Martinez-Mateo and Elkouss *EPJ Quantum Technology* (2025) 12:71
https://doi.org/10.1140/epjqt/s40507-025-00376-9

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Efficient reconciliation of continuous variable quantum key distribution with multiplicatively repeated non-binary LDPC codes

Jesus Martinez-Mateo[1] and David Elkouss[2*]

*Correspondence:
david.elkouss@oist.jp
[2]Networked Quantum Devices Unit, Okinawa Institute of Science and Technology Graduate University, Onna, Japan
Full list of author information is available at the end of the article

Abstract

Continuous variable quantum key distribution bears the promise of simple quantum key distribution directly compatible with commercial off the shelf equipment. However, for a long time its performance was hindered by the absence of good classical postprocessing capable of distilling secret-keys in the noisy regime. Advanced coding solutions in the past years have partially addressed this problem enabling record transmission distances of up to 165 km, and 206 km over ultra-low loss fiber. In this paper, we show that a very simple coding solution with a single code is sufficient to extract keys at all noise levels. This solution has performance competitive with prior results for all levels of noise, and we show that non-zero keys can be distilled up to a record distance of 192 km assuming the standard loss of a single-mode optical fiber, and 240 km over ultra-low loss fibers. Low-rate codes are constructed using multiplicatively repeated non-binary low-density parity-check codes over a finite field of characteristic two. This construction only makes use of a $(2, k)$-regular non-binary low-density parity-check code as mother code, such that code design is in fact not required, thus trivializing the code construction procedure. The construction is also inherently rate-adaptive thereby allowing to easily create codes of any rate. Rate-adaptive codes are of special interest for the efficient reconciliation of errors over time or arbitrary varying channels, as is the case with quantum key distribution. In short, these codes are highly efficient when reconciling errors over a very noisy communication channel, and perform well even for short block-length codes. Finally, the proposed solution is known to be easily amenable to hardware implementations, thus addressing also the requirements for practical reconciliation in continuous variable quantum key distribution.

Keywords: Continuous variable quantum key distribution; Quantum Key Distribution; Information reconciliation; Low-rate coding; Non-binary low-density parity-check codes

1 Introduction

Quantum key distribution (QKD) [1] allows two distant parties, typically named Alice and Bob, communicating through a quantum channel to exchange an information-

theoretically secure key. As usual in quantum communications, quantum states carrying information are encoded into photons and transmitted via fiber optics between the parties. However, due to imperfections when preparing and measuring the transmitted quantum states, and also due to noise in the quantum channel, there may be disparities (errors) in the exchanged raw keys—that must be assumed to be caused by any hypothetical eavesdropper. In consequence, once the raw key exchange or key generation process is concluded, a key distillation process has to be performed to convert their correlated but noisy raw keys into a shared, error free, secret key. Then, some information from the raw keys needs first to be disclosed during an information reconciliation (error correction) procedure [2], carried out over a public noiseless and authenticated channel, to produce a common string, that is, an identical key on both sides. Subsequently, some information needs to be removed in a privacy amplification procedure [3] to produce a shorter, but secret, key. Therefore, to maximize the secret key rate and to achieve greater distances between the parties, highly efficient information reconciliation methods are necessary in every experimental realization of QKD.

Discrete-variable (DV) QKD makes use of discrete modulation of quantum states, and generates correlated discrete variables at Alice's and Bob's sides. In a typical DV-QKD protocol, such as the well-known BB84 proposed by Bennett and Brassard in 1984 [4], each quantum state encodes a single bit, so that the exchanged raw keys are correlated bit strings. In such a context, standard binary linear codes, that have been demonstrated to be highly efficient, can be used for reconciling errors in the exchanged keys. Several examples of efficient information reconciliation methods have been proposed using, for instance, low-density parity-check codes [5–8] and polar codes [9]. Other reconciliation methods, such as Cascade and its modified versions [10, 11], have also been demonstrated to be highly efficient despite not using conventional decoding techniques.

In continuous-variable (CV) QKD the situation is significantly different. CV-QKD makes use of continuous modulation of quantum states, and generates correlated Gaussian variables at Alice's and Bob's sides. Contrary to what happens in DV-QKD, these devices typically operate in the regime of low signal-to-noise ratio (SNR), that is, the information is transmitted over a very noisy communication channel. Moreover, the reconciliation efficiency of correlated Gaussian variables is decisive when determining the achievable secret key rate, thus limiting the maximum attainable distance between the parties. Unfortunately, correcting errors with low-rate codes is relatively complicated, since the efficiency of common decoding techniques drops in the low SNR regime and also the decoding complexity is significantly increased. For CV-QKD with Gaussian modulation several approaches have been explored to improve the reconciliation efficiency of correlated Gaussian variables. Originally, a slice reconciliation scheme was proposed in [12]. This scheme divides a continuous function into slices that are reconciled independently using codes of different rates, being thus compatible with existing standard binary low-density parity-check and polar codes. Later, another approach called multidimensional reconciliation was proposed in [13], with the idea of reducing the problem of reconciling correlated Gaussian variables to the well-known channel coding problem over the additive white Gaussian noise (AWGN) channel. In this approach, the physical Gaussian channel is transformed into a channel close to the binary-input AWGN channel. Numerous alternatives have been proposed for information reconciliation in CV-QKD, most of them based on low-density parity-check codes (considering both schemes, slice and multidi-

mensional reconciliation). Multi-edge type low-density parity-check codes are probably the most widely used method for reconciling errors in the low SNR regime [14–19], sometimes also considering rate-adaptive techniques for highly efficient decoding [20–22], or quasi-cyclic codes for layered and fast decoding [23]. Additionally, it can also be found proposals that use other codes, such as repeat-accumulate codes [24], raptor codes [25, 26], or polar codes [9, 27] among others.

Traditional DV-QKD and CV-QKD protocols were severely limited in distance because the transmittance of the quantum channel decreases exponentially with distance. However, recent advances, both theoretical and experimental, have made it possible to extend this distance to a few hundred kilometers. A recent discrete-variable proposal called twin-field QKD (TF-QKD) allows one to extend this distance by changing the fundamental scaling of the rate [28] with state-of-the-art demonstrations reaching up to approximately one thousand kilometers [29–31].

In this contribution, we discuss a family of low-rate codes that efficiently correct errors on the binary-input AWGN channel, even at low and ultra low SNR regime. These codes are constructed from $(2, k)$-regular non-binary low-density parity-check codes, and their construction is quite simple since no code design is required. These low-rate codes are of particular interest for CV-QKD given that their decoding is highly efficient and their construction is also inherently rate-adaptive, that is, they remain efficient even when the channel varies or the channel noise is different. Furthermore, the proposed codes and their decoding are suitable for hardware implementations as demonstrated in [32].

The remainder of this paper is organized as follows. In Sect. 2 we review the background of binary and non-binary low-density parity-check codes and their interest for correcting or reconciling errors in QKD. Then, we describe the proposed low-rate code construction and the corresponding efficient decoding algorithm. We validate the construction with comprehensive numerical simulations in Sect. 3. Finally, we present our conclusions in Sect. 4.

2 Background

2.1 Information reconciliation with non-binary low-density parity-check codes

Low-density parity-check (LDPC) codes were introduced by Gallager in the early 1960s [33], but remained largely unexplored until the late 90s, when MacKay and Neal revisited these codes and explored their potential [34, 35]. It soon turned out that their performance over binary input memoryless channels was very close to channel capacity [36], that is, they have good thresholds. Furthermore, the sparsity of LDPC matrices allows high performance and low complexity decoding using iterative message-passing algorithms based on belief propagation (such as the sum-product algorithm). Other decoding algorithms and techniques (for instance, normalized and offset min-sum algorithms, or serial and parallel schedule) also exhibit a good trade-off between performance and complexity, making them suitable for hardware implementations. Consequently, LDPC codes were regarded as one of the most promising coding techniques.

Non-binary LDPC codes were also considered by Gallager in his seminal work [33]. Davey and MacKay later found that these codes can outperform binary LDPC codes [37]. However, this improvement was achieved at the expense of increased decoding complexity. Several low-complexity algorithms were then proposed [32, 38, 39] for decoding non-binary LDPC codes over finite (Galois) fields of order q, in the following denoted by GF(q),

where q is a power of prime $q = p^m$, $q > 2$ with p prime and positive integer $m \geq 1$. Thereafter, these codes have attracted much attention thanks to their good performance.

As linear codes, binary and non-binary LDPC codes can be represented by a Tanner or bipartite graph, that is, a graphical depiction of a parity-check matrix H. Nodes in a Tanner graph are divided between symbol (or variable) nodes and check (or constraint) nodes. Each check node corresponds to a parity-check constraint (that is, an implicit equation of a linear code, a row in H), and thus it is connected by edges to those variables (symbols nodes) involved in the equation. This representation is useful for both decoding and code construction. On the construction of these codes, it is well known that good binary LDPC codes are designed allowing symbols to participate in different checks in an irregular fashion [40]. Therefore, each symbol node connects to a number of check nodes, and we refer to this as symbol node degree. Such codes are referred to as irregular LDPC codes, and good code ensembles are designed by optimizing symbol and check node degree distributions on Tanner graphs [36, 41]. However, while irregular Tanner graphs help improve the performance of binary LDPC codes, this is not the case for non-binary LDPC codes, where $(2, k)$-regular non-binary LDPC codes over GF(q) are empirically known to be the best performing codes [42]. This is another significant advantage of non-binary LDPC codes.

Based on both binary and non-binary LDPC codes efficient methods have been proposed for information reconciliation in DV-QKD, all of them in the high-rate regime (that is, for code rates greater than one half). Notable examples are, for instance, highly efficient reconciliation methods using rate-adaptive binary [5] and non-binary LDPC codes [43, 44], blind (or interactive) reconciliation using also rate-adaptive but short block-length LDPC codes [6, 45, 46], and high-throughput reconciliation with layered decoding and quasi-cyclic LDPC codes [7]. These methods can also be used for information reconciliation in CV-QKD with slice reconciliation.

