:

$$C = I_{AB} = \frac{1}{2}\log_2(1+\text{SNR}) = \frac{1}{2}\log_2\left(\frac{V+\xi_{\text{total}}}{1+\xi_{\text{total}}}\right), \tag{10}$$

where $V_A = V_s + 1$ and V_s is Alice's modulation variance,[13] while ξ_{total} is the total amount of noise between Alice and Bob, which can be expressed as

$$\xi_{\text{total}} = \xi_{\text{line}} + \frac{\xi_{\text{hom}}}{T}, \tag{11}$$

where $\xi_{\text{hom}} = \frac{1+v_{el}}{\eta} - 1$ is the homodyne detector's noise, and v_{el} stands for the electric noise, while η represents the detection efficiency. Furthermore, $\xi_{\text{line}} = (\frac{1}{T} - 1) + \xi_{\text{ch}}$ represents the channel noise from the sender Alice, where T represents the path loss and ξ_{ch} is the excess noise [90] (i.e., imperfect modulation noise, Raman noise, phase-recovery noise, etc.). Assuming a single-mode fiber having an attenuation of $\alpha = 0.2$ dB/km, the distance-dependent path loss of such a channel is $T = 10^{-\alpha L/10}$, where L denotes the distance between the two parties.

The Holevo information between Bob and Eve can be calculated as follows [61]

$$\chi_{EB} = S(\rho_E) - S\big(\rho_{E|B}\big) = S(\rho_{AB}) - S\big(\rho_{A|B}\big), \tag{12}$$

where $S(\cdot)$ is the von Neumann entropy defined in [61]. The von Neumann entropy of a Gaussian state ρ containing M modes can be written in terms of its symplectic eigenvalues [101]

$$S(\rho) = \sum_{m=1}^{M} G(\upsilon_m), \tag{13}$$

where

$$G(\upsilon) = \left(\frac{\upsilon+1}{2}\right)\log_2\left(\frac{\upsilon+1}{2}\right) - \left(\frac{\upsilon-1}{2}\right)\log_2\left(\frac{\upsilon-1}{2}\right). \tag{14}$$

To elaborate on Eq. (14), generally these symplectic eigenvalues can be calculated based on the covariance matrix (CM) V of the Gaussian state using the formula [48]

$$\upsilon = |i\mathbf{\Omega}V|, \quad \upsilon \geq 1, \tag{15}$$

where $\mathbf{\Omega}$ defines the symplectic form given by

$$\mathbf{\Omega} \coloneqq \bigoplus_{m=1}^{M} \boldsymbol{\omega} = \begin{pmatrix} \boldsymbol{\omega} & & \\ & \ddots & \\ & & \boldsymbol{\omega} \end{pmatrix}, \boldsymbol{\omega} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{16}$$

Here $\bigoplus$ is the direct sum indicating the construction of a block-diagonal matrix $\mathbf{\Omega}$ having the same dimensionality as $\mathbf{V}$ by placing M blocks of $\boldsymbol{\omega}$ diagonally. Eq. (15) indicates that first we have to find the eigenvalue of the matrix $i\mathbf{\Omega}V$ and then take the absolute values. However, in some circumstances, we can simplify the calculation of the eigenvalues. To elaborate further, firstly we consider a generic two-mode CM in the form of

$$V = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}. \tag{17}$$

Based on [61], the symplectic eigenvalues υ_1 and υ_2 of V can be written in the form of [48]

$$\upsilon_{1,2} = \sqrt{\frac{1}{2}\Big(\Delta \pm \sqrt{\Delta^2 - 4\det V}\Big)}, \tag{18}$$

where $\det V$ represents the determinant of the matrix V and we have

$$\Delta \coloneqq \det\mathbf{A} + \det\mathbf{B} + 2\det\mathbf{C}. \tag{19}$$

In light of this, the CM related to the information between Alice and Bob, - namely the mode of ρ_{AB} after transmission through the QuC - can be expressed as

$$\begin{aligned}\mathbf{V}_{AB} &= \begin{pmatrix} V_A\mathbf{I}_2 & \sqrt{\eta T\big(V_A^2-1\big)}\mathbf{Z} \\ \sqrt{\eta T\big(V_A^2-1\big)}\mathbf{Z} & \eta T(V_A+\xi_{\text{total}})\mathbf{I}_2 \end{pmatrix} \\ &= \begin{pmatrix} a\mathbf{I}_2 & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I}_2 \end{pmatrix},\end{aligned} \tag{20}$$

where we have

$$\mathbf{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{21}$$

[11] Note that the finite-size offset can be viewed as a penalty term imposed by the imperfect parameter estimation step as shown in Fig. 3 when using finite length data. The value of N_{privacy} set in our analysis is 10^{12}, which is a value chosen in most of the literature.

[12] This security parameter corresponds to the failure probability of the whole protocol, implying that the protocol is assured to perform as requested except for a probability of at most ϵ. The value of ϵ is chosen to be 10^{-10} in our following analysis, which is widely used in the literature.

[13] The modulation variance here represents the variance of Gaussian signals used in the modulator of CV-QKD.

TABLE 4. Simulation parameters.

Parameter	Value
Coding rate (fixed)	0.5
Code length	1024
Decoding algorithm	BF/BP
Maximum number of iterations	50
Quantum equivalent channel type	BI-AWGN
ClC type	AWGN/Rayleigh
QuC quality	SNR
ClC quality	SNR^C

which are the two Pauli matrices. Therefore, the symplectic eigenvalues of ρ_{AB} required are given by

$$\upsilon_{1,2}^2 = \frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4D^2}\right), \tag{22}$$

where we have:

$$\begin{aligned} \Delta &= a^2 + b^2 - 2c^2, \\ D &= ab - c^2. \end{aligned} \tag{23}$$

As for the symplectic eigenvalue of $\rho_{A|B}$, it can be shown that:

$$\upsilon_3 = \sqrt{a\left(a - \frac{c^2}{b}\right)}. \tag{24}$$

Hence, the Holevo information can be formulated as

$$\chi_{BE} = G(\upsilon_1) + G(\upsilon_2) - G(\upsilon_3), \tag{25}$$

where υ_1, υ_2 and υ_3 are symplectic eigenvalues. Upon substituting Eq. (10) and Eq. (25) into Eq. (7), the corresponding SKR can be obtained.

In summary, SKR versus distance L performance metric, used in our following analysis are as follows.

- Once the BLER versus SNR performance is obtained, a fixed BLER corresponds to a fixed SNR.
- The noise term ξ_{total} in Eq. (10) is a function of L. Hence, the value of V_A is adjusted for each L to satisfy the fixed SNR based on Eq. (10).
- Once V_A is adjusted for each L, χ_{BE} can be obtained, since it is a function of V_A.
- Finally, the target SKR versus distance is derived.

