ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A COLLABORATIVE QUANTUM ASSISTED EXTENDED ELLIPTIC CURVE CRYPTOGRAPHY TECHNIQUE FOR SECURE DATA TRANSMISSION OVER NETWORK

GOVINDU SURLA[1], R. LAKSHMI[2]

[1]Research Scholar, Pondicherry University, Department of Computer Science, India
[2]Associate Professor, Pondicherry University, Department of Computer Science, India

E-mail: [1]govindu561@gmail.com , [2]prof.rlakshmi@gmail.com.

ABSTRACT

The notion of a quantum computer is no longer just theoretical. It is the most significant technology in the world, and nations are competing to become the leaders in quantum computing. The computing time will be cut down from years to hours or even minutes thanks to technology. The scientific community will greatly benefit from the capabilities of quantum computing. It does, however, represent severe risks to cyber security. All encryption algorithms are theoretically prone to damage. Compared to RSA-based cryptosystems, elliptic curve cryptography (ECC) is quicker, more effective, and more sensitive to quantum attacks. Standard ECC is still unworthy of establishing a secure network connection, nonetheless. The improved ECC method is used to extend the communication strategy, reconfiguring the message with the number of cipher-text from both sides. Therefore, we need to carefully evaluate the quantum security of EECC to prepare for the advent of quantum computers. In this, work a new strategy (CQAEECC) known as a collaborative quantum-assisted Extended Elliptic Curve Cryptography (EECC) to protect the transmission of information across networks. The mechanism of merging cryptographic methods and the private key is retrieved from the Quantum Cryptography used by Extended Elliptic Curve Cryptography to ensure greater security over networks. The novel cryptography is compared with standard algorithms and the results show that it is one of the most efficient public key cryptosystems (PKC) for desirable security. Thereupon, the proposed method has the ability to ensure confidentiality, integrity, and availability over the network.
Keywords: *Quantum Computing, Public Key Cryptography, Elliptic Curve Cryptography.*

1. INTRODUCTION

New advances in quantum computing have shown the flaws in the traditional public cryptosystem. In response to this security problem, the National Institute of Standards and Technology (NIST) has begun searching for a post-quantum encryption technique that is resistant to the design of potential quantum computers. When practical quantum computers having millions of qubits of capacity become available, they would be capable of breaking almost all current public-key cryptography methods. We need to be prepared with quantum-safe cryptography algorithms, tools, methodologies, and deployment approaches to preserve the ICT infrastructure before quantum computers with enough "qubit" capacity become available. The key distribution issue is resolved by public key cryptography (PKC) [1], yet it is thought to be computationally costly. Because of the exponential growth in processing power, most conventional encryption techniques became ineffective. In order to maintain security, the RSA algorithm—which is still extensively used worldwide—now needs extremely big keys. For PKC, elliptic curve cryptography (ECC) [2] is a chosen method. It needs a key that is 160 bits or longer to be deemed safe, although other PKC algorithms allow for considerably larger key sizes to reach the same degree of security; for example, the RSA cryptosystem requires a 1024-bit key to attain the same level of security [3]. ECC is now used for a wide range of purposes, including digital signatures, operating systems, financial applications, and communications. Accelerating the elliptic curve calculations has become essential, particularly with the advancements in quantum computing and the potential risks this technology poses to present cryptosystems. There is no data encryption or decoding involved in quantum

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

cryptography. It simply uses light polarity to transfer a shared secret key among two parties. Extended Elliptic Curve Cryptography is used in Quantum Cryptography for both data encryption and decryption. In order to secure data transfer across networks, collaborative quantum-assisted cryptography using Extended Elliptic Curve Cryptography is created in this study. In this study a new cryptography model was developed by combining Extended Elliptic Curve Cryptography with Quantum cryptography to enhance the security. The mechanism of merging cryptographic methods and the private key is retrieved from the Quantum Cryptography used by Extended Elliptic Curve Cryptography to ensure greater security over networks. The rest of the paper is organized as follows section 2 presents related works. The necessary methods and concepts are shown in Section 3. The suggested technique is described in Section 4. Section 5 describes the outcomes and evaluation. Section 6 concludes the research.

2. RELATED WORK

The elliptic curve encryption strategy is an encryption technique that has been suggested by [4]. This method divides the data into many segments. As a result, the encryption process is repeated with different keys, and it is subsequently decrypted using the same key. [4] recommend using a Quantum authenticated key distribution method to handle key distribution. Additionally, it was intended to guarantee that the communication groups were both formal and intuitive. For the protocol's authentication component, the participants depend on a 3rd party. Therefore, the suggested method may be used to network systems which handle the sensitive data, such as those in use by research institutions, the army, and healthcare providers. In order to ensure authenticity and safe key distribution, they utilized polarized photons at levels of juxtaposition, which provide a strong defense against a variety of attacks. [6] In combination with Shamir's (t, n) secure communication, A (t, n) threshold quantum cryptosystem (or (t, n)-QSS) proposes exchanging mixed conventional content and quantum states depending on monolithic phase shift function on the mono qubit. Its secret reconfiguration ensures authenticity. The framework minimizes eavesdropping by using false photons and the confidential value in Shamir's technique as the hidden value. Tests show that it is hence strong against competing risks such as entangled swapping assaults, entangle-and-measure threats, and intercept-and-resend threats. The proposed solution that includes a authentication common form, a protected secret key change, and renewal protects against several types of cyberattacks, including forging, replay, masquerade, internal, and prediction. The suggested method improves verification and offers superior privacy in mobile ad hoc networks. [7] attempted to compare QGA (Quantum Genetic Algorithms), which executed 25 times and again for 500 iterations, with genetic algorithms. The general difficulty of QGA appears to lie on the O(N) measure, where N is the whole population. Conversely, a GA's hardness has been measured on a scale an O (N2). As a consequence, the complexity is reduced to a linear state. [8] Identify the vehicle identity verification security problem and provide a quantum defensive mechanism for vehicular ad hoc networks (VANETs). It is based on the BB84 quantum secure-key exchange method and quantum physics. Furthermore, the special quantum system is able to ward off the majority of attacks aimed at VANETs. Additionally, because the recommended quantum technique addresses the issues of reliability and security, all cars may be connected. Moreover, by skillfully using aspects of quantum physics, their proposed system offers special advantages including irreversibility, identity revocation, and remote identity verification.

3. METHODS AND CONCEPTS

The section first describes the important methods and concepts involved for a better understanding of the complete study.

3.1 Cryptography

Cryptography is a technique that creates a protected communication channel among 2 parties in order to secure data while unauthorized users are present. The Institute of Electrical and Electronics Engineers (IEEE) invented this method. In cryptography, the two operations that are performed by both the sender and the recipient are encryption and decryption. Cryptographic techniques fall into two main categories: symmetric and asymmetric. Figure 1 depicts the whole classification of cryptographic methods. A single key is all that is needed for the decryption and encryption of data in symmetric cryptography. This approach requires the utilization of a private key. This alludes to the need for a private key be kept secret and distributed only to senders and recipients who have the proper authorization. Figure 2a depicts the symmetric cryptography process, whereas Figure 2b shows the asymmetric cryptography process in a similar manner.

