IEEE Open Journal of Vehicular Technology

Received 9 December 2025; accepted 30 December 2025. Date of publication 5 January 2026;
date of current version 27 January 2026. The review of this article was coordinated by Editor Prakash Chaki.

Digital Object Identifier 10.1109/OJVT.2025.3650700

Rate-Compatible Polar- and LDPC-Coded Hybrid ARQ Aided Reverse Reconciliation in CV-QKD

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

The School of Electronics and Computer Science University of Southampton SO17 1B Southampton U.K.

CORRESPONDING AUTHOR: LAJOS HANZO (e-mail: lh@soton.ac.uk).

This work was supported in part by Engineering and Physical Sciences Research Council (EPSRC), in part by Platform for Driving Ultimate Connectivity (TITAN) under Grant EP/Y037243/1 and Grant EP/X04047X/1, in part by Robust and Reliable Quantum Computing (RoaRQ) under Grant EP/W032635/1, and in part by India-U.K. Intelligent Spectrum Innovation ICON UKRI-1859, PerCom, under Grant EP/X012301/1, Grant EP/X01228X/1, and Grant EP/Y037243/1.

ABSTRACT Continuous-variable quantum key distribution (CV-QKD) systems face challenges in maintaining efficient reconciliation over long distances due to the time variant signal-to-noise ratio (SNR) imposed by channel quality fluctuations. Hence fixed-rate error-correction schemes using low-density parity-check (LDPC) or Polar codes lead to high block-error rates (BLER) and degraded secret key rates (SKR). To overcome this, we propose an incremental redundancy aided hybrid automatic repeat request (IR-HARQ) protocol using rate-compatible Polar and LDPC codes. Explicitly, by puncturing a mother code and progressively transmitting additional redundant bits, our method dynamically adapts the effective coding rate to the prevalent channel conditions, achieving 2–3 dB SNR gains per retransmission. This adaptive strategy avoids unnecessary redundancy in good channels and strengthens protection in poor channels, thereby improving reconciliation efficiency. Simulation results show that our IR-HARQ scheme significantly enhances the BLER, throughput, and secure transmission distance compared with single-transmission schemes. Moreover, our study highlights that Polar IR-HARQ achieves superior performance in short block-length and low-SNR scenarios, while LDPC IR-HARQ is more competitive for longer codes and higher SNR. These findings confirm IR-HARQ as an attractive and versatile reconciliation solution for real-world CV-QKD deployments.

INDEX TERMS Automatic repeat request (ARQ), continuous variable quantum key distribution (CV-QKD), Polar code, secret key rate.

I. INTRODUCTION

In continuous-variable quantum key distribution (CV-QKD), reliable and efficient information reconciliation is critical for achieving high secret key rates, especially over long distances characterized by inherently low signal-to-noise ratios (SNR). Early reconciliation schemes, such as the Cascade algorithm [1] introduced by Brassard and Salvail in 1993, and WINNOW [2] introduced in 2003, used interactive parity checks and Hamming codes, respectively, to correct errors. Although effective, these methods require multiple rounds of classical communication, which increase latency and elevate the risk of information leakage due to extensive interactivity.

To mitigate these shortcomings, later developments focused on forward error correction (FEC) schemes utilizing low-density parity-check (LDPC) codes [3], [4], [5]. These LDPC-based approaches significantly enhanced reconciliation efficiency by reducing the number of required communication rounds, but introduced challenges in designing optimal parity-check matrices, especially for short block lengths. More recently, polar codes have emerged as promising alternatives due to their deterministic construction and superior short-block performance compared to LDPC codes. Jouguet et al. [6], Nakassis et al. [7], and Yan [8] demonstrated the potential of polar codes in CV-QKD,

highlighting their improved secret key rates (SKR) using successive-cancellation list (SCL) decoding.

Despite these advances, traditional reconciliation methods based on fixed-rate LDPC and polar codes struggle to cope with dynamically time-varying quantum channel conditions. This inflexibility leads to increased block-error rates (BLER), degraded secret key performance, and reduced adaptability in practical deployment scenarios subjected to channel fluctuations. Furthermore, existing fixed-rate approaches offer limited flexibility in balancing the trade-offs among throughput, latency, and secure transmission distance.

To address the need for dynamic rate adaptation, classical communication systems commonly employ Hybrid Automatic Repeat Request (HARQ) and its incremental redundancy variant (IR-HARQ), which provide robust adaptive mechanisms for error correction [9], [10], [11], [12], [13]. HARQ methods incrementally transmit additional redundancy based on real-time decoding feedback, enabling adaptation without precise channel state estimation [14]. Rate-compatible (RC) codes complement HARQ by offering a single encoder/decoder pair that flexibly adjusts its effective coding rate, significantly reducing implementation complexity.

Gümüş et al. [15] recently introduced a protocol referred to as Multiple Decoding Attempts (MDA), which can be regarded as a CV-QKD implementation of the blind-reconciliation paradigm originally developed for DV-QKD [16]. In MDA, Bob performs iterative LDPC decoding and, upon failure, progressively discloses portions of his information bits to Alice, thereby gradually reducing the effective code rate and enhancing the decoding success probability without explicit SNR estimation. Although this adaptive redundancy-based strategy improves reliability, it increases the classical information leakage that must be subtracted from the secret-key rate (SKR).

By contrast, the proposed IR-HARQ framework introduces incremental redundancy in the *quantum domain* rather than through classical bit disclosure. Specifically, the proposed IR-HARQ transmits additional Gaussian-modulated variables on demand to regenerate finite-valued log-likelihood ratios (LLRs) at the receiver with the aid of the multidimensional reconciliation algorithm [5], [17], enabling iterative soft-information refinement without revealing information bits. Blind reconciliation (including MDA) instead adjusts reliability by revealing bit values (forcing LLRs to $\pm\infty$), while rate-adaptive schemes rely on *a priori* SNR estimation for single-shot rate selection. In contrast to these approaches, IR-HARQ incorporates structured quantum retransmissions with the aid of modest classical signaling (ACK/NACK and frozen-bit indices), preserves secrecy, and achieves SKR-aware rate adaptation through feedback-driven redundancy scheduling.

Overall, while all three protocols share the objective of adaptive-rate reconciliation, they differ fundamentally in terms of both their operation domain and security level: MDA and rate-adaptive methods operate purely in the classical domain, whereas IR-HARQ extends the incremental redundancy concept into the quantum layer, enabling continuous soft-information refinement under information-theoretic security constraints.

Motivated by these advantages, we propose a novel IR-HARQ-based reverse reconciliation (RR) protocol tailored for CV-QKD systems using rate-compatible polar and LDPC codes. For polar codes, our scheme leverages a single mother code with block length $N = 512$ and nominal code rate $R = 0.5$, initially punctured to an effective rate of $R = 0.70$ (transmitting 366 bits). In response to decoding failures, our protocol incrementally retransmits the most reliable frozen bits, as determined by Gaussian-approximation reliability metrics, sequentially lowering the effective code rate to $R = 0.63$ (427 bits) and ultimately to $R = 0.52$ (512 bits). For LDPC codes, we adopt a parity-bit puncturing strategy, where only a subset of parity bits is transmitted initially, in addition to the information bits. At the decoder, the punctured bits are initialized as 0/1 with equal probability to facilitate decoding. Successive transmissions then replenish the punctured parity bits until the mother code is fully restored, ensuring that both 0.5-rate coding families can be compared under the same IR-HARQ framework in a fair fashion.

The primary contributions of this work are listed at Table I and summarized as follows:

- We propose the **first quantum-domain incremental redundancy (IR-HARQ) based reconciliation framework** for continuous-variable quantum key distribution (CV-QKD). In contrast to classical IR-HARQ – which transmits extra parity bits – our technique performs **incremental quantum-variable disclosure** that refines soft information for improved decoding. Each newly transmitted Gaussian variable is mapped, via multidimensional reconciliation, into additional LLR evidence, which Alice beneficially fuses with the previously received information through soft-combining. This establishes a direct bridge between quantum-domain redundancy and classical-domain decoding reliability, achieving SKR-driven adaptivity while maintaining information-theoretic security.
- The proposed protocol employs **rate-compatible polar and LDPC codes** derived from a single mother code ($N = 512$, $R = 0.5$). By puncturing the mother code to an initial high rate (e.g., $R = 0.70$) and then progressively disclosing the additional quantum variables that Bob requests Alice to generate in each retransmission round (e.g., $R = 0.63 \rightarrow 0.52$), the system achieves dynamic rate adaptation without prior SNR estimation. This blind adaptation capability ensures robust operation over time-varying quantum channels, including fiber links and potential free-space optical (FSO) scenarios.
- A **reliability-driven frozen-bit scheduling algorithm** is designed for polar codes based on Gaussian-approximation metrics, determining the most informative quantum variables to be released first. Similarly, an adaptive **parity-bit puncturing and replenishment strategy** is also developed for LDPC codes. These

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

Contributions	This work	[7]	[18]	[19]	[20]	[21]	[22]	[23]	[6]	[5]	[17]
CV-QKD	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Soft-decoding based frozen-bits index	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Fixed code rate scheme	✓	✓						✓	✓	✓	✓
Adaptive rate scheme reconciliation			✓	✓	✓		✓				
IR-HARQ reconciliation for CV-QKD	✓										
Frozen-bit redundancy selection rule for IR-HARQ	✓										
Variable coding scheme and code length	✓										
Enhanced secure distance under fixed bit budget	✓										

mechanisms prioritize the incremental disclosure of high-impact variables, accelerating decoder convergence and minimizing retransmission overhead.

