Quantum Assisted Blockchain Security Model Using Artificial Intelligence to Reduce Quantum Attacks

Ammar AbdRaba Sakran[1,*], Ruwaida Mohammed Yas[2], Ali Fadhil Rashid[3], Massila Kamalrudin[4], Mustafa Musa[5]

[1]University of Information Technology and Communications, Baghdad, Iraq

[2]Informatics Institute for Postgraduate Student, University of Information Technology and Communications, Iraq

[3]Department of Computer Science - College for Education of Pure Sciences - University of Wasit, Iraq

[4]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Malaysia

[5]Center of Research and Innovation Management, Universiti Teknikal Malaysia Melaka, Malaysia

Emails: ammarabdraba@uoitc.edu.iq; Roueida.m.yas@iips.edu.iq; alirashid@uowasit.edu.iq; massila@utem.edu.my; mustafmusa@utem.edu.my

Abstract

Presently, smart sensors ensure commercial decisions where integrated electronic systems can be securely organized using blockchain and quantum computing because of their unique characteristics and features. In the current scenario, large-scale quantum computers can be built in which most current cryptographic systems can be hacked. Since digital and quantum computers can conduct computations simultaneously, a quantum tool for blockchain framework design is required. Based on these concerns in this research, an enhanced quantum-assisted blockchain security model using the artificial intelligence (EQ-BSM-AI) technique has been proposed. This model validates cryptosystems and blockchain technologies to determine their vulnerability to quantum attacks. Further, in this model, quantum assisted edge computing technique has been used to model the Human-centric Internet of Things (HIoT) system by introducing a quantum key generation process. Based on the post-quantum blockchain (PQB), a secured cryptosystem that is highly resistant to quantum computer attacks has been introduced in this research. This quantum channel with multiple inputs and outputs (MIMO) is designed for a quantum-based communication system to make this model more efficient and withstand errors. In EQ-BSM-AI, an improved quantum encryption algorithm (IQEA) stores the keys for encryption with a generalized probability accumulation model. For the current quantum computers and communications, our proposed system resulted in an improved sampling error reduction of 12.4%, enhanced efficiency of quantum entanglement of 96.3%, information randomness of 93.9%, correlation analysis of 93.2%, and increased resistance to quantum computing attacks of 90.8% when compared with other existing approaches.

Keywords: Quantum Computing; Edge; Artificial Intelligence; Blockchain; Cryptography

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025

1. Introduction

All over the world, quantum computer science research has been gaining momentum in the last few years public-key cryptographic techniques such as Rivest-Shamir-Adleman (RSA) and elliptic-curve cryptography (ECC) will become less secure if quantum computers are being developed, as predicted [1]. Elliptic Curve Cryptography (ECC) is a key-based encryption method. For decryption and encryption of online traffic, ECC depends on pairs of public and private keys. ECC is commonly mentioned in combination with the Rivest-Shamir-Adleman (RSA) encryption method. RSA, on the other hand, is a method used by sophisticated computers to encrypt and decode messages. Asymmetric implies there are two distinct keys, because one of the keys may be supplied to anyone, known as public key cryptography. Quantum computing is a new technology that uses the rules of quantum physics to tackle problems that are simply too complicated for traditional computers. Traditional computing is based on the classical phenomena of electrical circuits being in a single state, either on or off, at any one moment. Elliptic Curve Cryptography (ECC) provides the same degree of encryption strength as the RSA (Rivest-Shamir-Adleman) method but with a lower key length. As a result, the speed and security provided by an ECC certificate for Public Key Infrastructure (PKI) are better than the RSA certificate. Latency and response time are reduced when computation is performed close to the network's logical edge. Endpoints are referred to as network edges. It is the initial step between the network's endpoints and its centre. These consist of PCs, adapters, modems, and the hardware that connects to them. The elements that offer services to people on the edge are referred to as the network core. Data generation is rising, necessitating more computation power by reducing sampling error enhancement [2]. The perspective of existing cryptography is being questioned as quantum computers become increasingly powerful. The blockchain is an example of advanced technology that relies heavily on cryptography's security [3]. Individuals and companies to protect their privacy and keep their communications and data confidential use cryptography daily. Cryptography maintains security by encrypting transmitted communications with an algorithm and a key known only to the receiver and the sender. Here, a cryptographic value of the previous block must be included in every new block in this new chain structure [4]. Cryptographic techniques are essential to creating digital signatures and link blocks in a blockchain [5]. Blockchain frameworks are a type of software that simplifies the process of to design, implementing, and supporting technically advanced products. The framework often simply provides the blockchain framework and its fundamental modules, and all individual components developed by the developer based on them. The sender generates a digital signature system by hashing the document to be signed. Then encrypt it with their private key to transmit it. Utilizing the sender's public key, the recipient decrypts the sent file and guarantees the predictable sender sends it.

Besides cryptographic techniques, HIoT's data sharing can benefit from blockchain technology. Here, Internet of Things (IoT) devices can securely exchange critical data for information processing [6]. This helps to explore the financial sector's drive for its exponential growth in quantum entanglement and the inferences with different sciences such as geometrical and database management systems [7]. Most existing public-key cryptographic systems are at risk due to the increasing power of quantum systems and the ability to exist quantum algorithms [8]. A more desirable solution would be a quantum blockchain built from quantum based on information fully incorporated into a quantum system. Quantum cryptography is a method that employs quantum mechanics to protect the distribution of symmetric encryption keys. It is more precisely known as quantum key distribution (QKD). It operates by transmitting photons, or "quantum particles" of light, through an optical network. In addition to the quantum key distribution (QKD) layer, quantum computing benefits over a conventional blockchain for information randomness [9]. Quantum key distribution (QKD) is a secure communication technology that allows for the transmission of encryption keys that are only known to the relevant parties. The communication technique employs quantum physics capabilities to communicate cryptographic keys in a verifiable and secure manner. There are numerous post-quantum data encryption strategies to choose from if one is prepared to sacrifice bandwidth and collection [10].

Based on quantum computing, the risk of a cyber-attack is increased when multiple technologies are combined on a single framework to help the treatment process. The eavesdropping may access the patient's private information, leading to misuse of the information [11]. There are protocols to ensure that nodes in the distributed network agree on the storage components, which are consistent across the network [12].

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025

Quantum computing has made blockchain cryptosystems less secure and exponential than their classical counterparts [13]. These innovations evoke high consumer expectations and perceptions of imminent changes to the current system in the case of technological innovations using the MIMO method [14]. For public and private keys that are assumed to be resistant to damage by quantum computers, post-quantum encryption technology incorporates a new generation of methodologies for the creation [15].

Research and business have become intertwined due to the enormous change and the associated rapid advancement of technology [16]. Two keys are used for data encryption and decryption in public-key cryptography [17]. To clarify, there are two major components in the crypto exchange implementation of modern cryptosystems [18]: a majority view protocol for creating new frames and a data encryption signature scheme for verifying transactions [19]. Because traditional cryptography relies on existing computer connections and equipment, the implementation costs are extremely low compared with other techniques [20]. However, classical techniques are still extremely useful, and a bridge between classical mechanics and computing is required to maintain continuity and facilitate transitions [21]. While individual users' privacy and information security are important, corporate entities, which stand to lose a lot more if their security is compromised, are more [22]. The above analyses of quantum computing theory have been incorporated into blockchain to safeguard the system from quantum attacks. The major contributions of this paper are given as,

- To design and develop secure cryptosystems that are highly resistant to quantum computer attacks hav e been proposed in this paper by PQ.
- For quantum-based communication systems, MIMO is designed to improve the efficiency of randomn ess and withstand sampling errors.
- For quantum key preparation, IQEAis designed based on keys for encryption with a generalized predi ction accumulation model stored in this instance.