Journal of Theoretical and Applied Information Technology
15th December 2023. Vol.101. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Asymmetric cryptography sometimes referred to as public key cryptography, utilizes a key pair for both decryption & encryption. The pair of keys includes one publicly available key. For encryption, the sender would utilize a public key, and the receiver would utilize a private key that they alone know [9]. The functioning of an asymmetric cryptography system is shown in Figure 2b.

Symmetric key algorithms are very effective and simple to use. Key management is a difficult problem in symmetric cryptography, however. Before starting a conversation, the two parties need to exchange the key. The most common attacks on symmetric cyphers are chosen-plaintext, known-plaintext, linear, and differential cryptanalysis. Algorithm for Asymmetric Cryptography: An asymmetric cryptography algorithm uses two keys, one for each party. One of the keys is kept private, or secret, while the other is made available to the public, or the public key. A public-key algorithm is another name for an asymmetric cryptography method. Data is encrypted through sender utilizing a public key, and it is decrypted by the recipient utilizing a private key. Asymmetric encryption methods often need more processing power and time due to their resource-intensive nature.

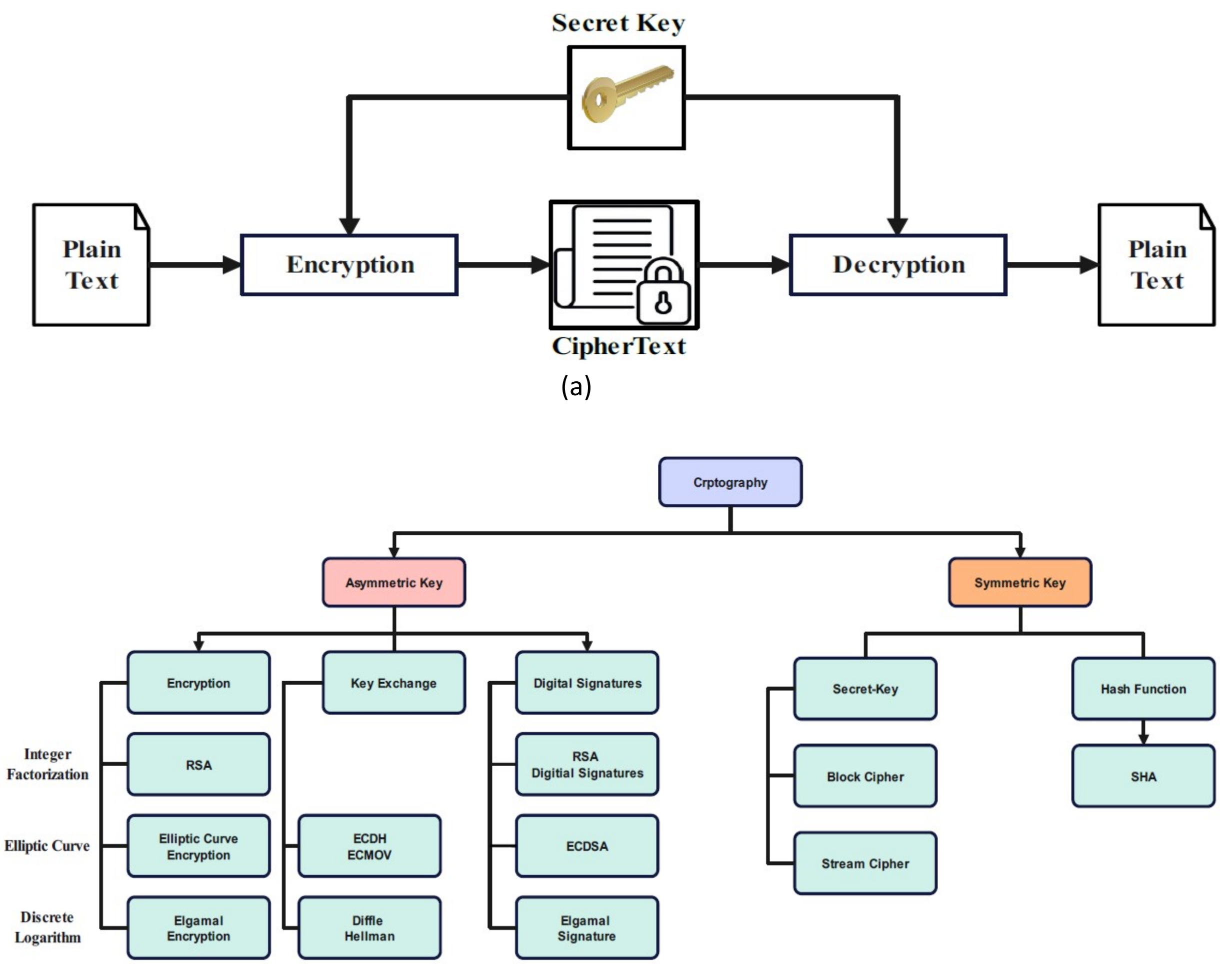


Figure 1. The Classification of Cryptography Methods

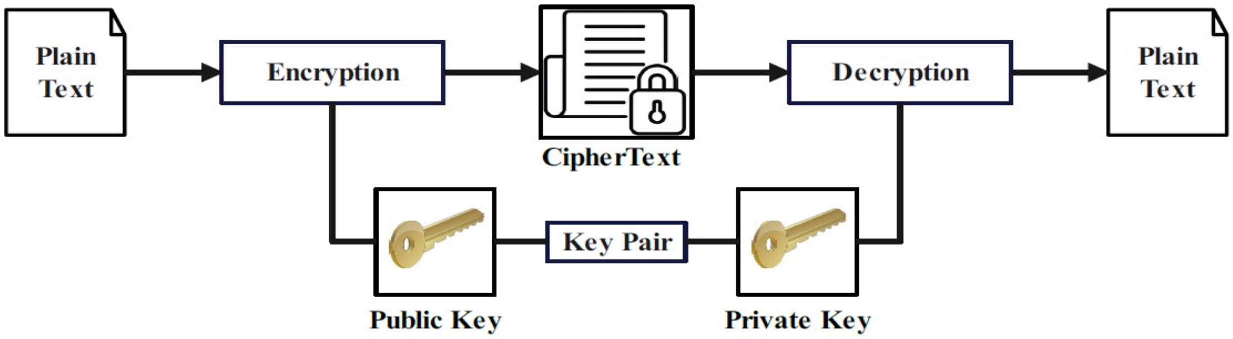


Figure 2. The process framework of Symmetric and Asymmetric Cryptography

3.1.1 quantum cryptography

With its unfathomable processing capacity, quantum computers are quickly becoming a reality [10]. We need to think about how Internet security will change as quantum computing capacity grows in the near future. Based on the ideas of quantum theory, quantum computing is a technology that processes information much more quickly than traditional computer methods. Quantum computers can exploit classical cryptography schemes with perfect impunity. The current IT infrastructure will become entirely hazardous as a result of the shift to quantum computing, necessitating the creation of quantum-resistant or quantum-safe cryptographic techniques. Given the capabilities of quantum computing, a great deal of research is being done to find solutions to the challenging issues in contemporary cryptography. This