- Comprehensive system-level simulations – including BLER, throughput, secure distance, and latency – demonstrate that the proposed IR-HARQ framework effectively balances efficiency, reliability, and delay. Each incremental redundancy round yields approximately 2–3 dB SNR improvement, extending secure transmission distances **beyond conventional single-shot polar and LDPC reconciliation schemes** under identical block-length constraints. Moreover, **polar-coded IR-HARQ** performs better at short block lengths and low SNRs, while **LDPC-coded IR-HARQ** becomes advantageous at higher SNR and larger block sizes.
- This work establishes a **unified SKR-aware adaptation framework** that jointly exploits quantum-domain incremental redundancy and classical soft-information refinement, providing a principled pathway toward adaptive, efficient, and secure CV-QKD implementations for both fiber-based and FSO environments.

The remainder of this paper is organized as follows. Section II provides some preliminaries on HARQ, Polar, and LDPC codes. Section III describes the IR-HARQ reverse-reconciliation protocol in detail, including the puncturing strategy, frozen/parity-bit scheduling, and retransmission procedures. Section IV derives analytical expressions for the SKR under collective Gaussian attacks, incorporating reconciliation efficiency and finite-block-length considerations. Section V presents a thorough performance analysis, comparing their BLER, throughput, secure distance, and latency against conventional schemes. Finally, Section VI concludes with a summary of key findings and highlights directions for future research.

II. PRELIMINARIES

A. HARQ

HARQ beneficially integrates the principles of automatic repeat request (ARQ) and forward error correction (FEC) for improving both communication reliability and throughput efficiency [13]. Pure ARQ requires repeated retransmissions of entire packets without utilizing previously received information, which leads to unnecessary redundancy, when errors are sparse. Conversely, pure FEC may inefficiently allocate resources by transmitting an excessive number of parity bits even under favorable channel conditions. The integration of ARQ and FEC therefore allows HARQ to dynamically balance error-correction capability with retransmission overhead, adapting more effectively to time-varying channel qualities.

Early HARQ implementations, such as Type I HARQ [24], operate by transmitting identical packets comprising both information and parity bits at every transmission attempt. At the receiver, each retransmission is decoded independently without combining with earlier ones. Although this approach is conceptually simple and straightforward, it may result in inefficient bandwidth utilization, since retransmitted packets often contain redundant parity information that does not necessarily improve decoding performance.

To address these inefficiencies, Type II HARQ [25] introduces the concept of incremental redundancy (IR). Instead of resending identical packets, Type II HARQ initially transmits only the information bits. If decoding at the receiver fails, subsequent retransmissions provide additional parity bits that are combined with the previously received data to enable joint decoding. This mechanism ensures that redundancy is supplied on demand: reliable blocks consume minimal bandwidth, while unreliable blocks progressively gain additional protection. As a result, Type II HARQ improves both decoding reliability and spectral efficiency across a broad range of channel conditions.

Further extending this principle, Type III HARQ [26], [27] employs retransmissions of differently structured redundancy packets. Each packet is independently decodable, yet when combined with earlier packets they enhance decoding accuracy. This strategy provides higher throughput and robustness by progressively supplying complementary parity information, thereby supporting flexible decoding strategies tailored to the instantaneous channel quality experienced.

In terms of packet combining at the receiver, HARQ schemes primarily employ two approaches: Chase Combining (CC) [28] and IR based combining [29]. CC aggregates soft information from multiple noisy replicas of the same packet, thereby providing diversity gain. By contrast, IR-based schemes transmit distinct sets of parity bits in each retransmission, which can be progressively combined with previously received packets. This approach reconstructs the original message with higher decoding efficiency compared to

repetition-based methods, particularly in challenging channel conditions.

In summary, these developments highlight the strength of HARQ in providing robust error correction, reduced retransmission overhead, and improved throughput under fluctuating channel quality. In this work, we focus our attention on Type II IR-HARQ, as it enables incremental transmission of redundancy bits, making it especially well suited for CV-QKD scenarios, where the SNR varies significantly with distance.

B. POLAR CODE AND PUNCTURING ALGORITHM

Polar codes, first introduced by Arikan [30], represent a class of near-capacity error-correcting codes suitable for Binary Discrete Memoryless Channels (BDMCs). Unlike Turbo and LDPC codes, Polar codes benefit from deterministic code construction, simpler encoding and decoding algorithms. Furthermore, their hardware complexity scales linearly with the code length [31].

Polar coding relies on the principle of channel polarization, which transforms a set of N identical channels into polarized channels comprising K highly reliable (good) channels and $(N-K)$ unreliable (bad) channels. The original information bits are transmitted exclusively through these reliable channels, while predetermined frozen bits, known to both encoder and decoder, are transmitted through the remaining less reliable channels. The Polar encoding operation can be mathematically formulated as:

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

where $\mathbf{x}_1^N$ is the encoded bit sequence, while $\mathbf{u}_1^N$ includes both information bits ($\mathbf{u_A}$) and frozen bits ($\mathbf{u_{A^C}}$). Furthermore, $\mathbf{G}_N$ is the Polar generator matrix defined as:

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

with $\mathbf{F}_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ representing the Polar kernel matrix, and $\otimes n$ denoting the n-th Kronecker power. The bit-reversal permutation matrix $\mathbf{B}_N$ separates odd-indexed and even-indexed input bits recursively. Consequently, Polar encoding can also be expressed as:

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

where $\mathbf{G_A}$ and $\mathbf{G_{A^C}}$ denote sub-matrices extracted from the generator matrix $\mathbf{G}_N$ corresponding to information and frozen bit indices, respectively.

We introduce an IR-HARQ scheme based on Polar codes initially employing puncturing, followed by the successive incremental transmission of the previously punctured frozen bits. The primary idea of the proposed scheme is as follows: we start from a mother code having a fixed low-rate (e.g., 0.5) to ensure robust error correction capabilities. Initially, this mother code is punctured to achieve an arbitrary higher code rate suitable for the prevalent channel condition (for instance, rate 0.7). The puncturing is performed by selectively removing frozen bits from the mother code based on their relative reliability [32], retaining the bits having the highest reliability for initial transmission.

If the initial decoding attempt at this higher code rate is unsuccessful, the proposed IR-HARQ mechanism is activated. Subsequent retransmissions are conducted incrementally by releasing previously punctured frozen bits. Specifically, if the initial transmission at rate 0.7 fails, the scheme retransmits the next most reliable frozen bits in the reliability rank order corresponding to the intermediate code rate (e.g., 0.6). If decoding continues to fail, additional retransmissions follow, progressively transmitting the remaining originally punctured frozen bits in order of decreasing reliability, until either successful decoding occurs or all bits from the mother code have been utilized.

This progressive approach leverages channel polarization to prioritize the retransmission of frozen bits based on their reliability ranking, effectively adapting the redundancy provided for the receiver. Consequently, the proposed scheme achieves flexible rate-compatibility and improved reliability, maintaining high throughput at favorable channel conditions, while significantly enhancing decoding performance and hence the SKR or distance under adverse conditions.

III. SYSTEM MODEL

The CV-QKD system establishes a connection between a pair of legitimate users, typically referred to as Alice and Bob. Initially, Alice generates Gaussian-modulated coherent states and transmits them to Bob over a quantum channel. Subsequently, Bob randomly measures one of the quadratures using homodyne detection.[1] After this quantum transmission phase, both parties engage in classical post-processing by exchanging necessary information through a public classical channel, with the aim of deriving secure secret keys [5]. The classical post-processing comprises two primary steps: reconciliation and privacy amplification. During reconciliation, Alice and Bob utilize FEC codes to generate matching reconciled keys. Following reconciliation, privacy amplification is applied to further minimize the potential information accessible to any eavesdropper.

A. GENERAL CV-QKD PROTOCOL

Fig. 1(a) illustrates the general progress of CV-QKD systems, including quantum-domain (QD) transmission and classical post-processing. After the coherent states modulated by Gaussian variables are transmitted from block (1) to block (2) over the quantum channel, the same number of Gaussian variables is prepared related as the block length of the mother code in this process. Alice and Bob proceed to sift their raw keys from blocks (3) and (4). These keys are correlated, i.e. they exhibit similarity, but may have been affected by channel impairments. Subsequently, Alice and Bob perform multidimensional reconciliation relying on error correction, as

[1] It is important to note that heterodyne detection requires measurement of both quadratures.

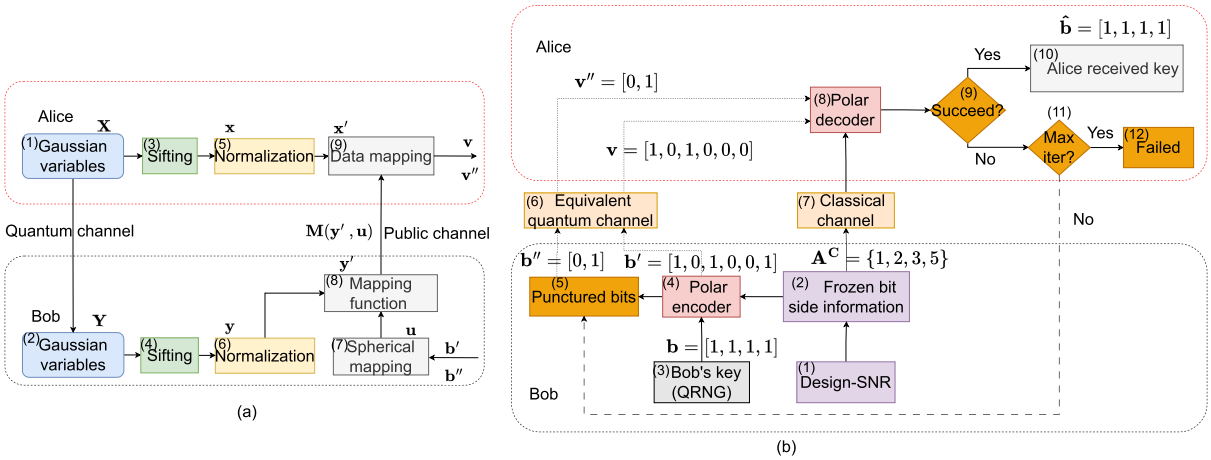

FIGURE 1. **(a) General CV-QKD system including quantum transmission and classical post-processing and (b) toy example of IR-HARQ polar-coded RR scheme.**

illustrated in Fig. 1(b). The detailed description of the general CV-QKD progress is provided below.

