Quantum-Safe Authentication Protocol Using Post-Quantum Key Encapsulation Mechanism for Transportation Systems

Rohini Poolat Parameswarath
Department of ECE
College of Design and Engineering
National University of Singapore
Singapore
rohini.p@nus.edu.sg

Biplab Sikdar
Department of ECE
College of Design and Engineering
National University of Singapore
Singapore
bsikdar@nus.edu.sg

***Abstract*—The integration of Internet of Things (IoT) technology into transportation systems holds immense potential to transform the way we move people and goods, offering benefits such as increased efficiency, reduced emissions, improved safety, and enhanced user experience. With the ubiquitous and high-speed connectivity, sixth-generation (6G) technology is envisaged to make unprecedented revolutions in several fields and applications including IoT applications and transportation systems. The convergence of 6G networks with these applications will provide seamless connectivity and help to integrate functionalities such as sensing, communication, and computing, resulting in superior service quality. However, the IoT network is highly vulnerable to cyber-attacks. With the recent developments in quantum computers and quantum algorithms, it is important to make them secure from quantum attacks as well. In this paper, we propose a quantum-safe authentication protocol using a Post-Quantum Key Encapsulation Mechanism (PQKEM) for IoT applications in transportation systems. The protocol is built using CRYSTALS-Kyber, a lattice-based PQKEM, selected by the National Institute of Standards and Technology (NIST) in round 3 of the post-quantum standardization process. We provide a formal security proof of the proposed authentication protocol using the Real-Or-Random (RoR) model. We also present a performance analysis of the proposed authentication protocol.**

***Index Terms*—Internet of Things (IoT), key encapsulation mechanism (KEM), post-quantum cryptography (PQC), sixth-generation (6G).**

I. Introduction

The integration of the Internet of Things (IoT) into transportation systems can revolutionize mobility, offering enhanced efficiency, enhanced customer experience, and sustainability. IoT technology enables a range of innovative applications in the transportation sector such as vehicle monitoring and diagnostics, optimized route suggestions, fleet management, energy management, autonomous driving, and smart charging infrastructure [1], [2].

The sixth generation (6G) network offers ubiquitous connectivity by integrating space, air, ground, and underwater networks [3] and has the potential to redefine the future of intelligent and autonomous systems through this ubiquitous connectivity. The IoT, which connects physical things or objects to the Internet, is expected to have immense benefits in terms of quality of service, scalability, and better customer experience by converging with 6G [4].

In the IoT network, a set of IoT devices periodically send the collected data to a server through the Internet. The communication in the IoT network is susceptible to different types of attacks [5], [6]. The data may be tampered with during transmission by malicious parties [7]. There have been many studies in the literature on the attacks against IoT networks. Several authentication protocols to protect them from attacks also have been proposed in the literature. The authentication solutions based on public-key cryptography assume that it is difficult to solve hard mathematical problems such as the discrete logarithm problem and the integer factorization problem. However, with the introduction of quantum computers and certain quantum algorithms such as Shor's algorithm [8], these problems can be solved efficiently. Hence, it is essential to develop an authentication protocol that is quantum-safe. As part of the Post-Quantum Cryptography (PQC) standardization process, the National Institute of Standards and Technology (NIST) ran three rounds of evaluation, and selected CRYSTALS-Kyber [9] as a quantum-safe Key Encapsulation Mechanism (KEM) in 2022. Its security relies on the hardness of solving the learning-with-errors (LWE) problem over module lattices [10]. Kyber has reasonable key length and computation costs [11]. We propose an authentication protocol based on CRYSTALS-Kyber for IoT applications in transportation systems.