work is anticipated to have a major influence on the security of the existing conventional public key cryptosystems in future. Public key primitives are in danger because of recent advancements in quantum computing, which may solve complicated cryptographic issues in polynomial time. Adopting protocols and algorithms that are specifically intended to resist the attacks of quantum computers is important. These techniques usually depend on mathematical puzzles that are challenging for computers, both classical & quantum. Asymmetric cryptographic approaches which are resistant to assaults from a quantum computer are known as post-quantum cryptography or PQC.

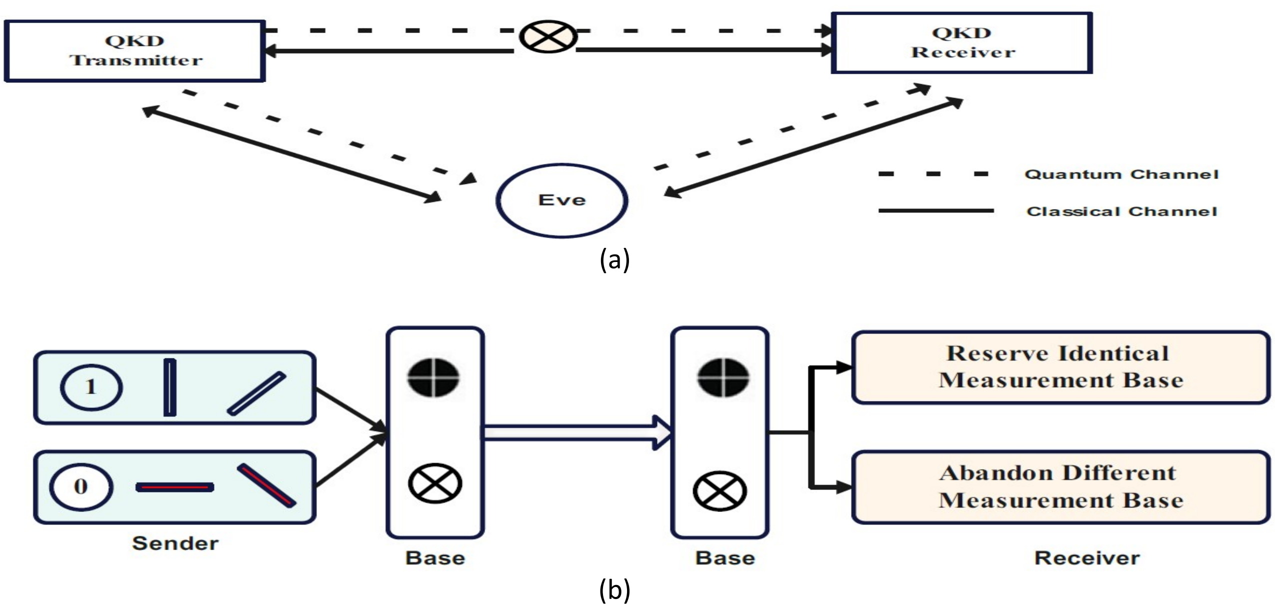


Figure 3. Quantum Computing

15th December 2023. Vol.101. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The most secure cryptosystem in the world is created by the fascinating field of quantum cryptography, which makes use of quantum physics. Given that no system can have its quantum state discovered without alerting it, photons and their fundamental quantum properties are the foundation of quantum cryptography, which uses them to construct an unbreakable cryptosystem. It cannot be compromised without the knowledge of the communication's sender and receiver. The foundation of quantum cryptography is the photons utilization, the smallest individual particles in nature. These photons are capable of being in several states at once, and their conditions only change when they are quantized. This is the main property that quantum cryptography methods make use of. The sender or recipient detects the change in photon status immediately when a message is sent along a channel from sender to recipient and an adversary tries to intercept the transmission. Furthermore, there is a kind of approach that utilizes the property of quantum entanglement. Because of a phenomenon known as quantum entanglement, which occurs even when two quantum particles or photons are physically separated, every change in one causes a change in the other, it becomes simpler to detect intrusions in networks.

4. PROPOSED METHOD: CQAEECC

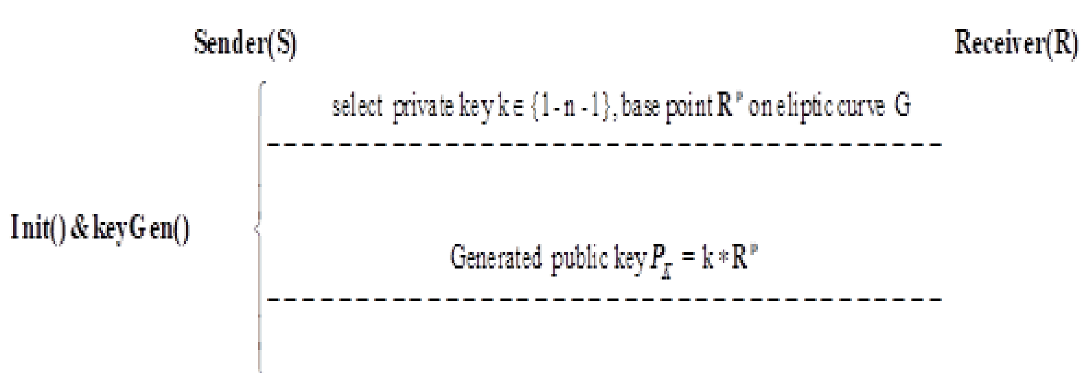
The proposed scheme is described in terms of Preliminaries, the System Methods, Formal Method, while the construction of the proposed model is described below.

4.1. Preliminaries

In this section, we introduce the basic principles of the ECH and EECC.