The rest of the paper is organized as; Section 2 provides a comprehensive overview of blockchain and quantum concepts, as well as a detailed description of each. The approach and system architecture of the proposed system (EQ-BSM-AI) are in detail in Section 3. Section 4 illustrates the experimental analysis and conclusion in Section 5, respectively.

2. Related Work

The basic surveys of the blockchain technology before diving into quantum and classical cryptography schemes are analyzed based on vulnerability to quantum attacks given below.

Blockchain technology creates decentralized digital currency systems known as cryptosystems. Digital certificates related to public cryptography algorithms securer the transaction records in these systems [23]. Under quantum attacks, this paper assesses the security of current cryptosystems distributed ledgers (SCCDL). In addition, it examined some of the solutions that have been proposed to safeguard private blockchain in the quantum century.

Quantum computing (QC) is an alternative to conventional methods that use bits composed of 0's and 1's. However, the storage and computation problems must be addressed [24]. RSA algorithms can be broken by Shor's algorithm, which will be discussed in this paper on (QCA) quantum computer algorithms. In expediting computation, entanglement and a combination of quantum bits can be used effectively.

With the help of an Emergency Supporting Representative (ESR), the doctor has access to the patient's Attribute-based Key, which the ESR shares with a group of other ESRs.The suggested model secures information retrieval using lightweight cryptography (SIRLC)for the ciphertext and the time required to generate the secret key [25]. According to a performance evaluation, SIRLC is a better choice for healthcare IoT with increased security and reduced computational complexity than other methods. The computational complexity, or simply complexity, of an algorithm, is the number of resources required to operate it. The processing time and memory storage need special consideration.

Lattice-based cryptography is an exciting post-quantum cryptographic algorithm, both in its fundamental properties or implementation to existing and innovative security issues [26]. Lattice-based cryptographic

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025

schemes (L-CS) were discussed in this paper for their application in information security, as well as issues related to their implementation and new demands for their adoption. Based on computation mechanics, mapping strategies to existing equipment or synthesized parts or the entirety of a system on advanced hardware can be implemented using (L-CS).

In QKD systems were introduced, their security implications were discussed along with standardization activities for QKD networks [27]. Quantum random number generators (QRNGs) were introduced to solve security concerns posed by quantum computers. Breaking all current asymmetric algorithms for key exchange and cryptographic signature using large quantum computers.

Based on public-key encryptions (PKE) schemes, the learning with errors (LWE) challenge was difficult to solve in lattice-based cryptographic techniques. Large decryption sizes were required for LWE decryption to ensure correctness [28]. The authors developed this new PKE scheme for a small-ciphertext version of LWE. Results show that this method was 0.015 ms, extremely slow than others in decryption. A similar level of security can be achieved with our method of key generation and message encryption.

Based on the above-related works, our proposed system (EQ-BSM-AI) is compared with other traditional methods such as [23], [24], [25], [26], [27], and [28] referred to give an improved sampling errors reduction, improved efficiency of quantum entanglement, information randomness**,** the safety of private keys, quantum computing attacks resistance when compared with other existing approaches. To make secure transactions, the problem for overcoming storage and computational problems based on existing techniques is overcome in our proposed method EQ-BSM-AI.

3. quantum-assisted blockchain security model using artificial intelligence technique

In the current scenario, large-scale quantum computers can be built in which most current cryptographic systems can be hacked. Since digital and quantum computers can conduct computations at the same level, a quantum tool for blockchain framework design is required. The blockchain security model for cryptosystems used in the technology is not secure enough because of the rapid field of quantum computing. These issues are resolved and explained in the following sections based on a mathematical model.

Sectional analysis 1: To design and develop a secure cryptosystem that is highly resistant to quantum computer attacks has been proposed in this paper by (PQB).

Compared to today's systems, the quantum information system will have the tremendous processing power and strong artificial intelligence (AI) to enable the Internet of Things (IoT).

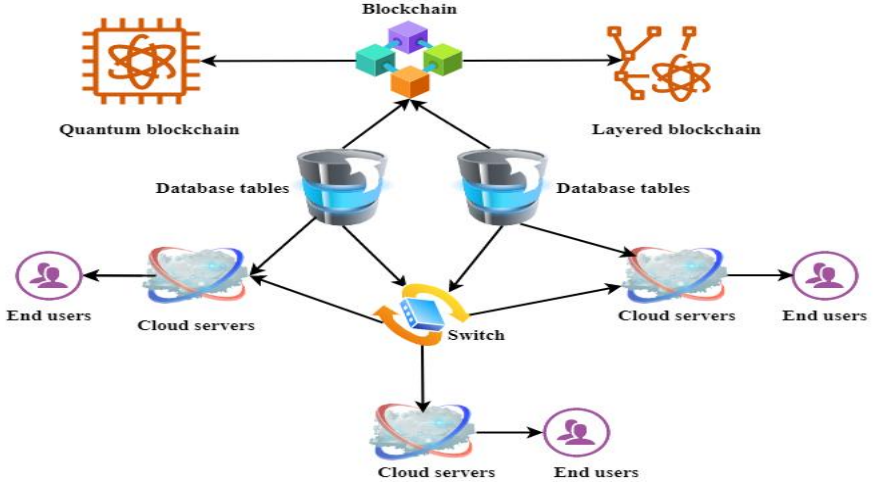


Figure 1: The evolution of the blockchain protocol and the architecture of the quantum computing

There is an interactive hardware or software system within the Internet of things network, as shown in figure 1. Internet protocols (IP) packets are traditionally not saved or stored in full because of a lack of storage and

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025

distribution capacity based on database tables. Blockchain technology with 256-bit hash encryption at each node can be implemented and even predicted for use in communication systems with improved service capacity due to the use of data storage and processing at each node by the users of a secure cryptosystem that is highly resistant to quantum computer attacks have been proposed here by PQB. Using network-managed quantum blockchain-based cloud servers with layered blockchain for service management software, a quantum cloud-computing center will transmit quantum bits data packets from one end-user to the next via a quantum IP network. The term "quantum blockchain" refers to a decentralized, encrypted, and distributed database that is based on quantum computing and quantum information theory. Once the information is stored in the quantum blockchain, it cannot be modified intentionally.

$$\begin{cases} |st = \prod_{en_i \in \{0,1\}, i \in \{0,1\}} cc_{en_i,..en_n} |en_i, \ldots . en_n \\ \left\{\prod_{en_i \in \{0,1\}, i \in \{0,1\}} |cc_{en_i,..en_n}|^2 = 1 \right. \end{cases} \quad (1)$$

One of the most fundamental units of information in quantum computing is an nb based quantum bits with $nb \in \{1,2,\ldots\}$. The state of quantum bits can be represented asst, which can be defined in the above equation (1). Here for all $en_i \in \{0,1\}, i \in \{0,1\}$, en is eigen nodes with coefficient complexity cc for reducing sampling errors with each quantum bit from $\{1,2,\ldots\}$ in the remaining 2^n states in total. Meanwhile, the computational basis is referred to as the model based on bit strings by the sum functions$\prod_{en_i \in \{0,1\}, i \in \{0,1\}} cc_{en_i,..en_n}$. Bit-strings are collections of binary digits (bits). The length of the value is defined as the number of bits in the sequence. A null string is a bit-string that has no length.

$$hg = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$hg|0 = \frac{(|0+|1)}{\sqrt{2}}, \quad (2)$$

$$hg|1 = \frac{(|0-|1)}{\sqrt{2}}$$

Complex numbers encode by a magnitude$\frac{1}{\sqrt{2}}$ moreover, a direction in the complex plane$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, in the above equation (2) and therefore, phase distance between any two-correlation coefficient$hg|0$ and $hg|1$ is a meaningful measurement by Hadamard gate hg for enhancement of correlation analysis. The Hadamard gate, often known as the H gate, is one of the most commonly used quantum gates. It may be utilized to transform a clustered qubit to a uniform superposed state. A Hadamard gate is not normally a physical device through which qubits are transmitted. The Hadamard gate is used with superconducting qubits and operates by bouncing microwaves off the qubits. There are key differences between quantum computer technology are given as$(|0+|1), (|0-|1)$ and classical probability and statistics by the value $\sqrt{2}$.