A. Related Work

We now present the related work on IoT, 6G, and transportation systems. Future IoT networks will benefit greatly from 6G [12]. A model of the IoT with 6G was presented in [13]. According to the authors, 6G will have three key aspects: mobile ultra-broadband, super IoT, and artificial intelligence. A review of machine learning algorithms that

can be used with IoT on 6G was presented in [14]. In the IoT network, the IoT devices must collect and send large amounts of data to train machine-learning models, and adversaries may modify data during transmission [7]. To solve this issue, a federated learning model for secure communication over the IoT was proposed in [7]. Banerjee et al. proposed a user-authenticated session key exchange scheme based on symmetric encryption/decryption technique for generic IoT deployment in [15]. Zhang et al. proposed an authentication scheme based on blockchain for IoT-enabled maritime transportation systems in [16]. An authentication protocol for 6G-IoT aided maritime transport system was proposed in [17]. Srinivas et al. proposed a mutual authentication protocol for IoT-based intelligent transportation systems based on elliptic-curve cryptography in [18]. Though the protocols in [15]–[18] addressed some of the security issues in IoT-based transportation systems, none of them are quantum-safe.

B. Motivation and Contributions

Combining 6G and IoT with transportation systems has the potential to transform services and user experience. To realize this potential, it is important to secure communication in IoT networks. Also, the solution should be quantum-secure to protect the communication from future attacks by an adversary equipped with robust quantum computers. Motivated by these requirements, this paper makes the following contributions:

- **A quantum-safe authentication protocol for IoT applications in 6G-enabled transportation systems:** We propose a quantum-safe authentication protocol to ensure secure data transmission in IoT applications in 6G-enabled transportation systems.
- **Protection against several attacks:** The proposed protocol provides protection against several conventional attacks. The protocol is built on the concept of post-quantum KEM to establish a session key so that it is secure against quantum attacks as well.
- **Security analysis:** We provide a formal security proof using the Real-Or-Random (RoR) model [19] and informal security analysis to demonstrate that the proposed protocol provides robust security features.
- **Performance analysis:** We provide a performance analysis of the proposed protocol to show that it is computationally efficient. We use the C/C++-based Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL) [20] for the calculation of computation cost.

II. Preliminaries

In this section, we discuss the main building block of the proposed authentication protocol, the key encapsulation mechanism.

A. Key Encapsulation Mechanism

The key encapsulation mechanism enables secure key exchange between two parties. The KEM involves three functions [9]:

Key Generation: This algorithm generates a public key and a private key pair. We denote the key generation function as $KeyGen()$. Key generation can be expressed as $(pu_k, pr_k) \leftarrow KeyGen()$.

Encapsulation: The encapsulation algorithm $Encapsulate()$ encapsulates a shared secret key k in a ciphertext c using pu_k. Encapsulation can be expressed as $(c, k) \leftarrow Encapsulate(pu_k)$.

Decapsulation: The inputs for the algorithm $Decapsulate()$ are pr_k and c. The output is the shared secret key k. Decapsulation can be expressed as $k \leftarrow Decapsulate(pr_k, c)$.

In the proposed protocol, we use the CRYSTALS-Kyber KEM, which is secure against quantum attacks, and has been selected by NIST for post-quantum cryptography standardization.

III. System and Adversary Models

A. System Model

The system model is depicted in Figure 1. Applications such as smart healthcare, smart grid, smart homes, and autonomous vehicles are connected to their respective cloud servers through the 6G communication network. The vehicles are installed with IoT devices $\{\mathcal{N}_1, \mathcal{N}_2, ...\mathcal{N}_n\}$ which send the collected data to the cloud server ($\mathcal{CS}$) through the Internet. The $\mathcal{CS}$ has sufficient resources to do computation. We also consider a trusted authority ($\mathcal{T}$) which is in charge of registering devices.

B. Adversary Model

The IoT devices send the collected data periodically to the cloud server through the insecure channel, the Internet. We consider an adversary who can control the communication channels between the IoT devices and the cloud server. The adversary may listen to the exchanged messages or modify them. The adversary may also perform a replay attack by capturing the exchanged messages and replaying them later. Further, with quantum-computing capabilities, the adversary can break the security of certain classical systems by using quantum algorithms.

IV. Proposed Authentication Protocol

We now present the quantum-safe authentication protocol. The proposed protocol consists of setup, registration, and authentication phases.

A. Setup Phase

Step 1: The cloud server $\mathcal{CS}$ generates its private key $pr_{\mathcal{CS}}$ and public key $pu_{\mathcal{CS}}$ using the $KeyGen()$ function mentioned in Section II-A.