V. PERFORMANCE ANALYSIS

In this section, our BLER performance comparisons will be presented for different reconciliation schemes. Moreover, the SKR versus distance performance indicator will be analyzed. The common simulation parameters,[14] which are used in our LDPC based reconciliation scheme are summarized in Table 4.

[14]Note that the code length and code rate used in both the QuC and ClC are the same.

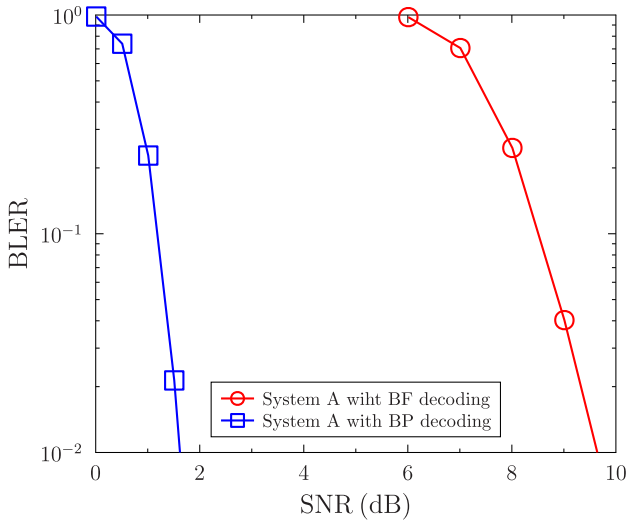


FIGURE 12. Performance comparison between System A of Fig. 8 and System B of Fig. 9. The code length and code rate of the LDPC code are 1024 and 0.5, respectively. BF decoding is used in System A and BP decoding is utilized in System B. The classical authenticated channel is assumed to be error-free.

A. PERFORMANCE COMPARISON BETWEEN BF AND BP DECODING IN SYSTEM A

Firstly, the performance comparison between the BF and BP decoding in System A is presented by Fig. 12, where the classical authenticated channel is assumed to be error-free. Observe from Fig. 12 that as expected, BP decoding outperforms BF decoding. Since the BLER performance is a key performance factor in the SKR of Eq. (7), the BP decoding algorithm will be adopted in the rest of performance analysis.

B. PERFORMANCE COMPARISON AMONG SYSTEM B, SYSTEM C AND SYSTEM D

Let us now compare System B of Fig. 9 and System C of Fig. 10 as well as System D of Fig. 11, given that the authenticated channel is no longer error-free. Instead, an AWGN channel and an uncorrelated Rayleigh fading channel as well as perfect channel estimation are assumed for the classical side-information in Fig. 13 and Fig. 14, respectively.

Fig. 13 demonstrates that the performance of the uncoded System B is severely degraded, when the ClC is contaminated by AWGN and hence it is no longer error-free, which confirms that error correction is required for both the ClC and QuC. By contrast, it can be seen in Fig. 13 that when System B, System C and System D employed FEC to protect their ClC, they no longer suffer from performance loss compared to the scenario of the idealistic assumption of having an error-free ClC. The ClC of $SNR^C = 3$dB is sufficient for supporting System B, System C and System D for approaching the performance of the error-free ClC, which is shown by the solid line associated with stars, representing the BP-based performance of System A.

Similarly, Fig. 14 provides our performance comparison, when the ClC is modelled by an uncorrelated Rayleigh fading

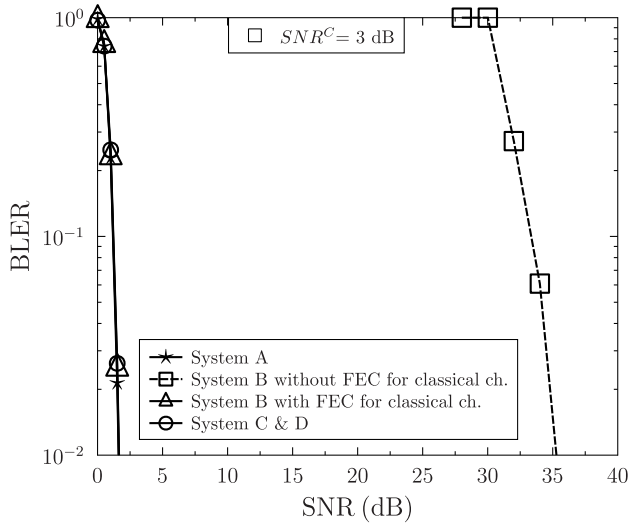


FIGURE 13. Performance comparison among System B, System C and System D. The code length and code rate of the LDPC code are 1024 and 0.5, respectively. BP decoding algorithm is used in System B, System C and System D, as well as System A. The authenticated ClC is assumed to be an AWGN channel and the corresponding SNR^C is 3 dB.

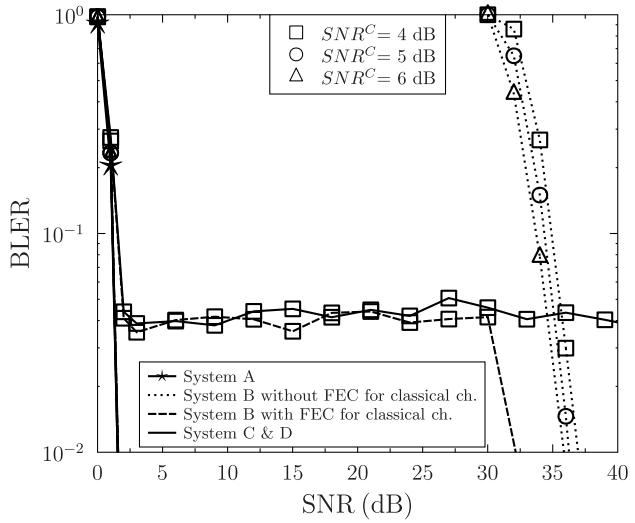


FIGURE 14. Performance comparison among System B, System C and System D. The code length and code rate of the LDPC code are 1024 and 0.5, respectively. BP decoding algorithm is used in System B, System C and System D, as well as System A. The authenticated ClC is assumed to be a Rayleigh fading channel.

channel having $SNR^C = 4, 5, 6$dB. It can be seen in Fig. 14 that System B operating without error protection for the ClC performs worst, requiring excessive SNR. By contrast, Fig. 14 shows that when FEC is applied to the ClC, at say $SNR^C = 5, 6$dB, System B, System C and System D approach the idealistic scenario of an error-free ClC. By contrast, an error floor is encountered by both System B, System C and System D at $SNR^C = 4$dB, which is too low to mitigate the errors imposed by the Rayleigh faded ClC.

