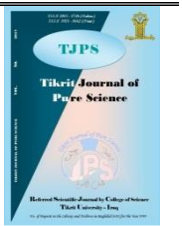
IASJ
المجلات الاكاديمية العراقية

Tikrit Journal of Pure Science
ISSN: 1813 – 1662 (Print) --- E-ISSN: 2415 – 1726 (Online)

Journal Homepage: http://tjps.tu.edu.iq/index.php/j



A Hybrid Cryptosystem based on Latin Square and the Modified BB84 Quantum Key Distribution

Hamza B. Habib, Wadhah Abdulelah Hussein, Asmaa Kh. Abdul-Rahman

College of Science, University of Diyala, Diyala, Iraq

https://doi.org/10.25130/tjps.v27i4.42

ARTICLE INFO.

Article history:

-Received: 11 / 4 / 2022
-Accepted: 13 / 6 / 2022
-Available online: / / 2022

Keywords: Latin square, quasigroup, BB84 protocol, Legendre symbol, cryptography.

Corresponding Author:

Name: Hamza B. Habib

E-mail:

halsaadi18@yahoo.com ,
wadhah.hussein2@gmail.com,
asmaaalshaiby@gmail.com

Tel:

ABSTRACT

A new algorithm to improve the security of the transmitted data over the communication channels is presented in this paper. This algorithm is combining Latin square with the modified version of the BB84 Quantum Key Distribution protocol. As the order of the Latin square increases, then $N(L^n)$, which is the total number of Latin squares of *order-n*, increases quickly. Moreover, the modified BB84 key distribution protocol is a secure method to exchange the encryption keys between two parties. The reason behind that is that the modified BB84 uses the Legendre symbol to generate the quantum key, and it uses the quantum channel only to perform the distribution process instead of using both channels, classic and quantum, as in the standard BB84 protocol. Therefore, the proposed algorithm is secure, reliable and efficient for future communications.

1. Introduction

In the past few years, transmitting data over insecure communication channels has increased. To keep the transmitted data confidential over these channels, cryptography is used. Cryptography, which is an application of Number Theory, is the method of converting the plaintext to a ciphertext known only to the two parties ([1] and [2]). Using Latin squares in cryptography provides the feature of constructing algebraic cryptographical systems because the total number of Latin squares $N(L^n)$ of order-n increases quickly with n, (see [3] and [4]). However, such systems become insecure with the technology advances. Thus, quantum systems are used in cryptography to prevent attackers from breaking the encrypted messages.

In quantum information, the quantum key distribution (QKD) is considered to be a secure method to distribute the keys between two parties ([5] and [6]). The reason behind that is it can detect whether the eavesdropper exists when the key distribution process is performed. The earliest protocol presented for QKD was BB84 in 1984 which uses both quantum and classical channels to distribute the keys [7]. However, using two channels in the BB84 protocol means the execution of the protocol should be repeated to reduce the quantum error rate. Without repeating the execution makes the quantum error rate high, and that leads to terminating the BB84 protocol and starting the protocol over again [8]. Starting the protocol over again means more time to implement the key distribution [8].

The Legendre symbol is used to improve the security of some cryptosystem algorithms including the modified BB84 protocol ([8], [9] and [10]). Using the Legendre symbol to improve the security of the BB84 protocol provides the idea of applying two distinct BB84 protocols to encode and decode the message [8]. Moreover, the modified BB84 protocol uses only the quantum channel that makes the execution process not repeated if the error rate is exceeding a certain limit [8]. In this study, we present the construction of a new cryptosystem based on combining the Latin squares with the modified BB84 Quantum Key Distribution. In section 2, we first recall the modified BB84 protocol. In section 3, we discuss Latin Square and Quasigroup. In section 4, we present the proposed algorithm. Finally, we provide a conclusion to the study in section 5.

2. The Modified BB84 Quantum Key Distribution Protocol

In this section, we recall the modified algorithm of the BB84 quantum key distribution protocol that was presented in [8]. The modification is based on using the Legendre symbol to choose a suitable filter for each transmitted photon. The algorithm states that let p be an agreed prime number between the two parties, then the polarizing filters (→,↗,↑ and ↖) are applied to send a bit string of length $(p-1)$.

Both parties calculate the Legendre symbol $\left(\frac{a}{p}\right)$, where $1 \leq a < p$, and they transmit the data based on the agreed secret formula, Formula 1.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \begin{cases} \rightarrow, \text{if the bit is } 0; \\ \uparrow, \text{if the bit is } 1. \end{cases} \\ -1, \begin{cases} \nwarrow, \text{if the bit is } 0; \\ \nearrow, \text{if the bit is } 1. \end{cases} \end{cases} \quad \dots (1)$$

3. Latin Square and Quasigroup

3. 1 Basic Definitions

Definition (1) A $n \times n$ matrix of distinct symbols is called a Latin square of order-n, and it is denoted by L^n, if each symbol exactly appears once in each column and each raw, (see [3]).