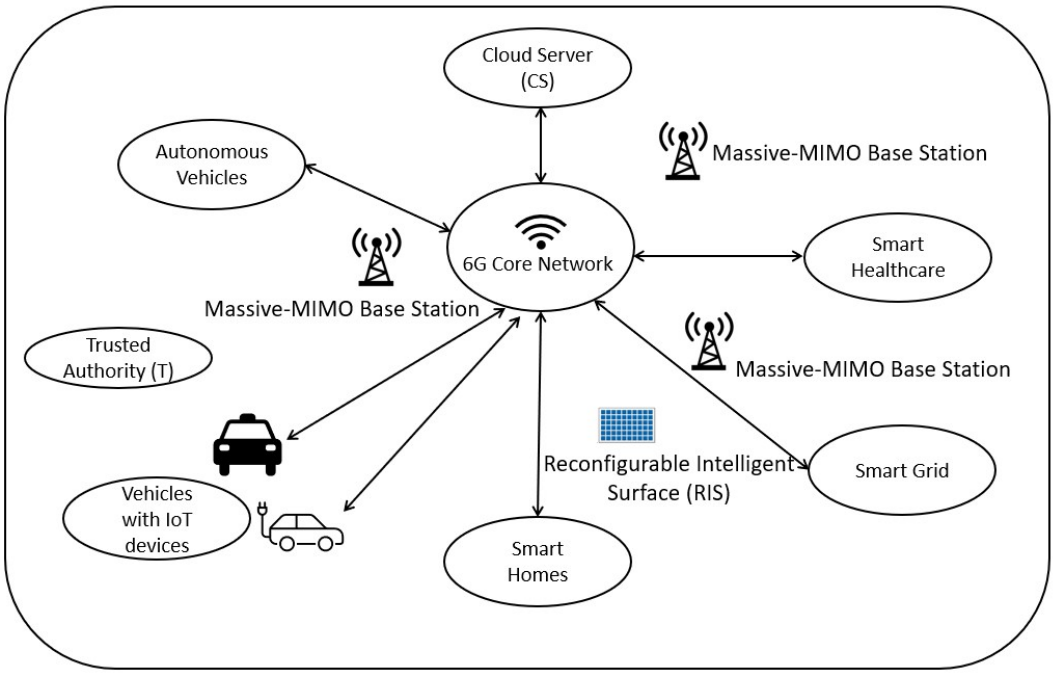

Fig. 1. System model.

B. Registration Phase

In this phase, the IoT devices $\{\mathcal{N}_1, \mathcal{N}_2, ...\mathcal{N}_n\}$ and the $\mathcal{CS}$ register with the $\mathcal{T}$.

Step 1: The $\mathcal{CS}$ composes a message with a registration request and $pu_{\mathcal{CS}}$ as $R_1 = \{Reg_{Req}, pu_{\mathcal{CS}}\}$. Then, $\mathcal{CS}$ sends R_1 to the $\mathcal{T}$ through a secure channel.

Step 2: The $\mathcal{T}$ registers the $\mathcal{CS}$.

Step 3: The IoT device $\mathcal{N}_i$ with an identity ID_{Ni} composes a message with a registration request as $R_2 = \{Reg_{Req}, ID_{Ni}\}$. Then, $\mathcal{N}_i$ sends R_2 to the $\mathcal{T}$.

Step 4: The $\mathcal{T}$ registers $\mathcal{N}_i$ and assigns it to the $\mathcal{CS}$. The $\mathcal{T}$ generates a key s_i for $\mathcal{N}_i$ and composes a message $R_3 = \{\mathcal{CS}, pu_{\mathcal{CS}}, s_i\}$. Then, the $\mathcal{T}$ sends R_3 to $\mathcal{N}_i$ through a secure channel. $\mathcal{N}_i$ stores $pu_{\mathcal{CS}}$ and s_i. The $\mathcal{T}$ also composes a message $R_4 = \{ID_{Ni}, s_i\}$ and sends R_4 to the $\mathcal{CS}$. The $\mathcal{CS}$ stores ID_{Ni} and s_i.