Binary and non-binary LDPC codes have been empirically shown to have good performance for high-rate codes. However, when transmitting information over a very noisy communication channel, that is, for low-rate coding, their performance degrades rapidly [47]. Multi-edge type LDPC codes were originally proposed by Richardson and Urbanke to design high-rate codes with low error floors and low-rate codes with high performance [48]. These codes are an extension of standard binary LDPC codes where in the Tanner graph only one type of edges is considered. In multi-edge type LDPC codes, there are different edge types such that a node is no longer characterized by a single degree but by a vector degree. Unfortunately, a major shortcoming of low-rate multi-edge type LDPC codes is the large number of check node computations which significantly increases their decoding complexity.

Efficient reconciliation methods based on multi-edge type LDPC codes have been proposed for information reconciliation in CV-QKD [14–17, 19–21, 23, 49]. However, most of these proposals consider very large block-length codes of approximately 10^6 bits, or even larger, which make hardware implementations unrealistic. Therefore, these approaches neither allow for efficient decoding using short or intermediate block-length codes, nor can be efficiently implemented. Their decoding complexity can only be reduced by limiting the maximum check node degree that may lead to suboptimal codes [50].

However, we consider that the potential of non-binary LDPC codes has not been explored enough in the context of CV-QKD, that is, for reconciling continuous correlated

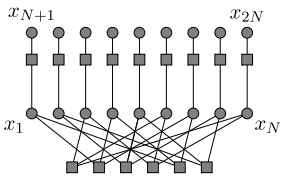

Figure 1 Example of C_2. A $(2,3)$-regular linear (mother) code is concatenated with an inner multiplicative repetition code of length 2, resulting in a code of rate 1/6

variables.[1] The purpose of this work is to study the possibility of adapting non-binary LDPC codes to efficiently operate in the low SNR regime. To this end, we carried out a comprehensive analysis of the multiplicatively repeated non-binary LDPC codes proposed in [52], and in this paper we show their interest for low-rate coding and their application in CV-QKD postprocessing. In the following, we first describe these codes in Sect. 2.2, and then a modified decoding algorithm for reconciling errors is given in Sect. 2.3.

2.2 Multiplicatively repeated non-binary LDPC codes

Kasai and Declerq proposed in [52] the concatenation of non-binary LDPC codes with multiplicative repetition inner codes. According to their proposal, a $(2,k)$-regular non-binary LDPC code over a finite field of order 2^p is multiplicatively repeated to construct non-binary LDPC codes of lower rates. Surprisingly, as we show below, such simple low-rate non-binary LDPC code construction using high order fields outperforms other low-rate codes so far, particularly when considering short and intermediate block-length codes.

Let C_1 be a $(2,3)$-regular non-binary LDPC code over GF(2^p) of length N symbols, or equivalently Np bits,[2] and rate 1/3. In the following, we refer to this code as *mother code*. From this mother code we construct a code C_2 in the following way. We choose N coefficients $r_{N+1},\dots,r_{2N}$ uniformly at random from the finite set GF(2^p) $\setminus \{0\}$, then for each codeword in C_1 we define a codeword in C_2 as follows:

$$C_2 = \{(x_1,x_2,\dots,x_{2N}) : (x_1,\dots,x_N) \in C_1,$$
$$x_{N+n} = r_{N+n}x_n \text{ for } n = 1,\dots,N\}.$$

We say that the symbol x_{N+n} (with $x_{N+n} = r_{N+n}x_n$) is a *multiplicative repetition* symbol of x_n, for $n = 1,\dots,N$. Therefore, we construct C_2 by multiplicatively repeating each symbol node of the mother code C_1. Note also that, for each multiplicative repetition symbol we have an additional parity-check constraint, that is, it holds $x_{N+n} + r_{N+n}x_n = 0$ for $n = 1,\dots,N$. Hence, in other words, we construct the code C_2 by connecting each symbol node x_n of C_1 to a new check node (the additional parity-check constraint), which is also connected to a second symbol node x_{N+n} (the multiplicative repetition symbol of x_n). Figure 1 depicts an example of C_2. As shown, each symbol node of degree one in the figure represents a multiplicative repetition symbol x_{N+n} of x_n for $n = 1,\dots,N$, and each check node of degree two represents a new parity-check constraint.

[1] Except for the case of the correlated bivariate normal distribution [51].

[2] For convenience and faster decoding [38], we only consider finite fields of characteristic two, that is, binary finite fields of order 2^p. The elements of the finite field are binary polynomials of degree less than or equal to $p-1$, that is, polynomials whose coefficients are either 0 or 1. Operations in the finite field (that is, addition and multiplication, and their inverse operations, subtraction and division, respectively) can then be efficiently implemented.

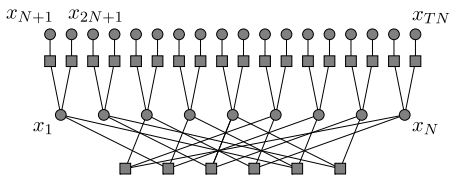

Figure 2 Example of C_3. A (2, 3)-regular linear code is concatenated with an inner multiplicative repetition code of length 3. The code rate is 1/9

Clearly, the constructed code C_2 has the same number of codewords as the mother code C_1, however the codewords of C_2 are twice as long as the codewords of C_1, that is, the code length of C_2 is $2N$ symbols, thus resulting in a lower code rate of 1/6.

Next, from C_2 we construct another code C_3 in a similar way. We choose again N coefficients $r_{2N+1}, \ldots, r_{3N}$ uniformly at random from the finite set $\mathrm{GF}(2^p) \setminus \{0\}$, and then we construct C_3 from C_2 by multiplicatively repeating each symbol of C_1 as follows:

$$C_3 = \{(x_1, x_2, \ldots, x_{3N}) : (x_1, \ldots, x_{2N}) \in C_2, \\ x_{2N+n} = r_{2N+n} x_n \text{ for } n = 1, \ldots, N\}.$$

C_3 has the same number of codewords as C_2 and C_1, but the codeword length is now of $3N$ symbols. Thus, the code rate of C_3 is 1/9. Figure 2 depicts an example of C_3. Again, symbol nodes of degree one correspond to multiplicative repetition symbols, whereas check nodes of degree two correspond to parity-check constraints induced by each multiplicative repetition symbol.

Subsequent lower rate codes are constructed recursively, as we have shown above for C_2 and C_3. A code C_T, with $T \geq 2$, is defined recursively as follows. We choose N coefficients $r_{(T-1)N+1}, \ldots, r_{TN}$ uniformly at random from $\mathrm{GF}(2^p) \setminus \{0\}$, then we construct C_T from C_{T-1} by multiplicatively repeating each symbol of C_1 as follows:

$$C_T = \left\{(x_1, x_2, \ldots, x_{TN}) : (x_1, \ldots, x_{(T-1)N}) \in C_{T-1}, \right. \\ \left. x_{(T-1)N+n} = r_{(T-1)N+n} x_n \text{ for } n = 1, \ldots, N\right\}.$$

The code C_T has a length of $T \cdot N$ symbols, and rate $1/(3T)$. We refer to T as *repetition parameter*.

Note that, this code construction is inherently rate-adaptive since in the construction of the last code C_T from C_{T-1} we can add as many multiplicative repetition symbols as we wish, obviously between 1 and N. Hence, from a code C_{T-1} with codewords of length $(T-1)N$ symbols we can construct a code C_T with codewords of length from $(T-1)N+1$ to TN symbols, resulting in a code of rate $1/3(T-1) < R \leq 1/3T$.

2.3 Non-binary LDPC decoding algorithm

In this section we describe a belief propagation algorithm for efficiently decoding multiplicatively repeated non-binary LDPC codes.[3] The algorithm is adapted to the source coding problem with side information studied by Slepian and Wolf [54], that more accurately describes the problem of correcting disparities between correlated sources—also

[3] It is well-known that a belief propagation algorithm would produce the exact posterior probabilities of all the symbols after a number of iterations, that is, optimum decoding, but only if the Tanner graph contains no cycles [53].

known as information reconciliation or simply reconciliation in the context of secret-key agreement.

Source coding with side information: Let x and y be two correlated strings of length N (that is, two strings of symbols, or equivalently, two bit strings of length Np) belonging to Alice and Bob, respectively, that is, these strings are realizations of the correlated sources X and Y. The encoder computes the syndrome z of his string x, that is, $z = Hx$ (where H is the parity-check matrix of a given linear code), and sends it to the decoder through a noiseless channel. Then the decoder, given the coset index z (the syndrome of x), look for the sequence in the coset C_z that is closest to y, where the coset C_z is a set that includes all strings of length N with z syndrome, that is, $C_z = \{x : Hx = z\}$. For further information see the Wyner's binning scheme [55], or the modified decoding algorithm for binary LDPC codes proposed by Liveris [56].

In the scenario presented above Alice is the encoder and Bob the decoder, then if Alice is also the emitter of quantum states and Bob the receiver we say that the parties perform direct reconciliation. Otherwise, that is, when the emitter and encoder are on different sides, we consider it as reverse reconciliation. To switch from one scheme to another we just need to exchange the roles (encoder and decoder).

Note that, in the following we will consider the decoding of a multiplicatively repeated non-binary LDPC code over GF(2^p) of length N symbols. Therefore, each sequence of p bits represents the binary polynomial corresponding to an element of the finite field GF(2^p), that is, a symbol.

Decoding algorithm: Let $\mathcal{N}(m)$ be the set of indexes of symbol nodes adjacent to the check node z_m, and let $\mathcal{M}(n)$ be the set of indexes of check nodes adjacent to the symbol node x_n, that is, $\mathcal{N}(m) = \{n : h_{mn} \neq 0\}$ and $\mathcal{M}(n) = \{m : h_{mn} \neq 0\}$, respectively, where $H = (h_{mn})$ is the parity-check matrix of a given linear code. An iterative decoding (belief propagation based) algorithm for non-binary LDPC codes, such as in the binary case, is a message-passing algorithm where probabilities are propagated along the edges of the Tanner graph associated with the parity-check matrix H. The algorithm consists mainly of two alternating steps. On each iteration ℓ, first messages $r_{mn}^{(\ell)}$ are exchanged from check to symbols nodes, and later messages $q_{mn}^{(\ell)}$ are exchanged from symbol to check nodes. Figure 3 depicts how these messages are iteratively updated using extrinsic information, that is, probabilities obtained in a previous iteration from other neighboring nodes. Both steps are repeated until all of symbol values are known (that is, all the parity-check constraints are satisfied), or a maximum number of decoding iterations is reached.