Based on the BLER performances shown above, the corresponding SKR versus distance comparison is portrayed in Fig. 15. The parameters are as follows: the modulation

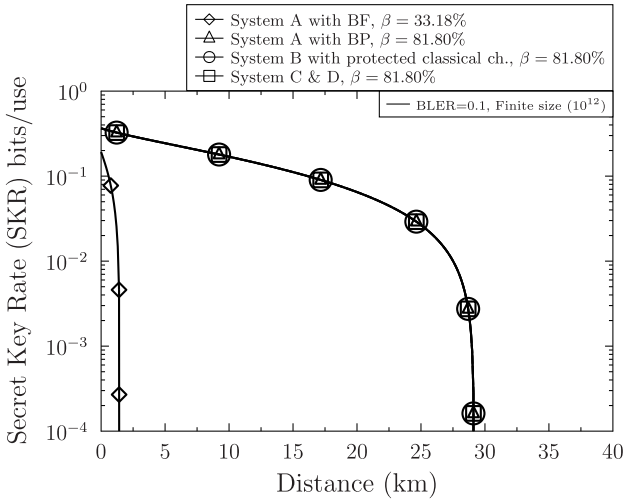


FIGURE 15. The secret key rate analysis versus distance. The values of different reconciliation efficiency are calculated based on the corresponding SNR at the threshold of BLER equals to 0.1.

variance is adjusted to get a certain target SNR, which is related to the BLER threshold of 0.1 utilized for comparison; the excess noise is $\xi_{\text{ch}} = 0.002$; the efficiency of the homodyne detector is $\eta = 0.98$; the attenuation of a single-mode optical fibre is $\alpha = 0.2$dB/km, and the electric noise is $v_{el} = 0.01$. More explicitly, Fig. 15 demonstrates that the maximum secure distance of System A using BF decoding is limited at around 1km, while that of System A using BP decoding is about 30 km. A similar performance as that of System A using BP decoding is attained for System B for a protected ClC at $SNR^C = 3$dB, which is a sufficiently high SNR^C. System C and System D also achieve a similar SKR performance, as evidenced by Fig. 15. Note that the SKR versus distance performance of System B without protecting the ClC is not shown here, because it is extremely low at such low reconciliation efficiency.

C. PERFORMANCE COMPARISON AMONG DIFFERENT FEC CODES IN SYSTEM D

In this section, comparisons have been made among three different types of FEC codes, which are LDPC codes, CC and IRCC, respectively. The number of LDPC decoding iteration is 50 and that of IRCC decoding is 30.

Fig. 16 and Fig. 17 characterize the performance of our codeword-based reconciliation scheme using a 1/2-rate CC of constraint-length 7 under AWGN and Rayleigh channels, respectively. The same trend can be observed in Fig. 16 and Fig. 17, where a higher SNR^C of the ClC leads to reduced error floor. We note that as expected, compared to the AWGN scenario of Fig. 16, the Rayleigh scenario of Fig. 17 requires a higher SNR^C for achieving a low BLER.

Let us now consider the most sophisticated FEC scheme of this study, namely the IRCC used, which was discussed in great detail in [102], [103] and shown in Fig. 18, where P_{out} and P_{in} represents the number of irregular coding components used. In Fig. 18(a), the extrinsic information transfer

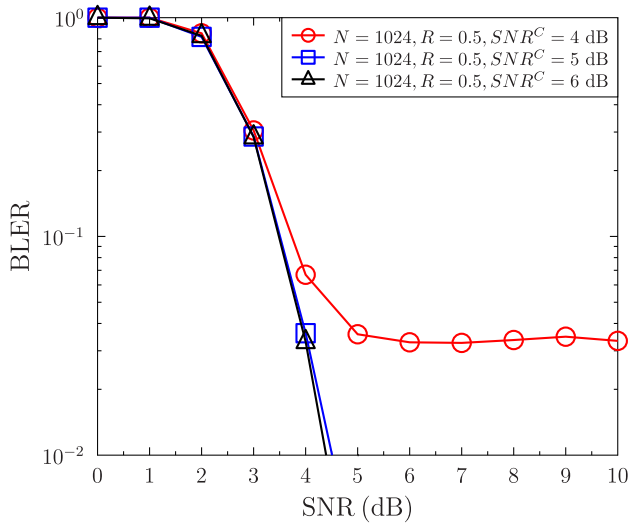


FIGURE 16. Performance comparison in System D with CC. The code length and code rate of the CC code are 1024 and 0.5, respectively. The authenticated CIC is assumed to be a AWGN channel.

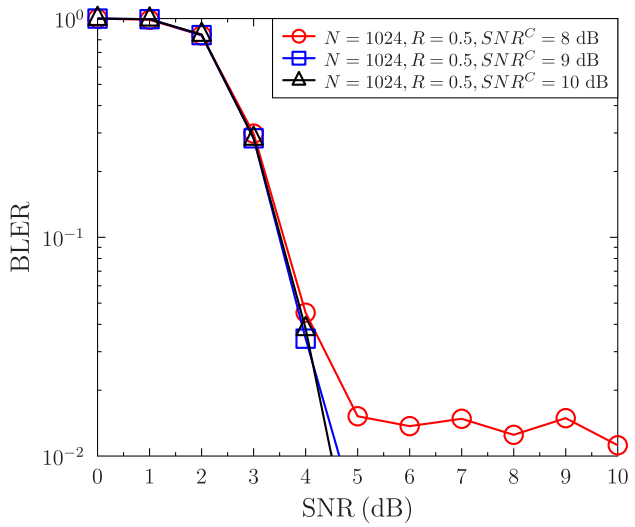
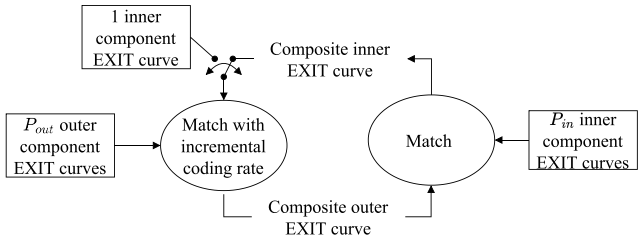
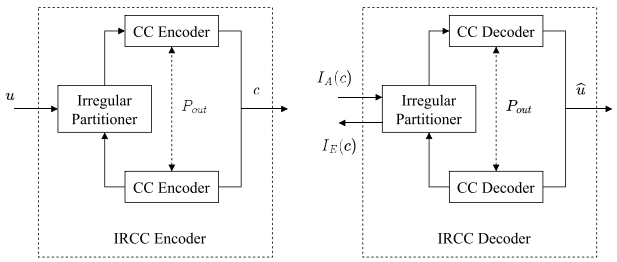


FIGURE 17. Performance comparison in System D with CC. The code length and code rate of the CC code are 1024 and 0.5, respectively. The authenticated CIC is assumed to be a Rayleigh fading channel.



