Error Reconciliation based on Integer Linear Programming in Quantum Key Distribution

Zahra Eskandari*
Department of Computer Engineering, Quchan University of Technology, Quchan, Iran
z.eskandari@qiet.ac.ir
Mohammad Rezaee
Department of Computer Engineering, Quchan University of Technology, Quchan, Iran
rezaee@qiet.ac.ir

Received: 14/Sep/2021 Revised: 24/Nov/2021 Accepted: 12/Dec/2021

Abstract
Quantum telecommunication has received a lot of attention today by providing unconditional security because of the inherent nature of quantum channels based on the no-cloning theorem. In this mode of communication, first, the key is sent through a quantum channel that is resistant to eavesdropping, and then secure communication is established using the exchanged key. Due to the inevitability of noise, the received key needs to be distilled. One of the vital steps in key distillation is named key reconciliation which corrects the occurred errors in the key. Different solutions have been presented for this issue, with different efficiency and success rate. One of the most notable works is LDPC decoding which has higher efficiency compared to the others, but unfortunately, this method does not work well in the codes with a high rate. In this paper, we present an approach to correct the errors in the high rate LDPC code-based reconciliation algorithm. The proposed algorithm utilizes Integer Linear Programming to model the error correction problem to an optimization problem and solve it. Testing the proposed approach through simulation, we show it has high efficiency in high rate LDPC codes as well as a higher success rate compared with the LDPC decoding method - belief propagation – in a reasonable time.

Keywords: Key reconciliation algorithm; error correction; LDPC codes; Belief Propagation; Integer Linear Programming.

1- Introduction

Quantum key distribution protocols [1,2] share a secure key between two remote parties and then establish secure communication between them using two channels; quantum channel and public channel. Quantum channel is used to carry qubits which include secret key information and after the key agreement between the two parties, Alice (A) and Bob (B), they use the secret key to establish secure communication in the public channel. It is unfortunate that the key establishment process always takes along with errors because of channel noise, device imperfection [3, 4], or the presence of eavesdropper (Eve) [5]. Thus, after transmitting the key via the quantum channel, A and B use the public channel to estimate the amount of Quantum Bit Error Rate (QBER) and correct errors in the key to establish symmetric key on both sides of the connection.

To do this, A send a key, and then at the side B, 1- the key bits are sifted, then 2- B estimates errors in sifted key bits, QBER, using the error estimation approaches [6-9]. Comparing the estimated QBER with a determined threshold, B decides that the channel is affected by channel or device noises or the presence of Eve. If QBER is higher than the determined threshold, because of the no-cloning theorem [10], it shows that Eve spoofs the connection and the key is not safe anymore. Otherwise, the next step is begun, 3- B uses a reconciliation algorithm [11-15,45-47] to correct the errors and then uses some privacy amplification methods [16,17] to remove the disclosed information along the reconciliation step.

Key reconciliation is important because using an efficient approach with minimum information leakage, in addition to increase secure key generation rate, it impacts on the security of the communication between two sides. The first error reconciliation was the BBBSS protocol [11] which uses some passes to exchange raw key subsets and check the parity of the blocks to determine and correct the errors in the subset. This approach was then improved by [12] as the Cascade algorithm. Other common approaches based on the BBBSS algorithm are Furukawa–Yamazaki [13] and Winnow protocol [14] which uses a Hamming code to reduce the number of errors.

Currently, LDPC (low-density parity check) [18] method has been widely used in this subject [15, 48, 49] as the Belief propagation algorithm (BP) [19], also known as sum-product algorithm, was used to correct the errors. This approach has attracted a lot of attention because it works more efficiently rather than others [20]. It should be

*Corresponding Author

mentioned in comparison to Cascade and Winnow, LDPC provides lower communication overhead and also it can reconcile errors at a higher rate than those.

Using artificial neural networks for error correction was introduced in [21]. The work uses the mutual synchronization of artificial neural networks to correct errors in the sifted key after the transmission in the quantum channel. Two sides create the neural networks based on the keys that they have. After the mutual learning process, they correct all errors and can use the key. But, this approach suffers from high processing time and source consumption so it has not been investigated in higher code length.

In this paper, we propose an efficient approach to reconcile errors in quantum keys distribution. As mentioned earlier, by comparing reconciliation efficiency of the three most common reconciliation algorithms, LDPC, Cascade and Winnow, it shows that the efficiency of the LDPC based reconciliation algorithm is superior to the two other in most of the QBERs. So, by considering this fact, we focus on LDPC codes approach. But as discussed later, the reconciliation based on the decoding of these codes suffers from lack of efficiency in codes with high code rate.

Indeed, the code rate has a direct influence on the amount of disclosed information in the reconciliation process. In higher rates that benefit from less leakage, LDPC approach or more specifically, BP decoding approach does not work with enough success. Focusing mentioned problem, in this paper, we decided to propose an approach to correct the errors in high rate codes. To do this we utilize Integer Linear Programming (ILP) approach.