4.1.1. elliptic curve cryptography (ECC)

The ECC algorithm performs better cryptography with improved security when it is compared with conventional cryptographic methods like DH, RSA, and DSA. The ECC algorithm provides the same level of security even if the key size is reduced compared to the conventional techniques. Elliptic Curve Cryptography (ECC) was viewed as an elliptic curve analogous to the older discrete logarithmic (DL) cryptosystem suggested by [11]. The ECC strength depends on the Elliptic Curve Discrete Logarithmic Problem (ECDLP). The two values $\mathbf{a}$ and $\mathbf{b}$ is used to define the elliptic curve and is represented as $E(a,b)_p : y^2 + ax + b \bmod p$ with discriminant $4a^3 + 27b^2 \bmod p \neq 0$. The set of points on this curve includes a point at infinity denoted by δ and all points (x, y) within $F_p * F_p$ that satisfy the equation. The variants are ECC are the Diffie-Hellman Algorithm (ECDHA), ECC-based digital signature (ECDSA) [12], and ECC-based encryption is called as Elliptic Curve-based Integrated Encryption Scheme (ECIES). The complete idea behind the Elliptic Curve Cryptography scheme is described in the flow graph and is shown in Figure 4.



ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Encry()

Let message 'm' on eliptic curve G with point Q, select $L \in \{1\text{-}n\text{-}1\}$,

Generated *Two Cipher Texts* $\mathbf{CT_1} = L * \mathbf{R^p}$ & $\mathbf{CT_2} = Q + L * \boldsymbol{P_K}$

Send()

send $\mathbf{CT_1}$ & $\mathbf{CT_2}$ —> **Receiver**

Recieve()

Sender <— recieved $\mathbf{CT_1}$ & $\mathbf{CT_2}$

Decry()

Message is retieved $m = \mathbf{CT_2} - k * \mathbf{CT_1}$

Figure 4. Elliptic curve cryptography (ECC) Scheme: A Flow graph

Figure 4. shown the flow process behind ECC and the complete shame is described in terms of the below steps from which established communication between Sender(S) and Receiver(R)

1. First, the sender chooses the private secret key k from the range $\{1 \text{ to } n-1\}$ and also selects the base point R^P from the elliptic curve G.
2. Next, public key is generated with the private key and base point and is defined as $P_K = k * R^P$
3. In order to perform the encryption of messages m. The selected point Q on the elliptic curve G and key $L \in \{1 \text{ to } n-1\}$
4. Based on the above assumption two cipher texts were defined: $CT_1 = L * R$ & $CT_2 = Q + L * P_K$
5. Now the two cipher texts are transferred from sender to receiver over a secure channel.
6. Finally, the receiver gets the CT_1 & CT_2 and obeys the secret key, and at final message is decrypted $m = CT_2 - k * CT_1$.

4.1.2. Extended Elliptic Curve Cryptography (EECC):

The points of an elliptical curve are used by the basic cryptographic method known as ECC to encrypt data. A particular type of algebraic mathematical curve over prime finite fields is called an elliptic curve, or E. The EECC method works better than the traditional ECC in terms of cypher text, decryption time, encryption, and security. It is made to be more difficult since it replaces the text's repeating letters with a new cypher text in each cycle. The ECCC differs from the standard ECC with the generation of public keys from both users allowed here with the single base point. Also, cipher text generations also had variations compared to standard ECC.

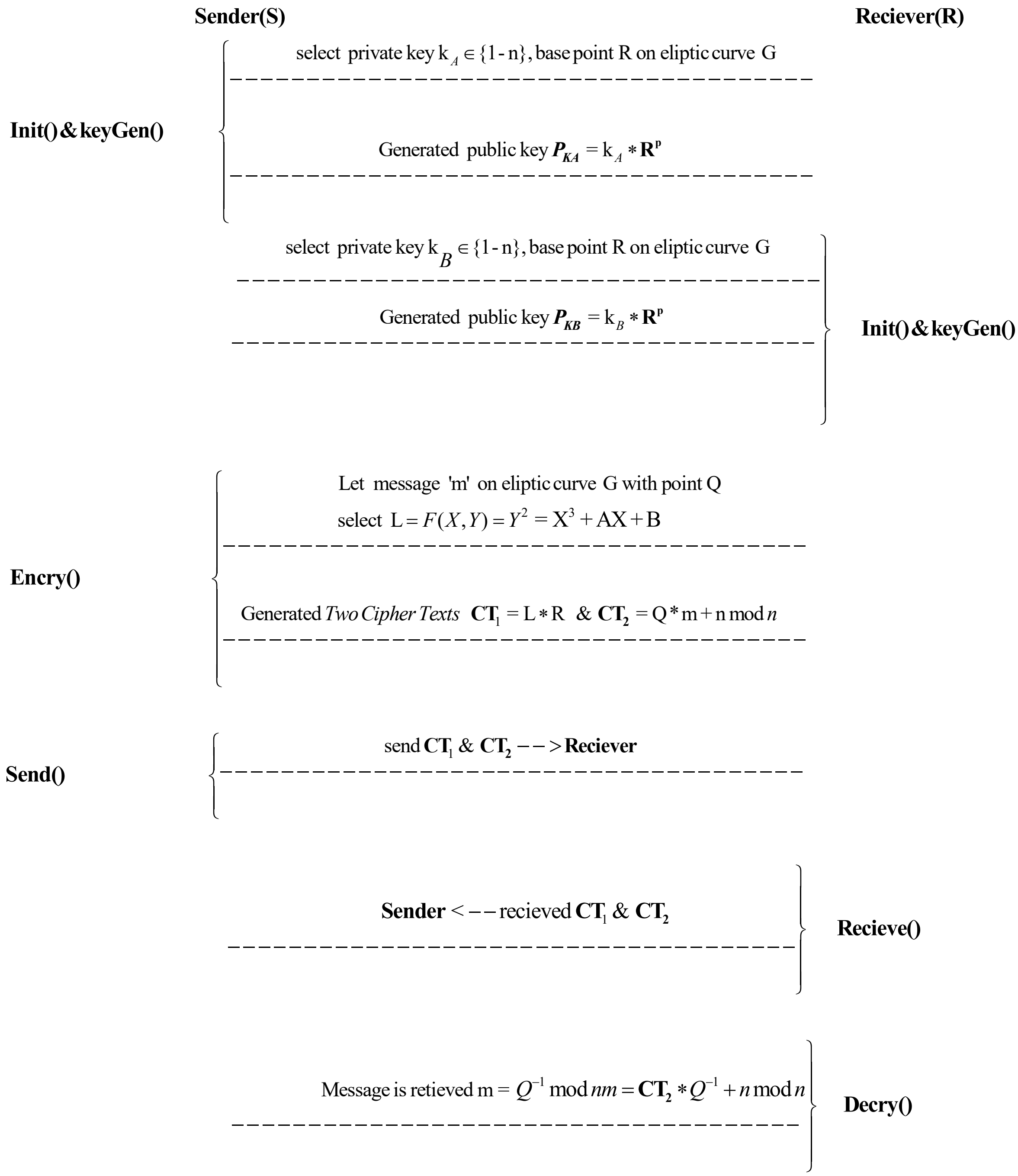


Figure 5. Extended Elliptic Curve Cryptography (EECC) Scheme: A flow graph

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 5, shows the flow process behind EECC, and the complete shame is described in terms of the below steps from which established communication between the Sender(S) and Receiver(R)