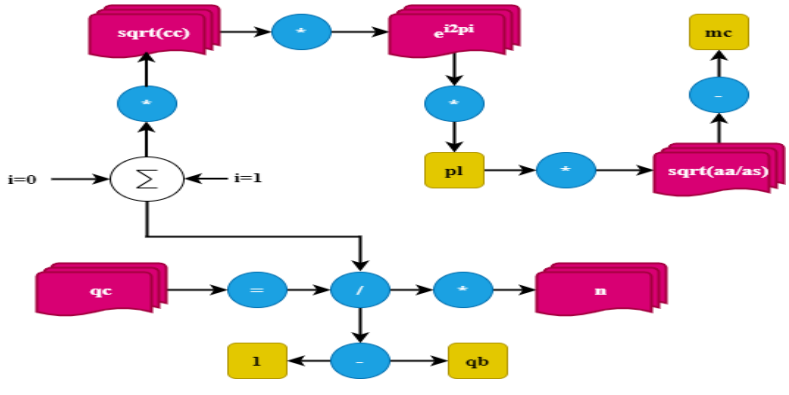


Figure 2: Representation of post-quantum-based blockchain

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025

$$qc = \frac{\sum_{i=0}^{1} \sqrt{cc} * e^{i2\pi\emptyset}.pl\sqrt{\left(\frac{aa}{as}\right) - mc}}{1-qb} * n \quad (3)$$

PQB is a secure cryptosystems scheme that can withstand quantum computer attacks when used with the suggested quantum computing qc based on blockchain given in figure 2. Cryptography enables safe communication in the presence of harmful third parties known as adversaries. Encryption employs an algorithm and a key to convert an input (i.e., plaintext) into an encrypted output (i.e., ciphertext). Each pair of nodes in the quantum blockchain is connected via a classical channel cc. In addition, quantum channels $\sqrt{cc} * e^{i2\pi\emptyset}.pl\sqrt{\left(\frac{aa}{as}\right) - mc}$ link these nodes together to form a quantum key distribution network with a summation of limits $i = 0\ to\ 1$. Many different PQB networks are available, and each one can be used with quantum bits qb from the above equation (3). There are n multipath components mc and the phase difference $\emptyset$ and path loss pl for the lth multipath, respectively. Moreover, the $l - th$ multipath's angle of arrival aa at receivers uniform linear array (ULA) by 2π is given as $\left(-\right)$ a and the n multipath's angle of separation as from senders as $\sqrt{\left(\frac{aa}{as}\right) - mc}$. A Uniform Linear Array (ULA) is a set of sensor units that are positioned uniformly along a straight line. The most popular form of the sensor is a dipole antenna, which can broadcast and receive Electromagnetic Waves over the air.

Sectional analysis 2: Multiple-Input Multiple-Output (MIMO) is a wireless technique that combines multiple transmitters and receivers to carry more data simultaneously. MIMO is supported by all 802.11n wireless equipment. It enables 802.11n to operate at rates that are faster than those of comparable technologies are. MIMO is designed to improve efficiency and withstand errors for quantum-based communication systems. Quantum communication is a branch of applied quantum physics that is strongly connected to quantum information processing and quantum teleportation. The use of quantum cryptography to secure information channels against eavesdropping is its most fascinating application.

By enhancing these quantum computing features, the innovative quantum-based Moore's law targets the achievement of an ever increases in the number of qubit-based quantum computers by nb bits. Moore's Law applies to conventional CPUs but does not apply to quantum processors. Entanglement is an odd property of qubits. Users effectively increase the amount of information that the quantum system can compute by adding one more qubit to a system. Moore's Law has had a direct influence on the advancement of computer power. This especially indicates that transistor speeds in integrated circuits have enhanced. Transistors are devices that transmit electricity and include carbon and silicon molecules that allow electricity to move much faster through a circuit. Researchers can expect quantum IP to change the original internet protocol and MIMO network when communicating.

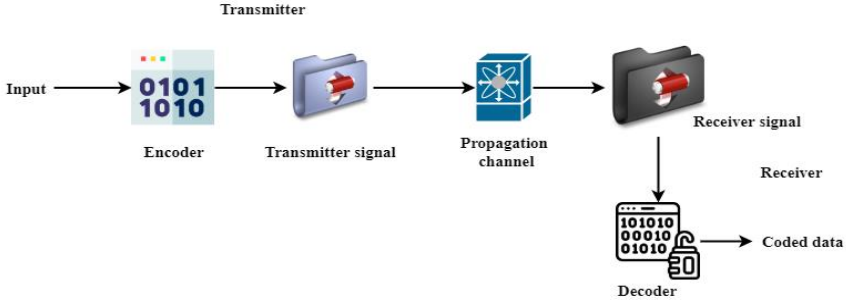


Figure 3: Utilization of MIMO in quantum-based blockchain

Numerous physical-layer options for inputs and outputs have been proposed in response to an exponential rise in demand for high speed, including MIMO systems, and the utilization of the terahertz (THz) multiple frequencies is achieved in figure 3, where the input data is processed in the encoder for encoding the input data. Then, the encoded data is processed in the transmitter signal for further processing. Further, the data

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025

is processed in the propagation channel. Propagation channel modelling is a critical component of communication system design and simulation. The performance of the system can be enhanced by modifying transfer parameters like components attached and assigned power when channel status information is accessible. Finally, the received signal is decoded to get the output data. Despite this, massive systems have an inherent increment in computation time necessary for decoding. As a result, combining lower-layer encryption with traditional upper-layer encryption can improve security. Without the key, eavesdroppers are unable to decode the signal. According to recent reports, the MIMO framework appears to be well suited to these types of encryption methods. Ensure that the receiver completes the decoding process in a reasonable amount of time. Using the encoder for encoded data illustrated above, a quantum computer encodes the signals encoded by the encoder.

$$bp(x,y) = hg * \begin{cases} x & (y=0) \\ x+0.5 & (y=1, x>0.5) \\ x+1 & (y=1, x>1) \end{cases} \quad (4)$$

Using blockchain propagation bp, each element is allotted to a transmit antenna and sent to the receiving antennas to be used for encoding and decoding here a(x,y) by the equation mentioned above (4). It is assumed that the receiver has access to the channel conditions at all times for information randomness; therefore, the receiver can decode the signal by quantum bits selections given as x and $(y=0)$, $x+0.5$ and $(y=1, x>0.5)$, and$x+1$ $(y=1, x>1)$. Encryption key duration Encryption is performed using a single actual bit and a secret key.

$$qb_{(x,y)} = \begin{cases} \left|sin\left(\frac{piv}{2}\right)\right| qb_x(1,es) * en_i, \ldots . en_n, piv \geq 0 \\ \left|sin\left(\frac{piv}{2}\right)\right| qb_y(1,rr) * en_i, \ldots . en_n, piv < 0 \end{cases} \quad (5)$$

The location of the encrypted signal$qb_x(1,es)$ that is sent by the previous iteration's value piv, and the parameter describe the replica's reliability$qb_y(1,rr)$ in such a manner, challenges, as it increases, are given in equation (5). The quantum bits $qb_{(x,y)}$ between the analysis of trigonometric function$\left|sin\left(\frac{piv}{2}\right)\right|$and the notation node is defined based on piv either ≥ or <0 using Eigen values $en_i, \ldots . en_n$,.

$$isf = \sqrt{rwf^2 + cnf^2} * \sqrt{\left(\frac{aa}{as}\right) - mc} \quad (6)$$

Images' spatial frequencies are f measures the amount of activity in the image's space. This equation (6) illustrates the spatial frequency description of an image with rows and columns$\sqrt{rwf^2 + cnf^2}$.In this example, rwf stands for the image's row frequency and cnf stands for the image's column frequency$\sqrt{\left(\frac{aa}{as}\right) - mc}$ from equation (1). Our solution to this problem is to reconstruct the encoding propagation channel for a blockchain-based quantum system to decode data transmitted across massive MIMO systems.