It is noteworthy that the (Mixed) (Integer) Linear programming approaches have already been used to decoding the LDPC codes [22-25], but as it known, it is the first time that an Integer Linear Programming (ILP) model is utilized to reconcile the key in Quantum key distribution and more specifically key reconciliation algorithms. Furthermore, compared to mentioned works, the way we model the problem here is completely different in the number of variables and constraints which has a direct impact on the complexity of solving the ILP problem.

The rest of the paper proceeds as follows: in section 2 we review briefly the required preliminaries, LDPC coding concepts and ILP basics. In section 3, a detailed description of the proposed approach based on ILP is presented. The experimental results are evaluated, discussed and compared in section 4. Finally, section 5 concludes the work.

2- Preliminaries

In this section, we describe the basic concepts of this study. First, a brief overview of the LDPC codes is given, and then the concepts of (Mixed) (Integer) Linear Programming are discussed.

2-1- LDPC Codes

Low-density parity check (LDPC) codes were first introduced by Gallager in 1962 [18] as a method of transmitting a message over a noisy channel with error correction capability. Later, significant attentions were drawn to LDPC code due to its near-Shannon performance [26, 27]. The decoders for LDPC codes are based on Belief propagation (BP) algorithm and its variants [28-30]. However, BP decoding usually suffers from decreasing the success rate in presence of high error rates.

LDPC codes (n, k) can be considered as a k-dimensional subspace of $\{0,1\}^n$ which represented by a generator matrix G whose rows span code C and a parity check matrix H whose rows span $C^{\perp}$ - i.e., $c \in C$ if and only if $cH^T = 0$, where $m = n \times (1 - r)$. In LDPC codes, n and m are defined as the code and codeword length, correspondingly. The parameter r is as code rate in range $[0, 1]$ which defines the correcting power and efficiency.

When the sender wants to send vector a through noisy channel, instead of sending raw data, to have correction chance, considering G as generator matrix, she calculates codeword b as

$$b = a \times G \tag{1}$$

The symbol $\times$ corresponds to matrix (vector) multiplication in modulo 2 arithmetic.

At the channel end, the receiver receives the codeword c and use H as parity check matrix to verify that the received codeword c is error-free or not. If $c = b$, it means the error syndrome

$$S = H \times c^T \tag{2}$$

is equal to a zero vector. Otherwise, the non-zero elements of S can provide that the channel was noisy and there are some positions in the received codeword which are affected by some errors. In conditions that the occurred errors do not exceed the correction capacity of the channel code, the decoding process can correct the errors.

Decoding algorithms for LDPC codes are called message passing algorithms [19, 28-30], and work iteratively. These algorithms work based on Tanner graph [31], considering LDPC code as a graph consisting of message and check nodes corresponding to columns and the rows of the H, respectively. The reason for their name is that at each round of the algorithms, messages are passed from

message nodes to check nodes, and from check nodes back to message nodes, iteratively until the state of the graph converge to a valid codeword.
What is important about BP algorithm is that the iteration of decoding is ended when all parity check equations are satisfied and a valid codeword has been found. In some cyclic graphs, or when errors are higher than they can be decoded correctly, more iterations do not change the state of the graph and errors cannot be corrected. So, decoding fails without finding the correct codeword as the output.
For more details about LDPC codes, the readers can refer to [18, 19].

2-2- Optimization Approaches

Combinatorial optimization deals with the problem of minimizing or maximizing a function of several variables subject to some constraints. The constraints can be in the form of equality or inequality, linear or nonlinear. If the constraints are linear, the feasible region is a convex polyhedron, which has a global minimum, and the solving methods can converge to this optimal point. But if the constraints are nonlinear, solving the problem has some complexity and requires more provisions [32].
Linear programming (LP) problem is defined as follows:

$$\min\{\mathrm{Cx} \mid \mathrm{Ax} \leq \mathrm{b}, \mathrm{x} \in \mathrm{R}^{\mathrm{n}}\} \quad (3)$$

The $Ax \leq b$ inequalities determine the feasible region which is bounded by the system of constraints, including the possible values of the variables that satisfy all of the constraints. The aim of linear programming is to find the best solution to a problem by maximizing or minimizing the objective function Cx. As shown in equation (3), the objective function and all constraints are linear. It must be mentioned that the complexity of solving the LP problem is polynomial [33].
If the variables are integer, we have Integer Linear Programming (ILP) problem as follows:

$$\min\{\mathrm{Cx} \mid \mathrm{Ax} \leq \mathrm{b}, \mathrm{x} \in \mathrm{Z}^{\mathrm{n}}\} \quad (4)$$

As the variables are discrete in these problems, the solving methods differ and consequently the complexity of solving is affected such that in general, the time complexity of solving these problems is exponential [33].
However, some works have been done and some improvements have been achieved. A prominent one is LP relaxation which by analyzing the problem constraints, some conversions could be performed [31] or some new constraints may be added to the problem [34] and convert the ILP problem to LP one with polynomial solving time which is practical way to solve large size problem.
In addition to this naïve approach, Branch-and-bound [35] and cutting-plane [36] methods have been principle tools for solving ILP models in recent times. Both of them deal with the models by solving a sequence of LP problems by simplex methods [33]. It will be clear that only finitely many LP problems need to be solved in principle.
It is noteworthy that because of great industrial interest in optimization applications, there exist many well-develop solvers such as IBM ILOG Cplex [40], Gurobi [41], and so forth which employ proper techniques to solve large problems with reasonable complexity in terms of time and space.