(a) Diagram of interative double EXIT chart matching [102]



(b) Schematic of the IRCC encoding and decoding [103]

FIGURE 18. Schematic of IRCC codes.

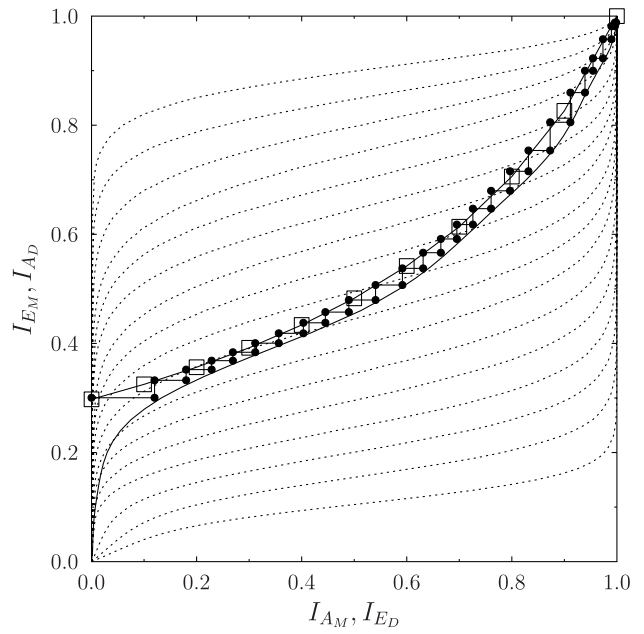


FIGURE 19. EXIT chart and a decoding trajectory of IRCC and URC coded BPSK having a block-length of 10^5, communicating over a classical AWGN channel.

(EXIT) chart matching process detailed in [104] is briefly illustrated, and the process of IRCC encoding and decoding is shown in Fig. 18(b). The EXIT charts [87], [105], [106] and the iterative decoding trajectory of IRCC and Unity Rate Code (URC) coded BPSK modulation communicating over classical AWGN channel are portrayed in Fig. 19. More explicitly, the dotted EXIT curves seen in Fig. 19 correspond to 17 component CCs having coding rates ranging from 0.1 to 0.9 with a step size of 0.05. The IRCC design assigns different-length segments to different-rate component codes, so that a narrow tunnel is formed between the inner URC-BPSK coding component's EXIT curve and that of the outer IRCC decoder, as seen in Fig. 19. It was shown in [104] that the open tunnel area is proportional to the distance from capacity. More explicitly, as this area tends to zero, the scheme tends to approach the capacity. Hence, the presence of the narrow but open decoding tunnel of Fig. 19 indicates decoding convergence at a low SNR that approaches the capacity limit. The IRCC fractions of the component codes are found to be [0.0120603 0 0 0 0 0 0.605992 0.0780007 0 0 0 0.0672488 0.177274 0 0 0 0.0594503] for the 17 subcodes used in Fig. 19. To elaborate briefly, for a 1000-bit IRCC the cod-rate of 0.05 is used for $0.0120603 \cdot 1000 \approx 12$ bits. Then the code-rates of 0.1, 0.15, 0.2, 0.25 and 0.3 have 0 weight,

TABLE 5. Reconciliation efficiency of different FEC codes calculated from Eq. (9) at the BLER threshold that equals to 0.1, together with the corresponding SNRs. The code length and code rate of them are the same for all of them, which are $N = 10^4$, $R = 0.5$. The authenticated ClCs are AWGN and uncorrelated Rayleigh channel.

	AWGN		Rayleigh	
Code type	SNR(dB)	$\beta(\%)$	SNR(dB)	$\beta(\%)$
CC	4.4	52.40	4.4	52.40
LDPC code	1.31	81.04	1.31	81.40
IRCC	0.9	86.41	1.0	85.06
IRCC (10^5)	0.7	89.21	0.7	89.21

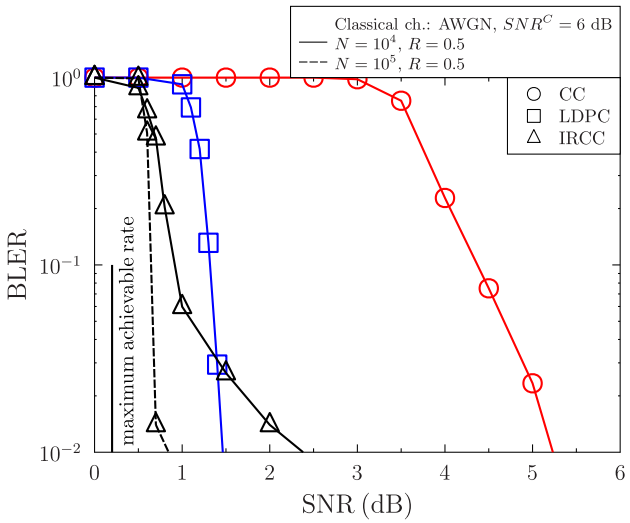


FIGURE 20. Performance comparison of different FEC codes in System D of Fig. 11. The code length and code rate of different codes are 10^4 and 0.5, respectively. The authenticated ClC is an AWGN channel.

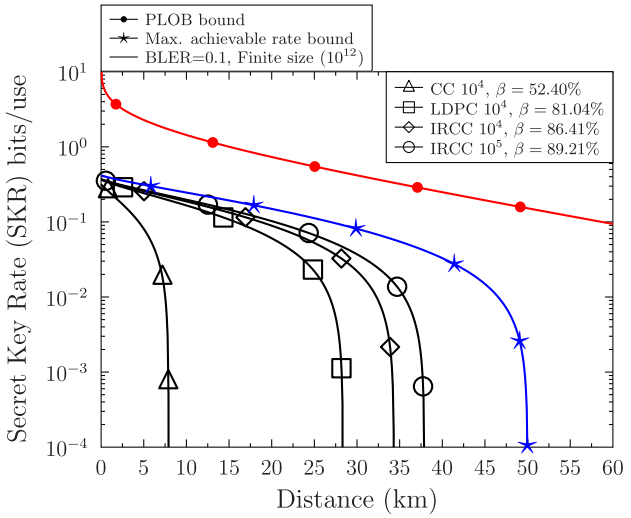


FIGURE 21. The secret key rate versus distance. The values of different reconciliation efficiencies are shown in Table 5 at the BLER threshold of 0.1. The other parameters are as follows: the modulation variance is adjusted to get a target SNR, the excess noise is $\xi_{ch} = 0.002$, the efficiency of the homodyne detector is $\eta = 0.98$, the attenuation of a single-mode optical fibre is $\alpha = 0.2$dB/km, and the electric noise is $v_{el} = 0.01$. The corresponding PLOB [86] bound and the maximum achievable rate bound are shown as well.

so they are unused. The code-rate of 0.35 has a weight of 0.605992, hence it is used for $0.605992 \cdot 1000 \approx 606$ bits and this process is applied to the remaining code-rates as well.