1. First, the sender and receiver choose the private secret keys K_A and K_B from the range $\{1 \text{ to } n-1\}$ and also select the base point R from the elliptic curve G.
2. Next, the two public keys are generated for both S and R with private keys and base point and are defined as $P_{KA} = k_A * R^P$ and $P_{KB} = k_B * R^P$
3. In order to perform the encryption of message m. A selected point Q on elliptic curve G and key $L = F(X,Y) = Y^2 = X^3 + AX + B$
4. Based on the above assumption two cipher texts were defined as: $CT_1 = L * R$ & $CT_2 = Q * m + n \bmod n$
5. Now the two cipher texts are transferred from sender to receiver over a secure channel.
6. Finally, the receiver got the CT_1 & CT_2 and obey on the secret key and at final message is decrypted as $m = Q^{-1} \bmod nm = CT_2 * Q^{-1} n \bmod n$

4.2. System Model

The proposed model consists of seven systems, which include the Key Generation System (KGS), Sender (S), Receiver(R), Quantum Cryptography (QC), Key Accordance (KA), Encryption (E), and Decryption (D). The algorithms in the system model are explained as follows:
The proposed model CQAEECC uses the following functions:

- **Key Generation System (KGS):** The trusted authority system is used to create the private & public keys.
- **Sender (S):** The sender who wishes to communicate to the receiver in a secure manner with encrypted a cipher text CT of the message m.
- **Receiver (R):** The trusted user-initiated requests to the Sender for the cipher text decryption and extracted the desired message m.
- **Quantum Cryptography (QC):** The system, ensures additional security by providing a separate private key to the receiver.
- **Key Accordance (KA):** The system is used to define the secret shared key obeyed by both Sender and Receiver.
- **Encryption (E):** Symmetric encryption algorithm used for the encryption of message m.
- **Decryption (D):** Symmetric encryption algorithm used for the decryption of message m.

4.3 Formal Model

Figure 6-7, shows the flow process behind CQAEECC, and the complete scheme is described in terms of the below steps from which established secure communication between Sender(S) and Receiver(R). The complete proposed scheme CQAEECC is described in terms of the four algorithms which are described below:

1. Key Generation - $keyGen()$: The algorithm considers the two-input parameter including the private key k_s and a base point R^P on G.The KGS outputs a public key PK_S for Receiver R.

i. First, the sender and receiver choose the private secret keys k_s and k_r from the range $\{1 \text{ to } n-1\}$ and also select the base point R^T from the elliptic curve G.

ii. Next, the two public keys are generated for both S and R with private keys and base point and are defined as $P_{K_S} = k * R^T$ and $P_{K_R} = k_r * R^T$

iii. Later, one additional private key is generated from the Quantum Cryptography QC used for additional security k_q received by the R and same communicated to S.

Journal of Theoretical and Applied Information Technology
15th December 2023. Vol.101. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. **Key Accordance - $\mathbf{keyAcc()}$:** The algorithm considers the two-input parameter including the private key $\mathbf{k_q}$ generated by the $\mathbf{QC}$ and public key $\mathbf{P_{K_R}}$. The $\mathbf{KGS}$ outputs are a secret shared key $\mathbf{SA_V}$ for both Sender ($\mathbf{S}$) and Receiver ($\mathbf{R}$). Intern this output is applied to the $\mathbf{keyDer(SA_V)}$ function and derived the key pair for the further process $\{\mathbf{E_{key}}, \mathbf{S_{key}}\}$

3. **Encryption- $\mathbf{Encry()}$:** The algorithm considers the three-input parameters including the message $\mathbf{m}$ and the key pair $\{\mathbf{E_{key}}, \mathbf{S_{key}}\}$ delivered by $\mathbf{keyDer()}$ the algorithm. The $\mathbf{E}$ outputs $\mathbf{C_P}$ a Crypto pair to the Receiver ($\mathbf{R}$).
   i. In order to perform the encryption of messages $\mathbf{m}$. The selected point $\mathbf{Q}$ on elliptic curve $\mathbf{G}$ and the key pair $\{\mathbf{E_{key}}, \mathbf{S_{key}}\}$.
   ii. With the above parameters applied the $\mathbf{Encry()}$ and $\mathbf{Tag\_Gen()}$ functions generated Ciphertext and Tag $\mathbf{C_T = Encry(E_{key}, m)}$ & $\mathbf{T = Tag\_Gen(S_{key}, C_T)}$ respectively.
   iii. Next, derived Crypto pair $\mathbf{C_p = (C_T, PK_S, T)}$ and communicated to the sender $\mathbf{S}$ over the secure channel.

4. **Decryption - $\mathbf{Decry()}$** The algorithm considers the three-input parameter including the private key $\mathbf{k_q}$ generated by the $\mathbf{QC}$ public key of $\mathbf{PK_R}$ and Crypto pair $\mathbf{C_P}$. The $\mathbf{D}$ outputs $\mathbf{m}$.
   i. In order to perform the decryption of the message $\mathbf{m}$. First Select private key $\mathbf{k_q}$ and public key of $\mathbf{PK_R}$ and generate the key pair $\{\mathbf{E_{Key}}, \mathbf{S_{key}}\} \leftarrow \mathbf{keyDer(SA_V)}$.
   ii. With the $\mathbf{S_{key}}$ and $\mathbf{C_P}$ generated the Tag $\mathbf{T_R = S_{key}(C_P)}$.
   iii. If $\mathbf{(T_R = T)}$ consider the $\mathbf{C_P}$ otherwise drop the $\mathbf{C_P}$.
   iv. Once the above condition is satisfied finally the message $\mathbf{m}$ is retrieved with $\mathbf{m = Decry(C_P)}$.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

KEY ACCORDANCE(KA) : keyAcc()

Sender(S) **Reciever (R)**

Sender:
- $Generate\ SA_V = k_q * \boldsymbol{PK_R}$
- $\{E_{key}, S_{key}\} <- KeyDer(SA_V)$

ENCRYPTION(E) : Encry()

Sender(S) **Reciever (R)**

Sender:
- message 'm' on G with point Q, E_{key}, S_{key}
- $\mathbf{C_T} = \text{Encry}(E_{key}, m)$ & $\mathbf{T} = \text{Tag\_gen}(S_{key}, \mathbf{C_T})$
- $Cryptopair = \mathbf{C_P} = (\mathbf{C_T}, \boldsymbol{PK_S}, \mathbf{T})$

Sender:
- send $\mathbf{C_P} = (\mathbf{C_T}, \boldsymbol{PK_S}, \mathbf{T})$

Reciever:
- recieved $\mathbf{C_P} = (\mathbf{C_T}, \boldsymbol{PK_S}, \mathbf{T})$

Figure 6. The flow graph of the Key Generation System in CQAEECC

KEY GENERATION SYSTEM(KGS) : keyGen()

