ARTICLE OPEN

Rate-compatible multi-edge type low-density parity-check code ensembles for continuous-variable quantum key distribution systems

Suhwang Jeong[1], Hyunwoo Jung[2] and Jeongseok Ha[2]✉

In this paper, we propose a design rule of rate-compatible punctured multi-edge type low-density parity-check (MET-LDPC) code ensembles with degree-one variable nodes for the information reconciliation (IR) of continuous-variable quantum key distribution (CV-QKD) systems. In addition to the rate compatibility, the design rule effectively resolves the high error-floor issue which has been known as a technical challenge of MET-LDPC codes at low rates. Thus, the proposed design rule allows one to implement rate-compatible MET-LDPC codes with good performances both in the threshold and low-error-rate regions. The rate compatibility and the improved error-rate performances significantly enhance the efficiency of IR for CV-QKD systems. The performance improvements are confirmed by comparing complexities and secret key rates of IR schemes with MET-LDPC codes whose ensembles are optimized with the proposed and existing design rules. In particular, the SNR range of positive secrecy rate increases by 1.44 times, and the maximum secret key rate improves by 2.10 times as compared to the existing design rules. The comparisons clearly show that an IR scheme can achieve drastic performance improvements in terms of both the complexity and secret key rate by employing rate-compatible MET-LDPC codes constructed with code ensembles optimized with the proposed design rule.

npj Quantum Information (2022)8:6 ; https://doi.org/10.1038/s41534-021-00509-9

INTRODUCTION

Quantum key distribution (QKD) systems allow two remote parties to share secret keys by utilizing quantum mechanics[1], which is known to provide unconditional security[2,3]. In QKD systems, the secret keys are established by performing the following two phases: (1) exchanging quantum states through a quantum channel and (2) post-processing through an authenticated classical channel[4]. QKD systems are usually categorized into discrete-variable QKD (DV-QKD)[1,2,4], and continuous-variable QKD (CV-QKD) systems[5–7], according to their modulation techniques adopted in the quantum state exchanges. In the DV-QKD systems, the polarization of the single-photon is modulated by the information while both the amplitude and phase quadrature of coherent state are modulated in the CV-QKD systems. Recently, there have been extensive studies on practical CV-QKD system developments[8–10] since CV-QKD systems can be readily deployed in the existing optical communication infrastructure[11] and also overcome limitations of applicability of DV-QKD systems, e.g., the requirement of a sophisticated single-photon detector[12].

To achieve a higher key rate and longer operation range, it is important to increase the efficiency of information reconciliation (IR). In particular, CV-QKD systems operate in the very low signal-to-noise ratio (SNR) region where error-correcting codes (ECCs) for the IR must be designed at extremely low rates. It is technically challenging to design strong ECCs tailored for such a low SNR region, and there have been extensive efforts[13–15] to improve the efficiency of IR by designing stronger ECCs of low rates. For instance, Raptor codes are designed at low rates for the IR in refs.[14–17] where Raptor codes have capacity-approaching performances. In addition, the rateless feature of Raptor codes enables the IR to maintain high efficiencies across a range of SNRs. However, Raptor codes require a high decoding complexity as compared to other types of ECCs, e.g., multi-edge-type low-density parity-check (MET-LDPC) codes, due to high check node degrees, which leads to excessively long decoding latency.

Meanwhile, MET-LDPC codes at low rates, e.g., 1/50, are employed in the IR for CV-QKD systems due to their good error-correcting performances and more amenable decoding complexity[18–20]. In ref. [18], the authors demonstrated high-speed error correction for MET-LDPC codes utilizing a graphic processing unit (GPU). In ref. [19], it was shown that a quasi-cyclic code construction of MET-LDPC codes is suitable for hardware-accelerated decoding. In the studies[18–20], MET-LDPC codes are implemented based on degree distributions simply taken from an open literature[13], and the authors focus on the demonstrations of practical decoder implementation for MET-LDPC codes. In this work, we are instead interested in designing strong MET-LDPC codes.

There have been studies on MET-LDPC code design[13,21,22] which pay their attention only to the optimization of the threshold performance. Thus, the designed MET-LDPC codes suffer from high error floors which limit the efficiency of the IR[18,19]. In particular, the error floors are mainly due to an anomaly called the decoder errors, i.e., decoding into wrong codewords, which requires QKD systems to employ additional error-detection codes such as cyclic redundancy check (CRC) codes to confirm whether the decoded codeword is the transmitted one. In the case that a decoder-error event happens, the QKD system may discard the shared randomness obtained via the first phase, i.e., exchanging quantum state over the quantum channel. It is also possible that the QKD system performs additional communications through a classical public channel to resolve the problem, which however leads to extra information leakage and eventually degrades the secret key rate in the key distillation. In addition, the CRC codes increase the hardware complexity. Thus, it is highly desirable to

[1]Samsung Electronics, Suwon, Korea. [2]School of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST), Daejeon 305–701, Korea.
✉email: jsha@kaist.edu

design MET-LDPC codes without suffering from the error-rate performance loss due to the high error floors caused by the decoder errors.

It was shown[23] that small-weight codewords of MET-LDPC codes mainly induce the decoder errors, and thus the design of MET-LDPC code ensembles must be carried out to avoid small-weight codewords. Then, MET-LDPC codes without error floors can be implemented with ensembles that have diminishing average numbers of small-weight codewords with the growing code length. It is known that if an MET-LDPC code ensemble satisfy a certain condition so called, the *t*-value condition, it has exponentially few codewords of small weight[24]. Recently, the *t*-value condition is further extended[23] to MET-LDPC code ensembles with degree-one variable nodes which are essential for code ensembles of low rates to have good threshold performances[25].

The efficiency of IR depends on the code rate of ECC, namely the amount parity bits, which is determined by the quality of the quantum channel. It is often observed that the quality of the quantum channel varies in time due to various factors such as the number of photons affected by the attacker, noise variations, the thermally induced length fluctuations, the timing jitter, etc. Thus, to maximize the IR efficiency, the code rate must be adapted to the variation of quantum channel quality, which can be realized with multiple encoder and decoder pairs of different rates. While the scheme with multiple encoder/decoder pairs seems conceptually straightforward, it is not a pragmatic solution due to the growing complexity as the number of pairs increases. In addition, when the decoding is not successful, the transmitted codeword must be discarded, and a new codeword of a lower rate will be requested, which leads to a loss of IR efficiency.

In this work, we instead consider an IR scheme with a rate-adaptive punctured ECCs which are derived by puncturing the parity bits of a code, called mother code. The puncturing provides a sequence of codes whose rates increase from that of the mother code depending on the number of punctured parity bits. In addition, the puncturing is carried out in the rate-compatible fashion[26] where a code of higher rate is embedded in codes of lower rates. That is, punctured bits in a code of a rate must also be punctured in codes of higher rates than the rate. The beauty of rate-compatible punctured ECCs is that only one encoder/decoder pair is needed for the entire range of rates given the puncturing locations are a priori known to the receiver, which conveniently resolves the complexity issue in the scheme using multiple encoder/decoder pairs. More importantly, when the decoding fails, the scheme with rate-compatible punctured ECCs simply transmits some punctured parity bits which will be combined with the already received codeword resulting in a new codeword of a lower rate. The transmission of punctured parity bits can be repeated until the receiver successfully decodes the transmitted codeword. Thus, the scheme with rate-compatible punctured ECCs is an efficient solution to maximize the IR efficiency at reduced complexity. Recently, an IR scheme with punctured MET-LDPC codes was studied in ref. [20] where MET-LDPC codes are randomly punctured to adapt their rates. However, the recent work[20] takes degree distributions of MET-LDPC codes from ref. [13] which will be shown to have poor error-floor performances. In addition, the random puncturing in ref. [20] results in such poor error-floor performances at all the rates derived from the mother code.

In this work, by utilizing the recent result[23] for designing MET-LDPC codes with both good threshold and error-floor performances, this work proposes an IR scheme using optimized rate-compatible punctured MET-LDPC codes. Since we consider the rate-compatible puncturing to realize the rate adaptability in this work, we simply call rate-adaptive punctured MET-LDPC codes as rate-compatible MET-LDPC codes. The improvements of MET-LDPC codes in the threshold and error-floor regions allow the IR scheme to achieve higher key rates and/or longer distances of CV-QKD systems. The improved error-floor performances enable one to design CV-QKD systems without resorting to certain error-detection codes, which not only improves the efficiency of CV-QKD systems but also reduces the complexity of an IR scheme. In particular, we propose a design of MET-LDPC code ensembles with degree-one variable nodes which have exponentially few small-weight codewords. The designed ensembles allow one to implement MET-LDPC codes with better performances in both the threshold and error-floor regions at a reduced decoding complexity as compared to the ensembles based on the existing design rules[18,19,25]. In addition, we will show how to design rate-compatible MET-LDPC codes while holding the *t*-value condition over a range of code rates that the rate-compatible MET-LDPC codes support. The rate-compatible MET-LDPC codes can be utilized for implementing efficient IR schemes for CV-QKD systems. The details of CV-QKD system and the IR scheme considered in this work will be introduced in “Methods”. We will conduct performance comparisons among IR schemes with rate-compatible MET-LDPC codes and a fixed-rate MET-LDPC code. For implementing the MET-LDPC codes, their code ensembles are optimized with the proposed design rule and existing design rules. The performance comparisons clearly show that significant performance improvements are achievable by employing the rate-compatible MET-LDPC codes using ensembles with the proposed design rule.

