Journal of Algebra and Applied Mathematics
Vol. 20 (2022), No.2, pp.75-91
ISSN: 2319-7234

URL : www.sasip.net

Improving the BB84 quantum key distribution protocol as based on graph theory

R.Z. Khalaf, A.S. Abdul-Kareem* and S.S. Mahdi

Abstract. Key distribution is considered to be among the most significant stages in any cryptographic system, and quantum key distribution is a secure method used to exchange keys between entities involved in communication.

In this study, we propose to improve the BB84-quantum key distribution protocol using graph-based coding, where agreement between the two parties is agreed on the graph used in quantum-bases encoding at both ends.

This paper presents a simulation of the proposed protocol using python language. The experimental results, which have been very promising, show that the proposed protocol is more effective and secure than the standard BB84 protocol.

AMS Subject Classification (2020): 81P94

Keywords: Quantum cryptography, QKD, BB84 protocol, graph theory, adjacency matrix

1. Introduction

Lately, cryptography has become one of the most important fields in computer networks due to the rapid development of Internet networks and the need to provide protection for data. Encryption is defined as the conversion of an explicit text to non-explicit text using a secret key for the purpose of encryption. Generally, there are two types of encryption

*Corresponding author

algorithms: symmetric encryption that relies upon private or secret keys, and asymmetric encryption that relies on the public keys [15].

The main problem of any symmetric encryption system is the distribution of encryption keys, where the encryption key can be defined as a sequence of zeroes and ones, which both parties involved in the connection known and unknown to a third party [8]. There are several classic algorithms used to distribute keys across an unreliable channel, such as Diffie-Hellman and RSA. Although the principles used by classical algorithms are different, they generally depend on the computational complexity of a prime factors problem or a discrete logarithm.

On the other hand, quantum key distribution (QKD) is the most interesting area in the field of information security, due to the exploitation of the laws of quantum physics to allow the exchange of secret keys between the two parties [6].

A series of quantum states is transmitted over a public quantum channel (such as a fiber-optic channel). The first quantum key distribution protocol was proposed by Charles H. Bennet and Gilles Brassard in 1984 called BB84 in which two bases are used (rectilinear + and diagonal $\times$) to generate four non-orthogonal polarized quantum states ($\longrightarrow = 0°$, $\uparrow = 90°$, $\nearrow = 45°$, $\nwarrow = 135°$) [5].

The BB84 protocol can be summarized in two stages. The first stage involves preparing the photons using random bases specific of the sender and sending them through the quantum channel, while these photons are measured at the receiver side using its own bases. While the second stage is through a classic channel in which it is agreed on the bases that were used by the two parties.

In addition, the condition of the probability of Alice and Bob choosing

the same basis and obtaining a successful measurement, the quantitative error rate (QBER) is added [10]. Due to random assignment of a bit value, double-click events cause 50% of the error rates.

In this paper, we propose to optimize BB84 protocol by relying on the graph theory where the bases are coded using an agreed graph at both ends. Thus, the quantum channel is only used to transmit photons (quantum states) and the classical channel is not needed in process of key distribution [9].

In our work, adjacency matrix is extracted from the graph to be coded into quantum bases, thus both parties will obtain identical bases. In this way, the time required to prepare the quantum encryption key is reduced and the quantum bit error rate (QBER) is reduced, thus increasing the key space in a more efficient manner.

This paper reviews related works in Section 2 and in Section 3 describing the graph theory and its application in coding theory. Section 4 presents the proposal to enhance BB84 protocol using the graph theory, while in Section 5 an illustrative example is provided. We review the experimental results and the security analysis of the proposed protocol in Section 6 and conclude the paper in Section 7.

2. Related works

There are many studies in the field of quantum cryptography that dealt with the modified BB84 protocol, and in this section we review some important contributions.

The researchers in [16] proposed a new method for modifying the BB84 protocol based on two-way classical and parallel entanglement protocol purification. The proposed protocol was optimized to reduce QBER and the results reached a maximum error rate of 20%. On the other hand, the

general declaration of the rules was dispensed in this model.

The researchers in [4] used the quantum key distribution protocol (BB84) with traditional cryptography to obtain more secure authentication mechanisms and also reduce authentication cost.