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

$$\mathbf{x}' = \frac{\mathbf{x}}{\|\mathbf{x}\|} \quad \mathbf{y}' = \frac{\mathbf{y}}{\|\mathbf{y}\|}. \tag{4}$$

2) Then Bob maps bit stream $\mathbf{b}'$ which is encoded by a Polar code as illustrated in Fig. 1(b) onto the unit sphere in block (7) as follows[2] [33]:

$$\mathbf{u} = \left(\frac{(-1)^{b'_1}}{\sqrt{D}}, \frac{(-1)^{b'_2}}{\sqrt{D}}, \ldots, \frac{(-1)^{b'_D}}{\sqrt{D}} \right). \tag{5}$$

3) Bob generates a mapping function in block (8) based on the unit sphere $\mathbf{u}$ and its normalized Gaussian variables $\mathbf{y}'$, as follows [33]:

$$\mathbf{M}\left(\mathbf{y}', \mathbf{u}\right) = \sum_{d=1}^{D} \alpha_d \left(\mathbf{y}', \mathbf{u}\right) \mathbf{A}_d, \tag{6}$$

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

4) Alice then applies the same mapping function gleaned from Block (8) as Bob signaled over the public channel to her normalized data $\mathbf{x}'$ to get $\mathbf{v}$ in block (9), which is a noisy version of $\mathbf{u}$. Based on this observation, it was demonstrated in [5], [33] that the quantum channel of a CV-QKD system can be characterized by a binary-input additive white Gaussian noise (BI-AWGN) model.
5) Finally, Alice carries out Polar-code based RR in Fig. 1(b) to get the reconciled key.

The processes in block (1) to (9) of Fig. 1(a) establish the equivalent quantum channel in block (6) of Fig. 1(b), where the input is $\mathbf{b}'$ and $\mathbf{b}''$ and the output is $\mathbf{v}$ and $\mathbf{v}'$, respectively. Traditional QKD channel models frequently adopt a Gaussian noise approximation to characterize quantum channel imperfections [17], [34].

While fiber channels are generally stable after calibration, it should be noted that the optical signals used in CV-QKD are extremely weak and thus highly sensitive to small environmental fluctuations such as temperature drift, polarization rotation, and mechanical vibration, particularly in metro-access networks [35], [36]. Hence, adaptive reconciliation schemes like the proposed IR-HARQ provide enhanced robustness against such residual variations. But, the underlying principle of incremental redundancy offers a promising solution for dynamic free-space optical (FSO) links, where atmospheric turbulence and pointing errors cause strong transmittance fluctuations [37]. Although the present work focuses on fiber-based CV-QKD, extending the IR-HARQ concept to satellite or FSO scenarios constitutes an interesting direction for future research.

B. IR-HARQ POLAR-CODED RR SCHEME

This scheme shows the SCL decoding based IR-HARQ Polar-coded CV-QKD reconciliation scheme of Fig. 1(b) relying on the idealized simplifying assumption of having error-free transmission of the side information. The frozen bit indices represent the side information, which are transmitted over the public channel from Bob to Alice. The operation is described below.

1) In block (1) of Fig. 1(b), Bob generates an initial raw key stream by employing a quantum random number generator (QRNG). As an illustrative example, we consider a half-rate Polar code with parameters [8,4], where Bob's generated raw key sequence is denoted as $\mathbf{b} = [1, 1, 1, 1]$.
2) Given that the equivalent channel model is a BI-AWGN channel, the Gaussian approximation method described in [38] is utilized to determine the frozen-bit

[2]We note that the dimension normally takes D=1,2,4,8. But it was shown in [33] that D=8 has the best BLER, hence D=8 is the default choice in this paper.

indices. Under a specific predetermined design-SNR[3] scenario [39], selected because the actual quantum-channel conditions are assumed unknown in practice, the set of frozen indices obtained is $\mathbf{A^C} = \{1, 2, 3, 5\}$, as shown at the output of block (2).

3) Next, in block (4), Bob encodes the information bits $\mathbf{b}$ using the Polar encoder in conjunction with the frozen indices $\mathbf{A^C}$ obtained from block (2). This produces the non-systematically encoded Polar bit sequence, represented as $[\mathbf{b}'', \mathbf{b}'] = [0, 1, 1, 0, 1, 0, 0, 1]$.
4) In the subsequent puncturing stage at block (5), Bob selectively punctures the encoded bit sequence based on the bit-channel reliability metrics [32]. In this illustrative scenario, indices $\mathbf{A^C} = \{1, 2\}$ correspond to the least reliable bit-channel positions. Thus, the bit stream to be transmitted over the quantum channel of block (6) becomes $\mathbf{b}' = [1, 0, 1, 0, 0, 1]$, while the bits $\mathbf{b}'' = [0, 1]$ are retained by Bob for potential transmission in case of decoding errors.
5) Simultaneously, Bob conveys the indices of the frozen bits $\mathbf{A^C} = \{1, 2, 3, 5\}$ to Alice via an error-free classical auxiliary channel in block (7) in supporting of Alice's decoding procedure.
6) Alice then receives a noisy version of Bob's transmitted bit sequence through the hostile quantum channel, represented by $\mathbf{v} = [1, 0, 1, 0, 0, 0]$, which contains a single bit error in the last position. By utilizing the frozen-bit indices received through the classical channel, Alice performs Polar decoding at block (8). Due to the absence of the bits in the punctured positions $\mathbf{A^C} = \{1, 2\}$, the log-likelihood ratios (LLRs) for these positions are initially set to zero during the decoding process. This corresponds to having both 0 and 1 with 0.5 probability in these positions.
7) Following decoding within block (9), Alice assesses the decoding outcome. If successful, Alice discards the bits associated with the frozen indices and extracts the remaining decoded bits as her reconciled key $\hat{\mathbf{b}} = [1, 1, 1, 1]$, as shown at the output of block (10).
8) If decoding fails, Alice evaluates whether the number of retransmissions has reached the predefined maximum (max iter). If the limit is exceeded, the current key block is discarded, and reconciliation fails. Otherwise, Alice requests the further transmission of punctured bits from Bob, who then sends the previously punctured bits having the next highest reliability from block (5). In the current example, only two punctured bits remain ($\mathbf{b}'' = [0, 1]$), both of which are then transmitted. Alice updates the previously zero-valued LLRs accordingly with newly received bit information, hence enhancing the decoding reliability for positions $\mathbf{A^C} = \{1, 2\}$.

[3]We provide a value for system to determine the frozen bits indices using Gaussian approximation method, this value can be chosen by different block length, coding rate.etc.

In this work, the standard parameter-estimation (PE) and privacy-amplification (PA) stages of CV-QKD are explicitly included after reconciliation. The proposed IR-HARQ mechanism modifies only the reconciliation step by adaptively generating and transmitting extra quantum-domain variables based on the previous decoding outcomes, while the equivalent BI-AWGN model is employed solely for the analytical evaluation of β and SKR. The overall security framework – including the estimation of channel transmittance T, total excess noise ξ_{total}, and the finite-block size based correction $\Delta(n)$ – remains identical to conventional CV-QKD. In contrast to conventional rate-adaptive schemes that fix the code rate according to a single estimated SNR obtained from PE, the proposed IR-HARQ dynamically adjusts redundancy via multiple feedback rounds. This decoupling of PE and reconciliation ensures that the system maintains full information-theoretic security while providing robust, real-time adaptation to varying channel conditions.

C. IR-HARQ LDPC-CODED RR SCHEME

LDPC codes constitute a class of linear block codes characterized by a sparse parity-check matrix (PCM) $\mathbf{H}$ of size $(N-K) \times N$, where N denotes the block length and K is the number of information bits, giving a code rate of $R=K/N$. Each row of $\mathbf{H}$ contains d_c ones (check-node degree) and each column d_v ones (variable-node degree). The PCM can be visualized as a bipartite Tanner graph [40] connecting variable and check nodes whenever $H_{i,j}=1$. For example, a regular (10,5) LDPC code associated with $d_v=2$ and $d_c=4$ has

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

The benchmark PCMs used in this work follow the design procedures of [41].

For the LDPC-based IR-HARQ scheme, the transmission process is implemented through puncturing and incremental transmission of parity bits [42]. Specifically, the mother code is first punctured by uniformly [43] removing a portion of the parity bits, so that only the information bits and a subset of parity bits are transmitted in the initial round. This parity-only puncturing is standard in rate-compatible LDPC designs and enables using the same decoder across rates [42]. For example, a mother code with rate $R = 0.5$ can be punctured to $R = 0.7$ in the initial transmission. If decoding fails, transmission proceeds by sequentially supplementing the previously punctured parity bits, thereby reducing the code rate to $R = 0.6$. In the case of a second retransmission, the remaining parity bits are transmitted, restoring the unpunctured mother code of rate $R = 0.5$.

This procedure ensures that the incremental redundancy mechanism of LDPC follows a structure analogous to that of Polar codes: each extra transmission progressively reduces the

effective code rate by providing additional parity information, thereby enhancing the decoding reliability, while maintaining flexibility in terms of throughput adaptation. The belief propagation (BP) decoding is used for LDPC codes, while the structure of LDPC codes and the associated decoding complexity comparison between Polar and LDPC are elaborated in [17].

