International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 13, No.1 (Jan-2023)

http://dx.doi.org/10.12785/ijcds/130122

Fog Enabled Cyber Physical System Authentication and Data Security using Lattice and Quantum AES Cryptography

Roopa Golchha[1], **Jaykumar Lachure**[2] **and Rajesh Doriya**[3]

[1,2,3]*Department of IT, National Institute of Technology, Raipur, Chhattisgarh, India*

Received 13 May. 2022, Revised 12 Dec. 2022, Accepted 12 Jan. 2023, Published 31 Jan. 2023

Abstract: With the widespread use of the internet, there is a need to secure the communication channel through Cyber-Physical Systems as they carry essential information, for which we rely upon various cryptographic algorithms. With the advancement of Quantum Computers, security-related public-key encryption methods would become ineffective. Furthermore, the critical research areas for ensuring security against quantum attacks are Quantum Cryptography and Post Quantum techniques, such as Lattice-Based Cryptography, Code-Based Techniques, Hash-based and Multivariate-based techniques. One of the best techniques is Lattice-based cryptography, which provides security against Quantum attacks through its unique, light weighted, and complex security properties that can be used effectively to secure the Fog-cloud network. This paper deals with key generation and digital signature algorithms based on Ring Learning with Error using Lattice-based schemes. The proposed Lattice-based Quantum Advanced Encryption Standard method provides less time for encryption, decryption, and validation of signatures along with distinct keys. The maximum encryption and decryption time for the message is 34.1 μ*second* and 0.0280 *second*, respectively. The quantum bit required for the encryption and decryption of text is between 10 to 21.

Keywords: Fog enabled Cyber-Physical System, Lattice-Based Cryptography, Post Quantum Cryptography, Public key Cryptography, Quantum Advanced Encryption Standard, Ring Learning With Errors scheme

1. INTRODUCTION

Cryptography is a technique that ensures the security of data and systems. Early examples of this method for encoding communications can be found in the Roman era, where Caesar Ciphers were used. Recently, cryptographic algorithms have been used for data privacy and security in complex network-enabled systems for dedicated work, including the Internet of Things (IoT), Robots, and Cyber-Physical Systems (CPS). Fog-enabled Cyber-Physical Systems (Fog-CPS) promote local computing by integrating computational, and communication capabilities with the physical environment [1]. These systems have several security and trust issues. Additionally, the CPS devices and fog nodes are subject to multiple threats because the Fog-CPS systems may be placed in open and unprotected areas. Hence, the National Institute of Standards and Technology (NIST) standardized various cryptographic techniques based on their performance, which are being used today for securing the data flowing through the classical computing machines [2].

The breakthrough came in 1994 when Peter Shor [3] pointed out that a Quantum Computer (QC) can effectively attack cryptographic schemes whose security is based on the hardness of theoretical assumptions. Shor's algorithm states that using a QC, factoring integer problems and discrete logarithmic problems can be processed in polynomial time. QC works on a computational model, which uses quantum mechanics, *i.e.*, the physical properties of matter. It uses the superpositioning state of quantum bits, *i.e.,* Qubits, and can efficiently solve the problems upon which the existing cryptographic techniques rely.

Thus the current Public-key Cryptography (PKC) is threatened by the development of QC; therefore, many research works are springing up in the area of Quantum Cryptography and Post Quantum Cryptography (PQC) [4]. Among the various cryptographic schemes proposed for security against QC, the Lattice-Based Cryptography (LBC) scheme is the most promising candidate. LBC hides information in high-dimensional geometric structures called lattices and uses them to create keys and digital signatures that are believed to be impossible to crack till date, even by QCs. LBC offers a secure approach for algorithm design that is assumed to be complex mathematical problems [5]. As the devices in Fog-CPS systems demand low-latency services from adjacent fog nodes, thus, LBC can provide better security mechanisms to secure them. The main contribution of this paper is to provide the following:

E-mail address: roopajain@live.com, jaykumarlachure@gmail.com, rajeshdoriya.it@nitrr.ac.in

- A framework to support the cybersecurity vulnerability in Fog-CPS system.
- The Quantum-Advanced Encryption Standard (QAES) model is being proposed to generate the key for authentication.
- The encryption, decryption, and verification of various sample messages for validating the proposed QAES methodology.
- The qubits are calculated for different data lengths to check the security of the communication channel.

In the rest of the paper, section 2 explains the background of current cryptographic techniques and related drawbacks of the classical cryptography methods *w.r.t.* to quantum computing. The following section deals with the need for PQC and the basics of Quantum computing. Section 4 discusses the brief about Lattices and LBC. The Fog-enabled Cloud computing architecture is explained in section 5. Section 6 presents the proposed QAES methodology for security and authentication purposes. Section 7 provides the result analysis and comparative study of the proposed QAES model with various other techniques, and the conclusion and future work are discussed in the final section.

2. CURRENT CRYPTOGRAPHIC SCHEMES

Cryptography is required when communication is across any insecure channel, including most networks, especially the internet. The key objectives of cryptography are privacy, integrity, non-repudiation, authentication, and key exchange. Nowadays, various cryptographic algorithms are designed using the logic related to integer factorization and discrete logarithmic problems for security [6][7]. The current cryptography techniques can be broadly classified into Symmetric Key and Asymmetric Key algorithms. These schemes are based on mathematical problems which were assumed to be very difficult and could only be solved with high computational logic.