Whereas researchers in [14] presented a solution to the problem of insecurity in the classical key distribution methods, and the solution to this problem is obtained through the use of quantum key distribution, where QKD reduces risks in key distribution and thus provides high security in addition to error detection.

The authors in [1] proposed another way to enhance the quantum key distribution protocol BB84, that came from using the basis of the original BB84 protocol. The proposal is based on enabling the two parties to negotiate a shared secret key without using the classic channel. Their results indicated that the proposed protocol utilized approximately 60%–80% of the bits generated therefore provide better results compared to the standard BB84 protocol.

The researchers in [2] relied on the Legendre symbol to encode a stream of bits into polarized photons. In their proposal, a public channel was not used to negotiate the bases. Rather, both the sender and the receiver negotiate to use the Legendre code function and then only use a quantum channel, thus reducing the time and increasing the length of the final key.

In [3] the researchers proposed a hybrid protocol based on QKD protocol and public key cryptography in order to obtain a strong key based on the quantum physical properties and mathematical intricacies of the public key algorithm.

3. Graph theory

Graph theory is one of the most important branches of applied mathematics [11]. A graph G is expressed by a group of vertices V and a group of edges E that link the vertices to each other. Where vertices represent a finite set while edges represent binary relationship on vertices, and edges represent a pair of vertices (v, u).

In graph theory, two ways to represent graphs are adjacent list and adjacent matrix.

- Adjacent list: consists of an array of vertices where for every vertex V, adjacent V list contains all vertices adjacent to it.

- Adjacent matrix: is a square matrix consisting of $|V| * |V|$, where $|V|$ represent number of vertices in graph. Each value in the matrix indicates whether the vertex pairs are adjacent or not in the graph.

  Therefore, the proximity matrix M with size $n \times n$ associated with G can be defined by:

$$v_{ij} = \begin{cases} p, & \text{if there is a path from } v_i \text{ to } v_j; \\ 0, & \text{if there is no path from } v_i \text{ to } v_j, \end{cases} \tag{1}$$

  where p is the weight of the edge. In a special case (un-weighted graph) the adjacent matrix is a matrix (0, 1) and defined by:

$$v_{ij} = \begin{cases} 1, & \text{if there is a path from } v_i \text{ to } v_j; \\ 0, & \text{if there is no path from } v_i \text{ to } v_j. \end{cases} \tag{2}$$

On the other hand, graph theory is an essential component of cryptography and information security as it is successfully integrated and allows the development of more robust cryptographic algorithms which have proven difficult to crack [13]. So there are many researchers, who have highlighted the use of graph theory in many applications in computer science.

4. Proposed protocol

In the proposed algorithm we used a random algorithm to generate the graphs randomly. In the graph algorithm, we need to determine the number of vertices and the link probability of each vertex (The number of nodes and the probability of edges for each node are assigned randomly). Algorithm 1 shows the basic steps for generating random graphs.

Algorithm 1: Generate graphs randomly
Input: Number of vertices (n), Probability of edges $P(E)$ Output: Graph $G(V, E)$ where vertices (V); edge (E) 1. $V \leftarrow \{0, 1, 2, \cdots, n-1\}$ 2. $E \leftarrow 0$ 3. For each $\{V_i, V_j\} \in V$,where $V_i \neq V_j$ do 4. $R \leftarrow$ random (0,1) 5. If $R < P(E)$ then 6. $E \leftarrow E \cup \{V_i, V_j\}$ 7. return $G(V, E)$.

After generating the graph randomly, the phase of generating the quantum bases begins, depending on the graph as follows:

a) The first step is to calculate the matrix adjacent to the graph, as the matrix consists of a number of rows and columns (n, m).

b) Then the binary matrix is converted into a one dimensional matrix by reading row after row of the binary matrix.

c) Finally, each value in the binary array (a) is coded to a quantum base depending on the following condition:

$$\text{Quantum Bases} = \begin{cases} +, & \text{if } a_i = 0; \\ \times, & \text{if } a_i = 1. \end{cases} \tag{3}$$

And thus obtaining a series of quantum bases that are used by the sender to initialize the photons and by the receiver to perform the measurement process for these photons. The sender generates a series of random bits as a raw key and prepares the photons, as shown in Table 1.