Although binary rate-compatible polar and LDPC codes are used in this work for implementation convenience, the proposed IR-HARQ framework is generic and can incorporate other code families. As a design alternative, non-binary and multi-edge LDPC codes achieve excellent reconciliation efficiency in the very-low-SNR regime of CV-QKD [44]. Their flexible degree distributions allow near-capacity performance, but the irregular graph structure and multi-edge message-passing operations substantially increase the decoding complexity, which in turn complicates incremental-redundancy decoding and code-rate scheduling. By contrast, binary rate-compatible designs enable deterministic puncturing and replenishment across retransmission rounds, supporting fast feedback-driven adaptation across a wide range of SNRs. Future work will investigate the feasibility of integrating non-binary or multi-edge LDPC constructions into the IR-HARQ framework to further enhance performance at extremely low SNRs.

IV. SECRET KEY RATE ANALYSIS

A. REVERSE RECONCILIATION

Since collective attacks[4] and finite-length codes are considered, the SKR for a CV-QKD system using RR is defined as [5]:

$$K^{RR} = \gamma(1-\theta)[\beta I_{AB} - \chi_{BE} - \Delta(n)], \tag{7}$$

where γ indicates the specific fraction of key extractions by Eve, normalized to the total amount of data exchanged between Alice and Bob. Additionally, θ represents the BLER estimated during reconciliation. In Equation (7), I_{AB} denotes the classical mutual information shared between Alice and Bob based on correlated data, while χ_{BE} represents Eve's extractable amount of Holevo information [48]. The term Δn quantifies the reduction in SKR due to finite block-length effects.

The finite-size offset factor $\Delta(n)$ accounts for the statistical deviation caused by finite-length parameter estimation. As established in [49], for block sizes satisfying $n > 10^4$, it simplifies to:

$$\Delta(n) \approx 7\sqrt{\frac{\log_2\left(\frac{2}{\epsilon}\right)}{n}}, \tag{8}$$

where ϵ represents the protocol's security failure probability, widely set as $\epsilon = 10^{-10}$ in the literature [49]. In our framework, the block size selected is $n = 10^{12}$, commonly employed in benchmark studies such as [5].

The reconciliation efficiency β in (7) is calculated according to [50]:

$$\beta = \frac{\Upsilon}{C} = \frac{\Upsilon}{0.5\log_2(1+\mathrm{SNR}_\beta)} = \frac{\Upsilon}{0.5\log_2\left(1+\frac{E_S}{E_N}\right)}, \tag{9}$$

where Υ is the measured throughput,

$$\Upsilon = \frac{K}{\hat{N}}, \tag{10}$$

with K denoting the number of information bits and $\hat{N}$ representing the average number of transmitted bits until successful decoding is achieved. Here SNR_β represents the simulated SNR corresponding to the BLER equal to 10^{-1}. The mutual information between Alice and Bob is expressed as [51]:

$$I_{AB} = \frac{1}{2}\log_2(1+\mathrm{SNR}_{\text{target}}) = \frac{1}{2}\log_2\left(\frac{V+\xi_{\text{total}}}{1+\xi_{\text{total}}}\right). \tag{11}$$

where $\mathrm{SNR}_{\text{target}}$ is adjusted to the same as SNR_β via power control of V, which is the variance of Alice's initially transmitted signals defined by $V = V_S + 1$, with V_S representing the variance of Gaussian signals used in CV-QKD modulation [5]. Additionally, ξ_{total} denotes the total receiver noise, expressed as:

$$\xi_{total} = \xi_{line} + \frac{\xi_{hom}}{T_{ch}}, \tag{12}$$

where $\xi_{hom} = \frac{1+v_{el}}{\eta} - 1$ is the homodyne detector's noise, with v_{el} representing electronic noise, and η denoting detection efficiency. The channel-induced noise is $\xi_{line} = (\frac{1}{T_{ch}} - 1) + \varepsilon$, with T_{ch} as channel transmittance and ε as the excess noise, including modulation, phase-recovery, and Raman noise [51]. Excess noise is measured in terms of shot-noise units (SNU), normalized by the shot-noise power [52]. Assuming a single-mode fiber channel having an attenuation of $\alpha = 0.2$ dB/km, the channel path-loss is given by $T_{ch} = 10^{-\alpha d/10}$, where d is the distance between the communicating parties.

The Holevo information between Bob and Eve is calculated as [51]:

$$\chi_{BE} = S_E - S_{(E|B)} = S_{AB} - S_{(E|B)}, \tag{13}$$

where S is the von Neumann entropy, defined in [48]. For Gaussian states, von Neumann entropy is related to the symplectic eigenvalues [53]:

$$S = \sum_f h(f), \tag{14}$$

where we have:

$$h(f) = \left(\frac{f+1}{2}\right)\log_2\left(\frac{f+1}{2}\right) - \left(\frac{f-1}{2}\right)\log_2\left(\frac{f-1}{2}\right), \tag{15}$$

Finally, the Holevo information is:

$$\chi_{BE} = h(f_1) + h(f_2) - h(f_3), \tag{16}$$

[4]In the security analysis of CV-QKD protocols, like the collective Gaussian attacks [45] represent the most significant family allowed by quantum mechanics [46]. The detailed framework for collective Gaussian attacks is explicitly outlined in [37], [47].

TABLE 2. Simulation Parameters Used in Paper

Parameter	Value
Coding type	Polar code, LDPC code
Block length	512, 1024, 2048
Decoding algorithm	SCL for Polar ($L = 16$), BP for LDPC
Mother code	$N = 512$, $R = 0.5$
Modulation	BPSK
Equivalent quantum channel	BI-AWGN
Classical channel	Error-free

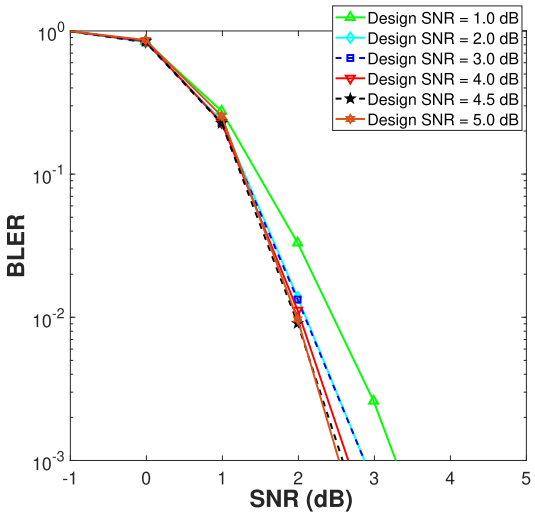

FIGURE 2. BLER performance comparison for different design-SNR values. The block length and coding rate of the Polar code are 512 and 0.5, respectively. SCL decoding with $L = 16$ is used.

where f_1, f_2 and f_3 are symplectic eigenvalues of S_{AB} and $S_{(E|B)}$. The SKR is then obtained by substituting (11) and (16) into (7).

V. SYSTEM PERFORMANCE

A. CLASSICAL IR-HARQ PERFORMANCE

The simulation parameters are summarized at Table II, Fig. 2 shows the BLER performance of a Polar code with block length $N = 512$ and code rate $R = 0.5$ under different design-SNR values. The results demonstrate that an excessively low design-SNR (e.g., 1.0 dB) results in a significant rightward shift of the BLER curve, requiring nearly 2.7 dB SNR to reach BLER $= 10^{-2}$. By contrast, higher design-SNR values between 4.0 dB and 5.0 dB achieve the best performance, and 4.5 dB, which yields the steepest BLER drop. Thus, a design-SNR in the range of 4–5 dB provides the most favorable error-rate performance for the mother code chosen. Different block lengths require different design-SNR.

Figs. 3 and 4 present the same BLER dataset under two standard normalization metrics. Fig. 3 plots BLER versus SNR, while Fig. 4 uses E_b/N_0, where the two scales satisfy $E_b/N_0 = \text{SNR} + 10\log_{10}(R_c)$. The apparent horizontal shift between the curves arises naturally from this relation for different code rates (R_c=0.9 to 0.5). Thus, both plots are retained

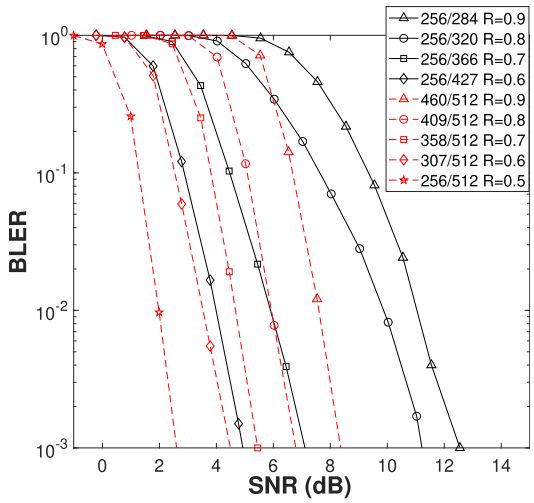

FIGURE 3. BLER performance versus SNR, where black continuous lines represent punctured results using a Polar mother code of $N = 512$, $R = 0.5$ and red dashed lines represent different codes using the same block length.

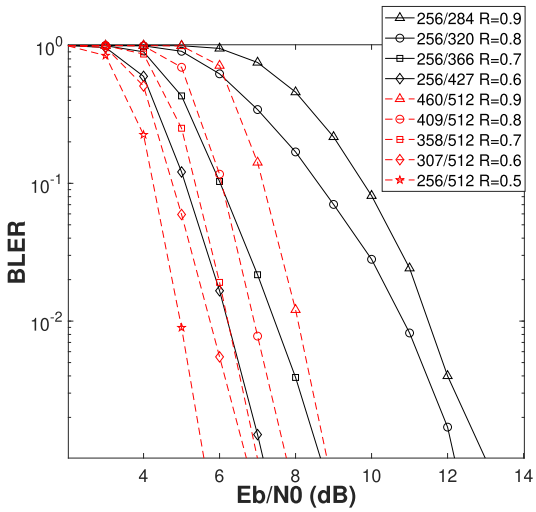

FIGURE 4. BLER performance versus Eb/N0, where black continuous lines represent punctured results using a Polar mother code of $N = 512$, $R = 0.5$ and red dashed lines represent different codes using the same block length.

to offer complementary channel-domain and rate-normalized perspectives of the BLER performance. Explicitly, the discrepancy between the two scales is a direct function of the code rate.