A. Symmetric Key Cryptography

In this scheme, the sender and receiver use the same key that they share in advance to encrypt and decrypt the message. As computers have become more sophisticated, symmetric-key cryptography has evolved with more complicated encryption mechanisms and significant key sizes. The most widely used symmetric-key algorithm are Data Encryption Standard (DES), Triple DES, and Advanced Encryption Standard(AES). Usually, AES-256, with the 256-bit key size, is a secure algorithm for communication [8].

B. Asymmetric Key Encryption

This scheme uses private and public keys where the public key is shared, whereas the private key is kept secret. The methodology is that the sender will encrypt the plaintext using the public key, and at the receiver, decryption is done using his private key. The various asymmetric algorithms are Rivest–Shamir–Adleman (RSA), ElGamal, and Elliptic Curve Cryptography (ECC) which are used for key exchange, encryption, and digital signatures [9] [10].

3. REQUIREMENT FOR POST QUANTUM ENCRYPTION

PQC is the scheme that provides security against attacks from QC. They aim to substitute for cryptographic primitives while offering compatibility with the existing systems. Though the RSA algorithm is secure with traditional computers, it may be broken using QCs. Shor's algorithm uses Quantum Fourier Transform to solve the prime factorization problem by converting it to a period-finding problem. Using Shor's Algorithm, one could work out the prime factors of a large number in $O(log(n))$, where n is the size of the integer [11]. Even though such a speedup does not make classical cryptographic technologies obsolete, they have an effect by acquiring larger key sizes, even in symmetric-key techniques. Table 1 summarizes the impact of large-scale QC on conventional cryptographic algorithms using Shor's Algorithm. The record for the most significant integer factored using Shor's Algorithm is 35 qubits [12][13].

The research article [14] provides a detection method for fog computing environment security. The physical layer key generation is modeled using wireless channel parameters to create the secret keys that connect the trustworthy and protect users from impersonators. The research [15] demonstrates a proof-of-principle for simulating the natural laws using a communication architecture model and its implementation. From a theoretical, methodological, and practical standpoint, the model is based on the BB84 Quantum Key Distribution (QKD) protocol with two scenarios, without and with the existence of an eavesdropper via the interception-resend attack model. It also discusses a Double Sarsa strategy to recognize the pretenders at the receiving end. The study [16] provides a comprehensive encryption and decryption procedure for end-users and fog servers based on multi-authority, attribute revocation, and outsourcing computation. Additionally, it uses the fog server to handle the challenging encryption and decryption duties.

The work of [17] examines interconnected device-to-device communication characteristics crucial for accepting and implementing their security and privacy. To achieve the ideal test threshold in the impersonation attack, [18] suggests the Q-learning algorithm. The proposed scheme's effectiveness confirms and ensures its ability to identify impersonation attacks in fog computing networks precisely. Using the quantum-safe PQC algorithms [19], this study developed an authenticated encryption scheme for use with the conventional channel. In the study [20], a clever assault defense strategy was suggested. Based on prospect theory, they build a static zero-sum game model between clever attackers and trustworthy users. The Double Q-Learning (DQL) approach is proposed dynamically to limit intelligent attackers' attack motivation.

TABLE I. Impact of large-scale quantum computers on conventional cryptographic algorithms.

Algorithm	Algorithm Type	Impact of quantum computers
AES	Private key	Large key size needed
RSA	Public key	Not Secure
ECDSA, ECDH	Public key	Not Secure
DSA	Public key	Not Secure

As a result, to address the issue regarding information security in quantum computing, a large international community emerged with the expectation that the public key infrastructure might stay integral by employing innovative quantum-resistant primitives *i.e.* the PQC. Each PQC family uses a mathematical problem that is assumed to be difficult to solve even if the attacker has access to a QC. Thus, the cryptographic community examines which of the proposed ways is the most efficient and provides the most protection.

A. *Quantum Computing and Cryptography*

Quantum computing uses the quantum phenomena like superposition, interference, and entanglement for performing computation and is a subfield of quantum information science. Its foundations are based upon quantum mechanics principles which is a fundamental concept that describes the physical properties of the nature of atoms or subatomic particles. With the discovery of elementary particles, it was found that they could carry information and perform computations [21]. Unlike current cryptography, which counts on the computational complexity of mathematical problems, quantum computing has become more diverse and functional in numerous scientific fields even though their ability is restricted, particularly on the number of qubits [22].

B. *Qubits*

A Quantum Bit (Qubit) is the quantum equivalent of a classical bit. The classical bit encodes or transmits the information either with a value of zero or one, and in contrast, qubits have a state in zero, one, or any linear combination of both states. The two basis qubit states are usually written as $|0\rangle$, $|1\rangle$, and together they form an orthonormal basis for the vector space. A statevector describes a system's state and helps keep track of quantum systems [14] [23]. For example :

$$|q\rangle = \begin{bmatrix} 0 \\ . \\ . \\ 1 \\ . \\ . \\ 0 \end{bmatrix} \leftarrow \textit{Probability of an object being at position k}$$

and the general state of a Qubit $|q\rangle$, can be given as:

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

Here α,β are scalars (such that $\alpha,\beta \; \epsilon \; C$, where C is a scalar field set) and are used for representing the basis of the qubit state. Any qubit state can be plotted on the surface of a sphere called the Bloch sphere and is represented in figure 1 [11][24].