Table 1: **Preparation of polarized photons by sender**

Random bits	Quantum bases	Polarized photon
0	+	$\rightarrow = 0°$
1	+	$\uparrow = 90°$
0	×	$\nearrow = 45°$
1	×	$\nwarrow = 135°$

Then the sender sends these photons to the second party (receiver) through a quantum channel (such as a fiber optic channel). Meanwhile on the receiver side, the receiver uses the same quantum bases to measure the photons to calculate the value for each photon, as shown in Table 2.

Table 2: **Measurement of photons by receiver**

Quantum bases	Photon	Secret key
+	$\rightarrow$	0
+	$\uparrow$	1
×	$\nearrow$	0
×	$\nwarrow$	1

In the end, both parties get the same key without the need for a classic channel to agree with each other on the quantum bases used, as in the standard BB84 protocol.

In our proposal, we assume that the two parties ratify and agree on a set of graphs that are used to generate quantum bases before starting communications, and thus the two parties do not need to agree on quantum bases during the generation and exchange of quantum keys.

On the other hand, any unauthorized attempt to change the state

of the transmitted photon will be detected by the other party and the connection will be terminated because authentication is not achieved.

5. Working example

Suppose the graph was previously agreed upon between the two parties, the graph is as shown in Figure 1.

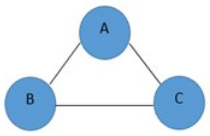

Fig. 1: Graph example (3 vertices and 3 edges)

The matrix adjacent to the graph at both ends is calculated as follows:

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

After that, the adjacent matrix is converted into a one-dimensional array by reading row after row, as follows:

$$[0, 1, 1, 1, 0, 1, 1, 1, 0]$$

Depending on this sequence of bits, both parties generate the common bases between them.

$$[+, \times, \times, \times, +, \times, \times, \times, +]$$

On the other hand, the sender generates a string of random bits as raw key and prepares the photons and sends them to the recipient while the recipient measures the photons using the bases generated by graph.

Table 3 illustrates an example of enhanced BB84 protocol based on graph theory. In the example, we will take Alice as the sender and Bob as the recipient.

Table 3: **Example of our proposed protocol**

Alice's bit	0	1	1	0	1	0	0	1	1
Alice's bases	+	×	×	×	+	×	×	×	+
Alice's polarization	→	↖	↖	↗	↑	↗	↗	↖	↑
Bob's bases	+	×	×	×	+	×	×	×	+
Bob's measurement	0	1	1	0	1	0	0	1	1
Shared secret key	0	1	1	0	1	0	0	1	1

6. Experiment results and analysis

This section includes evaluating the performance and efficiency of the enhanced BB84 protocol and its comparison with standard BB84 protocol, as well as how the protocol can react in terms of strength against specific attacks through a comprehensive security analysis.

6.1. Simulation results

Simulation performed with a Core i5 CPU processor associated with 4 GB RAM as a hardware, and Windows 10 pro (64-bit) as an operating system and programmed with Python programming language, PyCharm development environment.

Table 4 summarizes the main characteristics (number of vertices and number of edges) of the random graphs used to calculate the results. Also, the Figures 2, 3 and 4 display the graphs A, B and C in sequence.

Table 4: **The graphs characteristics used in our experiments**

Graph Name	No. Vertices	No. Edges
Graph A	8	11
Graph B	16	53
Graph C	32	205

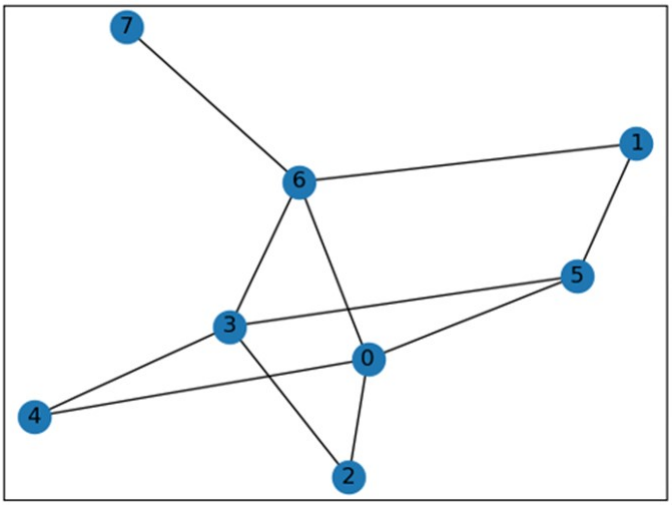

Fig. 2: Random graph generation (Graph A)