The BLER of the codeword based reconciliation scheme (System D) of a variety of FEC codes is shown in Fig. 20. The corresponding (BLER, β) pair can be obtained as tabulated in Table 5. In light of the BLER performance comparison among different FEC codes, the corresponding SKR versus distance performances of different FEC code based reconciliation schemes can be obtained with the aid of the reconciliation efficiencies as shown in Fig. 21. For the same BLER, for example BLER=0.1, given the same block length of 10^4 bits, the reconciliation performances associated with IRCC, LDPC and CC exhibit different reconciliation efficiencies, which are 86.41%, 81.04% and 52.40%, respectively. Therefore, the SKR performance of the IRCC scheme is the best. More explicitly, the maximum secure distance associated with the IRCC code (the diamond solid line) is longer than that of LDPC (the square solid line) and of the CC (the square dash line) code. Furthermore, the SKR at each specific secure distance associated with IRCC code is higher than that of the LDPC or CC codes. To elaborate further, the maximum secure distance of the IRCC code with BLER=0.1, $\beta = 86.41\%$ is around 35km, whereas the corresponding maximum secure distance of the LDPC (BLER=0.1, $\beta = 81.04\%$) and CC (BLER=0.1, $\beta = 52.40\%$) codes are around 28km and 8km, respectively. The same conclusion can be drawn for the comparison between LDPC and CC codes at BLER=0.01. Moreover, Fig. 21 demonstrates that the SKR performance of a longer block length of $N = 10^5$ is superior to that of $N = 10^4$, since a longer block length can offer near-capacity performance, hence leading to a longer secure transmission distance of around 37km. Note that the vertical line shown in Fig. 20 represents the minimum SNR required to achieve near-error-free transmission. It is obtained based on [87], [106], [107]

$$C^{DCMC}(SNR) = 1 - \frac{1}{2}\sum_{i=0}^{1}\mathbb{E}\left\{\log_2\left[\sum_{\bar{i}=0}^{1}\exp\left(\Psi_{i,\bar{i}}\right)\right]\right\}, \quad (26)$$

where we have $\Psi_{i,\bar{i}} = \frac{-\|s^i - s^{\bar{i}} + n\|^2 + \|n\|^2}{N_0}$, s^i represents the BPSK symbols, while n is the noise, whose distribution obeys $n \sim \mathcal{CN}(0, N_0)$. The corresponding SNR can be obtained by solving $C^{DCMC}(SNR) = 0.5$, since we consider BPSK and $R = 0.5$, FEC codes. The same capacity line is also drawn in Fig. 22.

On the other hand, based on the reconciliation efficiencies seen in Table 5 and inferred from Fig. 20 as well as Fig. 22, the reconciliation efficiencies are similar for the Rayleigh-faded and for the AWGN ClC. This is because the reconciliation efficiencies are mainly determined by the QuC quality characterized by the equivalent channel SNR, provided that the ClC quality is high enough for ensuring that the errors from the classical transmission do not unduly erode the overall system performance, as demonstrated in Fig. 22. Intuitively, a higher SNR^C is required in Rayleigh faded ClCs compared to the SNR^C in an AWGN based ClC

to achieve nearly the same system performance. Therefore, given that the βs are nearly the same, the SKR of a Rayleigh faded ClC is similar to that in Fig. 21.

VI. CONCLUSION

The codeword based reconciliation concept was proposed as a general reconciliation scheme that can be applied in conjunction with diverse FEC codes. This is a significant improvement because the popular syndrome-based LDPC-coded reconciliation scheme can only be applied for FEC codes that possess syndromes. Furthermore, in contrast to the general assumption that the classical authenticated channel is error-free and noiseless, a realistic ClC has been considered, which may contain errors. We investigated the performance of our QKD systems when the classical authenticated channel is modelled as an AWGN channel or a Rayleigh channel. We demonstrated that when the ClC quality is sufficiently high, the QKD system will have a relatively low BLER. An error floor is exhibited by the system, when the ClC has errors due to employing a weak channel code or when the ClC quality is too low. More specifically, we have investigated LDPC codes, CC and IRCCs assisted CV-QKD schemes. It was demonstrated that the IRCC associated system performs the best among them, followed by the LDPC codes, whilst the CC code performs the worst. In light of this, the SKR versus distance performance of different FEC codes using optical fibre as the QuC has been compared. It was demonstrated that near-capacity FEC codes such as IRCC can provide higher reconciliation efficiency, hence they can offer a longer secure transmission distance.

APPENDIX
MAPPING FUNCTION OF MULTIDIMENSIONAL RECONCILIATION

Mapping function calculation: Bob calculates the mapping function $\mathbf{M}_i(\mathbf{y}_i', \mathbf{u}_i)$ for each 8-element vector, which meets $\mathbf{M}_i(\mathbf{y}_i', \mathbf{u}_i)\mathbf{y}_i' = \mathbf{u}_i$, using the following formula:

$$\mathbf{M}_i(\mathbf{y}_i', \mathbf{u}_i) = \sum_{d=1}^{8} \alpha_i^d \mathbf{A}_8^d, \tag{27}$$

$$\mathbf{A}_8^1 = \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1 \end{bmatrix}, \quad \mathbf{A}_8^2 = \begin{bmatrix} 0&-1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&-1&0&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&-1&0&0&-1\\ 0&0&0&0&0&0&1&0 \end{bmatrix},$$

$$\mathbf{A}_8^3 = \begin{bmatrix} 0&0&-1&0&0&0&0&0\\ 0&0&0&-1&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&-1&0&0&0\\ 0&0&0&0&0&-1&0&0 \end{bmatrix}, \quad \mathbf{A}_8^4 = \begin{bmatrix} 0&0&0&-1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&-1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&-1&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&-1&0&0&0 \end{bmatrix},$$

$$\mathbf{A}_8^5 = \begin{bmatrix} 0&0&0&0&-1&0&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&0&0&0&0&-1&0\\ 0&0&0&0&0&0&0&-1\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0 \end{bmatrix}, \quad \mathbf{A}_8^6 = \begin{bmatrix} 0&0&0&0&0&-1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&-1\\ 0&0&0&0&0&0&1&0\\ 0&-1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&-1&0&0&0&0\\ 0&0&1&0&0&0&0&0 \end{bmatrix},$$

$$\mathbf{A}_8^7 = \begin{bmatrix} 0&0&0&0&0&0&-1&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&-1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&-1&0&0&0&0&0&0 \end{bmatrix}, \quad \mathbf{A}_8^8 = \begin{bmatrix} 0&0&0&0&0&0&0&-1\\ 0&0&0&0&0&0&-1&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&-1&0&0&0&0\\ 0&0&-1&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0 \end{bmatrix} \tag{28}$$