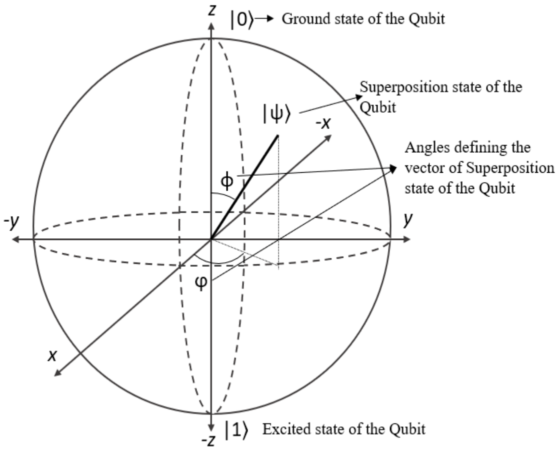

z
|0⟩ → Ground state of the Qubit
Superposition state of the Qubit
|ψ⟩
-x
Angles defining the vector of Superposition state of the Qubit
ϕ
-y
y
φ
x
-z
|1⟩ Excited state of the Qubit

Figure 1. Bloch Sphere representation of a Qubit [25].

C. *Quantum Superposition*

The principle of Quantum Superposition implies that a quantum particle can exist simultaneously in two separate locations. According to this theory, a quantum particle can be in more than one state simultaneously unless it is measured *i.e.,* a qubit does not exist in just one state but in a superposition of different states. A Qubit is in superposition of states $|0\rangle$, $|1\rangle$ corresponding to $\theta = \frac{\pi}{2}$ and $\varphi = 0$ along the x-axis. With a QC of n qubits, there can be $2n$ superposition states where each state is equivalent to a single list of classical n bits of 1's and 0's and can operate on $2n$ states simultaneously.

D. *Quantum Entanglement*

The quantum mechanical property of particles or atoms that are spatially separated can be described with reference to each other, leading to the correlations between observable physical properties of the system. When two particles get entangled, their quantum states become strongly connected and unified, and measurements of one of the particles automatically influence the other, no matter how far apart the particles are. Cryptography is one of the most common applications of quantum entanglement. In this context, a sender and a receiver create an encrypted communication link using entangled particle pairs. The sender and receiver use the entangled particles to create private keys that are only known to them and can be used to encrypt their messages. If someone intercepts the signal and attempts to read the private keys, the entanglement is broken since measuring an entangled particle affects its state. As a result, both the sender and the recipient will be aware that their communications have been intercepted [17][26].

E. Single Qubit Gates

The operations that change the state of a qubit are called gates. Qubits are limited to the form:

$$|q\rangle = \cos\frac{\theta}{2}|0\rangle + \varepsilon^{i\theta}\sin\frac{\theta}{2}|1\rangle \tag{2}$$

A significant characteristic of a quantum circuit is that the gates (operations) are always reversible between initializing the qubits and measuring them. These reversible gates can be visualized as rotations around the Bloch sphere and as unitary matrices (square matrices). Some of the basic quantum gates are Pauli's (X, Y, and Z) gate, Hadamard gate, Phase gate, T-gate, *etc.*

F. Hadamard Gate (H-gate)

It is the most widely used basic quantum gate. When a qubit passes through H-gate, it moves away from the poles of the Bloch sphere and creates a superposition of state $|0\rangle$ and $|1\rangle$. Figure 2 describes the statevector representation of a qubit using H-gate, and figure 3 is the quantum circuit representation of H-gate using IBM Quantum Circuit Composer [27]. By default, qubits are initially in the zero states, and when an H-Gate is applied to a qubit, there is a 50% chance that the qubit will be zero when measured and a 50% chance that it will be one [28].

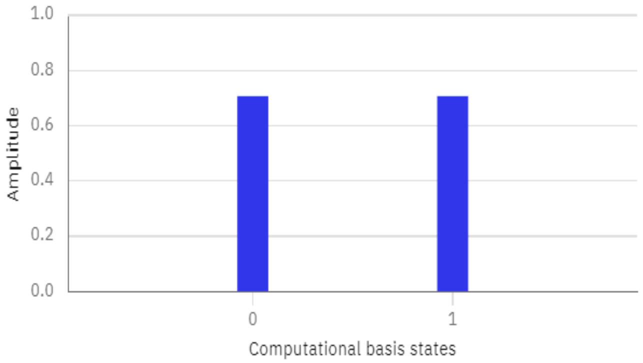


Figure 2. State Vector representation of Hadamard gate. [27].

One-Qubit Hadamard Gate can be represented as a unitary matrix:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \tag{3}$$

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{4}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{5}$$

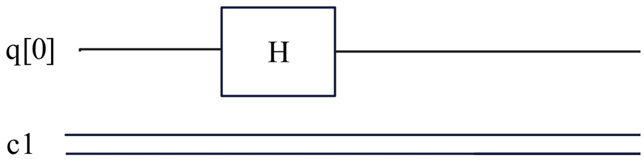


Figure 3. Quantum Circuit representation of Hadamard gate [27].

The above equations show the superposition of qubit on applying an H-Gate. While using two H-gates (one after the other), the qubit state can be kept the same.