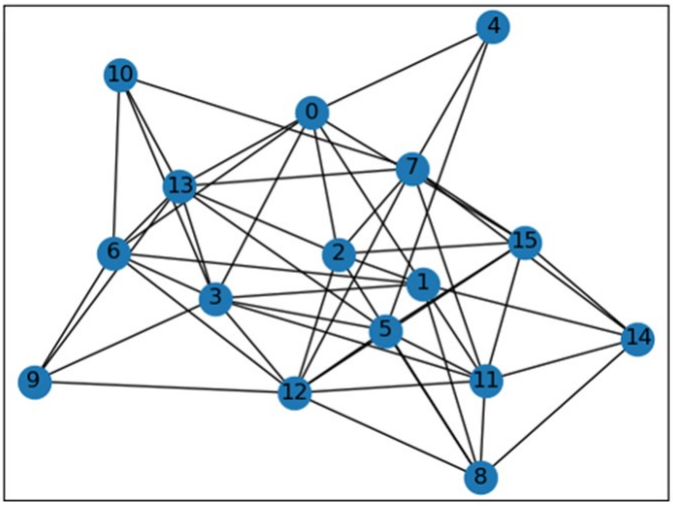

Fig. 3: Random graph generation (Graph B)

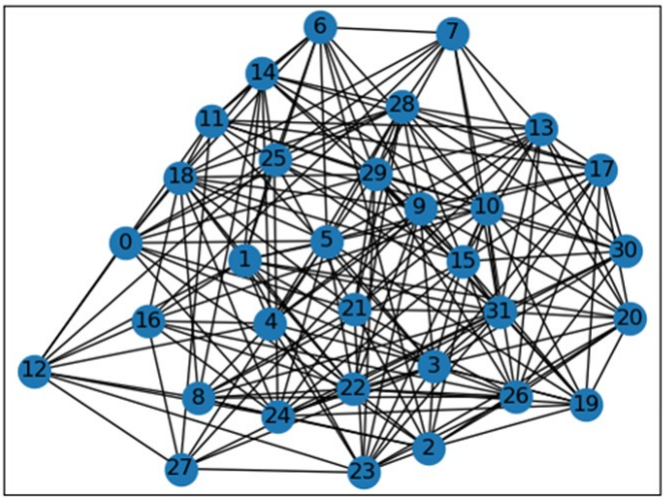

Fig. 4: Random graph generation (Graph C)

In order to evaluate our work, the standard BB84 protocol was implemented for the purpose of comparison with our graph-based work.

Table 5 shows the results of implementing the standard BB84 protocol with different initial key entries (raw key), while Table 6 shows the results of our proposal for the same entries. The results indicate the efficiency of our proposal in terms of key length and execution time as compared to the standard BB84 protocol.

Table 5: **Results of standard BB84 protocol execution**

Keys	Raw Key Length (in bit)	Execution Full Time (in millisecond)	Final Key Length (in bit)
Key 1	64	321	47
Key 2	256	337	196
Key 3	1024	369	713

Table 6: **Results of our proposed protocol execution**

Keys	Raw Key Length (in bit)	Execution Full Time (in millisecond)	Final Key Length (in bit)
Key 1	64	272	64
Key 2	256	290	256
Key 3	1024	353	1024

Figure 5 summarizes the difference in the final key length between the standard BB84 protocol and our proposal. Key length (key space) is one of the most important criteria for key strength against many attacks.

The main reason for the large key length of our proposal as compared to the standard BB84 is the ideal use of a graph to generate quantum bases at both parties.