C. Authentication Phase

Each time before sending the data to the $\mathcal{CS}$, $\mathcal{N}_i$ and the $\mathcal{CS}$ authenticate each other and establish a session key. The steps involved in the j^{th} round of the authentication phase are given below:

Step 1: $\mathcal{N}_i$ generates a random number r_j. Then, $\mathcal{N}_i$ encapsulates a key k_j in a ciphertext c_j using $pu_{\mathcal{CS}}$ as mentioned in Section II-A. It also generates a random value sk_1, which will be used to compute the session key, and encrypts it with k_j to get $sk_1^* = Enc(sk_1)_{k_j}$. The Advanced Encryption Standard (AES) symmetric encryption is used here to encrypt sk_1. Subsequently, $\mathcal{N}_i$ computes the authentication parameter $V_1 = h(r_j \parallel k_j \parallel sk_1 \parallel s_i)$. Finally, $\mathcal{N}_i$ generates a message $A_1 = \{ID_{Ni}, c_j, r_j, V_1, sk_1^*\}$ and sends it to the $\mathcal{CS}$.

TABLE I
AUTHENTICATION PHASE

IoT Device		Cloud Server
Generate: r_j		
$(c_j, k_j) \leftarrow Encapsulate(pu_{\mathcal{CS}})$		
Generate: sk_1		
$sk_1^* = Enc(sk_1)_{k_j}$		
$V_1 = h(r_j \parallel k_j \parallel sk_1 \parallel s_i)$		
$A_1 = \{ID_{Ni}, c_j, r_j, V_1, sk_1^*\}$		
	$\xrightarrow{A_1}$	
		$k_j \leftarrow Decapsulate(c_j, pr_{\mathcal{CS}})$
		$sk_1 = Dec(sk_1^*)_{k_j}$
		Verify: V_1
		Generate: s_j
		$V_2 = h(s_j \parallel k_j \parallel ID_{Ni})$
		$SK = h(r_j \parallel s_j \parallel sk_1)$
		$A_2 = \{Ack, s_j, V_2\}$
	$\xleftarrow{A_2}$	
Verify: V_2		
$SK = h(r_j \parallel s_j \parallel sk_1)$		

Step 2: The $\mathcal{CS}$ decapsulates the key k_j from c_j using $pr_{\mathcal{CS}}$ as mentioned in Section II-A and decrypts sk_1^* with k_j as $sk_1 = Dec(sk_1^*)_{k_j}$. Next, the $\mathcal{CS}$ computes $h(r_j \parallel k_j \parallel sk_1 \parallel s_i)$ and verifies it against the received V_1. After successful verification of V_1, the $\mathcal{CS}$ generates a random number s_j. Then, the $\mathcal{CS}$ computes the authentication parameter $V_2 = h(s_j \parallel k_j \parallel ID_{Ni})$ and the session key $SK = h(r_j \parallel s_j \parallel sk_1)$. Finally, the $\mathcal{CS}$ composes a message A_2 with an acknowledgement Ack, s_j, and V_2 as $A_2 = \{Ack, s_j, V_2\}$ and sends it to $\mathcal{N}_i$.

Step 3: $\mathcal{N}_i$ computes $h(s_j \parallel k_j \parallel ID_{Ni})$ and verifies it against the received V_2. After successful verification of V_2, the session key is calculated as $SK = h(r_j \parallel s_j \parallel sk_1)$. Thus, a session key is established between $\mathcal{N}_i$ and the $\mathcal{CS}$. The steps involved in the j^{th} round of the authentication phase are given in Table I.

V. Security Analysis

In this section, we provide a formal proof of the proposed protocol using a random oracle model followed by an informal security analysis.

A. Formal Security Analysis

We use the RoR model [19] to analyze the security of the proposed protocol.