Sender(S) **Reciever(R)** **Quantum Cryptography(QC)**

Sender:
- private key $k_s \in \{1 - n\}$, base point $\mathbf{R}^T$ on G
- public key $PK_S = k_s * \mathbf{R}^T$

Reciever:
- private key $k_r \in \{1 - n\}$, base point $\mathbf{R}^T$ on G
- public key $PK_R = k_r * \mathbf{R}^T$

Quantum Cryptography:
- private key k_q
- send private key k_q to reciver

Reciever:
- received k_q from Quantum Cryptography
- Send k_q to Sender

Figure 7. The flow graph of the Key Accordance and Encryption Systems in CQAEECC

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DECRYPTION : Decry()

Sender(S) **Reciever (R)**

$$\text{retieved } SB_V = k_q * \boldsymbol{PK_R}$$

$$Generate\ \{E_{key}, S_{key}\} <- KeyDer(SA_V)$$

$$\text{retieved } \mathbf{T}_R = S_{key}(\mathbf{C_P})$$

$$if\ (\mathbf{T}_R == \mathbf{T})\ \text{consider } \mathbf{C_P}\ \text{, otherwise drop } \mathbf{C_P}$$

$$m = Decry(\mathbf{C_P})$$

Figure 8. The flow graph of the Decryption Systems in CQAEECC

Suppose an eavesdropper saw the communication and attempted to decipher it. If the value does not match, the message cannot be decrypted without the recipient's private key, which is needed to produce encryption as the sender and use KDF functions. We may state that the eavesdroppers cannot access the plaintext. If the private key is unknown and does not supply the same optional parameter as the sender, the eavesdropper will not be able to decode the message, as the above CQAEECC method explains.

5. RESULTS AND ANALYSIS

Present-day research is focused on how quantum cryptography is used by CQAEECC for the secure transmission of data over the network. In this section, we compare the performance of proposed cryptography with standard public-key encryption schemes. All schemes have been measured on an Intel(R) Core (TM) i7-1165G7 @ 2.80GHz using Qis kit Simulator. Table 2-5 and Figure 9-12, shows the runtime execution time of encryption and decryption of the proposed cryptography algorithm over standard techniques. The results show that the proposed algorithms are the best compared to the others in performing the key operations. The calculation of the standard ECC, ECDH, ECDSA, ECC_QC, and CQAEECC is verified under the following parameters.

- Key Generation Time
- Decryption Time
- Encryption Time
- Execution Time

5.1. Key Generation Time

Time is taken for generating the elliptic curve's secret key of both standard four ECC, ECDH, ECDSA, ECC_QC, and CQAEECC methods. Table 2 and Figure 9, below shows the key generation time of the suggested and standard public key cryptography algorithm in different file sizes with and without using quantum cryptography. From the consequences shown in Table 2 and Figure 9, a comparison analysis of key generation time for many file sizes is performed. If the file size is from 8 KB to 1024 KB means, then the key generation time for the proposed

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CQAEECC approach is running from 89ms to 208ms respectively. While comparing to the existing approaches ECC, ECDH, ECDSA, and ECC_QC approaches take much more time and show the strongest security concern. Moreover, it is observed that ECC_QC had closure results with the suggested CQAEECC method. This result also depicts that the key generation time of the proposed CQAEECC strategy is slightly higher compared with the entire standard techniques intern improves the security level.

Table 2. Key Generation Time Analysis of Non-Quantum and Quantum-based Cryptographic Algorithms

File size (KB)	Time (ms)				
	ECC	ECDH	ECDSA	ECC_QC	CQAEECC
8	48	54	72	81	89
16	51	80	85	90	97
32	59	89	101	111	136
64	74	95	117	127	153
128	88	124	145	158	172
256	91	131	150	159	178
512	98	143	157	171	187
1024	102	151	162	195	208

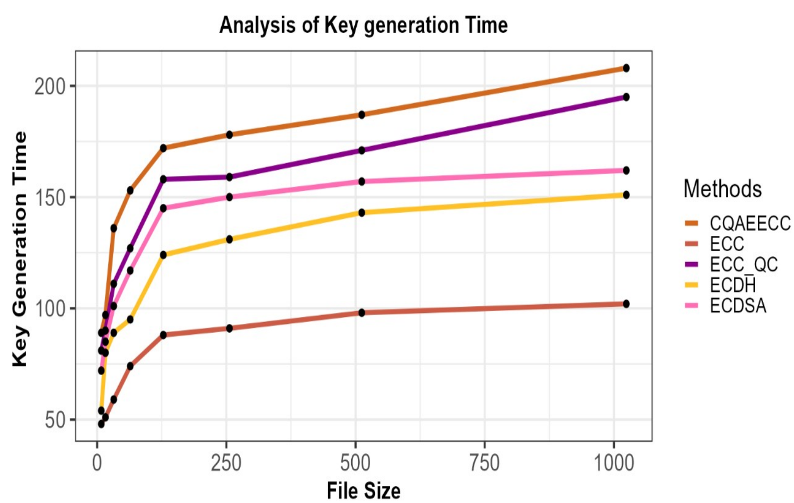


Figure 9. Key Generation Time Analysis of Non-Quantum and Quantum-based Cryptographic Algorithms

5.2. Encryption Time

Time is taken for generating cipher text over the message of both standard and CQAEECC methods. Table 3 and Figure 10, below shows the encryption time of the proposed and standard public key cryptography algorithm in different file sizes with and without using quantum cryptography. From the results shown in Table 3 and Figure 10, a comparison evaluation of encryption time for various sizes of file is performed. If the file size is from 8 KB to 1024 KB means, then the key generation time for the proposed CQAEECC method is running from 75 ms to 172 ms correspondingly. While comparing to the existing methods ECC, ECDH, ECDSA, and ECC_QC approaches take much more time which shows that this technique puts additional effort into making encryption much better. Moreover, it is observed that ECC_QC had also retained some closure effort to make the encryption strategy much better compared to ECC, ECDH, and ECDSA but not as well as the proposed CQAEECC method. This result also displays that the encryption time of the suggested CQAEECC strategy is slightly higher compared with the entire standard techniques.