3- Proposed Error Correction Approach based on ILP Model

In this section, we present the detail of the proposed approach to correct errors in the sifted key based on the Integer Linear Programming approach.
Suppose A and B prepare H and share it. A after choosing the key X_A, calculates syndrome S_A as equation (2) and send them to B via quantum and public channel, respectively.
After B obtains the sifted key, X_B and syndrome of A, S_A, through mentioned channels, because of the presence of the noise, indeed he received a noisy version of X_A:

$$X_B = X_A \oplus e \quad (5)$$

Where e is the noise vector and $\oplus$ used for summation operation in module 2.
Then B calculates the syndrome of X_B as equation (2), S_B using H and X_B. Comparing S_A and S_B, he gets some information about error occurrence. In a more precise view, he has:

$$S_B = H \times X_B = H \times (X_A \oplus e) = H \times X_A \oplus H \times e = S_A \oplus H \times e \quad (6)$$

Which equals to:

$$H \times e = S_A \oplus S_B \quad (7)$$

Where the symbol $\times$ and $\oplus$ corresponds to matrix multiplication and summation operation in modulo 2 arithmetic.
B should determines e vector as it satisfies equation (7). Indeed along with decoding approaches aim to find the nearest codeword to the received one, B should determines e vector with minimum weight. In the other word, B searches for a codeword with minimum Hamming distance to received codeword to decode it.
So B can model the problem to an optimization problem aiming to find an error vector with minimum weight to satisfy equation (7). To do this, he defines variables, constraints, and objective function based on the nature of the original problem. After modeling the problem, using

solving tools, B solves it to find the solution and determine the error vector e. Defining e as:

$$e = (e_1, e_2, \dots, e_n) | e_i = \{0,1\}, i = 1, \dots, n \quad (8)$$

Where e_i value 1 or 0 corresponds to the presence or absence of noise at the position i in the received key, X_B. As B tries to find nearest codeword to the received key X_B which equally means he should find e vector with minimum weight. So, the objective function is defined as follow:

$$\min \sum_{i=1}^{n} e_i \quad (9)$$
$$e_i = \{0,1\}, i = 1, \dots, n$$

To find the feasible region for possible values of noise vector, it should be mentioned that the noise vector should be satisfied by the equation (7). Each row of the $H(H_j)$ behaves like a parity check equation that must be satisfied. Given the equation (7), the variable b, as a m binary vector, is defined as:

$$b = S_A \oplus S_B \quad (10)$$

Therefore, the constraints could be shown as:

$$H_j \times e = b_j, \quad j = 1, \dots, m \quad (11)$$

More precisely, the constraints are as follows:

$$\oplus_{i=1}^{n} H_{ji} * e_i = b_j, \quad j = 1, \dots, m \quad (12)$$

Where $*$ used for multiplication operation over integer numbers and by $\oplus_{i=1}^{n} H_{ji} * e_i$, we mean $H_{j1} * e_1 \oplus H_{j2} * e_2 \oplus \dots \oplus H_{jn} * e_n$.

Thus the model is as follow:

$$\min \sum_{i=1}^{n} e_i \quad (13)$$
$$\oplus_{i=1}^{n} H_{ji} * e_i = b_j, \quad j = 1, \dots, m$$
$$e_i = \{0,1\}, i = 1, \dots, n$$

As seen in the problem, the variables are binary and the constraints are using module 2 multiplication operation. So, here we convert the module 2 constraints to constraints over Z by doing as follows: in [42], The Integer Adapted Standard Conversion Method (IASC) was proposed to apply to Boolean polynomials.

This method is based on the ability of presenting an equation modulo 2 as an equation over Z and works as follows: considering a Boolean polynomial f over $F2$ and assume this polynomial as a polynomial g over the integers by replacing XOR by addition. All solutions of the Boolean equation $f = 0$ will yield a multiple of 2 when plugged into g. Thus, for $x \in \{x | f(x) = 0\}$ it holds that $g(x) = 2 \cdot k$. Then we obtain an integer equation by subtracting a multiple of 2 from g: $g - 2 \cdot k = 0$ where $0 \leq k$.