Security Model: An adversary A interacts with the $\mathcal{CS}$ and $\mathcal{N}_i$ by calling the following oracle queries:

- *Execute():* This query models a passive attack where $\mathcal{A}$ listens to the messages transmitted between the $\mathcal{CS}$ and $\mathcal{N}_i$.
- *Hash(m):* Using this query, $\mathcal{A}$ calculates the hash value of a string m.
- *Send(m):* This query simulates an active attack. Through this query, $\mathcal{A}$ can send a message m to the $\mathcal{CS}$ or $\mathcal{N}_i$ and get a response.
- *Test():* This query defines the session key's semantic security. $\mathcal{A}$ can call *Test()* query only once. When $\mathcal{A}$ executes this query, a bit b will be flipped. If $b = 1$, the actual session key is returned to $\mathcal{A}$. If $b = 0$, $\mathcal{A}$ receives a random string.

Definition 1: Let S be the event in which $\mathcal{A}$ correctly guesses b in the *Test()* query. The advantage of $\mathcal{A}$ in breaking the semantic security of the protocol ϕ is the probability of correctly guessing b. It can be written as:

$$Adv_A(\phi) = \mid 2.Pr[S] - 1 \mid .$$

If $Adv_A(\phi)$ is negligible, ϕ is secure.

Theorem 1. Let q_h represent the number of hash queries. Let $|H|$ denote the length of the hash function's output and let Adv_A^{KEM} denote A's advantage in solving the post-quantum key encapsulation mechanism. Then, the advantage of A is $Adv_A(\phi) \leq \frac{q_h^2}{|H|} + 2Adv_A^{KEM}$, which is negligible.

Proof: Consider the games G_i for $i \in \{0, 1, 2, 3\}$. In a game G_i, let $S_A^{G_i}$ denote A's success and Adv_{A,G_i} denote A's advantage, respectively. Hence, we can write that $Adv_{A,G_i} = Pr[S_A^{G_i}]$. If Adv_{A,G_i} is negligible, the protocol is secure.

Game G_0: G_0 represents a real attack by A. Since A guesses the bit b randomly in G_0, according to Definition 1, the advantage of A is:

$$Adv_A(\phi) = \mid 2Adv_{A,G_0} - 1 \mid . \tag{1}$$

Game G_1: In this game that models a passive attack, A runs the $Execute()$ query and listens to all the exchanged messages. Then, A runs the $Test()$ query. A does not have any additional advantage by doing so. Hence, G_0 and G_1 are indistinguishable and we can write that:

$$Adv_{A,G_1} = Adv_{A,G_0}. \tag{2}$$

Game G_2: In G_2, A executes $Hash(m)$ queries and send the hash outputs through $Send()$ queries to find a message digest collision. According to the birthday paradox, we can write that:

$$\mid Adv_{A,G_1} - Adv_{A,G_2} \mid \leq \frac{q_h^2}{2 \mid H \mid}. \tag{3}$$

Game G_3: The difference between G_3 and the previous games is that A uses its computing capabilities to solve the KEM in G_3. In G_3, A calls the $Execute()$ query to capture all the exchanged messages. Then, A calls the $Test()$ query. Finally, A outputs b. In the proposed protocol, the session key SK is computed as $SK = h(r_j \parallel s_j \parallel sk_1)$. To calculate SK, A must know sk_1. Before transmitting sk_1 to $\mathcal{CS}$, $\mathcal{N}_i$ encrypts sk_1 using k_j to get sk_1^* as $sk_1^* = Enc(sk_1)_{k_j}$. To extract sk_1 from sk_1^* as $sk_1 = Dec(sk_1^*)_{k_j}$, A must know k_j. However, k_j is encapsulated as $(c_j, k_j) \leftarrow Encapsulate(pu_{\mathcal{CS}})$ using the post-quantum key encapsulation mechanism. The advantage of A in breaking it is Adv_A^{KEM}. Hence, even if A runs the $Execute()$ query and captures the messages A_1 and A_2, A cannot decrypt sk_1^* to find sk_1 since A does not know k_j. Hence, we can write that:

$$\mid Adv_{A,G_2} - Adv_{A,G_3} \mid \leq Adv_A^{KEM}. \tag{4}$$

If A has executed all the above games to break the security of ϕ and has not had a successful attempt, A calls the $Test()$ query and guesses the bit b. Then, we can write that:

$$Adv_{A,G_3} = \frac{1}{2}. \tag{5}$$

Combining (1) and (2), we can write the following:

$$\begin{aligned} \frac{1}{2}Adv_A(\phi) &= \mid Adv_{A,G_0} - \frac{1}{2} \mid \\ &= \mid Adv_{A,G_1} - \frac{1}{2} \mid . \end{aligned} \tag{6}$$