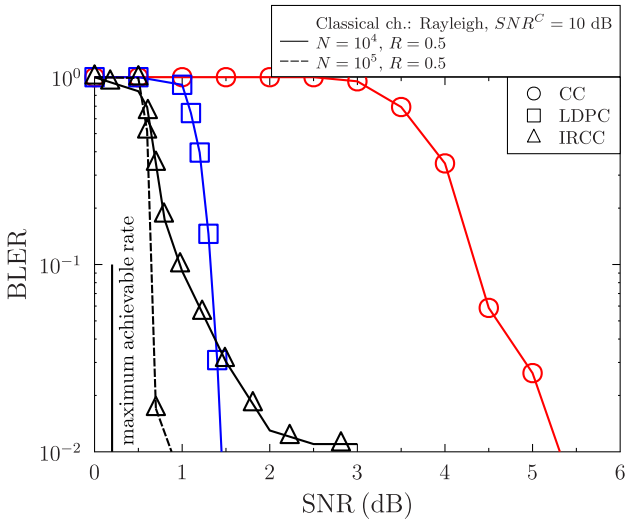


FIGURE 22. Performance comparison of different FEC codes in System D of Fig. 11. The code length and code rate of different codes are 10^4 and 0.5, respectively. The authenticated CIC is a Rayleigh channel.

where α_i^d is the d-th element of $\boldsymbol{\alpha}_i(\mathbf{y}_i', \mathbf{u}_i) = (\alpha_i^1, \alpha_i^2, \ldots, \alpha_i^8)^T$, which is the coordinate of the vector $\mathbf{u}_i$ under the orthonormal basis $(\mathbf{A}_8^1\mathbf{y}_i', \mathbf{A}_8^2\mathbf{y}_i', \ldots, \mathbf{A}_8^8\mathbf{y}_i')$ and it can be expressed as $\boldsymbol{\alpha}_i(\mathbf{y}_i', \mathbf{u}_i) = (\mathbf{A}_8^1\mathbf{y}_i', \mathbf{A}_8^2\mathbf{y}_i', \ldots, \mathbf{A}_8^8\mathbf{y}_i')^T\mathbf{u}_i$. Note that $\mathbf{A}_8^d$, $d = 1, 2, \ldots, 8$ is the orthogonal matrix of size 8×8 provided in [78, Appendix]. Note that the 8 orthogonal matrices used in our scheme are listed in Eq. (28), as shown at the bottom of the previous page.

REFERENCES

[1] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, and L. Gyongyosi, "Wireless myths, realities, and futures: From 3G/4G to optical and quantum wireless," *Proc. IEEE*, vol. 100, pp. 1853–1888, May 2012.

[2] P. Botsinis et al., "Quantum search algorithms for wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1209–1242, 2nd Quart., 2019.

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

[4] D. Maslov, Y. Nam, and J. Kim, "An outlook for quantum computing [point of view]," *Proc. IEEE*, vol. 107, no. 1, pp. 5–10, Jan. 2019.

[5] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security, and intelligence," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 126–132, Oct. 2020.

[6] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021.

[7] D. Coppersmith, "The data encryption standard (DES) and its strength against attacks," *IBM J. Res. Develop.*, vol. 38, no. 3, pp. 243–250, 1994.

[8] J. Nechvatal et al., "Report on the development of the advanced encryption standard (AES)," *J. Res. Nat. Inst. Stand. Technol.*, vol. 106, no. 3, p. 511, 2001.

[9] 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.

[10] M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[11] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. Conf. Theory Appl. Cryptograph. Techn.*, 1985, pp. 417–426.

[12] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[13] H. Mani, "Error reconciliation protocols for continuous-variable quantum key distribution," Ph. D. dissertation, Dept. Comput. Sci., Tech. Univ. Denmark, Kongens Lyngby, Denmark, 2021.

[14] R. A. Mollin, *An Introduction to Cryptography*. Hoboken, NJ, USA: CRC Press, 2000.

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

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

[17] 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.

[18] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 281–291, 2020.

[19] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 881–919, 1st Quart., 2019.

[20] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the Qinternet," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 839–894, 2nd Quart., 2022.

[21] Z. Wang, R. Malaney, and J. Green, "Inter-satellite quantum key distribution at Terahertz frequencies," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2019, pp. 1–7.

[22] S. P. Kish, E. Villaseñor, R. Malaney, K. A. Mudge, and K. J. Grant, "Feasibility assessment for practical continuous variable quantum key distribution over the satellite-to-earth channel," *Quant. Eng.*, vol. 2, no. 3, p. e50, 2020.

[23] X. You et al., "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Sci. China Inf. Sci.*, vol. 64, no. 1, pp. 1–74, 2021.

[24] M. Fujiwara, R. Nojima, T. Tsurumaru, S. Moriai, M. Takeoka, and M. Sasaki, "Long-term secure distributed storage using quantum key distribution network with third-party verification," *IEEE Trans. Quant. Eng.*, vol. 3, pp. 1–11, 2022.

[25] A. Stanco et al., "Versatile and concurrent FPGA-based architecture for practical quantum communication systems," *IEEE Trans. Quant. Eng.*, vol. 3, pp. 1–8, 2022.

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

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

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

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

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

[31] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Phys. Rev. Lett.*, vol. 81, no. 14, pp. 3018–3021, 1998.

[32] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, 2002, Art. no. 57902.

[33] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, 2003, Art. no. 57901.

[34] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, no. 5, 2004, Art. no. 057901.

[35] A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation," *Phys. Rev. Lett.*, vol. 102, May 2009, Art. no. 180504.

[36] 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.

[37] 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.

[38] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," *Phys. Rev. X*, vol. 8, Aug. 2018, Art. no. 31043.

[39] S. Pirandola et al., "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020.

[40] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.*, vol. 92, no. 2, 2020, Art. no. 25002.

[41] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photon.*, vol. 8, no. 8, pp. 595–604, 2014.

[42] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: principle, security and implementations," *Entropy*, vol. 17, no. 9, pp. 6072–6092, 2015.