Step 1. Initialization: Let X_n and Y_n be the random variables of the n-th transmitted and received symbols, respectively, and let y_n be n-th received symbol, that is, the channel output of the n-th transmitted symbol. For each symbol node x_n in the mother code C_1, with $n = 1,\ldots,N$, we calculate 2^p prior probabilities, that is, the *a priori* probability of symbol x_n being α:

$$p_n^{(0)}(\alpha) = \Pr(X_n = \alpha | Y_n = y_n), \quad \forall \alpha \in \mathrm{GF}(2^p).$$

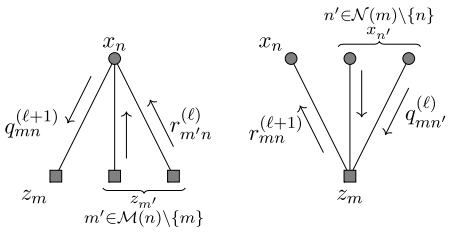

Figure 3 Iterative decoding messages (probabilities) propagated along the edges of a Tanner graph. Messages $q_{mn}(\boldsymbol{\alpha})$ for all $\boldsymbol{\alpha} \in \mathrm{GF}(2^p)$ are exchanged from symbol to check nodes, that is, the probability that symbol $x_n = \boldsymbol{\alpha}$ given the information obtained from other checks (Left). Messages $r_{mn}(\boldsymbol{\alpha})$ for all $\boldsymbol{\alpha} \in \mathrm{GF}(2^p)$ are exchanged from check to symbol nodes, that is, the probability of check z_m being satisfied if symbol $x_n = \boldsymbol{\alpha}$ given the information obtained from other symbols (Right). Note that, messages or probabilities in iteration $\ell + 1$ are calculated from the messages exchanged in the previous iteration ℓ

In order to calculate the a priori probability of each symbol node x_n in the mother code C_1 we have to consider also the a priori probabilities of the multiplicative repetition symbols x_{tN+n} of x_n, given the check constraints $x_{tN+n} = r_{tN+n}x_n$, for $t = 1, \ldots, T-1$.

Then, each symbol node x_n initially sends the message $q_{mn}^{(0)} = p_n^{(0)}$ to its adjacent check nodes z_m, for all $m \in \mathcal{M}(n)$, that is:

$$q_{mn}^{(0)}(\alpha) = p_n^{(0)}(\alpha), \quad \forall \alpha \in \mathrm{GF}(2^p).$$

Note also that, messages reaching symbol nodes of degree one or degree two check nodes do not participate in messages that are sent back from these nodes (see Fig. 3). Therefore, in a multiplicatively repeated non-binary LDPC code the decoder does not need to propagate messages either to those symbol nodes of degree one or to their adjacent check nodes of degree two (see the upper part of the Tanner graph in Figs. 1 and 2). Consequently, in the following steps 2 and 3 (that is, in the message-passing part of the algorithm), for decoding we only consider the lower part of the graphs, that is, the mother code C_1.

Step 2. Messages from checks to symbols: Each check node z_m has incoming messages $q_{mn}^{(\ell)}$ received in the iteration ℓ from its adjacent symbol nodes x_n, for all $n \in \mathcal{N}(m)$. In the subsequent iteration, we calculate the messages sent back from the check node to its neighboring nodes, $r_{mn}^{(\ell+1)}$, but only using extrinsic information, that is, the message sent back from the check node z_m to the symbol node x_n is calculated using only the incoming messages from other edges, that is $q_{mn'}^{(\ell)}$ with $n' \in \mathcal{N}(m) \setminus \{n\}$.

Therefore, we compute[4] first:

$$\tilde{q}_{mn}^{(\ell)}(\alpha) = q_{mn}^{(\ell)}(h_{mn}^{-1}\alpha), \quad \forall \alpha \in \mathrm{GF}(2^p)$$

and then

$$\tilde{r}_{mn}^{(\ell+1)}(\alpha) = \bigotimes_{n' \in \mathcal{N}(m)\setminus\{n\}} \tilde{q}_{mn'}^{(\ell)}(\alpha), \quad \forall \alpha \in \mathrm{GF}(2^p)$$

[4]Note that, for convenience instead of computing $f(x) = h^{-1}(x)$ we could use $f(h(x)) = x$.

where $q_1 \otimes q_2$ is a convolution of q_1 and q_2, that is:

$$(q_1 \otimes q_2)(\alpha) = \sum_{\substack{\alpha_1,\alpha_2 \in \mathrm{GF}(2^p) \\ \alpha=\alpha_1+\alpha_2}} q_1(\alpha_1) q_2(\alpha_2), \quad \forall \alpha \in \mathrm{GF}(2^p).$$

This is the most complex part of the decoding. However, the convolution can be efficiently calculated in the frequency domain using the Fourier transform over finite fields. This transform can be easily computed when the Galois field GF(q) is a binary extension field with order $q = 2^p$. The decoding of non-binary LDPC codes is then optimized using for instance the p-dimensional Walsh-Hadamard transform as proposed in [38, 57]. By applying the Walsh-Hadamard transform $\mathcal{W}\{\cdot\}$ the discrete convolution turns into a multiplication as follows:

$$\mathcal{W}\{\tilde{r}_{mn}^{(\ell+1)}(\alpha)\} = \prod_{n' \in \mathcal{N}(m)\setminus\{n\}} \mathcal{W}\{\tilde{q}_{mn'}^{(\ell)}(\alpha)\}, \quad \forall \alpha \in \mathrm{GF}(2^p).$$

Moreover, since the Hadamard transform coincides with its inverse, it follows:

$$\tilde{r}_{mn}^{(\ell+1)}(\alpha) = \mathcal{W}\{\prod_{n' \in \mathcal{N}(m)\setminus\{n\}} \mathcal{W}\{\tilde{q}_{mn'}^{(\ell)}(\alpha)\}\}, \quad \forall \alpha \in \mathrm{GF}(2^p).$$

Note that, both the input and output of the Walsh-Hadamard transform are 2^p dimensional real-valued vectors. Then, by $\mathcal{W}\{f(\alpha)\}$ we denote the result of applying the Walsh-Hadamard transform over the 2^p values of the function $f(\alpha)$, with $\alpha \in \mathrm{GF}(2^p)$, but considering only the component of the output vector that corresponds to the input $f(\alpha)$ for a given α. This can be efficiently implemented via the fast Walsh-Hadamard transform.

Finally, each check node z_m sends the message $r_{mn}^{(\ell+1)}$ to the symbol node x_n for all $n \in \mathcal{N}(m)$ that is calculated as follows:

$$r_{mn}^{(\ell+1)}(\alpha) = \tilde{r}_{mn}^{(\ell+1)}(h_{mn}\alpha), \quad \forall \alpha \in \mathrm{GF}(2^p).$$

Note that, this is the channel coding version of the decoding algorithm, that is, when the transmitted message is always a codeword with zero syndrome. For the source coding with side information problem, the decoder look for the closest word with a given syndrome z (the syndrome of x), and thus the decoding is calculated as follows:

$$r_{mn}^{(\ell+1)}(\alpha) = \tilde{r}_{mn}^{(\ell+1)}(h_{mn}\alpha - z_m), \quad \forall \alpha \in \mathrm{GF}(2^p).$$

Step 3. Messages from symbols to checks: Each symbol node x_n has incoming messages $r_{mn}^{(\ell+1)}$ (computed in step 2) received from its adjacent check nodes z_m, for all $m \in \mathcal{M}(n)$. Then, messages $q_{mn}^{(\ell+1)}$ are sent back from the symbol node x_n to its neighboring nodes, again only using extrinsic information, that is, the message sent back from the symbol node x_n to the check node z_m is calculated using only the incoming messages from other edges, that is $r_{m'n}^{(\ell+1)}$ with $m' \in \mathcal{M}(n) \setminus \{m\}$, as follows:

$$q_{mn}^{(\ell+1)}(\alpha) = \beta_m p_n^{(0)}(\alpha) \prod_{m' \in \mathcal{M}(n)\setminus\{n\}} r_{m'n}^{(\ell+1)}(\alpha), \quad \forall \alpha \in \mathrm{GF}(2^p)$$

where β_m is a normalizing factor such that messages $q_{mn}^{(\ell+1)}(\alpha)$ are probabilities, that is, β_m is chosen such that:

$$\sum_{\alpha\in \mathrm{GF}(2^p)} q_{mn}^{(\ell+1)}(\alpha) = 1.$$

Step 4. Tentative decision: Finally, for each symbol node in the mother code C_1 we calculate an estimation of the *a posteriori* probability of symbol x_n being α, with $n = 1,\ldots,N$, as follows:

$$p_n^{(\ell)}(\alpha) = p_n^{(0)} \prod_{m'\in\mathcal{M}(n)} r_{m'n}^{(\ell)}(\alpha), \quad \forall\alpha \in \mathrm{GF}(2^p).$$

We make then a tentative decision for the value of each symbol x_n based on the highest probability:

$$\hat{x}_n^{(\ell)} = \max_{\alpha\in \mathrm{GF}(2^p)} \{p_n^{(\ell)}(\alpha)\}.$$

Multiplicative repetition symbols x_{tN+n} of x_n, for each $n = 1,\ldots,N$, are then calculated with the newly obtained value $\hat{x}_n^{(\ell)}$ of symbol x_n and using the parity-check constraints $x_{tN+n} = r_{tN+n}x_n$, for all $t = 1,\ldots,T-1$.