Using Equations (3) to (6) and by applying the triangle inequality, we have:

$$\begin{aligned} \frac{1}{2}Adv_A(\phi) &= \mid Adv_{A,G_1} - \frac{1}{2} \mid \\ &= \mid Adv_{A,G_1} - Adv_{A,G_3} \mid \\ &\leq \frac{q_h^2}{2 \mid H \mid} + Adv_A^{KEM}. \end{aligned} \tag{7}$$

By multiplying both sides of Equation (7) by 2, we get:

$$Adv_A(\phi) \leq \frac{q_h^2}{\mid H \mid} + 2Adv_A^{KEM}. \tag{8}$$

B. Informal Security Analysis

- **Quantum Security:** The proposed protocol leverages the quantum-safe key encapsulation mechanism CRYSTALS-Kyber. The security of traditional public key cryptographic solutions is based on mathematical problems that are hard to solve by classical computers. On the contrary, the security of CRYSTALS-Kyber arises from the difficulty of solving the LWE problem over module lattices. As a result, the proposed protocol offers quantum security.
- **Protection from Eavesdropping and Man-In-The-Middle (MITM) Attacks:** The parameter sk_1 in message A_1, which is used to compute the session key, is encrypted with the encapsulated key k_j. Hence, an adversary cannot eavesdrop and modify it as he/she does not know k_j to decrypt it. Thus, the proposed protocol ensures resilience against eavesdropping and MITM Attacks.
- **Message Integrity:** If an adversary eavesdrops and modifies the parameters in the message A_1, the verification of the authentication parameter $V_1 = h(r_j \parallel k_j \parallel sk_1 \parallel s_i)$ will fail at the $\mathcal{CS}$. Similarly, any modification of the parameters in the message A_2 will result in the failure of the verification of the authentication parameter $V_2 = h(s_j \parallel k_j \parallel ID_{Ni})$ at $\mathcal{N}_i$. Thus, $\mathcal{N}_i$ and $\mathcal{CS}$ will notice any modification in the messages and the proposed protocol ensures the integrity of the exchanged messages.
- **Protection Against Replay Attacks:** The parameters r_j, c_j, and sk_1 used to compose A_1 are generated in every iteration of the protocol. Similarly, the parameter s_j used to compose A_2 is not reused. Thus, the adversary cannot replay messages and there is protection against replay attacks.
- **Authentication:** $\mathcal{N}_i$ encapsulates k_j using $pu_{\mathcal{CS}}$ to get the ciphertext c_j and composes A_1 with c_j and other parameters. Then, it sends A_1 to the $\mathcal{CS}$. Only the $\mathcal{CS}$ knows the private key, $pr_{\mathcal{CS}}$, to decapsulate k_j from c_j. Similarly, only a registered IoT device $\mathcal{N}_i$ knows the key s_i to compute the authentication parameter $V_1 = h(r_j \parallel k_j \parallel sk_1 \parallel s_i)$. Thus, a successful iteration of the protocol ensures that the IoT device is sending information to a legitimate, registered server and the server is receiving information from a legitimate IoT device.
- **Session Key Agreement:** Both $\mathcal{N}_i$ and the $\mathcal{CS}$ verify the authentication parameters to ensure that the messages are not tampered with by an adversary during message transmission. After that, a session key $SK = h(r_j \parallel s_j \parallel sk_1)$ is established between $\mathcal{N}_i$ and the $\mathcal{CS}$.

VI. Performance Analysis

In this section, first, we compare the proposed protocol with other similar protocols in terms of security features. Then, we analyze the computation cost of the proposed protocol and compare it with other protocols.