B. ARQ AIDED RR PERFORMANCE ANALYSIS

1) BLER AND THROUGHPUT V.S. SNR PERFORMANCE

The BLER performance of Type I ARQ with $N = 512$, $K = 256$, and $R = 0.5$ seen in Fig. 5 reveals distinct differences between Polar and LDPC codes. For the initial transmission, Polar codes outperform LDPC codes, achieving noticeably lower BLER at the same SNR, which indicates their superior finite-length performance for short blocks. Observe that both coding schemes benefit from accumulated redundancy,

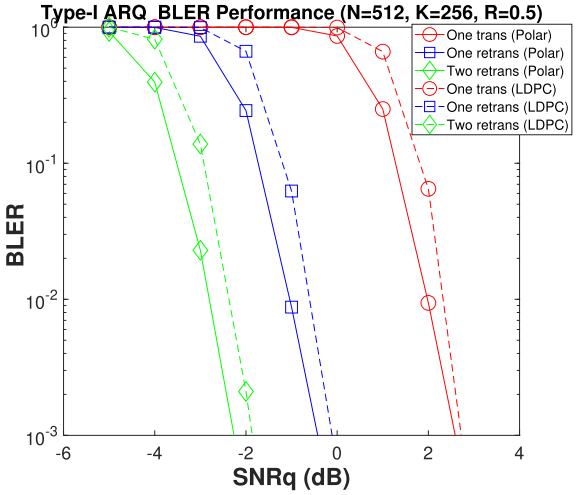

FIGURE 5. BLER performance versus SNR of Type I ARQ comparing LDPC (dashed line) and Polar codes (solid line).

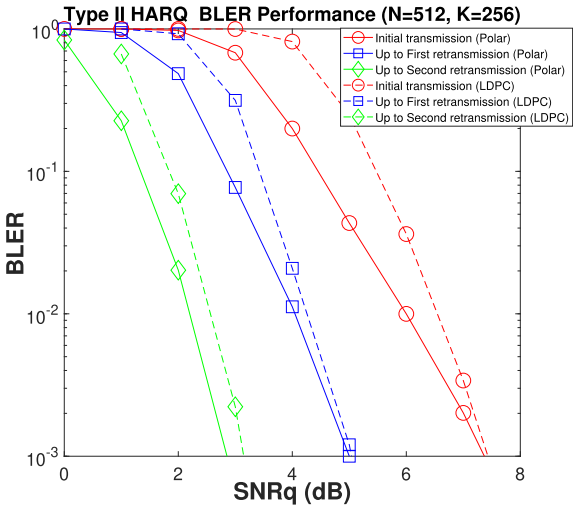

FIGURE 6. BLER performance versus SNR of Type II ARQ comparing LDPC (dashed line) and Polar codes (solid line).

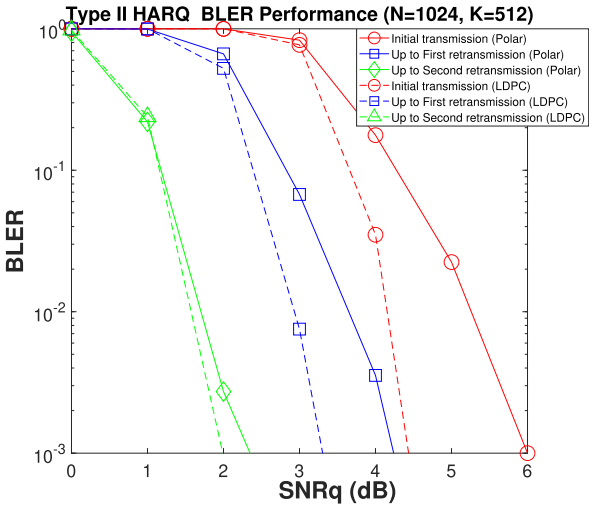

FIGURE 7. BLER performance versus SNR of Type II ARQ comparing LDPC (dashed line) and Polar codes (solid line).

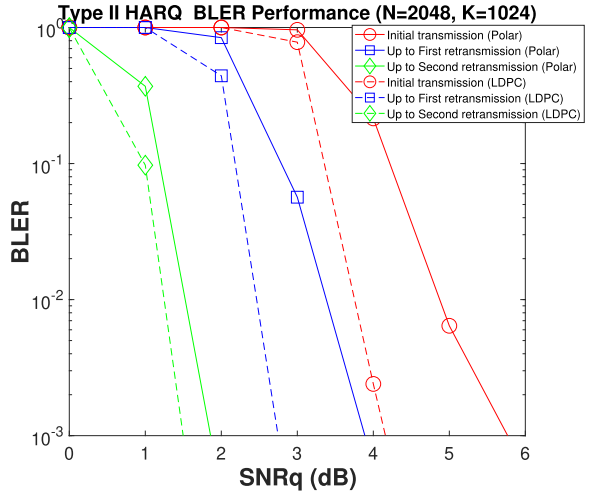

FIGURE 8. BLER performance versus SNR of Type II ARQ comparing LDPC (dashed line) and Polar codes (solid line).

leading to considerable SNR gains and leftward shifts of the BLER curves. Nevertheless, Polar codes consistently maintain an advantage over LDPC codes, achieving a target BLER at lower SNR values across all transmission rounds. These results demonstrate that under Type I ARQ, Polar codes are more suitable for scenarios having strict reliability requirements and limited block length, since they require lower SNR to achieve the same performance compared to LDPC codes.

Figs. 6 to 8 illustrate the detailed retransmission evolution of the proposed Type II IR-HARQ scheme for both Polar and LDPC codes. Each color represents a distinct transmission round: the red curve corresponds to the initial transmission (r=0), the blue curve to the first retransmission (r=1), and the green curve to the second retransmission (r=2). For each stage, both the block error rate for the polar code (solid lines) and the LDPC code (dashed lines) are plotted under the same mother-code configuration. As incremental redundancy accumulates, the BLER curves progressively shift leftward, indicating lower required SNR for successful decoding, while the throughput decreases slightly due to additional transmitted bits. This joint presentation explicitly reveals how IR-HARQ dynamically trades redundant transmission for reliability enhancement, allowing direct comparison of Polar- and LDPC-coded implementations across all retransmission rounds.

Figs. 9– 12 summarize the BLER and throughput of both Type I ARQ and Type II IR-HARQ schemes for Polar- and LDPC-coded reconciliation. For clarity, the colors indicate the retransmission round—red, blue, and green correspond to the initial transmission (r=0), first retransmission (r=1), and second retransmission (r=2), respectively. Furthermore, the line style in each plot matches the coding family (solid for Polar, dashed for LDPC).

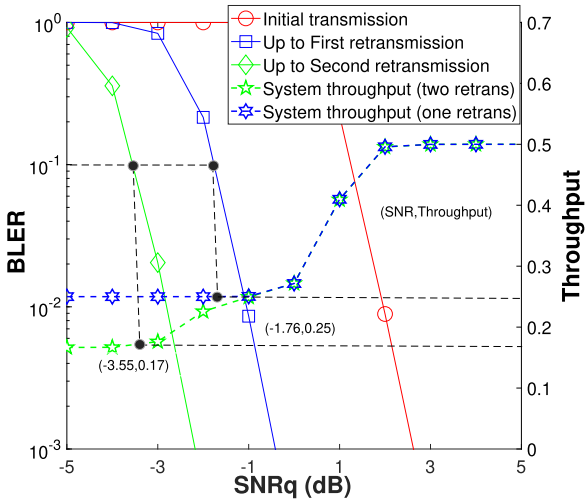

FIGURE 9. BLER performance of the Type I ARQ scheme for each stage of system and also the system throughput (Polar mother code of $N = 512, K = 256$).

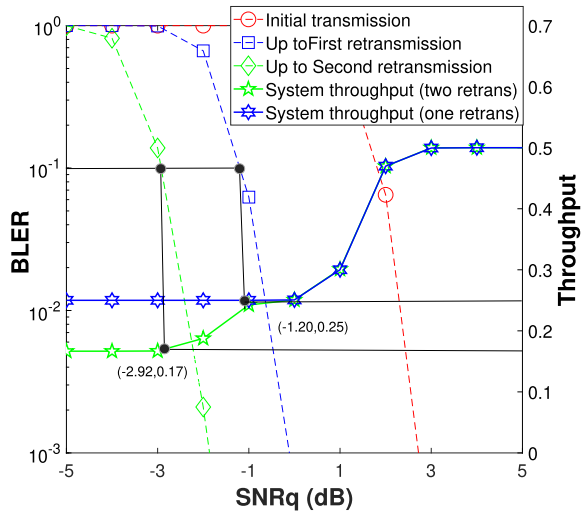

FIGURE 10. BLER performance of the Type I ARQ scheme for each stage of the system and also the system throughput (LDPC mother code of $N = 512, K = 256$).