Reconstructing the encoding propagation channel for blockchain-based quantum systems to allow decoding of data transmitted across massive MIMO systems is our solution to this problem to enhance the efficiency of quantum entanglement. Analyzing numerically demonstrates that the suggested method can be used to decode quantum data by improving the efficiency of a MIMO system.

Sectional analysis 3: For quantum key preparation, IQEA is designed based on keys for encryption with a generalized prediction accumulation model stored in this instance.

Quantum key images are used to create an image encryption algorithm that is much simpler than previous approaches. Algorithms generate the encryption keys and prepare them for the IQEA process. The plain image performs the XOR operations on this quantum key image bit by bit. A new quantum image encryption technique is designed based on a quantum key image. As depicted in figure 4, the algorithm consists of three steps (i) key generation, (ii) preparation, and (iii) XOR operation.

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025

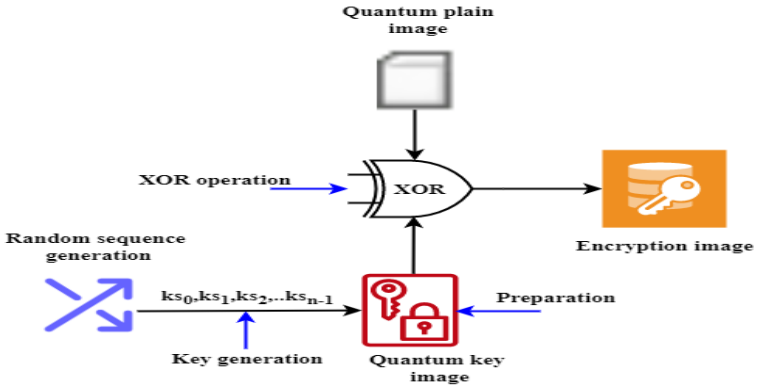


Figure 4: Steps involved in the IQEA process

Step 1: The keystream can be generated by any device that can generate a random sequence with key sequence ks, where the keystream is denoted as $ks = [0, 1]$. Assume that the key length ks_{n-1}.

Step 2: In contrast, the key image is in two dimensions, and the keystream ks is in one dimension. As depicted in figure 4, the transformation is completed. Keystream ks is serially used to determine the grey value of each pixel safety of private keys. As a result, each block of the keystream contains two blocks $b1$ and $b2$, where each block contains k bits.

$$is_0 = |k^{\otimes b1+b2+k}|$$
$$qo = ig^{\otimes k} \otimes hg^{b1+b2}$$
$$qo(is_0) = (is|0)^{\otimes b1} \otimes hg^{b1+b2}||in \quad (7)$$
$$qo = \left(is \otimes \sum_{b1,b2\neq 0} b1_{is} b2_{is}\right) + cqo \otimes |b1 \otimes b2|$$

is andhg are used to build a $b1 + b2$ box using the single-quantum bit gates for $b1$ and $b2$ respectively. From the initial stateis_0 to the intermediate state in, it performs the transformation that can be given using quantum operation qo in the above equation (7). In the keystream, the grey values for blocks$|b1 \otimes b2|$ with one pixel per block. In this step, the keystream for each pixel is divided into suboperations cqo.

Step 3:

$$\langle b1\rangle \otimes \langle b2\rangle = \frac{1}{\sqrt{2}^{b1+b2}} \sum_{i=0}^{b1-1} \sum_{j=0}^{b2-1} \otimes i = 0^{k-1}|\, b1b2 \otimes \frac{1}{\sqrt{2}^{b1+b2}} \sum_{i=0}^{b1-1} \sum_{j=0}^{b2-1} \otimes i = 0^{k-1}|b2b1 \quad (8)$$

The image for key quantum qo the quantum key image is represented by the symbol for XOR can be given in the below figure. The encrypted quantum image eqi can be decrypted by combining it with plain image is_0. The XOR procedure is denoted in the above equation (8).

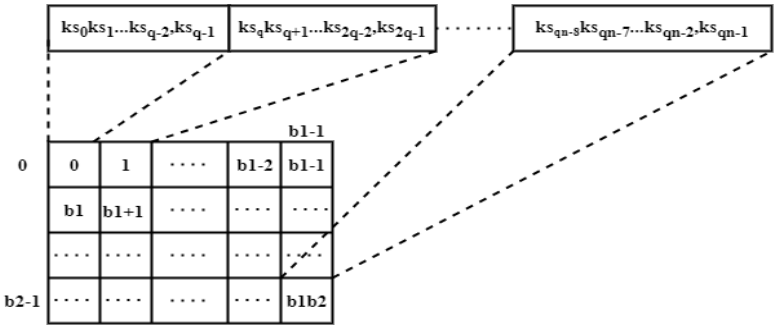


Figure 5 (a): Process of generating quantum key

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025

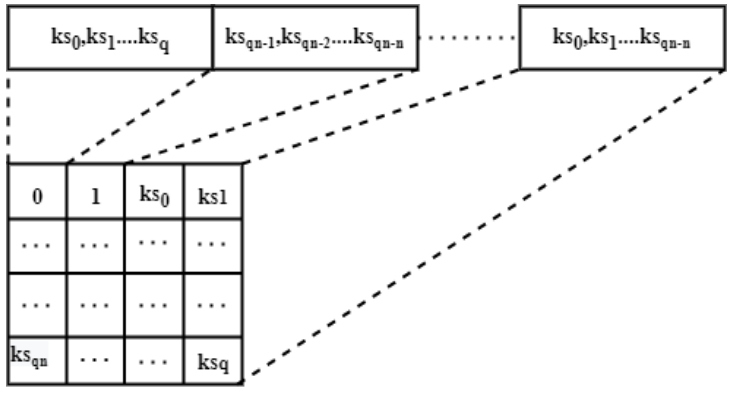


Figure 5 (b): Process of generating plain quantum key

In the IQEA process, algorithms generate and prepare the encryption keys. XOR operations are performed bit by bit on the quantum key image by the plain picture by summation process having limits$i = 0\ to\ b1 - 1$ and$j = 0\ to\ b2$. Based on the quantum key image, a new quantum image encryption method has been devised in above Figures5 (a) and 5(b). The image key dimensions are 2 x 2, and each pixel ranges from 0 to 3. Consequently, four quantum bits are required: one is used to store $b1$, one is used to store $b2$, and the final two are used to find $b1$, and b2 from the grey value. The key image uses the same number of qubits as the plain image in Figure 6.

$$sd(x) = rc(x) \otimes bc$$

$$bc_{0,1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} + \sum_{b1,b2\neq 0} b1_0 b2_1 * \sum_{b1,b2\neq 0} b1_1 b2_0 \qquad (9)$$

Service delivery sd to end-users(x) is based on the resource consumption rc by various HIoT applications, which can all benefit from the emergence of edge computing by matrix $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$. It is possible to use the blockchain bc as a public or private database while still maintaining transaction records' confidentiality and integrity by using Boolean values $bc_{0,1}$. This is done by allowing each node by summation $\sum_{b1,b2\neq 0} b1_1 b2_0$to hold a local backup of the data using the XOR function for each block $b1_1 b2_0$and relying on a decentralised network$b1_0 b2_1$ for contract on the current condition of the blockchain from the above equation 9.

