Scientific Research Publishing

Journal of Information Security, 2022, 13, 257-271
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Low-Density Parity-Check Codes: Research Status and Development Direction

Jie Xu, Zhiyong Zheng, Kun Tian*

Engineering Research Center of Ministry of Education for Financial Computing and Digital Engineering,
Renmin University of China, Beijing, China

Email: *tkun19891208@ruc.edu.cn

How to cite this paper: Xu, J., Zheng, Z.Y. and Tian, K. (2022) Low-Density Parity-Check Codes: Research Status and Development Direction. *Journal of Information Security*, **13**, 257-271.
https://doi.org/10.4236/jis.2022.134014

Received: August 20, 2022
Accepted: September 20, 2022
Published: September 23, 2022

Abstract

In this paper, we conclude five kinds of methods for construction of the regular low-density parity matrix *H* and three kinds of methods for the construction of irregular low-density parity-check matrix *H*. Through the analysis of the code rate and parameters of these eight kinds of structures, we find that the construction of low-density parity-check matrix tends to be more flexible and the parameter variability is enhanced. We propose that the current development cost should be lower with the progress of electronic technology and we need research on more practical Low-Density Parity-Check Codes (LDPC). Combined with the application of the quantum distribution key, we urgently need to explore the research direction of relevant theories and technologies of LDPC codes in other fields of quantum information in the future.

Keywords

Low-Density Parity-Check (LDPC), Parity Check Matrix *H*, Quasi-Cyclic (QC) LDPC, Spatially Coupled Low-Density Parity-Check (SC-LDPC) Codes

1. Introduction

LDPC code is a forward error correction code, which was invented by Robert Gallager in his doctoral dissertation at MIT in the 1960s [1]. Although LDPC code is one of the most practical realizations of Shannon's theory [2], with high computational complexity for forwarding error correction and highly structured algebraic block codes and convolutional codes, LDPC codes have been neglected for a long time.

Until about 30 years after the LDPC code's invention, MacKay and Neal in [3] proved that LDPC code has the performance of approaching the Shannon limit under the condition of combining iterative decoding based on belief pmpagation

[4]. After many researchers invented a new irregular LDPC code, which is called the new generalization of Gallager's LDPC code, and its performance is better than the best turbo code with certain practical advantages. LDPC code has once again entered the seriousness of the world and stepped on the stage of history.

In [5], T. J. Richardson *et al.* have also made great contributions to the development of LDPC codes. Firstly, they propose a new coding algorithm, which greatly reduces the huge computational and storage requirements of randomly constructed LDPC codes. Secondly, they invent the density evolution theory, which can effectively analyze the decoding threshold of a large class of LDPC decoding algorithms. Simulation results show that this is a compact decoding threshold. Finally, they prove density evolution theory can also be used to guide the design of irregular LDPC codes to obtain the best performance possible.

LDPC code has great application potential and will be widely used in deep space communication, optical fiber communication, satellite digital video (see [6] [7] [8]), digital watermark, magnetic/optical/holographic storage, mobile and fixed wireless communication, cable modulator/demodulator and digital subscriber line (for more details see [9] and [10]).

LDPC code chips have been developed in the industry. Among them, the vector LDPC solution based on ASIC launched by Flarion, which is in the leading position, uses about 2.6 million gates, can support a maximum code length of 50,000, a code rate of 0.9, and the maximum number of iterations is 10. The decoder can achieve a throughput of 10 Gbps. Its performance has been very close to the Shannon limit, and can meet the needs of most communication services at present. AHA and digital fountain have also launched their own coding and decoding solutions.

A large number of qubits and gate operations on them are involved in most practical applications of quantum computing. There is also practical use of single qubits. C. H. Bennett and G. Brassard in [11] give a surprisingly secure way of distributing a cryptographic key using a sequence of individual qubits called BB84 protocol, which is already available commercially. Quantum Key Distribution (QKD) is a secure way of distributing an encryption and decryption key by making use of qubits. The sender and the receiver can detect a possible third party eavesdropping on their communication by comparing the sequence sent with that of the received one. LDPC codes have other many applications in QKD. We will give some examples in Section IV.

In recent years, international theoretical research on LDPC has made important progress. X. Zheng in [12] designed short-length LDPC codes with the aim to shorten the average distance between any two variable nodes. In [13], Chung *et al.* presented a block length (ten million bits) rate-LDPC code that achieves reliable performance—a bit error rate—on an additive white Gaussian noise channel with a signal-to-noise ratio within 0.04 dB of the Shannon limit. There are also many excellent researches on encoding (see [14] [15] [16]), decoding (see [17] [18]) and the rate of various LDPC codes (see [19] [20]).

In general, from the existing research, the construction of LDPC codes determines the efficiency of its application in various fields. Since LDPC codes have extremely important research significance in the coding field, most of the existing studies focus on a specific type of LDPC codes, and few comparative studies on the overall structure of LDPC codes. Therefore, this paper focuses on the construction methods of LDPC codes and summarizes the mainstream construction methods in depth, so as to help researchers interested in this field to provide a more comprehensive and faster way.

Basic Principles and the LDPC Code Related Terminology

Definition 1.1 A q-ary linear code C is a linear subspace of F_q^n. If C has dimension k then C is called a $[n,k]$ code.

Definition 1.2 A generator matrix G for a linear code C is a k by n matrix for which the rows are a basis of C.

Remark 1.1

1) If G is a generator matrix for C, then $C=\{aG \mid a\in Q^k\}$.

2) If $G=(I_k P)$, where I_k is the k by k identity matrix, we shall say G is in standard form. Then the first k symbols of a codeword are called information symbols. These can be chosen arbitrarily and then the remaining symbols, which are called parity check symbols, are determined.