[43] H. Ge, A. Tomita, A. Okamoto, and K. Ogawa, "Analysis of the effects of the two-photon temporal distinguishability on measurement-device-independent quantum key distribution," *IEEE Trans. Quant. Eng.*, vol. 4, pp. 1–8, 2023.

[44] C. Weedbrook et al., "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, no. 2, pp. 621–669, 2012.

[45] C. Ottaviani et al., "Terahertz quantum cryptography," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 483–495, Mar. 2020.

[46] Y. He, Y. Mao, D. Huang, Q. Liao, and Y. Guo, "Indoor channel modeling for continuous variable quantum key distribution in the Terahertz band," *Opt. Exp.*, vol. 28, no. 22, pp. 32386–32402, 2020.

[47] X. Liu, C. Zhu, N. Chen, and C. Pei, "Practical aspects of terahertz wireless quantum key distribution in indoor environments," *Quant. Inf. Process.*, vol. 17, no. 11, pp. 1–20, 2018.

[48] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, "Quantum cryptography approaching the classical limit," *Phys. Rev. Lett.*, vol. 105, no. 11, pp. 1–8, 2010.

[49] M. Gabay and S. Arnon, "Quantum key distribution by a free-space MIMO system," *J. Lightw. Technol.*, vol. 24, no. 8, pp. 3114–3120, Aug. 8, 2006.

[50] N. K. Kundu, S. P. Dash, M. R. McKay, and R. K. Mallik, "MIMO terahertz quantum key distribution," *IEEE Commun. Lett.*, vol. 25, no. 10, pp. 3345–3349, Oct. 2021.

[51] N. K. Kundu, S. P. Dash, M. R. Mckay, and R. K. Mallik, "Channel estimation and secret key rate analysis of MIMO Terahertz quantum key distribution," *IEEE Trans. Commun.*, vol. 70, no. 5, pp. 3350–3363, May 2022.

[52] N. K. Kundu, M. R. McKay, A. Conti, R. K. Mallik, and M. Z. Win, "MIMO terahertz quantum key distribution under restricted eavesdropping," *IEEE Trans. Quant. Eng.*, vol. 4, pp. 1–15, 2023.

[53] M. Zhang, S. Pirandola, and K. Delfanazari, "Millimeter-waves to Terahertz SISO and MIMO continuous variable quantum key distribution," *IEEE Trans. Quant. Eng.*, vol. 4, pp. 1–10, 2023.

[54] W. Zhao, Q. Liao, D. Huang, and Y. Guo, "Performance analysis of the satellite-to-ground continuous-variable quantum key distribution with orthogonal frequency division multiplexed modulation," *Quant. Inf. Process.*, vol. 18, no. 1, pp. 1–22, 2019.

[55] S. Zhao, Z. Shen, H. Xiao, and L. Wang, "Multidimensional reconciliation protocol for continuous-variable quantum key agreement with polar coding," *Sci. China Phys. Mech. Astronomy*, vol. 61, pp. 1–4, May 2018.

[56] H. Zhang, Y. Mao, D. Huang, J. Li, L. Zhang, and Y. Guo, "Security analysis of orthogonal-frequency-division-multiplexing-based continuous-variable quantum key distribution with imperfect modulation," *Phys. Rev. A, Atomic Mol., Opt. Phys.*, vol. 97, no. 5, pp. 1–9, 2018.

[57] Y.-J. Lin and M. Jarrahi, "Heterodyne Terahertz detection through electronic and optoelectronic mixers," *Rep. Progr. Phys.*, vol. 83, no. 6, 2020, Art. no. 66101.

[58] K. Ikamas, D. B. But, and A. Lisauskas, "Homodyne spectroscopy with broadband terahertz power detector based on 90-nm silicon CMOS transistor," *Appl. Sci.*, vol. 11, no. 1, p. 412, 2021.

[59] R. Cattaneo, E. A. Borodianskyi, A. A. Kalenyuk, and V. M. Krasnov, "Superconducting terahertz sources with % power efficiency," *Phys. Rev. A, Atomic Mol., Opt. Phys.ppl.*, vol. 16, no. 6, 2021, Art. no. 61001.

[60] J. R. Rain et al., "Wave functions for high-symmetry, thin microstrip antennas, and two-dimensional quantum boxes," *Phys. Rev. A, Atomic Mol., Opt. Phys.*, vol. 104, no. 6, 2021, Art. no. 62205.

[61] F. Laudenbach et al., "Continuous-variable quantum key distribution with Gaussian modulation—The theory of practical implementations," *Adv. Quant. Technol.*, vol. 1, no. 1, pp. 1–37, 2018.

[62] S.-K. Liao et al., "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[63] K. Zhang, X.-Q. Jiang, Y. Feng, R. Qiu, and E. Bai, "High efficiency continuous-variable quantum key distribution based on quasi-cyclic LDPC codes," in *Proc. 5th IEEE Int. Conf. Commun. Image Signal Process. (CCISP)*, 2020, pp. 38–42.

[64] Y. Guo, X. Wang, C. Xie, and D. Huang, "Free-space continuous-variable quantum key distribution in atmospheric channels based on low-density parity-check codes," *Laser Phys. Lett.*, vol. 17, no. 4, 2020, Art. no. 45203.

[65] M. Shirvanimoghaddam, S. J. Johnson, and A. M. Lance, "Design of raptor codes in the low SNR regime with applications in quantum key distribution," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2016, pp. 1–6.

[66] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Key reconciliation with low-density parity-check codes for long-distance quantum cryptography," 2017, *arXiv:1702.07740*.

[67] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography," *NPJ Quant. Inf.*, vol. 4, no. 1, p. 21, 2018.

[68] K. Gümüş et al., "A novel error correction protocol for continuous variable quantum key distribution," *Sci. Rep.*, vol. 11, no. 1, 2021, Art. no. 10465.

[69] X. Wen, Q. Li, H. Mao, X. Wen, and N. Chen, "Rotation based slice error correction protocol for continuous-variable quantum key distribution and its implementation with polar codes," 2021, *arXiv:2106.06206*.

[70] B.-Y. Tang, C.-Q. Wu, W. Peng, B. Liu, and W.-R. Yu, "Polar-code-based information reconciliation scheme with the frozen-bit erasure strategy for quantum key distribution," *Phys. Rev. A, Atomic Mol., Opt. Phys.*, vol. 107, no. 1, 2023, Art. no. 12612.

[71] 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. IEEE Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, 2017, pp. 301–306.

[72] C. Zhou, X. Wang, Y. Zhang, Z. Zhang, S. Yu, and H. Guo, "Continuous-variable quantum key distribution with rateless reconciliation protocol," *Phys. Rev. A, Atomic Mol., Opt. Phys.ppl.*, vol. 12, no. 5, 2019, Art. no. 54013.