$$qs >= \frac{1}{\sqrt{Mm}} \sum (is|0)^{\otimes b1} \otimes hg^{b1+b2} || in \qquad (10)$$

Knowledge of a quantum state computing qs for various blockchains with Markov matrix Mm that can be an initial state is from every allocation over several quantum bits which is greater than or equal $qs >= \frac{1}{\sqrt{Mm}}$with the very same to the homogenous distributionhg^{b1+b2} of those bits is required for verification from the above equation (10) by quantum computing attacks resistance. The final uniform dispersion$\frac{1}{\sqrt{Mm}}$ contains no bits for authenticating transactions on the blockchain and requires the use of public-key/asymmetric cryptographic algorithms$(is|0)$, which are provided by the blockchain by XOR operations.

$$\left(is \otimes \frac{1}{\sqrt{hd}} \sum_{i=1}^{n} < qs\right) \cup \left(is \otimes \frac{1}{\sqrt{hd}} \sum_{i=1}^{n} > qs\right) \qquad (11)$$

From the above equation (11), the homogeneous distribution hd of quantum bits $\frac{1}{\sqrt{hd}}$is required to verify various blockchains that can be initial states of quantum state computing qs. Union of public-key/asymmetric cryptographic algorithms based on$\sum_{i=1}^{n} < qs$, $\sum_{i=1}^{n} > qs$ must be used to authenticate transaction is on the blockchain because the final uniform dispersion contains no bits.

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025

$$qs_i = \frac{1}{\sqrt{hf}} \sum_{\triangle} \sum_{ks_0..ks_n} \frac{1}{2^{b1+b2}} * |\triangle_1 \dots \triangle_k| \quad (12)$$

Quantum state qsi employs hash functions$\frac{1}{\sqrt{hf}}$ that can withstand converging collisions key generation in each stage$ks_0..ks_n$ for an unorganized collection of degree-2 polynomials$\frac{1}{2^{b1+b2}}$ is used to define these hash functions illustrated in the above equation (12). Authenticating transactions on the blockchain requires the use of public-key/asymmetric cryptographic algorithms$\sum_{\triangle} \sum_{ks_0..ks_n} \frac{1}{2^{b1+b2}}$Which is provided by the blockchain.$\triangle$is defined in a way that allows us to perform a calculation that maps to$|\triangle_1 \dots \triangle_k|$ in quantum computing.

$$qs(bb) = \frac{(00b1)+(11b2)}{\sqrt{2}} * \frac{(01b1)-(10b2)}{\sqrt{2}} \quad (13)$$

A blockchain-based quantum system $qs(bb)$ that can decode data transmitted across massive MIMO networks is our solution to this problem mentioned above (13). This is automatically verified and split by the system before being sent to the receiver address using Boolean values$(00b1) + (11b2)$, $(01b1) - (10b2)$along with the quantum state, and the signature is then compiled with the remaining transaction details in the quantum network.

It is found that our proposed method EQ-BSM-AI resulted in improved sampling error reduction, increased efficiency of quantum entanglement, optimised fault-tolerance of private keys, and increased resistance to quantum computing attacks when compared to other existing methods. These enhancements enhance the safety and efficiency of the cryptographic network.

4. Results and discussion

The EQ-BSM-AI suggested method is run on a Raspberry Pi v2 with a low-power pocket PC (ARMv6 700 MHz, 512 MB). Running at 100%, the Raspberry Pi consumes approximately 3.8 W of electricity, minimizing the risk of additional power consumption. The problem's computational complexity is used as the foundation for the security of blockchain cryptography. Cryptography is a technique for protecting data from unauthorized intrusion. Transactions between two nodes in a blockchain network are secured using cryptography in the blockchain. Cryptography and hashing are the two key ideas of a blockchain. Quantum computing for blockchain security relies heavily on public-key cryptography for data encryption and identity verification are compared and analyzed with other existing approaches. On the other hand, traditional cryptographic algorithms face a serious threat from quantum computing, which has powerful parallel computational resources. The parameters used to implement our proposed method are given in table 1 using datasets.

Table 1: Parameters used to implement our proposed method

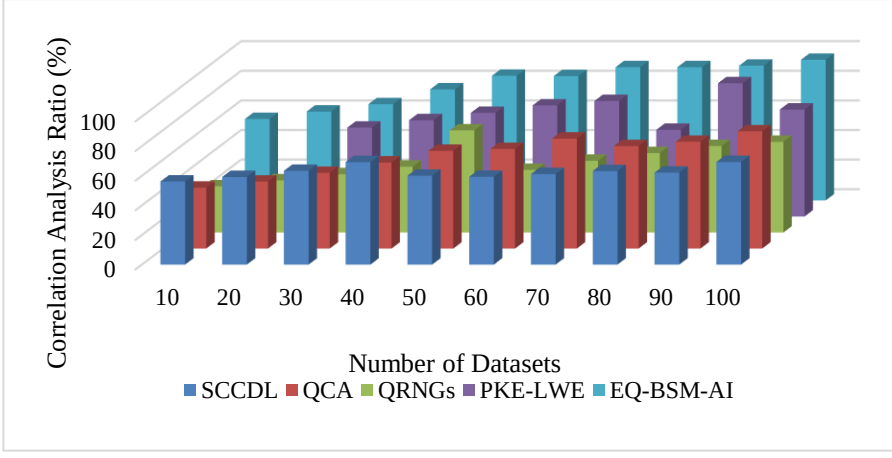
Parameters	Specifications
Threshold	37 GHz
cell's configuration	48 GHz
pattern of work	Rayleigh
Frequency of the carrier	38 GHz
Throughput	10.5 Gbps
Processing time	m/s

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025

4.1 Correlation analysis of EQ-BSM-AI

$$cr = \frac{(en(gv - en(gv))(en(gv1 - en(gv1))}{\sqrt{D(gv)D(gv1)}} \quad (14)$$

Visually comparing the correlation coefficient of neighboring pixels before and after cryptography, as well as horizontally, vertically, and diagonally, is a powerful measurement index to examine using the above equation (14). gv and $gv1$ are the grey values of adjacent pixels in an image; $(gv)D(gv1)$ are the assumption and variance, respectively, for correlation analysis cr. For the most part, correlations between adjacent pixels in a plain image are close, and it is compared and given in below figures 6(a) and 6(b) varying $(gv)D(gv1)$ values. A 45-degree slash is the focal point of the majority of points. A 90-degree angle is generated when two rays are exactly divided in half by 45 degrees. It is an acute angle, and two 45-degree angles make a straight angle or a 90-degree angle. An angle is generated when two rays intersect at a vertex. However, an efficient quantum bits encryption scheme should ensure that the relation between two adjacent pixels in the encryption algorithm tends to zero. As a result, the points are evenly distributed across the rectangular area in cryptosystems. Using the correlation coefficients of corresponding pixel pairs in the directions of the image, the encryption algorithm's spatial correlation phases can be compared and given in our proposed method EQ-BSM-AI.