4. Lattice-Based Cryptography (LBC)

LBC refers to asymmetric cryptographic primitives that are based on lattices and the proposed method mainly focuses on LBC. Some preliminaries are discussed below as [22]:

A. Lattice

A Lattice, *L* is a geometric structure representing objects, formed from a set of *n* independent vectors $b_1, b_2, b_3, ..., b_n \ \epsilon\ R^n$, that are uniformly or evenly spaced in an *n −1* dimension periodic grid of points, and mathematically represented as $L = \Sigma_{i=1}^{n} x_i b_i$ where $x_i\ \varepsilon\ z$.

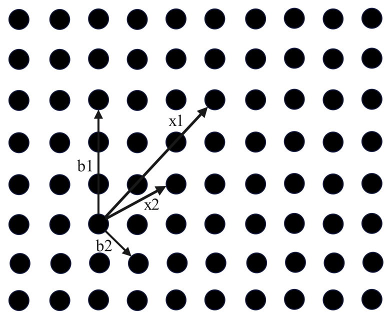


Figure 4. Lattice representation using basis $[b_1, b_2]$ *and* $[x_1, x_2]$ [12].

The lattice produced by basis vector $[x_1, x_2]$ and $[b_1, b_2]$ is represented in figure 4. The vectors $[b_1, b_2]$ are orthogonal and are referred to as a good basis, whereas the basis $[x_1, x_2]$ is referred to as a bad basis. The choice of basis is independent and invariant and is mainly the geometrical parameters of the lattice.

Due to their simple structure, rich and strong primitives, and ability to perform linear and parallel operations, it offers a unique security property and it has been used in combination with cryptography [13] [16]. The first work on LBC algorithms was in 1997 by Ajtai and Dwork, when Ajtai introduced the Short Integer Solution (SIS) problem on lattices [10]. Ajtai's remarkable finding was that lattices, which were previously only used in cryptanalysis, could also be used to create cryptographic primitives. This discovery attracted a lot of attention to the complexity of lattice problems and also their connection with cryptography.

Another reason was that the security of the cryptographic primitive was dependent on the worst-case hardness of lattice problems. Additionally, employing lattice has the advantage that their computations are frequently merely a matter of modular addition and are thus relatively straightforward. When encryption has to be carried out using a low-cost device, lattices are helpful in various real-world situations [23]. This concept inspired Hoffstein, Pipher, and Silverman to create the open-source public key cryptosystem, which was designed at NTRU. They developed a novel method for LBC that uses polynomial rings. They put out two distinct approaches, one for digital signatures and the other for encryption. As a result, it differs significantly from pure Ajtai-Dwork and may withstand attacks from Shor's algorithm. For instance, the key sizes were significantly smaller with proper parameter initialization and resisted cryptanalytic efforts. Thus, the following are the various reasons why the lattice is employed in cryptography:

- Simple and efficient due to the linear and parallelizable structure.
- Its ability to resist sub-exponential and quantum attacks.
- Faster encryption and decryption techniques are possible with lattice issues.

B. *Learning with Errors (LWE)*

LWE was first introduced by O Regev, which closely relates to the SIS problem defined by Ajtai. The main concept used was to make the lattice problem more secure by adding some noise called errors. The errors introduced are from random hash functions, generally random oracle, so the solution could not be recovered using Gaussian elimination as that can be done in polynomial time. In the LWE problem, the perturbation of error is not in a fixed quantity but rather a variable under distribution (e.g., normally Gaussian distribution) [12]. In LWE, we initially create a secret key value s and another value e. Next we select a number of values A and calculate B as:

$$B = A * s + e. \tag{6}$$

The values of A and B become the public key. This LWE problem is considered suitable for PKC applications as they are assumed to be very hard regarding the current best-performing algorithms that run in exponential time in n and have no known polynomial QC algorithm to date.

C. *Ring-Learning With Errors (Ring-LWE)*

Ring-LWE was an adaptation of the original LWE problem, with the key difference between them being the use of a polynomial ring for a finite field of variables for lattice, A and secret key, s, that is we divide the whole polynomial with the highest factor of x plus one thus creating a ring structure which has values always in the region of x. The main idea behind this approach is to reduce the working dimension of the lattice. Similar to LWE, Ring-LWE is also believed to be NP-Hard. The biggest advantage of Ring-LWE in PKC systems is the reduction in key size, as Ring-LWE key sizes can be reduced to the square root of LWE key sizes [18] [29].

5. FOG-ENABLED CYBER PHYSICAL SYSTEM (Fog-CPS)

Fog-CPS support local computing by combining processing and communication capabilities with the physical world. It is an extension of cloud computing and improves the management of next-generation CPS. Fog computing creates a large distributed network, enhancing the IoT cloud services by attaining efficiency in correlated factors like latency, power, traffic, *etc.* [30]. A Fog-CPS generally comprises three layers organized in order of increasing computational and storage capacities: CPS devices, Fog layer, and Cloud layer [31].