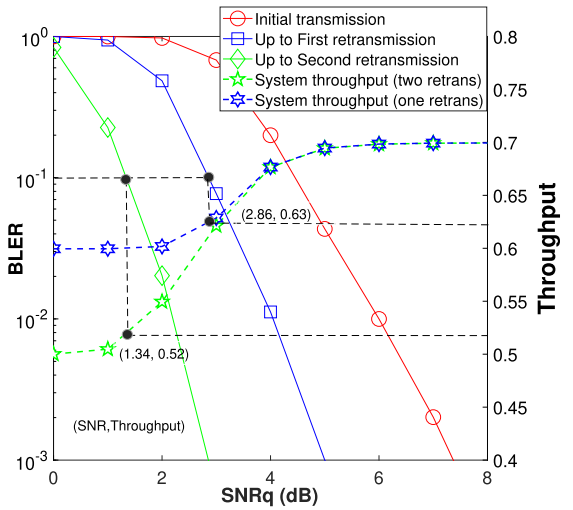

FIGURE 11. BLER performance for each stage of Polar-coded Type II ARQ system and also the system throughput (mother code of $N = 512, K = 256$).

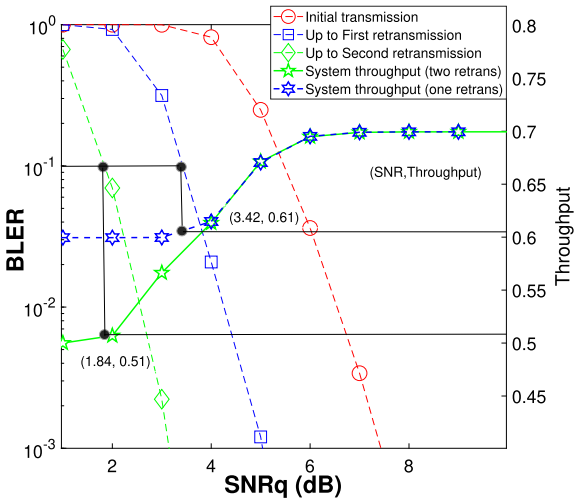

FIGURE 12. BLER performance for each stage of LDPC-coded Type II ARQ system and also the system throughput (mother code of $N = 512, K = 256$).

In Figs. 9–10, corresponding to Type I ARQ, the BLER curves shift leftward with each retransmission, demonstrating that accumulated redundancy improves reliability at lower SNR. However, this comes at the expense of reduced throughput, which monotonically decreases from Υ=0.50 for the first transmission to Υ=0.25 and Υ=0.17 after the first and second retransmissions, respectively. Polar codes maintain steeper BLER slopes and achieve the target BLER values at lower SNR compared to LDPC, confirming their advantage in finite-length operation.

By contrast, Figs. 11–12 (Type II IR-HARQ) exhibit both improved reliability and sustained throughput under incremental redundancy. Each additional retransmission supplies additional frozen or parity bits, reducing the SNR threshold required for successful decoding, while retaining higher throughput than Type I ARQ (e.g., Υ=0.70 → 0.63 → 0.52 for Polar, and Υ=0.70 → 0.59 → 0.51 for LDPC). In contrast to Type I, where retransmissions only consume extra bandwidth, Type II IR-HARQ leverages soft-information combining to enhance decoding reliability and maintain higher reconciliation efficiency across retransmission stages. Polar-coded IR-HARQ shows clear benefits in the low-SNR region, whereas LDPC becomes competitive at higher SNRs and longer block lengths. These results collectively confirm that the proposed IR-HARQ achieves superior reliability–throughput trade-offs compared to classical domain ARQ, while preserving the complementary strengths of Polar and LDPC codes within a unified adaptive reconciliation framework.

Tables 3 and 4 summarize the SNR–throughput relationships obtained from the simulation results seen in Figs. 9–12.

TABLE 3. SNR–Throughput for Each Stage of Polar and LDPC Codes ($N = 512, K = 256$, Type I)

Code	Stage	Υ	SNR (dB)	K	$\hat{N}$
Polar	Initial	0.50	1.24	256	1×512
	1st retrans.	0.25	-1.76	256	2×512
	2nd retrans.	0.17	-3.55	256	3×512
LDPC	Initial	0.50	1.81	256	1×512
	1st retrans.	0.25	-1.20	256	2×512
	2nd retrans.	0.17	-2.92	256	3×512

TABLE 4. SNR–Throughput for Each Stage of Polar and LDPC Codes ($N = 512, K = 256$, Type II)

Code	Stage	Υ	SNR (dB)	K	$\hat{N}$
Polar	Initial	0.70	4.44	256	366
	1st retrans.	0.63	2.86	256	$366 + 40$
	2nd retrans.	0.52	1.34	256	$366 + 40 + 86$
LDPC	Initial	0.70	5.47	256	366
	1st retrans.	0.59	3.42	256	$366 + 68$
	2nd retrans.	0.51	1.84	256	$366 + 68 + 68$

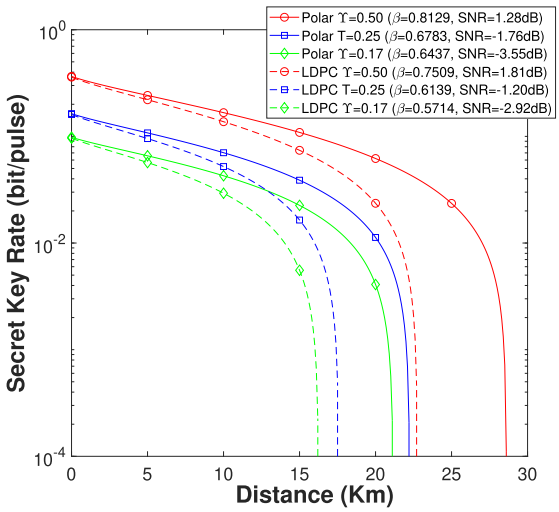

FIGURE 13. Performance of SKR for Type I based RR scheme for LDPC and Polar codes. The homodyne detector efficiency is set to $\eta = 0.98$, and the detector electronic noise is fixed at $v_{el} = 0.01$ SNU. The reconciliation efficiencies (βs) are computed based on the SNR corresponding to BLER of 0.1, while the excess noise is assumed to be $\varepsilon = 0.002$ SNU (mother code of $N = 512, K = 256$).

The values listed represent the average simulated SNR and corresponding throughput Υ achieved at each retransmission stage (initial, first, and second), under the same mother-code configuration of N=512, K=256. These data provide a compact numerical reference, illustrating how incremental redundancy reduces the SNR required while slightly decreasing throughput as additional transmissions accumulate.

2) SKR PERFORMANCE

Fig. 13 characterizes the Type I ARQ based RR scheme, where the SKR decreases rapidly with transmission distance

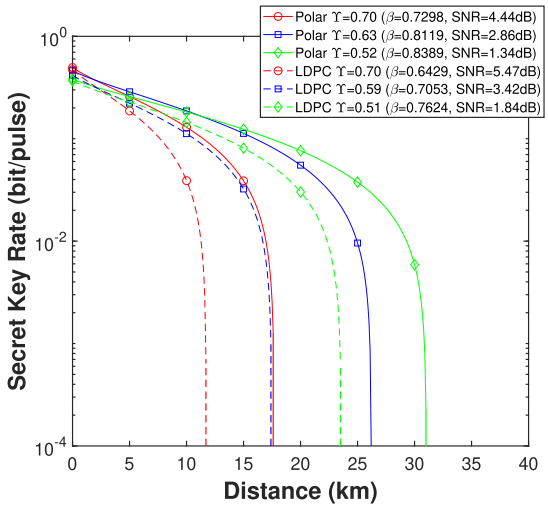

FIGURE 14. SKR of the Type II IR-HARQ based RR scheme for LDPC and Polar codes. The homodyne detector efficiency is set to $\eta = 0.98$, and the detector electronic noise is fixed at $v_{el} = 0.01$ SNU. The reconciliation efficiencies (βs) are computed based on the SNR corresponding to BLER of 0.01, while the excess noise is assumed to be $\varepsilon = 0.002$ SNU (mother code of $N = 512, K = 256$).

for both Polar and LDPC codes. The reconciliation efficiencies β are derived at the SNR values corresponding to a block error rate (BLER) of 0.1. At higher initial throughputs (e.g., $\Upsilon = 0.50$), Polar codes achieve moderately longer transmission distances than LDPC codes under similar conditions. However, as the throughput decreases ($\Upsilon = 0.25$ or $\Upsilon = 0.17$), the SKR curves also show a pronounced reduction in achievable distance, reflecting the inefficiency of Type I retransmissions. Explicitly the additional redundancy does not effectively improve the performance. Overall, the Type I scheme suffers from reduced reconciliation efficiency and limited adaptability with respect to SNR variations, leading to eroded robustness at longer distances.

In contrast, Fig. 14 characterizes the IR-HARQ based RR scheme which exhibits a significant improvement in both throughput and achievable distance. By exploiting incremental redundancy, the effective throughput values ($\Upsilon = 0.70, 0.59, 0.52$, etc.) remain relatively high even as distance increases, while maintaining reconciliation efficiencies β close to their theoretical limits at the corresponding SNR. Compared to Type I ARQ, the SKR curves extend considerably further, with Polar codes in particular outperforming LDPC codes at higher throughputs. This indicates that IR-HARQ can achieve both higher efficiency and extended coverage range, since the adaptive use of redundancy allows for better reconciliation efficiency across different SNR conditions. Thus, IR-HARQ effectively mitigates the trade-off between throughput and distance observed in Type I, offering a more robust and scalable solution for secret key generation.

In the Type I ARQ scheme, retransmissions substantially reduce the BLER, thereby enhancing reliability, but at the cost of reduced throughput. Polar codes deliver superior error-rate performance and maintain higher throughput at a given

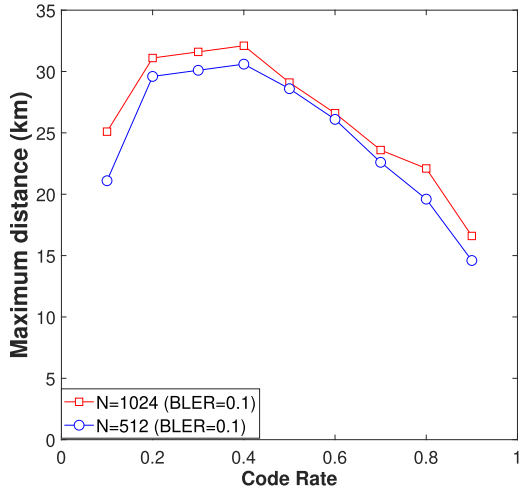

FIGURE 15. Maximum distance versus code rate of single-transmission at block lengths of $N = 512, 1024$ and a BLER value of 0.1 for Polar codes.