Table 3. Encryption Time Analysis of Non-Quantum and Quantum-based Cryptographic Algorithms

File size (KB)	Time (ms)				
	ECC	ECDH	ECDSA	ECC_QC	CQAEECC
8	20	32	53	67	75
16	23	38	62	74	82
32	32	58	88	91	98
64	35	65	98	103	117
128	38	73	109	112	128
256	44	87	127	138	147
512	48	95	139	149	169
1024	67	112	146	165	172

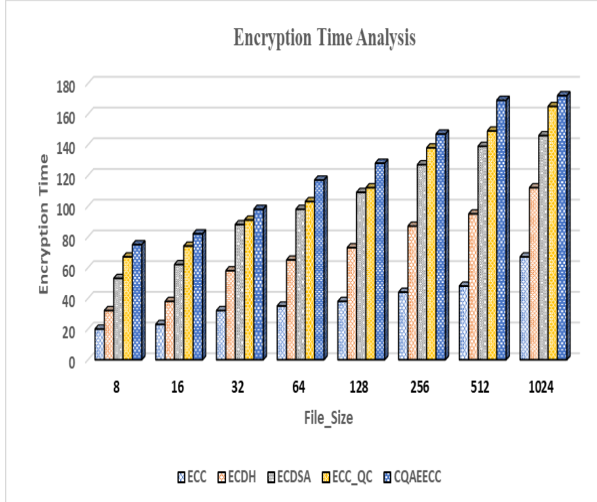


Figure 10. Encryption Time Analysis of Non-Quantum and Quantum-based Cryptographic Algorithms.

5.3. Decryption Time

Time taken for retrieving message over Ciphertext of both standard and CQAEECC methods. Table 4 and Figure 11, below shows the decryption time of the proposed and standard public key cryptography algorithm in different file sizes with and without using quantum cryptography. From the outcomes presented in Table 4 and Figure 11, a comparison analysis of decryption time for various sizes of files is performed. If the file size is from 8 KB to 1024 KB means, then the key decryption time for the suggested CQAEECC method is running from 83 ms to 219 ms correspondingly. Compared to the existing methods ECC, ECDH, ECDSA, and ECC_QC approaches take much more time, which shows that this technique puts additional effort into making decryption much better. Moreover, it is observed that ECC_QC had also retained some closure effort to make the decryption strategy much better compared to ECC, ECDH, and ECDSA but not as well as the proposed CQAEECC method. This result also depicts that the decryption time of the suggested CQAEECC strategy is slightly higher compared with the entire standard techniques respectively.

Table 4. Decryption Time Analysis of Non-Quantum and Quantum-based Cryptographic Algorithms

File size (KB)	Time (ms)				
	ECC	ECDH	ECDSA	ECC_QC	CQAEECC
8	18	26	28	69	83
16	26	32	39	73	95
32	30	38	84	88	110
64	39	46	90	95	116
128	42	73	98	103	132
256	50	82	111	116	139
512	65	89	119	125	146
1024	79	119	160	180	219

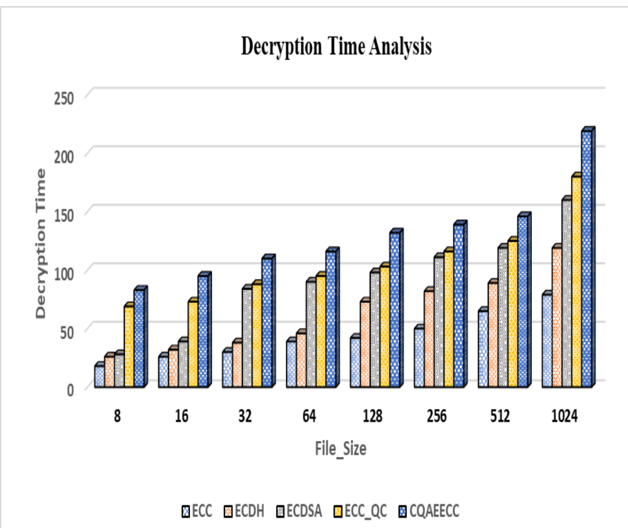


Figure 11. Decryption Time Analysis of Non-Quantum and Quantum-based Cryptographic Algorithms

5.4. Execution Time

Time taken for execution entire process of secure communication from sender to receiver of both standard and CQAEECC methods. Table 5 and Figure 12, below shows the execution time of the proposed and standard public key cryptography algorithm in different file sizes with and without using quantum cryptography. From the outcomes shown in Table 5 and Figure 12, a comparison analysis of execution time for various sizes of files is performed. If the size of the file is from 8 KB to 1024 KB means, then the execution time for the suggested CQAEECC method is running from 497 ms to 11946 ms respectively. While comparing to the present approaches ECC, ECDH, ECDSA, and ECC_QC approaches take much more time and show the strongest security concern. Moreover, it is observed that ECC_QC had closure results with the proposed CQAEECC method. This result also depicts that the execution time of the suggested CQAEECC strategy is slightly higher compared with the entire standard techniques intern improves the security level.

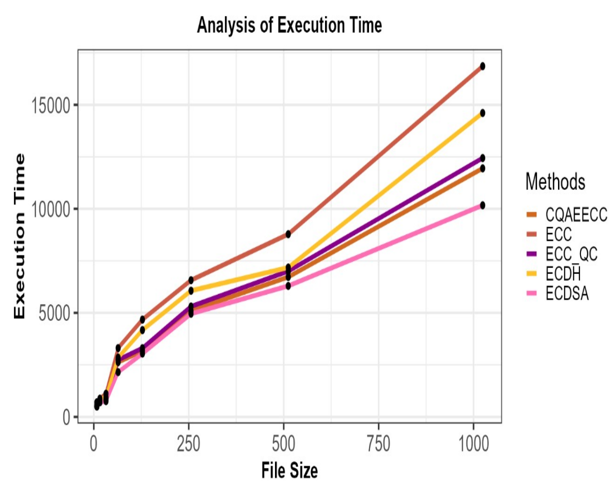


Figure 12. Execution Time Analysis of Non-Quantum and Quantum-based Cryptographic Algorithms.

6. CONCLUSION

In this research, we examine the effective methods that have been suggested for safe network-based data transfer. A novel approach called the CQAEECC is put forward to guarantee the integrity of the data that users in the network share and to exchange secret keys. Two techniques—EECS and quantum cryptography—are used in the development of the proposed CQAEECC method to shield data owners against network attacks. By exchanging shared keys produced by quantum cryptography, this technique allows both parties to maintain their confidentiality. To maintain the secrecy of the data, all active owners share a secret key and authenticate each other using their public and private keys. The parties guarantee the integrity of the exchanged data by using these algorithms. The suggested architecture increases the data's encryption and decryption time efficiency. The results show that our suggested CQAEECC works better in both the data sharing and mutual authentication procedures than the conventional ECC, ECDH, ECDSA, and ECC QC. Our next research will concentrate on expanding this technique to a wider cloud environment in order to evaluate cryptographic threats and improve the method's performance.