As an example, consider the Boolean equation

$$x1 + x2 + x3 + x4 = 0 \quad (14)$$

If we evaluate the corresponding real-valued polynomial $y1 + y2 + y3 + y4 = 0$ for all solutions of (14), we get 0, 2, 4 as results. That means that a solution of (14) is a solution to the following equation over the integers

$$y1 + y2 + y3 + y4 - 2.k = 0 \quad (15)$$

where $k \in \{0, 1, 2\}$ and $yi \in \{0, 1\}$ for $i = 1 \dots 4$.

The number of variables per equation is increased only by one compared to the Boolean polynomial.

ILP formulation over Z: In order to conquer Boolean constraints, we use the IASC conversion method to convert the model to ILP one. Indeed, we convert summation in binary to integer space, so we define new variables as:

$$k_j, \quad k_j \in Z^+, j = 1 \dots m \quad (16)$$

Thus, the proposed ILP model for error correction problem is as follows:

$$\min \sum_{i=1}^{n} e_i$$
$$\oplus_{i=1}^{n} H_{ji} * e_i - 2 * k_j = b_j, \quad j = 1, \dots, m$$
$$e_i = \{0,1\}, i = 1, \dots, n,$$
$$k_j \in Z^+, j = 1 \dots m \quad (17)$$

Computational and Space Complexity Analysis: The proposed ILP model, has $n + m$ variables, m bits for error vector and n integer variables, and m linear constraints corresponds to the rows of parity check matrix and n integer constrains for error vector bits. As mentioned before, solving this type of problems is known to be NP-hard in general [51]. It should be noted that decoding methods and more specifically BP algorithms are known as NP-hard problems [50] and in addition, the performance of these algorithms depend on the iteration numbers.

Though LDPC codes were constructed using a sparse Tanner graph, so the corresponding generator and parity check matrices were sparse, too. Such as in this work, we model the error correction in LDPC codes as ILP, so the sparsity property of H parity matrix causes the sparsity in the constraints set and we have a sparse ILP. Recently some works [37, 38] have been done on Sparse Integer Linear Programming (SILP), the case that the coefficient

matrix is sparse. It was shown that SILP can be solved in polynomial time in such problems [39].

4- Evaluation of the Results

To evaluate the proposed ILP approach for error correction, in this section, we provide the detailed comparisons of the original BP algorithm, Multi-matrix BP (MBP) [8] and ILP proposed approach in different parameters; efficiency, success rate, and speed as three criteria for judging a key reconciliation algorithm. All simulation data are generated by random scenarios. In Multi-matrix BP (MBP) [8] approach, in each iteration multiple matrices were employed to generate more useful information in error correction. As claimed by the authors the iteration number falls and the convergence speed increases. Indeed cycles which appear in one matrix and reduce the success rate, could be eliminated by other matrices.

For comparisons, we use 4 pool standard LDPC codes [43, 44] with code length $n = 1944$ with different code rates $r = \{0.5, 0.6667, 0.75, 0.8333\}$.

To evaluate the performance of ILP proposed approach, we compare it with recent approaches to correct errors, BP and MBP. To do this, we generate different sets of keys at QBERs in range [1,1.7] step by 0.1. At a given QBER, we generate 100 random scenarios of keys, perform each approach on the keys, and present the results as the average over the random scenarios for each QBER. The simulation parameters were presented in table 1.

Table 1: simulation parameters

Parameter	***Value***
Code length	1944
Code rates	0.5, 0.6777, 0.75, 0.8333
QBER range	[1,1.7]
Number of random keys	100

It should be mentioned that the ILP, BP and MBP approaches were implemented in Python programming language and all the experiments were done on Intel (R) core (TM) i7-9750H CPU @ 2.60 GHz with 16 GB memory.

4-1- Efficiency of LDPC-based Approach

As the most important factor in reconciliation algorithms, we can name reconciliation efficiency f which shows the relation of the amount of information B obtains to the minimum amount of information he needs for correcting all errors that theoretically calculated. Therefore, to ensure that he can correct all errors, f must be greater than or equal to 1, i.e. $f \geq 1$. In theory, $f = 1$ happens when LDPC code tends to be infinite in length and no cycles in structure, which can reach the Shannon Limit [9]. So in practice, $f > 1$. The reconciliation efficiency f which implies the efficiency and security of a reconciliation strategy, is calculated as:

$$f = \frac{m}{n.h(e)} \tag{17}$$

where m and n are the numbers of check nodes and variable nodes of the corresponding Tanner graph of LDPC code, equivalent by number of rows and columns of parity check matrix H, e is the result of Quantum Bit Error Rate estimation, and $h(e)$ is the Shannon binary entropy represented as:

$$h(e) = -e \log_2 e - (1-e) \log_2 (1-e) \tag{18}$$

In figure (1), we present the efficiency of the LDPC codes for different code rates in QBERs in range $[1, 1.7]$. As seen, by increasing the QBER, the efficiency of LDPC codes in all code rate scenarios was decreased. But, in higher code rate, the efficiency of LDPC codes gets closer to 1.