Example (1) A Latin square L^3 is given below.

$$\begin{matrix} a & b & c \\ c & a & b \\ b & c & a \end{matrix}$$

Definition (2) A reduced Latin square is a Latin square L^n, such that, its first raw and first column are in the natural order, (see [11]).

Example (2) The Latin square L^3 below is in the reduced form.

$$\begin{matrix} a & b & c \\ b & c & a \\ c & a & b \end{matrix}$$

Definition (3) The process of performing one or more of the following operations, row permutation, column permutation, and symbols permutation on a Latin square L^n is said to be Isotopy. The resulting Latin square is called Isotopic to the original Latin square [12].

Example (3) Suppose we have the two Latin squares below, L_1^3 and L_2^3.

$$\begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{matrix} \qquad \begin{matrix} 3 & 2 & 1 \\ 1 & 3 & 2 \\ 2 & 1 & 3 \end{matrix}$$

Latin squares L_1^3 Latin squares L_2^3

L_2^3 is resulting from L_1^3 after changing the positions of the first and third columns; therefore, the two Latin squares are Isotopic.

Definition (4) Let $N(L^n)$ denotes to the total number of Latin squares of order-n, then $N(L^n)$ is given as

$N(L^n) = n!\,(n-1)\,LR^n$,

where LR^n is the number of reduced Latin squares of order-n, (for more information regarding $N(L^n)$ see [3] and [11]).

Definition (5) A nonempty set S with the binary operation $*$ is called quasigroup, which is denoted by $(S, *)$ if it satisfies the conditions below, (see [13]),

i. $\forall\, r, s \in S$, then $r * s \in S$.

ii. $\forall\, r, s \in S$, $\exists$ unique $x, y \in S$, such that, $r * x = s$ and $y * r = s$.

Example (4) Let $S = \mathbb{Z}_4 = \{0, 1, 2, 3\}$, and let $x * y = (x +_4 y)\ (mod\ 4)$, such that,

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Therefore, $(S, +_4)$ is a quasigroup.

Note (1) If the order of the set S, which is denoted by $|S|$, equals n, then $(S, *)$ form a Latin square of order-n. Also, the Isotopy property is an unlimited source of quasigroups of order-n.

3. 2 The Encryption and Decryption Processes

The encryption process is performed by Bob (the sender) as follows, (see [3]):

1. Given a quasigroup $(S, *)$, where $|S| = n$.
2. Convert the message M of n characters to suitable numerical blocks.
3. A positive number $k < n$ is chosen.
4. The encoded message $(EM\ )$ is given as

$$\begin{matrix} EM_1 = k * b_1, \\ EM_i = EM_{i-1} * b_i, \end{matrix} \quad \dots (2)$$

where b_1 is the 1^{st} block, and b_i is the i^{th} block, such that, $2 \leq i \leq n$. Therefore, $EM = \{EM_i\}_{i=1}^{n}$ is the encoded message, and it is sent to Alice.

The decryption process is performed by Alice as follows, (see [3]):

1. Alice constructs a quasigroup $(S, \circ)$ by using Formula (3).

$$r \circ s = t \Leftrightarrow r * t = s, \dots \dots (3)$$

where $r, s, t \in S$.

2. Alice uses Formula (4) for the decryption process.

$$\begin{matrix} b_1 = k \circ EM_1, \\ b_i = EM_{i-1} \circ EM_i,\ \ i = 2, 3, \cdots, n, \end{matrix} \quad \dots (4)$$

where k is the same as in the encryption process. Therefore, the original message is recovered.

4. The Proposed Algorithm

4.1 Theoretical Part

The proposed algorithm is based on combining the Latin square with the modified algorithm of the BB84 protocol as shown in Figure 1. Both Bob and Alice agree on choosing a prime number p.

The Encryption Process

1. Be calculates the Legendre symbol $\left(\frac{a}{p}\right)$, where $1 \leq a < p$.

2. By Formula (1), Bob sets the suitable filter (↑,→,↖ or ↗) for each transmitted bit of the quantum key Qk.

3. Bob considers a quasigroup $(S, *)$, where $|S| = n$.

4. Bob chooses a positive number k, such that, $k < n$.

5. Bob converts the message M to a numerical form based on ASCII code and then to suitable blocks.
6. Using Formula (2), Bob finds the encoded message $EM = \{EM_i\}_{i=1}^{n}$.
7. Bob applies the operation XOR on the binary form of EM with Qk to get the ciphertext C, which will be sent to Alice.

Note (2) $(S, *)$, p and k are shared secretly with Alice.