A. Comparison of Security Features

The proposed protocol offers authentication, session key agreement, protection against replay attacks, message integrity, protection from eavesdropping and MITM attacks, and post-quantum security. The protocols in [15], [17], [18] offer several security features for generic IoT deployment and IoT-enabled transportation systems. However, none of them provide post-quantum security. The proposed protocol offers conventional security features and post-quantum security by using the post-quantum key encapsulation mechanism. The key feature that sets the proposed protocol apart from other protocols is post-quantum security.

B. Computation Cost

In this subsection, we calculate the time taken by the protocol during the authentication phase and compare it with that of other similar schemes. During authentication, the IoT device executes one encapsulation, one symmetric encryption, and three hash (including the authentication parameter verification) operations. Since the time taken by the concatenation operation is negligible, we do not consider it for the computation cost calculation. The cloud server executes one decapsulation, one symmetric decryption, and three hash operations during one iteration of the authentication phase. The simulations are carried out on a personal computer with Intel (R) Core (TM) i5-11320H @3.20 GHz and 8 GB of RAM. To calculate the time required to execute various cryptographic operations, we use MIRACL [20]. We use AES-256 for the encryption and decryption operations. From the simulations, the total computation cost during authentication is 1.2726 ms.

Next, we compare the execution time of the proposed protocol with that of other protocols. We consider protocols in [15], [17], [18] for the comparison. Let T_{epm}, T_h, T_{ed}, T_{fe}, T_{eca}, $T_{encap/decap}$ represent the time taken by elliptic curve point multiplication, hash, symmetric encryption/decryption, fuzzy extractor, elliptic curve point addition, and encapsulation/decapsulation operations, respectively. From the analysis, T_{epm} = 0.3211 ms, T_h = 0.0144 ms, T_{ed} = 0.072 ms, T_{fe} = 0.401 ms, T_{eca} = 0.0019 ms, and $T_{encap/decap}$ = 0.5211 ms. The computation costs of protocols in [15], [17] and [18] are summarised in Table II. We have also plotted the graph for computation costs of various schemes in Figure 2. From the graph, the computation cost of the proposed protocol is reasonable.

TABLE II
Computation Cost

Scheme	Computation Cost (ms)
Banerjee et al. [15]	$T_{fe} + 19T_h + 10T_{ed} \approx 1.3946$ ms
Chaudhry et al. [17]	$13T_h + 7T_{ed} \approx 0.6912$ ms
Srinivas et al. [18]	$T_{fe} + 3T_h + 11T_{epm} + 2T_{eca} \approx 3.9801$ ms
Proposed Protocol	$2T_{encap/decap} + 2T_{ed} + 6T_h \approx 1.2726$ ms

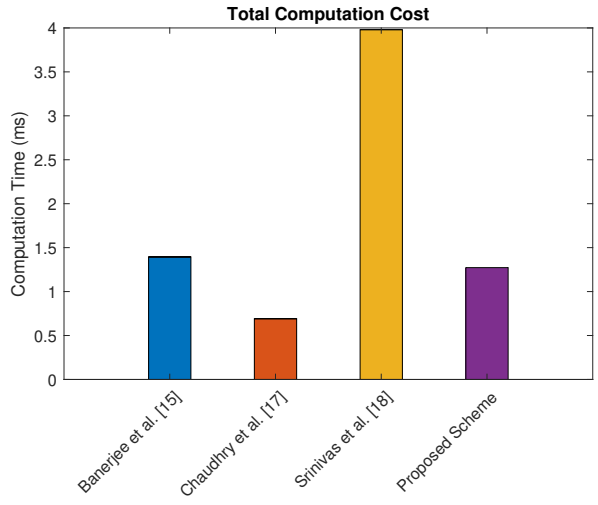

Fig. 2. Comparison of computation cost.