RESULTS

The *t*-value condition for MET-LDPC codes

In this work, we consider a Tanner graph of MET-LDPC code ensemble with degree-one variable nodes shown in Fig. 1 where the entire set of variable node classes, denoted by $\mathcal{V}$, is partitioned into the subsets, $\mathcal{V}_1$, $\mathcal{V}_2$, and $\mathcal{V}_{12}^c$, and $\mathcal{V}_{12}^c$ is the complement of the set $\mathcal{V}_{12} = \mathcal{V}_1 \cup \mathcal{V}_2$. Note that the variable node class $\mathcal{V}_1$ consists of two sub-classes denoted by $\mathcal{V}_{1,p}$ and $\mathcal{V}_{1,np}$ which represent punctured and unpunctured variable nodes of degree-one, respectively. Similarly, the check node class $\mathcal{C}_1$ consists of two sub-classes denoted by $\mathcal{C}_{1,p}$ and $\mathcal{C}_{1,np}$ which represent check nodes connected to the punctured and unpunctured variable nodes of degree-one, respectively. In this section, it is assumed that the all variable nodes of degree-one are unpunctured, and later in “Results”, we modify the result in ref. [23] to include the MET-LDPC codes with punctured variable nodes of degree-one.

In a similar manner, the entire sets of check node classes and edge types in Fig. 1, denoted by $\mathcal{C}$ and $\mathcal{E}$, respectively, are partitioned into $\mathcal{C}_1$ and $\mathcal{C}_1^c$, and $\mathcal{E}_1$, $\mathcal{E}_2$, and $\mathcal{E}_{12}^c$, respectively, where $\mathcal{E}_{12}^c$ is the complement of $\mathcal{E}_{12} = \mathcal{E}_1 \cup \mathcal{E}_2$, and $\mathcal{C}_1^c = \mathcal{C} \setminus \mathcal{C}_1$. The blocks denoted by ET in Fig. 1 are uniform interleavers each of which permutes edges of a type. In particular, $\mathcal{V}_1$ is the set all variable node classes of degree-one, i.e., $\sum_j d_{i,j} = 1$ for $i \in \mathcal{V}_1$, and $\mathcal{E}_1 = \{j | d_{i,j} = 1, \ \forall\ i \in \mathcal{V}_1\}$. Note that $\mathcal{E}_1$ is the set of edge types corresponding to the variable nodes classes in $\mathcal{V}_1$. Meanwhile, $\mathcal{C}_1$ is the set of all check node classes which have check nodes incident with edges of types in $\mathcal{E}_1$, i.e., for every $i \in \mathcal{C}_1$, $\exists\ j \in \mathcal{E}_1$ such that $g_{i,j} = 1$. Note that the threshold of MET-LDPC code ensemble will not be defined if a check node is incident with more than one edge of a type in $\mathcal{E}_1$. Thus, each check node of a class in $\mathcal{C}_1$ has a single edge of a type in $\mathcal{E}_1$. Then, $\mathcal{E}_2$ is the set of all edge types for the edges incident to the check node of classes in $\mathcal{C}_1$ except for the ones of types in $\mathcal{E}_1$, i.e., for every $j \in \mathcal{E}_2$, $\exists\ i \in \mathcal{C}_1$ such that $g_{i,j} > 0$. The set $\mathcal{V}_2$ contains all variable node classes which have variable nodes incident with edges of types in $\mathcal{E}_2$, i.e., for every $i \in \mathcal{V}_2$, $\exists\ j \in \mathcal{E}_2$ such that $d_{i,j} > 0$. It is assumed that for each edge type of $j \in \mathcal{E}_{12}^c$, there exists a check node of class $i \in \mathcal{C}_1^c$ such that $g_{i,j} \geq 2$, which is also considered in ref. [24].

An MET-LDPC code ensemble can also be described with a pair of multinomials, and the pair of multinomials for the MET-LDPC

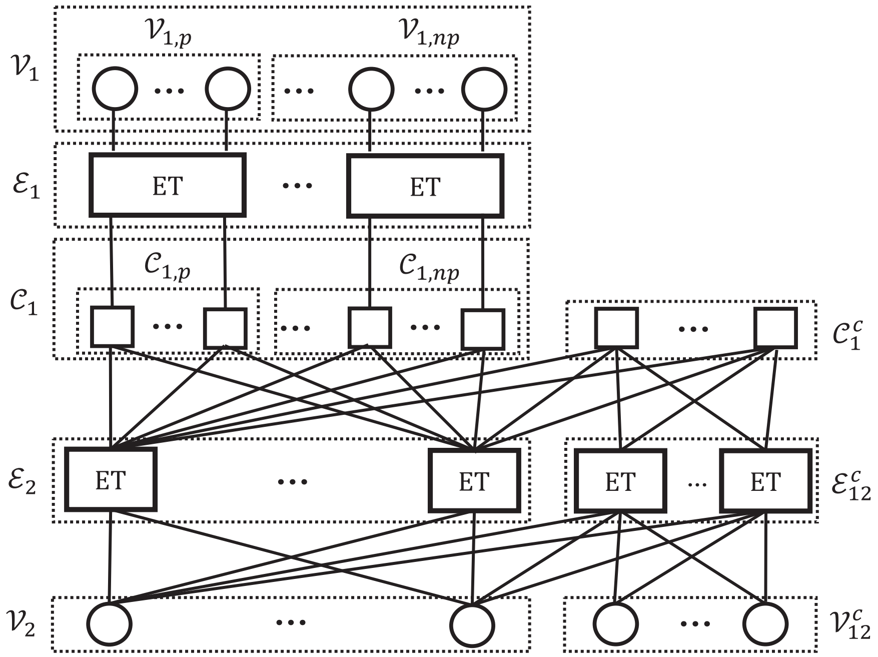


Fig. 1 Tanner graph of MET-LDPC code ensemble with degree-one variable nodes. The block denoted by ET are uniform interleaver each of which permutes edges of a type.

code ensemble in Fig. 1 are given by

$$\begin{aligned} v(\mathbf{x}) = & \sum_{\substack{i\in\mathcal{V}_1\\ d_{i,j}=1}} v_i r x_j^1 + \sum_{i\in\mathcal{V}_2} v_i r \prod_{j\in\mathcal{E}_2} x_j^{d_{i,j}} \prod_{j\in\mathcal{E}_{12}^c} x_j^{d_{i,j}} \\ & + \sum_{i\in\mathcal{V}_{12}^c} v_i r \prod_{j\in\mathcal{E}_{12}^c} x_j^{d_{i,j}}, \\ \mu(\mathbf{x}) = & \sum_{\substack{i\in\mathcal{C}_1\\ g_{i,j}=1}} \mu_i x_j^1 \prod_{k\in\mathcal{E}_2} x_k^{g_{i,k}} + \sum_{i\in\mathcal{C}_1^c} \mu_i \prod_{j\in\mathcal{E}_1^c} x_j^{g_{i,j}}, \end{aligned} \tag{1}$$

where the variable node classes in $\mathcal{V}_1$, $\mathcal{V}_2$, and $\mathcal{V}_{12}^c$ correspond to the first, second and third terms in $v(\mathbf{x})$, respectively, and the check nodes classes in $\mathcal{C}_1$ and $\mathcal{C}_1^c$ are represented by the first and second terms in $\mu(\mathbf{x})$, respectively. The code rate of MET-LDPC code ensemble[27] is given by

$$R = 1 - \frac{\sum_{i\in\mathcal{C}} \mu_i}{\sum_{i\in\mathcal{V}} v_i}. \tag{2}$$

For an MET-LDPC code ensemble, the average number of codewords of weight ℓ is expressed by the asymptotic exponential growth rate defined in Definition 1.

Definition 1 (the asymptotic exponential growth rate)

$$\gamma(w) = \lim_{n\to\infty} \frac{1}{n} \log A(\lfloor nw \rfloor), \tag{3}$$

where A (ℓ) is the average number of codewords of weight ℓ, and w is the normalized weight.

Meanwhile, for small-weight codewords, i.e., $w \ll 1$, Theorem 1 tells the asymptotic exponential growth rate, i.e., $\gamma(w)$ in Definition 1.