REFERENCES

[1]. Vangala, A.; Das, A.K.; Mitra, A.; Das, S.K.; Park, Y. Blockchain-Enabled Authenticated Key Agreement Scheme for Mobile Vehicles-Assisted Precision Agricultural IoT Networks. IEEE Trans. Inf. Forensics Secur. 2022, 18, 904–919. [Google Scholar] [CrossRef]

[2]. Shafi, U.; Mumtaz, R.; García-Nieto, J.; Hassan, S.A.; Zaidi, S.A.R.; Iqbal, N. Precision Agriculture Techniques and Practices: From Considerations to Applications. Sensors 2019, 19, 3796. [Google Scholar] [CrossRef] [PubMed][Green Version]

[3]. Shi, X.; An, X.; Zhao, Q.; Liu, H.; Xia, L.; Sun, X.; Guo, Y. State-of-the-Art Internet of Things in Protected Agriculture. Sensors 2019, 19, 1833. [Google Scholar] [CrossRef][Green Version]

[4]. Vangala, A.; Das, A.K.; Chamola, V.; Korotaev, V.; Rodrigues, J.J. Security in IoT-enabled smart agriculture: Architecture, security solutions and challenges. Cluster Comput. 2022, 26, 879–902. [Google Scholar] [CrossRef]

[5]. Bera, B.; Vangala, A.; Das, A.K.; Lorenz, P.; Khan, M.K. Private blockchain-envisioned drones-assisted authentication scheme in IoT-enabled agricultural environment. Comput. Stand. Interfaces 2022, 80, 103567. [Google Scholar] [CrossRef]

[6]. Rangwani, D.; Sadhukhan, D.; Ray, S.; Khan, M.K.; Dasgupta, M. An improved privacy preserving remote user authentication scheme for agricultural wireless sensor network. Trans. Emerg. Telecommun. Technol. 2021, 32, e4218. [Google Scholar] [CrossRef]

[7]. Lan, G.; Brewster, C.; Spek, J.; Smeenk, A.; Top, J. Blockchain for Agriculture and Food; Findings from the Pilot Study, Report; Wageningen Economic Research: Wageningen, The Netherlands, 2017; p. 34. [Google Scholar]

[8]. Nyangaresi, V.O.; Ibrahim, A.; Abduljabbar, Z.A.; Hussain, M.A.; Al Sibahee, M.A.; Hussien, Z.A.; Ghrabat, M.J.J. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges. In Proceedings of the 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 9–10 December 2021; pp. 1–6. [Google Scholar]

[9]. Sontowski, S.; Gupta, M.; Chukkapalli, S.S.L.; Abdelsalam, M.; Mittal, S.; Joshi, A.; Sandhu, R. Cyber attacks on smart farming infrastructure. In Proceedings of the 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC), Atlanta, GA, USA, 1–3 December 2020; pp. 135–143. [Google Scholar]

[10]. Khanna, A.; Kaur, S. Evolution of Internet of Things (IoT) and its significant impact in the field of Precision Agriculture. Comput. Electron. Agric. 2019, 157, 218–231. [Google Scholar] [CrossRef]

[11]. Van der Merwe, D.; Burchfield, D.R.; Witt, T.D.; Price, K.P.; Sharda, A. Drones in agriculture. Adv. Agron. 2020, 162, 1–30. [Google Scholar]

[12]. Dagar, R.; Som, S.; Khatri, S.K. Smart farming–IoT in agriculture. In Proceedings of the 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 11–12 July 2018; pp. 1052–1056. [Google Scholar]

[13]. Sanjeevi, P.; Prasanna, S.; Kumar, B.S.; Gunasekaran, G.; Alagiri, I.; Anand, R.V. Precision agriculture and farming using Internet of Things based on wireless sensor network. Trans. Emerg. Telecommun. Technol. 2020, 31, e3978. [Google Scholar] [CrossRef]

[14]. Nyangaresi, V.O.; Abduljabbar, Z.A.; Refish, S.H.A.; Al Sibahee, M.A.; Abood, E.W.; Lu, S. Anonymous Key Agreement and Mutual Authentication Protocol for Smart Grids. In Cognitive Radio Oriented Wireless Networks and Wireless Internet, Proceedings of the 16th EAI International Conference, CROWNCOM 2021, Virtual Event, 11 December 2021, and 14th EAI International Conference, WiCON 2021, Virtual Event, 9 November 2021; Springer International Publishing: Cham, Switzerland, 2022; pp. 325–340. [Google Scholar]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[15]. Wazid, M.; Das, A.K.; Bhat, V.; Vasilakos, A.V. LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. J. Netw. Comput. Appl. 2020, 150, 102496. [Google Scholar] [CrossRef]

[16]. Wang, D.; Li, W.; Wang, P. Measuring Two-Factor Authentication Schemes for Real-Time Data Access in Industrial Wireless Sensor Networks. IEEE Trans. Ind. Inform. 2018, 14, 4081–4092. [Google Scholar] [CrossRef]

[17]. Challa, S.; Das, A.K.; Gope, P.; Kumar, N.; Wu, F.; Vasilakos, A.V. Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems. Futur. Gener. Comput. Syst. 2018, 108, 1267–1286. [Google Scholar] [CrossRef]

[18]. Vangala, A.; Das, A.K.; Lee, J. Provably secure signature-based anonymous user authentication protocol in an Internet of Things-enabled intelligent precision agricultural environment. Concurr. Comput. Prac. Exp. 2021, 35, e6187. [Google Scholar] [CrossRef]

[19]. Alsamhi, S.H.; Shvetsov, A.V.; Kumar, S.; Shvetsova, S.V.; Alhartomi, M.A.; Hawbani, A.; Rajput, N.S.; Srivastava, S.; Saif, A.; Nyangaresi, V.O. UAV Computing-Assisted Search and Rescue Mission Framework for Disaster and Harsh Environment Mitigation. Drones 2022, 6, 154. [Google Scholar] [CrossRef]

[20]. Vangala, A.; Sutrala, A.K.; Das, A.K.; Jo, M. Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming. IEEE Internet Things J. 2021, 8, 10792–10806. [Google Scholar] [CrossRef]

[21]. Akram, S.V.; Malik, P.K.; Singh, R.; Anita, G.; Tanwar, S. Adoption of blockchain technology in various realms: Opportunities and challenges. Secur. Priv. 2020, 3, e109. [Google Scholar] [CrossRef][Green Version]

[22]. Lin, Y.-P.; Petway, J.R.; Anthony, J.; Mukhtar, H.; Liao, S.-W.; Chou, C.-F.; Ho, Y.-F. Blockchain: The Evolutionary Next Step for ICT E-Agriculture. Environments 2017, 4, 50. [Google Scholar] [CrossRef][Green Version]

[23]. Almadhoun, R.; Kadadha, M.; Alhemeiri, M.; Alshehhi, M.; Salah, K. A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In Proceedings of the 2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA), Aqaba, Jordan, 28 October–1 November 2018; pp. 1–8. [Google Scholar]

[24]. Wang, L.; Xu, L.; Zheng, Z.; Liu, S.; Li, X.; Cao, L.; Li, J.; Sun, C. Smart Contract-Based Agricultural Food Supply Chain Traceability. IEEE Access 2021, 9, 9296–9307. [Google Scholar] [CrossRef]