Once we have an estimate of the values for all symbols, $\hat{x}$, we may calculate all the parity-check constraints to verify if they are satisfied (syndrome validation), that is, for the source coding with side information problem we verify if the received syndrome z equals $H\hat{x}$. In such a case the algorithm concludes with successful decoding. Otherwise, the decoding algorithm continues iteratively, repeating steps 2 to 4, until the parity-check constraints are satisfied or a maximum number of iterations is reached without successful decoding. Note, however, that sometimes (typically in hardware implementations) the decoding algorithm continues iteratively without verifying whether the constraints are satisfied, that is, without a syndrome validation step. In that case the algorithm concludes after a given number of decoding iterations.

Compared to the decoding of binary LDPC codes, non-binary LDPC decoding demands a high computational complexity in the check-node processing (that is, when computing the messages from checks to symbols in Step 2 of the decoding algorithm) and requires a large amount of memory to store the messages exchanged in each iteration. However, there are several proposals in the literature to reduce both computational complexity and memory requirement.

Recent hardware (HW) implementations of non-binary LDPC codes for CV-QKD [58] suggest that the constructions discussed here should similarly be amenable to HW. Let us review in more detail the state-of-the-art to understand where the challenges may lie. In [32] there are summarized multiple HW implementations (in FPGA and ASIC architectures) of non-binary LDPC decoders. Some of these also consider the sum-product algorithm here described, over finite fields of order 2^8, and with block-lengths of up to 1024 symbols and rate one half. We instead require codes of rate 1/3, with less computational complexity. However, to the best of the authors' knowledge, there are no hardware implementations of non-binary LDPC codes over finite fields of higher orders. In particular, its implementation over a finite field of order 2^{10} remains open.

Table 1 Multi-edge type LDPC ensembles

R	ν_m	m			μ_m	m		
0.01	0.012	2	95	0	0.004	4	0	0
	0.009	3	95	0	0.007	5	0	0
	0.979	0	0	1	0.942	0	2	1
					0.037	0	3	1
0.015	0.028	2	53	0	0.005	3	0	0
	0.009	3	53	0	0.017	4	0	0
	0.963	0	0	1	0.928	0	2	1
					0.035	0	3	1
0.02	0.031	2	45	0	0.019	4	0	0
	0.013	3	45	0	0.005	5	0	0
	0.956	0	0	1	0.888	0	2	1
					0.068	0	3	1
0.03	0.017	2	58	0	0.011	9	0	0
	0.025	3	58	0	0.001	10	0	0
	0.958	0	0	1	0.438	0	2	1
					0.52	0	3	1
0.04	0.027	2	44	0	0.015	9	0	0
	0.029	3	44	0	0.001	6	0	0
	0.944	0	0	1	0.368	0	2	1
					0.576	0	3	1

3 Results

Comprehensive simulations were performed to analyze the performance and efficiency of multiplicatively repeated non-binary LDPC codes, and such results are initially presented in Sect. 3.1. Next, we verified that these codes are efficient enough to exchange secret-keys over long distances using a CV-QKD protocol, and secret-key rates are then given in Sect. 3.2.

3.1 Performance and reconciliation efficiency

In this section we study the performance and efficiency of multiplicatively repeated non-binary LDPC codes for correcting errors at very low SNRs, and compare these codes to other similar proposals in the literature. Simulations were performed over the binary input additive white Gaussian noise (BIAWGN) channel, as it is commonly used in prior work [14–16, 19, 22–26, 59]. This is a good model that approximates well, though not exactly, the correlations between input and output [60]. This channel is also the correct model for binary modulated CV-QKD [61]. Although we could perform a similar analysis for this protocol, to avoid being repetitive, we focused on the application to Gaussian modulated CV-QKD.

First, we have simulated the performance of low-rate multi-edge type LDPC codes proposed in [48]. We designed ensembles of irregular multi-edge type LDPC codes using a modified version of the differential evolution algorithm described in [62]. The designed codes (see Table 1) have thresholds similar to others published in the literature. Thresholds were computed using a modified version of the discretized density evolution algorithm described in [41]. Both, differential and density evolution were modified according to the suggestions given in [48, 63], where the authors describe how the analysis for standard LDPC codes given in [36, 40] extends to multi-edge type LDPC codes. Then, we constructed instances of the code ensembles given in Table 1 using a modified progres-

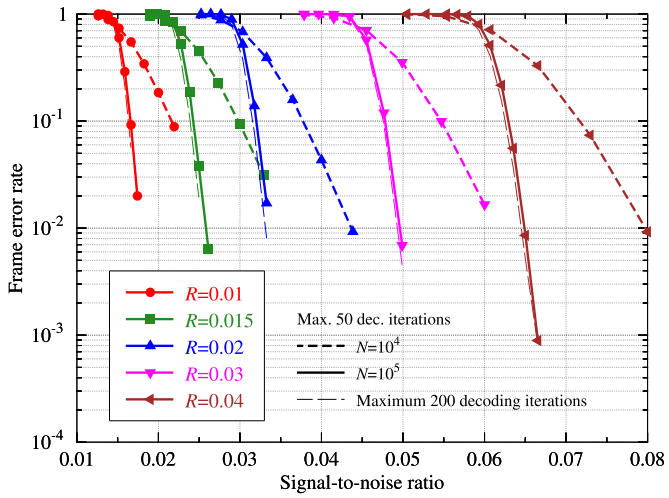

Figure 4 Performance (that is, frame error rate as a function of signal-to-noise ratio) of low-rate multi-edge type LDPC codes over the BIAWGN channel, for several code rates R and code lengths N in bits

sive edge-growth algorithm [64]. Code lengths of 10^4 and 10^5 bits were chosen.[5] Numerical results were finally computed using iterative LDPC decoding. For decoding we used a sum-product algorithm with serial schedule and a maximum of 50 decoding iterations (that is, after each iteration we make a tentative decision and syndrome validation, thus the algorithm stops assuming that decoding was successful if the syndrome is satisfied or the maximum number of decoding iterations is reached). Figure 4 shows the performance of these codes over the BIAWGN channel. For the codes of 10^5 bits length, simulations were also performed increasing the maximum number of decoding iterations to 200, but however, as shown, the performance does not improve significantly.

Next, we have simulated the performance of multiplicatively repeated non-binary LDPC codes. We considered as mother code C_1 a $(2,3)$-regular non-binary LDPC code over GF(2^{10}) of rate 1/3. From such a code we constructed multiplicatively repeated codes of lower rates 1/30, 1/45, 1/60, and 1/90, as described in Sect. 2.2. For the mother code two code lengths of $N = 10^3$ and 10^4 symbols, were considered. Given that each element of the finite field is represented by a binary polynomial of degree less than or equal to 9 (that is, a polynomial with 10 binary coefficients or 10-bit string), we are using 10 bits per symbol. Thus, the lengths considered for the mother codes equal the lengths in bits previously considered for multi-edge type LDPC codes. Note that, the length of a multiplicatively repeated code actually depends on the repetition parameter T, that is, the actual number of symbols or codeword length is NT. However, as we already argued in Sect. 2.3, multiplicative repetition symbols do not contribute to the messages computed in the message-passing part of the decoding algorithm. Therefore, for the sake of convenience, in the following when we refer to the length of multiplicatively repeated non-binary LDPC codes we consider the length N of the mother code (instead of the actual but unrealistic code length NT). Numerical results were computed using iterative LDPC

[5]Note that, the code lengths here chosen are relatively short compared to the lengths considered in most proposals using multi-edge type LDPC codes in CV-QKD. For instance, a code length of 2^{20} bits was considered in [14], a length of 10^6 bits were used in [17, 21, 23], and 1.024×10^6 bits length in [19].

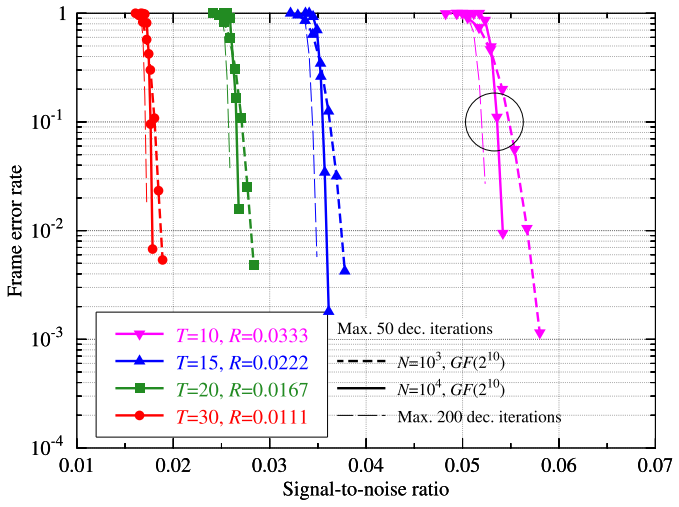

Figure 5 Performance of multiplicatively repeated non-binary LDPC codes over GF(2^{10}) and the BIAWGN channel, for several code rates R and code lengths N in symbols

decoding. For decoding we used the sum-product algorithm described in Sect. 2.3 with a maximum of 50 decoding iterations (again, making a tentative decision and verifying the syndrome after each iteration). Figure 5 shows the performance of these multiplicatively repeated non-binary LDPC codes over the BIAWGN channel. As shown, it is noteworthy that the performance of shorter codes, of 10^3 symbol lengths, is almost as good as that of longer codes. For the codes of 10^4 symbols length, simulations were also performed increasing the maximum number of decoding iterations to 200. As shown, unlike multi-edge type LDPC codes, the number of iterations plays a determining role for multiplicatively repeated non-binary LDPC codes. This behavior is depicted in Fig. 5, where a circle marks the performance (at a frame error rate of 10^{-1}) of the code of rate $R = 1/30$ considering different code lengths and decoding iterations. In summary, to improve the performance (and consequently the efficiency) of these codes, it is necessary to increase both the code length (as usual) and the maximum number of decoding iterations.

