JCTA Journal of Computing Theories and Applications ISSN:3024-9104

Research Article

Hybrid Quantum Key Distribution Protocol with Chaotic System for Securing Data Transmission

De Rosal Ignatius Moses Setiadi[1],* and Muhamad Akrom[1],[2]

[1] Informatics Engineering Department, Faculty of Computer Science, Dian Nuswantoro University, Semarang 50131, Indonesia; e-mail : moses@dsn.dinus.ac.id

[2] Research Center for Materials Informatics, Faculty of Computer Science, Dian Nuswantoro University, Semarang 50131, Indonesia; e-mail : m.akrom@dsn.dinus.ac.id

* Corresponding Author : De Rosal Ignatius Moses Setiadi

Abstract: This research proposes a combination of Quantum Key Distribution (QKD) based on the BB84 protocol with Improved Logistic Map (ILM) to improve data transmission security. This method integrates quantum key formation from BB84 with ILM encryption. This combination creates an additional layer of security, where by default, the operation on BB84 is only XOR-substitution, with the addition of ILM creating a permutation operation on quantum keys. Experiments are measured with several quantum measurements such as Quantum Bit Error Rate (QBER), Polarization Error Rate (PER), Quantum Fidelity (QF), Eavesdropping Detection (ED), and Entanglement-based detection (EDB), as well as classical cryptographic analysis such as Bit Error Ratio (BER), Entropy, Histogram Analysis, and Normalized Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI). As a result, the proposed method obtained satisfactory results, especially perfect QF and BER, and EBD, which reached 0.999.

Keywords: Hybrid BB84; Post-Quantum Key Exchange**;** Secure Data Transmission; Quantum Cryptography; Quantum Key Distribution.

Received: November, 25th 2023
Revised: December, 18th 2023
Accepted: December, 19th 2023
Published: December, 20th 2023

1. Introduction

The development of internet technology is increasingly rapid and has become a human need today to speed up message sending and data transmission. Cyber attacks are the main challenge in sending messages and data transmission [1]–[3]. Cryptographic technology is essential to data security [4], where cryptography will be directly related to data. If the computer's protection has been breached, then cryptography is the only last bastion. Chaos systems are a cryptographic method that is very popular in use today. This is due to its extreme level of sensitivity to initial conditions and control parameters, pseudorandom properties, ergodicity, and aperiodicity [3]–[6]. Logistic maps are chaotic systems that are very popular and are continually being developed to produce higher levels of randomness. One of the developments in the logistic map method is the improved logistic map (ILM)[4], [6], [7]. One indicator of ILM's superiority is the increase in Lyapunov exponent (LE) compared to traditional logistic maps. Like a logistic map, ILM only has one dimension, parameter, and initial value, so it is relatively uncomplex and can be efficient for encryption.

The key is the most important component in the encryption process. In chaotic algorithms, parameters and initial values can be used as keys. Even though the key has been made complex and has a large key space, if there is a man-in-the-middle attack during the key transmission process, the unprotected key is easily known to third parties. However, if the key has fallen to a third party in an encrypted state, the key needs to be decrypted so the message cannot be immediately known. Quantum computing significantly impacts cryptography because it can compromise cryptographic security, especially in key cracking. Quantum computing has characteristics such as superposition and entanglement to solve difficult mathematical problems quickly[8], [9]. Quantum algorithms such as Shor[10] and Grover[11] can threaten the classical encryption algorithms commonly used today. Shor's algorithm, which is designed to solve factorization problems at high speed, threatens asymmetric cryptography such as Rivest Shamir Adleman (RSA), while Grover's algorithm can solve search problems with quadratic speed and can speed up symmetric key searches in hash functions[12].

According to Vernam's theory[13] which is confirmed by Shanon[14], One-Time Pad (OTP) encryption is considered absolutely safe because it uses a random key that is only used once. However, there are obstacles in implementing OTP practically because key distribution problems and the existence of true random numbers are difficult to achieve. So truly secure key distribution over insecure channels is impossible because information can be replicated[15]. This can be solved with quantum key distribution (QKD) technology. The QKD protocol has a foundation of the quantum no-cloning theorem[16], which is related to superposition and entanglement. In the context of no-cloning, these quantum states cannot be copied perfectly because the cloning process would involve separating one state from a superposition, which is impossible without disturbing the other states[17], [18]. An entangled state is a condition where the states of several quantum particles depend on each other. Perfect cloning is impossible to produce from an entangled state, because the cloning process will damage the entangled state. Quantum cryptography also has the characteristic of true randomness, this is closely related to the probabilistic properties of quantum mechanics. This characteristic differs from the pseudorandom generator (PRNG) in classical encryption, which has deterministic properties. So, with quantum mechanics, "OTP" can be done to provide very safe protection in the key distribution process.

One of the well-known QKD methods is the BB84 protocol developed by Charles Bennett and Gilles Brassard [19], [20]. BB84 is a protocol that relies on quantum principles to securely secure the exchange of cryptographic keys between the sender (Alice) and the recipient (Bob). After receiving the qubits from Alice, Bob randomly selects a measurement base for each qubit received and performs measurements on those qubits. Bob's use of a random basis is important to avoid incorrect measurements, which could occur if Alice and Bob did not use the same basis. After taking measurements, Alice and Bob share public information about the bases they used for each qubit. They then compared the basis they used for a particular qubit and discarded the measurement results on those qubits that did not have a matching basis. The appropriate measurement results will form the cryptographic key used for encryption and decrypting messages that will be sent classically in the future. The advantages of the BB84 protocol include reliability in distributing quantum keys, resistance to intercept-resend attacks because quantum properties cannot be measured or observed without interference, and efficiency in exchanging quantum keys using relatively simple qubits [21]–[23]. The BB84 protocol became the basis for developing other QKD protocols and is one of the earliest and best-known examples of real applications of quantum cryptography in information security. Based on the literature above, this paper contributes to combining a combination of the QKD method and the ILM chaotic system. This provides double protection for messages and keys, so it can provide protection that is more resistant to attacks.