Definition 1.3 For a linear code $C\subset F_q^n$, let

$$C^{\perp}=\{y\in\mathbb{R} \mid \forall x\in C[\langle x,y\rangle=0]\}.$$

A generator matrix H for $C^{\perp}$ is called a parity check matrix of C.

In other words, if a matrix H is a parity check matrix of C, then

Definition 1.4 LDPC code is a linear error correction code that has a parity check matrix H, which is sparse, *i.e.*, with less nonzero elements in each row and column [1].

LDPC codes can be categorized into regular and irregular LDPC codes.

$$\forall x\in C \Leftrightarrow xH^{\mathrm{T}}=0$$

Definition 1.5 Let C is a LDPC code, if the parity check matrix $H_{(n-k)\times k}$ has the same number n_c of ones in each column and the same number w_r of ones in each row, we call C is a regular LDPC, write as (n_c,n_r). If LDPC code's length is n, it can be denoted as (n,w_c,w_r).

Definition 1.6 Let C is a LDPC code, if the parity check matrix $H_{(n-k)\times k}$ has the different number n_c of ones in each column and the same number w_r of ones in each row, we call C is an irregular LDPC.

The original Gallager codes [4] are regular binary LDPC codes. The size of H is usually very large, but the density of nonzero element is very low.

Definition 1.7

Let $C=\{c_1,c_2,\cdots,c_{|C|}\}$, $V=\{v_1,v_2,\cdots,v_{|V|}\}$ and E are the sets of check nodes, variable nodes, and edges, respectively. The (small) bipartite graph $G=(V\cup C,E)$ is called an LDPC figure. For every check node $\in C$, we denote by d_C its edge degree. Similarly, we write d_V for the edge degree of a variable node $\in V$.

A Tanner graph is generated from a figure G by a lifting ("copy-and-permute") operation specified by a lifting parameter L (for more details see [3] [21] [22] [23]). The design rate of the derived LDPC code is independent of L and given by $R_G = 1 - |C|/|V|$.

The following sections of this paper will introduce the structure and optimization of parity check matrix H for LDPC, some applications of LDPC in QKD, and the prediction of the development trend of LDPC codes in the future.

2. Construction of Parity Check Matrix *H*

In this section, we show the constructions for various LDPC codes. Since LDPC code is completely specified by its parity-check matrix, an ensemble of LDPC code usually is defined in terms of an ensemble of the parity-check matrix.

2.1. Construction of *H* for Regular LDPC

1) Gallager Method for Random Construction of H for LDPC

In RG Gallager's method [24], the transpose of regular (n, w_c, w_r) parity check matrix H has the form

$$H^{\mathrm{T}} = \left[H_1^{\mathrm{T}}, H_2^{\mathrm{T}}, \cdots, H_{w_c}^{\mathrm{T}}\right] \tag{2.1}$$

The matrix H_1 has n columns and n/w_r rows. The H_1 contains a single 1 in each column and contains 1 s in its i row from column $(i-1)w_r + 1$ to column iw_r. Permuting randomly the columns of H_1 with equal probability, the matrices H_2 to H_{w_c} are obtained.

Example 2.1. The parity check matrix for [20, 3, 4] code constructed by Gallager [25] is given as elements $a = 2$, $b = 5$ are chosen from GF (31); then $o(a) = 5$, $o(b) = 3$, and the parity-check matrix is given by

$$H = \begin{pmatrix}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}_{15\times 20} \tag{2.2}$$

2) Algebraic Construction of H for LDPC [1]

The construction of the parity check matrix H using algebraic construction as follows [26] [27]. Consider an identity matrix I_a where $a > (w_c - 1)(w_r - 1)$ and obtain the following matrix by cyclically shifting the rows of the identity matrix I_a one position to the right.

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 1 \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \tag{2.3}$$

Defining $A_0 = I_a$, the parity check matrix H can be constructed as

$$H = \begin{pmatrix} A^0 & A^0 & A^0 & \cdots & A^0 \\ A^0 & A^1 & A^2 & \cdots & A^{(w_r-1)} \\ A^0 & A^2 & A^4 & \cdots & A^{2(w_r-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A^0 & A^{(w_c-1)} & A^{2(w_c-1)} & \cdots & A^{(w_c-1)(w_r-1)} \end{pmatrix} \tag{2.4}$$

The constructed H matrix has $w_c a$ rows and $w_r a$ columns, and it is of a regular $[w_r a, w_c, w_r]$ having the same number of w_r ones in each row and the same number of w_c ones in each column. It is four-cycle free construction. The algebraic LDPC codes are easier for decoding than random codes. For intermediate *n*, well-designed algebraic codes yield a low bit error ratio (see [28] [29]).

Example 2.2. Construct H matrix with $w_c = 3$ and $w_r = 4$ using algebraic construction method.

Since $(w_c - 1)(w_r - 1)$, then

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{2.5}$$

then

$$H = \begin{pmatrix} A^0 & A^0 & A^0 & A^0 \\ A^0 & A^1 & A^2 & A^3 \\ A^0 & A^2 & A^4 & A^6 \end{pmatrix}, \tag{2.6}$$

R. M. Tanner [30] *et al.* also give a construction of H for quasi-cyclic (QC) LDPC. They use the structure of multiplicative groups in the set of integers modulo to "place" circulant matrices within a parity-check matrix so as to form regular QC LDPC block codes with a variety of block lengths and rates. For prime, the integers form a field under addition and multiplication the Galois