The Decryption Process

1. Alice calculates the Legendre symbol $\left(\frac{a}{p}\right)$, where $1 \le a < p$.
2. From Formula (1), Alice uses suitable filters to find Qk.
3. Alice applies XOR operation on C and Qk to get the encoded message $EM = \{EM_i\}_{i=1}^{n}$.
4. By Formula (3), Alice constructed the quasigroup $(S, \circ)$.
5. Alice finds the original massage M by Formula (4).

4. 2 Practical Example

For simplicity, suppose that Bob and Alice choose an agreed prime number p, say $p = 29$. Then, Bob calculates the Legendre symbol. By using Formula (1), Bob sets the suitable filter for each bit of the quantum key Qk as shown in Table 1.

Table 1: The quantum key using the Legendre symbol along with the used filters.

a	$\left(\frac{a}{p}\right)$	Qk	Polarization Filter
1	1	1	↑
2	-1	0	↖
3	-1	0	↖
⋮	⋮	⋮	⋮
26	-1	1	↗
27	-1	0	↖
28	1	0	→

Now, suppose that the quasigroup of order 4 with the operation $*$ is given as

$*$	0	1	2	3
0	2	0	3	1
1	1	3	0	2
2	3	1	2	0
3	0	2	1	3

Bob chooses an agreed number k, such that $k \in \{0, 1, 2, 3\}$, say $k = 1$.

Now, if Bob wants to send the plaintext M = ccbda to Alice, firstly, Bob converts the plaintext to a numerical form as ccbda ⟶ 22130 and into blocks as 2 2 1 3 0. To encode the blocks, Bob uses the Formula (2), then

$$EM_1 = 1 * 2 = 0$$
$$EM_2 = 0 * 2 = 3$$
$$EM_3 = 3 * 1 = 2$$
$$EM_4 = 2 * 3 = 0$$
$$EM_5 = 0 * 0 = 2$$

Therefore, the encoded message is $EM = 03202$, and the binary form of it is given as

00000 00011 00010 00000 00010

Now, Bob applies the operation XOR on EM and Qk as shown in Table 2 to get the ciphertext.

Table 2: EM XOR Qk

Encoded Message	00000	00011	00010	00000	00010
Quantum Key	10010	11010	11001	01001	11101
Ciphertext	10010	11001	11011	01001	11111

Therefore, the ciphertext C is 1001011001110110100111111, and it will be sent to Alice.

After receiving the ciphertext, Alice calculates the Legendre symbol. By Formula (1), she uses the Legendre symbol along with the suitable filter to find the quantum key Qk, (see Table 1). Also, she applies the XOR operation on C and Qk to get the encoded message as shown in Table 3.

Table 3: The C XOR Qk

Ciphertext	10010	11001	11011	01001	11111
Quantum Key	10010	11010	11001	01001	11101
Encoded Message	00000	00011	00010	00000	00010

Alice now converts the resulting string to decimal to get $EM = \{0, 3, 2, 0, 2\}$. Then, by Formula (3) the quasigroup $(S, \circ)$ is constructed. That is,

$\circ$	0	1	2	3
0	1	3	0	2
1	2	0	3	1
2	3	1	2	0
3	0	2	1	3

By Formula (4) and $k = 1$, then

$$b_1 = 1 \circ 0 = 2$$
$$b_2 = 0 \circ 3 = 2$$
$$b_3 = 3 \circ 2 = 1$$
$$b_4 = 2 * 0 = 3$$
$$b_5 = 0 * 2 = 0$$

Thus, the string 22130 is converted to the plaintext M = ccbda.

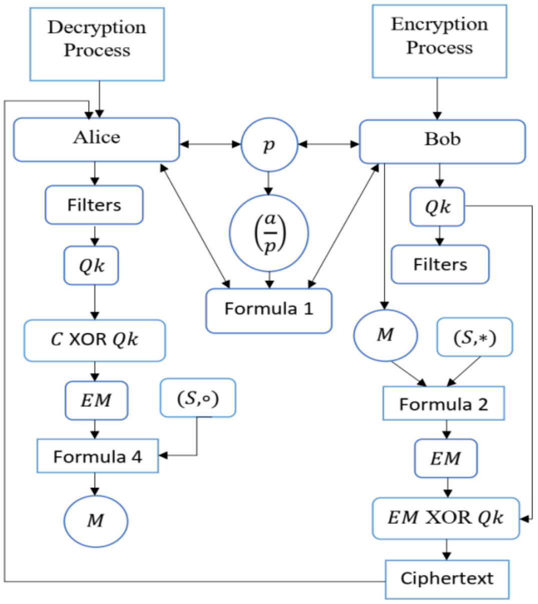


Fig. 1: The structure of the proposed algorithm

5. Conclusions

A new algorithm to enhance the security of the transmitted data over the communication channels is proposed in this paper. This algorithm is constructed by using the modified BB84 protocol and Latin square. The modified BB84 protocol is a secure method to distribute the encryption keys between two parties because it generates the quantum key based on the Legendre symbol, and it uses only the quantum channel to distribute the keys. Moreover, as n , which is the order of the used Latin Square, goes larger, then the total number of Latin squares $N(L^n)$ of order n goes larger. That is, a huge number of Latin squares (quasigroups) is generated, and this makes it harder for the attackers to break the transmitted data. Therefore, combining the modified BB84 protocol along with the Latin square provide a high level of security to the proposed algorithm.