2. Preliminaries

2.1. Quantum Protocol BB84

BB84 is a quantum protocol used for quantum cryptographic key exchange between two parties, Alice (sender) and Bob (receiver). The basic concept of BB84 involves the principles of quantum mechanics, such as using qubits and measurements on a specific basis. A qubit is a basic unit of quantum information that can be represented by a photon, a particle of light that functions as a qubit in a quantum system. The general representation of a qubit ($|\psi\rangle$) can be described by Equation (1).

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

Where Equation (1) represents the quantum superposition state of the qubit. Here, $|0\rangle$and $|1\rangle$ are the basis of the quantum system (usually associated with the base of classical computing in quantum computing), which represents the ground state of the qubit (usually associated with the "up" and "down" spins in a given quantum system), $\alpha$and $\beta$are the complex coefficients that each represents the amplitude or probability of finding a qubit in state $|0\rangle$and $|1\rangle$, provided that $\alpha^2 + \beta^2 = 1$ corresponds to the normalization condition for quantum states.

Furthermore, regarding the practical implementation of BB84 on quantum hardware, Hadamard gates (H) and Rx gates (for x-axis rotation) can be used to manipulate qubits in x-basis or to adjust the polarization of photons, which creates the necessary polarization angles. Equations (2) and (3) refer to the mathematical representation of the H gate and Rx gate in the context of their use for qubit manipulation in the BB84 protocol.

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{2}$$

$$Rx(\theta) = \frac{1}{\sqrt{2}}\begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix} \tag{3}$$

Where θ is the angle of rotation, $-i$ is a complex imaginary unit, where $i^2 = -1$.

Here, Rx(θ) is an x-axis rotation gate that manipulates the qubit phase by θ (in radians) along the x-axis in its matrix representation. Hadamard (H) gates are used in BB84 to prepare qubits on an x basis before sending or measurement.

The development of the BB84 protocol focuses on the exchange of quantum information and the application of quantum mechanical principles to create secure cryptographic keys based on measurements in the base. How BB84 works in general is as follows:

1. Alice generates pairs of quantum qubits. Each qubit can be in one of four quantum states representing two bases, usually Z-basis: $\{|0\rangle, |1\rangle\}$and X-basis $\{|+\rangle, |-\rangle\}$. The gate $H$is applied to each qubit that is in base X, creating a superposition between $|+\rangle$and $-|-\rangle$, while the Rx gate is not applied to qubits that are in base Z, so they remain in state $\{|0\rangle, |1\rangle\}$.
2. For each qubit, Alice randomly chooses one of two bases (Z or X) to measure that qubit. Alice sends the qubit along with the base used to Bob. For example, if there is a message 11011010, and the base chosen by Alice is ZXXZXZXZ or 01101010, then the resulting qubit, polarity and angle are in Table 1.

Table 1. Alice Qubit.

Message	Base	Qubit	Polarity	Polarity Angel
1	Z	$|1\rangle$	$|\uparrow\rangle$	0°
1	X	$|-\rangle$	$|\rightarrow\rangle$	90°
0	X	$|-\rangle$	$|\rightarrow\rangle$	90°
1	Z	$|1\rangle$	$|\uparrow\rangle$	0°
1	X	$|-\rangle$	$|\rightarrow\rangle$	90°
0	Z	$|1\rangle$	$|\uparrow\rangle$	0°
1	X	$|-\rangle$	$|\rightarrow\rangle$	90°
0	Z	$|1\rangle$	$|\uparrow\rangle$	0°

3. Bob receives qubits from Alice, and for each qubit, he randomly chooses one of the bases to measure it with. The base chosen randomly by Bob is ZXXZXZXZ or 11011010, so the measurement results are presented in Table 2.

Table 2. Bob Measurement.

Base	Measurement	Polarity	Polarity Angel	Results
Z	$|1\rangle$	$|\uparrow\rangle$	0°	Match
X	$|-\rangle$	$|\rightarrow\rangle$	90°	Match
X	$|-\rangle$	$|\rightarrow\rangle$	90°	Match
Z	$|0\rangle$	$|\downarrow\rangle$	180°	Not Match
X	$|-\rangle$	$|\rightarrow\rangle$	90°	Match
Z	$|1\rangle$	$|\uparrow\rangle$	0°	Match
X	$|+\rangle$	$|\nearrow\rangle$	45°	Not Match
Z	$|1\rangle$	$|\uparrow\rangle$	0°	Match

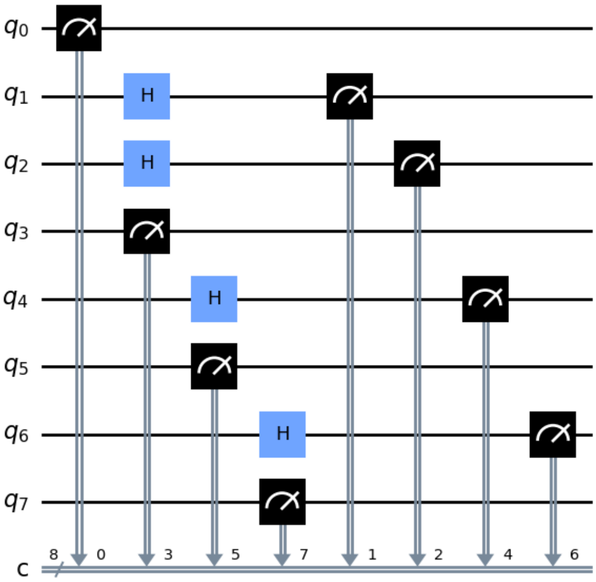


Figure 1. Illustration of BB84 Protocol implementation (based on steps 1-3)