A. *Security characteristics of Fog Network*

Securing the fog network is essential since it connects to edge devices and network infrastructures such as wireless sensor networks, RFID-based sensor networks, cloud computing, and the IoT. The most admirable security goal is to safeguard the data gathered. Thus this system must be adaptable to data-related threats and provide security, and privacy [32]. The different security objectives are:

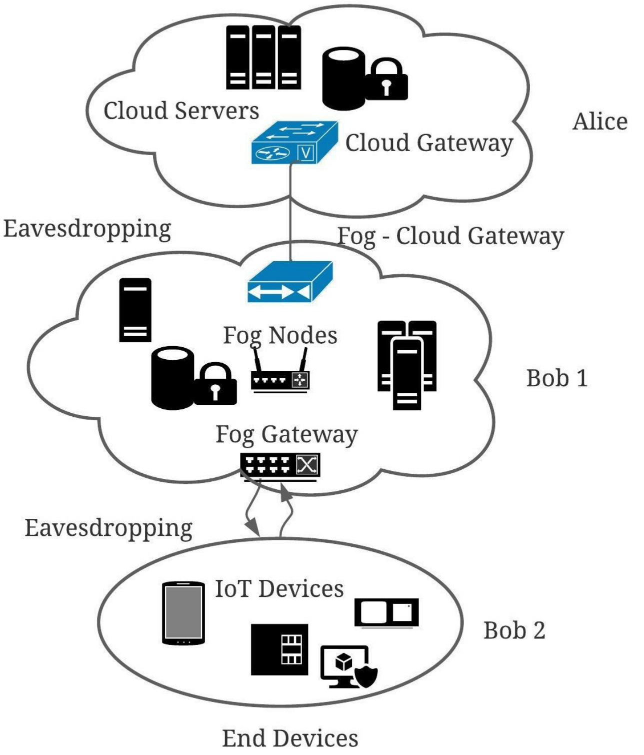


Figure 5. Securing Fog enabled Cyber-Physical System Architecture.

- Secure Communication: This motivates confidentiality, integrity, and availability for secure communication within the communication channel.

- Access Control for Fog: To provide appropriate data and services by authorizing and authenticating the control access.
- Trustworthiness of Fog: To offer reliable platform modules for upholding security and privacy to enable new degrees of trust.
- Data Sharing in Fog: For administering the nodes through Information Flow Control (IFC).

Fog-CPS systems are prone to a variety of security, privacy, and trust issues, which can cause communication between Fog-CPS entities to be disrupted. Figure 5 shows the basic Fog-enabled CPS architecture with the cloud servers as Alice and the fog and edge nodes as Bob. There can be numerous attacks between the fog-cloud nodes and fog-end nodes, the most common is eavesdropping. As the Fog-CPS offers real-time and faster data communication and the existing solutions have several drawbacks thus, to secure the Fog-CPS, lightweight cryptographic approaches could be used [30].

6. METHODOLOGY

The proposed QAES method for securing the Fog-CPS describes the key generation, encryption, and decryption algorithm discussed in this section. The steps for the decryption of the given cipher text with the generated secret key using round keys, for decoding and shifting rows, for the proposed QAES scheme are depicted in Algorithm 1. Algorithm 2 shows the steps for encryption using the given message, generated public key, and a random key using 16 rounds for the proposed QAES method. Algorithm 3 helps to generate the public and private keys with the help of four qubits. The proposed QAES algorithm encrypts the provided message in blocks. It uses 16 rounds of permutations and substitutes the key to return both the private and public keys for connection establishment. Firstly, the message is converted to its ASCII representation and then to its hexadecimal equivalent. Further, the basic operations of the AES method using the quantum approach with four quantum bits are performed on the message. The same steps are performed to decrypt the message. For a key generation, the substitution and rotation of the random keys using a 16-bit integer are performed. The key generation algorithm for our proposed model works as same as the key generation for the classical AES technique.

Algorithm 1 Algorithm for Decryption

```
Require: Secret key $sk \in B^{16 \cdot k \cdot n/16}$
Require: Ciphertext $c \in B^{d_u \cdot k \cdot n/16 + d_v \cdot n/16}$
Ensure: Message $m \in B^{32}$
  $u := Decrypt_q(RoundKey_{d_u}(c), d_u)$
  $v := SubstituteInv_q(Decode_{d_v}(u), d_v)$
  $s := ShiftRowsInv(sk)$
  $m := MixColInv(Compress_q(s, 1))$
  $return\ m$
```

Algorithm 2 Algorithm for Encryption

```
Require: Public key $pk \in B^{16 \cdot k \cdot n/16}$
Require: Message $m \in B^{32}$, Random key $r \in B^{32}$
Ensure: Ciphertext $c \in B^{d_u \cdot k \cdot n/16 + d_v \cdot n/16}$
  $Matrix = []$
  for i from 0 to 3 do
    $arr = []$
    $arr1 = block[i]$, $arr2 = key[i]$
    for j from 0 to 3 do
      $tmp = arr1[j] \diamond arr2[j]$
    end for
    $convert = hex(tmp)$
    if len(convert)==3 then
      $convert = convert + c0$
    end if
    $c1 = convert[3]$, $c2 = convert[2]$
    $convert = convert[0:2]$
    $convert = convert + c1 + c2$
    $arr.append(convert)$
  end for
  $c = Matrix.append(arr)$
  $return\ c$
```

Algorithm 3 Algorithm for Key Generation

```
Ensure: Secret key $sk \in B^{16 \cdot k \cdot n/16}$, Public key $pk \in B^{16 \cdot k \cdot n/16}$
  $key\_gen = []$, $rotword = substitution(key)$
  for i from 0 to 3 do
    $arr = key[i]$
    $arr1 = []$
    if i>0 then
      $rotword = key\_gen[len(key\_gen) - 1]$
    end if
    for j from 0 to 3 do
      if i==0 then
        $temp = arr[j] \wedge rotword[j] \wedge r\_Con[index][j]$
      else
        if i≠ 0 then
          $temp = arr[j] \wedge rotword[j]$
        end if
      end if
      $convert = hex(temp)$
      if len(convert)==3 then
        $convert = convert + c0$
      end if
      $c1 = convert[3]$, $c2 = convert[2]$
      $convert = convert[0:2]$
      $convert = convert + c1 + c2$
      $arr1.append(convert)$
      $key\_gen.append(arr1)$
    end for
  end for
  $return\ key\_gen$
```

TABLE II. Encrypted Text, Encryption Time, Decryption Time, and Qubits required for different messages.