Theorem 1 Ref. [22]. *For $t \neq 0$, we have*

$$\gamma(w) = \sup_{t\in\mathfrak{T}} -\log(t) w + O(w^2), \tag{4}$$

where $\mathfrak{T}$ is the set of all t values such that

$$\det(I - t\Lambda'(t)P') = 0 \tag{5}$$

where $\tilde{u} = (\tilde{u}_1, \tilde{u}_2, \ldots, \tilde{u}_{|\mathcal{E}_{12}^c|})$ (resp. $\tilde{s} = (\tilde{s}_1, \tilde{s}_2, \ldots, \tilde{s}_{|\mathcal{E}_{12}^c|})$) is a vector whose elements, $\tilde{u}_i$'s (resp. $\tilde{s}_i$'s) are given by $u_{f(j_i)}$'s (resp. $s_{f(j_i)}$'s) for $1 \leq i \leq |\mathcal{E}_{12}^c|$ and a bijective mapping $f: \mathcal{E}_{12}^c \to \{1, 2, \ldots, |\mathcal{E}_{12}^c|\}$, and $\Lambda'(t)$ is a square matrix whose elements are given by

$$\Lambda'_{f(j),f(k)}(t) = \frac{\left.\frac{\partial^2 v(\mathbf{x})}{\partial x_j \partial x_k}\right|_{\mathbf{x}=\tilde{\mathbf{0}}}}{\mu_{x_j}(\mathbf{1})}, \tag{6}$$

P' is a square matrix whose elements are given by

$$P'_{f(j),f(k)} = \frac{\left.\frac{\partial^2 \mu(\mathbf{x})}{\partial x_j \partial x_k}\right|_{\mathbf{x}=\mathbf{1}}}{\mu_{x_j}(\mathbf{1})}, \tag{7}$$

$\tilde{\mathbf{0}} = (o_1, o_2, \ldots, o_{n_e})$ is a vector of length n_e, $o_m = t\frac{\sum_{i\in\mathcal{C}_1} \mu_i g_{i,m}}{\mu_{x_m}(\mathbf{1})}$ for $m \in \mathcal{E}_2$ and zeros for the other elements.

It is shown in Theorem 1 that an MET-LDPC code ensemble with degree-one variable nodes has exponentially few codewords of small weights when the infimum of the solution set for the equation in Eq. (5) is larger than one, which is the t-value condition and summarized in Definition 2.

Definition 2 (t-value condition) *For an MET-LDPC code ensemble, the infimum of $\mathfrak{T}$ is larger than unity. The infimum of $\mathfrak{T}$ will be called the t-value of the ensemble.*

Rate-compatible MET-LDPC codes for CV-QKD systems

We will show that it is possible to design rate-compatible MET-LDPC codes with good error-rate performances in both the threshold and error-floor regions, which is carried out by proving that there exists a sequence of punctured MET-LDPC code ensembles of rates with exponentially few codewords of small weights. To this end, we utilize the design rule in ref. [23] to optimize an MET-LDPC code ensemble with degree-one variable nodes for the threshold performance with the constraint of the t-value condition. It was shown in ref. [23] that MET-LDPC codes based on the ensemble have good error-rate performances both in the threshold and error-floor regions. The designed MET-LDPC code ensemble is called the mother code ensemble from which MET-LDPC code ensembles of higher rates are derived by puncturing parity bits of the mother code ensemble. Then, it will be shown that the punctured MET-LDPC code ensembles derived from the mother code ensemble also satisfy the t-value condition regardless of the number of punctured parity bits if the mother code ensemble has a certain structure. In the next section, we will show that rate-compatible MET-LDPC codes with good error-floor performances can be implemented using the punctured MET-LDPC code ensembles.

In the design of punctured MET-LDPC code ensembles, we puncture only degree-one variable nodes due to a few practical reasons. The Tanner graph in Fig. 1 shows that each degree-one variable node is incident to a different check node whose neighboring variable nodes are all unpunctured except for the degree-one variable node. Thus, the punctured degree-one variable nodes are one-step-recoverable (1-SR)[28], i.e., recoverable in the first iteration of the belief-propagation (BP) decoding. It was demonstrated in ref. [28] that punctured LDPC codes have good threshold performances when only 1-SR variable nodes are punctured. In addition, the generation of coded bits for the punctured variable nodes can be performed with a linear complexity, which reduces the complexity of progressive parity bit generation and transmission.

For an MET-LDPC code ensemble with the degree distribution pair in Eq. (1), the degree distribution of the punctured MET-LDPC code ensemble becomes

$$\begin{aligned} v'(\mathbf{x}) =& \sum_{\substack{i\in\mathcal{V}_{1,p}\\ d_{i,j}=1}} v_i r_0 x_j^1 + \sum_{\substack{i\in\mathcal{V}_{1,np}\\ d_{i,j}=1}} v_i r_1 x_j^1 \\ &+\sum_{i\in\mathcal{V}_2} v_i r_1 \prod_{j\in\mathcal{E}_2} x_j^{d_{i,j}} \prod_{j\in\mathcal{E}_{12}^c} x_j^{d_{i,j}} + \sum_{i\in\mathcal{V}_{12}^c} v_i r_1 \prod_{j\in\mathcal{E}_{12}^c} x_j^{d_{i,j}}, \\ \mu'(\mathbf{x}) =& \sum_{\substack{i\in\mathcal{C}_{1,p}\\ g_{i,j}=1}} \mu_i x_j^1 \prod_{k\in\mathcal{E}_2} x_k^{g_{i,k}} + \sum_{\substack{i\in\mathcal{C}_{1,np}\\ g_{i,j}=1}} \mu_i x_j^1 \prod_{k\in\mathcal{E}_2} x_k^{g_{i,k}} + \sum_{i\in\mathcal{C}_1^c} \mu_i \prod_{j\in\mathcal{E}_1^c} x_j^{g_{i,j}}, \end{aligned} \tag{8}$$

where $\mathcal{V}_1=\mathcal{V}_{1,p}\cup\mathcal{V}_{1,np}$, $\mathcal{V}_{1,p}$, and $\mathcal{V}_{1,np}$ indicate the sets of punctured and unpunctured degree-one variable node classes, respectively, and r_0 and r_1 represent the channels for the punctured the unpunctured variable nodes, respectively. The code rate of the punctured MET-LDPC code ensemble becomes

$$\begin{aligned} R_\pi &= 1-\frac{\sum_{i\in\mathcal{C}/\mathcal{C}_{1,p}}\mu_i}{\sum_{i\in\mathcal{V}/V_{1,p}}v_i} = 1-\frac{\sum_{i\in\mathcal{V}}\mu_i-\pi\sum_{i\in\mathcal{V}}v_i}{\sum_{i\in\mathcal{V}}v_i(1-\pi)} \\ &= \frac{\sum_{i\in\mathcal{V}}v_i(1-\pi)-\sum_{i\in\mathcal{C}}\mu_i+\pi\sum_{i\in\mathcal{V}}v_i}{\sum_{i\in\mathcal{V}}v_i(1-\pi)} \\ &= \frac{R}{1-\pi}, \end{aligned} \tag{9}$$

where π is the fraction of punctured degree-one variable nodes.

It should be noted that in the belief-propagation (BP) decoding, the punctured degree-one variable nodes in $\mathcal{V}_{1,p}$ output their messages of zero log-likelihood ratio (LLR) value regardless of decoding iterations. In addition, for the check nodes incident to punctured variable nodes, the messages to unpunctured neighboring variable nodes are bounded by the LLR value of zero. Thus, the punctured degree-one variable nodes and their incident check nodes do not participate in the BP decoding, which allows us to exclude the punctured nodes from the ensemble. That is, the MET-LDPC code ensemble with punctured degree-one variable nodes can be expressed with an equivalent degree distribution pair that has only unpunctured variable nodes. Then, the equivalent MET-LDPC code ensemble is given by

$$\begin{aligned} v'(\mathbf{x}) =& \sum_{\substack{i\in\mathcal{V}_{1,np}\\ d_{i,j}=1}} v_i r_1 x_j^1 + \sum_{i\in\mathcal{V}_2} v_i r_1 \prod_{j\in\mathcal{E}_2} x_j^{d'_{i,j}} \prod_{j\in\mathcal{E}_{12}^c} x_j^{d_{i,j}} \\ &+ \sum_{i\in\mathcal{V}_{12}^c} v_i r_1 \prod_{j\in\mathcal{E}_{12}^c} x_j^{d_{i,j}}, \\ \mu'(\mathbf{x}) =& \sum_{\substack{i\in\mathcal{C}_{1,np}\\ g_{i,j}=1}} \mu_i x_j^1 \prod_{k\in\mathcal{E}_2} x_k^{g_{i,k}} + \sum_{i\in\mathcal{C}_1^c} \mu_i \prod_{j\in\mathcal{E}_1^c} x_j^{g_{i,j}}, \end{aligned} \tag{10}$$

where $d'_{i,j}$ is the degree of the variable node class $i\in\mathcal{V}_2$ for $j\in\mathcal{E}_2$. Note that the removal of punctured variable nodes deletes some edges in $\mathcal{E}_2$ and check nodes of $\mathcal{C}_1$, which makes the degree $d'_{i,j}$ less than or equal to $d_{i,j}$. i.e., $d'_{i,j}\le d_{i,j}$. The degree $d'_{i,j}$ is decided in such a way that the numbers of edges in $\mathcal{E}_2$ from variable nodes and check nodes are the same after removing the punctured variable nodes and their incident check nodes, which is so called the socket count equality[23].