4. Alice and Bob exchange information about the basis they used to measure each qubit, but do not provide measurement results.
5. Alice and Bob retain measurement results only when the bases used by both match. This creates a subset of exchanged qubits that can be used for cryptographic key formation. From the example above, a subset of qubits is produced $|1\rangle, |-\rangle, |-\rangle, |1\rangle, |-\rangle, |1\rangle, |+\rangle, |1\rangle$.
6. The same subset of qubits is used to form a cryptographic key, which in the example above produces the key 10111011. This key is secure because quantum properties prohibit measurements that do not strictly correspond to the quantum state being measured, and involve XOR operations.

2.2 Improved Logistic Map (ILM)

ILM is a development of the traditional logistic map introduced by and has now been implemented in several encryption studies such as [24], [25]. ILM was introduced in the context of information security and image encryption. In ILM, an iteration formula differentiates it, namely, the one presented in Equation (4).

$$x_{n+1} = 2\alpha - \alpha_n^2/\alpha \tag{4}$$

Where x_n is initial, and α is the parameter for iteration, α_n is a constant parameter, and a full mapping range of $x_n \in [-2\alpha, 2\alpha]$.

Equation (3) will produce a chaotic sequence that can be used for permutation and substitution operations. The advantage of ILM lies in its ability to create a more expansive key space and a more extensive mapping range compared to standard logistic maps. This can increase the complexity and level of chaos in generating values during the iteration process, thereby providing a better level of security. In addition, using the Lyapunov exponent concept in ILM provides a deeper understanding of the chaotic nature of its iterations, which can be an additional advantage in improving the security of encryption systems.

3. Proposed Method

The BB84 algorithm has been modified in research [9]to improve its performance by combining it with the Sailfish Optimization Algorithm (SOA), AES and RC4. This research proposes to improve the performance of BB84 by hybridizing it with the ILM method. However, BB84 has provided security by converting bits to qubits, which can be in a state of superposition or rotation. ILM is implemented to add permutation effects to the BB84 encryption process, which only uses the XOR operation by default. A combination of XOR-substitution and permutation operations can produce super encryption on BB84. What super encryption means is an encryption method that consists of at least two layers to combine substitution and permutation operations [25], so that encryption becomes increasingly difficult to crack and intercepted by irresponsible parties. The BB84-ILM hybrid method is illustrated in Figure 2, and the stages of the proposed method are explained in detail in sections 3.1 to 3.3.

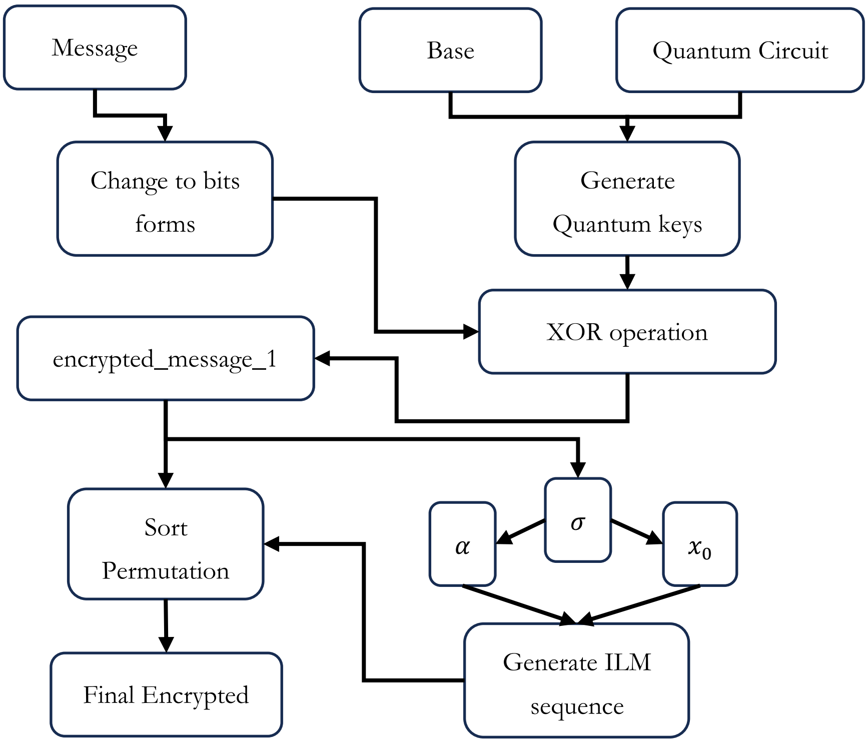


Figure 2. Proposed Hybrid BB84-ILM.

3.1. Read Message and Generate Quantum Key

1. Read the message, then break the message into several blocks, in this case, each block only consists of 8-bits due to limited quantum resources used. For each bit in the message that Alice will encrypt, it is randomly selected between 0 and 1.
2. Each of these bits becomes part of the quantum key that will be sent to Bob. Use Hadamard basis if bit equals 0 or Rx basis with a random angel if bit equals 1, according to the bits generated by Alice.
3. The selection of bases and the resulting bits form a quantum key (qubit). In other words, the quantum key Alice generates consists of a number of qubits that represent the bits of the message to be encrypted. Alice's choice of basis on each qubit creates a quantum representation of the classical bits.