Message	Encrypted Text	Encryption Time (μsec)	Validating Text using Quantum	Decryption Time (sec)	Quantum Bit
cps security	[[’0x63’,’0x70’,’0x73’,’0x20’], [’0x73’,’0x65’,’0x63’,’0x75’], [’0x72’,’0x69’,’0x74’,’0x79’], [’0x72’,’0x69’,’0x74’,’0x79’], [’0x00’,’0x00’,’0x00’,’0x00’]]	32.7	[[’0xa8’,’0x97’,’0xdb’,’0x63’], [’0x48’,’0x18’,’0xf1’,’0xbe’], [’0x36’,’0xf0’,’0xda’,’0xea’] [’0xb6’,’0x52’,’0x91’,’0x9f’]]	0.012441	11
alice communication	[[’0x61’,’0x6c’,’0x69’,’0x63’], [’0x65’,’0x20’,’0x63’,’0x6f’], [’0x6d’,’0x6d’, ’0x75’, ’0x6e’], [’0x69’, ’0x63’, ’0x61’, ’0x74’], [’0x69’, ’0x6f’, ’0x6e’, ’0x00’], [’0x00’, ’0x00’, ’0x00’, ’0x00’], [’0x00’, ’0x00’, ’0x00’, ’0x00’], [’0x00’, ’0x00’, ’0x00’, ’0x00’]]	34.1	[[’0x02’,’0x83’,’0x82’,’0x5d’], [’0xb9’,’0x00’,’0xe9’,’0x2d’], [’0x49’,’0xc7’,0x6b’, ’0x12’] [’0x6a’, ’0x0a’, ’0xe5’, ’0xd0’]]	0.012342	18
information technology	[[’0x69’, ’0x6e’, ’0x66’, ’0x6f’], [’0x72’, ’0x6d’, ’0x61’, ’0x74’], [’0x69’, ’0x6f’, ’0x6e’, ’0x20’], [’0x74’, ’0x65’, ’0x63’, ’0x68’], [’0x6e’, ’0x6f’, ’0x6c’, ’0x6f’], [’0x67’, ’0x79’, ’0x00’, ’0x00’], [’0x00’, ’0x00’, ’0x00’, ’0x00’], [’0x00’, ’0x00’, ’0x00’, ’0x00]]	29.6	[[’0xbe’, ’0x55’, ’0x87’, ’0x5d’], [’0xb9’, ’0xdf’, ’0x1b’, ’0x06’], [’0x82’, ’0x50’, ’0x07’, ’0x3d’], [’0x1b’, ’0xcb’, ’0x5d’, ’0xc4’]]	0.012536	21
Quantum Computer	[[’0x51’, ’0x75’, ’0x61’, ’0x6e’], [’0x74’, ’0x75’, ’0x6d’, ’0x20’], [’0x43’, ’0x6f’, ’0x6d’, ’0x70’], [’0x75’, ’0x74’, ’0x65’, ’0x72’]]	31.0	[[’0xab’, ’0xf1’, ’0xfc’, ’0x17’], [’0x28’, ’0x2b’, ’0x22’, ’0x7a’], [’0xf5’, ’0x54’, ’0x95’, ’0x68’], [’0x95’, ’0x9d’, ’0x2c’, ’0xfb’]]	0.01058	15
NIT Raipur	[[’0x4e’, ’0x49’, ’0x54’, ’0x20’], [’0x52’, ’0x61’, ’0x69’, ’0x70’], [’0x75’, ’0x72’, ’0x00’, ’0x00’], [’0x00’, ’0x00’, ’0x00’, ’0x00’]]	32.3	[[’0x83’, ’0x68’, ’0x49’, ’0x62’], [’0xd9’, ’0x60’, ’0x96’, ’0x8f’], [’0xd4’, ’0x53’, ’0xda’, ’0x8a’], [’0x0f’, ’0xad’, ’0x5c’, ’0x1f’]]	0.0280342	10

7. Result

We have implemented the proposed approach using AES and quantum methodology with RLWE for key generation, encryption, and decryption.

Table 2 shows the analysis of time and qubits required for different messages given as input to our QAES model. It shows that the message, when encrypted using the QAES, is different from the cipher text generated after the validation, thereby maintaining the security and confidentiality of the message at both ends. For this, the maximum encryption time is 34.1 $\mu second$ for the text ‘alice communication’ and the decryption time is 0.0280 *second i.e.* for the message ‘NIT Raipur’. The quantum bit required for the encryption and decryption of various text ranges between 10 to 21.