For the equivalent code ensemble in Eq. (10), we have to test the t-value condition[23] to confirm that the punctured MET-LDPC code ensemble has exponentially few codewords of small weight. It is also especially important to know the maximum proportion of punctured bits below which the t-value condition of the mother MET-LDPC code ensemble holds. In Theorem 2, we will prove that the t-value condition of a mother code ensemble holds regardless of the proportion of punctured bits when the mother code ensemble has a certain structure. While the theorem is limited to MET-LDPC codes with the structure, it will be shown that some good mother MET-LDPC code ensembles can be readily designed even if the structural limit is imposed.

Theorem 2 *For the MET-LDPC code ensemble of three edge types of $\mathcal{E}_1=\{1\}$, $\mathcal{E}_2=\{2\}$, and $\mathcal{E}_{12}^c=\{3\}$ with $g_{i,2}=0$ for all $i\in\mathcal{C}_1^c$, the following arguments are true:*

1. *If a mother code ensemble satisfies the t-value condition, punctured MET-LDPC code ensembles also satisfy the t-value condition regardless of the amount of punctured bits.*
2. *If a mother code ensemble does not satisfy the t-value condition, none of punctured MET-LDPC code ensembles satisfies the t-value condition.*

Proof For an MET-LDPC code ensemble of three edge types of $\mathcal{E}_1=\{1\}$, $\mathcal{E}_2=\{2\}$, and $\mathcal{E}_{12}^c=\{3\}$ with $g_{i,2}=0$ for all $i\in C_1^c$, the ensemble in Eq. (1) can be rewritten as

$$\begin{aligned} v(\mathbf{x}) &= \sum_{\substack{i\in\mathcal{V}_1\\ d_{i,1}=1}} v_i r x_1^1 + \sum_{i\in\mathcal{V}_2} v_i r x_2^{d_{i,2}} x_3^{d_{i,3}} + \sum_{i\in\mathcal{V}_{12}^c} v_i r x_3^{d_{i,3}}, \\ \mu(\mathbf{x}) &= \sum_{\substack{i\in\mathcal{C}_1\\ g_{i,1}=1}} \mu_i x_1^1 x_2^{g_{i,2}} + \sum_{i\in\mathcal{C}_1^c} \mu_i x_3^{g_{i,3}}. \end{aligned} \tag{11}$$

For the ensemble in Eq. (11), the equality in Eq. (5) can be expressed as

$$\begin{aligned} &\frac{2}{\mu_{x_3}(\mathbf{1})}\cdot\left\{\sum_{\substack{i\in\mathcal{V}_2\\ d_{i,3}=2}} v_i t^{d_{i,2}+1} + \sum_{\substack{i\in\mathcal{V}_{12}^c\\ d_{i,3}=2}} v_i t\right\} \\ &\quad\times\frac{\sum_{i\in\mathcal{C}_1^c}\mu_i g_{i,3}(g_{i,3}-1)}{\mu_{x_3}(\mathbf{1})} = 1. \end{aligned} \tag{12}$$

Suppose that there exists a solution $t\le1$ satisfying the equality in EQ. (12), which implies

$$\left\{\sum_{\substack{i\in\mathcal{V}_2\\ d_{i,3}=2}} v_i + \sum_{\substack{i\in\mathcal{V}_{12}^c\\ d_{i,3}=2}} v_i\right\}\times\frac{2\sum_{i\in\mathcal{C}_1^c}\mu_i g_{i,3}(g_{i,3}-1)}{\mu_{x_3}(\mathbf{1})^2}\ge1, \tag{13}$$

where the lefthand side in Eq. (13) is obtained by replacing t in Eq. (12) with unity and is larger than or equal to the lefthand side in Eq. (12). Thus, when the inequality in Eq. (13) does not hold, the solutions of the equality in Eq. (12) must be larger than unity, i.e., $\inf\mathfrak{T}>1$. That is, the t-value condition, i.e., $\inf\mathfrak{T}>1$, can be equivalently expressed as

$$\left\{\sum_{\substack{i\in\mathcal{V}_2\\ d_{i,3}=2}} v_i + \sum_{\substack{i\in\mathcal{V}_{12}^c\\ d_{i,3}=2}} v_i\right\}\times\frac{2\sum_{i\in\mathcal{C}_1^c}\mu_i g_{i,3}(g_{i,3}-1)}{\mu_{x_3}(\mathbf{1})^2}<1. \tag{14}$$

If degree-one variable nodes in the ensemble of Eq. (11) are punctured with a fraction of π, the punctured ensemble can be represented as

$$\begin{aligned} \nu'(\mathbf{x}) &= \sum_{\substack{i\in\mathcal{V}_{1,np}\\ d_{i,1}=1}} \nu_i r x_1^1 + \sum_{i\in\mathcal{V}_2} \nu_i r x_2^{d'_{i,2}} x_3^{d_{i,3}} + \sum_{i\in\mathcal{V}_{12}^c} \nu_i r x_3^{d_{i,3}}, \\ \mu'(\mathbf{x}) &= \sum_{\substack{i\in\mathcal{C}_{1,np}\\ g_{i,1}=1}} \mu_i x_1^1 x_2^{g_{i,2}} + \sum_{i\in\mathcal{C}_1^c} \mu_i x_3^{g_{i,3}}. \end{aligned} \tag{15}$$

For the degree distribution pair in Eq. (15), the equality in Eq. (5) can be expressed as exactly the same as the one in Eq. (12) except that $d_{i,2}$ is changed to $d'_{i,2}$, which however does not affect the inequality in Eq. (14). Thus, if the t-value condition holds for the mother code, so does for all punctured code ensembles.□

For arbitrary MET-LDPC code ensembles shown in Fig. 1, it is mathematically intractable to express in a closed-form the maximum proportion of punctured parity bits below which the t-value condition holds. However, it is sufficient to numerically test whether the punctured MET-LDPC code ensemble of the highest rate satisfy the t-value condition since the ones of lower rates have additional parity bits, which does not induce smaller weight codewords.

Performance evaluations

In this section, we compare error-rate performances and efficiencies of IR schemes that have rate-compatible MET-LDPC codes and fixed-rate MET-LDPC codes implemented using code ensembles with/without satisfying the t-value condition. Refer to “Methods” for the CV-QKD system in which the IR schemes are employed. We consider the multidimensional reconciliation with a dimension of 8. It is known in ref. [29] that the channel can safely be assumed to be a binary-input additive-white-Gaussian-noise (BI-AWGN) channel. For decoding MET-LDPC codes, we employ the sum-product algorithm in which the maximum number of iteration is set to 1000. The iterative decoding terminates when all the parity checks are satisfied even before the iteration reaches the preset maximum number of iterations. The error-rate performances are measured in terms of both bit-error rate (BER) and word-error rate (WER) which are evaluated at each SNR value by transmitting codewords until a hundred failed codewords are observed. In addition, the practicality of the MET-LDPC codes is compared in terms of three different metrics, i.e., the maximum variable node degree $d_{\max}$, the maximum check node degree $g_{\max}$, and a normalized edge density in ref. [30] which is defined as the average number of edges per message bit, i.e., $|\mathcal{E}|/(R\cdot n)$ where $|\mathcal{E}|$, R, and n are the total number of edges, code rate and code length, respectively. The maximum degrees are often used as a measure of decoding latency[31] while the normalized edge density is adopted to measure the decoding complexity in ref. [30].

First, we design a mother MET-LDPC code ensemble by optimizing the ensemble for the threshold performance[22] with the constraint of the t-value condition[23]. The MET-LDPC code ensemble is optimized at a code rate of 0.02 for the BI-AWGN channel, and is denoted by $\mathcal{C}_1$ in Table 1. For comparisons, we take a code ensemble in ref. [19], and denote it by $\mathcal{C}_2$ in Table 1. Note that $\mathcal{C}_1$ has its t-value of $1.0078 > 1$ and thus satisfies the t-value condition. Whereas $\mathcal{C}_2$ has its t-value of $0.9743 < 1$ and does not meet the t-value condition. The t-value condition tells when the number of small-weight codewords diminishes, which is obtained by a balance of degree-one and degree-two of edge types at nodes. In the design of $\mathcal{C}_2$, the code optimization is carried out only for a good threshold performance, which more weighs the degree-one nodes and thus results in poor error-floor performances. Based on the degree distributions of $\mathcal{C}_1$ and $\mathcal{C}_2$, two MET-LDPC codes of length 10^6 are implemented with random parity-check matrices, and they are denoted by $\mathbb{C}_1$ and $\mathbb{C}_2$, respectively. In this work, MET-LDPC codes are denoted by bold symbols, e.g., $\mathbb{C}_1$ and $\mathbb{C}_2$, while their ensembles are represented by script symbols, e.g., $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Their BER and WER performances on the BI-AWGN channel are compared in Fig. 2 where it is witnessed that $\mathbb{C}_2$ has a high error-floor. The high error-floor associated with $\mathcal{C}_2$ is mainly due to the decoder errors, i.e., decoding into wrong codewords, caused by small-weight codewords as predicted by the test of the t-value condition. To substantiate the claim, we depict the decoder-error rate (DER) in Fig. 2 where the DER and WER overlap each other in the error-floor region. It should also be noted that the WER and BER of $\mathbb{C}_2$ have a wide gap, which is due to the fact that the decoder-error events are caused by small-weight codewords[23]. On the contrary, for the competing code, i.e., $\mathbb{C}_1$, we do not observe any decoder-error event until its WER and BER reach 10^{-4} and 10^{-5}, respectively, and thus no error-floor appears in Fig. 2.