3.2. Encrypt Message

1. Quantum messages and keys are used as input at this stage.
2. Encrypt each bit of the original message using an XOR operation with the corresponding quantum key bit, thus obtaining encrypted_message_1.
3. Convert each bit of encrypted_message_1 to an integer, then calculate the standard deviation (σ) value of encrypted_message_1. Use the values σas $\alpha$and $x_0$as ILM input, while the number of iterations is the length of encrypted_message_1, so get the ILM sequence and calculate it with Equation (3).
4. Use the ILM sequence for permutation operations on encrypted_message_1 to get final_encrypted_message. Please note that the permutation operation does not change the value σ, so the value $\sigma$of final_encrypted_message will be the same as encrypted_message_1

3.3. Decrypt Message

1. At this stage final_encrypted_message and quantum key are used as input. Bob receives the quantum key by reading the qubits with the appropriate basis.
2. Calculate the standard deviation (σ) value of final_encrypted_message. Use the values σ as $\alpha$and $x_0$as ILM input, while the number of iterations is the length of final_encrypted_message.
3. After obtaining the same ILM sequence as the encryption stage, do inverse permutation on final_encrypted_message to get decrypted_message_1.
4. To obtain a decrypted message, perform an XOR operation with the appropriate quantum key.

4. Implementation and Results

This research used a Jupyter notebook with the Python programming language to implement the proposed method. The implementation is not carried out with quantum hardware but uses a quantum simulator, namely Qiskit. In order to activate this simulator, you need to import several libraries, such as QuantumCircuit Aer, and execute from Qiskit. Apart from that, the random and numpy libraries are also used. The random library generates random bit selections, while numpy is used to process array data. The implementation of the proposed method described above is explained in the stages below:

4.1 Dataset Gathering

In the research, a text dataset was used, which was generated from the URL www.lipsum.com. Five types of messages were generated with lengths of 128, 512, 1024, 4096, and images with dimensions of 128×128. Next, we remove all entered characters from the text so that the number is precisely the same. Sample message generated by lorem ipsum generators and standard image used are presented in Table 3.

Table 3. Sample Message Dataset.

Message Length	Message
128 bytes	Lorem ipsum dolor sit amet, … eu dapibus leo posuere accumsan.
512 bytes	Lorem ipsum dolor sit amet, … Aenean id erat non tortor efficitur.
1024 bytes	Lorem ipsum dolor sit amet, … gravida vitae, sagittis a tellus.
4096 bytes	Lorem ipsum dolor sit amet, … , odio ac gravida dapibus cras amet.
128×128 pixels	

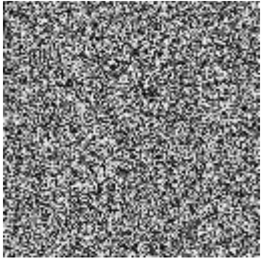
4.2 Encryption Results and Quantum Assessment

In Table 4, the encryption results and quantum assessment are presented. In the encryption column field, the encryption results are presented at the beginning and end of the text because the text is very long if written in full. The following fields contain an assessment of quantum bit error rate (QBER), polarization error rate (PER), quantum fidelity (QF), eavesdropping detection (ED), and entanglement-based detection (EBD). Each assessment is explained in sections 4.2.1 to 4.2.5.

4.2.1 Quantum Bit Error Rate (QBER)

QBER is a parameter used to assess the extent to which the quantum key sent from the sender to receiver Bob is error-prone. QBER is calculated as the ratio between the number of mismatched key bits and the total number of key bits sent on a certain basis [20], see Equation (5). QBER is important to tell how well the quantum key is working. The smaller

Table 4. Encryption Results.

Message	Encryption Results	QBER	PER	QF	ED	EBD
Text 128 bytes	[TNÂ²Â¸ ÃŸV—————— 8Â□ MÂ … eÃ©Ã¹Ã½_Â¶	0.4511	0.3333	1.0	0.25	0.9999
Text 512 bytes	êéczËWb□ X7jWýE□ Ên~… e- …. □ "»*bqÜ□ ü□ iCŸ	0.4936	0.1666	1.0	0.3333	0.9999
Text 1024 bytes	ïj± É'GØVdª Ê□ .□ +Åçªö1 ….	0.4946	0.5	1.0	0.375	0.9999
Text 4096 bytes	□ è|øz BùÞ□ >a¬ÖH L□ ?£¡¸¨iGN□ Hú&¢°óµ¼ … □ àSÂn<W}Á.ô¤“ Êf□	0.4891	0.5	1.0	0.25	0.9999
Image 128×128 pixels		0.4619	0.3333	1.0	0.25	0.9999
	Average	**0.4781**	**0.3666**	**1.0**	**0.2917**	**0.9999**

the QBER value, the better. The QBER value needs to be managed because a low value indicates that the quantum keys sent and received are almost identical, so they are safe from tampering. However, the QBER value is difficult to approach zero because the sender chooses a base randomly to send qubits, and the receiver also chooses a base randomly to assess the qubits received. Due to choosing different bases, some measurement results will not match. Therefore, the focus is not on an absolute value of zero, but on minimizing the QBER so that the risk of interference is as minimal as possible.

$$QBER = \frac{Number\ of\ mismatched\ bits}{Total\ number\ of\ bits\ measured\ in\ a\ specific\ basis} \tag{5}$$

QBER is typically measured during the decryption process, where the number of mismatched bits refers to the count of bits that do not match between the expected and assessed values, and the total number of bits measured on a specific basis is the total number of qubits measured by the receiver (Bob) using a specific basis.

Table 4 shows that the QBER value is relatively high but does not exceed 0.5. However, it is important to note that QBER does not necessarily indicate a protocol failure or an irreparable error. Essentially, quantum key protocols are designed to detect possible interference or eavesdropping but cannot always correct every error. More sophisticated error correction and the use of more robust intrusion detection methods may be required to reduce QBER further.