Indeed under same value of n, in a high code rate compared to lower code rate, m is smaller which means the sender needs to send syndrome with smaller length. So based on equation (17), the f value gets closer to 1 meaning that it needs to disclose a lower amount of data.

So by using LDPC codes with high code rates in key reconciliation algorithms, we can achieve better efficiency as well as a higher secure key generation rate.

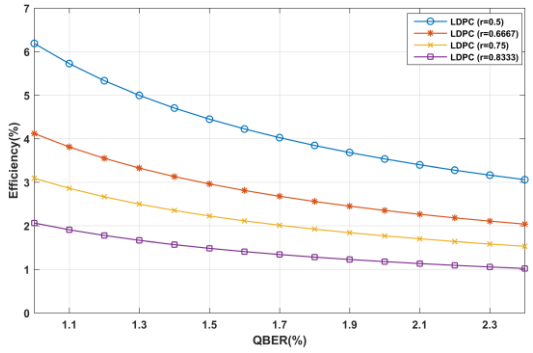

Fig. 1 Comparison of reconciliation efficiency of LDPC codes with different code rate values at different QBER.

4-2- Success Rate

The success rate of reconciliation algorithms shows the number of the successful scenarios that the reconciliation algorithm can correct the errors. Unfortunately, the success rate of the BP algorithm may be relatively impacted by cycles which means if LDPC codes are not cycle-free [31], it cannot get to the corrected answer even by consuming more time or with running the message passing in more iterations. So in these situations, the success rate of the BP is decreased.

In higher code rate, because of the lower number of check nodes in comparison to message nodes in Tanner graph of LDPC codes, the probability of successful decoding and correcting the errors is decreased, so as a result, the success rate is decreased too.
As shown in figure (2), in the code rate $r = 0.6667$, the BP algorithm works well and it could decode all the corrupted received keys even in high QBER values, and it achieve 100% success rate. But, in a higher code rate $r = 0.8333$ which the number of check nodes, m is decreased compared to $r = 0.6667$, the BP falls in wrong decoding or fails to reach the result. So the success rate of BP decreased drastically by increasing the QBERs.
So we can conclude that the BP algorithm is not proper enough to correct errors in high rate LDPC codes and we should look forward to a more successful approach to correct errors in such codes.

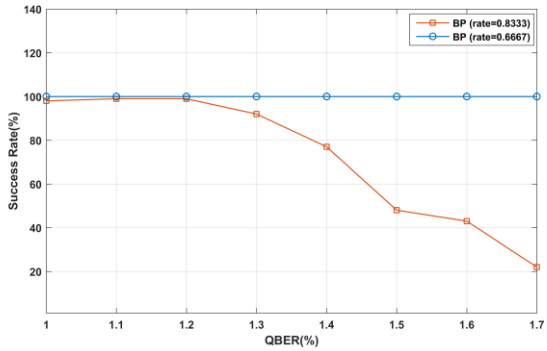

Fig. 2 Comparison of success rate of BP algorithm with different code rate values at different QBER.

About ILP-based error correction proposed algorithm, in low code rate $r = 0.6667$, the proposed approach can correct the errors in all scenarios in reasonable time and it has a success rate 100% for all QBERs in range $[1, 1.7]$ as well as the BP at code rate $r = 0.6667$.

But in contrast to BP algorithm, as shown in figure (3), at code rate $r = 0.8333$, the ILP proposed approach has more success in comparison to the BP and MBP algorithms. Indeed by analyzing the results, it reveals that in all scenarios which BP gets the results, the ILP proposed approach gets the correct result too, and in addition, in most of the failed scenarios by BP, ILP approach can solve the problem and correct the errors successfully. In fact we can conclude that in such problems that the cycles could degrade the performance of the decoding, ILP approach can step forward and correct errors.

4-3- Reconciliation Speed

For key reconciliation, the convergence speed is calculated as the required time to correct the errors. Here we evaluate the convergence speed of BP, MBP and ILP proposed algorithms in error correction of the LDPC codes with different code rate $r = \{0.6667, 0.8333\}$ by calculating the consumed time to perform error correction under different QBERs. At a given QBER, we generate 100 sets of keys, perform each algorithm on the keys, and calculate the average amount of the required time for error correction. The results are shown in figure (4) and figure (5) for different code rates. Clearly, under different code rates, the algorithms spend reasonable time for correcting errors. As shown in figure (4) in code rate $r = 0.6667$, by increasing the QBER, the speed of the correction algorithm grows slightly. Indeed, enough number of check nodes in comparison with message nodes causes the algorithms to obtain the solution and correct the errors in the low time. As seen in figure (4) and (5), since MBP did the decoding computation for some matrices, even it achieves less iteration number, it consumes much more time in comparison to BP with only one matrix.