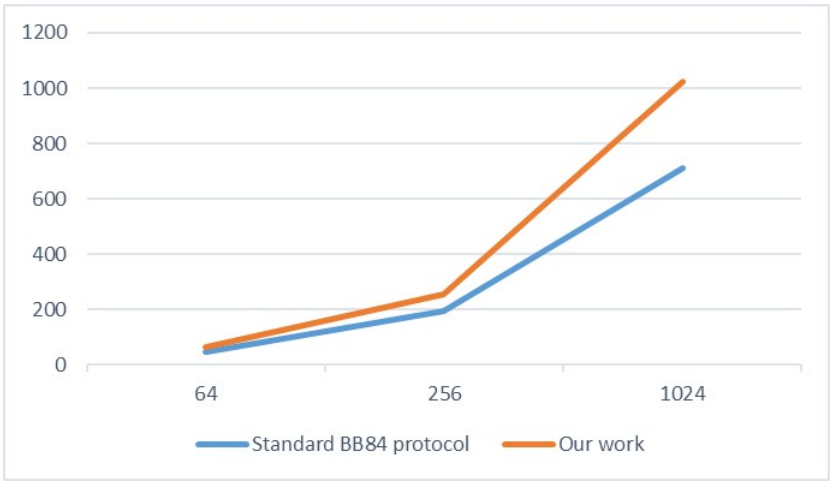

Fig. 5: Key length for standard BB84 protocol and our proposed protocol

Table 7 shows the results of the final keys randomization rate calculation of our proposed protocol. The NIST suites test is used through calculating the p-value, which represents the rate of randomness and whenever it is close to 1, i.e. the sequence contains a high randomness [18].

Table 7: **NIST (random numbers test) results of simulations of our work**

Statistical Test	P-value			Passed/Fail
	Key 1	Key 2	Key 3	
Frequency Test	0.4532	0.3815	0.7076	Pass
Block Frequency (n = 128)	0.4532	0.8592	0.6791	Pass
Runs	0.0662	0.8393	0.1050	Pass
Approximate Entropy	1	1	0.9995	Pass
Cumulative Sums	0.42224	0.6292	0.8313	Pass

6.2. Security analysis

The space and sensitivity of a key are the most important strength points of any key against attacks such as a brute force attack. In our proposal we were able to achieve the highest key space, thus reducing the QBER in the key compared to the standard BB84 protocol and the reframes [2], [3].

Figure 6 shows the difference in key length between our proposal and previous works. The key space refers to 2^n and n is considered the length of key where a brute force attack needs 2^{n-1} try to obtain the key used. This process is very difficult for a brute-force attack based on classic and quantum computers [12], [7].

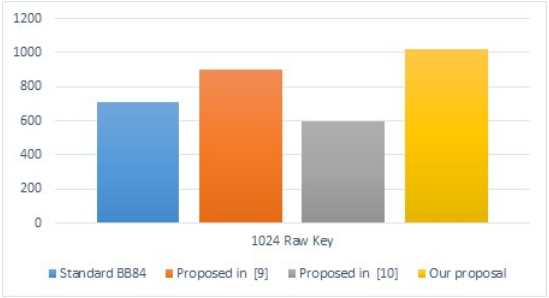

Fig. 5: Comparison of key length with previous works

The error rate depends on whether or not any noise exists on the

communication channel. Therefore, the permissible error threshold limit rate is determined.

On the other hand, the sensitivity of the key is one of the most important criteria, and depends on the physical properties of the photons sent through the quantum channel, it has a high sensitivity that allows the two parties to detect any change that takes place in the state of the photon [17].

In our proposal, there is no classical channel for agreement between the two parties on the bases used, and therefore there are no parameters available about the key for the attacker. Any attempt by the attacker to change the state of the quantum photon leads to the breaking of the photon and its discovery by both parties depending on the quantum laws [6], [17].

7. Conclusion

In this paper, an improved protocol was proposed over the standard BB84 protocol. Our proposal was based on the bases generation graph. The proposed protocol has been clarified in detail and its advantages over the standard BB84 protocol are highlighted, as our proposal does not depend on the existence of a classic (public) channel between the two parties.