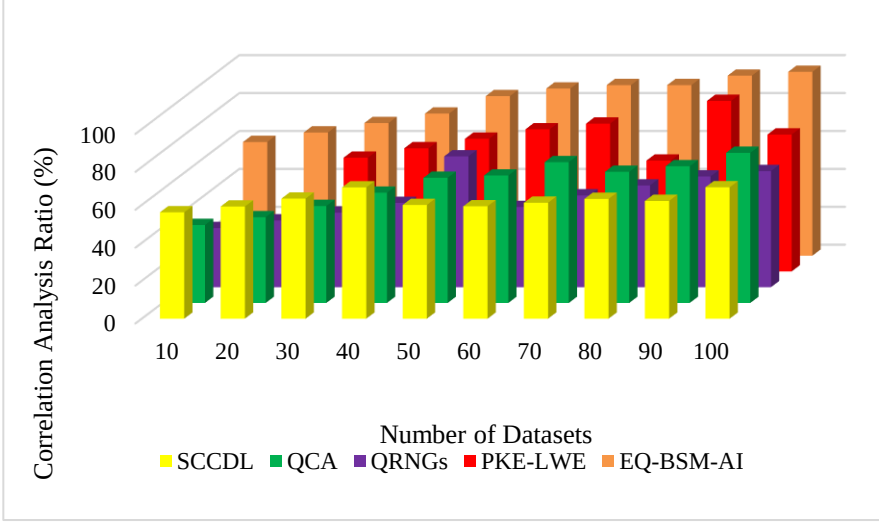


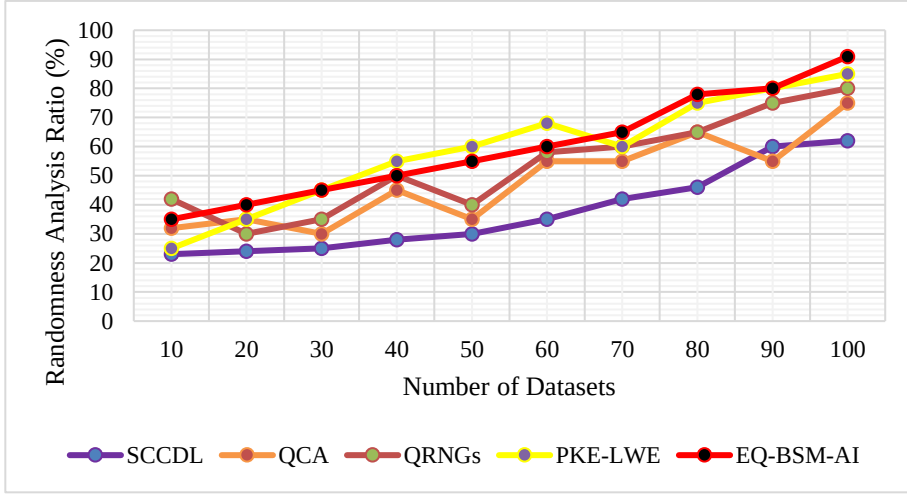
Figure 6 (a) and 6 (b):Correlation analysis comparison

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025

4.2 Information randomness analysis in EQ-BSM-AI

$$isf = \sqrt{rwf^2 + cnf^2} * \sqrt{\left(\frac{aa}{as}\right) - mc} \quad (15)$$

The more uniform the image's greyscale distribution is the higher the image's information randomness, which can be used to express the image's level of uncertainty. Figure 7(a) and 7(b) below information randomness definition is shown below. The plain and encrypted images have the same information randomness value. It's very close to the ideal value for the plain that has been encrypted. Therefore, the encryption algorithm that can resist attacks on its security is analyzed using equation (15). Images' spatial frequencies are f measures the amount of activity in the image's space. This equation (6) illustrates the spatial frequency description of an image with rows and columns$\sqrt{rwf^2 + cnf^2}$.In this example, rwf stands for the image's row frequency and cnf stands for the image's column frequency $\sqrt{\left(\frac{aa}{as}\right) - mc}$ from equation (1). Our solution to this problem is to reconstruct the encoding propagation channel for a blockchain-based quantum system to decode data transmitted across massive MIMO systems.



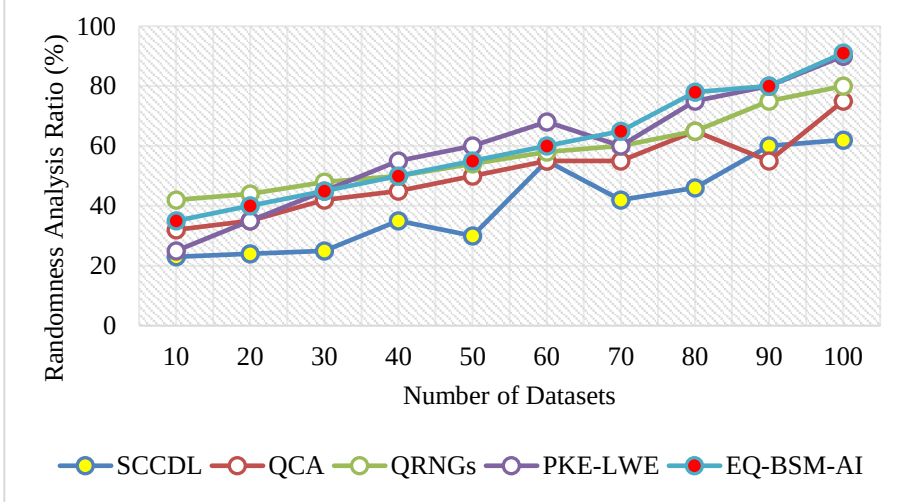


Figure 7(a) and 7(b): Correlation analysis comparison

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025

4.3 Sampling errors reduction in EQ-BSM-AI

Table 2: Comparison of sampling errors

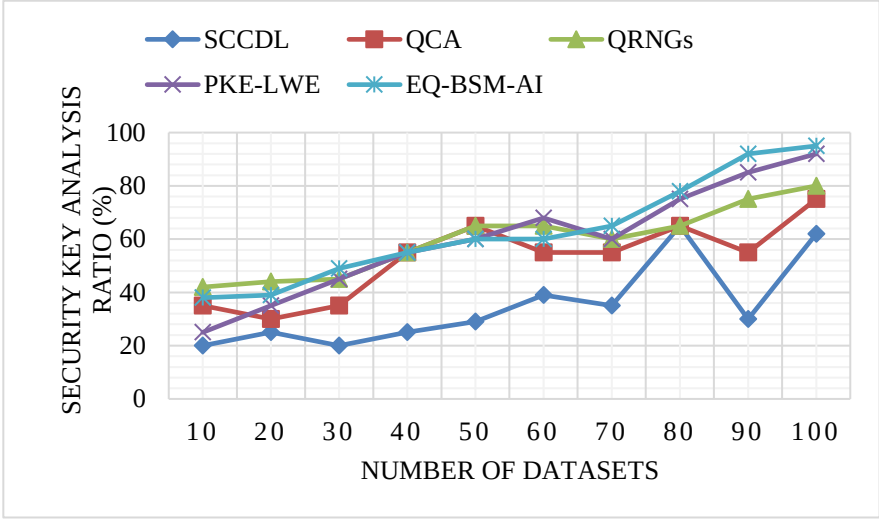
Number of Datasets	SCCDL	QCA	SIRLC	L-CS	QRNGs	PKE-LWE	EQ-BSM-AI
10	81.3	80.7	78.9	69.1	50.4	48.6	30.7
20	79.6	77.9	71.0	67.4	55.6	43.7	30.1
30	80.2	76.7	74.3	63.7	57.8	41.0	32.6
40	74.4	74.3	79.5	59.9	59.0	39.1	29.2
50	76.6	72.2	70.9	55.1	41.3	30.3	24.4
60	77.9	69.5	69.1	53.5	48.6	30.6	25.8
70	68.9	66.1	67.3	58.7	43.9	32.8	21.0
80	64.0	63.0	63.5	52.0	45.2	29.0	19.3
90	62.2	59.3	59.0	50.4	48.5	24.8	15.5
100	60.3	58.2	55.3	50.1	46.7	35.4	12.4

From the above table 2, st can represent the state of quantum bits, as shown in equation (1) above. To reduce sampling errors in the remaining 2^n states in total, en is used as eigen nodes with coefficient complexity cc for all $en_i \in \{0,1\}, i \in \{0,1\}$. As a result, existing lattice-based cryptography is widely regarded as having the advantage of resisting attacks from quantum computers, which is enhanced in our proposed system shown in the table. Testing methods for the algorithm's resilience for all the secret keys in modern cryptographic techniques will take almost infinite time. Using a sampling technique IQEA, a smaller proportion of the total number of key configurations en is evaluated, and then system performance for all keys is determined with a defined sampling error n, which helps avoid this issue.