Field GF (m). The nonzero elements of GF (m) form a cyclic multiplicative group. Let a and b be two nonzero elements with orders $o(a)=k$ and $o(b)=j$, respectively. Then a matrix H can be formed as shown in the following:

$$H=\begin{pmatrix} I_1 & I_a & I_{a^2} & \cdots & I_{a^{k-1}} \\ I_b & I_{ab} & I_{a^2b} & \cdots & I_{a^{k-1}b} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ I_{b^{j-1}} & I_{ab^{j-1}} & I_{a^2b^{j-1}} & \cdots & I_{a^{k-1}b^{j-1}} \end{pmatrix}, \tag{2.7}$$

where I_x is an $m\times m$ identity matrix with rows cyclically shifted to the left by x positions. The resulting binary parity-check matrix is of size $jm\times km$, which means the associated code has a rate $R\geq 1-\frac{j}{k}$. By construction, every column of contains ones and every row contains ones, and so represents a regular LDPC code. (Hakimi *et al.* in [31] has proposed the graph-theoretic error-correcting codes for the case $j=2$.)

Example 2.3. A [155, 20, 64] QC code (m = 31) [5].

Elements $a=2$, $b=5$ are chosen from $GF(31)$; then $o(a)=5$, $o(b)=3$, and the parity-check matrix is given by

$$H=\begin{pmatrix} I_1 & I_2 & I_4 & I_8 & I_{16} \\ I_5 & I_{10} & I_{20} & I_9 & I_{18} \\ I_{25} & I_{19} & I_7 & I_{14} & I_{28} \end{pmatrix}_{(93\times 155)}, \tag{2.8}$$

where I_x is an 31×31 identity matrix with rows cyclically shifted to the left by x positions.

For nonprime m, the set of nonnegative integers less than m and relatively prime to m, $\mathbb{Z}_m^*$, forms a multiplicative group. In general, $\mathbb{Z}_m^*$ has order

$$\phi(m)=m\prod_{p|m,\,p\text{ is prime}}\left(1-\frac{1}{p}\right), \tag{2.9}$$

i.e. the Euler "phi" function.

Example 2.4. A [104, 30] QC code (m = 26) [30].

Elements $a=5$, $b=9$ are chosen from $\mathbb{Z}_{26}^*$; then $o(a)=4$, $o(b)=3$, and the parity-check matrix is given by

$$H=\begin{pmatrix} I_1 & I_5 & I_{25} & I_{21} \\ I_9 & I_{19} & I_{17} & I_7 \\ I_3 & I_{15} & I_{23} & I_{11} \end{pmatrix}_{(78\times 104)}, \tag{2.10}$$

where I_x is an 26×26 identity matrix with rows cyclically shifted to the left by x positions.

3) Construction of H for Rugular Spatially Coupled (SC) LDPC.

E. Ram and Y. Cassuto in [32] give an (l,r)-regular SC-LDPC protograph, which is constructed by coupling together a number of (l,r)-regular protographs and truncating the resulting chain. This coupling operation introduces a convolutional structure to the code, which can be visualized through the matrix representation of the protograph. Let $H=1_{(l,r)}$ be an all-ones base matrix representing an (l,r)-regular LDPC protograph, and let $(H_\tau)_{\tau=0}^{T}$ be binary matrices such that $H=\sum_{\tau=0}^{T}H_r$ (in this paper, we consider only binary H matrices). Coupling a limitless number of copies of H amounts to diagonally placing copies of $\left(H_0;H_1;\cdots;H_T\right)$ ('; ' represents vertical concatenation) as follows:

$$\begin{pmatrix} H_0 & & \\ H_1 & H_0 & \ddots \\ \vdots & H_1 & \ddots \\ H_T & \vdots & \ddots \\ & H_T & \ddots \\ & & \ddots \end{pmatrix}. \tag{2.11}$$

By truncating the above infinite matrix at some width, and removing all-zero rows, a spatially coupled LDPC protograph is constructed. Compared with the code set corresponding to the basic matrix *H*, this truncation leads to a small number of terminating check nodes (to a lower extent), which leads to a decrease in the design rate and an increase in the decoding threshold. However, with the increase of the coupling chain length, the design rate of the coupling prototype graph converges to the design rate of the underlying code set, and its belief propagation threshold shows a phenomenon called threshold saturation [31], so it converges to the maximum a posteriori probability threshold of the underlying code set.

Example 2.5. A spatially coupled $(3,6)$ protograph with 18 variable nodes. The protograph is generated by

$$H_0=\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \tag{2.12}$$

and $B_1=1^{3\times6}-B_0$. The design rate of the coupled protograph is $R=0.389$, and the belief propagation threshold is 0.512 (for more details see [33] [34]).

2.2. Construction of *H* for Irregular LDPC

1) Construction of *H* for Irrugular QC LDPC.

R. M. Tanner, D. Sridhara, A. Sridharan, *et al.* in [30] choose a regular (j,k) parity check matrix H at first. Then for $0\le i\le j-3$, they replace the last $(j-1-i)$ circulant submatricess in the row of circulant submatrices with all-zero matrices. The modified parity-check matrix $\tilde{H}$ is as follows:

$$\begin{pmatrix} I_1 & \cdots & I_{a^{k-j-1}} & I_{a^{k-j}} & 0 & \cdots & 0 & 0 & 0 \\ I_b & \cdots & I_{a^{k-j-1}b} & I_{a^{k-j}b} & I_{a^{k-j+1}b} & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ I_{b^{j-3}} & \cdots & I_{a^{k-j-1}b^{j-3}} & I_{a^{k-j}b^{j-3}} & I_{a^{k-j+1}b^{j-3}} & \cdots & I_{a^{k-3}b^{j-3}} & 0 & 0 \\ I_{b^{j-2}} & \cdots & I_{a^{k-j-1}b^{j-2}} & I_{a^{k-j}b^{j-2}} & I_{a^{k-j+1}b^{j-2}} & \cdots & I_{a^{k-3}b^{j-2}} & I_{a^{k-2}b^{j-2}} & I_{a^{k-1}b^{j-2}} \\ I_{b^{j-1}} & \cdots & I_{a^{k-j-1}b^{j-1}} & I_{a^{k-j}b^{j-1}} & I_{a^{k-j+1}b^{j-1}} & \cdots & I_{a^{k-3}b^{j-1}} & I_{a^{k-2}b^{j-1}} & I_{a^{k-1}b^{j-1}} \end{pmatrix} \tag{2.13}$$

where 0 is the $m\times m$ all-zero matrix and the LDPC code is now irregular. The irregular codes are still QC, and hence their parity check matrices can be described efficiently and they can be used to generate LDPC convolutional codes (see Section II-B in [30]).