Now, based on the two mother code ensembles, i.e., $\mathcal{C}_1$ and $\mathcal{C}_2$ in Table 1, we design rate-compatible MET-LDPC code ensembles which have their code rates between 0.02 and 0.025, equivalently, $\pi\in[0, 0.2]$. The equivalent degree distributions for the rate-compatible MET-LDPC codes at the highest code rate, i.e., 0.025, are described in Table 1, where the ones based on the code ensembles $\mathcal{C}_1$ and $\mathcal{C}_2$ are denoted by $\mathcal{C}_1^\pi$ and $\mathcal{C}_2^\pi$, respectively. Note that both the ensembles $\mathcal{C}_1$ and $\mathcal{C}_2$ are not designed for puncturing. It is possible to investigate into a design rule which also takes the puncturing into account, while it is beyond the scope of this work. Since the puncturing is carried out in the rate-compatible fashion[26], it enables one to progressively transmit additional parity bits when a decoding failure happens or an error-detection code finds out a decoder-error event. Note that the rate-compatible MET-LDPC code using $\mathcal{C}_1$, i.e., $\mathcal{C}_1^\pi$ in Table 1, also satisfies the t-value condition which is tested with the equivalent degree distribution pair in the $\mathcal{C}_1^\pi$ row of Table 1. It should be noted that the ensemble of the mother code, $\mathcal{C}_1$, has the structure discussed in Theorem 2, and thus the t-value condition is always satisfied regardless of the amount of punctured parity bits. Meanwhile, it is shown in Table 1, the code ensemble using $\mathcal{C}_2$ does not satisfy the t-value condition. It is also noticed in Table 1 that the thresholds of $\mathcal{C}_1$ and $\mathcal{C}_1^\pi$ are better than those of $\mathcal{C}_2$ and $\mathcal{C}_2^\pi$ while both $\mathcal{C}_1$ and $\mathcal{C}_1^\pi$ have lower complexities in terms of all the complexity measures, i.e., edge density, maximum variable node, and check node degrees. Thus, the rate-compatible MET-LDPC codes constructed with ensembles using the proposed design rule not only outperform the rate-compatible MET-LDPC codes using the existing design rule but also have practical advantages.

By puncturing the MET-LDPC codes, i.e., $\mathbb{C}_1$ and $\mathbb{C}_2$ in Fig. 2, two rate-compatible MET-LDPC codes of rate 0.025 (equivalently, $\pi = 0.2$) are implemented and evaluated in terms of BER and WER on the BI-AWGN channel in Fig. 3 where the rate-compatible MET-LDPC codes are denoted by $\mathbb{C}_1^\pi$ and $\mathbb{C}_2^\pi$. Note that while the rate-compatible MET-LDPC codes $\mathbb{C}_1^\pi$ and $\mathbb{C}_2^\pi$ are obtained by puncturing their mother codes $\mathbb{C}_1$ and $\mathbb{C}_2$, the asymptotic behaviors of $\mathbb{C}_1^\pi$ and $\mathbb{C}_2^\pi$, e.g., thresholds and t-value conditions, are given by the degree distributions in the $\mathcal{C}_1^\pi$ and $\mathcal{C}_2^\pi$ rows of Table 1, respectively. As predicted by Theorem 2, the rate-compatible MET-LDPC code, $\mathbb{C}_2^\pi$ suffers from the error floors as its mother code, i.e., $\mathbb{C}_2$ in Fig. 2, does. Whereas the error-floor does not appear in the error rates of $\mathbb{C}_1^\pi$ as predicted by the test of the t-value condition for the equivalent degree distribution pair. The comparison of error-rate performances in Fig. 3 confirms the results in “Results”.

The key rate of CV-QKD systems is often[9,19] assumed as

$$K = (1 - \mathrm{WER})(\beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}}). \tag{16}$$

However, a recent work[16] shows that the key rate formula in Eq. (16) does not reconcile with the results of quantum information theory in some situations. In particular, the issue can happen when the error rates of ECCs are relatively high, which is frequently encountered in long-distance CV-QKD systems. Thus, instead of the key rate in Eq. (16), as suggested in ref. [16], we use a

Table 1. Code parameters; the thresholds are measured in terms of SNR in dB.

Codes	n	Rate	Threshold in dB	inf $\mathfrak{I}$	$\frac{\lvert\mathcal{E}\rvert}{Rn}$	$d_{\max}$	$g_{\max}$	$\nu(x)$	$\mu(x)$
$\mathcal{C}_1$	10^6	0.02	− 15.248	1.0078	147.0	39	3	$0.8968x_1^1 + 0.0600x_2^4x_3^2 + 0.0432x_2^{36}x_3^3$	$0.8968x_1x_2^2 + 0.0832x_3^3$
$\mathcal{C}_2$ [19]	10^6	0.02	− 15.199	0.9743	166.9	60	7	$0.9600x_1^1 + 0.0225x_2^{57}x_3^2 + 0.0175x_2^{57}x_3^3$	$0.600x_1x_2^2 + 0.3600x_1x_2^3 + 0.0106x_3^7 + 0.0094x_3^3$
$\mathcal{C}_1^\pi$		0.025	− 14.254	1.0095	117.0	31	3	$0.8711x_1^1 + 0.0669x_2^3x_3^2 + 0.0081x_2^4x_3^2 + 0.0015x_2^{27}x_3^3 + 0.0524x_2^{28}x_3^3$	$0.8711x_1x_2^2 + 0.1039x_3^3$
$\mathcal{C}_2^\pi$		0.025	− 14.198	0.9678	133.1	60	7	$0.9500x_1^1 + 0.0246x_2^{45}x_3^2 + 0.0035x_2^{46}x_3^2 + 0.0192x_2^{45}x_3^3 + 0.0027x_2^{57}x_3^3$	$0.5937x_1x_2^2 + 0.3562x_1x_2^3 + 0.0133x_3^7 + 0.0117x_3^3$

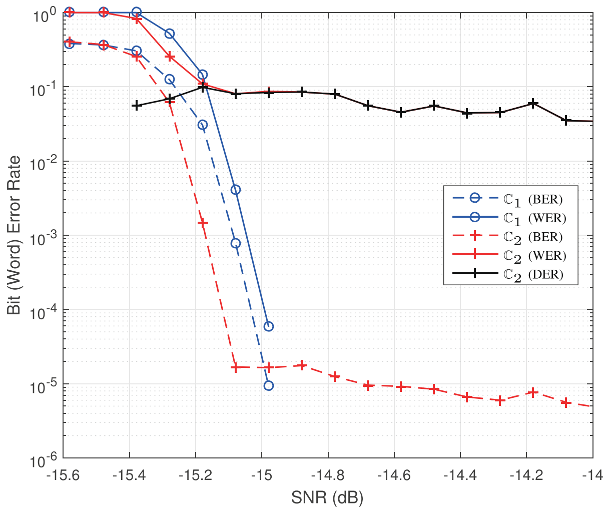


Fig. 2 BER and WER comparison between existing MET-LDPC code and optimized MET-LDPC code. Based on the degree distributions of $\mathcal{C}_1$ and $\mathcal{C}_2$, two MET-LDPC codes of length 10^6 are implemented with random parity-check matrices, and they are denoted by $\mathbb{C}_1$ and $\mathbb{C}_2$, respectively.