The simulation was carried out using Python language, and the results showed the effectiveness of our proposal in terms of key length and greatly reduced QBER compared to previous work. Therefore, our proposal is considered the best solution to achieve security for future quantum communications.

Acknowledgement. We would like to express our sincere gratitude to the referees for their valuable suggestions and comments which improved the paper.

References

[1] A.A. Abdullah and Y.H. Jassem, *Enhancement of Quantum Key Distribution Protocol BB84*, Journal of Computational and Theoretical Nanoscience, 16 (2019), 1138–1154.

[2] A.A. Abdullah, R.A. Khalaf abd H.B. Habib, *Modified BB84 quantum key distribution protocol using legendre symbol*, 2019 2nd Scientific Conference of Computer Sciences (SCCS), pp.154–157.

[3] A.A. Abdullah and S.S. Mahdi, *Hybrid Quantum-Classical Key Distribution*, October, 10–14, 2019. https://doi.org/10.35940/ijitee.1081219

[4] S.T.F. Al-janabi and O.K. Jasim, *Reducing the Authentication Cost in Quantum Cryptography*, In The 12th Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNet2011), UK , June 2011, pp.363-368.

[5] C.H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science*, 560 (2014), 7–11. https://doi.org/10.1016/j.tcs.2014.05.025

[6] D. Bruss, G. Erdélyi, T. Meyer, T. Riege and J. Rothe, *Quantum cryptography: A survey*, ACM Computing Surveys (CSUR), 39 (2007), 6-es.

[7] L. Chen, L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner and D. Smith-Tone, Report on post-quantum cryptography, US Department of Commerce, National Institute of Standards and Technology (2016).

[8] T. Elgamal, *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, I, 1985, 469–472.

[9] G.-J. Fan-Yuan, C. Wang, S. Wang, Z.-Q. Yin, H. Liu, W. Chen, D.-Y. He, Z.-F. Han, and G.-C. Guo, *Afterpulse analysis for quantum key distribution*, Physical Review Applied, 10 (2018), 64032.

[10] G.-J. Fan-Yuan, C. Wang, S. Wang, Z.-Q. Yin, H. Liu, W. Chen, D.-Y. He, Z.-F. Han, and G.-C. Guo, *Modeling alignment error in quantum key distribution based on a weak coherent source*, Physical Review Applied, 12 (2019), 064044.

[11] D.A. Marcus, *Graph theory*, Vol. 53 (2020), American Mathematical Soc.

[12] V. Mavroeidis, K. Vishi, M.D. Zych and A. Jøsang, *The impact of quantum computing on present cryptography*, International Journal of Advanced Computer Science and Applications, 9 (2018), 405–414. https://doi.org/10.14569/IJACSA.2018.090354

[13] P.L.K. Priyadarsini, *A survey on some applications of graph theory in cryptography*, Journal of Discrete Mathematical Sciences and Cryptography, 18 (2015), 209–217.

[14] R.D. Sharma and A. De, *A new secure model for quantum key distribution protocol*, 6th International Conference on Industrial and Information Systems(2011), pp.462–466.

[15] D.R. Stinson and M. Paterson, Cryptography: Theory and Practice, CRC Press (2018).

[16] K. Wen and G.L. Long, *Modified Bennett-Brassard 1984 quantum key distribution protocol with two-way classical communications*, Physical Review A, 72 (2015), 22336.

[17] W.K. Wootters and W.H. Zurek, *The no-cloning theorem*, Physics Today, 62 (2009), 76–77. https://doi.org/10.1063/1.3086114.

[18] J. Zaman and R. Ghosh, *Review on fifteen statistical tests proposed by NIST*, Journal of Theoretical Physics and Cryptography, 1 (2012), 18–31.

College of Science
University of Diyala
Diyala
Iraq
E-mail: drrifaat8@gmail.com

College of Science
University of Diyala
Diyala
Iraq
E-mail: arbah_sultan@yahoo.com

Al-Mustaqbal University College
Babylon
Iraq
E-mail: suadad.safaa@mustqbal-college.edu.iq

(*Received: March, 2022; Revised: April, 2022*)