Example 2.6. A [155, 63] irregular QC code [30].

Consider the [155, 64, 20] QC code of **Example 3.1**. This irregular LDPC code with parity-check matrix given by

$$H=\begin{pmatrix} I_1 & I_2 & I_4 & 0 & 0 \\ I_5 & I_{10} & I_{20} & I_9 & I_{18} \\ I_{25} & I_{19} & I_7 & I_{14} & I_{28} \end{pmatrix}_{(93\times 155)}, \tag{2.14}$$

where I_x is an 31×31 identity matrix with rows cyclically shifted to the left by *x* positions and 0 is the 31×31 all-zero matrix (for more details also can see [35] [36] [37] [38]).

2) Construction of LDPC Convolutional Codes

R. M. Tanner *et al.* in [30] proved an LDPC convolutional code can be constructedy by replicating the constraint structure of the QC LDPC block code to infinity. They gave the specific construction process as follows.

Each circulant in the parity-check matrix of a QC block code can be specified by a unique polynomial; the polynomial represents the entries in the first column of the circulant matrix. For example, a circulant matrix whose first column is $[111010]^{\mathrm{T}}$ is represented by the polynomial $1+D+D^2+D^4$. Thus, the $jm\times km$ binary parity-check matrix of a regular LDPC code obtained from the construction described above can be expressed in polynomial form (with indeterminate *D*) to obtain $j\times k$ matrix

$$H(D)=\begin{pmatrix} D & D^{a} & D^{a^2} & \cdots & D^{a^{k-1}} \\ D^{b} & D^{ab} & D^{a^2b} & \cdots & D^{a^{k-1}b} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ D^{b^{j-1}} & D^{ab^{j-1}} & D^{a^2b^{j-1}} & \cdots & D^{a^{k-1}b^{j-1}} \end{pmatrix}_{(j\times k)}. \tag{2.15}$$

The rate of the LDPC convolutional codes obtained from the QC codes was $R=1-\dfrac{j}{k}$.

Example 2.7. A rate $\dfrac{2}{5}$ LDPC convolutional code.

From the [155, 64, 20] QC code in **Example 2.1**, a rate $\dfrac{2}{5}$ convolutional code with parity-check and generator matrices given by

$$H(D)=\begin{pmatrix} D & D^2 & D^4 & D^8 & D^{16} \\ D^5 & D^{10} & D^{20} & D^9 & D^{18} \end{pmatrix}_{(2\times 5)}. \tag{2.16}$$

3) Construction of IrRugular SC LDPC.

H. Esfahanizadeh, E. Ram and Y. Cassuto in [39] propose two protograph constructions for local codes of a SC-LDPC code with sub-block locality and parameters γ_L, κ, and ν, where $\nu\in[0,\kappa-1]$ is the number of zero circulants per local code.

For integers *l*, *k*, and *i* such that $0 \le i < l$, let $Q(l,k;i)$ and $S(l,k)$ be $l \times k$ matrices, such that

$$[Q(l,k;i)]_{s,t} = \begin{cases} 0, s = i \\ 1, \text{otherwise} \end{cases} \tag{2.17}$$

$$[S(l,k)]_{s,t} = \begin{cases} 0, s \in [0,k), t = k - s - 1 \\ 1, \text{otherwise} \end{cases}. \tag{2.18}$$

Let $1(l,k)$ be an all-one matrix and $0(l,k)$ be an all-zero matrix with size $l \times k$, and let $\nu = a\gamma_L + b$ with integers *a*, *b* such that $0 \le b < \gamma_L$. The balanced and unbalanced local code constructions are represented by the protograph matrices B_β and B_U, respectively, and defined as follows:

$$B_\beta = (1(\gamma_L, \kappa - \nu), S(\gamma_L, b), Q(\gamma_L, a; \gamma_L - 1), \cdots, Q(\gamma_L, a; 0)), \tag{2.19}$$

$$B_U = (1(\gamma_L, \kappa - \nu), Q(\gamma_L, \nu; 0)), \tag{2.20}$$

where the vertical dashed lines represent the horizontal concatenation of sub-matrices. B_β and B_U are both $\gamma_L \times \nu$ matrices with ν zero entries; in B_β, zeros are uniformly distributed among the rows, while in B_U, all zeros are in the first row.

Example 2.8. Let $\gamma_L = 3$, $\kappa = 13$, $\nu = 10$. Then,

$$B_\beta = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \tag{2.21}$$

$$B_U = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{2.22}$$

3. LDPC's Application in QKD

Currently, there are two mainstream schemes for QKD research, namely, discrete-variable QKD (DV-QKD) and continuous variable QKD (CV-QKD) (see [40]). In DV-QKD systems, the polarization or phase of a single-photon state is encoded by key information, whereas in CV-QKD systems, the amplitude and phase quadrature of quantum states are encoded.