4.2.2 Polarization Error Rate (PER)

PER is a metric that can assess how often the polarization of photons sent in a quantum protocol experiences errors during transmission. In the context of quantum key protocols such as BB84, photon polarization represents the quantum bit value, and PER assesses how often this polarization does not match the expected one [26]. PER is calculated as the ratio of the number of incorrectly measured quantum bits to the total number of quantum bits measured on a specific basis. Equation (6) represents the PER calculation.

$$PER = \frac{Number\ of\ incorrect\ bits}{Total\ number\ of\ bits\ measured\ in\ a\ specific\ basis} \tag{6}$$

It should be noted that PER is measured on each basis, and PER values can vary depending on the basis used. Generally, PER values range from 0 to 1. Low PER values are more desirable because they indicate higher accuracy in measuring photon polarization.

PER measurements are usually carried out at the decryption stage after the photons sent by Bob arrive. When Bob receives a photon, he matches the polarization of the received photon with the basis he chose during the sending phase by Alice. If the polarization of the photon does not match the basis chosen by Bob, a polarization error occurs, which is calculated in PER. In other words, PER gives an idea of how often the photons received by Bob do not match the polarization he should have chosen. These assessments help assess the quality of the quantum key distribution. The PER values presented in Table 4 show fluctuating and different results, although the average value is relatively smaller than QBER.

4.2.3 Quantum Fidelity (QF)

QF is a assess of the similarity between two quantum states. It measures how close one quantum state is to another. In the context of quantum information and computing, QF is often used to assess the quality of quantum operations, gates, or algorithms. This provides a way to evaluate how well a quantum system can replicate a targeted quantum state. QF between two quantum states $|\psi\rangle$and $|\phi\rangle$can be calculated with Equation (7) [27].

$$QF(\psi,\phi) = |\langle\psi|\phi\rangle| \quad (7)$$

Where $\langle\psi|\phi\rangle$is the inner product of the two states, and $|\langle\psi|\phi\rangle|^2$is the square of the modulus of the inner product. Fidelity has a value range between 0 and 1, where 1 indicates perfect similarity between the two states, $0 < F < 1$ indicates states that are similar but not identical, and 0 means orthogonal states.

Fidelity can also be used to detect snooping attempts (eavesdropping) in the BB84 protocol. Interactions with the quantum system may affect fidelity if a third party attempts to intercept the transmitted quantum key. Low-fidelity measurements can indicate the presence of snoopers. The value 1.0 in Table 4 indicates very good performance results of the proposed method.

4.2.4 Eavesdropping Detection (ED)

ED involves a comparison of the expected quantum key with the received one. The Mismatch Ratio measures how big the difference is between the supposed and received keys, and high values can indicate potential information theft attempts. Quantum security protocols are designed to detect and overcome eavesdropping to maintain the confidentiality of information sent over quantum channels [9]. The Mismatch Ratio value for eavesdropping detection ranges from 0 (no mismatch) to 1 (all key bits do not match). The higher the Mismatch Ratio value, the greater the indication of an eavesdropping attempt or interference with the sent quantum key, and vice versa. Therefore, a low Mismatch Ratio value is desirable to ensure the security of quantum communications. ED can be calculated using Equation (8).

$$ED = \frac{Number\ of\ mismatched\ bits}{Total\ number\ of\ bits\ in\ the\ quantum\ key} \quad (8)$$

Where the number of mismatched bits is the number of key bits that do not match between the supposed quantum key and the received quantum key, while the total number of bits in the quantum key is the total number of bits in the quantum key used for communication.

4.2.5 Entanglement-Based Detection (EBD)

EBD is used to assess the extent to which two qubits in a state generated by a Bell circuit are related to entanglement and detect interference in the quantum channel. Entanglement is a phenomenon in quantum mechanics in which the states of two or more particles are quantum related such that the state of one particle cannot be explained independently of the state of another particle. In the context of the Bell circuit being created, the main goal is to generate a Bell state, which is a type of entangled state for two qubits. The most general Bell state is $\left(|00\rangle + |11\rangle/\sqrt{2}\right)$, which is a superposition of two different elementary states. Concurrence measurements provide information about the degree of entanglement between two qubits.

Concurrence values range between 0 (no entanglement) and 1 (full entanglement). The higher the concurrence value, the stronger the entanglement [27]. Equation (9) is used to calculate the concurrence value.

$$C_\rho = \max(0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4) \tag{9}$$

Where ρ is the reduced state matrix reflecting the quantum state of the two qubits. $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ is the singular value of the reduced matrix in non-decreasing order.

In Table 4, it appears that the total EBD value is 0.9999, this is very close to 1 (full entanglement), where full entanglement can ensure that the particles involved in the quantum key distribution are quantum related. This means that any measurement attempt by a third party will change the state of the particle, and the communicating party can detect this. Therefore, entanglement can provide an additional layer of security against potential eavesdropping.

4.3 Classical Assessment

4.3.1 Bit Error Ratio (BER) and Entropy

BER and Entropy testing on the classical side of QKD implementations have an important role in evaluating the security and performance of quantum cryptographic systems. After the quantum key exchange process, the key is used to secure the classical message. BER testing of classical messages after classical encryption and decryption processes helps asses the extent to which the message can maintain its integrity during transmission over a quantum channel. By comparing the messages before and after the classical process, a number of bit errors can be identified. BER encryption can be calculated by comparing each bit in the encrypted and original messages. Meanwhile, decryption BER can be calculated by comparing each bit in the original and decrypted messages. The BER values for encryption and decryption are generally the opposite, for encryption, it must have a value of around 0.5, which means that the desired uncertainty in the encryption process can work well. Meanwhile, the ideal decryption BER value is close to or equal to zero [28]. However, the decryption BER value does not guarantee security but proves data integrity or in other words the decryption process can run perfectly. BER can calculate with Equation (10).