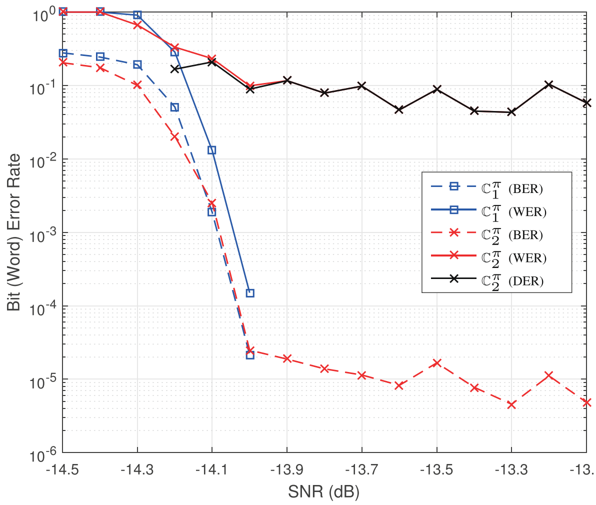


Fig. 3 BER and WER comparison between the punctured code of existing MET-LDPC code and optimized MET-LDPC code. By puncturing the MET-LDPC codes, i.e., $\mathbb{C}_1$ and $\mathbb{C}_2$ in Fig. 2, two rate-compatible MET-LDPC codes of rate 0.025 (equivalently, $\pi = 0.2$) are implemented and evaluated in terms of BER and WER on the BI-AWGN channel. The rate-compatible MET-LDPC codes based on $\mathbb{C}_1$ and $\mathbb{C}_2$ are denoted by $\mathbb{C}_1^\pi$ and $\mathbb{C}_2^\pi$, respectively.

bound on the key rate which is given by

$$K = (1 - \mathrm{WER})(\beta I_{\mathrm{AB}}) - \chi_{\mathrm{BE}}, \tag{17}$$

where β is the IR efficiency defined as R_π / I_{AB}, R_π is the code rate, π is the maximum fraction of punctured bits when the IR succeeds, I_{AB} is the mutual information of the virtual Gaussian channel, and χ_{BE} is the Holevo bound on the information leaked to the eavesdropper, Eve[11]. The secret key rate depends on various physical parameters such as the length and standard loss of fiber and homodyne detector efficiency, etc. In this work, we take the physical parameters from ref. [19] where the noise in the quantum channel denoted by χ_{tot} modeled as the sum of noises from the fiber and detector denoted by χ_{line} and χ_{det}, respectively. Then, the

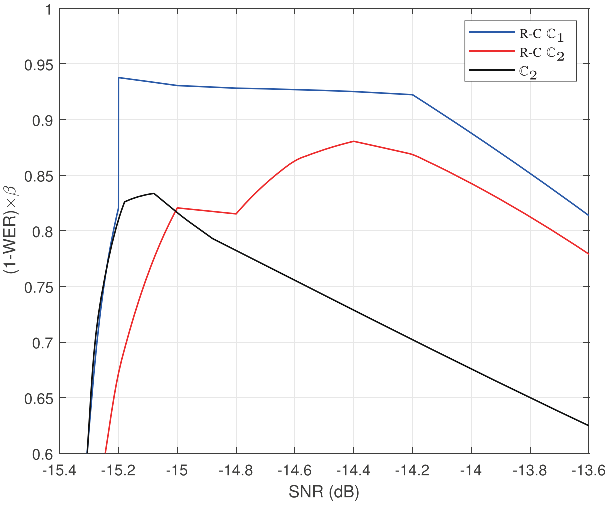


Fig. 4 Comparisons of effective efficiency. We compare the effective efficiencies, i.e., $(1-\text{WER})\times\beta$ of the IR schemes with three different error-correcting codes denoted by R-C $\mathbb{C}_1$, R-C $\mathbb{C}_2$, and $\mathbb{C}_2$ in which R-C $\mathbb{C}_1$ and R-C $\mathbb{C}_2$ indicate the IR schemes with the rate-compatible MET-LDPC codes using $\mathbb{C}_1$ and $\mathbb{C}_2$, respectively. Meanwhile, the IR scheme with the fixed-rate MET-LDPC code of $\mathbb{C}_2$ is denoted by $\mathbb{C}_2$.

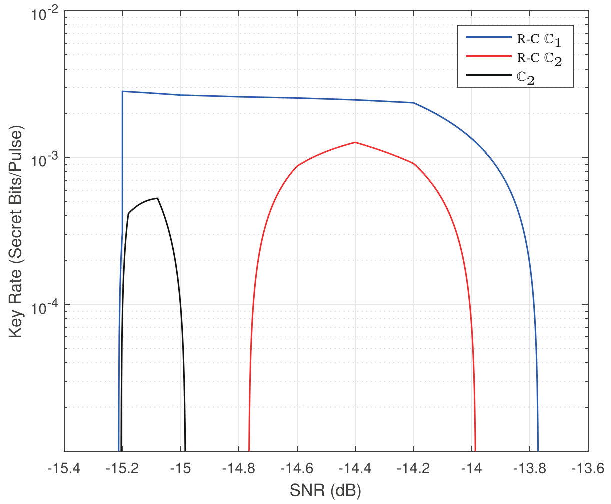
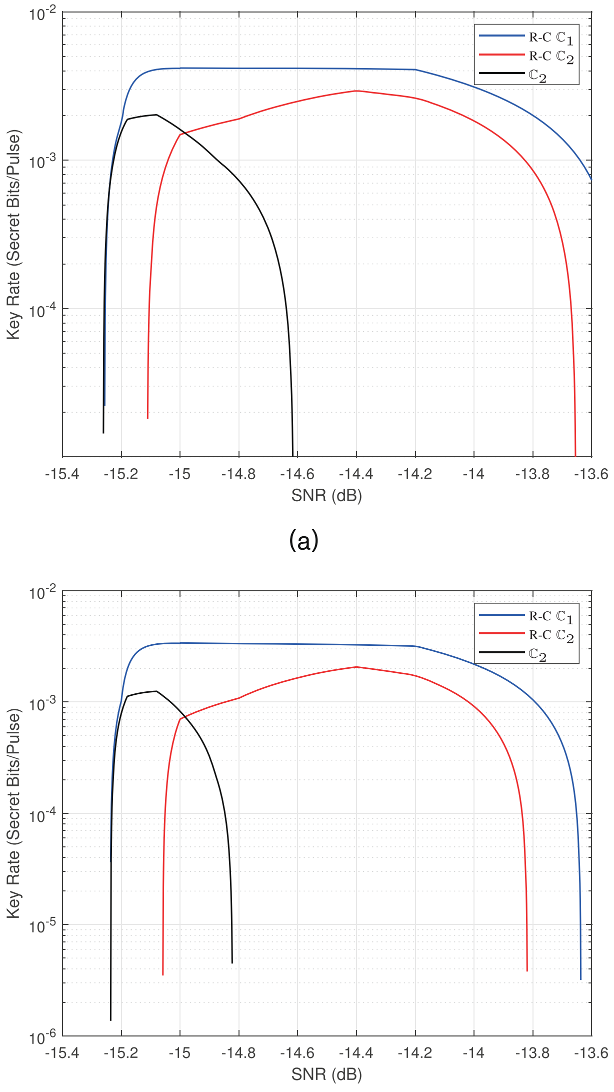


Fig. 5 Comparisons of key rates. The key rate is evaluated in terms of bits per pulse for the three IR schemes denoted by R-C $\mathbb{C}_1$, R-C $\mathbb{C}_2$, and $\mathbb{C}_2$ when the length of fiber is assumed to be $\ell = 90$ Km.



(a)

(b)

Fig. 6 Comparisons of key rates. a The key rate is evaluated in terms of bits per pulse for the three IR schemes denoted by R-C $\mathbb{C}_1$, R-C $\mathbb{C}_2$, and $\mathbb{C}_2$ when the length of fiber is assumed to be $\ell = 80$ Km. **b** The key rate is evaluated when the length of fiber is assumed to be $\ell = 85$ Km.

noise due to fiber of length ℓ with a transmittance $T = 10^{\alpha\ell/10}$ is given by $\chi_{\text{line}} = 1/T - 1 + \varepsilon$ where $\alpha = 0.2\text{dB/Km}$ is the standard loss of a single-mode fiber, and the excess channel noise (measured in shot noise units) is $\varepsilon = 0.01$ for 0 Km $\leq \ell \leq$100 Km, and $\varepsilon = 0.01 + 0.001 \times (\ell - 100)$ for 100 Km $\leq \ell \leq$170 Km. Meanwhile, the noise in the homodyne detector is given by $\chi_{\text{det}} = (1 + V_{\text{el}})/\eta - 1$ where η and V_{el} represent the homodyne detector efficiency and additive electronic noise, respectively, and it is assumed that $\eta = 0.606$ and $V_{\text{el}} = 0.041$. Then, the total noise in the quantum channel follows as $\chi_{\text{tot}} = \chi_{\text{line}} + \chi_{\text{det}}/T$. In addition, the SNR of the virtual Gaussian channel is expressed as $V_A/(1 + \chi_{\text{tot}})$ where V_A is a modulation variance of Alice and has to be optimized to achieve the highest key rate[13].