[73] M. B. Asfaw, X. Q. Jiang, M. Zhang, J. Hou, and W. Duan, "Performance analysis of raptor code for reconciliation in continuous variable quantum key distribution," in *Proc. IEEE Int. Conf. Comput. Netw. Commun. (ICNC)*, 2019, pp. 463–467.

[74] M. Zhang, H. Hai, Y. Feng, and X.-Q. Jiang, "Rate-adaptive reconciliation with polar coding for continuous-variable quantum key distribution," *Quant. Inf. Process.*, vol. 20, no. 10, pp. 1–17, 2021.

[75] C. Zhou, X. Y. Wang, Z. G. Zhang, S. Yu, Z. Y. Chen, and H. Guo, "Rate compatible reconciliation for continuous-variable quantum key distribution using Raptor-like LDPC codes," *Sci. China Phys. Mech. Astronomy*, vol. 64, no. 6, 2021, Art. no. 260311.

[76] 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," *Quant. Inf. Process.*, vol. 20, no. 10, pp. 1–16, 2021.

[77] X. Ai and R. Malaney, "Optimised multithreaded CV-QKD reconciliation for global quantum networks," *IEEE Trans. Commun.*, vol. 70, no. 9, pp. 6122–6132, Sep. 2022.

[78] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Phys. Rev. A, Atomic Mol., Opt. Phys.*, vol. 77, no. 4, 2008, Art. no. 42325.

[79] 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. A, Atomic Mol., Opt. Phys.ppl.*, vol. 19, Apr. 2023, Art. no. 44023.
[80] J. Lodewyck et al., "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Phys. Rev. A, Atomic Mol., Opt. Phys.*, vol. 76, no. 4, 2007, Art. no. 42305.
[81] M. Bloch, A. Thangaraj, and S. W. McLaughlin, "Efficient reconciliation of correlated continuous random variables using LDPC codes," 2005, *arXiv:cs/0509041*.
[82] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," *Phys. Rev. A, Atomic Mol., Opt. Phys.*, vol. 84, no. 6, 2011, Art. no. 62317.
[83] H. Mani, T. Gehring, P. Grabenweger, B. Ömer, C. Pacher, and U. L. Andersen, "Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution," *Phys. Rev. A, Atomic Mol., Opt. Phys.*, vol. 103, Jun. 2021, Art. no. 62419.
[84] C. Xu et al., "Near-perfect finite-cardinality generalized space-time shift keying," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 9, pp. 2146–2164, Sep. 2019.
[85] C. Xu et al., "Sixty years of coherent versus non-coherent tradeoffs and the road from 5G to wireless futures," *IEEE Access*, vol. 7, pp. 178246–178299, 2019.
[86] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nat. Commun.*, vol. 8, no. 1, 2017, Art. no. 15043.
[87] L. Hanzo, O. Alamri, M. El-Hajjar, and N. Wu, *Near-Capacity Multi-Functional MIMO Systems: Sphere-Packing, Iterative Detection and Cooperation*. Hoboken, NJ, USA: Wiley, 2009.
[88] X. Ai, R. Malaney, and S. X. Ng, "Quantum key reconciliation for satellite-based communications," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2018, pp. 1–6.
[89] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables," 2003, *arXiv:quant-ph/0306141*.
[90] C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-variable quantum key distribution using thermal states," *Phys. Rev. A, Atomic Mol., Opt. Phys., Atomic Mol., Opt. Phys.*, vol. 86, no. 2, pp. 1–12, 2012.
[91] R. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 5, pp. 533–547, Sep. 1981.
[92] M. Luby, M. Mitzenmacher, M. Shokrollahi, and D. Spielman, "Improved low-density parity-check codes using irregular graphs," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 585–598, Feb. 2001.
[93] W. Ryan and S. Lin, *Channel Codes: Classical and Modern*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
[94] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inf. Theory*, vol. 47, pp. 498–519, Feb. 2001.
[95] V. K. Ralegankar et al., "Quantum cryptography-as-a-service for secure UAV communication: Applications, challenges, and case study," *IEEE Access*, vol. 10, pp. 1475–1492, 2022.
[96] N. Alshaer, A. Moawad, and T. Ismail, "Reliability and security analysis of an entanglement-based QKD protocol in a dynamic Ground-to-UAV FSO communications system," *IEEE Access*, vol. 9, pp. 168052–168067, 2021.
[97] M. Wang, Z. Yan, and V. Niemi, "UAKA-D2D: Universal authentication and key agreement protocol in D2D communications," *Mobile Netw. Appl.*, vol. 22, pp. 510–525, May 2017.
[98] M. Wang and Z. Yan, "Security in D2D communications: A review," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015, pp. 1199–1204.
[99] A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," *Phys. Rev. A, Atomic Mol., Opt. Phys., Atomic Mol., Opt. Phys.*, vol. 81, no. 6, 2010, Art. no. 62343.
[100] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2008.
[101] A. S. Holevo, M. Sohma, and O. Hirota, "Capacity of quantum Gaussian channels," *Phys. Rev. A, Atomic Mol., Opt. Phys., Atomic Mol., Opt. Phys.*, vol. 59, no. 3, pp. 1820–1828, 1999.
[102] R. G. Maunder and L. Hanzo, "Near-capacity irregular variable length coding and irregular unity rate coding," *IEEE Trans. Wireless Commun.*, vol. 8, no. 11, pp. 5500–5507, Nov. 2009.
[103] N. Wu and L. Hanzo, "Near-capacity irregular-convolutional-coding-aided irregular precoded linear dispersion codes," *IEEE Trans. Veh. Technol.*, vol. 58, no. 6, pp. 2863–2871, Jul. 2009.
[104] M. El-Hajjar and L. Hanzo, "EXIT charts for system design and analysis," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 127–153, 1st Quart., 2013.
[105] S. ten Brink, "Convergence behavior of iteratively decoded parallel concatenated codes," *IEEE Trans. Commun.*, vol. 49, no. 10, pp. 1727–1737, Apr. 2001.
[106] C. Xu, S. Sugiura, S. X. Ng, P. Zhang, L. Wang, and L. Hanzo, "Two decades of MIMO design tradeoffs and reduced-complexity MIMO detection in near-capacity systems," *IEEE Access*, vol. 5, pp. 18564–18632, 2017.
[107] S. X. Ng and L. Hanzo, "On the MIMO channel capacity of multidimensional signal sets," *IEEE Trans. Veh. Technol.*, vol. 55, no. 2, pp. 528–536, Mar. 2006.