In addition, Entropy testing on classical messages that have been encrypted with quantum keys measures the level of uncertainty or complexity of the information contained in the message. Entropy is also included in the category of statistical tests on encryption. A message with high Entropy means it carries a lot of information that is difficult to predict. This combination of tests helps ensure the reliability and security of the quantum cryptographic process on the classical side, confirming that messages remain secret and their integrity is maintained after going through classical encryption and decryption steps. A good entropy value, in this case, should be close to 8 because the value calculation uses 2^8. Entropy can calculate with Equation (11).

Table 5. BER and Entropy Results.

Message	**BER**		**Entropy**	
	Encryption	**Decryption**	**Original**	**Encryption**
Text 128 bytes	0.51465	0	4.0186	6.5389
Text 512 bytes	0.51277	0	4.1232	7.5808
Text 1024 bytes	0.49841	0	4.1776	7.8402
Text 4096 bytes	0.50058	0	4.2121	7.9568
Image 128×128 pixels	0.49969	0	7.0451	7.9888

Based on Table 5, all encryption BER values are close to 0.5, this shows the success of the quantum protocol in providing random properties to encrypted messages. Meanwhile, all decryption BERs are 0, meaning the proposed method can work perfectly. The increase in Entropy in encrypted messages emphasizes the additional uncertainty obtained from quantum protocols. Overall, these results illustrate that the quantum protocol provides good security and integrity in the encryption and decryption process on the classical side based on BER and Entropy.

$$BER = \frac{Number\ of\ Bits\ in\ Error}{Total\ Number\ of\ Transmitted\ Bits} \tag{10}$$

$$H = \sum_{i=1}^{n} p(c_i)log_2\left(\frac{1}{p(c_i)}\right) \tag{11}$$

Entropy H is computed by considering the overall count of symbols (n), the information conveyed by each ciphertext element c_i, and the probability of occurrence for eachc_i denoted by $p(c_i)$.

4.3.2 Normalized Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI)

NPCR and UACI assessments are generally used to analyze the resistance of encryption methods to differential attacks[6]. NPCR is used to assess the percentage of pixel changes between two different encrypted images, while UACI assesses the average intensity of pixel changes, where both encrypted images are produced by modifying a small portion of the plaintext.[6], [29]. In this study, plaintext changes were made to the very first byte by subtracting one. The NPCR and UACI values should ideally be ≈ 0.9961 and ≈ 0.3346, respectively. Table 6 shows the results of NCPCR and UACI assessments, where based on the results of these measurements, the proposed method gets results that are very close to the ideal value, thus showing that this method is proven to be resistant to differential attacks.

$$NPCR = \left[\frac{1}{N \times M}\sum_{i=1}^{N}\sum_{j=1}^{M} Diff(i,j)\right],$$
$$Diff(i,j)\begin{cases}0\ if\ C1(i,j) = C2(i,j)\\ 1\ if\ C1(i,j) \neq C2(i,j)\end{cases} \tag{12}$$

$$UACI = \left[\frac{1}{N \times M}\sum_{i=1}^{N}\sum_{j=1}^{M}\frac{|C1(i,j) - C2(i,j)|}{255}\right] \tag{13}$$

$C1$ and $C2$ denote the initial cipher and the modified cipher, respectively. N and M refer to the width and height dimensions, respectively, while i and j specify the coordinates of individual pixels.

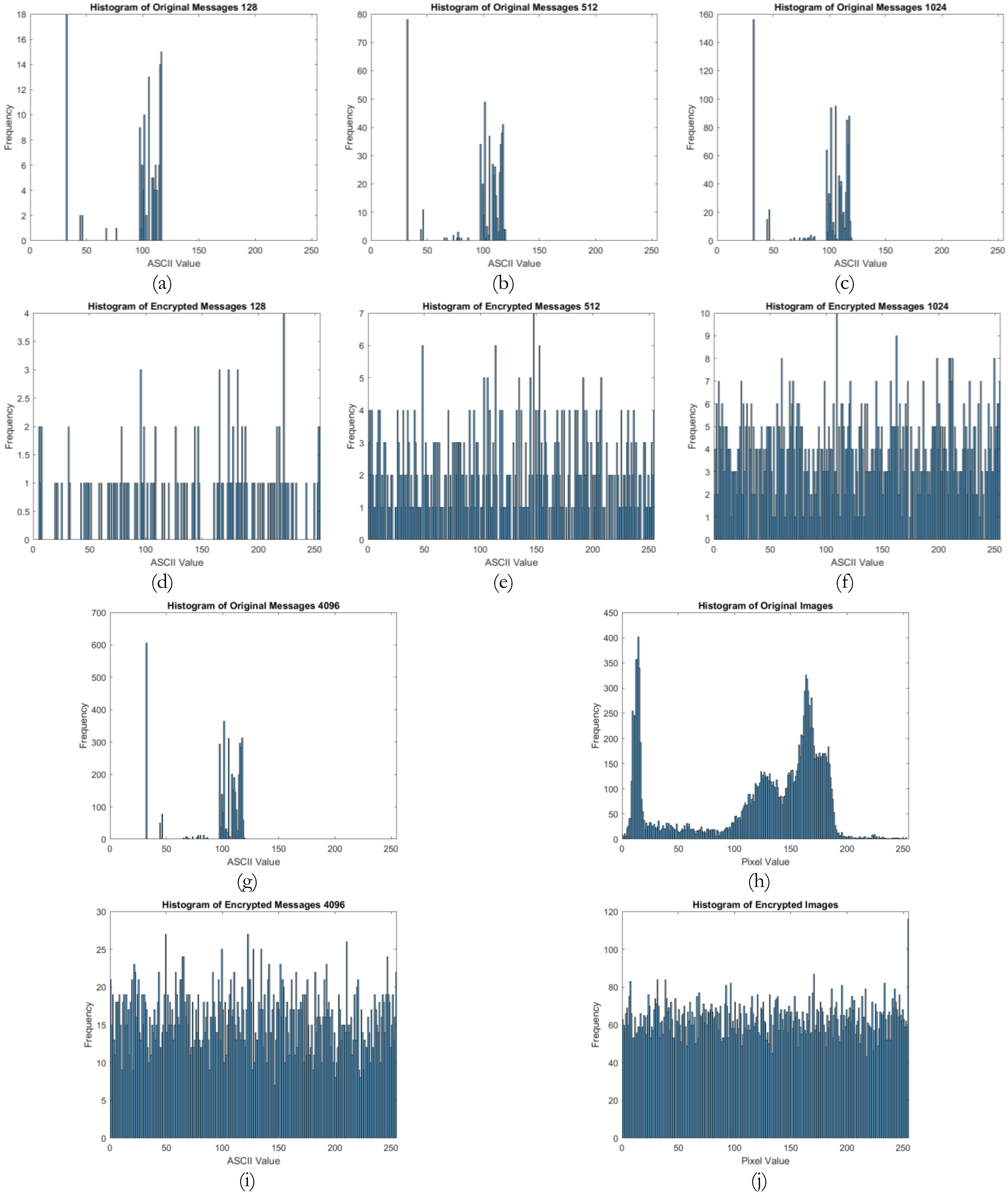
Table 6. NPCR and UACI Results.