Table 3 shows the comparative analysis of the proposed QAES model for Fog-enabled CPS using Lattice and Quantum AES cryptography with other state-of-the-art approaches in terms of the methodology used, the time required for encryption and decryption, and the qubits (attributes) required. From this, we can incur that our proposed QAES model outperforms the limitations of other models.

Figure 6 shows the circuit representation of the Quantum Circuit of the proposed Quantum AES method.

Figure 7 shows the graphical representation of the result of the proposed QAES *w.r.t* encryption and decryption time required for the sample messages.

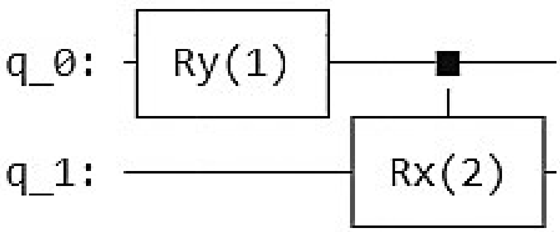


Figure 6. Quantum Circuit representation of the proposed Quantum AES method.

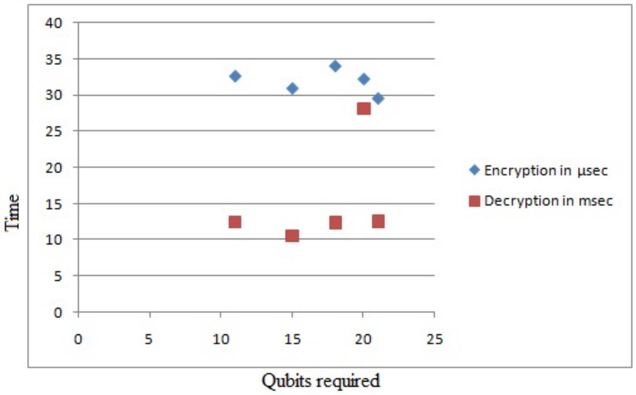


Figure 7. Analysis of Encryption and Decryption time w.r.t. Qubits.

TABLE III. Comparison of the proposed QAES model with other approaches.

Model	Method	Limitations	Encryption time (in *second*)	Decryption Time (in *second*)	Qubits required
A revocable multi-authority ABE scheme[16]	Attribute-based Encryption	Outsourcing of encryption and Decryption requires more communication delays and the energy consumption	0.6	0.1	20
AE in the QKD using PQC[19]	Authenticated-Encryption scheme	More runtime of the model	3.12	2.38	100
ABE with Privacy Protection [33]	Attribute-based Encryption	Issues related to privacy protection and accountability of ABE scheme	2.5	0.049	30
Proposed Fog enabled CPS using LBC	Quantum AES	———	0.0296	0.0125	21

8. Conclusions and Future Work

In numerous disciplines, combining quantum and lattices has proven to be more effective, among other schemes. Securing them is challenging as the Fog-CPS carries crucial data through unprotected channels. To ensure these systems, we propose a light weighted scheme using Lattice-based Quantum cryptography. The proposed QAES methodology integrates the quantum approach with the classical AES technique. The proposed QAES approach requires a maximum encryption time of 34.1 $\mu second$, a decryption time of 0.0280 *second*, and the quantum bit needed for encryption and decryption of given sample messages ranges between 10 to 21. QAES also improves security because the encrypted message changes at both ends *i.e.,* at encryption and validation, which is beneficial to security. Building a quantum circuit, however, is seriously affected by decoherence in the quantum systems due to its interactions with the environment. Although Quantum Error-Correcting approaches have successfully combat some decoherence effects, there is still a long way to go before a large-scale quantum computer can be developed.

References

[1] A. K. Junejo, N. Komninos, M. Sathiyanarayanan, and B. S. Chowdhry, “Trustee: A trust management system for fog-enabled cyber physical systems,” *IEEE transactions on emerging topics in computing*, vol. 9, no. 4, pp. 2030–2041, 2019.

[2] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of lipschitz-hankel type involving products of bessel functions,” *Philosophical Transactions of the Royal Society of London. Series A, Mathematical and Physical Sciences*, vol. 247, no. 935, pp. 529–551, 1955.

[3] D. J. Bernstein and T. Lange, “Post-quantum cryptography,” *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[4] S. Anyanwu, B. Alese, and O. Obe, “Quantum and lattices,” *International Journal of Computer Applications*, vol. 81, no. 9, 2013.

[5] L. Chen, L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology …, 2016, vol. 12.

[6] J. A. Buchmann, D. Butin, F. Göpfert, and A. Petzoldt, “Post-quantum cryptography: state of the art,” *The new codebreakers*, pp. 88–108, 2016.

[7] F. Song, “A note on quantum security for post-quantum cryptography,” in *International Workshop on Post-Quantum Cryptography*. Springer, 2014, pp. 246–265.

[8] D. J. Bernstein, “Introduction to post-quantum cryptography,” in *Post-quantum cryptography*. Springer, 2009, pp. 1–14.

[9] R. Bhattacharyya, “Tutorials: Lattice based cryptgraphy,” in *2017 International Conference on Public Key Infrastructure and its Applications (PKIA)*. IEEE, 2017, pp. 16–16.

[10] M. Ajtai, “Generating hard instances of lattice problems,” in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 99–108.

[11] D. Micciancio and O. Regev, “Lattice-based cryptography,” in *Post-quantum cryptography*. Springer, 2009, pp. 147–191.