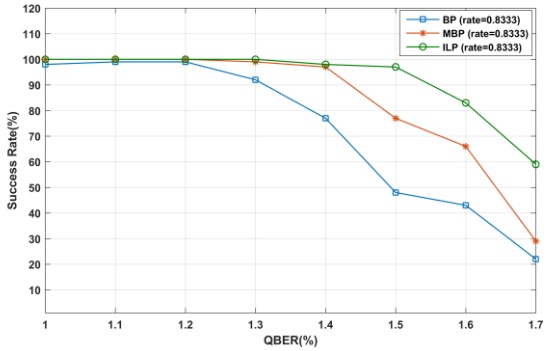

Fig. 3 Comparison of success rate of BP algorithm and Proposed ILP model in error correction of LDPC code with r=0.8333 at different QBER.

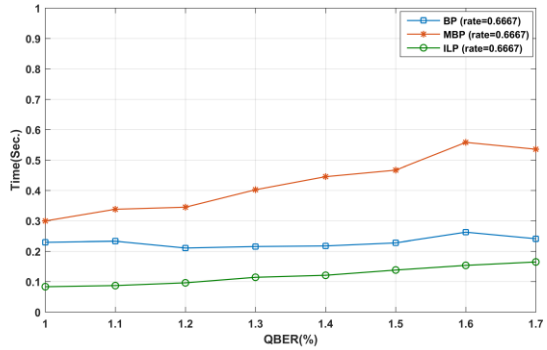

Fig. 4 Comparison of speed of BP algorithm and Proposed ILP model in error correction of LDPC code with r=0.6667 at different QBER.

But as seen in figure (5), which is correspond to the code rate $r = 0.8333$ with the lower number of check nodes at the same number of message nodes compared to the previous scenario, determining the right codeword requires more time in both BP approaches and ILP proposed algorithms. So the consumed time is increased compared to the code rate $r = 0.6667$.

It is notable that the solving time of the ILP problem is less than the required time for BP algorithms in both of the mentioned code rates. The increase in the consumed time of ILP at the high values of QBER in the figure (5) is caused by the fact that in most of the scenarios with high QBER that the BP algorithm fails, the ILP purposed model continue and solve the problem. considering the difference in the success rate of these algorithms presented at figure (3) can justify the results in the figure (5).

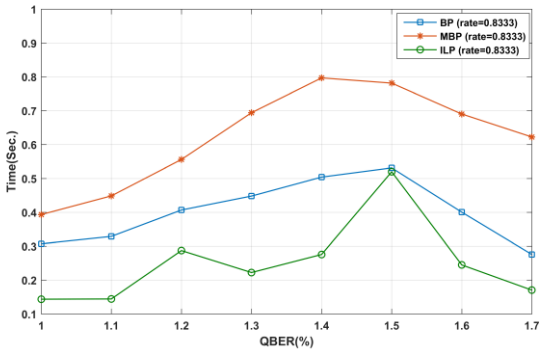

Fig. 5 Comparison of speed of BP algorithm and Proposed ILP model in error correction of LDPC code with r=0.8333 at different QBER.

5- Conclusion and Future Works

Quantum key distribution protocols share a secure key to using the Quantum channel. Because of the unavoidability of the existence of noise, distillation algorithms are necessary to purify the key. As one step in the distillation process, key reconciliation has the responsibility to correct errors of the key efficient manner.

Comparing reconciliation efficiency of the reconciliation algorithms, LDPC code-based reconciliation algorithms have revealed the higher efficiency but as the code rate grows, the success rate of the most used decoding algorithm, belief propagation, decreased considerably. Besides the fact that in such codes, the amount of disclosed information was decreased. So to use this helpful feature of high rate LDPC codes, we have to overcome this problem. In this paper, focusing on high rate LDPC codes, we propose an approach to correct the errors in such codes. The proposed approach utilizes Integer Linear Programming (ILP) approaches. To do this, we model the error correction problem, by defining the variables, constraints, and objective function corresponding to the reconciliation algorithm aim. Then to have more efficient modeling, we convert the binary model to a model over Z. So the final ILP model is defined over Z and it has sparsity property, which led to having an efficient model in terms of time and space solving complexity to have with reasonable solving time.

Finally, by evaluating the proposed algorithm at the crucial parameters for judging the efficiency of the reconciliation algorithms, our approach is superior to the BP algorithm in high rate codes regarding success rate and reconciliation speed in different rates and different QBERs.

As future work, by considering scalability the presented optimization model can be improved, so it can be utilized more efficiently in problems with more variables and constraints. By utilizing this improvement it can be employed to perform error correction in codes with longer length.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys. 74(1), 145–195 (2002).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” Rev. Mod. Phys. 81(3), 1301–1350 (2009).

[3] H. Weier, H. Krauss, M. Rau, M. Fuerst, S. Nauerth, and H. Weinfurter, “Quantum eavesdropping without interception: an attack exploiting the dead time of single photon detectors,” New J. Phys. 13(7), 073024 (2011).

[4] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, “Device calibration impacts security of quantum key distribution,” Phys. Rev. Lett. 107(11), 110501 (2011).