In the following we study and compare the efficiency of multiplicatively repeated non-binary LDPC codes with other proposals, but let us first see how we calculate it. Let R be the rate of the code used for correcting errors, then the reconciliation efficiency in CV-QKD, denoted by β, is calculated as follows:

$$\beta = \frac{R}{C}, \tag{1}$$

where C is the channel capacity, that is, here the capacity of the BIAWGN channel. Hence, the channel capacity and therefore also the efficiency are functions of SNR. Note that, for small SNR values s the capacity of the BIAWGN channel is well approximated by that of the AWGN channel, given by $C = \frac{1}{2}\log_2(1+s)$.

Table 2 shows the reconciliation efficiencies, β, for the multi-edge type LDPC and multiplicatively repeated non-binary LDPC codes simulated in Figs. 4 and 5, respectively. A number of significant cases were chosen for several code rates R, code lengths N, and maximum number of decoding iterations (iters). In the case of multi-edge type LDPC

Table 2 Information reconciliation efficiencies

Multi-edge type				Multiplicatively repeated			
R	N	iters	β	R	N	iters	β
0.01	10^5	50	0.8475	0.0111	10^3	200	**0.8732**
0.01	10^5	200	0.875	0.0111	10^4	200	**0.9079**
0.015	10^5	50	0.8647	0.0166	10^3	200	**0.876**
0.015	10^5	200	0.871	0.0166	10^4	200	**0.9087**
0.02	10^5	50	**0.8793**	0.0222	10^3	200	0.8775
0.02	10^5	200	0.8911	0.0222	10^4	200	**0.9092**
0.03	10^5	50	**0.894**	0.0333	10^3	200	0.8781
0.03	10^5	200	0.898	0.0333	10^4	200	**0.9112**

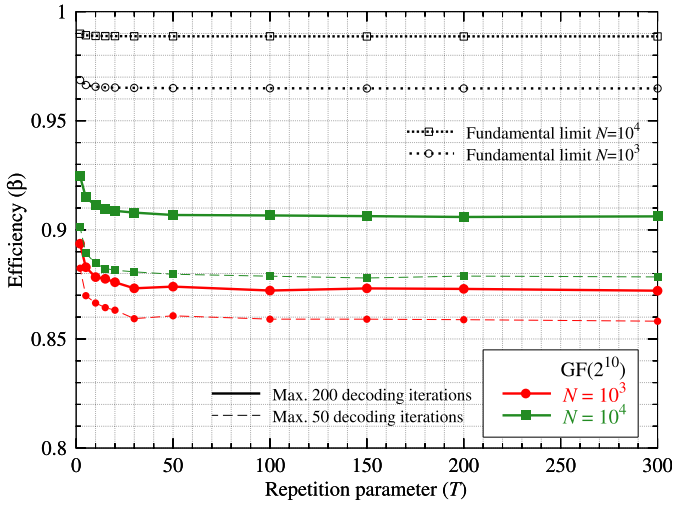

Figure 6 Reconciliation efficiency of multiplicatively repeated non-binary LDPC codes over GF(2^{10}). Efficiency was computed considering a target FER of 10^{-1}

codes were only considered larger code lengths of 10^5 bits, but results are compared for a maximum of 50 and 200 decoding iterations. For the multiplicatively repeated non-binary LDPC codes were considered both code lengths, 10^3 and 10^4 symbols, but only a maximum of 200 decoding iterations. Efficiencies were calculated for a target frame error rate (FER) of 10^{-1} as suggested in [7], that is, given a code of rate R we first compute the SNR for which the code works at a FER of 10^{-1}, then we calculate the channel capacity C and efficiency β using equation (1) with the obtained SNR. As shown in Table 2, multiplicatively repeated non-binary LDPC (even when using short block-length) codes outperform multi-edge type LDPC codes, but the maximum number of decoding iterations is a determining parameter, since, while multi-edge type LDPC codes do not substantially improve the efficiency with larger decoding iterations, this is not the case with multiplicatively repeated non-binary LDPC codes. A comprehensive analysis of this behavior was performed below.

Figure 6 shows the reconciliation efficiency of multiplicatively repeated non-binary LDPC codes over GF(2^{10}) as a function of the repetition parameter T. As shown, the efficiency gradually decreases at the beginning, that is with $2 \leq T \leq 10$, but surprisingly remains almost constant for higher values of the repetition parameter, that is for $T \geq 20$. Therefore, low-rate and very low-rate codes are almost equally efficient. It is notewor-

thy that extremely low-rate codes, that is, codes of rates $R = 1/300$, $R = 1/600$ and up to $R = 1/900$, with length 10^4 symbols, have an efficiency above 90%. Furthermore, for very low-rate codes, that is $R < 0.02$, the efficiency of codes of length 10^3 symbols is even better than the efficiency of multi-edge type LDPC codes of length 10^5, as reported in Table 2. Note also that, to better understand the significance of the number of decoding iterations, the figure shows simulation results for a maximum of 50 (dashed line) and 200 (solid line) iterations.

In the figure, we also show the fundamental limits on the efficiency when reconciling errors using multiplicatively repeated non-binary LDPC codes over GF(2^{10}) with a mother code of lengths $N = 10^3$ and $N = 10^4$. We used recent results in non-asymptotic classical information theory [65] for upper bounding the reconciliation efficiency in CV-QKD with only one-way communications. These results were adapted to calculate the efficiency β as given in Eq. (1):

$$\beta(n,\epsilon,\sigma) = 1 - \frac{\sqrt{v(\sigma)/n}}{1-h(\sigma)}\Phi^{-1}(1-\epsilon), \tag{2}$$

where n is the length of the code (in bits), ϵ is the frame error rate, and σ is the signal-to-noise ratio. On the other hand, $\Phi(\cdot)$ is the cumulative standard normal distribution, $h(\sigma) = 1 - C$ is the conditional entropy, and $v(\sigma) = e(\sigma) - h(\sigma)^2$ is the conditional entropy variance, where:

$$f_{XY}(x,y) = \sqrt{\frac{\sigma}{8\pi}}e^{\sigma(y-x)^2/2}, \qquad f_Y(y) = f_{XY}(1,y) + f_{XY}(-1,y),$$
$$C = -\int_{-\infty}^{\infty} f_Y(y)\log_2 f_Y(y)dy + \frac{1}{2}\log_2\left(\frac{\sigma}{2\pi e}\right) \approx \frac{1}{2}\log_2(1+\sigma),$$

and

$$e(\sigma) = 2\int_{-\infty}^{\infty} f_{XY}(1,y)\left(\log_2\frac{f_{XY}(1,y)}{f_Y(y)}\right)^2 dy.$$

Note that each point in the figure corresponds to the efficiency of a multiplicatively repeated non-binary LDPC code for a given repetition parameter T, where each symbol of the mother code is then multiplicatively repeated T times, thus expanding the codeword length to NT symbols. Given that we are using 10 bits per symbol, the length of the equivalent binary code is $n = 10NT$ bits. Furthermore, for each T value we consider the signal-to-noise ratio σ at which the efficiency shown was achieved. Finally, taking into account that efficiencies were calculated for a target frame error rate of $\epsilon = 10^{-1}$, we may obtain an upper bound for the reconciliation efficiency given by $\beta(n,\epsilon,\sigma)$.

For a constant block-length code, this upper bound on the reconciliation efficiency is a monotonically decreasing function for decreasing signal-to-noise ratios. However, both the fundamental limits and reconciliation efficiencies shown remain constant. This behavior occurs because, as the repetition parameter increases, more symbol nodes are multiplicatively repeated, thereby increasing the effective length n (in bits) of the reconciled string.

Figure 7 shows again the performance of multiplicatively repeated non-binary LDPC codes but now for ultra-low rates, up to $R = 0.00111$ (that is, with repetition parameter

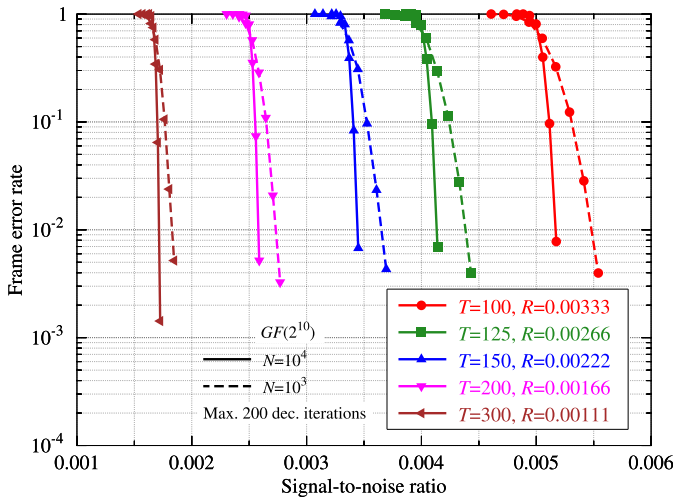

Figure 7 Performance of multiplicatively repeated non-binary LDPC codes over GF(2^{10}) and the BIAWGN channel, for several ultra-low code rates R and code lengths N in symbols

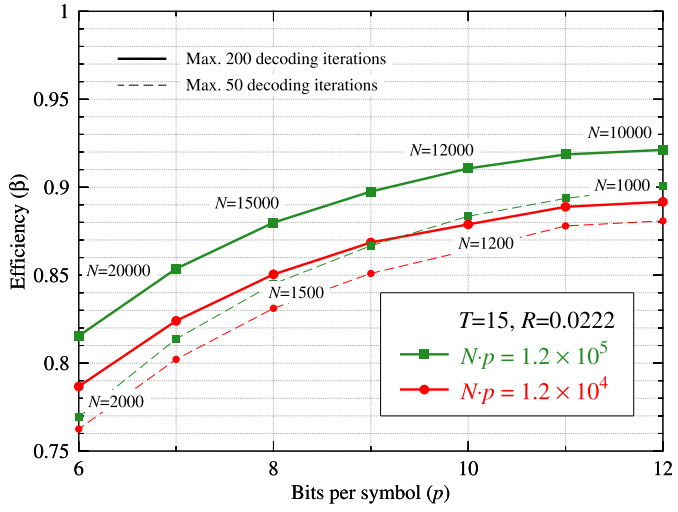

Figure 8 Reconciliation efficiency of multiplicatively repeated non-binary LDPC codes over GF(2^p) with repetition parameter $T = 15$. Efficiency was computed considering a target FER of 10^{-1}

$T = 300$). The mother codes C_1 used are the same as for Fig. 5, that is, a $(2, 3)$-regular non-binary LDPC code over GF(2^{10}) of rate 1/3 and lengths of 10^3 and 10^4 symbols. However, in this case simulations were performed only considering 200 decoding iterations maximum. The figure shows the performance of those codes with lowest code rates that perform well over the BIAWGN channel (as confirmed in Fig. 6).