In typical DV-QKD protocols as, e.g. the Bennett-Brassard 1984 (BB84) protocol [11], the raw key is bit-wise encoded for the quantum communication. Hence, standard binary codes, which are highly efficient and have a large throughput, can be used for information reconciliation (for more details see [41] [42] [43] [44] [45]). Based on the belief propagation decoding of LDPC codes over Galois fields of the form GF (2*q*) (see [46] [47] [48]), C. Pacher, J. Martinez-Mateo, J. Duhme *et al.* give an information reconciliation method for continuous-variable quantum key distribution with Gaussian modulation that is based on non-binary LDPC codes in [49] (for more details see [50] [51] [52] [53] [54]).

The CV-QKD system offers good application prospects for the implementation of classical telecom components, which attracting considerable researcher's attention. Research activities have primarily focused on extending the transmission distance and improving secret key rate between two parties in the CV-QKD systems. For example, N. Hosseinidehaj and R. Malaney in [55] investigate the role played by the Gaussian CV states as compared to non-Gaussian states. They find that beam-wandering induced atmospheric losses results in QKD performance levels that are in general quite different from those found in fixed-attenuation channels. Their findings show that the nature of the atmospheric channel can have a large impact on the QKD performance. Y. Shen *et al.* give an on-chip continuous-variable quantum key distribution (CV-QKD) system, which is integrated using silicon photonics fabrication process and demonstrates the capability of transceiving Gaussian-modulated coherent states and homodyne detection in [56].

MET-LDPC codes (see [10] [57]) exhibiting low rates combined with the reverse multidimensional reconciliation scheme can achieve excellent correction performance in the CV-QKD system. The signal-to-noise ratio (SNR) of an optical quantum channel is low in such a long distance transmission, thus requiring a low code rate and long code block length. For example, when the SNR is less than 15 dB, the code rate is less than 0.02 and the block length has an order of 106 [58]. However, designing a parity-check matrix with good performance is complex, and it is extremely complicated to design all matrices for different SNRs [59]. Therefore, to improve the reconciliation efficiency, the system must change the modulation variance at Alice's side to ensure the receiving variables achieve the target SNR. The frame error rate and post-processing speed must also be considered in the practical application of the CV-QKD system (see [60] [61]). Multiple interactions and decoding steps of Alice and Bob in the information reconciliation step will increase system delay. In [59], C. Zhou, X. Y. Wang, Z. G. Zhang, *et al.* introduce Raptor-like LDPC codes into the continuous-variable quantum key distribution system, exhibiting both the rate compatible property of the Raptor code and capacity-approaching performance of Multi-Edge Type Low-Density Parity-Check (MET-LDPC) codes.

4. Potential Future Research Directions

N. Bonello, S. Chen, and L. Hanzo in [62] have offered a glimpse of six decades of research pertaining to LDPC codes as well as the more recent efforts concentrated on rateless coding. Ten years later, based on the improvement of LDPC code construction in recent ten years, this paper gives the following predictions:

- With the progress of electronic technology, the implementation of traditional LDPC code is no longer a difficult problem. However, due to the complexity of LDPC code structure, the current cost is still high, which limits its practicability. Therefore, how to simplify the algebraic structure of check matrix and how to improve coding and decoding algorithms are still the focus of future research (for more details can see [63]).
- Many cryptologists have given many different versions of LDPC code in the

research of the theory and application of quantum key distribution (like [64]). It can be seen that LDPC code still plays an indispensable and important role in the quantum era. Therefore, the application of LDPC code in the efficient implementation of quantum key distribution and other fields of quantum information is also an important field of future research.

5. Conclusion

In this study, we give the most mainstream and classical construction methods of regular LDPC and irregular LDPC, give examples of construction to make the construction methods more specific and easy to understand, and give our views on future research trends, hoping to promote the research in this field.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Gallager, R.G. (1963) Low-Density Parity-Check Codes. MIT Press, Cambridge. https://doi.org/10.7551/mitpress/4347.001.0001

[2] Shannon, C.E. (1957) Certain Results in Coding Theory for Noisy Channels. *Information and Control*, **1**, 6-25. https://doi.org/10.1016/S0019-9958(57)90039-6

[3] MacKay, D.J.C. and Neal, R.M. (1995) Good Codes Based on Very Sparse Matrices, *IMA International Conference on Cryptography & Coding*, Cirencester, 17-19 December 1995, 100-111. https://doi.org/10.1007/3-540-60693-9_13

[4] Soleymani, M.R., Gao, Y. and Vilaipornsawai, U. (2002) Low Density Parity Check Codes. In: *Turbo Coding for Satellite and Wireless Communications*, Springer, Boston, 177-194. https://doi.org/10.1007/0-306-47677-0_9

[5] Richardson, T.J. and Urbanke, R.L. (2001) The Capacity of Low-Density Parity-Check Codes Under Message-Passing Decoding. *IEEE Transactions on Information Theory*, **47**, 599-618. https://doi.org/10.1109/18.910577

[6] Eroz, M. and Lee, L. (2005) Structured Low-Density Parity-Check Code Design for Next Generation Digital Video Broadcast. *MILCOM* 2005—2005 *IEEE Military Communications Conference*, Vol. 4, Atlantic, 17-20 October 2005, 2461-2466. https://doi.org/10.1109/MILCOM.2005.1606037

[7] Purnamasari, R., Wijanto, H. and Hidayat, I. (2014) Design and Implementation of LDPC (Low Density Parity Check) Coding Technique on FPGA (Field Programmable Gate Array) for DVB-S2 (Digital Video Broadcasting-Satellite). 2014 *IEEE International Conference on Aerospace Electronics and Remote Sensing Technology*, Yogyakarta, 13-14 November 2014, 83-88. https://doi.org/10.1109/ICARES.2014.7024407

[8] Van Nghia, T. (2016) Development of the Parallel BCH and LDPC Encoders Architecture for the Second Generation Digital Video Broadcasting Standards with Adjustable Encoding Parameters on FPGA, 2016 *International Conference on Engineering and Telecommunication* (*EnT*), Moscow, 29-30 November 2016, 104-109. https://doi.org/10.1109/EnT.2016.031

[9] IEEE Std. 1890-2018 (2019) IEEE Standard for Error Correction Coding of Flash Mem-

ory Using Low-Density Parity-Check Codes. Institute of Electrical and Electronics Engineers, Manhattan, 1-51.