4.4 Private key security in a quantum blockchain

The entire block's memory will be occupied because of the cryptographic techniques signature's public key length. At this point, the primary solution to a quantum-resistant software blockchain network is to change the methodology and shorten the private key. Our proposed system EQ-BSM-AI enhances these problems compared with other methods given in Figures 8(a) and 8(b). From equation (8), any device that can generate a random sequence with the key sequence ks, denoted as$ks = [0, 1]$, can generate the keystream. Assume ks_{n-1}. is the length of the key $(n - 1)$. The image's location in PQB and colour are typically scrambled using a variety of transformations in this type of security key process. In terms of encryption, quantum encrypted images are based on the cipher, which uses the text to encrypt the image. The quantum encrypted images use text to encrypt the images during encryption.

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025



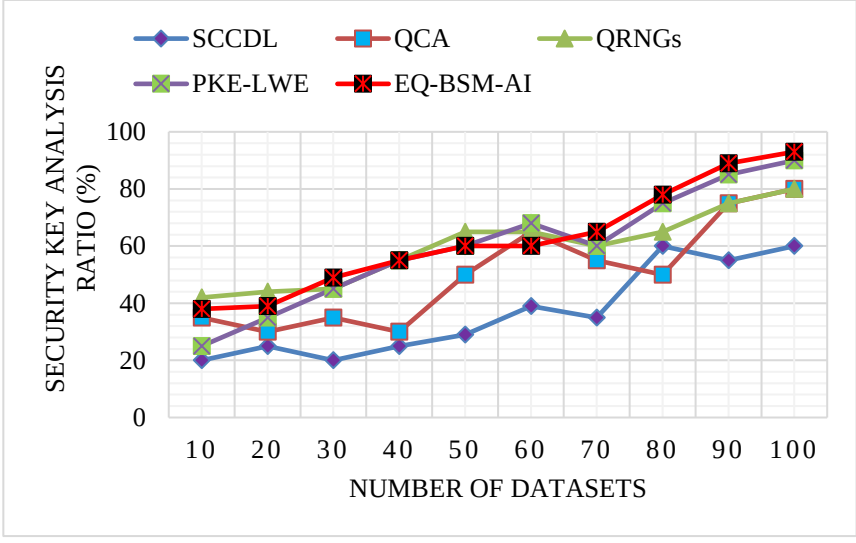
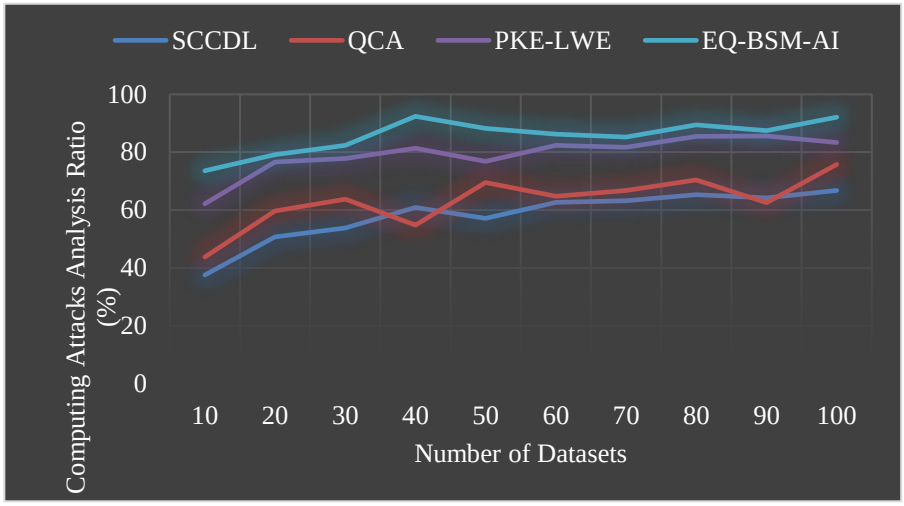


Figure 8 (a) and 8 (b): Security key analysis comparison

4.5 Comparison of quantum computing attacks analysis

The capabilities of quantum bits to concurrently exist in different states are called quantum states. Consider how much computing power could be increased if multiple versions of the $1s\ and\ 0s$ existed simultaneously in the same quantum bits from equation (3). The quantum bit's power is enhanced in quantum computing in blockchain in our system EQ-BSM-AI. The binary series of $0s\ and\ 1s$ is the fundamental language of traditional computers are compared and given in figures 9(a) and 9(b). Here, the $l-th$ multipath's angle of arrival aa at receivers uniform linear array (ULA) by$2\pi$is given as$\left(\frac{aa}{as}\right)$ and the n multipath's angle of separation as from senders as $\sqrt{\left(\frac{aa}{as}\right)-mc}$. Quantum computing will get more powerful and accessible in our proposed system by using PQB. Absolutely guarantee, however, a quantum-resistant cryptographic infrastructure will help ensure the integrity and privacy of our organization's data.

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025



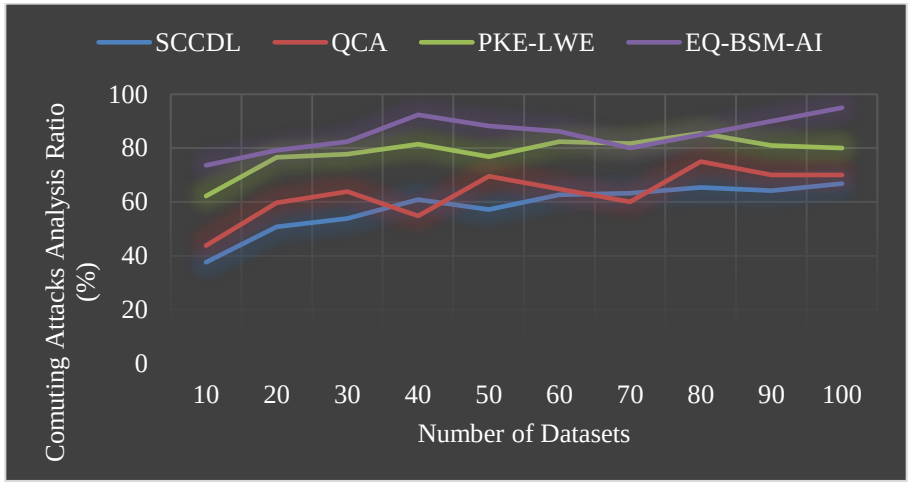


Figure 9 (a) and 9(b): Computing attacks comparison

4.6 Quantum entanglement comparison

Quantum computers use physical phenomena to speed up computations by employing quantum states and other quantum effects. Our solution to this problem is to reconstruct the encoding propagation channel for a blockchain-based quantum system in time to enable the decoding of data transmitted across massive MIMO systems, and comparisons are given in table 3. A numerical analysis shows that the proposed method can decode quantum data and increase the MIMO system's efficiency using this method. The amount of activity in an image's space is measured by its spatial frequencies. An image's spatial frequency $is\ f$ description illustrated in this equation (6) by rows and columns $\sqrt{rwf^2 + cnf^2}$. The number of pairs of bars displayed within a specific distance on the location is referred to as "spatial frequency." Because an image the size is considered to delimit one degree of visual angle on the point, one-third of a millimeter is a useful metric of point distance. When a paired quantum bits state is altered, the entangled quantum bits are altered instantly in quantum systems. This means that entanglement speeds up the computations of quantum computers. According to research, a quantum algorithm's exponential performance boost over classical computations necessitates quantum entanglement.