Finally, we analyze the relationship between the efficiency and the order of the Galois field used in the construction and decoding of multiplicatively repeated non-binary LDPC codes. Figure 8 reports the reconciliation efficiency of multiplicatively repeated non-binary LDPC codes over different Galois fields GF(q) being a binary extension field with order $q = 2^p$. For all the codes the repetition parameter is $T = 15$, hence the code rate is $R = 1/45$. However, different code length N were chosen such that the mother code

lengths in bits are $Np = 1.2 \times 10^4$ and $Np = 1.2 \times 10^5$. As shown, as the order of the Galois fields increases, the efficiency also improves. Therefore, high orders are also a necessary condition to achieve good performance and reconciliation efficiency using the proposed codes. Again, as in the previous figure, results are shown for a maximum of 50 (dashed line) and 200 (solid line) decoding iterations.

3.2 Secret-key rate

The asymptotic secret-key rate for collective attacks of a CV-QKD protocol using reverse reconciliation is given by $K = \beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}}$, where I_{AB} is the mutual information between Alice and Bob (emitter/decoder and receiver/encoder, respectively), χ_{BE} is the Holevo bound on the information leaked to the eavesdropper Eve (that is, the maximum information she may have access to) for reverse reconciliation [66], and β is the reconciliation efficiency. This efficiency gives a fraction of the raw keys shared by Alice and Bob after the reconciliation procedure, that is, the length $n\beta I_{\mathrm{AB}}$ of the reconciled bit strings that the parties are left with. Good efficiency values are then necessary to achieve high secret-key rates over long distances, but there are also other parameters that need to be considered, such as FER, since both efficiency and FER are correlated as shown in Sect. 3.1.

In the finite-size scenario, that is, when considering finite-size effects (mainly in the parameter estimation procedure) the secret-key rate is then given by [67]

$$K = \frac{n}{N}(1-F)(\beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}} - \Delta(n)), \tag{3}$$

where n is the length of the raw key (a reconciled and therefore common bit string) used in the privacy amplification procedure, N is the number of exchanged signals (thus, $N - n$ signals are used for parameter estimation), F is the reconciliation FER, and $\Delta(n)$ is a function related to the security of privacy amplification in the finite-size regime. When $n \geq 10^4$ this function is essentially determined by [67]

$$\Delta(n) \approxeq 7\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}},$$

where $\bar{\epsilon}$ is a smoothing parameter.

Figure 9 shows the finite-size secret-key rate as a function of the signal-to-noise ratio for several transmission distances $L = 20$, $L = 50$, $L = 100$, $L = 125$ and $L = 150$, and different reconciliation efficiencies $\beta = 0.87$, $\beta = 0.9$ and $\beta = 0.92$. Efficiencies $\beta = 0.87$ and $\beta = 0.9$ correspond to multiplicatively repeated non-binary LDPC codes of length 10^3 and 10^4, respectively, over GF(2^{10}), as reported in Table 2. An efficiency of $\beta = 0.92$ corresponds to multiplicatively repeated non-binary LDPC codes of length 10^4 over GF(2^{12}). For the secret-key rate calculation, the quantum channel and CV-QKD devices were characterized using common parameters previously published in the literature [22, 23, 59, 66]. Hence, we assume the standard loss of a single-mode optical fiber of $\alpha = 0.2$ dB/km, a constant excess channel noise of $\varepsilon = 0.005$ (in shot noise units), and Bob's homodyne detector efficiency of $\eta = 0.606$, with electronic noise $V_{\mathrm{el}} = 0.041$ (in shot noise units). Alice's modulation variance V_A (in shot noise units) is considered within the interval $[1, 100]$ and optimized at each transmission distance to maximize the secret-key rate. Furthermore, as suggested in [23, 67] we have also considered a raw key length of $n = 10^{12}$ bits with $N = 2n$, and a conservative choice for the security parameter $\bar{\epsilon} = 10^{-10}$.

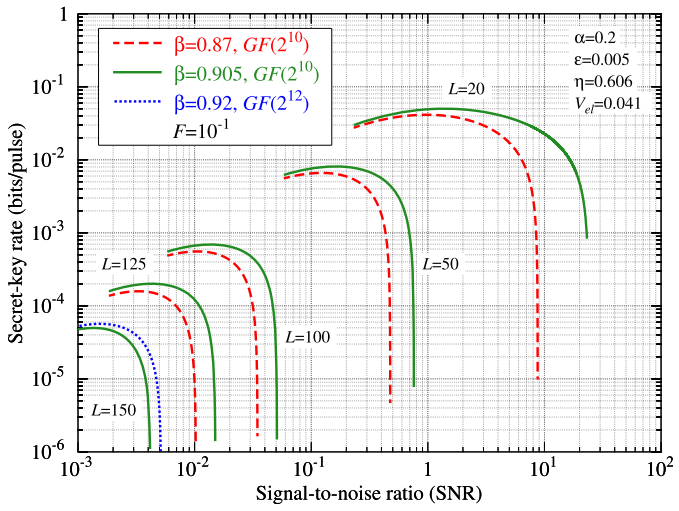

Figure 9 Secret-key rate for collective attacks with respect to the SNR

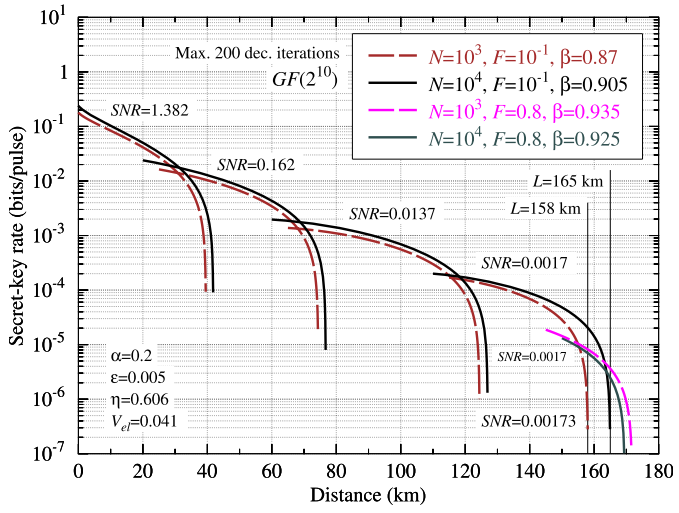

Figure 10 Secret-key rate for collective attacks with respect to the distance

Finally, Fig. 10 shows the finite-size secret-key rate with respect to the transmission distance using the optimal SNR values for each distance, as calculated for Fig. 9. We have considered the performance and efficiency of multiplicatively repeated non-binary LDPC codes over GF(2^{10}) of lengths $N = 10^3$ symbols (long-dashed lines) and $N = 10^4$ symbols (solid lines), that is, as previously reported in Table 2, we considered the reconciliation efficiencies of $\beta = 0.87$ and $\beta = 0.90$, respectively, with a FER of 10^{-1}. As shown, the maximum achievable distance of a CV-QKD protocol using the proposed codes is around 158 km with a multiplicatively repeated non-binary LDPC code over GF(2^{10}) of 10^3 symbols length, and around 165 km with a code of 10^4 symbols length, in both cases with a FER of $F = 10^{-1}$. Additionally, we have also considered an efficiency of $\beta = 0.925$ and $\beta = 0.935$, which are achieved at a higher FER of 80%, both for the codes of length 10^4 symbols and 10^3 symbols, respectively. The maximum distance is then slightly increased

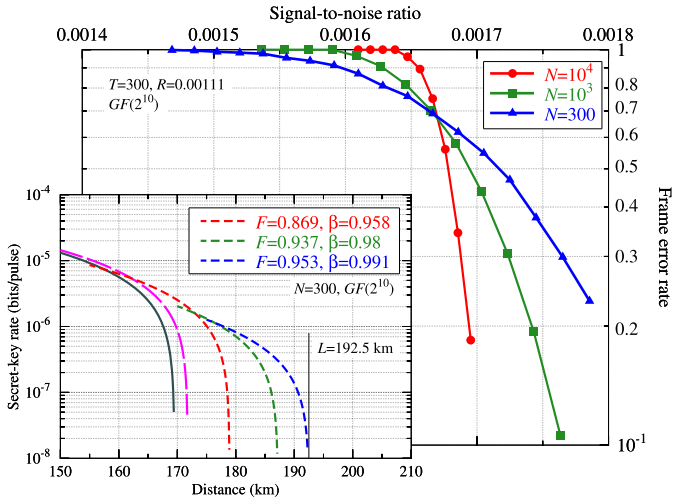

Figure 11 Performance of multiplicatively repeated non-binary LDPC codes for several code lengths N, and secret-key rate for collective attacks with respect to the distance using short block-length codes

to approximately 169.4 km using the code of length 10^4 symbols, and 171.7 km using the code of length 10^3 symbols.

Regarding the performance of error-correcting codes in the high FER region, in coding theory it is well known that in this region there is an SNR value at which codes of different block-lengths have the same performance. Then, on the one hand, for higher SNRs the performance of long codes is much better than that of short ones. On the other hand, however, for lower SNRs the performance of short block-length codes is better. This behavior is shown in Fig. 11 (although this can also be seen in Figs. 4, 5 and 7). According to this behavior, it is interesting to study how short block-length codes can help to increase the maximum distance at which a key can be securely exchanged and reconciled. Indeed, Fig. 11 also shows that for short codes there is still a range of SNRs for which it is still possible to exchange secret-keys, and thus increase the maximum secure distance of a CV-QKD protocol.