[10] Wetcharungsri, J., Buabthong, N., Jantarachote, S., Sangwongngam, P. and Sripimanwat, K. (2013) Field-Programmable Gate Array Implementation of Low-Density Parity-Check Codes Decoder and Hardware Testbed. *IEEE 2013 Tencon—Spring*, Sydney, 17-19 April 2013, 104-107. https://doi.org/10.1109/TENCONSpring.2013.6584426

[11] Bennett, C.H. and Brassard, G. (1984) Quantum Cryptography: Public Key Distribution and Coin Tossing. *IEEE International Conference on Computers*, *Systems & Signal Processing*, Bangalore, 9-12 December 1984, 175-179.

[12] Zheng, X., Lau, F.C.M., Tse, C.K., He, Y. and Hau, S. (2009) Application of Complex-Network Theories to the Design of Short-Length Low-Density-Parity-Check Codes. *Communications IET*, **3**, 1569-1577. https://doi.org/10.1049/iet-com.2008.0503

[13] Chung, S.Y., Forney Jr., G.D., Richardson, T.J. and Urbanke, R. (2001) On the Design of Low-Density Parity-Check Codes within 0.0045 dB of the Shannon Limit. *IEEE Communications Letters*, **5**, 58-60. https://doi.org/10.1109/4234.905935

[14] Mahdi, A., Kanistras, N. and Paliouras, V. (2021) A Multirate Fully Parallel LDPC Encoder for the IEEE 802.11n/ac/ax QC-LDPC Codes Based on Reduced Complexity XOR Trees. *IEEE Transactions on Very Large Scale Integration* (*VLSI*) *Systems*, **29**, 51-64. https://doi.org/10.1109/TVLSI.2020.3034046

[15] Zhong, H. and Zhang, T. (2005) Block-LDPC: A Practical LDPC Coding System Design Approach. *IEEE Transactions on Circuits and Systems I*: *Regular Papers*, **52**, 766-775. https://doi.org/10.1109/TCSI.2005.844113

[16] Zhao, Y. and Lau, F.C.M. (2014) Implementation of Decoders for LDPC Block Codes and LDPC Convolutional Codes Based on GPUs. *IEEE Transactions on Parallel and Distributed Systems*, **25**, 663-672. https://doi.org/10.1109/TPDS.2013.52

[17] Amaricai, A., Stein, D. and Boncalo, O. (2020) Generalized Very High Throughput Unrolled LDPC Layered Decoder, 2020 28*th Telecommunications Forum* (TELFOR), Belgrade, 24-25 November 2020, 1-4. https://doi.org/10.1109/TELFOR51502.2020.9306537

[18] Chan, C.H. and Lau, F.C.M. (2012) Parallel Decoding of LDPC Convolutional Codes Using OpenMP and GPU. 2012 *IEEE Symposium on Computers and Communications* (*ISCC*), Cappadocia, 1-4 July 2012, 225-227. https://doi.org/10.1109/ISCC.2012.6249298

[19] Li, Y., Liu, B., Rong, B., Wu, Y., Gagnon, G., Gui, L., *et al.* (2013) Rate-Compatible LDPC-RS Product Codes Based on Raptor-Like LDPC Codes. 2013 *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting* (*BMSB*), London, 5-7 June 2013, 1-6. https://doi.org/10.1109/BMSB.2013.6621783

[20] Vafi, S. and Majid, N. (2016) Half Rate Quasi Cyclic Low Density Parity Check Codes Based on Combinatorial Designs. *Journal of Computer and Communications*, **4**, 39-49. https://doi.org/10.4236/jcc.2016.412002

[21] Dehghan, A. and Banihashemi, A.H. (2018) On the Tanner Graph Cycle Distribution of Random LDPC, Random Protograph-Based LDPC, and Random Quasi-Cyclic LDPC Code Ensembles. *IEEE Transactions on Information Theory*, **64**, 4438-4451. https://doi.org/10.1109/TIT.2018.2805906

[22] Mitchell, D.G.M., Lentmaier, M. and Costello, D.J. (2015) Spatially Coupled LDPC Codes Constructed from Protographs. *IEEE Transactions on Information Theory*, **61**, 4866-4889. https://doi.org/10.1109/TIT.2015.2453267

[23] Thorpe, J. (2003) Low-Density Parity-Check (LDPC) Codes Constructed from Protographs. Interplanetary Network Progress Report. Progress Report 42-154.

[24] Gallager, R.G. (2015) Low-Density Parity-Check Codes. Springer India, New Delhi.

[25] Gallager, R. (1962) Low-Density Parity-Check Codes. *IRE Transactions on Information Theory*, **8**, 21-28. https://doi.org/10.1109/TIT.1962.1057683

[26] Fan, J.L. (2000) Array Codes as Low-Density Parity-Check Codes. *Proceedings of* 2*nd International Symposium on Turbo Codes and Related Topics*, Brest, 543-546.