Message	NPCR	UACI
Text 128 bytes	0.9922	0.3421
Text 512 bytes	0.9941	0.3347
Text 1024 bytes	0.9941	0.3326
Text 4096 bytes	0.9968	0.3303
Image 128×128 pixels	0.9959	0.3354

4.3.3 Histogram Analysis

Histograms can provide insight into how even or varied data distribution in classical messages is before and after quantum encryption and decryption processes. By observing the histogram, the distribution pattern of pixel or bit values in the message can be identified, allowing the observer to see changes that may occur during the cryptographic process.

On the classical side, histogram analysis can help detect potential interference or oddities in messages after going through a quantum protocol. The even distribution of the histogram indicates that the quantum encryption and decryption process does not cause major changes in the message values. On the other hand, a significant change in the histogram distribution could suggest interference or modification of the message during quantum processing. The histogram of the original and encrypted messages is presented in Figure 3, where it can be seen that the histogram of the encrypted image has a relatively uniform distribution, which indicates that the proposed cryptography method can work well.



(a) (b) (c) (d) (e) (f) (g) (h) (i) (j)

Figure 3. Message Histogram (**a**) Original Messages 128 bytes; (**b**) Encrypted Messages 128 bytes; (**c**) Original Messages 512 bytes; (**d**) Encrypted Messages 512 bytes; (**e**) Original Messages 1024 bytes; (**f**) Encrypted Messages 1024 bytes; (**g**) Original Messages 4096 bytes; (**h**) Encrypted Messages 4096 bytes; (**i**) Original Images 128×128 pixels; (**j**) Encrypted Images 128×128 pixels.

5. Conclusions

This research has successfully implemented a combination of the QKD BB84 protocol and the ILM chaotic system. So the encryption algorithm becomes more complex. Not only does the XOR operation between the quantum key and the message but also permutation operations are carried out based on ILM. This adds a layer of security to the data transmission system. This method has been tested with quantum and classical assessments, where satisfactory results were obtained based on the assessment results. The encryption and decryption process can work as expected, especially for QF and EBD assessments. Meanwhile, the QBER and PER values may need to be increased again because the values are still relatively high. However, QBER does not always indicate a protocol failure or an uncorrectable error. Quantum key protocols are designed to detect interference or eavesdropping, although they cannot always correct every error. To further reduce QBER, more sophisticated error correction methods and more robust fault detection are needed, as well as PER. Testing under classical conditions has also shown satisfactory results based on BER, Entropy, histogram analysis, NPCR and UACI values.

Author Contributions: Conceptualization: D.R.I.M.S.; methodology: D.R.IM.S.; software: D.R.IM.S. and M.A.; validation: D.R.IM.S. and M.A.; formal analysis: D.R.IM.S. and M.A.; investigation: D.R.IM.S. and M.A.; resources: D.R.IM.S.; data curation: D.R.IM.S.; writing—original draft preparation: D.R.IM.S.; writing—review and editing: D.R.IM.S. and M.A.; visualization: M.A.; funding acquisition: all.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] D. R. I. M. Setiadi, R. Robet, O. Pribadi, S. Widiono, and M. K. Sarker, "Image Encryption using Half-Inverted Cascading Chaos Cipheration," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 61–77, Oct. 2023, doi: 10.33633/jcta.v1i2.9388.

[2] B. M. P. Waseso and N. A. Setiyanto, "Web Phishing Classification using Combined Machine Learning Methods," *J. Comput. Theor. Appl.*, vol. 1, no. 1, pp. 11–18, Aug. 2023, doi: 10.33633/jcta.v1i1.8898.

[3] P. N. Andono and D. R. I. M. Setiadi, "Improved Pixel and Bit Confusion-Diffusion Based on Mixed Chaos and Hash Operation for Image Encryption," *IEEE Access*, vol. 10, no. November, pp. 115143–115156, 2022, doi: 10.1109/ACCESS.2022.3218886.