[5] C. H. Bennet and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” in Proceedings of the IEEE International Conference on Computers Systems and Signal Processing (IEEE, 1984), pp. 175–179

[6] X.B. Wang, “Beating the photon-number-splitting attack in practical quantum cryptography,” Phys. Rev. Lett. 94(23), 230503 (2005).

[7] P. Treeviriyanupab, T. Phromsaard, C.M. Zhang, M. Li, P. Sangwongngam, T. S. N. Ayutaya, N. Songneam, R. Rattanatamma, C. Ingkavet, W. Sanor, W. Chen, Z.F. Han, and K. Sripimanwat, “Rate-adaptive reconciliation and its estimator for quantum bit error rate,” in Proceedings of International Symposium on Communications and Information Technologies (IEEE, 2014), pp. 351–355.

[8] C. Gao, J. Dong, G. Yu, L. Chen, Multi-matrix error estimation and reconciliation for quantum key distribution. Optics Express. (2019). 27. 14545. 10.1364/OE.27.014545.

[9] C. Gao, Y. Guo, D. Jiang, L. Chen, Multi-matrix rate-compatible reconciliation for quantum key distribution. ArXiv(2020)., abs/2001.01074.

[10] Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature 299, 802–803 (1982)

[11] Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.: Experimental quantum cryptography. J. Cryptol. 5, 3–28 (1992)

[12] Brassard, G., Salvail, L.: Secret-Key Reconciliation by Public Discussion, pp. 410–423. Springer, Berlin (1994)

[13] Furukawa, E., Yamazaki, K.: Application of existing perfect code to secret key reconciliation. In: Proceedings of International Symposium on Communication and Information Technologies, pp. 397– 400 (2001)

[14] Buttler, W.T., Lamoreaux, S.K., Torgerson, J.R., Nickel, G.H., Donahue, C.H., Peterson, C.G.: Fast, efficient error

reconciliation for quantum cryptography. Phys. Rev. A 67, 052303 (2003)

[15] E. Kiktenko, A. Malyshev, A. Bozhedarov, N. Pozhar, M. Anufriev, and A. Fedorov, "Error estimation at the information reconciliation stage of quantum key distribution," J. Russ. Laser Res. 39(6), 558–567 (2018).

[16] C. H. Bennett, G. Brassard, and J.M. Robert, "Privacy amplification by public discussion," SIAM J. Comput. 17(2), 210–229 (1988).

[17] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," IEEE Trans. Inf. Theory 41(6), 1915–1923 (1995).

[18] R. G. Gallager, Low Density Parity-Check Codes. MIT Press, Cambridge, MA, 1963.

[19] S. Chung, T. J. Richardson, and R. L. Urbanke, "Analysis of sum-product decoding of low-density parity-check codes using a Gaussian approximation," IEEE Trans. Inf. Theory 47(2), 657–670 (2001).

[20] Mehic M., Niemiec M., Siljak H., Voznak M. (2020) Error Reconciliation in Quantum Key Distribution Protocols. In: Ulidowski I., Lanese I., Schultz U., Ferreira C. (eds) Reversible Computation: Extending Horizons of Computing. RC 2020. Lecture Notes in Computer Science, vol 12070. Springer, Cham.

[21] Niemiec, M. Error correction in quantum cryptography based on artificial neural networks. Quantum Inf Process 18, 174 (2019). https://doi.org/10.1007/s11128-019-2296-4

[22] J. Feldman, "Decoding Error-Correcting Codes via Linear Programming". PhD thesis, M.I.T., Cambridge, MA, 2003

[23] K. Yang, X. Wang, and J. Feldman, "A new linear programming approach to decoding linear block codes," IEEE Trans. Inf. Theory, vol. 54, no. 3, pp. 1061–1072, Mar. 2008.

[24] H. Wei and A. H. Banihashemi, "An iterative check polytope projec tion algorithm for ADMM-based LP decoding of LDPC codes," IEEE Commun. Lett., vol. 22, no. 1, pp. 29–32, Jan. 2018.

[25] J. Bai, Y. C, Wang, and F. C. M. Lau, "Minimum-polytope-based linear programming decoder for LDPC Codes via ADMM approach", IEEE Wireless Commun. Lett., vol. 8, no. 4, pp. 1032-1035, Aug. 2019

[26] D. J. C. MacKay and R. M. Neal, "Good codes based on very sparse matrices," in Cryptography and Coding, ser. Lecture Notes in Computer Science, C. Boyd, Ed. Heidelberg/Berlin: Springer, 1995, vol. 1025, pp. 100-111.

[27] D. J. C. MacKay and R. M. Neal, "Near Shannon-limit performance of low density parity check codes," Electron. Lett., vol. 33, no. 6, pp. 457- 458, Mar. 1997.