We define $(1 - \text{WER}) \times \beta$ in Eq. (17) as an effective efficiency which depends on both the WER and the efficiency of ECC, i.e., the maximum code rate at which the IR is successfully performed. We consider IR schemes with rate-compatible MET-LDPC codes by puncturing $\mathbb{C}_1$ and $\mathbb{C}_2$ in Fig. 2 as their mother codes. In addition, an IR scheme with the MET-LDPC code at a fixed rate of 0.02 denoted by $\mathbb{C}_2$ in Fig. 2. The effective efficiencies of three schemes are compared in Fig. 4 where R-C $\mathbb{C}_1$ and R-C $\mathbb{C}_2$ indicate the IR schemes with the rate-compatible MET-LDPC codes using $\mathbb{C}_1$ and $\mathbb{C}_2$, respectively. Meanwhile, the IR scheme with the fixed-rate MET-LDPC code of $\mathbb{C}_2$ is denoted by $\mathbb{C}_2$ in Fig. 4. The performance comparison in Fig. 4 is carried out over a range of SNR values over which the maximum effective efficiencies of three schemes are observed. In practice, the SNR values are adjusted by controlling the modulation variance, V_A at a given length of fiber, ℓ. In Fig. 4, the efficiencies of the three schemes are depicted with the curves in blue, red, and black, respectively. In the IR scheme with $\mathbb{C}_2$, the shared randomness obtained via the quantum channel will be discarded when the decoding for ECC fails. Meanwhile, the IR schemes with R-C $\mathbb{C}_1$ and R-C $\mathbb{C}_2$ transmit

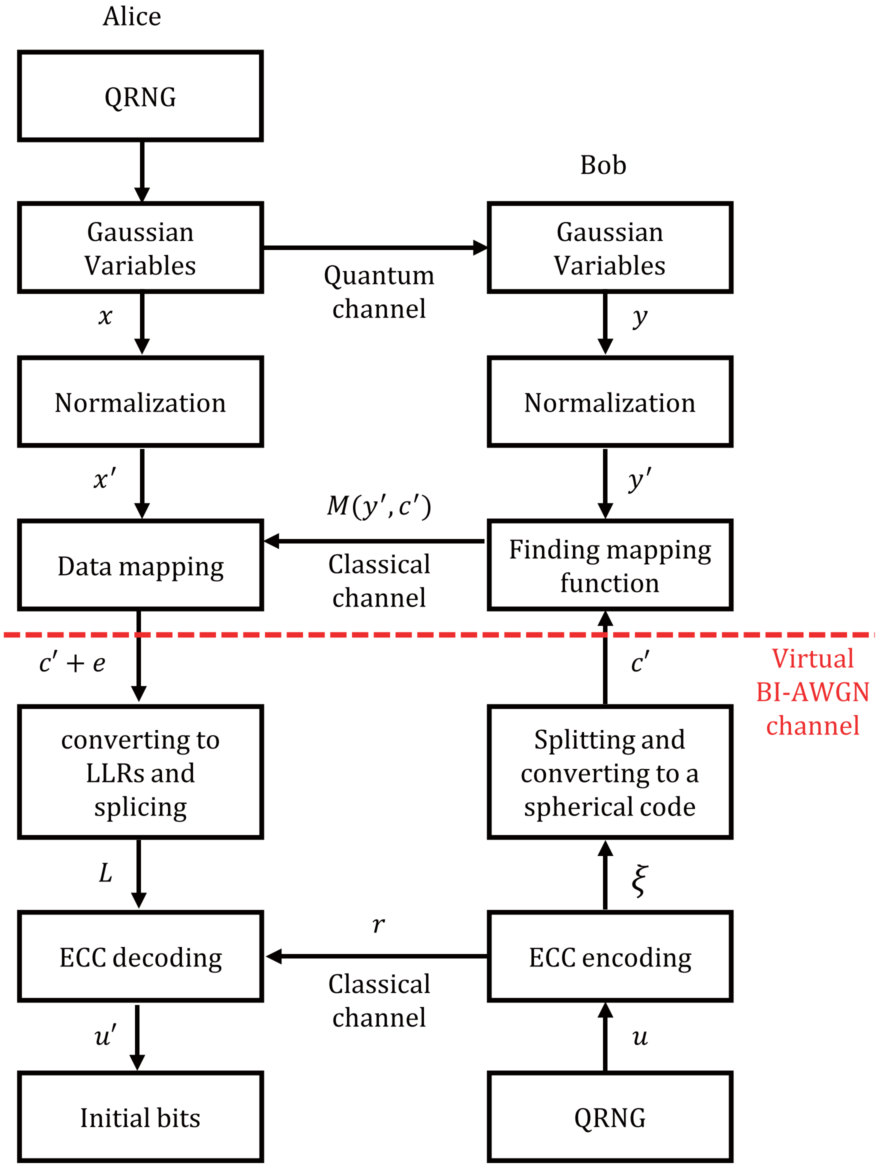


Fig. 7 Block diagram of reverse-reconciliation CV-QKD systems. The quantum channel is modeled as a virtual BI-AWGN channel, and a rate-compatible MET-LDPC code is assumed as the ECC whose rate is set to the maximum value or the capacity of the virtual BI-AWGN channel by puncturing parity bits.

additional parities when Alice requests on the decoding failure, which results in significant improvements of efficiency. However, the scheme with R-C $\mathbb{C}_2$ suffers from decoder-error events, which requires additional parity bits for the CRC code. In the case that the decoding for CRC code detects a decoder-error event, i.e., $u' \neq u$, the scheme discards the shared randomness obtained via the communication over the quantum channel. On the contrary, the scheme with R-C $\mathbb{C}_1$ has no decoder-error event as the consequences of Theorem 2 promise. The comparisons in Fig. 4 quantitively demonstrate the performance improvements obtained by employing the rate-compatible MET-LDPC codes based on the ensemble satisfying the *t*-value condition. That is, the scheme with R-C $\mathbb{C}_1$ has a clear performance advantage over a wide range of SNR values as compared to the other two schemes, i.e., R-C $\mathbb{C}_2$ and $\mathbb{C}_2$.

It should be mentioned that the comparison between the schemes with $\mathbb{C}_2$ and R-C $\mathbb{C}_2$ has a crossover at the SNR of -15dB. In the region of SNR less than -15dB, the variation of efficiency, β is relatively small while the WER of $\mathbb{C}_2$ drastically improves with the growing SNR value since the threshold of error rate for $\mathbb{C}_2$ starts at around -15.3dB as shown in Fig. 2. Meanwhile, the improvement of WER for R-C $\mathbb{C}_2$ is limited since the retransmissions of parity bits lead to decoder-error events. This is why the scheme with $\mathbb{C}_2$ has better effective efficiency in the region of SNR less than -15dB. Note that efficiency is defined as the ratio of code rate and channel capacity. Thus, the efficiency β of the scheme with $\mathbb{C}_2$ sharply decreases as the SNR value further increases passing the crossover point, i.e., -15dB, considering that the capacity grows while the rate is fixed. On the contrary, it is not serious for the scheme with R-C $\mathbb{C}_2$ due to the rate adaptability, i.e., the code rate adapts to the channel quality. It is noticed in Fig. 4 that the scheme with R-C $\mathbb{C}_2$ outperforms the one with $\mathbb{C}_2$. As compared to the two schemes with $\mathbb{C}_2$ and R-C $\mathbb{C}_2$, the scheme with $\mathbb{C}_1$ does not suffer from the decoder-error events while taking the advantage of rate adaptability, which provides the performance superiority over the range of SNR values over the competing IR schemes, i.e., the ones with $\mathbb{C}_2$ and R-C $\mathbb{C}_2$.

The key rate in Eq. (17) is evaluated in terms of bits per pulse for the three IR schemes in Fig. 5 where the length of fiber is assumed to be $\ell = 90$ Km. It is clearly witnessed that the IR scheme with R-C $\mathbb{C}_1$ outperforms the other two schemes over a wider range of SNR values. In addition, Fig. 6 shows that the IR scheme with R-C $\mathbb{C}_1$ consistently performs better than the other schemes at different lengths of fiber of $\ell = 80$ Km and 85 Km. In practice, the modulation variance V_A is determined to make the CV-QKD system operate at a certain SNR value of the virtual Gaussian channel. The adjustment of V_A requires a precise channel estimation of the quantum channel, which is hard to achieve in practice. Thus, the SNR value has some variations, and the IR scheme must be designed robust to the SNR variation. In this sense, the IR scheme with R-C $\mathbb{C}_1$ has clear advantages of both performance and practicality.

DISCUSSION

In this paper, we proposed a design rule of multi-edge type low-density parity-check code ensembles with degree-one variable nodes. It was shown that the design rule allows one to implement rate-compatible MET-LDPC codes with good performances both in the threshold and low-error-rate regions. It is also demonstrated that the rate-compatible MET-LDPC codes can improve the efficiency of information reconciliation for CV-QKD systems.