[4] E. Winarno, K. Nugroho, P. W. Adi, and D. R. I. M. Setiadi, "Integrated dual hyperchaotic and Josephus traversing based 3D confusion-diffusion pattern for image encryption," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 9, p. 101790, Oct. 2023, doi: 10.1016/j.jksuci.2023.101790.

[5] D. R. I. M. Setiadi, E. H. Rachmawanto, and R. Zulfiningrum, "Medical Image Cryptosystem using Dynamic Josephus Sequence and Chaotic-hash Scrambling," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6818–6828, Oct. 2022, doi: 10.1016/j.jksuci.2022.04.002.

[6] E. Winarno, K. Nugroho, P. W. Adi, and D. R. I. M. Setiadi, "Combined Interleaved Pattern to Improve Confusion-Diffusion Image Encryption Based on Hyperchaotic System," *IEEE Access*, vol. 11, pp. 69005–69021, 2023, doi: 10.1109/ACCESS.2023.3285481.

[7] C. Han, "An image encryption algorithm based on modified logistic chaotic map," *Optik (Stuttg).*, vol. 181, no. December 2018, pp. 779–785, Mar. 2019, doi: 10.1016/j.ijleo.2018.12.178.

[8] C. Bernhardt, *Quantum Computing for Everyone*. Fairfield University: MIT Press, 2019.

[9] S. K. Sehgal and R. Gupta, *SOA Based BB84 Protocol for Enhancing Quantum Key Distribution in Cloud Environment*, vol. 130, no. 3. Springer US, 2023. doi: 10.1007/s11277-023-10354-y.

[10] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134. doi: 10.1109/SFCS.1994.365700.

[11] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*, 1996, pp. 212–219. doi: 10.1145/237814.237866.

[12] R. Kuang and A. Chan, "Quantum encryption in phase space with displacement operators," *EPJ Quantum Technol.*, vol. 0, 2023, doi: 10.1140/epjqt/s40507-023-00183-0.

[13] G. S. Vernam, "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications," *Trans. Am. Inst. Electr. Eng.*, vol. XLV, pp. 295–301, Jan. 1926, doi: 10.1109/T-AIEE.1926.5061224.

[14] C. E. Shannon, "Communication Theory of Secrecy Systems*," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.

[15] B. Qi, L. Qian, and H. Lo, "Quantum Encryption," in *Optical and Digital Image Processing*, Wiley, 2011, pp. 769–787. doi: 10.1002/9783527635245.ch34.

[16] A. A. Abdullah and S. S. Mahdi, "Implementing Quantum Image Security Algorithm Based on Geometric Transformation and Quantum Random Number Generation," *J. Eng. Sci. Technol.*, vol. 17, no. 5, pp. 3570–3582, 2022.

[17] A. M. A. Al-muqarm, F. Abedi, and A. S. Abosinnee, "Quantum Computing Cryptography and Lattice Mechanism," *J. Inf. Commun. Converg. Eng.*, vol. 20, no. 4, pp. 242–249, 2022, doi: 10.56977/jicce.2022.20.4.242.

[18] F. Cavaliere, J. Mattsson, and B. Smeets, "The security implications of quantum cryptography and quantum computing," *Netw. Secur.*, vol. 2020, no. 9, pp. 9–15, Sep. 2020, doi: 10.1016/S1353-4858(20)30105-7.

[19] N. S. Yanofsky and M. A. Mannucci, *Quantum Computing for Computer Scientists*. Brooklyn College, City University of New York: Cambridge University Press, 2008.

[20] H. Shu, "Asymptotically Optimal Prepare-Measure Quantum Key Distribution Protocol," *Int. J. Theor. Phys.*, vol. 62, no. 8, pp. 1–13, 2023, doi: 10.1007/s10773-023-05447-0.

[21] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, 1992, doi: 10.1007/BF00191318.

[22] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991, doi: 10.1103/PhysRevLett.67.661.

[23] G. Vest *et al.*, "Quantum key Distribution with a Hand-Held Sender Unit," *Phys. Rev. Appl.*, vol. 18, no. 2, p. 024067, Aug. 2022, doi: 10.1103/PhysRevApplied.18.024067.

[24] L. Moysis, A. Tutueva, C. Volos, D. Butusov, J. M. Munoz-Pacheco, and H. Nistazakis, "A Two-Parameter Modified Logistic Map and Its Application to Random Bit Generation," *Symmetry (Basel).*, vol. 12, no. 5, p. 829, May 2020, doi: 10.3390/sym12050829.

[25] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik (Stuttg).*, vol. 272, no. November 2022, p. 170316, Feb. 2023, doi: 10.1016/j.ijleo.2022.170316.

[26] A. Gaidash, A. Kozubov, S. Medvedeva, and G. Miroshnichenko, "The influence of signal polarization on quantum bit error rate for subcarrier wave quantum key distribution protocol," *Entropy*, vol. 22, no. 12, pp. 1–10, 2020, doi: 10.3390/e22121393.

[27] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2012. doi: 10.1017/CBO9780511976667.

[28] D. E. Sari, H. N. N. Muchsin, D. R. I. M. Setiadi, C. A. Sari, and E. H. Rachmawanto, "Hybrid encryption technique using cyclic bit shift and RC4," in *2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2019*, Nov. 2019, pp. 205–209. doi: 10.1109/ICITISEE48480.2019.9003848.

[29] D. R. I. M. Setiadi and N. Rijati, "An Image Encryption Scheme Combining 2D Cascaded Logistic Map and Permutation-Substitution Operations," *Computation*, vol. 11, no. 9, p. 178, Sep. 2023, doi: 10.3390/computation11090178.