[27] Honary, B., Lin, S., Gabidulin, E.M., Xu, J., Kou, Y., Moinian, A. and Ammar, B. (2004) On Construction of Low Density Parity Check Codes. 2nd *International Workshop on Signal Processing for Wireless Communication* (SPWC 2004), London, 11-26.

[28] Ammer, B., Honary, B., Xu, Y. and Lin, S. (2004) Construction of Low-Density Parity-Check Codes on Balanced Incomplete Block Designs. *IEEE Transactions on Information Theory*, **50**, 1257-1269. https://doi.org/10.1109/TIT.2004.828144

[29] Miladinovic, N. and Fossorier, M. (2004) Systematic Recursive Construction of LPDC Codes. *IEEE Communications Letters*, **8**, 302-304. https://doi.org/10.1109/LCOMM.2004.827431

[30] Tanner, R.M., Sridhara, D., Sridharan, A., Fuja, T.E. and Costello, D.J. (2004) LDPC Block and Convolutional Codes Based on Circulant Matrices. *IEEE Transactions on Information Theory*, **50**, 2966-2984. https://doi.org/10.1109/TIT.2004.838370

[31] Hakimi, S.L. and Bredeson, J. (1969) Ternary Graph Theoretic Error-Correcting Codes. *IEEE Transactions on Information Theory*, **15**, 435-436. https://doi.org/10.1109/TIT.1969.1054312

[32] Zhang, K., Jiang, X.Q., Feng, Y., Qiu, R. and Bai, E. (2020) High Efficiency Continuous-Variable Quantum Key Distribution Based on Quasi-Cyclic LDPC Codes. 2020 5*th International Conference on Communication, Image and Signal Processing* (*CCISP*), Chengdu, 13-15 November 2020, 38-42. https://doi.org/10.1109/CCISP51026.2020.9273490

[33] Ali, I., Lee, H., Hussain, A. and Kim, S. (2019) Protograph-Based Folded Spatially Coupled LDPC Codes for Burst Erasure Channels. *IEEE Wireless Communications Letters*, **8**, 516-519. https://doi.org/10.1109/LWC.2018.2878562

[34] Liu, K., El-Khamy, M. and Lee, J. (2016) Finite-Length Algebraic Spatially-Coupled Quasi-Cyclic LDPC Codes. *IEEE Journal on Selected Areas in Communications*, **34**, 329-344. https://doi.org/10.1109/JSAC.2015.2504273

[35] Kong, L., He, L., Chen, P., Han, G. and Fang, Y. (2015) Protograph-Based Quasi-Cyclic LDPC Coding for Ultrahigh Density Magnetic Recording Channels. *IEEE Transactions on Magnetics*, **51**, 1-4. https://doi.org/10.1109/TMAG.2015.2437397

[36] Kulkarni, V. and Sankar, K.J. (2015) Design of Structured Irregular LDPC Codes from Structured Regular LDPC Codes. *Proceedings of the* 2015 *3rd International Conference on Computer, Communication, Control and Information Technology* (C3IT), Hooghly, 7-8 February 2015, 1-4. https://doi.org/10.1109/C3IT.2015.7060128

[37] Mankar, M.V., Patil, A. and Asutkar, G.M. (2014) Single Mode Quasi-Cyclic LDPC Decoder Using Modified Belief Propagation. 2014 *International Conference on Communication and Signal Processing*, Melmaruvathur, 3-5 April 2014, 862-866. https://doi.org/10.1109/ICCSP.2014.6949966

[38] Pisek, E., Rajan, D. and Cleveland, J.R. (2015) Trellis-Based QC-LDPC Convolutional Codes Enabling Low Power Decoders. *IEEE Transactions on Communications*, **63**, 1939-1951. https://doi.org/10.1109/TCOMM.2015.2424434

[39] Esfahanizadeh, H., Ram, E. and Cassuto, Y. (2020) Spatially Coupled Codes with Sub-Block Locality: Joint Finite Length-Asymptotic Design Approach. 2020 *IEEE International Symposium on Information Theory* (*ISIT*), Los Angeles, 21-26 June 2020, 467-472. https://doi.org/10.1109/ISIT44484.2020.9174265

[40] Ram, E. and Cassuto, Y. (2021) Spatially Coupled LDPC Codes with Sub-Block Locality. *IEEE Transactions on Information Theory*, **67**, 2739-2757. https://doi.org/10.1109/TIT.2021.3059751

[41] Elkouss, D., Martinez-Mateo, J. and Martin, V. (2011) Information Reconciliation for Quantum Key Distribution. *Quantum Information and Computation*, **11**, 226-238. https://doi.org/10.26421/QIC11.3-4-3

[42] Martinez-Mateo, J., Elkouss, D. and Martin, V. (2012) Blind Reconciliation. *Quantum Information and Computation*, **12**, 791-812. https://doi.org/10.26421/QIC12.9-10-5

[43] Martinez-Mateo, J., Elkouss, D. and Martin, V. (2013) Key Reconciliation for High Performance Quantum Key Distribution. *Scientific Reports*, **3**, Article No. 1576. https://doi.org/10.1038/srep01576

[44] Martinez-Mateo, J., Pacher, C., Peev, M., Ciurana, A. and Martin, V. (2015) Demystifying the Information Reconciliation Protocol Cascade. *Quantum Information and Computation*, **15**, 453-477. https://doi.org/10.26421/QIC15.5-6-6

[45] Pedersen, T.B. and Toyran, M. (2015) High Performance Information Reconciliation for QKD with CASCADE. *Quantum Information and Computation*, **15**, 419-434. https://doi.org/10.26421/QIC15.5-6-4

[46] Barnault, L. and Declercq, D. (2003) Fast Decoding Algorithm for LDPC over GF (2q). 2003 *IEEE Information Theory Workshop*, Paris, 31 March-4 April 2003, 70-73. https://doi.org/10.1109/ITW.2003.1216697

[47] Davey, M.C. and MacKay, D. (1998) Low-Density Parity Check Codes over GF (q). *IEEE Communications Letters*, **2**, 165-167. https://doi.org/10.1109/4234.681360

[48] Declercq, D. and Fossorier, M. (2007) Decoding Algorithms for Nonbinary LDPC Codes over GF (q). *IEEE Transactions on Communications*, **55**, 633-643. https://doi.org/10.1109/TCOMM.2007.894088

[49] Pacher, C., Martinez-Mateo, J., Duhme, J., Gehring, T. and Furrer, F. (2016) Information Reconciliation for Continuous-Variable Quantum Key Distribution Using Non-Binary Low-Density Parity-Check Codes. arXiv: 1602.09140.