[28] F. R. Kschischang, B. J. Frey, and H. A. Loeliger, "Factor graphs and the sum-product algorithm," IEEE Trans. Inf. Theory, vol. 47, no. 2, pp. 498-519, Feb. 2001. 16

[29] W. Ryan and S. Lin, Channel Codes: Classical and Modern. Cambridge University Press, 2009.

[30] T. Richardson and R. Urbanke, Modern Coding Theory. Cambridge University Press, 2008.

[31] R. M. Tanner, "A recursive approach to low complexity codes," IEEE Trans. Inf. Theory 27(5), 533–547 (1981).

[32] L. A. Wolsey and G. L. Nemhauser: Integer and Combinatorial Optimization Wiley-Interscience, November 1999.

[33] Clovis C. Gonzaga, On the Complexity of Linear Programming, Resenhas IME-USP 1995, Vol. 2, No. 2, 197-207.

[34] EgonBalas, Sebastián Ceria, Gérard Cornuéjols: A lift-and-project cutting plane algorithm for mixed 0–1 programs, Mathematical Programming, Volume 58, January 1993, pp 295-324

[35] H. Land , A. G. Doig, An Automatic Method of Solving Discrete Linear Programming Problems, July 1960, Econometrica 28(3):497-520

[36] Ralph Gomory, Outline of an Algorithm for Integer Solutions to Linear Programs, September 1958, Bulletin of the American Mathematical Society 64(5):275-278

[37] Pritchard, D., Chakrabarty, D. Approximability of Sparse Integer Programs. Algorithmica 61, 75–93 (2011). https://doi.org/10.1007/s00453-010-9431-z

[38]Andres Iroume, SPARSITY IN INTEGER PROGRAMMING. PhD thesis, Georgia Institute of Technology, 2017

[39] Koutecký, Martin; Levin, Asaf; Onn, Shmuel (2018). A Parameterized Strongly Polynomial Algorithm for Block Structured Integer Programs. Michael Wagner: 14 pages. arXiv:1802.05859. doi:10.4230/LIPICS.ICALP.2018.85. S2CID 3336201.

[40]www.ibm.com/software/commerce/optimization/cplex-optimizer/

[41] www.gurobi.com/

[42] J. Borghoff, Mixed-integer Linear Programming in the Analysis of Trivium and Ktantan, IACR Cryptol. ePrint Arch. 2012.

[43] EEE Standard for Information Technology—Local and Metropoli tan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Spec ifications Amendment 5: Enhancements for Higher Throughput, IEEE Standard 802.11n-2009, Oct. 2009

[44] Elkouss, D., Martinez-Mateo, J. & Martin, V. Untainted Puncturing for Irregular Low-Density Parity-Check Codes. IEEE Wireless Communications Letters 1, 585–588 (2012).

[45] Guo, D., He, C., Guo, T. et al. Comprehensive high-speed reconciliation for continuous-variable quantum key distribution. Quantum Inf Process 19, 320 (2020).

[46] E. O. Kiktenko, A. O. Malyshev and A. K. Fedorov, "Blind Information Reconciliation With Polar Codes for Quantum Key Distribution," in IEEE Communications Letters, vol. 25, no. 1, pp. 79-83, Jan. 2021.

[47] Liu, Z., Wu, Z. & Huang, A. Blind information reconciliation with variable step sizes for quantum key distribution. Sci Rep 10, 171 (2020). https://doi.org/10.1038/s41598-019-56637-y

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

[49] B. Bilash, B. K. Park, C. Hoon Park and S. -W. Han, "Error-Correction Method Based on LDPC for Quantum Key Distribution Systems," 2020 International Conference on Information and Communication Technology Convergence

(ICTC), 2020, pp. 151-153, doi: 10.1109/ICTC49870.2020.9289451.
[50] Georgios Papachristoudis, John W. Fisher, Adaptive Belief Propagation, 32th International Conference on Machine Learning, Lille, France, 2015. JMLR: W&CP volume 37.
[51] Daniel Lokshtanov, New Methods in Parameterized Algorithms and Complexity, Dissertation for the degree of Philosophiae Doctor (PhD) University of Bergen Norway April 2009.

Zahra Eskandari received the B.S degree in Computer Engineering from Kharazmi University, Tehran, Iran, in 2006. She received her M.S. and PhD. degrees in Computer Engineering from Ferdowsi University of Mashhad, Iran, in 2008 and 2020, respectively. She was with the cybersecurity section at DTU compute, Denmark as a visiting researcher from July 2016 to March 2017. She is a full-time Assistant-Professor in the Department of Computer Engineering at Quchan University of Technology, Iran. Her research interests include security and cryptography. She is particularly interested in algebraic cryptanalysis and optimization approaches.

Mohammad Rezaee received the PhD degree in computer engineering from Ferdowsi University of Mashhad, Mashhad, Iran, in 2019. Currently, he is an assistant professor at the Computer Engineering Department, Quchan University of Technology. His research interests include Smart Grid Communication, and Optimization of Communication Networks.