[12] P. K. Pradhan, S. Rakshit, and S. Datta, “Lattice based cryptography: Its applications, areas of interest & future scope,” in *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*. IEEE, 2019, pp. 988–993.

[13] D. P. Chi, J. W. Choi, J. San Kim, and T. Kim, “Lattice based cryptography for beginners,” *Cryptology ePrint Archive*, 2015.

[14] J. Wan, M. Waqas, S. Tu, S. Hussain, S. U. Rehman, and A. Shah, “An efficient impersonation attack detection method in fog computing,” *Cmc -Tech Science Press-*, vol. 68, 03 2021.

[15] A. Adu-Kyere, E. Nigussie, and J. Isoaho, “Quantum key distribution: Modeling and simulation through bb84 protocol using python3,” *Sensors*, vol. 22, no. 16, p. 6284, 2022.

[16] S. Tu, M. Waqas, F. Huang, G. Abbas, and Z. H. Abbas, “A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing,” *Computer Networks*, vol. 195, p. 108196, 2021.

[17] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, “Security and privacy in device-to-device (d2d) communication: A review,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1054–1079, 2017.

[18] S. Tu, M. Waqas, S. U. Rehman, M. Aamir, O. U. Rehman, Z. Jianbiao, and C.-C. Chang, “Security in fog computing: A novel technique to tackle an impersonation attack,” *IEEE Access*, vol. 6, pp. 74 993–75 001, 2018.

[19] A. Prakasan, K. Jain, and P. Krishnan, “Authenticated-encryption in the quantum key distribution classical channel using post-quantum cryptography,” in *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*. IEEE, 2022, pp. 804–811.

[20] S. Tu, M. Waqas, Y. Meng, S. U. Rehman, I. Ahmad, A. Koubaa, Z. Halim, M. Hanif, C.-C. Chang, and C. Shi, “Mobile fog computing security: A user-oriented smart attack defense strategy based on dql,” *Computer Communications*, vol. 160, pp. 790–798, 2020.

[21] T. Laarhoven, J. van de Pol, and B. de Weger, “Solving hard lattice problems and the security of lattice-based cryptosystems,” *Cryptology ePrint Archive*, 2012.

[22] R. Niederhagen and M. Waidner, “Practical post-quantum cryptography,” *Fraunhofer SIT*, 2017.

[23] D. Buell, “Lattice-based cryptography and ntru,” in *Fundamentals of Cryptography*. Springer, 2021, pp. 205–221.

[24] V. B. Dang, F. Farahmand, M. Andrzejczak, and K. Gaj, “Implementing and benchmarking three lattice-based post-quantum cryptography algorithms using software/hardware codesign,” in *2019 International Conference on Field-Programmable Technology (ICFPT)*. IEEE, 2019, pp. 206–214.

[25] Plotting on the bloch sphere — qutip 4.1 documentation. [Online]. Available: https://qutip.org/docs/4.1/guide/guide-bloch.html

[26] C. Peikert, “Lattice cryptography for the internet,” in *International workshop on post-quantum cryptography*. Springer, 2014, pp. 197–219.

[27] Ibm quantum. [Online]. Available: https://quantum-computing.ibm.com/

[28] R. Campbell Sr, “Evaluation of post-quantum distributed ledger cryptography,” *The Journal of The British Blockchain Association*, vol. 2, no. 1, p. 7679, 2019.

[29] Q. Guo, E. Mårtensson, and P. S. Wagner, “On the sample complexity of solving lwe using bkw-style algorithms,” in *2021 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2021, pp. 2405–2410.

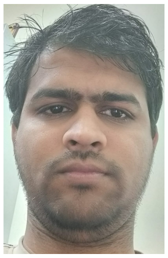
[30] A. V. Gurjanov, A. G. Korobeynikov, I. O. Zharinov, and O. O. Zharinov, “Edge, fog and cloud computing in the cyber-physical systems networks,” 2021.

[31] J. Singh, P. Singh, and S. S. Gill, “Fog computing: A taxonomy, systematic review, current trends and research challenges,” *Journal of Parallel and Distributed Computing*, vol. 157, pp. 56–85, 2021.

[32] M. Snehi and A. Bhandari, “Vulnerability retrospection of security solutions for software-defined cyber–physical system against ddos and iot-ddos attacks,” *Computer Science Review*, vol. 40, p. 100371, 2021.

[33] J. Li, Y. Zhang, J. Ning, X. Huang, G. S. Poh, and D. Wang, “Attribute based encryption with privacy protection and accountability for cloudiot,” *IEEE Transactions on Cloud Computing*, 2020.

Roopa Golchha Roopa Golchha is pursuing Masters in Information Technology from National Institute of Technology, Raipur. Her main research interests are in the area of Quantum Computing, Pattern Recognition, Cryptography, Internet of Things, and Information Security.



Jaykumar lachure Jaykumar Lachure is pursuing Ph.D. in Information Technology from National Institute of Technology, Raipur. His main research interests are in the area of Quantum Computing, Quantum Security, Cyber-Physical Security, Cryptography, Agriculture, and Information Security.

Rajesh Doriya Rajesh Doriya received his Ph.D. from Indian Institute of Information Technology Allahabad. He is currently working as an Assistant Professor in the Department of Information Technology at NIT Raipur. His research area includes Distributed and Cloud Computing, Robotics and Artificial Intelligence.