[50] Al-Rubaye, G.A., Tsimenidis, C.C. and Johnston, M. (2015) Non-Binary LDPC Coded OFDM in Impulsive Power Line Channels. 2015 23*rd European Signal Processing Conference* (*EUSIPCO*), Nice, 31 August-4 September 2015, 1431-1435. https://doi.org/10.1109/EUSIPCO.2015.7362620

[51] Gehring, T., Händchen, V., Duhme, J., Furrer, F., Franz, T., Pacher, C., *et al.* (2015) Implementation of Continuous-Variable Quantum Key Distribution with Composable and One-Sided-Device-Independent Security against Coherent Attacks. *Nature Communications*, **6**, Article No. 8795. https://doi.org/10.1038/ncomms9795

[52] Montorsi, G. (2012) Analog Digital Belief Propagation. *IEEE Communications Letters*, **16**, 1106-1109. https://doi.org/10.1109/LCOMM.2012.020712.112133

[53] Sayir, J. (2014) Non-Binary LDPC Decoding Using Truncated Messages in the Walsh Hadamard Domain. *ISITA* 2014, *International Symposium on Information Theory and Its Applications*, Melbourne, 26-29 October 2014, 16-20.

[54] Voicila, A., Declercq, D., Verdier, F., Fossorier, M. and Urard, P. (2010) Low-Complexity Decoding for Non-Binary LDPC Codes in High Order Fields. *IEEE*

Transactions on Communications, **58**, 1365-1375.
https://doi.org/10.1109/TCOMM.2010.05.070096

[55] Hosseinidehaj, N. and Malaney, R. (2016) CV-QKD with Gaussian and Non-Gaussian Entangled States over Satellite-Based Channels. 2016 *IEEE Global Communications Conference* (*GLOBECOM*), Washington DC, 4-8 December 2016, 1-7.
https://doi.org/10.1109/GLOCOM.2016.7841711

[56] Shen, Y., Cao, L., Wang, X.Y., Zou, J., Luo, W., Wang, Y.X., *et al*. (2020) On-Chip Continuous-Variable Quantum Key Distribution (CV-QKD) and Homodyne Detection. 2020 *Optical Fiber Communications Conference and Exhibition* (*OFC*), San Diego, 8-12 March 2020, 1-3. https://doi.org/10.1364/OFC.2020.W2A.53

[57] Jayasooriya, S., Shirvanimoghaddam, M., Ong, L., Lechner, G. and Johnson, S.J. (2016) A New Density Evolution Approximation for LDPC and Multi-Edge Type LDPC Codes. *IEEE Transactions on Communications*, **64**, 4044-4056.
https://doi.org/10.1109/TCOMM.2016.2600660

[58] Leverrier, A. and Grangier, P. (2009) Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation. *Physical Review Letters*, **102**, Article ID: 180504.
https://doi.org/10.1103/PhysRevLett.102.180504

[59] Zhou, C., Wang, X.Y. and Zhang, Z.G. (2021) Rate Compatible Reconciliation for Continuous-Variable Quantum Key Distribution Using Raptor-Like LDPC Codes. *Science China Physics*, *Mechanics & Astronomy*, **64**, Article No. 260311.
https://doi.org/10.1007/s11433-021-1688-4

[60] Wang, X., Zhang, Y., Yu, S., Xu, B., Li, Z. and Guo, H. (2017) Efficient Rate-Adaptive Reconciliation for Continuous-Variable Quantum Key Distribution. *Quantum Information and Computation*, **17**, 1123-1134.
https://doi.org/10.26421/QIC17.13-14-4

[61] Rakita, A., Nikoli'c, N., Mildner, M., Matiasek, J. and Elbe-Bürger, A. (2020) Re-Epithelialization and Immune Cell Behaviour in an *ex Vivo* Human Skin Model. *Scientific Reports*, **10**, Article No. 1. https://doi.org/10.1038/s41598-019-56847-4

[62] Bonello, N., Chen, S. and Hanzo, L. (2011) Low-Density Parity-Check Codes and Their Rateless Relatives. *IEEE Communications Surveys & Tutorials*, **13**, 3-26.
https://doi.org/10.1109/SURV.2011.040410.00042

[63] Yu, Y., Jia, Z., Tao, W. and Dong, S. (2016) LDPC Codes Optimization for Differential Encoded LDPC Coded Systems with Multiple Symbol Differential Detection. 2016 *IEEE* 5*th Global Conference on Consumer Electronics*, Kyoto, 11-14 October 2016, 1-2. https://doi.org/10.1109/GCCE.2016.7800541

[64] Yang, S.S., Lu, Z.G. and Li, Y.M. (2020) High-Speed Post-Processing in Continuous-Variable Quantum Key Distribution Based on FPGA Implementation. *Journal of Lightwave Technology*, **38**, 3935-3941.
https://doi.org/10.1109/JLT.2020.2985408