METHODS

Information reconciliation of QKD system

In this work, we consider the IR scheme for CV-QKD systems introduced in ref. [15] where the scheme employs rate-compatible error-correcting codes, i.e., rate-compatible MET-LDPC codes in this work. The IR scheme is depicted in Fig. 7 where Alice transmits Gaussian random variables $x_i \sim \mathcal{N}(0, \sigma_A^2)$ for $i = 1, 2, \ldots, d$ over the quantum channel, and for each Gaussian random variable x_i, Bob receives a noisy observation $y_i = x_i + n_i$ from the quantum channel where $n_i \sim \mathcal{N}(0, \sigma_n^2)$ and σ_n^2 indicates the noise power. Then, Alice and Bob have the correlated random vectors $x = (x_1, x_2, \ldots, x_d)$ and $y = (y_1, y_2, \ldots, y_d)$, respectively, which are normalized to $x' = x/||x||$ and $y' = y/||y||$ where $||x||$ and $||y||$ are the Euclidean norms of the vectors x and y, respectively, and d is called the dimension of multidimensional reconciliation[29].

In the reverse reconciliation[32], Bob generates a uniformly random binary sequence u from the quantum random number generator (QRNG), and encodes the sequence u into a codeword ξ, i.e., a codeword of MET-LDPC code in this work. Then, Bob divides ξ into sub-groups of coded bits of length d. Suppose that one of the sub-groups is denoted by $c = (c_1, c_2, \ldots c_d)$ which is converted to a spherical codes c' as follows:

$$(c_1, c_2, \ldots, c_d) \rightarrow c' = \left(\frac{(-1)^{c_1}}{\sqrt{d}}, \frac{(-1)^{c_2}}{\sqrt{d}}, \ldots, \frac{(-1)^{c_d}}{\sqrt{d}} \right). \tag{18}$$

Note that c' is uniformly distributed on the unit sphere in the d dimensional Euclidean vector space. For a pair of vectors, c' and y', Bob calculates the linear mapping $M(y', c')$ in ref. [29] such that

$$M(y', c') \cdot y' = c'. \tag{19}$$

The mapping $M(y', c')$ is transmitted to Alice over the classical channel. When Alice receives the mapping $M(y', c')$, she performs $M(y', c') \cdot x' = c' + e$ where e follows a Gaussian distribution with zero mean[29]. According to ref. [29], as the dimension denoted by d grows, the d consecutive instances of the physical Gaussian channel, i.e., the quantum channel, are reformulated to d copies of a virtual BI-AWGN channel[29]. Since this work focuses on the benefit of rate-compatible MET-LDPC codes, it is assumed for simplicity that the dimension is fixed to $d = 8$ at which the quantum channel can be modeled as a BI-AWGN channel as shown in Fig. 7. Since the gain in key rate is mainly due to the proposed coding scheme, the gain is also achievable with different dimensions. The transmission of sub-group c is repeated until the entire codeword ξ is transmitted. Then, in practical systems, the received signal $c' + e$ is often represented as a log-likelihood ratio (LLR) vector denoted by L in Fig. 7, and the LLR vector L is fed to the ECC decoder as its input.

In this work, a rate-compatible MET-LDPC code is assumed as the ECC in Fig. 7, and the rate of ECC is set to the maximum value or the capacity of the virtual BI-AWGN channel by puncturing parity bits. If the decoding at the Alice side fails, she requests for additional parity bits. Upon the request, Bob transmits additional parity bits by sending a sequence of mappings corresponding to the punctured parity bits to be transmitted. The request and transmission will be continued until Alice successfully obtains her estimate of the message u'. In some cases, the estimate u' is different from the true message u, which can be detected by employing an additional error-detection code such as a CRC code. In Fig. 7, the parity bits for CRC code is denoted by r. Note that the transmission of parity bits for the CRC code degrades performance of the IR scheme, which can be avoided by carefully designing the ECC. More details of the IR of CV-QKD can be found in refs. [15,19].

DATA AVAILABILITY

The authors can confirm that the data supporting the findings of this study are available within the article.

CODE AVAILABILITY

The code that supports the findings of this study is available on reasonable request from the author.

Received: 22 April 2021; Accepted: 9 November 2021;
Published online: 21 January 2022

REFERENCES

1. Bennett, C. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems and Signal Processing* 175–179 (1984).
2. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
3. Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. *npj Quantum Inf.* **2**, 1–12 (2016).
4. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
5. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
6. Braunstein, S. L. & Van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **77**, 513 (2005).
7. Weedbrook, C. et al. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621 (2012).
8. Zhang, G. et al. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nat. Photonics* **13**, 839–842 (2019).
9. Zhang, Y. et al. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys. Rev. Lett.* **125**, 010502 (2020).
10. Zhang, Y. et al. Continuous-variable QKD over 50 km commercial fiber. *Quantum Science and Technology* **4**, 035006 (2019).
11. Lodewyck, J. et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **76**, 042305 (2007).
12. Gyöngyösi, L., Bacsardi, L. & Imre, S. A survey on quantum key distribution. *Infocom. J.* **11**, 14–21 (2019).
13. Jouguet, P., Kunz-Jacques, S. & Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **84**, 062317 (2011).
14. Shirvanimoghaddam, M., Johnson, S. J. & Lance, A. M. Design of Raptor codes in the low SNR regime with applications in quantum key distribution. in *2016 IEEE International Conference on Communications (ICC)* 1–6 (IEEE, 2016).
15. Zhou, C. et al. Continuous-variable quantum key distribution with rateless reconciliation protocol. *Phys. Rev. Applied* **12**, 054013 (2019).
16. Johnson, S. J. et al. On the problem of non-zero word error rates for fixed-rate error correction codes in continuous variable quantum key distribution. *New J. Phys.* **19**, 023003 (2017).
17. Asfaw, M. B., Jiang, X.-Q., Zhang, M., Hou, J. & Duan, W. Performance analysis of Raptor code for reconciliation in continuous variable quantum key distribution. in *International Conference on Computing, Networking and Communications* 463–467 (2019).

18. Wang, X., Zhang, Y., Yu, S. & Guo, H. High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code. *Sci. Rep.* **8**, 1–7 (2018).
19. Milicevic, M., Feng, C., Zhang, L. M. & Gulak, P. G. Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography. *npj Quantum Inf.* **4**, 1–9 (2018).
20. Wang, X. et al. Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution. *Quantum Inf. Comput.* **17**, 1123–1134 (2017).
21. Jayasooriya, S., Shirvanimoghaddam, M., Ong, L., Lechner, G. & Johnson, S. J. A new density evolution approximation for LDPC and multi-edge type LDPC codes. *IEEE Trans. Commun.* **64**, 4044–4056 (2016).
22. Jeong, S. & Ha, J. On the design of multi-edge type low-density parity-check codes. *IEEE Trans. Commun.* **67**, 6652–6667 (2019).
23. Jeong, S. & Ha, J. MET-LDPC code ensembles of low code rates with exponentially few small weight codewords. *IEEE Trans. Commun.* **69**, 3517–3527 (2021).
24. Kasai, K., Awano, T., Declercq, D., Poulliat, C. & Sakaniwa, K. Weight distributions of multi-edge type LDPC codes. *IEICE Trans. Fundamentals Electronics, Commun. Computer Sci.* **93**, 1942–1948 (2010).
25. Andriyanova, I. & Tillich, J. P. Designing a good low-rate sparse-graph code. *IEEE Trans. Commun.* **60**, 3181–3190 (2012).
26. Wicker, S. B. *Error Control Systems for Digital Communication and Storage*, Vol. 1 (Prentice hall Englewood Cliffs, 1995).
27. Richardson, T. et al. Multi-edge type LDPC codes. in *Workshop Honoring Prof. Bob McEliece on His 60th Birthday, California Institute of Technology, Pasadena, California* 24–25 (2002).
28. Ha, J., Kim, J., Klinc, D. & McLaughlin, S. W. Rate-compatible punctured low-density parity-check codes with short block lengths. *IEEE Trans. Inf. Theory* **52**, 728–738 (2006).
29. Leverrier, A., Alléaume, R., Boutros, J., Zémor, G. & Grangier, P. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A* **77**, 042325 (2008).
30. Smith, B., Ardakani, M., Yu, W. & Kschischang, F. R. Design of irregular LDPC codes with optimized performance-complexity tradeoff. *IEEE Trans. Commun.* **58**, 489–499 (2010).
31. Bhatt, T., Sundaramurthy, V., Stolpman, V. & McCain, D. Pipelined block-serial decoder architecture for structured LDPC codes. *Proc. IEEE Int. Conference on Acoustics Speech Signal Processing Proceed.* **4**, IV–IV (2006).
32. Grosshans, F. & Grangier, P. Reverse reconciliation protocols for quantum cryptography with continuous variables. Preprint at https://arxiv.org/abs/quant-ph/0204127 (2002).

ACKNOWLEDGEMENTS

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2021-2018-0-01402) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation) and was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No. 2018-0-00831, A Study on Physical Layer Security for Heterogeneous Wireless Network). This was also supported by BK21 FOUR program.

AUTHOR CONTRIBUTIONS

S.J. and H.J. developed the theoretical framework with which he designed rate-compatible MET-LDPC codes for CV-QKD systems. Meanwhile, J.H. supervised this work and also contributed to writing the manuscript. All authors discussed the results and contributed to the writing of the manuscript.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Correspondence and requests for materials should be addressed to Jeongseok Ha.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.