VII. Conclusion

In this paper, we proposed a quantum-safe authentication protocol using a post-quantum key encapsulation mechanism for IoT applications in 6G-enabled transportation systems. The proposed protocol provides protection against several attacks including quantum attacks. We have also provided a performance analysis of the protocol. We compared the proposed protocol with other protocols and the comparison shows that the proposed protocol offers better security features than the other protocols. The proposed protocol shows the feasibility of using post-quantum key encapsulation mechanisms in IoT applications in transportation systems to make them quantum-safe.

VIII. Acknowledgement

This research is supported by the National Research Foundation, Singapore and A*STAR under its Quantum Engineering Programme (National Quantum-Safe Network, NRF2021-QEP2-04-P01).

References

[1] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A review of machine learning and iot in smart transportation," *Future Internet*, vol. 11, no. 4, p. 94, 2019.

[2] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, and K.-C. Wang, "Review of internet of things (iot) in electric power and energy systems," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 847–870, 2018.

[3] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji, and V. C. Leung, "Enabling massive iot toward 6g: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 11 891–11 915, 2021.

[4] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, and H. V. Poor, "6g internet of things: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 359–383, 2021.

[5] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 580–589, 2018.

[6] N. A. Khan, A. Awang, and S. A. A. Karim, "Security in internet of things: A review," *IEEE access*, vol. 10, pp. 104 649–104 670, 2022.

[7] Y. Qu, C. Xu, L. Gao, Y. Xiang, and S. Yu, "Fl-sec: Privacy-preserving decentralized federated learning using signsgd for the internet of artificially intelligent things," *IEEE Internet of Things Magazine*, vol. 5, no. 1, pp. 85–90, 2022.

[8] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.

[9] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-kyber: a cca-secure module-lattice-based kem," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2018, pp. 353–367.

[10] "CRYSTALS-Kyber Algorithm," Online,https://www.ibm.com/docs/en/zos/2.5.0?topic=cryptography-crystals-kyber-algorithm, [Accessed: Jan 2024].

[11] M. Kumar and P. Pattnaik, "Post quantum cryptography (pqc)-an overview," in *2020 IEEE High Performance Extreme Computing Conference (HPEC)*. IEEE, 2020, pp. 1–9.

[12] Z. Qadir, K. N. Le, N. Saeed, and H. S. Munawar, "Towards 6g internet of things: Recent advances, use cases, and open challenges," *ICT Express*, vol. 9, no. 3, pp. 296–312, 2023.

[13] L. Zhang, Y.-C. Liang, and D. Niyato, "6g visions: Mobile ultra-broadband, super internet-of-things, and artificial intelligence," *China Communications*, vol. 16, no. 8, pp. 1–14, 2019.

[14] M. R. Mahmood, M. A. Matin, P. Sarigiannidis, and S. K. Goudos, "A comprehensive review on artificial intelligence/machine learning algorithms for empowering the future iot toward 6g era," *IEEE Access*, vol. 10, pp. 87 535–87 562, 2022.

[15] S. Banerjee, V. Odelu, A. K. Das, J. Srinivas, N. Kumar, S. Chattopadhyay, and K.-K. R. Choo, "A provably secure and lightweight anonymous user authenticated session key exchange scheme for internet of things deployment," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8739–8752, 2019.

[16] P. Zhang, Y. Wang, G. S. Aujla, A. Jindal, and Y. D. Al-Otaibi, "A blockchain-based authentication scheme and secure architecture for iot-enabled maritime transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2322–2331, 2022.

[17] S. A. Chaudhry, A. Irshad, M. A. Khan, S. A. Khan, S. Nosheen, A. A. AlZubi, and Y. B. Zikria, "A lightweight authentication scheme for 6g-iot enabled maritime transport system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2401–2410, 2021.

[18] J. Srinivas, A. K. Das, M. Wazid, and A. V. Vasilakos, "Designing secure user authentication protocol for big data collection in iot-based intelligent transportation system," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7727–7744, 2020.

[19] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Public Key Cryptography-PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005. Proceedings 8*. Springer, 2005, pp. 65–84.

[20] "MIRACL Cryptographic SDK," Online,https://github.com/miracl/MIRACL, [Accessed: Jan 2024].