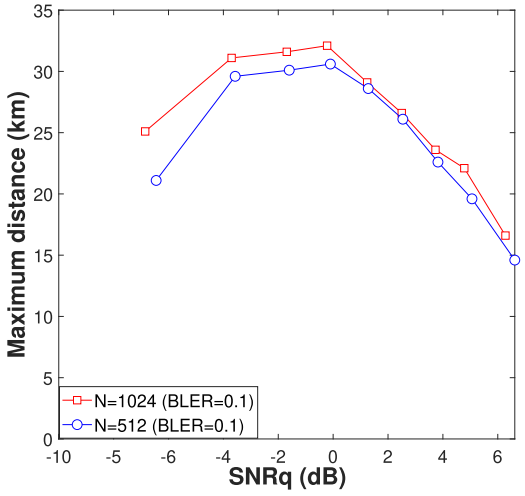

FIGURE 16. Maximum distance versus SNR of single-transmission at block lengths of $N = 512, 1024$ and a BLER value of 0.1 for Polar codes.

SNR, making them more favorable for short block lengths and stringent reliability constraints. By contrast, the Type II IR-HARQ scheme advocated introduces incremental redundancy, which reduces the SNR required for reliable decoding improves throughput through on-demand parity transmission. This demonstrates that Type II IR-HARQ achieves a better balance among reliability, efficiency, and coverage, while Type I ARQ provides a meaningful reference illustrating the baseline trade-offs of retransmission-based reconciliation in CV-QKD.

Figs. 15 and 16 portray the maximum transmission distance under a single-shot transmission versus the Polar code rate and SNR for block lengths of $N = 512$ and $N = 1024$ at a fixed BLER target of 0.1. The results serve as a baseline for evaluating retransmission strategies. As seen in Fig. 15, there exists a beneficial code rate region around $R = 0.3$–0.4 that maximizes the achievable distance. Beyond this, the performance degrades due to insufficient redundancy. Similarly,

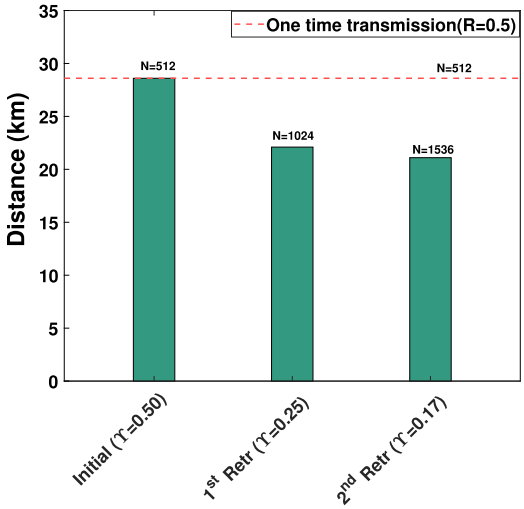

FIGURE 17. Performance comparison of a Type I scheme to single transmission using a Polar code of $N = 512$ and $R = 0.5$.

Fig. 16 illustrates that the achievable distance first increases with the SNR but eventually saturates, indicating diminishing returns at higher SNR levels. Moreover, the longer block lengths of $N = 1024$ consistently outperforms $N = 512$, highlighting the direct benefits of coding gain in extending the communication range.

All SKR curves in Figs. 15 and 16 are obtained under a constant receiver-SNR condition achieved by adaptive distance-dependent transmit power control. For each target SKR, the transmitter adjusts the modulation variance so that the received SNR remains fixed while the propagation distance varies, enabling fair distance comparison under equal-SNRs operation.

These baseline results are directly related to the main theme of the paper: they establish the limits of one-time transmission against which ARQ/HARQ schemes can be compared. Specifically, the improvements achieved by Type I and Type II HARQ in subsequent sections can be quantitatively benchmarked relative to the single-transmission case, thereby demonstrating how retransmission mechanisms and coding strategies enhance both reliability and coverage beyond the baseline performance.

3) DELAY ASPECTS

Fig. 17 characterizes Type I retransmission scheme, the distance exhibits a noticeable degradation upon increasing the number of transmissions. Specifically, as the number of transmissions increases, the effective throughput decreases from $\Upsilon = 0.50$ in the initial transmission to $\Upsilon = 0.25$ and $\Upsilon = 0.17$ after the first and second retransmissions, respectively. This reduction in throughput is accompanied by a substantial increase in the number of transmitted bits ($N = 512 \rightarrow 1024 \rightarrow 1536$). Moreover, the achievable distance under retransmissions is consistently shorter than that obtained by a single transmission for a code rate of $R = 0.5$. This is because

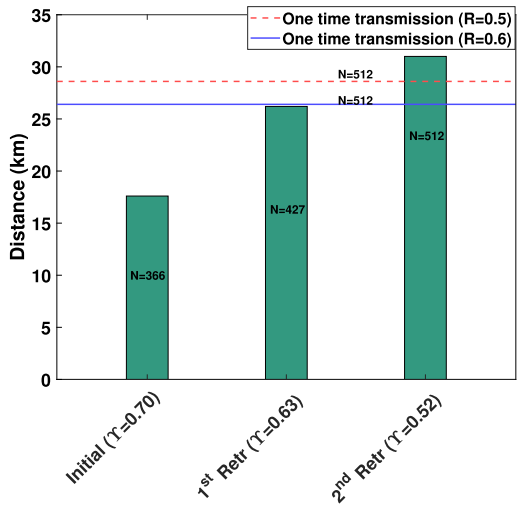

FIGURE 18. Performance comparison of IR-HARQ scheme to single transmission using a Polar code of $N = 512$ and $R = 0.5, 0.6$.

Type I retransmissions reduce the throughput, while the required SNR is not lower enough compared to that in a single transmission, as evidenced in Figs. 5 and 15. Consequently, the reconciliation efficiency β calculated based on (10) is reduced, which in turn shortens the achievable transmission distance. These results highlight the inefficiency of Type I retransmissions, where the accumulated redundancy leads to reduced spectral efficiency without extending the coverage distance.

By contrast, the IR-HARQ scheme characterized in Fig. 18 demonstrates a more favorable trade-off between throughput and coverage distance. At the second retransmission, the total number of transmitted bits matches that of a single transmission at $R = 0.5$ ($N = 512$), yet the effective throughput of $\Upsilon = 0.52$ surpasses that of the single-transmission case. Furthermore, the achievable distance extends beyond the reference distance of one-time transmission. After the first retransmission, the required number of transmitted bits ($N = 427$) is even lower than that of a single transmission at $R = 0.6$ ($N = 512$), while maintaining a comparable transmission distance. These observations confirm the efficiency of IR-HARQ, which intelligently exploits the incremental redundancy to achieve a higher throughput and longer coverage compared to both single transmission and Type I retransmissions.

VI. CONCLUSION

We have proposed an adaptive RR protocol for CV-QKD that integrates IR-HARQ with rate-compatible Polar and LDPC codes. We punctured a single mother code of length $N = 512$, rate $R = 0.5$ to an initial effective rate of $R = 0.70$. Then, upon decoding failure, we incrementally transmitted redundancy bits to arrive at rates of $R = 0.63$ and $R = 0.52$. As a benefit, our scheme dynamically matches redundancy to the prevalent channel conditions within the bit-budget of the mother code. Each retransmission provides approximately 2–3 dB extra SNR gain, yielding significantly improved BLER performance and extended secure transmission distance.

Under identical block-length constraints, IR-HARQ relying on Polar codes consistently outperforms fixed-rate Polar and LDPC codes in terms of both BLER performance and SKR, especially in low-SNR and short block-length regimes. On the other hand, the LDPC-based IR-HARQ using parity-bit puncturing demonstrates competitive performance at larger block lengths, highlighting the complementary nature of Polar and LDPC coding strategies. The system-level analysis further confirms that IR-HARQ effectively balances the throughput, latency, and reliability, providing substantial advantages over conventional single-transmission or Type I retransmission schemes. Our findings provide practical design guidelines: Polar-coded based IR-HARQ is advantageous in low-SNR or short-packet regimes, whereas LDPC-based IR-HARQ is more suitable for high-SNR and long-block scenarios.

To advance this work, future research will explore more sophisticated coding and ARQ schemes [13] and evaluate finite-size security bounds under realistic loss and noise models. Machine-learning-assisted puncturing and redundancy scheduling will be investigated to further minimize the number of retransmissions and latency. Hardware-in-the-loop prototyping will be pursued to validate decoding complexity and throughput in practical CV-QKD systems. In addition, integrating IR-HARQ with multidimensional reconciliation or non-Gaussian modulation schemes may unlock even higher reconciliation efficiency, enabling long-distance secure quantum communications.