References

[1] Barakat, M., Eder, C. and Hanke, T., 2018. “An introduction to cryptography”. *Timo Hanke at RWTH Aachen University*, pp.1-145.

[2] Easttom, W., 2021. “Essential Number Theory and Discrete Math”. In *Modern Cryptography* (pp. 73-104). Springer, Cham.

[3] Pal, S. K., Kapoor, S., Arora, A., Chaudhary, R. & Khurana, J., “Design of strong cryptographic schemes based on Latin Squares”, *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 13, no. 3, pp. 233–256, 2010, doi: 10.1080/09720529.2010.10698290

[4] McKay, B.D. and Wanless, I.M., 2022. “Enumeration of Latin squares with conjugate symmetry”. *Journal of Combinatorial Designs*, *30*(2), pp.105-130.

[5] Charles H. Bennett, Gilles Brassard, “Quantum cryptography: Public key distribution and coin tossing”. *Theoretical Computer Science*, Volume 560, Part 1, 2014, Pages 7-11, https://doi.org/10.1016/j.tcs.2014.05.025.

[6] Bunandar, D., Govia, L.C.G., Krovi, H. *et al.* “Numerical finite-key analysis of quantum key distribution”. *npj Quantum Inf* **6,** 104, 2020. https://doi.org/10.1038/s41534-020-00322-w

[7] Abdullah, Alharith A., Rifaat Z. Khalaf, & Hamza B. Habib. “Modified BB84 Quantum Key Distribution Protocol Using Legendre Symbol”. *2nd Scientific Conference of Computer Sciences (SCCS), University of Technology – Iraq, IEEE*, 2019.

[8] Habib, H. B. “Modifying Playfair Cipher Algorithm by using Legendre Symbol”. *Diyala Journal for Pure Science (DJPS)*, vol. 15, no. 4, pp. 74-84, 2019. DOI: https://dx.doi.org/10.24237/djps.15.04.502A

[9] Habib, H. B., Wadhah Abdulelah Hussein, & Diana Saleh Mahdi. “Improving the security of the Knapsack Cryptosystem by using Legendre Symbol”. *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 11, pp. 2249-2255, 2021.

[10] Schmidt, N. O. “Latin Squares and Their Applications to Cryptography”. *Boise State University*. 016.

[11] Grošek, Otokar and Sýs, Marek. “Isotopy of latin squares in cryptography”. *Tatra Mountains Mathematical Publications*, vol.45, no.1, pp.27-36, 2012 https://doi.org/10.2478/v10127-010-0003-z

[12] Prasad, V.B.V.N., & J.Venkateswara Rao. “Characterization of Quasigroups and Loops”. *International Journal of Scientific and Innovative Mathematical Research (IJSIMR)*, vol. 1, no. 2, pp. 95-102, 2013.

نظام تشفير هجين يعتمد على المربع اللاتيني و البروتوكول BB84 المعدل لتوزيع المفتاح الكمي

حمزة بركات حبيب ، وضاح عبد الاله حسين ، أسماء خوام عبد الرجمن

كلية العلوم , جامعة ديالى ، ديالى , العراق

الملخص

في هذا البحث تم تقديم خوارزمية جديدة لتحسين أمن البيانات المرسلة عبر قنوات الاتصال. تجمع هذه الخوارزمية بين المربع اللاتيني والنسخة المعدلة من بروتوكول BB84 لتوزيع المفتاح الكمي. بحيث انه مع زيادة رتبة المربع اللاتيني, فأن $N(L^n)$, والذي هو العدد الكلي للمربعات اللاتينية ذات الرتبة n, يزداد بسرعة فائقة. علاوة على ذلك ، يعد بروتوكول BB84 المعدل لتوزيع المفتاح طريقة آمنة لتبادل مفاتيح التشفير بين طرفين. السبب وراء ذلك هو أن BB84 المعدل يستخدم رمز Legendre لتوليد المفتاح الكمي، ويستخدم القناة الكمية فقط للقيام بعملية التوزيع بدلاً من استخدام كلتا القناتين، الكلاسيكية والكمية، كما هو الحال في بروتوكول BB84 الأعتيادي. لذلك ، فإن الخوارزمية المقترحة آمنة وموثوقة وفعالة للاتصالات المستقبلية.