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025

Table 3: Comparison of quantum entanglement

Number of Datasets	**SCCDL**	**QCA**	**QRNGs**	**PKE-LWE**	**EQ-BSM-AI**
10	53.7	63.7	75.7	85.4	91.7
20	54.8	65.8	76.8	85.5	92.8
30	55.7	67.7	77.7	86.7	92.7
40	56.7	68.7	78.7	87.9	93.7
50	57.9	69.9	79.9	88.3	93.9
60	58.8	70.8	80.8	88.1	94.8
70	60.6	71.6	81.6	89.3	94.6
80	61.8	72.8	82.8	90.9	95.8
90	62.5	73.0	83.9	90.5	95.1
100	63.0	74.6	84.9	90.5	96.3

From the above tables and graphs, it is proved that our proposed system EQ-BSM-AI enhances the drawbacks of existing research with an efficiency of improved sampling error reduction of 12.4%, increased efficiency of quantum entanglement of 96.3%, information randomness of 93.9%, correlation analysis of 93.2%, and increased resistance to quantum computing attacks of 90.8% when compared to other existing methods.

5. Conclusion

This paper proposes an enhanced quantum-assisted blockchain security model using artificial intelligence (EQ-BSM-AI). The bit stream generated by the traditional blockchain method creates the quantum key image. All required for the encryption and decryption process are XOR operations on the quantum plain image and the key image. Encryption and decryption quantum circuits are shown. It demonstrates that the proposed novel EQ-BSM-AI method is efficient and secure compared to others. EQ-BSM-AI enhances the drawbacks of existing research with an efficiency of improved sampling error reduction of 12.4%, increased efficiency of quantum entanglement of 96.3%, information randomness of 93.9%, correlation analysis of 93.2%, and increased resistance to quantum computing attacks of 90.8% when compared to other existing methods. It is proposed in this paper that a secure cryptosystem be designed and developed, which has a high level of resistance to quantum computer attacks through PQB. It is designed to increase efficiency and withstand errors in quantum-based communication systems by MIMO. The encryption keys for the generalized prediction accumulation model are stored in quantum key preparation by IQEA. In our opinion, the proposed method performance can be improved by properly considering the quantum bit effect when quantum computing in edge-based blockchain concept as a future scope.

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025

Acknowledgements

Not applicable.

Author's Contributions

The individual contributions of authors to the manuscript should be specified in this section.

Funding

This research was supported by the Dijlah University College l [grant number G2021-1].

Competing Interests

The authors declare that they have no competing interests.

References

[1] K. Kan and M. Une, "Recent trends on research and development of quantum computers and standardization of post-quantum cryptography," *Monetary and Economic Studies*, vol. 39, pp. 77–108, Jun. 2021.

[2] D. A. Dawar, "Enhancing wireless security and privacy: A 2-way identity authentication method for 5G networks," *Int. J. Math. Stat. Comput. Sci.*, vol. 2, pp. 183–198, 2024, doi: 10.59543/ijmscs.v2i.9073.

[3] N. Kappert, E. Karger, and M. Kureljusic, "Quantum computing—the impending end for the blockchain?" in *Proc. Pacific Asia Conf. Inf. Syst. (PACIS)*, Dubai, UAE, Jun. 2021.

[4] Y. L. Gao, X. B. Chen, G. Xu, K. G. Yuan, W. Liu, and Y. X. Yang, "A novel quantum blockchain scheme based on quantum entanglement and DPoS," *Quantum Inf. Process.*, vol. 19, no. 12, pp. 1–5, Dec. 2020.

[5] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 9, pp. 21091–21116, Jan. 2020.

[6] A. Farouk, A. Alahmadi, S. Ghose, and A. Mashatan, "Blockchain platform for industrial healthcare: Vision and future opportunities," *Comput. Commun.*, vol. 154, pp. 223–235, Mar. 2020.

[7] N. R. Mosteanu and A. Faccia, "Fintech frontiers in quantum computing, fractals, and blockchain distributed ledger: Paradigm shifts and open innovation," *J. Open Innov.: Technol., Market, Complexity*, vol. 7, no. 1, p. 19, Jan. 2021.

[8] X. Sun, M. Sopek, Q. Wang, and P. Kulicki, "Towards quantum-secured permissioned blockchain: Signature, consensus, and logic," *Entropy*, vol. 21, no. 9, p. 887, Sep. 2019.

[9] D. Rajan and M. Visser, "Quantum blockchain using entanglement in time," *Quantum Rep.*, vol. 1, no. 1, pp. 3–11, Apr. 2019.

[10] D. I. Ilie, K. Karantias, and W. J. Knottenbelt, "Bitcoin crypto–bounties for quantum capable adversaries," in *Mathematical Research for Blockchain Economy*, Springer, Cham, 2020, pp. 9–25.

[11] M. Bhavin, S. Tanwar, N. Sharma, S. Tyagi, and N. Kumar, "Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications," *J. Inf. Secur. Appl.*, vol. 56, p. 102673, Feb. 2021.

[12] J. Chen, W. Gan, M. Hu, and C. M. Chen, "On the construction of a post-quantum blockchain for a smart city," *J. Inf. Secur. Appl.*, vol. 58, p. 102780, May 2021.

[13] N. Dey, M. Ghosh, and A. Chakrabarti, "Quantum solutions to possible challenges of blockchain technology," *arXiv preprint*, arXiv: 2110.05321, Oct. 2021.

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025

[14] J. Kietzmann and C. Archer-Brown, "From hype to reality: Blockchain grows up," *Bus. Horizons*, Jan. 2019.

[15] M. Allende et al., "Quantum-resistance in blockchain networks," *arXiv preprint*, arXiv: 2106.06640, Jun. 2021.

[16] P. Sandner and P. M. Schulden, "Speciality grand challenges: Blockchain," *Front. Blockchain*, vol. 2, p. 1, Mar. 2019.

[17] W. Barker, W. Polk, and M. Souppaya, "Getting ready for post-quantum cryptography: Explore challenges associated with adoption and use of post-quantum cryptographic algorithms," *NIST Cyber Secur. White Paper (DRAFT)*, vol. 26, May 2020.

[18] A. H. Lone and R. Naaz, "Demystifying cryptography behind blockchains and a vision for post-quantum blockchains," in *Proc. IEEE Int. Conf. Innov. Technol. (INOCON)*, Bangalore, India, Nov. 2020, pp. 1–6.

[19] J. Chen, W. Gan, M. Hu, and C. M. Chen, "On the construction of a post-quantum blockchain for a smart city," *J. Inf. Secur. Appl.*, vol. 58, p. 102780, May 2021.

[20] M. Anderson, "Quantum cryptography needs a reboot: A failed security product could someday power large-scale quantum computing," *IEEE Spectr.*, vol. 56, no. 10, pp. 9–10, Sep. 2019.

[21] P. Nimbe, B. A. Weyori, and P. K. Yeng, "A framework for quantum-classical cryptographic translation," *Int. J. Theor. Phys.*, vol. 60, no. 3, pp. 793–818, Mar. 2021.

[22] N. Storublevtcev, "Cryptography in the blockchain," in *Proc. Int. Conf. Comput. Sci. Appl.*, Springer, Cham, Jul. 2019, pp. 495–508.

DOI: https://doi.org/10.54216/FPA.180210
Received: August 07, 2024 Revised: November 08, 2024 Accepted: January 19, 2025