REFERENCES

[1] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Proc. Workshop Theory Appl. Cryptographic Techn.*, 1993, pp. 410–423.
[2] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. Nickel, C. Donahue, and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," *Phys. Rev. A*, vol. 67, no. 5, 2003, Art. no. 052303.
[3] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *Proc. 2009 IEEE Int. Symp. Inf. Theory*, 2009, pp. 1879–1883.
[4] D. Elkouss, J. Martinez-Mateo, and V. Martin, "Information reconciliation for quantum key distribution," *Quantum Inf. Comput.*, vol. 11, no. 3-4, pp. 226–238, 2011.
[5] X. Liu, C. Xu, Y. Noori, S. X. Ng, and L. Hanzo, "The road to near-capacity CV-QKD reconciliation: An FEC-agnostic design," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 2089–2112, 2024.
[6] P. Jouguet and S. Kunz-Jacques, "High performance error correction for quantum key distribution using polar codes," *Quantum Inf. Comput.*, vol. 14, no. 3-4, pp. 329–338, 2014, .
[7] A. Nakassis and A. Mink, "Polar codes in a QKD environment," *Proc. SPIE*, vol. 9123, pp. 32–42, 2014.
[8] S. Yan, J. Wang, J. Fang, L. Jiang, and X. Wang, "An improved polar codes-based key reconciliation for practical quantum key distribution," *Chin. J. Electron.*, vol. 27, no. 2, pp. 250–255, 2018.
[9] A. U. Rehman, L.-L. Yang, and L. Hanzo, "Delay and throughput analysis of cognitive Go-Back-N HARQ in the face of imperfect sensing," *IEEE Access*, vol. 5, pp. 7454–7473, 2017.
[10] R. Zhang and L. Hanzo, "Superposition-coding-aided multiplexed hybrid ARQ scheme for improved end-to-end transmission efficiency," *IEEE Trans. Veh. Technol.*, vol. 58, no. 8, pp. 4681–4686, Oct. 2009.

[11] R. Zhang and L. Hanzo, "Multiplexed hybrid ARQ for energy efficient transmissions under delay constraints," in *Proc. 2010 IEEE Int. Conf. Commun.*, 2010, pp. 1–5.

[12] R. Zhang and L. Hanzo, "Superposition-aided delay-constrained hybrid automatic repeat request," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 2109–2115, May 2010.

[13] H. Chen, R. G. Maunder, and L. Hanzo, "A survey and tutorial on low-complexity turbo coding techniques and a holistic hybrid ARQ design example," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 1546–1566, Fourth Quarter 2013.

[14] H. Saber and I. Marsland, "An incremental redundancy hybrid ARQ scheme via puncturing and extending of polar codes," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 3964–3973, Nov. 2015.

[15] 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.

[16] J. Martinez-Mateo, D. Elkouss, and V. Martin, "Blind reconciliation," *Quantum Info. Comput.*, vol. 12, pp. 791–812, Sep. 2012.

[17] D. Wang, X. Liu, C. Xu, S. X. Ng, and L. Hanzo, "Short-block polar-coded reverse and direct reconciliation in CV-QKD," *IEEE Open J. Veh. Technol.*, vol. 6, pp. 2195–2209, 2025.

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

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

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

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

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

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

[24] E. Rocher and R. Pickholtz, "An analysis of the effectiveness of hybrid transmission schemes," *IBM J. Res. Dev.*, vol. RD-14, no. 4, pp. 426–433, 1970.

[25] S. Lin and P. Yu, "A hybrid ARQ scheme with parity retransmission for error control of satellite channels," *IEEE Trans. Commun.*, vol. TCOM-30, no. 7, pp. 1701–1719, Jul. 1982.

[26] Q. Chen and P. Fan, "On the performance of type-III hybrid ARQ with RCPC codes," in *Proc. 14th IEEE Proc. Pers., Indoor Mobile Radio Commun.*, 2003, vol. 2, pp. 1297–1301.

[27] W. Yafeng, Z. Lei, and Y. Dacheng, "Performance analysis of type-III HARQ with turbo codes," in *Proc. 57th IEEE Semiannual Veh. Technol. Conf.*, 2003, vol. 4, pp. 2740–2744.

[28] D. Chase, "A combined coding and modulation approach for communication over dispersive channels," *IEEE Trans. Commun.*, vol. TCOM-21, no. 3, pp. 159–174, Mar. 1973.

[29] D. Mandelbaum, "An adaptive-feedback coding scheme using incremental redundancy (Corresp.)," *IEEE Trans. Inf. Theory*, vol. TIT-20, no. 3, pp. 388–389, May 1974.

[30] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[31] C. Leroux, A. J. Raymond, G. Sarkis, I. Tal, A. Vardy, and W. J. Gross, "Hardware implementation of successive-cancellation decoders for polar codes," *J. Signal Process. Syst.*, vol. 69, pp. 305–315, 2012.

[32] 3rd Generation Partnership Project (3GPP), "Performance of rate matching schemes for polar codes," TSG RAN WG1 Meeting, Prague, Czech Republic, Tech. Rep. R1-1712647, Aug. 2017.

[33] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 77, no. 4, 2008, Art. no. 042325.

[34] X. Liu, C. Xu, S. X. Ng, and L. Hanzo, "OTFS-based CV-QKD systems for doubly selective THz channels," *IEEE Trans. Commun.*, vol. 73, no. 8, pp. 6274–6289, Aug. 2025.

[35] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, "Field demonstration of a continuous-variable quantum key distribution network," *Opt. Lett.*, vol. 41, no. 15, pp. 3511–3514, 2016.

[36] B. P. Williams, B. Qi, M. Alshowkan, P. G. Evans, and N. A. Peters, "Field test of continuous-variable quantum key distribution with a true local oscillator," *Phys. Rev. Appl.*, vol. 21, no. 1, 2024, Art. no. 014056.

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

[38] D. Wu, Y. Li, and Y. Sun, "Construction and block error rate analysis of polar codes over AWGN channel based on gaussian approximation," *IEEE Commun. Lett.*, vol. 18, no. 7, pp. 1099–1102, Jul. 2014.

[39] H. Vangala, E. Viterbo, and Y. Hong, "A comparative study of polar code constructions for the AWGN channel," 2015, *arXiv:1501.02473*.

[40] R. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. TIT-27, no. 5, pp. 533–547, Sep. 1981.

[41] W. Ryan and S. Lin, *Channel Codes: Classical and Modern*. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[42] J. Ha, J. Kim, and S. W. McLaughlin, "Rate-compatible puncturing of low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 11, pp. 2824–2836, Nov. 2004.

[43] D. G. Mitchell, M. Lentmaier, A. E. Pusane, and D. J. Costello, "Randomly punctured LDPC codes," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 2, pp. 408–421, Feb. 2016.

[44] 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*, vol. 103, no. 6, 2021, Art. no. 062419.

[45] M. Navascués, F. Grosshans, and A. Acín, "Optimality of Gaussian attacks in continuous-variable quantum cryptography," *Phys. Rev. Lett.*, vol. 97, Nov. 2006, Art. no. 190502.

[46] R. Renner and J. I. Cirac, "De Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," *Phys. Rev. Lett.*, vol. 102, Mar. 2009, Art. no. 110504.

[47] S. Pirandola, S. L. Braunstein, and S. Lloyd, "Characterization of collective gaussian attacks and security of coherent-state quantum cryptography," *Phys. Rev. Lett.*, vol. 101, Nov. 2008, Art. no. 200504.

[48] F. Laudenbach et al., "Continuous-variable quantum key distribution with Gaussian modulation—The theory of practical implementations," *Adv. Quantum Technol.*, vol. 1, no. 1, 2018, Art. no. 1800011.

[49] A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," *Phys. Rev. A—At., Mol., Opt. Phys.*, vol. 81, no. 6, 2010, Art. no. 062343.

[50] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," *Phys. Rev. A—At., Mol., Opt. Phys.*, vol. 84, no. 6, 2011, Art. no. 062317.

[51] C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-variable quantum key distribution using thermal states," *Phys. Rev. A—At., Mol., Opt. Phys.*, vol. 86, no. 2, 2012, Art. no. 022318.

[52] D. Milovančev, N. Vokić, F. Laudenbach, C. Pacher, H. Hübel, and B. Schrenk, "High rate CV-QKD secured mobile WDM fronthaul for dense 5G radio networks," *J. Lightw. Technol.*, vol. 39, no. 11, pp. 3445–3457, Jun. 2021.

[53] C. Liu, C. Zhu, X. Liu, M. Nie, H. Yang, and C. Pei, "Multicarrier multiplexing continuous-variable quantum key distribution at terahertz bands under indoor environment and in inter-satellite links communication," *IEEE Photon. J.*, vol. 13, no. 4, Aug. 2021, Art. no. 7600113.

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

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

CHAO XU (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in wireless communications from the University of Southampton, Southampton, U.K., in 2009 and 2015, respectively. He is currently a Senior Lecturer with the University of Southampton. He was the recipient of the Best M.Sc. Student in Broadband and Mobile Communication Networks by the IEEE Communications Society U.K. and Republic of Ireland Chapter in 2009, 2012 Chinese Government Award for Outstanding Self-Financed Student Abroad, 2017 Dean's Award, University of Southampton, 2023 Marie Sklodowska-Curie Actions Global Postdoctoral Fellowships with the highest evaluation score of 100/100.

SOON XIN NG (Senior Member, IEEE) received the B.Eng. degree (First class) in electronic engineering and the Ph.D. degree in telecommunications from the University of Southampton, Southampton, U.K., in 1999 and 2002, respectively. He is currently a Professor of next generation communications with the University of Southampton. His research interests include adaptive coded modulation, coded modulation, channel coding, space-time coding, joint source and channel coding, iterative detection, OFDM, MIMO, cooperative communications, distributed coding, quantum communications, quantum error correction codes, joint wireless-and-optical-fibre communications, game theory, artificial intelligence, and machine learning. He has authored orcoauthored more than 300 papers and co-authored two John Wiley/IEEE Press books in this field.

LAJOS HANZO (Life Fellow, IEEE) received the Honorary Doctorates from the Technical University of Budapest, Budapest, Hungary, in 2009, and Edinburgh University, Edinburgh, U.K., in 2015. He is a Foreign Member of the Hungarian Science-Academy, Fellow of the Royal Academy of Engineering, the IET of EURASIP. He is the recipient of IEEE Eric Sumner Technical Field Award.