In addition, to make this proposal comparable to other results reported in the literature, we included an additional figure. Figure 12 shows the secret-key rate again for collective attacks and the finite-size case, but considering the transmission over an ultra-low loss fiber with attenuation of $\alpha = 0.16$ dB/km, such as in [18]. The secret-key rate was calculated considering the same codes, their performance and efficiency, as in Figs. 10 and 11.

4 Conclusions

Multiplicatively repeated non-binary LDPC codes over a finite field of characteristic two were considered for correcting errors in the low SNR regime. These codes are of particular interest for information reconciliation in CV-QKD, since they outperform multi-edge type LDPC codes that were thought to be the best method for low-rate coding. The construction of these codes is very simple, and there is no need to design codes of different rates. Only a regular non-binary LDPC code, used as mother code, is required. Lower rate codes are then constructed from this mother code. They are also inherently rate-adaptive, which allows for an improved reconciliation efficiency when the channel parameter is estimated, as is the case with QKD. Furthermore, it has been shown that these codes perform well

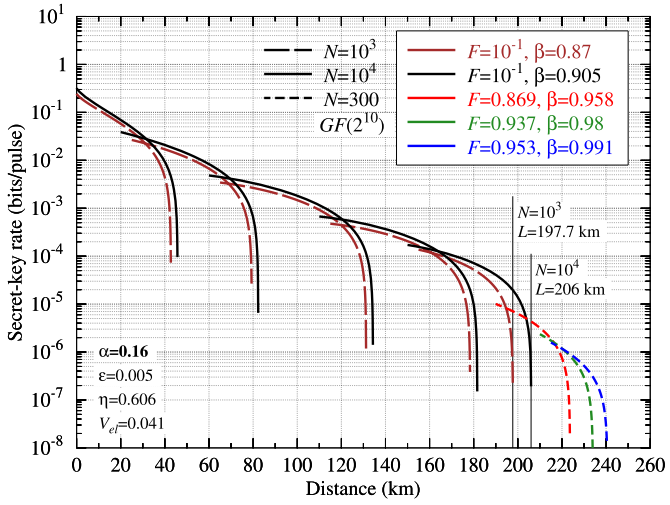

Figure 12 Secret-key rate for collective attacks with respect to the distance using an ultra-low loss fiber

even for short code lengths, and decoding has also been shown to perform with almost the same computational complexity as that of the mother code, thus making them suitable for hardware implementations. The only comparative drawback is the larger number of decoding iterations needed to ensure good efficiency.

As shown, the proposed codes are able to distill secret-keys from a single mother code of short and intermediate block-length, that by multiplicatively repeating symbols spans nearly the whole SNR range, that is, most distances. Additionally, very short block-length codes working in the high FER regime can likewise be used to distill secret-keys particularly for longer distances.

Author contributions

J.M. constructed the multiplicatively repeated non-binary LDPC codes and decoder, and performed the simulations. J.M. wrote the first version of the manuscript. J.M. and D.E. reviewed the main manuscript text and discussed the simulation results. J.M. and D.E. supervised this work.

Authors' information

Jesus Martinez-Mateo, jesus.martinez.mateo@upm.es.

Funding information

This research has been partially supported by the Ministerio de Ciencia e Innovación (MICINN), Government of Spain (grant PID2021-122905NB-C22). This work was partially supported by Japan's Council for Science, Technology and Innovation (CSTI) under the Cross-ministerial Strategic Innovation Promotion Program (SIP) for "Promoting the application of advanced quantum technology platforms to social issues" (grant JPJ012367).

Data availability

Data sets generated during the current study are available from the corresponding author on reasonable request.

Declarations

Competing interests

The authors declare no competing interests.

Author details

[1] Departamento de Matemática Aplicada a las Tecnologías de la Información y las Comunicaciones, Universidad Politécnica de Madrid, Boadilla del Monte, Spain. [2] Networked Quantum Devices Unit, Okinawa Institute of Science and Technology Graduate University, Onna, Japan.

Received: 25 February 2025 Accepted: 2 June 2025 Published online: 11 June 2025

References

1. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Rev Mod Phys. 2002;74(1):145–95. https://doi.org/10.1103/RevModPhys.74.145.
2. Brassard G, Salvail L. Secret-key reconciliation by public discussion. In: Eurocrypt'93, workshop on the theory and application of cryptographic techniques on advances in cryptology. Lecture notes in computer science. vol. 765. New York: Springer; 1994. p. 410–23.
3. Bennett CH, Brassard G, Roberts J-M. Privacy amplification by public discussion. SIAM J Comput. 1988;17(2):210–29. https://doi.org/10.1137/0217014.
4. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560:7–11. https://doi.org/10.1016/j.tcs.2014.05.025.
5. Elkouss D, Martinez-Mateo J, Martin V. Information reconciliation for quantum key distribution. Quantum Inf Comput 2011;11(3&4):226–38. https://doi.org/10.26421/QIC11.3-4-3.
6. Martinez-Mateo J, Elkouss D, Martin V. Blind reconciliation. Quantum Inf Comput 2012;12(9&10):791–812. https://doi.org/10.26421/QIC12.9-10-5.
7. Martinez-Mateo J, Elkouss D, Martin V. Key reconciliation for high performance quantum key distribution. Sci Rep. 2013;3(1576). https://doi.org/10.1038/srep01576.
8. Tarable A, Paganelli RP, Ferrari M. Rateless protograph ldpc codes for quantum key distribution. IEEE Trans Quantum Eng. 2024;5:1–11. https://doi.org/10.1109/TQE.2024.3361810.
9. Jouguet P, Kunz-Jacques S. High performance error correction for quantum key distribution using polar codes. Quantum Inf Comput 2014;14(3&4):329–38. https://doi.org/10.26421/QIC14.3-4-8.
10. Martinez-Mateo J, Pacher C, Peev M, Ciurana A, Martin V. Demystifying the information reconciliation protocol cascade. Quantum Inf Comput 2015;15(5&6):453–77. https://doi.org/10.26421/QIC15.5-6-6.
11. Pacher C, Grabenweger P, Martinez-Mateo J, Martin V. An information reconciliation protocol for secret-key agreement with small leakage. In: 2015 IEEE international symposium on information theory (ISIT). 2015. p. 730–4. https://doi.org/10.1109/ISIT.2015.7282551.
12. Van Assche G, Cardinal J, Cerf NJ. Reconciliation of a quantum-distributed Gaussian key. IEEE Trans Inf Theory. 2004;50(2):394–400. https://doi.org/10.1109/TIT.2003.822618.
13. Leverrier A, Alléaume R, Boutros J, Zémor G, Grangier P. Multidimensional reconciliation for a continuous-variable quantum key distribution. Phys Rev A. 2008;77:042325. https://doi.org/10.1103/PhysRevA.77.042325.
14. Jouguet P, Kunz-Jacques S, Leverrier A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. Phys Rev A. 2011;84:062317. https://doi.org/10.1103/PhysRevA.84.062317.
15. Jouguet P, Elkouss D, Kunz-Jacques S. High-bit-rate continuous-variable quantum key distribution. Phys Rev A. 2014;90:042329. https://doi.org/10.1103/PhysRevA.90.042329.
16. Bai Z, Yang S, Li Y. High-efficiency reconciliation for continuous variable quantum key distribution. Jpn J Appl Phys. 2017;56(4):044401. https://doi.org/10.7567/JJAP.56.044401.
17. 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. 2018;8(10543). https://doi.org/10.1038/s41598-018-28703-4.
18. Zhang Y, Chen Z, Pirandola S, Wang X, Zhou C, Chu B, Zhao Y, Xu B, Yu S, Guo H. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. Phys Rev Lett. 2020;125(1):010502. https://doi.org/10.1103/PhysRevLett.125.010502.
19. Mani H, Gehring T, Grabenweger P, Ömer B, Pacher C, Andersen UL. Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution. Phys Rev A. 2021;103:062419. https://doi.org/10.1103/PhysRevA.103.062419.
20. Jiang X-Q, Huang P, Huang D, Lin D, Zeng G. Secret information reconciliation based on punctured low-density parity-check codes for continuous-variable quantum key distribution. Phys Rev A. 2017;95:022318. https://doi.org/10.1103/PhysRevA.95.022318.
21. Wang X, Zhang Y, Li Z, Xu B, Yu S, Guo H. Efficient rate-adaptive reconciliation for continuous variable quantum key distribution. Quantum Inf Comput 2017;17(13&14):1123–34. https://doi.org/10.26421/QIC17.13-14-4.
22. Jeong S, Jung H, Ha J. Rate-compatible multi-edge type low-density parity-check code ensembles for continuous-variable quantum key distribution systems. npj Quantum Inf. 2022;8(6). https://doi.org/10.1038/s41534-021-00509-9.
23. Milicevic M, Feng C, Zhang LM, Gulak PG. Quasi-cyclic multi-edge ldpc codes for long-distance quantum cryptography. npj Quantum Inf. 2018;4(21). https://doi.org/10.1038/s41534-018-0070-6.
24. Johnson SJ, Chandrasetty VA, Lance AM. Repeat-accumulate codes for reconciliation in continuous variable quantum key distribution. In: 2016 Australian communications theory workshop (AusCTW). 2016. p. 18–23. https://doi.org/10.1109/AusCTW.2016.7433603.
25. Shirvanimoghaddam M, Johnson SJ, Lance AM. Design of raptor codes in the low snr regime with applications in quantum key distribution. In: 2016 IEEE international conference on communications (ICC). 2016. p. 1–6. https://doi.org/10.1109/ICC.2016.7510800.
26. Zhou C, Wang X, Zhang Y, Zhang Z, Yu S, Guo H. Continuous-variable quantum key distribution with rateless reconciliation protocol. Phys Rev Appl. 2019;12:054013. https://doi.org/10.1103/PhysRevApplied.12.054013.
27. Zhang M, Wang Q, Son T, Kim S. Evaluation of adaptive reconciliation protocols for cv-qkd using systematic polar codes. Quantum Inf Process. 2004;23(157). https://doi.org/10.1007/s11128-024-04371-4.
28. Lucamarini M, Yuan ZL, Dynes JF, Shields AJ. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature. 2018;557(7705):400–3. https://doi.org/10.1038/s41586-018-0066-6.
29. Chen J-P, Zhang C, Liu Y, Jiang C, Zhang W, Hu X-L, Guan J-Y, Yu Z-W, Xu H, Lin J, Li M-J, Chen H, Li H, You L, Wang Z, Wang X-B, Zhang Q, Pan J-W. Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km. Phys Rev Lett. 2020;124:070501. https://doi.org/10.1103/PhysRevLett.124.070501.
30. Wang S, Yin Z-Q, He D-Y, Chen W, Wang R-Q, Ye P, Zhou Y, Fan-Yuan G-J, Wang F-X, Zhu Y-G, Morozov PV, Divochiy AV, Zhou Z, Guo G-C, Han Z-F. Twin-field quantum key distribution over 830-km fibre. Nat Photonics. 2022;16(2):154–61. ISSN 1749-4893. https://doi.org/10.1038/s41566-021-00928-2.

31. Liu Y, Zhang W-J, Jiang C, Chen J-P, Zhang C, Pan W-X, Ma D, Dong H, Xiong J-M, Zhang C-J, et al. Experimental twin-field quantum key distribution over 1000 km fiber distance. Phys Rev Lett. 2023;130(21):210801. https://doi.org/10.1103/PhysRevLett.130.210801.
32. Ferraz O, Subramaniyan S, Chinthala R, Andrade J, Cavallaro JR, Nandy SK, Silva V, Zhang X, Purnaprajna M, Falcao G. A survey on high-throughput non-binary ldpc decoders: asic, fpga, and gpu architectures. IEEE Commun Surv Tutor. 2022;24(1):524–56. https://doi.org/10.1109/COMST.2021.3126127.
33. Gallager RG. Low-density parity-check codes. Cambridge: MIT Press; 1963.
34. MacKay DJC, Neal RM. Near Shannon limit performance of low density parity check codes. Electron Lett. 1996;32(18):1645–6. https://doi.org/10.1049/el:19961141.
35. MacKay DJC. Good error-correcting codes based on very sparse matrices. IEEE Trans Inf Theory. 1999;45(2):399–431. https://doi.org/10.1109/18.748992.
36. Richardson TJ, Shokrollahi MA, Urbanke RL. Design of capacity-approaching irregular low-density parity-check codes. IEEE Trans Inf Theory. 2001;47(2):619–37. https://doi.org/10.1109/18.910578.
37. Davey MC, MacKay DJC. Low density parity check codes over GF(q). In: IEEE information theory workshop (ITW). 1998. p. 70–1. https://doi.org/10.1109/ITW.1998.706440.
38. Barnault L, Declercq D. Fast decoding algorithm for LDPC over GF(2^q). In: ITW 2003, IEEE inf. theory workshop. IEEE; 2003. p. 70–3. https://doi.org/10.1109/ITW.2003.1216697.
39. Voicila A, Declercq D, Verdier F, Fossorier M, Urard P. Low-complexity decoding for non-binary LDPC codes in high order fields. IEEE Trans Commun. 2010;58(5):1365–75. https://doi.org/10.1109/TCOMM.2010.05.070096.
40. Richardson TJ, Urbanke RL. The capacity of low-density parity-check codes under message-passing decoding. IEEE Trans Inf Theory. 2001;47(2):599–618. https://doi.org/10.1109/18.910577.
41. Chung S-Y, Forney GD Jr, Richardson TJ, Urbanke RL. On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit. IEEE Commun Lett. 2001;5(2):58–60. https://doi.org/10.1109/4234.905935.
42. Poulliat C, Fossorier M, Declercq D. Design of regular $(2, d_c)$-LDPC codes over GF(q) using their binary images. IEEE Trans Commun. 2008;56(10):1626–35. https://doi.org/10.1109/TCOMM.2008.060527.
43. Kasai K, Matsumoto R, Sakaniwa K. Information reconciliation for QKD with rate-compatible non-binary LDPC codes. In: IEEE international symposium on information theory and its applications (ISITA). 2010. p. 922–7. https://doi.org/10.1109/ISITA.2010.5649550.
44. Mueller R, Ribezzo D, Zahidy M, Oxenløwe LK, Bacco D, Forchhammer S. Efficient information reconciliation for high-dimensional quantum key distribution. Quantum Inf Process. 2024;23(5):195. ISSN 1573-1332. https://doi.org/10.1007/s11128-024-04395-w.
45. Kiktenko EO, Trushechkin AS, Lim CCW, Kurochkin YV, Fedorov AK. Symmetric blind information reconciliation for quantum key distribution. Phys Rev Appl. 2017;8:044017. https://doi.org/10.1103/PhysRevApplied.8.044017.
46. Liu Z, Wu Z, Huang A. Blind information reconciliation with variable step sizes for quantum key distribution. Sci Rep. 2020;10(1):171. https://doi.org/10.1038/s41598-019-56637-y.
47. Andriyanova I, Tillich J-P. Designing a good low-rate sparse-graph code. IEEE Trans Commun. 2012;60(11):3181–90. https://doi.org/10.1109/TCOMM.2012.082712.100205.
48. Richardson TJ, Urbanke RL. Multi-edge type LDPC codes. Submitted IEEE IT, LTHC-REPORT-2004. 2004.
49. Johnson SJ, Lance AM, Ong L, Shirvanimoghaddam M, Ralph TC, Symul T. On the problem of non-zero word error rates for fixed-rate error correction codes in continuous variable quantum key distribution. New J Phys. 2017;19(2):023003. https://doi.org/10.1088/1367-2630/aa54d7.
50. Jeong S, Ha J. On the design of multi-edge type low-density parity-check codes. IEEE Trans Commun. 2019;67(10):6652–67. https://doi.org/10.1109/TCOMM.2019.2927567.
51. Pacher C, Martinez-Mateo J, Duhme J, Gehring T, Furrer F. Information reconciliation for continuous-variable quantum key distribution using non-binary low-density parity-check codes. 2016.
52. Kasai K, Declercq D, Poulliat C, Sakaniwa K. Multiplicatively repeated nonbinary LDPC codes. IEEE Trans Inf Theory. 2011;57(10):6788–95. https://doi.org/10.1109/TIT.2011.2162259.
53. Pearl J. Probabilistic reasoning in intelligent systems: networks of plausible inference. San Mateo: Morgan Kaufmann; 1988.
54. Slepian D, Wolf J. Noiseless coding of correlated information sources. IEEE Trans Inf Theory. 1973;19(4):471–80. https://doi.org/10.1109/TIT.1973.1055037.
55. Wyner A. On source coding with side information at the decoder. IEEE Trans Inf Theory. 1975;21(3):294–300. https://doi.org/10.1109/TIT.1975.1055374.
56. Liveris AD, Xiong Z, Georghiades CN. Compression of binary sources with side information at the decoder using LDPC codes. IEEE Commun Lett. 2002;6(10):440–2.
57. Declercq D, Fossorier M. Decoding algorithms for nonbinary LDPC codes over GF(q). IEEE Trans Commun. 2007;55(4):633–43. https://doi.org/10.1109/TCOMM.2007.894088.
58. Wei K, Garg D, Nagai R, Tomono T, Amano H. Fpt-ems: an fpga implementation using nb-ldpc code for continuous-variable quantum key distribution. In: Proceedings of the 15th international symposium on highly efficient accelerators and reconfigurable technologies. 2025. p. 117–25.
59. Yang S, Yan Z, Yang H, Lu Q, Lu Z, Cheng L, Miao X, Li Y. Information reconciliation of continuous-variables quantum key distribution: principles, implementations and applications. EPJ Quantum Technol. 2023;10(1):40. https://doi.org/10.1140/epjqt/s40507-023-00197-8.
60. Laudenbach F, Pacher C, Fung C-HF, Poppe A, Peev M, Schrenk B, Hentschel M, Walther P, Hübel H. Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations (adv. Quantum technol. 1/2018). Adv Quantum Technol. 2018;1(1):1870011. https://doi.org/10.1002/qute.201870011.
61. Leverrier A. Information reconciliation for discretely-modulated continuous-variable quantum key distribution. 2023. https://arxiv.org/abs/2310.17548.
62. Shokrollahi A, Storn R. Design of efficient erasure codes with differential evolution. In: IEEE international symposium on information theory (ISIT). 2000. p. 1–5. https://doi.org/10.1109/ISIT.2000.866295.
63. Rathi V, Urbanke R. Density evolution, thresholds and the stability condition for non-binary ldpc codes. IEE Proc, Commun. 2005;152:1069. https://doi.org/10.1049/ip-com:20050230.

64. Hu X-Y, Eleftheriou E, Arnold DM. Regular and irregular progressive edge-growth Tanner graphs. IEEE Trans Inf Theory. 2005;51(1):386–98. https://doi.org/10.1109/TIT.2004.839541.
65. Tomamichel M, Martinez-Mateo J, Pacher C, Elkouss D. Fundamental finite key limits for one-way information reconciliation in quantum key distribution. Quantum Inf Process. 2017;16(11):280. https://doi.org/10.1007/s11128-017-1709-5.
66. Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf NJ, Tualle-Brouri R, McLaughlin SW, Grangier P. Quantum key distribution over 25 km with an all-fiber continuous-variable system. Phys Rev A. 2007;76:042305. https://doi.org/10.1103/PhysRevA.76.042305.
67. Leverrier A, Grosshans F, Grangier P. Finite-size analysis of a continuous-variable quantum key distribution. Phys Rev A. 2010;81:062343. https://doi.org/10.1103/PhysRevA.81.062343.

Publisher's note